Genetec™ Security Center.

Guia de Administrador do Security Center 5.7

Clique aqui para obter a versão mais recente deste documento.

7 de maio de 2019

Genetec™

Avisos legais

Informação do documento

Título do documento: Guia de Administrador do Security Center 5.7

Número do documento: PT.500.003-V5.7.C5(1)

Data de atualização do documento: 7 de maio de 2019

Você pode enviar comentários, correções e sugestões sobre este guia para documentation@genetec.com.

Sobre este guia

Este guia apresenta as informações de que você precisa para instalar e configurar o seu sistema Security Center. Ele explica as configurações básicas que você precisa definir antes que o seu sistema possa ser usado, bem como outras configurações que você deverá alterar, como incluir usuários e recursos (servidores) adicionais em seu sistema.

Notas e avisos

As notas e os avisos a seguir podem aparecer neste guia:

- **Dica:** Sugere como aplicar as informações em um tópico ou em uma etapa
- **Observação:** Explica um caso especial ou abrange mais de um ponto importante.
- **Importante:** Aponta informações vitais sobre um tópico ou uma etapa.
- **Cuidado:** Indica que uma ação ou etapa pode causar perda de dados, problemas de segurança ou de desempenho.
- **Alerta:** Indica que uma ação ou etapa pode causar danos físicos ou danificar o hardware.

IMPORTANTE: Os tópicos neste guia que se referem a informações encontradas em sites de terceiros eram precisas no momento da publicação, porém estão sujeitas a alteração sem aviso prévio da Genetec Inc..

Conteúdo

Prefácio: Prefácio

Avisos legais ii
Sobre este guia iii

Introdução ao Security Center

Capítulo 1: O Security Center em um relance

Sobre o Security Center 3
Visão geral da arquitetura do Security Center 5
Como o Security Center é organizado 6
Fazer logon no Security Center através do Config Tool 7
Fazer logon usando autenticação passiva 9
Fechar Config Tool 12
Definir como o seu espaço de trabalho é salvo 12
Visão geral da página inicial 13
Visão geral da página Sobre 15
Visão geral do espaço de trabalho das tarefas de administração 17
Comandos contextuais em tarefas de administração 18
Visão geral do espaço de trabalho de manutenção 21
Sobre a exibição de área 23
Acerca de áreas 25
Organizar a exibição de área 26
Criar áreas 27
Ligar e desligar recursos 28
Configurar a bandeja de notificação 29
Ícones da bandeja de notificação 29
Mudar senhas 31
Abrir o Security Desk pelo Config Tool 32
Enviar feedback 33
Coletando dados de diagnóstico 34
Atalhos para ferramentas externas 36

Capítulo 2: Tarefas

Abrir tarefas 39
Salvar tarefas 40
Organização das tarefas salvas 42
Adicionar tarefas em sua lista Favoritos lista 43
Ocultar as Favoritos e Itens recentes listas da sua página inicial 43
Enviar tarefas 44
Mover a barra de tarefas 45
Personalizar comportamento de tarefas 46

Capítulo 3: Relatórios

Sobre os relatórios visuais 48
Gerar relatórios 53

Exportar relatórios gerados 54
Imprimir relatórios gerados 54
Personalizar configurações de fuso horário 55
Gerar relatórios visuais 57
Gerando e salvando relatórios 60
Personalizar o painel de relatório 61
Personalizar o comportamento dos relatórios 62
Sobre a função do Report Manager 63
Configurar resultados máximos para relatórios automatizados 64

Capítulo 4: Atalhos de teclado

Atalhos padrão no teclado 66
Personalizar atalhos de teclado 68

Administração comum do Security Center

Capítulo 5: Entidades

Sobre entidades 71
Entidades criadas automaticamente no Security Center 72
Alterar ícones de entidade 73
Configuração de locais geográficos de entidades 74
Pesquisar por entidades 75
Pesquisando por entidades usando a ferramenta de pesquisa 75
Copiar definições de configuração de uma entidade para a outra 77
Ajustar configurações copiadas para cada entidade usando a ferramenta de Copiar Configurações 77
Atribuir IDs lógicos a entidades 81
Modificar IDs lógicos 81
Customizar como as entidades são exibidas na tela 82
Excluir entidades 83
Estados de entidades 84
Solução de problemas: entidades 85
Sobre campos personalizados 86
Criar tipos de dados personalizados para campos personalizados 87
Editar tipos de dados personalizados 87
Criar campos personalizados 88
Sobre a Ferramenta de registro de unidades 90
Definir configurações de registro de unidades 90
Descobrir unidades em sua rede 90
Adicionar unidades 91
Limpar unidades adicionadas 91
Ignorar unidades 92
Removendo unidades de listas de unidades ignoradas 92
Visualizar propriedades das unidades 93
Colunas do painel de relatórios para a tarefa Inventário de hardware 93
Reativar a autenticação de acesso básica 94
Personalizar o comportamento do Security Center ao renomear unidades de hardware 96

Capítulo 6: Servidores e funções

Sobre servidores 98

Abrir o Server Admin usando um navegador da Web 99
Server Admin - Página de visão geral 101
Server Admin - Página do servidor principal 104
Server Admin - Página Servidor de expansão 107
Adicionando Servidores de Expansão 109
Converter o servidor principal em um servidor de expansão 110
Converter um servidor de expansão em servidor principal: 111
Conectar servidores de expansão ao servidor principal 112
Ativar sua licença do Security Center usando a Web 115
Ativar licenças do Security Center sem acesso à Internet 118
Reaplicar sua licença do Security Center 123
Substituir o servidor principal 129
Sobre funções 132
Mover funções para outros servidores 133
Desativar e ativar funções 134
Sobre a função Directory 135
Sobre Web-based SDK 136

Capítulo 7: Bancos de dados e redes

Bancos de dados 138
Mover bancos de dados para outros computadores 139
Conectar funções a servidores de bancos de dados remotos 140
Garantindo as permissões do SQL Server 142
Restringir a memória alocada a servidores de bancos de dados 143
Criar bancos de dados 144
Excluir bancos de dados 145
Atualizar o banco de dados do Security Center Directory 146
Compactar bancos de dados do Security Center após uma atualização 148
Visualizar informações do banco de dados 149
Receber notificações quando os bancos de dados estão quase cheios 150
Fazer backup de bancos de dados 151
Fazer backup de bancos de dados segundo uma agenda 152
Restaurar bancos de dados 153
Sobre redes 154
Sobre a exibição de rede 156
Adicionar redes 157
Criar conexões diretas entre redes 157
Personalizando opções de rede 159

Capítulo 8: Alta disponibilidade

Sobre os recursos de alta disponibilidade no Security Center 161
Failover de função 162
Funções com suporte a failover 163
Configurar failover de função 165
Alterar a prioridade do servidor para failover de funções 165
Failover e balanceamento de carga de Directory 167
Preparar failover e balanceamento de carga do Directory 168
Configurar failover e balanceamento de carga do Directory 169
Forçando um servidor do Directory a sempre ser o servidor principal 169

Configurar um servidor do Directory para recuperação de desastres 170
Alternar o servidor principal 171
Reativar a licença do Security Center para sistemas com failover do Directory 172
Reativar a licença do Security Center usando um arquivo de licença 173
Removendo servidores da lista de failover do Directory. 177
Ignorar o balanceamento de carga em estações de trabalho 178
Failover de banco de dados do Directory 179
Configurar failover do banco de dados do Directory por backup e restauração 181
Gerando backup completo do banco de dados do Directory 182
Configurar failover do banco de dados do Directory por espelhamento 183
Configurar failover de banco de dados do Directory através do SQL AlwaysOn 185
Failover do Archiver 186
Configurar failover do Archiver 188
Alterar a prioridade dos servidores para failover do Archiver 188
Atribuir prioridades de arquivamento para servidores em espera 189
Configurar um período de retenção diferente para o servidor de Archiver secundário 191
Gerar o arquivo Archiver.gconfig 191
Consolidar arquivos de vídeo após failover do Archiver 193
Solução de problemas do failover 195

Capítulo 9: Automação do sistema

Sobre agendamentos 197
Sobre agendas vespertinas 197
Criando agendamentos 199
Definir agendas diárias 199
Definir agendas semanais 200
Definir agendas ordinais 201
Definir agendas com datas específicas 202
Definir agendas vespertinas 203
Sobre eventos 205
Atribuir cores a eventos 206
Criar eventos personalizados 207
Criar eventos causa-efeito 208
Adicionar condições ao criar eventos causa-efeito para eventos de análise de vídeo 209
Elementos usados em condições de evento causa-efeito para eventos de análise de vídeo 211
Adicionar condições ao criar eventos causa-efeito para reconhecimento de placas de veículos 213
Elementos usados em condições de evento causa-efeito para leituras de placas de veículos 215
Modificar eventos causa-efeito 217
Tarefas agendadas 218
Agendar tarefa 219
Adicionar arquivos de áudio 220
Sobre macros 221
Criar macros 222

Capítulo 10: Federation

Sobre o recurso Federation 224
Sobre entidades federadas 225
Configurar uma Security Center Federation 228
Configurar uma Omnicast Federation 229

Usar configurações padrão do Security Desk para exibir câmeras federadas 231
Exigências para grandes sistemas Federation 232
Adicionar grupos de funções Federation 234

Capítulo 11: Mapas

Como trabalhar com mapas no Security Center 237
Instalar a solução de mapeamento BeNomad 238
Configurar a função Map Manager 239
Conectar a função Map Manager ao provedor de mapas ESRI ArcGIS 240
Conectar a função Map Manager a provedores de mapas baseados na Web 241
Exemplos de formatos de URL para provedores de mapas baseados na Web 242
Criar mapas 244
Configurar predefinição de mapa 244
Configurando informações padrão para exibição em mapas 245
Ajustar a opacidade das informações exibidas em mapas 246
Configurar objetos de mapa que se movem 246
Criar mapas a partir de arquivos de imagem 248
Georreferenciar uma imagem de mapa 250
Configurar a escala de uma imagem de mapa importada 251
Criar mapas por conexão a um GIS 253
Visão geral da tarefa Map designer 255
Objetos de mapa suportados 257
Adicionar objetos de mapa aos seus mapas 263
Adicionar unidades de controle de acesso aos seus mapas 264
Adicionar áreas aos seus mapas 265
Adicionar áreas como miniaturas de mapa em seus mapas 265
Adicionar áreas para contagem de pessoas em seus mapas 266
Adicionar texto, imagens e formas aos seus mapas 267
Adicionar portas aos seus mapas 268
Adicionar câmeras aos seus mapas 269
Desenhar paredes para bloquear o campo de visão de suas câmeras 270
Adicionar sequências de câmeras aos seus mapas 272
Adicionar layouts aos seus mapas 273
Adicionar câmeras LPR aos seus mapas 274
Adicionar alarmes aos seus mapas 275
Adicionar áreas de detecção de intrusão em seus mapas 276
Adicionar unidades de detecção de intrusão e entidades relacionadas em seus mapas 277
Adicionar zonas aos seus mapas 278
Adicionar pinos de entrada aos seus mapas 279
Adicionar relés de saída aos seus mapas 280
Adicionar objetos KML aos seus mapas 281
Adicionar macros aos seus mapas 282
Configurar opções de agrupamento de mapas no Security Center 283

Capítulo 12: Plug-ins

Sobre plug-ins 285
Sobre plug-ins de ladrilho 286
Criar plug-ins de ladrilho ligados a um website 287
Criar plugins de janela ligados a um arquivo executável 288

Capítulo 13: Monitoramento da saúde do sistema

Sobre monitoramento da saúde do sistema . . . 290
Sobre a função do Monitor de Saúde . . . 293
Redefinir o banco de dados do Health Monitor. . . . 294
Selecionar eventos de saúde a serem monitorados . . . 295
Definir entidades para modo de manutenção . . . 296
Habilitar eventos para câmeras em modo de manutenção . . . 297
Definir aplicativos clientes Security Center para o modo de manutenção . . . 299
Visualizar mensagens do sistema . . . 300
Visualizar eventos de saúde do sistema . . . 302
Colunas do painel de relatório para a tarefa Histórico de saúde do sistema . . . 303
Visualizar o estado de saúde e a disponibilidade de entidades . . . 304
Colunas do painel de relatório para a tarefa Estatísticas de saúde do sistema . . . 304
Monitorar recursos do seu computador . . . 306
Caixa de diálogo Informações de hardware . . . 306
Utilizar a ferramenta de parâmetro de comparação de hardware . . . 308
Visão Geral da tarefa de Status do sistema 264 . . . 310
Colunas da tarefa Status do sistema . . . 310
Monitorar o status do seu sistema Security Center . . . 316

Capítulo 14: Auditorias do sistema

Investigar atividades relacionadas a usuários no seu sistema Security Center . . . 319
Colunas de relatório para a tarefa Rastreio de atividades . . . 322
Configurar registro de eventos para sequências de vídeos . . . 323
Descobrindo quais mudanças foram feitas na configuração do sistema . . . 324
Colunas de relatório para a tarefa Rastreio de auditoria . . . 324
Alterações de configuração registradas pelo sistema Security Center . . . 325
Alterações de propriedades registradas com os valores antes e depois . . . 327

Capítulo 15: Web Client Server

Sobre Web Client Servers . . . 334
Criar Web Client Servers . . . 335
Configurar Web Client Servers . . . 337

Segurança do sistema

Capítulo 16: Introdução à segurança do sistema

Definir quem pode acessar o Security Center . . . 340
Proteger seu data center contra ameaças externas . . . 341

Capítulo 17: Partições

Sobre partições . . . 344
Criar partições . . . 345
Atualizar o conteúdo das partições . . . 346
Conceder direitos de acesso para as partições . . . 348

Capítulo 18: Usuários e Grupos de usuários

Sobre grupos de usuários . . . 350
Criando grupos de usuários . . . 351

Adicionar grupos de usuários subordinados 351
Adicionar usuários como membros de grupos de usuários 352
Sobre usuários 353
Criando usuários 355
Definir configurações de usuários 356
Desativar perfis de usuários 356
Alterar configurações de senhas para usuários 358
Sobre privilégios 359
Modelos de privilégios 361
Atribuir privilégios a usuários 362
Personalizar opções de logon de usuário 365
Forçando o Security Desk a ser executado no modo de tela cheia 367
Configurar o Security Desk para iniciar no modo de tela cheia em estações de trabalho . . 367
Selecionar quais estações de trabalho os usuários podem controlar remotamente 369
Selecionar quais atividades de usuários registrar 370

Capítulo 19: TLS e Autenticação no Directory

O que é o protocolo Transport Layer Security? 372
O que é a autenticação do diretório? 373
Alterar a configuração de autenticação no Directory 376
Desabilitar compatibilidade com versões anteriores 377
Substituir certificados padrão 378
Criar solicitações de certificados personalizadas para o Security Center 379

Capítulo 20: Integração do Active Directory

Integração com o Active Directory do Windows 384
Sincronização do Active Directory 386
Sobre grupos Universais e catálogos globais 388
Importar grupos de segurança de um Active Directory 389
Mapear campos personalizados para sincronizar com o Active Directory 392
Resolver conflitos causados por entidades importadas 393
Desativar usuários importados de um Active Directory 394
Atributos de catálogo global 395

Capítulo 21: Autenticação baseada em declarações

O que é a autenticação baseada em declarações? 398
Implementar autenticação baseada em declarações pelo ADFS 400
Adicionando confiança a um provedor de reivindicações para um ADFS de terceiros 403
Configuração de regras de reivindicações para um provedor de reivindicações de terceiros . . . 405
Adicionar uma parte confiável para o Security Center 406
Configurar regras de declaração para o Security Center 411
Mapear grupos ADFS remotos para o Security Center 412
Criar Active Directory Federation Services 413

Capítulo 22: Criptografia de transmissão de fusão

O que é a criptografia de transmissão de fusão? 417
Como a criptografia de transmissão de fusão funciona? 419
Cenários de criptografia de transmissão de fusão 420
Impacto no desempenho da criptografia de transmissão de fusão 422
Boas práticas para gerenciamento de chaves privadas 423

Configurar criptografia de transmissão de fusão 425
Solicitando e instalando certificados de criptografia 425
Habilitar a criptografia de transmissão de fusão 426
Desabilitar a criptografia de transmissão de fusão 428
Impedir que usuários visualizem dados criptografados em uma máquina específica 429
Impedir o uso de certificados comprometidos no seu sistema 430
Autorizar um cliente a visualizar novos dados de uma câmera criptografada 431
Autorizar um novo cliente a visualizar todos os dados de uma câmera criptografada 432
Removendo a criptografia de arquivos de vídeo 433

Vídeo

Capítulo 23: Vídeo em um relance

Sobre Security Center Omnicast 436
Entidades relacionadas à vigilância por vídeo 437

Capítulo 24: Implantação de vídeo

Preparar a implementação de seu sistema de vigilância por vídeo 439
Implementar seu sistema de vigilância por vídeo 441
Sobre Archivers 442
Configurar funções Archiver 443
Mover a função Archiver para outro servidor 444
Sobre unidades de vídeo 446
Adicionar unidades de vídeo manualmente 447
Definição das configurações padrão de câmeras 449
Definir configurações de gravação de câmeras 451
Configurar codecs de áudio 453
Visualizar estados de gravação de câmeras 454
Investigar eventos do Archiver 455
Colunas de relatório para a tarefa Eventos do Archiver 455
Sobre Archivers auxiliares 456
Diferenças entre Archivers e Archivers auxiliares 456
Criar Archivers auxiliares 458
Adicionando câmeras a Archivers auxiliares 459
Removendo câmeras de Auxiliary Archivers 459
Definindo configurações de gravação de câmera para um Archiver auxiliar 460
Sobre o Media Router 462
Configurar a função Media Router 463
Adicionar redirecionadores ao Media Router 464
Configurar o uso de placas de rede para um redirecionador 465
Sobre o Media Gateway 469
Criar a função Media Gateway 470
Configurar a função Media Gateway para receber solicitações de vídeo 471
Limitar conexões ao Media Gateway 472

Capítulo 25: Câmeras

Sobre as câmeras (codificadores de vídeo) 474
Sobre transmissões de vídeo 474
Definição das configurações de câmera 475
Configurar transmissões de vídeo de câmeras 477

Aumentar a qualidade de gravação de vídeo em eventos importantes 479
Aumentar a qualidade de gravação de vídeo manualmente 479
Alterar endereços multicast de câmeras 481
Alterar portas multicast de câmeras 482
Testar configurações de transmissão de vídeo de câmeras 483
Sobre a detecção de movimento 485
Configuração da detecção de movimento 487
Calibrar automaticamente a sensibilidade da detecção de movimento 488
Definir zonas de detecção de movimento 488
Selecionar quais eventos são acionados por movimento 489
Teste de configurações de detecção de movimento 490
Ajustar configurações de cor da câmera 492
Sobre a proteção de privacidade 493
Configurar proteção de privacidade 495
Acessar vídeos confidenciais usando cartões inteligentes 499
Sobre rastreamento visual 500
Configurar o rastreamento visual 501
Visualizar configurações de câmeras 502
Configurar motores PTZ 504
Calibrar coordenadas PTZ 504
Teste de controles PTZ 505
Widget PTZ 506
Definir níveis de usuário para controlar motores PTZ 508
Sobre sequências de câmeras 509
Criar sequências de câmeras 510
Sobre monitores analógicos 511
Configurar monitores analógicos 512
Adicionar monitores analógicos como destinatários de alarmes 512
Testar configurações de monitores analógicos 513
Câmeras usadas junto ao corpo 514
Configurar câmeras usadas junto ao corpo 515
Adicionar câmeras ou usuários à função Body-Worn Camera Manager 517

Capítulo 26: Arquivos de vídeos

Sobre arquivos de vídeos 520
Banco de dados de arquivos 520
Armazenamento de arquivos 520
Gerenciar arquivos de vídeos 522
Distribuir o armazenamento de arquivos por múltiplos discos 523
Monitorar o espaço em disco disponível para arquivos de vídeo 524
Liberando espaço de armazenamento para arquivos de vídeo 525
Transferir arquivos de vídeo 527
Recuperar gravações de vídeo das unidades 528
Ativar a gravação avançada 528
Definir configurações de transferência de vídeo para câmeras 529
Duplicar arquivo de vídeos 530
Fazer backup de arquivos de vídeos segundo uma agenda 532
Ignorar agendas de transferência de arquivos 533
Transferir arquivos de vídeos sob demanda 534

Restaurar arquivos de vídeo 535
Status e detalhes de transferência de arquivos 536
Proteger arquivos de vídeo contra exclusão 537
Proteção de arquivos de vídeo contra adulteração 539
Configurar uma chave de criptografia para marcas d'água de vídeo 539
Exibir propriedades de arquivos de vídeo 540
Colunas de relatório para a tarefa Detalhes de armazenamento do arquivo 541
Gerenciar os efeitos do Horário de Verão em arquivos de vídeo 542
Efeitos da hora atrasada 542
Efeitos da hora adiantada 542
Mudar o fuso horário para UTC 543
Importar arquivos de vídeo externos para o Security Center 544

Capítulo 27: Solução de problemas de vídeo

Mover unidades de vídeo para um Archiver diferente 548
Troca de unidades de vídeo 549
Atualizar o firmware da unidade de vídeo 551
Localizar arquivos órfãos em seu sistema 552
Localizar arquivos ausentes em seu sistema 554
Solução de problemas: problemas com a transmissão de vídeo 556
Optimizar o desempenho do decodificador de vídeo no seu computador 557
Não está sendo gravado vídeo 558
Solução de problemas de unidades de vídeo offline no Security Center 559
Executar rastreamentos de rede 560
Solução de problemas: erros "Impossível estabelecer sessão de vídeo com o servidor" 562
Impossível assistir vídeo ao vivo no Security Desk 563
Impossível assistir a reprodução de vídeo no Security Desk 565
Solução de problemas: As câmeras não estão gravando 566
Solução de problemas: Não é possível adicionar unidades de vídeo 569
Solução de problemas: Não é possível excluir unidades de vídeo 572
Solução de problemas: problemas com a transmissão de vídeo H.264: 573
Solução de problemas: problema de sensibilidade da câmera Axis P1428-E 574
A detecção de movimento não está funcionando no Security Center 575
Câmeras Axis não têm uma aba de Detecção de movimento 576
Configurar o Security Center para abrir vídeo ao vivo rapidamente 577
A proteção de privacidade não está a funcionar no Security Center 578
Erros de arquivos de configuração de câmeras usadas junto ao corpo 579
Avisos de conversão para câmeras usadas junto ao corpo 582
Failover está configurado no Archiver para câmeras usadas junto ao corpo 584
A porta de câmera usada junto ao corpo já está em uso 586
O relatório Arquivos de câmera usada junto ao corpo está vazio 587

Controle de acesso

Capítulo 28: Controle de acesso em um relance

Sobre o Security Center Synergis 590
Entidades relacionadas ao controle de acesso 592

Capítulo 29: Implantação do controle de acesso

Preparar a instalação do seu sistema de controle de acesso 594

Implantar seu sistema de controle de acesso 596
Implementar seu sistema de controle de acesso com vídeo 597
Sobre o Access Manager 598
Configurar funções do Access Manager 599
Adicionar extensões de unidades de controle de acesso 601

Capítulo 30: Unidades de controle de acesso

Sobre unidades de controle de acesso 603
Sobre a sincronização de unidades 604
Como as unidades de controle de acesso funcionam 605
Preparar a adição de unidades de controle de acesso HID 606
Adicionar unidades de controle de acesso 608
Definir configurações da unidade de controle de acesso 609
Inscrição automática de unidades de controle de acesso 610
Redefinir o certificado confiável 610
Habilitar a supervisão de leitores no HID VertX 611
Ativar dispositivos de controle de acesso externos 612

Capítulo 31: Áreas, portas e elevadores

Sobre portas 614
Criar portas 616
Mapear entidades de porta a ligações físicas de porta 617
Ligar câmeras a portas 618
Selecionar quem tem acesso a portas 619
Sobre elevadores 620
Diferenças entre unidades HID e Synergis em controle de elevadores 622
Criar elevadores 624
Selecionar o comportamento do relé de saída para andares de elevadores 625
Mapear a fiação de andares físicos de elevadores para entidades de elevador 626
Vincular câmeras a elevadores 627
Selecionar quem tem acesso a elevadores 628
Boas práticas para configurar exceções de acesso controlado 628
Sobre áreas protegidas 629
Configurar áreas protegidas 631
Adicionar portas a áreas 632
Aplicar anti-passback a áreas 633
Habilitar anti-passback global em funções do Access Manager 634
Definir limites de ocupação de área 635
Intertravar portas dentro de áreas 636
Fiscalizar uma presença de supervisão em áreas protegidas 637
Exigir que os visitantes sejam escoltados para acessar áreas protegidas não ANSSI 638
Configurar acompanhamento de visitantes para catracas conforme a ANSSI 639
Habilitar PIN de dureza 642
Sobre regras de acesso 643
Criar regras de acesso 644

Capítulo 32: Titulares de cartão

Sobre os titulares de cartão 646
Criar grupos de titulares de cartão 647
Criando titulares de cartão 648

Atribuir regras de acesso a titulares de cartão 650
Atribuindo regras de acesso temporárias a titulares de cartão 651
Cortar imagens 653
Aplicar fundos transparentes a imagens 654
Definir o tamanho máximo de arquivos de imagem 656
Atribuição de credenciais 657
Solicitar cartões de credencial 660
Impressão de credenciais em papel 661
Configurar estações de codificação de smart cards 663
Configurar perfis de credencial móvel 665
Modificar titulares de cartão importados de um Active Directory 667
Atribuir imagens a titulares de cartão importados. 667
Modificar o status de titulares de cartão importados 667
Selecionar quais campos do titular de cartão sincronizar com o Active Directory 669
Utilizar coletores de assinatura 670
Receber notificações quando os portadores de cartão estiverem para expirar 671

Capítulo 33: Credenciais

Sobre credenciais 674
Métodos de inscrição de credenciais 677
Registrar várias credenciais automaticamente 678
Inscrição de várias credenciais manualmente 680
Criar credenciais 682
Adicionar motivos para solicitações de cartão de credencial 686
Responder a solicitações de cartão de credencial 687
Como os formatos de cartão de credenciais funcionam com o Active Directory no Security Center . 688
Formatos de cartão personalizados 689
Ferramenta de edição de formato de cartão personalizado 690
Criar formatos de cartão personalizados 691
Definir campos ABA 692
Definir campos Wiegand 693
Adicionando verificações de paridade 694
Projetar modelos de crachá 695
Pré-visualizar impressões de modelos de crachá 698

Capítulo 34: Gerenciamento global de titulares de cartão

Gerenciamento global de titulares de cartão 700
Arquitetura de Gerenciamento global de titulares de cartão 700
Diferenças entre Federation e GCM 702
Diferenças entre integração do Active Directory e GCM 703
Sobre Global Cardholder Synchronizers 704
Regras e restrições do Gerenciamento global de titulares de cartões 705
Preparar para sincronizar entidades entre locais 708
Sincronizar entidades entre locais 709
Configurar partições para sincronização 709
Sincronização do seu sistema com a hospedagem de compartilhamento 709
Compartilhar entidades com outros locais 711
Interromper o compartilhamento de entidades com outros locais 711
Ignorar status sincronizados de titulares de cartão 712

Capítulo 35: Ferramenta de importação

Sobre a Ferramenta de importação 714
Arquivos CSV e a ferramenta de importação 715
Notas sobre nomes de entidades importadas 717
Importar titulares de cartão e credenciais 718
Substituir credenciais 721
Substituir grupos de titulares do cartão 722
Campos do banco de dados suportados pela ferramenta de importação 724

Capítulo 36: Teste do sistema de controle de acesso

Ferramenta Solução de problemas de acesso 728
Testar regras de acesso em portas e elevadores 729
Identificação de indivíduos que têm acesso a portas e elevadores 730
Colunas do painel de relatórios para a tarefa Solução de problemas de porta 730
Identificação de indivíduos que têm acesso concedido/negado nos pontos de acesso 731
Colunas de relatório para a tarefa Direitos de acesso dos titulares de cartão 731
Testar direitos de acesso de titulares de cartão 733
Teste de direitos de acesso de titular de cartão com base em credenciais 733
Exibir propriedades de credencial de titulares de cartão 734
Colunas do painel de relatórios para a tarefa Configuração de credenciais 734
Visualizar propriedades de membros de grupos de titulares de cartão 736
Colunas de relatório para a tarefa Configuração de titulares de cartão 737
Identificação de quais entidades são afetadas pelas regras de acesso 738
Colunas de relatório para a tarefa Configuração da regra de acesso 738
Visualizar a configuração de E/S de unidades de controle de acesso 739
Colunas de relatório para a tarefa Configuração de E/S 739

Capítulo 37: Solução de problemas de controle de acesso

Visualizar eventos de saúde de controle de acesso 741
Colunas de relatório para a tarefa Histórico de saúde de controle de acesso 741
Investigar eventos relacionados a unidades de controle de acesso 742
Colunas de relatório para a tarefa Eventos da unidade de controle de acesso 742
Mover unidades de controle de acesso para um Access Manager diferente 743
Preparar para substituir uma unidade de controle de acesso 744
Substituir unidades de controle de acesso 745
Atualizar firmware de unidade de controle de acesso 747
Habilitar ou desabilitar registros de suporte para unidades de controle de acesso 750
Solução de problemas: problemas de descoberta e inscrição de unidade HID 751
Solução de problemas: unidades HID não podem ser descobertas 751
Solução de problemas: unidades HID não podem ser inscritas 752
Solução de problemas: muitas solicitações para eventos de saída de portas 754
Solução de problemas: Credenciais não funcionam 755
Solução de problemas: Os cartões não funcionam nos leitores 756
Solução de problemas: A instalação do driver falha para os leitores USB HID OMNIKEY 757

Reconhecimento de placas de veículos

Capítulo 38: O LPR em um relance

Sobre o Security Center AutoVu 760

Entidades relacionadas a LPR do AutoVu 762

Capítulo 39: Funções e unidades LPR

Sobre o LPR Manager 764
Configuração das funções do LPR Manager 766
Configurar a função Archiver para LPR 769
Requisitos de armazenamento para imagens de LPR 772
Sobre unidades de LPR 774
Equivalência de LPR 775
Técnica de equivalência de LPR: Equivalência de OCR 775
Técnica de equivalência de LPR: Número de diferenças de caracteres 776
Técnica de equivalência de LPR: Caracteres comuns e adjacentes 778
Arquivo MatcherSettings.xml 780
Exemplo de arquivo MatcherSettings.xml 780
Boas práticas para definir configurações de equivalência de LPR 782
Definir configurações de equivalência de LPR 783
Atualizar o SharpV a partir do Security Center 786

Capítulo 40: Listas de procurados

Sobre listas de procurados 788
Criar listas de procurados 789
Selecionar quais listas de procurados e autorizações um veículo de patrulha monitora 791
Instalar o plug-in Atualizador de Arquivos de Lista de Procurados e Autorizações 792
Filtrar caracteres inválidos de listas de procurados e listas de autorização 797
Adicionar configurações de privacidade a leituras e ocorrências 798
Adicionar configurações de privacidade a listas de procurados 799
Permitir que usuários editem listas de procurados e autorizações 801
Recebendo notificações quando alertas da lista de procurados ocorrem 802
Receber eventos de Correspondência e Não correspondência no Security Desk 804
Listas de procurados curinga 805
Ativar listas de procurados curinga 806
Atributos padrão de lista de procurados e autorizações 807
Configurando lista de procurados padrão e atributos de autorização 808
Definir configurações avançadas de lista de procurados 810
Configurar correspondência de leitura passada no LPR Manager 811

Capítulo 41: Sistemas fixos AutoVu

Preparar para implantar sistemas fixos AutoVu 814
Implantar sistemas AutoVu fixos 815
Configurando LPR Managers para sistemas AutoVu fixos 816
conexões de câmeras Sharp, SharpV ou SharpX ao Security Center 817
Adicionando uma câmera Sharp, SharpV ou SharpX ao LPR Manager 819
Adicionar uma câmera Sharp, SharpV ou SharpX ao Archiver 820
Substituir unidades Sharp fixas 821
Controle de acesso baseado em LPR 823
Configurar o AutoVu para controle de acesso 825
Criar eventos causa-efeito para eventos de LPR ou de listas de procurados 826

Capítulo 42: AutoVu Free-Flow

Sobre AutoVu Free-Flow 830

Sobre sessões de estacionamento 832
Estados da sessão de estacionamento 833
Cenários de estacionamento comuns para AutoVu Free-Flow 833
Eventos de zona de estacionamento 835
Configurar o AutoVu Free-Flow 837
Adicionar e configurar regras de estacionamento 840
Adicionar e configurar zonas de estacionamento 842
Vincular câmeras a zonas de estacionamento 844
Como a ocupação da zona é calculada 846
Recomendações para melhoria das métricas da ocupação de zona de estacionamento . . . 847
Sobre autorizações compartilhadas no AutoVu Free-Flow 848
Habilitar autorizações de estacionamento compartilhadas 848
Atribuir um mapa a uma zona de estacionamento 850
Adicionar uma zona de estacionamento a um mapa 851
Adicionar visualizações drill-down a mapas 853

Capítulo 43: Sistemas móveis AutoVu

Preparar para implantar sistemas móveis AutoVu 859
Implantar sistemas AutoVu móveis 860
Sobre Genetec Patroller 861
Conectar o Genetec Patroller ao Security Center 862
Configurar a entidade de Genetec Patroller no Security Center 864
Adicionar campos personalizados pelo usuário a leituras e ocorrências 866
Criando campos personalizados do usuário 866
Adicionando campos personalizados como campos de anotação 868
Definir campos personalizado para usuários do Genetec Patroller 869
Arquivos de som usados no Genetec Patroller 870
Alterar arquivos de som para eventos de LPR 871
Alterar arquivos de som para eventos LPR usando o serviço de atualização 871

Capítulo 44: Sistemas de aplicação da lei AutoVu

Sobre a Aplicação da lei 874
Criar motivos de aceitação de ocorrência e rejeição de ocorrência para ocorrências de lista de procurados 875
Criar atributos e categorias de Novo procurado 876

Capítulo 45: Sistemas de fiscalização de estacionamento na cidade e na universidade AutoVu

Sobre a fiscalização municipal de estacionamento 879
Sobre a fiscalização municipal de estacionamento com imagens da roda 879
Horas extras a longo prazo 880
Sobre a Fiscalização de estacionamento na universidade 881
Diferenças entre fiscalização de estacionamento na cidade e na universidade 882
Implementar sistemas de fiscalização de estacionamento na cidade e na universidade AutoVu . . 883
Sobre regras de tempo extra 884
Criando regras de horas extras 888
Configurar regras de tempo extra 889
Sobre autorizações 892
Criar autorizações de estacionamento 894
Configurar autorizações 896

Sobre restrições de autorização 897
Criando restrições de autorização 898
Configurar restrições de autorização 899
Configurar estacionamentos no Security Center 901
Importar arquivos KML no Security Center 902
Definir configurações avançadas de autorização 904

Capítulo 46: Sistemas de inventário de placas de veículos móvel AutoVu

Inventário Móvel de Placas de Licença 906
Sobre estacionamentos 907
Criando instalações de estacionamento 908
Configurar instalações de estacionamento 909

Capítulo 47: Solução de problemas de LPR

Mover unidades Genetec Patroller ou LPR para um LPR Manager diferente 912

Alarmes e eventos críticos

Capítulo 48: Alarmes

Sobre alarmes 916
Criando alarmes 918
Selecionar opções de exibição de vídeo para alarmes 919
Configurar propriedades opcionais de alarmes 920
Testar alarmes 922
Solução de problemas: Alarmes não recebidos 923
Configurar alarmes usando eventos de causa-efeito 924
Tipos de eventos que podem exigir condições de confirmação 924
Acionar alarmes manualmente 927

Capítulo 49: Níveis de ameaça

Sobre níveis de ameaça 929
Ações de nível de ameaça 929
Diferenças entre níveis de ameaça e alarmes 930
Definir níveis de ameaça 933
Cenário de nível de ameaça: Incêndio 934
Cenário de nível de ameaça: pessoa armada 936

Capítulo 50: Zonas e detecção de intrusão

Sobre zonas 939
Diferenças entre os tipos de área 940
Sobre Zone Managers 942
Acerca de comportamentos de saída 943
Criar zonas de hardware 944
Definição de configurações de área de hardware 945
Criar áreas virtuais 947
Definir configurações de área virtuais 948
Criar zonas de E/S 950
Definição de configurações de área de E/S 951
Integração do painel de intrusão 953
Sobre Intrusion Managers 954

Criar a função Intrusion Manager 955
Sobre unidades de detecção de intrusão 957
Limitações no monitoramento de entradas do painel de intrusão 957
Sobre áreas de detecção de intrusão 958
Criando áreas de detecção de intrusão 959
Mover unidades de detecção de intrusão para um Intrusion Manager diferente 960

Referência do Config Tool

Capítulo 51: Tipos de entidade

Abas de configuração comum 964
Unidade de controle de acesso - HID - Aba Identidade 967
Unidade de controle de acesso - HID - Aba Propriedades 968
Unidade de controle de acesso - HID - Aba Sincronização 969
Unidade de controle de acesso - HID - Aba Periféricos 970
Unidade de controle de acesso - Synergis – Aba Identidade 972
Unidade de controle de acesso - Synergis – Aba Propriedades 973
Unidade de controle de acesso - Synergis – Aba Portal 974
Unidade de controle de acesso - Synergis – Aba Hardware 975
Unidade de controle de acesso - Synergis – Aba Sincronização 976
Unidade de controle de acesso - Synergis - Aba Periféricos 977
Regra de acesso - Aba Propriedades 979
Abas Configuração de alarmes 980
Monitor analógico - Aba Propriedades 982
Abas de configuração de área 984
Modelo de crachá - Aba Designer de crachás 987
Câmera - Aba vídeo 989
Câmera - Aba Gravação 993
Câmera - Aba Detecção de movimento 994
Câmera - Aba Cor 996
Câmera - Aba Rastreamento visual 997
Câmera - Aba hardware 998
Sequência de câmeras - Aba Câmeras 1001
Abas de configuração de titulares de cartão 1002
Grupo de titulares de cartão - Aba Propriedades 1003
Abas de configuração de credencial 1004
Abas Configuração de portas 1005
Abas de configuração de elevador 1008
Abas de configuração de zonas de hardware 1010
Abas de configuração de lista de procurados 1011
Zona de E/S - Aba Propriedades 1013
Área de detecção de intrusão - Aba Propriedades 1014
Abas de configuração da unidade de detecção de intrusão 1015
Unidade de LPR - Aba Propriedades 1016
Abas de configuração de macro 1017
Grupo de monitores - Aba Monitores 1018
Rede - Aba Propriedades 1019
Comportamento de saída - Aba Propriedades 1020
Abas de configuração de regra de horas extras 1021

Instalação de estacionamento - Aba Propriedades 1022
Partição - Aba Propriedades 1023
Genetec Patroller - Aba Propriedades 1024
Autorização - Aba Propriedades 1025
Abas de configuração de restrição de autorização 1026
Agendamento - Aba Propriedades 1027
Tarefa agendada - Aba Propriedades 1028
Servidor - Aba Propriedades 1029
Plug-in de Ladrilho - Aba Propriedades 1030
Abas de configuração do usuário 1031
Abas de configuração Grupo de usuários 1034
Unidade de vídeo - Aba Identidade 1036
Unidade de vídeo - Aba Propriedades 1037
Unidade de vídeo - Aba Periféricos 1039
Abas de configuração de zona virtual 1041

Capítulo 52: Tipos de função

Abas de configuração do Access Manager 1043
Abas de configuração do Active Directory 1045
Active Directory Federation Services - Aba Propriedades 1047
Archiver - Aba Configurações padrão de câmera 1048
Archiver - Aba Extensões 1050
Archiver - Aba Recursos 1053
Archiver auxiliar - Aba Gravação da câmera 1056
Archiver auxiliar - Aba Câmeras 1057
Archiver auxiliar - Aba Recursos 1058
Abas de configuração do Directory Manager 1061
Abas de configuração do Global Cardholder Synchronizer 1063
Abas de configuração do Health Monitor 1064
Abas de configuração do Intrusion Manager 1065
LPR Manager - Aba Propriedades 1066
LPR Manager - Aba Recursos 1074
Abas de configuração do Map Manager 1075
Abas de configuração do Media Gateway 1076
Abas de configuração do Media Router 1077
Abas de configurações Omnicast Federation 1079
Abas de configuração do Gerenciador de relatórios 1080
Abas de configuração do Security Center Federation 1081
Abas de configuração Web-based SDK 1082
Abas de configuração do Web Client Server 1083
Abas de configuração do Zone Manager 1084

Capítulo 53: Tarefas de administração

Tarefa LPR - Visualização de configurações gerais 1086
Tarefa do sistema - Configurações gerais - Página Campos personalizados 1089
Tarefa do sistema - Configurações gerais - Página Eventos 1090
Tarefa do sistema - Configurações gerais - Página de ações 1091
Tarefa do sistema - Configurações gerais - Página de ID lógico 1092
Tarefa do sistema - Configurações gerais - Página de configurações de senha do usuário . . . 1093

Tarefa do sistema - Configurações gerais - Página de trilhas de atividades 1094
Tarefa do sistema - Configurações gerais - Página de áudio 1095
Tarefa do sistema - Configurações gerais - Página de níveis de ameaça 1096
Tarefa do sistema - Configurações gerais - Página de categorias de incidentes 1097
Tarefa do sistema - Configurações gerais - Página Recursos 1098
Tarefa de controle de acesso - Visualização de configurações gerais 1099

Capítulo 54: Eventos e ações

Tipos de evento 1101
Tipos de ação 1120

Apêndices

Apêndice A: Opções de licença 1130
Ver informações da licença 1131
Opções de licença no Security Center 1132
Apêndice B: Portas padrão do Security Center 1136
Portas usadas por aplicativos principais no Security Center 1137
Portas usadas por aplicativos AutoVu no Security Center 1139
Portas usadas por aplicativos Omnicast no Security Center 1141
Portas usadas por aplicativos Synergis no Security Center 1144
Apêndice C: Referência do HID 1146
Hardware HID suportado 1147
Download de documentação de HID 1148
Controladores HID VertX suportados 1149
Subpainéis HID VertX suportados 1151
Controladores HID Edge suportados 1153
Módulos de interface Edge suportados 1155
Versões de firmware de HID suportadas 1156
O que pode ser feito ou não instalação do hardware HID 1157
Conexões do HID VertX V1000 RS-485 1159
Comportamento de E/S do HID VertX V1000 1160
Considerações sobre conexão de E/S do HID 1161
LEDs de Alimentação e Com. do HID 1162
Recursos e modelos de HID suportados pelo Security Center 1163
Habilitar suporte a PIN longos em unidades HID 1166
Configurações suportadas da unidade HID 1167
Recursos do Security Center suportados por unidades HID 1168
Apêndice D: Recurso de múltiplas leituras 1173
Sobre o recurso de múltiplas leituras 1174
Implementando o recurso de múltiplas leituras 1175

Glossário 1177

Onde encontrar informações do produto 1229
Suporte técnico 1230

Introdução ao Security Center

Esta parte inclui as seguintes chapters:

- "O Security Center em um relance" na página 2
- "Tarefas" na página 38
- "Relatórios" na página 47
- "Atalhos de teclado" na página 65

1

O Security Center em um relance

Esta seção inclui os seguintes tópicos:

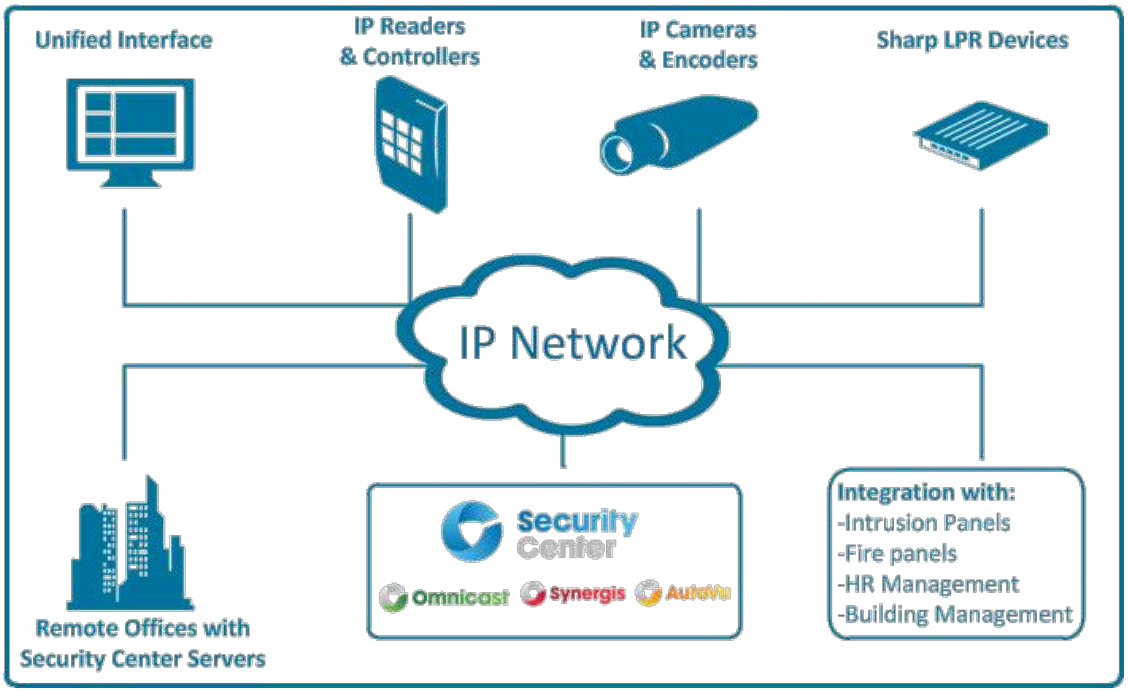
- "Sobre o Security Center " na página 3
- "Visão geral da arquitetura do Security Center" na página 5
- "Como o Security Center é organizado" na página 6
- "Fazer logon no Security Center através do Config Tool" na página 7
- "Fechar Config Tool" na página 12
- "Visão geral da página inicial" na página 13
- "Visão geral da página Sobre" na página 15
- "Visão geral do espaço de trabalho das tarefas de administração" na página 17
- "Visão geral do espaço de trabalho de manutenção " na página 21
- "Sobre a exibição de área" na página 23
- "Acerca de áreas" na página 25
- "Organizar a exibição de área" na página 26
- "Criar áreas" na página 27
- "Ligar e desligar recursos" na página 28
- "Configurar a bandeja de notificação" na página 29
- "Mudar senhas" na página 31
- "Abrir o Security Desk pelo Config Tool" na página 32
- "Enviar feedback" na página 33
- "Coletando dados de diagnóstico" na página 34
- "Atalhos para ferramentas externas" na página 36

Sobre o Security Center

Security Center é uma plataforma verdadeiramente unificada que combina vigilância por vídeo IP, controle de acesso, reconhecimento de placas de veículo, detecção de intrusão e comunicação em uma única solução modular intuitiva. Tirando partido de uma abordagem unificada à segurança, a sua organização ganha eficiência, toma melhores decisões e responde a situações e ameaças com maior confiança.

A plataforma de segurança unificada Security Center proporciona o seguinte:

- Uma plataforma de controle e gerenciamento de dispositivos de vídeo/acesso/LPR em unidade.
- Uma interface de usuário para monitoramento, relatórios e gerenciamento de eventos e alarmes para vigilância por vídeo, controle de acesso e LPR - *Security Desk*.
- Uma interface de usuário para configurar vigilância por vídeo, controle de acesso e LPR - *Config Tool*.
- Visualização unificada de vídeo ao vivo com pesquisas e reprodução de vídeo.



Os recursos do Security Center estão divididos em quatro categorias principais: Comum, Vigilância por vídeo (Omnicast), Controle de acesso (Synergis) e Reconhecimento de placas de veículo (AutoVu™).

Recursos comuns/centrais

- Gestão de alarme
- Gerenciamento de zona
- Federação
- Integração do painel de intrusão
- Gerenciamento de relatórios
- Gerenciamento de agenda e tarefas agendadas
- Gerenciamento de usuários e grupos de usuários
- Integração do Active Directory do Windows
- Comportamento programável do sistema automatizado

Omnicast – Recursos de vigilância em vídeo

- Configuração e gerenciamento total de câmeras
- Visualizar vídeo ao vivo e de reprodução de todas as câmeras
- Controle PTZ completo usando o teclado do PC ou de CCTV, ou na tela, usando o mouse
- Zoom digital
- Detecção de movimento
- Marcar qualquer cena importante para facilitar a futura pesquisa e recuperação de arquivo de vídeo
- Salvar e imprimir instantâneos
- Pesquisar vídeo por alarme, marcador, evento, movimentação ou data e hora
- Visualizar todas as câmeras em linhas do tempo independentes ou sincronizadas
- Rastreamento visual: seguir indivíduos ou objetos em movimento por diferentes câmeras
- Exportar vídeo
- Proteger vídeo contra exclusão acidental
- Proteger vídeo contra adulteração com o uso de marcas d'água
- Proteger a privacidade de indivíduos no vídeo

Synergis™ – Recursos de controle de acesso

- Gerenciamento de titulares de cartão
- Gerenciamento de credenciais
- Gerenciamento de visitantes
- Gerenciamento de portas
- Gerenciamento de regras de acesso
- Contagem de pessoas

AutoVu™ – Recursos de reconhecimento de placas de veículo (LPR)

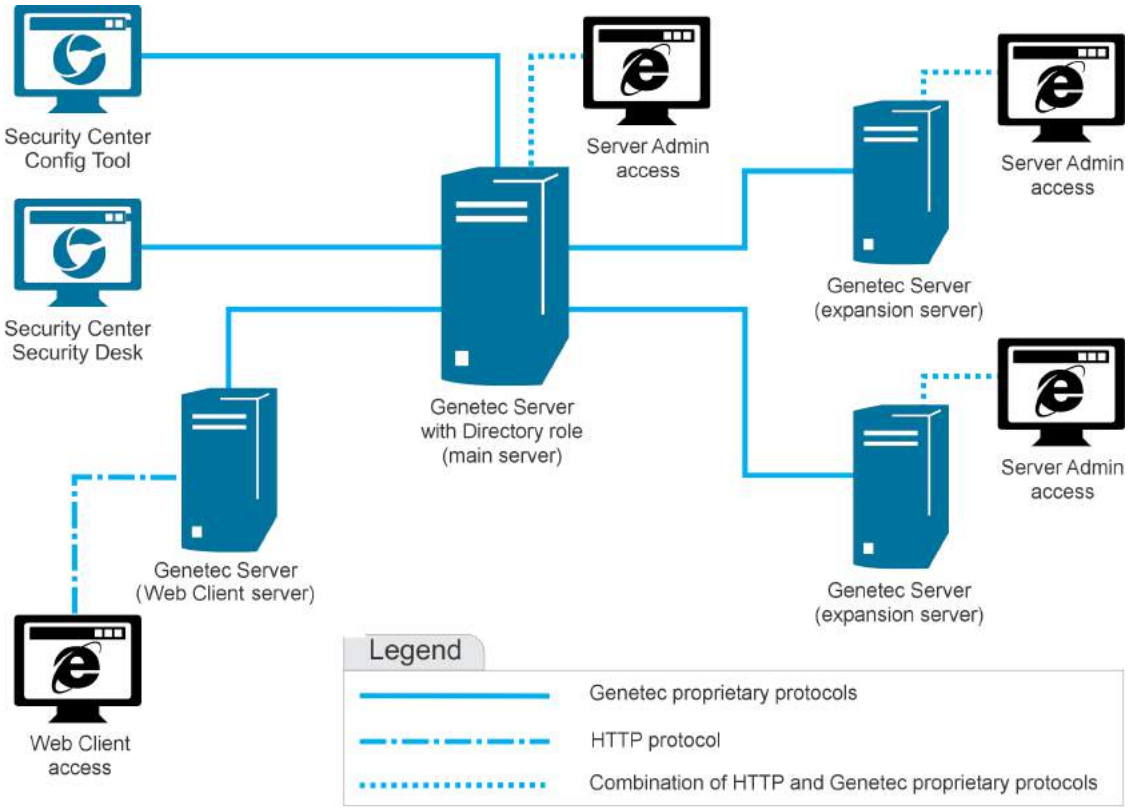
- Gestão de soluções de LPR fixas e móveis (com o Genetec Patroller™)
- Identificação automática de veículos roubados (ou contraventores)
- Fiscalização de regulamentos de estacionamento municipal (não envolvendo autorizações)
- Fiscalização de regulamentos de terrenos de estacionamento (envolvendo autorizações)
- Inventário de placa de licença em instalações de estacionamento grandes

Visão geral da arquitetura do Security Center

A arquitetura do Security Center é baseada em um modelo cliente/servidor, no qual todas as funções são controladas por um conjunto de computadores servidores distribuídos por uma rede IP.

Todo sistema do Security Center deve ter seu próprio conjunto de servidores. Seu número pode variar de uma única máquina para um sistema pequeno, até centenas de máquinas para um sistema de grande porte.

NOTA: Os ícones coloridos em azul representam os computadores onde os componentes de servidor e cliente do Security Center estão instalados.



Como o Security Center é organizado

Security Centeré organizado por tasks. Todas as tarefas podem ser personalizadas e várias tarefas podem ser executadas ao mesmo tempo. Você pode não conseguir ver todas as tarefas e comandos descritos sobre o Security Center, dependendo de suas opções de licença e seus privilégios de usuário. Há privilégios de usuário para cada tarefa e para muitos comandos no Security Center.

As tarefas na página inicial são organizadas nas seguintes categorias:

- **Administração:** (Somente Config Tool) Tarefas usadas para criar e configurar as entidades exigidas para modelar seu sistema.
- **Operação:** Tarefas relacionadas às operações diárias do Security Center.
- **Investigação:** (Somente Security Desk) Tarefas que permitem consultar o banco de dados do Security Center e os bancos de dados dos sistemas federados, em busca de informações críticas.
- **Manutenção:** Tarefas relacionadas à manutenção e solução de problemas.

Em cada categoria principal, as tarefas são subdivididas como segue:

- **Tarefas comuns:** Tarefas que são compartilhadas por todos os três módulos de software do Security Center. Essas tarefas estão sempre disponíveis, independentemente de quais módulos são suportados por sua licença de software.
- **Controle de acesso:** Tarefas relacionadas ao controle de acesso. As tarefas de controle de acesso são exibidas com uma linha vermelha sob seus ícones. Elas ficam disponíveis somente se o *Synergis™* for suportado por sua licença de software.
- **LPR:** Tarefas relacionadas a *leitura de placa de veículo (LPR)*. As tarefas de LPR são exibidas com uma linha de cor laranja sob seus ícones. Elas ficam disponíveis somente se o *AutoVu™* for suportado por sua licença de software.
- **Vídeo:** Tarefas relacionadas ao gerenciamento de vídeo. As tarefas de vídeo são exibidas com uma linha verde sob seus ícones. Elas ficam disponíveis somente se o *Omnicast™* for suportado por sua licença de software.

Fazer logon no Security Center através do Config Tool

Para fazer logon no Security Center, é necessário abrir o Config Tool e se conectar ao Security Center Directory.

Antes de iniciar

Certifique-se de ter o seu nome de usuário, senha e nome do *servidor principal* ao qual deseja se conectar.

O que você deve saber

Geralmente, fazer logon no Security Center implica uma autenticação bilateral:

- O *Directory* (servidor principal) deve ser autenticado pela parte que solicita a conexão (o usuário).
- A parte que solicita a conexão deve ser *autenticada* e *autorizada* pelo Directory.

O Security Center oferece várias opções para tratar do processo de autenticação. O seu procedimento de logon pode tomar diferentes caminhos dependendo da forma como o administrador configurou seu sistema.

Quando estiver logado, você pode se desconectar do Directory sem fechar o Config Tool. Fazer logoff sem fechar o aplicativo é útil se planejar fazer logon novamente usando um nome de usuário e senha diferentes.

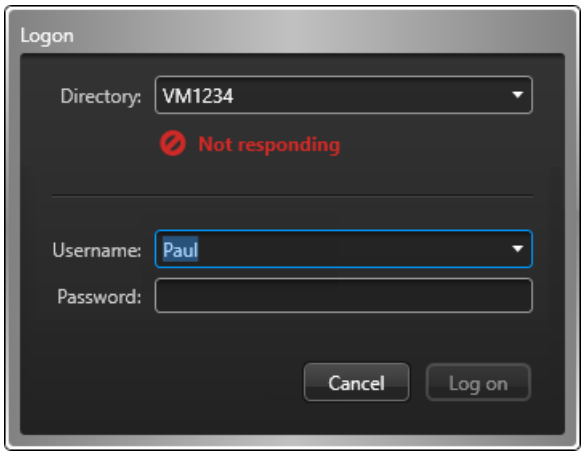
Para fazer log on no Security Center:

1 Abra o Config Tool clicando em **Início** > **Todos os programas** > **Genetec Security Center 5.7** > **Config Tool**.

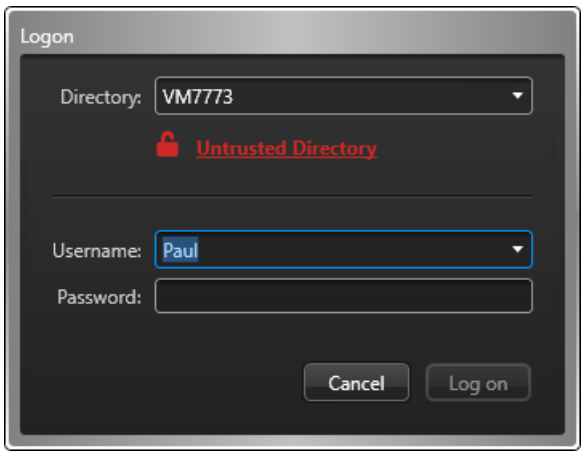
2 Na caixa de diálogo *Logon*, digite o nome e o endereço IP do seu servidor principal como **Directory**.

NOTA: Se estiver executando o Config Tool no servidor principal, você pode digitar `Localhost` em vez de o nome do servidor principal.

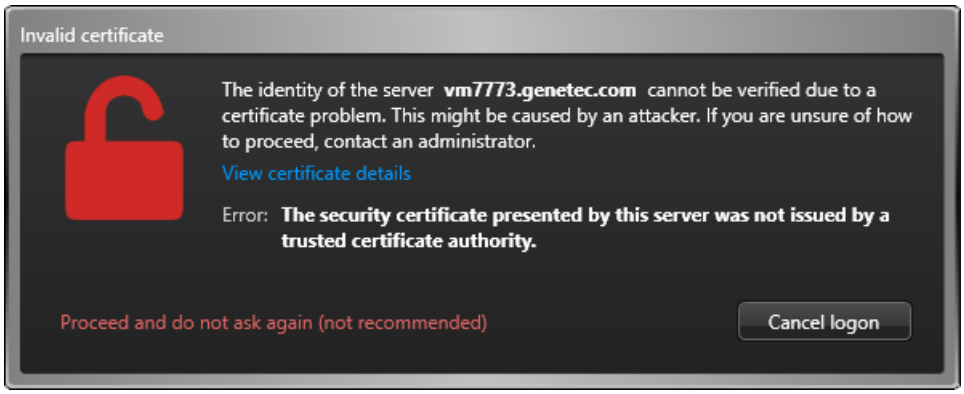
Se o Directory não estiver respondendo, certifique-se de que o servidor esteja online e que a configuração de rede permita ao seu computador contactar o servidor principal (verifique nome do host, endereço IP e regras de firewall).



Se o Directory não for confiável, pode ser um sinal de ataque man-in-the-middle. Não prossiga a menos que você (ou seu administrador) esteja certo de que o servidor que está contactando é seguro.

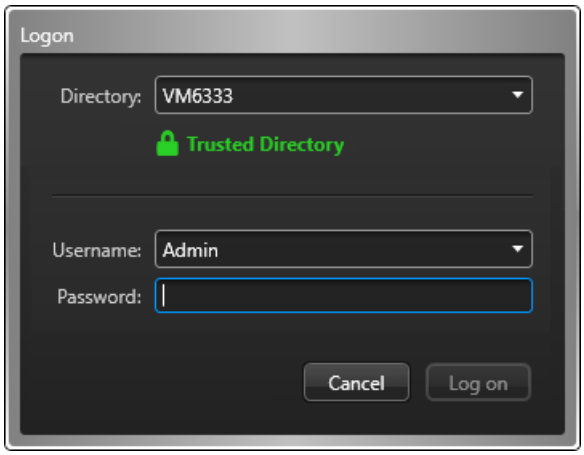


Clique no ícone de cadeado para obter mais informações.



Se o seu administrador confirmar que você pode confiar nesse servidor, clique em **Continuar e não voltar a perguntar**. O certificado nessa máquina será armazenado em sua máquina e as futuras conexões com esse mesmo Directory serão confiáveis, desde que o seu certificado não seja alterado.

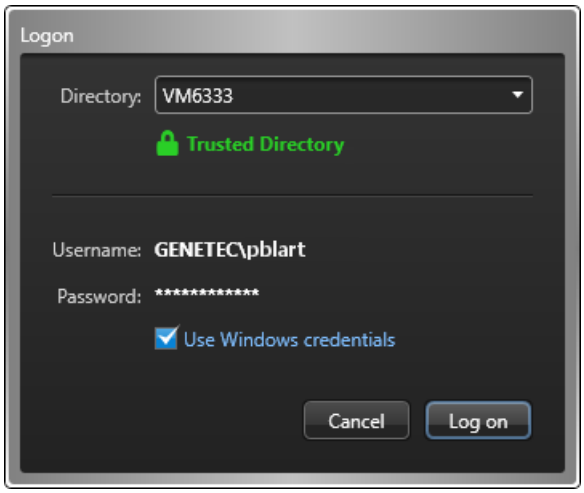
3 Digite seu nome do usuário e senha do Security Center.
Se você acabou de instalar o Security Center, digite `Admin` com uma senha em branco.



Se o logon único (Active Directory ou ADFS) for utilizado, é necessário anexar o nome de domínio ao seu nome de usuário como em `Username@DomainName`.

Se o Security Center detectar que *autenticação passiva* com ADFS está habilitado no seu domínio, você será redirecionado para um formulário Web exibido pelo *provedor de identidade* após ter digitado seu nome de usuário. Pule para Fazer logon usando autenticação passiva na página 9.

4 Para fazer o logon usando a sua conta de usuário do Windows, selecione **Usar credenciais do Windows**.
Essa opção está disponível somente se o Active Directory estiver habilitado no seu sistema.



NOTA: Se a sua estação de trabalho cliente não estiver no mesmo domínio do servidor, ou se você quiser fazer logon no Security Center com uma conta Windows diferente, você deve desmarcar a opção **Usar credenciais Windows** e digitar seu nome de usuário no formato *DOMAIN\Username*.

5 Clique em **Logon**.

6 Para fazer logoff, clique na aba página inicial ( ) e depois clique em **Logoff**.

Tópicos relacionados

O que é a autenticação do diretório? na página 373
Integração com o Active Directory do Windows na página 384
O que é a autenticação baseada em declarações? na página 398
Personalizar opções de logon de usuário na página 365

Fazer logon usando autenticação passiva

Se o Security Center detectar que o seu nome de usuário de logon corresponder ao domínio abrangido por um servidor ADFS com autenticação passiva habilitada, você será redirecionado para um formulário Web para digitar sua senha.

Antes de iniciar

Abra Config Tool e digite o nome do **Directory** na caixa de diálogo *Logon*.

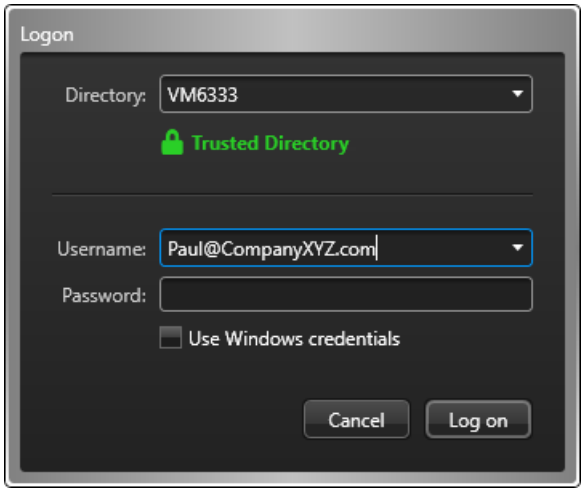
O que você deve saber

Autenticação passiva (também chamada autenticação baseada na Web) é quando o aplicativo cliente redireciona o usuário para um formulário Web gerido por um provedor de identidade confiável. O provedor de identidade pode solicitar qualquer número de credenciais (senhas, tokens de segurança, verificações biométricas e assim por diante) para criar uma defesa multicamada contra acesso não autorizado. Isto também é conhecido como autenticação multifator.

NOTA: O Config Tool memoriza todos os parâmetros de logon usados e recupera automaticamente os parâmetros usados na última tentativa de logon.

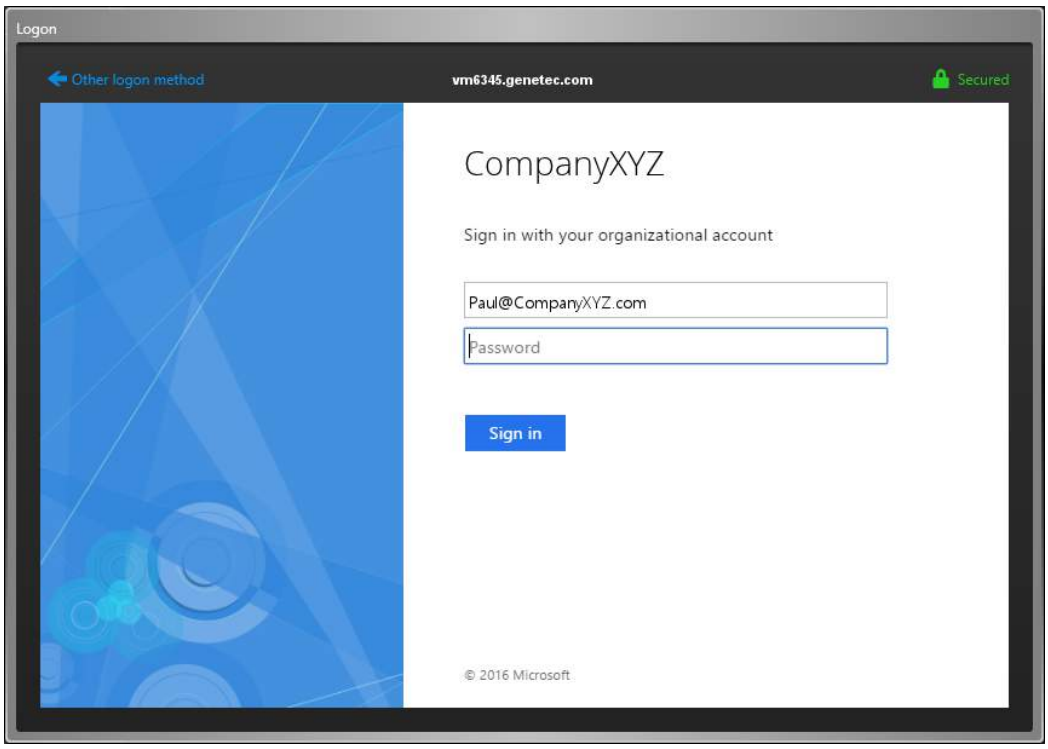
Para fazer logon usando autenticação passiva:

1 No campo **Nome de usuário**, digite seu nome de usuário seguido do nome do seu domínio, no formato *Username@DomainName*.



2 Clique no campo **Senha** ou pressione a tecla Tab.

Se o Security Center detectar que a *autenticação passiva* está habilitada em seu domínio, você será redirecionado para um formulário Web. A captura de tela a seguir é um exemplo. A sua página de logon poderá ser diferente.



3 No formulário Web, digite as informações necessárias e clique em **Entrar**.

NOTA: Você não pode fazer logon como usuário *Admin* usando autenticação baseada na Web. Para fazer logon como usuário *Admin*, clique em **Outro método de logon** para retornar à caixa de diálogo *Logon* do Security Center.

Fechar Config Tool

É possível fechar o Config Tool e salvar seu espaço de trabalho para a próxima vez que fizer log on.

O que você deve saber

Também há algumas opções que você pode personalizar para quando for fechar o Config Tool da Opções caixa de diálogo.

Para fechar Config Tool:

1 No canto superior direito da janela Config Tool, clique em **Sair** ().

Se tiver tarefas que não foram salvas no seu espaço de trabalho, será indagado a salvá-las.

2 Para carregar automaticamente a mesma lista de tarefas da próxima vez que abrir o Config Tool, clique em **Salvar**.

Tópicos relacionados

Definir como o seu espaço de trabalho é salvo na página 12

Definir como o seu espaço de trabalho é salvo

Para garantir que alterações ao seu espaço de trabalho sempre sejam tratadas da mesma maneira ao fechar, você pode definir como você quer que seu aplicativo se comporte, independentemente de ter ou não ter alterações não salvas em sua lista de tarefas.

O que você deve saber

Esta configuração é salva como parte do seu perfil de usuário e se aplica ao Security Desk e ao Config Tool.

Para definir as ações ao salvar seu espaço de trabalho:

1 Na página inicial, clicar em **Opções** > **Interação de usuários**.

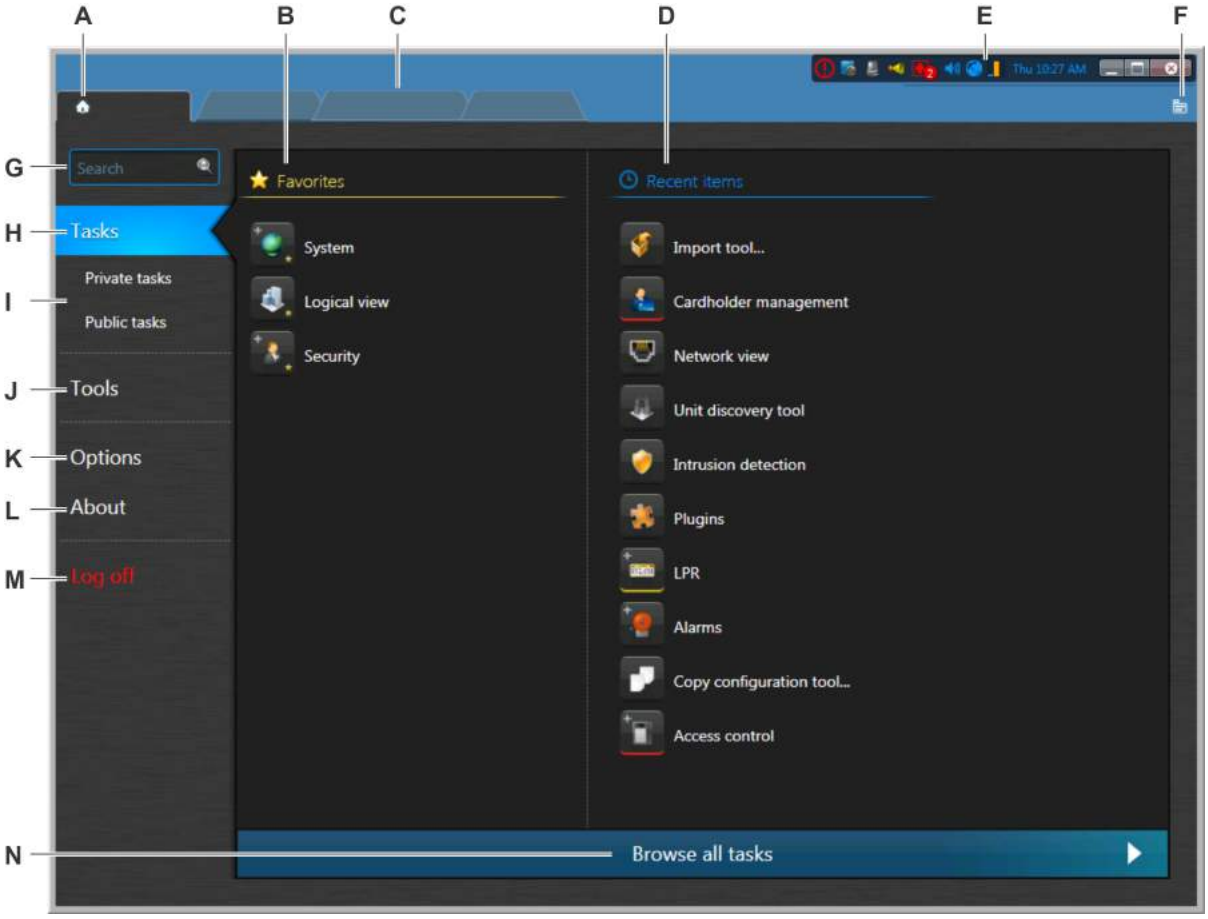
2 Na lista suspensa **Salvar a lista de tarefas**, selecione uma das opções seguintes:

- *Perguntar ao usuário*. Pergunta antes de salvar sua lista de tarefas.
- *Sim*. Salva o espaço de trabalho sem perguntar.
- *Não*. Nunca salva o espaço de trabalho.

3 Clique em **Salvar**.

Visão geral da página inicial

A página inicial é a principal página. É possível abrir a página inicial ao clicar na aba página inicial (🏠). Também é mostrada se a lista de tarefas está vazia.



A Página Inicial aba	• Clique para mostrar ou ocultar a página inicial. • Clique com o botão direito para obter uma lista de comandos (por exemplo, salvar o espaço de trabalho, fechar tarefas, etc.).
B Favoritos	Clique com o botão direito em qualquer tarefa ou ferramenta para adicionar ou remover da sua lista *Favoritos* . Também é possível arrastar a tarefa para essa lista. As tarefas listadas em seus *Favoritos* não aparecem mais na lista *Itens recentes* .
C Lista de tarefas	Mostra as tarefas que estão atualmente abertas e nas quais você está trabalhando em abas individuais. • Clique em uma aba de tarefa para alternar para aquela tarefa. • Clique com o botão direito em uma aba para obter uma lista de comandos.
D Itens recentes	Lista as tarefas e ferramentas recentemente abertas.

E	**Bandeja de notificação**	Exibe informações importantes sobre o seu sistema. Segure o ponteiro do mouse sobre um ícone para visualizar as informações do sistema, ou clique duas vezes no ícone para executar uma ação. É possível escolher quais os ícones que deseja que apareça na barra de notificações na seção Visual da caixa de diálogo*Opções* .
F	**Listar todas as tarefas**	Clique para visualizar uma lista de todas as tarefas abertas. Esse botão aparece apenas se as abas da tarefa ocupam toda a largura da barra de tarefas.
G	**Pesquisar caixa**	Digite o nome da tarefa que está procurando. Todas as tarefas contendo aquele texto na sua categoria, nome ou descrição são mostradas.
H	**Tarefas**	Lista os seus itens recentes, favoritos e todos os tipos de tarefas disponíveis para você. Selecione uma tarefa para abrir dessa aba.
Eu	**Tarefas privadas**, **Tarefas públicas**	Clique para visualizar as tarefas salvas disponíveis para você. • **Tarefas privadas**. Uma tarefa privada é uma tarefa somente visível para o usuário que a criou. • **Tarefas públicas**. Uma tarefa pública é uma tarefa salva que pode ser compartilhada e reutilizada entre vários usuários do Security Center.
J	**Ferramentas**	Clique para visualizar as ferramentas com as quais pode começar diretamente da sua página inicial. A Ferramentas página está dividida nas duas sessões que seguem: • **Ferramentas**. Esta seção mostra as ferramentas padrão do Security Center . • **Ferramentas externas**. Esta seção mostra os atalhos para as ferramentas e aplicativos externos.
K	**Opções**	Clique para configurar as opções para o seu aplicativo.
L	**Sobre**	Clique para visualizar as informações sobre o software Security Center , como licença, Contrato de Manutenção do Software e versão do software.
M	**Fazer logoff**	Clique para fazer logoff sem sair do aplicativo.
N	**Pesquisar todas as tarefas**	Clique para visualizar todas as tarefas disponíveis para você. Clique em um ícone de tarefa para abrir a tarefa. Se for uma tarefa de instância única, a tarefa abre. Se for possível ter várias instâncias da tarefa, é solicitado que um nome para a tarefa seja digitado.

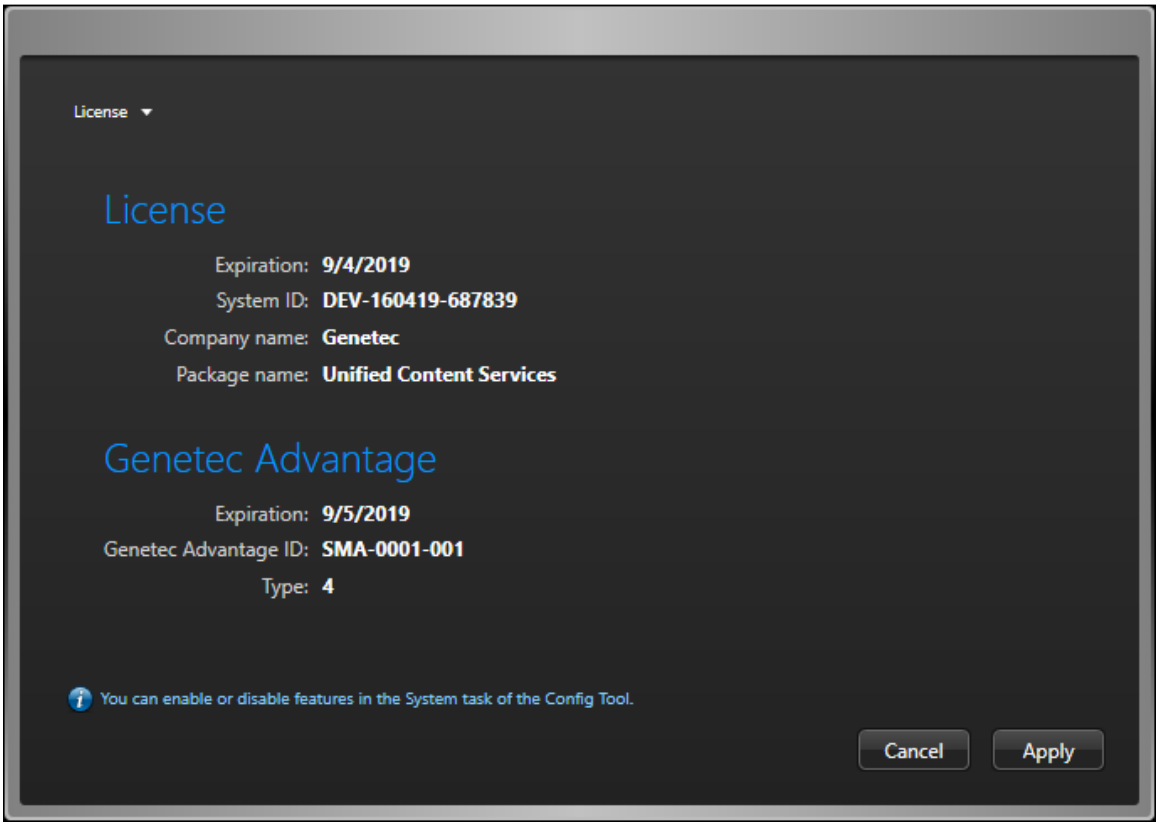
Tópicos relacionados

Configurar a bandeja de notificação na página 29
Salvar tarefas na página 40
Abrir tarefas na página 39
Atalhos para ferramentas externas na página 36

Visão geral da página Sobre

A página Sobre exibe informações sobre o software Security Center, como a licença comprada, número de SMA, data de validade da licença, versão de software e assim por diante.

Todas as opções de licença são suportadas, não suportadas ou limitadas por uma contagem máxima de usos. Para opções com uma contagem máxima de usos, o Config Tool mostra o uso atual e o máximo permitido.



As seguintes abas estão disponíveis, dependendo do que a sua licença suporta:

- **Licença:** Indica quando a licença do software expira e dá as informações necessárias que você deve fornecer ao entrar em contato com a Central de Assistência Técnica da Genetec™: ID do sistema, nome da empresa, nome do pacote e o número do seu acordo de manutenção de serviços (SMA).

  IMPORTANTE: Trinta dias antes do vencimento de sua licença ou do seu SMA, você receberá uma mensagem no Config Tool alertando que sua licença ou seu SMA está prestes a expirar. O Config Tool conecta ao GTAP para validar o SMA.
- **Security Center:** Esta aba mostra todas as opções genéricas do Security Center.
- **Synergis:** Esta aba mostra todas as opções de controle de acesso. Ela é exibida somente se o *Synergis™ (controle de acesso)* for suportado.
- **Omnicast:** Esta aba mostra todas as opções de vídeo. Ela é exibida somente se o *Omnicast (vigilância por vídeo)* for suportado.
- **AutoVu:** Esta aba mostra todas as opções de LPR. Ela é exibida somente se o *AutoVu (LPR)* for suportado.
- **Plan Manager:** Esta aba mostra todas as opções do Plan Manager.
- **Mobile:** Esta aba mostra todas as opções do Security Center Mobile. Ela é exibida somente se o Security Center Mobile for suportado.

- **Certificados:** Esta aba lista os *Certificados SDK* incluídos nesta chave de licença.
- **Pedido de compra:** Esta aba reproduz seu pedido.

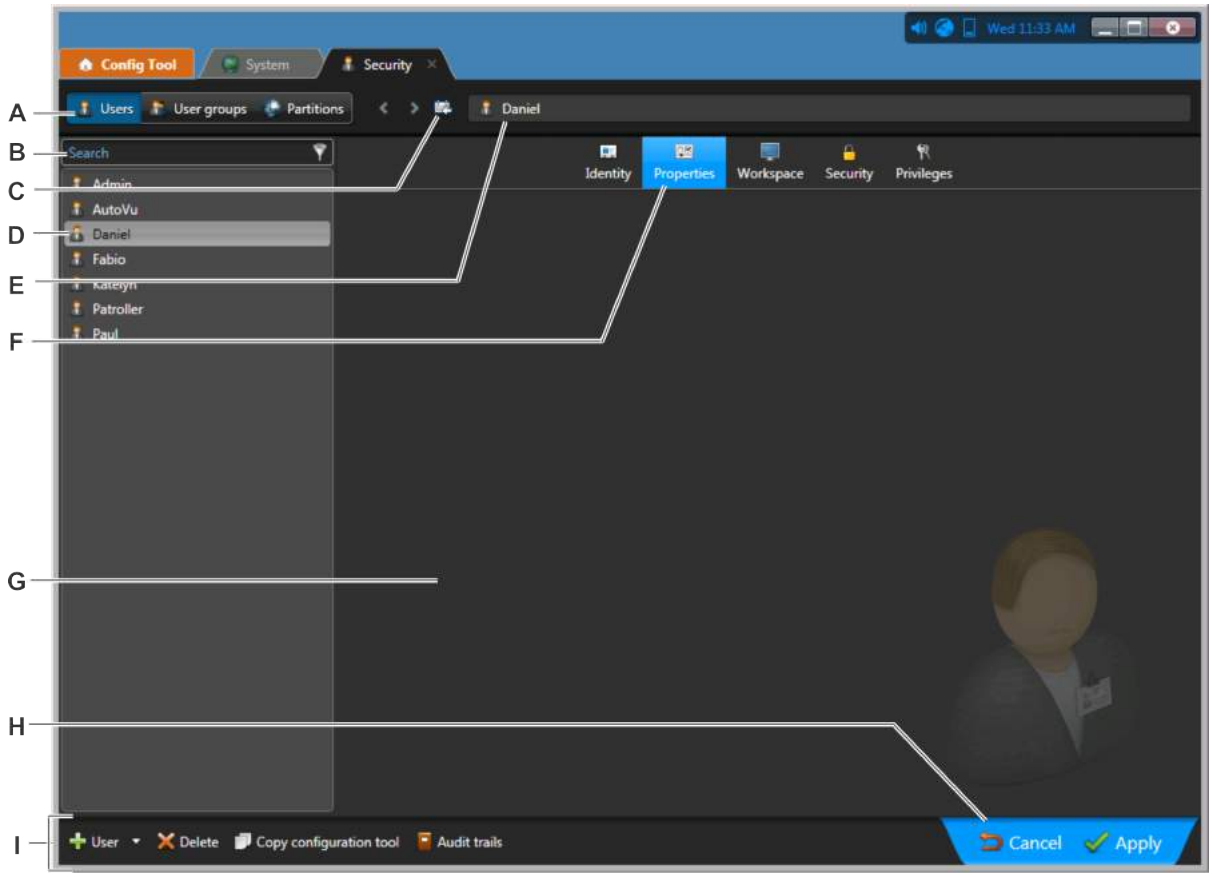
Na página Sobre, os seguintes botões também estão disponíveis:

- **Ajuda:** Clique para abrir a ajuda online. Você também pode usar F1.
- **Alterar senha:** Clique para mudar sua senha.
- **Entrar em contato:** Clique para visitar a GTAP ou o fórum da GTAP. Você precisa de uma conexão com a Internet para visitar esses sites.
- **Componentes instalados:** Clique para visualizar o nome e a versão de todos os componentes de software instalados (DLLs).
- **Direitos autorais:** Clique para exibir informações sobre direitos autorais do software.
- **Enviar feedback:** Clique para nos enviar feedback.

Visão geral do espaço de trabalho das tarefas de administração

As tarefas de administração servem para criar e configurar as *entidades* exigidas para modelar o seu sistema.

Esta seção mostra o layout da tarefa de administração e descreve os elementos comuns da maioria delas. A tarefa *Segurança* foi usada como exemplo. Você pode abrir a tarefa *Segurança* digitando seu nome na caixa *Pesquisa* na página inicial.



A	**Visualizações de entidade**	Visualizações para cada tipo de entidade gerenciado pela tarefa.
B	**Filtro de entidades**	Digite uma cadeia de caracteres neste campo e pressione *ENTER* para filtrar as entidades no navegador por nome. Clique em *Aplicar um filtro personalizado* ( ) para escolher as entidades que deseja exibir no navegador.
C	**Histórico da entidade**	Use esses botões para navegar pelas entidades usadas recentemente nesta tarefa.
D	**Navegador de entidades**	Clique em uma entidade no navegador para mostrar suas configurações à direita.
E	**Entidade atual**	O ícone e o nome da entidade selecionada são exibidos aqui.

F	**Abas de configurações**	As configurações da entidade são agrupadas por abas.
G	**Página de configurações**	Esta área exibe as configurações da entidade na aba de configurações selecionada.
H	**Aplicar/cancelar mudanças**	Você deve *Cancelar* ou *Aplicar* qualquer mudança feita na página atual antes de poder passar para uma página diferente.
I	**Comandos contextuais**	Comandos relacionados à entidade selecionada são exibidos na barra de ferramentas na parte inferior do espaço de trabalho.

Comandos contextuais em tarefas de administração

Comandos relacionados à entidade selecionada no navegador são exibidos na parte inferior do espaço de trabalho em tarefas de administração.

A tabela a seguir descreve todos os comandos contextuais em ordem alfabética.

Ícone	Comando	Aplica-se a	Descrição
	Ativar função	Todas as funções	Ativar a função selecionada.
	Adicionar um titular de cartão	Regras de acesso e grupos de titulares de cartão	Cria um titular de cartão e o atribui à entidade selecionada.
	Adicionar uma credencial	Titulares do cartão	Cria uma credencial e a adiciona ao titular de cartão selecionado.
	Adicionar uma entidade	Todas as entidades	Criar uma entidade
	Atribuir à nova porta	Unidades de controle de acesso	Cria uma porta e a atribui à unidade de controle de acesso selecionada.
	Rastreamento de auditoria	Todas as entidades	Criar uma tarefa de trilhas de auditoria para descobrir quais usuários fizeram alterações no sistema.
	resolução de conflitos	Função do Active Directory	Abrir a caixa de diálogo de resolução de conflitos do Active Directory para resolver conflitos causados por entidades importadas.
	Ferramenta copiar configuração	Todas as entidades	Abrir a Ferramenta copiar configuração.
	Criar uma regra de acesso	Áreas, portas, elevadores	Cria uma regra de acesso e a atribui à entidade selecionada.
	Desativar função	Todas as funções	Desativar a função selecionada.

Ícone	Comando	Aplica-se a	Descrição
	**Excluir**	Todas as entidades	Remover a entidade selecionada do banco de dados. As entidades descobertas somente podem ser excluídas quando estiverem inativas.
	**Diagnosticar**	Todas as funções e algumas entidades	Realiza um diagnóstico da função ou entidade selecionada.
	**Desativar registros de suporte**	Access Manager e unidades de controle de acesso	Desativar os registros de suporte se solicitado pela Assistência Técnica da Genetec™.
	**Ativar registros de suporte**	Access Manager e unidades de controle de acesso	Desativar os registros de suporte se solicitado pela Assistência Técnica da Genetec™.
	**Estatísticas de saúde**	Funções e dispositivos físicos	Cria uma tarefa e estatísticas de saúde para a entidade selecionada para visualizar a saúde e a disponibilidade das entidades.
	**Identificar**	Unidades de vídeo	Acende um LED na unidade selecionada para ajudar a localizá-la em um bastidor.
	**Vídeo ao vivo**	Câmeras	Abre uma caixa de diálogo mostrando vídeo ao vivo da câmera selecionada.
	**Modo de manutenção**	Funções e dispositivos físicos	Configura uma função ou um dispositivo físico no modo de manutenção para que seu tempo ocioso não afete o cálculo da sua disponibilidade no Monitor de Saúde.
	**Mover unidade**	Unidades de vídeo e controle de acesso	Abre a ferramenta de Movimento de unidade, com o qual é possível mover unidades de umr gerenciador para outro.
	**Ping**	Unidades de vídeo	Faz o ping na unidade de vídeo para verificar se você pode se comunicar Isto é útil para fins de solução de problemas.
	**Imprimir crachá**	Titulares de cartão e credenciais	Seleciona um modelo de crachá e imprima um crachá para o titular de cartão ou de credencial selecionado.
	**Reiniciar**	Unidades de vídeo e controle de acesso	Reinicia a unidade selecionada.
	**Reconectar**	Unidades de vídeo	Remove a unidade de vídeo selecionada do Archiver e a adiciona novamente.
	**Executar macro**	Macros	Executa a macro selecionada.
	**Disparar alarme**	Alarmes	Dispara o alarme selecionado para que possa ser visualizado no Security Desk.

Ícone	Comando	Aplica-se a	Descrição
	**Ferramenta de inscrição na unidade:**	Unidades de vídeo e controle de acesso	Abre a Ferramenta de inscrição de unidade, onde você pode encontrar unidades IP conectadas à sua rede.
	**Página da unidade na internet**	Unidades de vídeo	Abre um navegador para configurar a unidade usando a página da web hospedada na unidade.

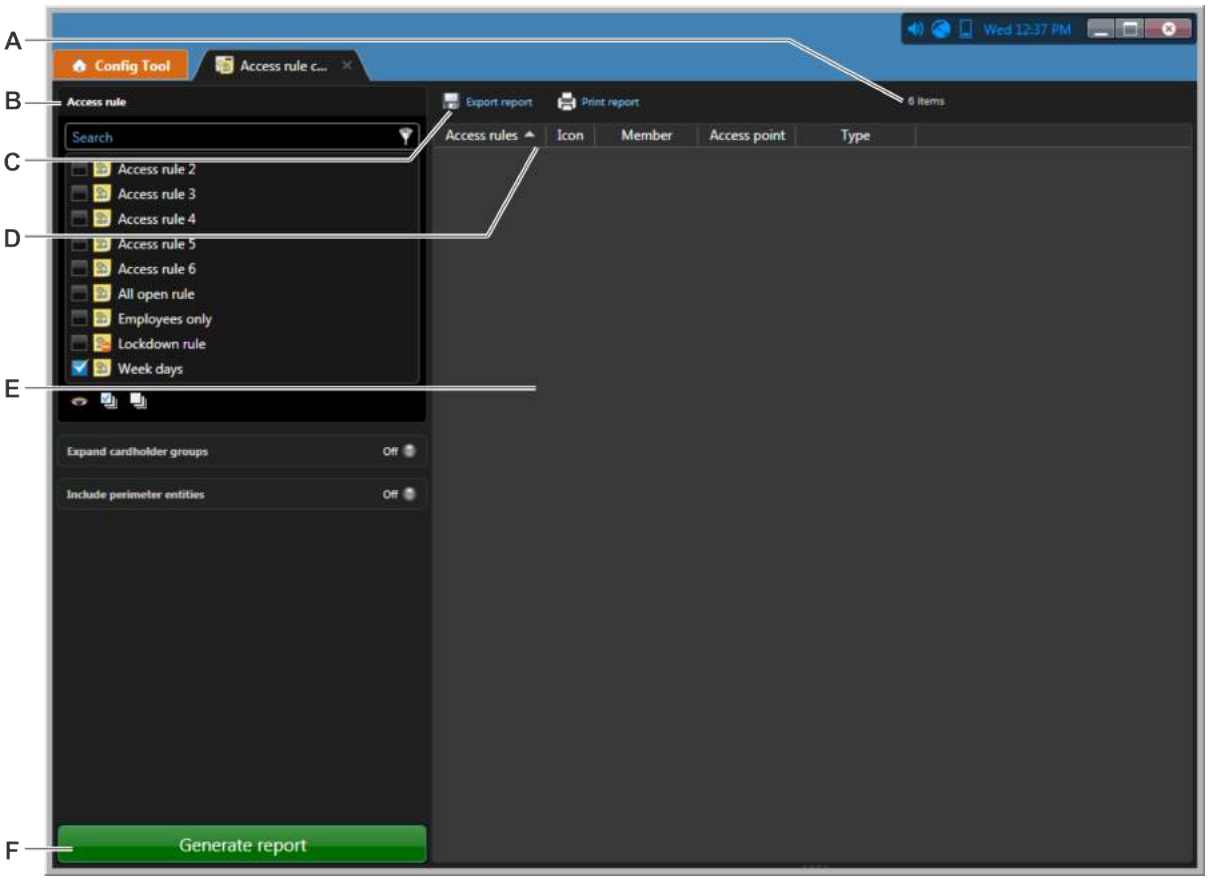
Tópicos relacionados

Descobrindo quais mudanças foram feitas na configuração do sistema na página 324
Resolver conflitos causados por entidades importadas na página 393
Copiar definições de configuração de uma entidade para a outra na página 77
Definir entidades para modo de manutenção na página 296
Criar macros na página 222
Testar alarmes na página 922

Visão geral do espaço de trabalho de manutenção

Tarefas de manutenção servem para gerar consultas personalizadas nas entidades, atividades e eventos no seu sistema Security Center para fins de manutenção e solução de problemas.

Esta seção mostra o layout da tarefa de manutenção e descreve os elementos comuns da maioria das tarefas de manutenção. A tarefa *Configuração de regra de acesso* foi usada como exemplo. Você pode abrir a tarefa Configuração de regra de acesso digitando seu nome na caixa *Pesquisa* na página inicial.



A	**Número de resultados**	Exibe o número do retorno de resultados. Uma advertência é feita quando a sua pesquisa retorna com barras demais. Se isso ocorrer, ajuste os filtros de pesquisa para reduzir o número de resultados.
B	**Filtros de pesquisa**	Usar os filtros na guia consulta para definir sua consulta. Clique em um cabeçalho de filtro para ativar ou ( ) desativar. Filtros inválidos aparecem como *Advertência* ou *Erro*. Passe o mouse sobre o filtro para visualizar o motivo pelo qual é inválido.
C	**Exportar/ imprimir relatório**	Clique para exportar ou imprimir o relatório assim que for gerado.
D	**Selecionar colunas**	Clique com o botão direito em um cabeçalho de coluna para selecionar quais colunas exibir.

E	**Painel de relatório**	Visualizar os resultados do seu relatório. Arraste um item da lista para um ladrilho na tela ou clique com o botão direito em um item na lista para visualizar mais opções associadas àquele item, se for aplicável.
F	**Gerar relatório**	Clique para executar o relatório. Esse botão é desativado se nenhum filtro de pesquisa tiver sido selecionado ou quando houver filtros inválidos. Enquanto a consulta estiver em execução, o botão muda para *Cancelar*. Clicar em *Cancelar* para interromper a consulta.

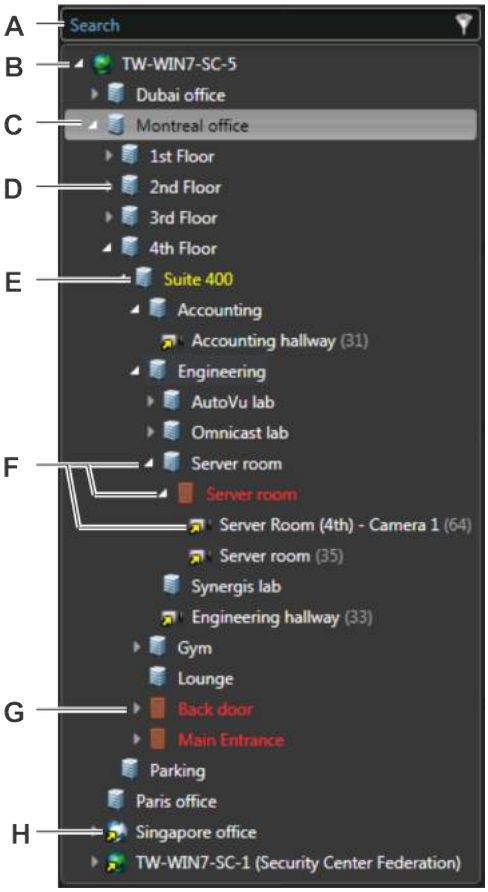
Sobre a exibição de área

Usando a visualização da área, é possível encontrar e visualizar todas as entidades no seu sistema rapidamente.

As *entidades* na visualização da área estão organizadas em hierarquia (ou *árvore de entidades*) de acordo com suas relações lógicas com as *áreas*. Por exemplo, as portas que levam a uma área e outros dispositivos localizados na área, como câmeras, estão exibidos abaixo daquela área na hierarquia como *entidades secundárias*.

Na visualização da área, é possível executar as seguintes ações:

- Encontrar entidades que deseja visualizar na tela.
- Arrastar entidades múltiplas da visualização da área na tela.
- Renomear as entidades locais.
- Alternar para as páginas de configuração de entidades, se tiver os privilégios necessários.



A	**Caixa de busca**	Digite na caixa de *Pesquisa* para encontrar as entidades que contêm esse texto na sua categoria, nome ou descrição.
B	**Entidade do sistema**	A entidade do sistema ( ) não pode ser visualizada na tela.
C	**Comandos adicionais**	Clique com o botão direito na visualização da área para usar os comandos adicionais, como criar ou excluir entidades, diagnosticar a entidade selecionada, lançar um relatório na entidade selecionada ou atualizar a visualização da área.

D	**Entidade da área**	Entidades da área ( ) podem representar um conceito ou local físico. É um agrupamento lógico.
E	**Entidade amarela**	Toda vez que o nome de uma entidade estiver exibido em amarelo, significa que existe um problema nas configurações.
F	**Ícones de seta**	Clique nas setas na árvore de entidades para exibir ou ocultar entidades secundárias.
G	**Entidade vermelha**	Indica que a entidade está offline e que o servidor não consegue se conectar a ela ou o servidor está offline.
H	**Entidade federada**	Todas as entidades importadas dos *sistemas federados* são exibidas com uma seta amarela sobreposta ao ícone regular da entidade ( ). São chamadas de *entidades federadas*.

Acerca de áreas

Uma entidade de área representa um conceito ou local físico (sala, andar, edifício, fábrica etc.) usada para agrupar outras entidades no sistema.

Você pode usar áreas para agrupar entidades do sistema de maneira lógica ou para impedir que usuários não autorizados visualizem entidades selecionadas do sistema. Uma área protegida é uma entidade de área que representa um local físico onde o acesso é controlado. Uma área protegida consiste em portas de perímetro (portas usadas para entrar ou sair da área) e restrições de acesso (regras que regem o acesso à área).

Tópicos relacionados

Organizar a exibição de área na página 26
Definir quem pode acessar o Security Center na página 340
Sobre áreas protegidas na página 629

Organizar a exibição de área

Como o administrador do sistema, você precisa criar uma estrutura de visualização de área que seja fácil para todos entenderem e navegar.

O que você deve saber

Você pode reorganizar as entidades na visualização da área arrastando-as para outra área, selecionando múltiplas entidades de uma vez e arrastando-as para outra área, renomeando entidades e copiando entidades. Você também pode criar e excluir entidades.

NOTA: Não é possível editar os nomes das entidades federadas.

O modo como você estrutura a exibição de área no Config Tool também é como ela será exibida no Security Desk.

Para organizar a área de visualização:

1 Na página inicial do Config Tool, abra a tarefa *Exibição de área*.

NOTA: A *tarefa* de exibição de área no Config Tool é o único local onde você pode mudar a estrutura da exibição de área. Não confunda esta tarefa administrativa com a *aba* de exibição de área encontrada na maioria das tarefas de investigação disponíveis no Security Desk.

2 Para mover as entidades em outra área, faça um dos seguintes:

- Selecione uma área ou entidade e então arraste-a para uma área diferente.
- Mantenha pressionada a tecla Shift, selecione várias entidades e arraste-as para uma área diferente.

As entidades selecionadas agora são entidades secundárias daquela área (abaixo daquela área na hierarquia).

3 Para renomear uma entidade, selecione a entidade, pressione **F2**, digite um novo nome e pressione **ENTER**.

DICA: Você pode renomear qualquer entidade da visualização de área de qualquer tarefa, desde que você tenha o privilégio administrativo para modificar aquela entidade.

4 Para copiar uma entidade para outra área, mantenha pressionada a tecla Ctrl e arraste a entidade para aquela área.

Uma cópia da entidade é criada na área. Se você tiver copiado uma área em outra área, todas as suas entidades secundárias (entidades abaixo daquela área) também serão copiadas.

5 Se necessário, crie novas áreas para agrupar entidades.

6 Se necessário, exclua entidades.

Criar áreas

Para organizar a visualização de área, use áreas para agrupar entidades com base em seus relacionamentos lógicos ou físicos.

O que você deve saber

- Uma área é um conceito ou local físico (sala, andar, edifício, fábrica, etc.) usado para o agrupamento lógico de entidades no sistema.
- Você pode criar áreas em qualquer parte da hierarquia de exibição de áreas.

Para criar uma área:

1 Abra a tarefa *Exibição de área*.
2 Clique em uma partição ( ) ou em uma entidade de área ( ) na qual queira criar a nova área.
3 Clique em **Adicionar uma entidade** ( ) > **Área**.
4 Digite um nome para a área e pressione **ENTER**.

Após terminar

Se você estiver definindo uma área para controle de acesso, proteja a área.

Tópicos relacionados
Organizar a exibição de área na página 26

Ligar e desligar recursos

Para simplificar sua interface, você pode desativar os recursos que não esteja usando.

Para ligar e desligar recursos:

1 Abra a tarefa **Sistema**, clique na visualização **Configurações gerais** e, em seguida, clique na página *Recursos*.

2 Selecione os recursos que deseja usar e limpe as opções dos recursos que você deseja desligar.

NOTA: Você somente pode selecionar entre recursos que sejam suportados por sua licença. Os recursos não suportados não são listados.

3 Clique em **Aplicar**.

Exemplo

A integração do Active Directory é um recurso que é suportado como padrão em sua licença. Porém, se você não planejar importar usuários de um Active Directory do Windows, você poderá desativar o recurso do Active Directory para que ele deixe de estar disponível.

Configurar a bandeja de notificação

Você pode escolher quais ícones exibir na bandeja de notificação.

O que você deve saber

A bandeja de notificação aparecerá no canto superior direito do aplicativo como padrão.

As configurações de bandeja de notificação são salvas como parte do seu perfil de usuário e se aplicam ao Security Desk e Config Tool.

MELHOR PRÁTICA: É uma boa ideia exibir os ícones que são usados diariamente, para que seja possível pular para as tarefas associadas.

Para personalizar os ícones da bandeja de notificação:

1 Na página inicial, clicar em **Opções** > **Visual**.
2 Na lista suspensa ao lado dos ícones na seção **Bandeja**, selecione como você deseja exibir cada item:
- **Mostrar:** Sempre exibir o ícone.
- **Ocultar:** Sempre ocultar o ícone.
- **Mostrar apenas notificações:** Exibir somente o ícone quando houver uma notificação.

3 Clique em **Salvar**.

Tópicos relacionados
Visão geral da página inicial na página 13

Ícones da bandeja de notificação

A tabela a seguir lista os ícones da bandeja de notificação e para o que eles podem ser usados.

Ícone	Nome	Descrição
	**Relógio**	Exibe a hora local Deixe o cursor do mouse sobre aquela área para ver a data atual na dica de ferramenta. Você pode personalizar as configurações de fuso horário.
	**Medidor de recursos**	Exibe o uso dos recursos do computador (CPU, memória, GPU e rede). Coloque o cursor do mouse sobre o ícone para visualizar o uso de recursos em porcentagem. Clique na caixa de diálogo Informações de hardware para visualizar informações adicionais e dicas para solução de problemas.
	**Informação de sessão**	Exibe o nome de usuário atual e o nome do diretório Security Center. Clique para alternar entre a tela longa e a curta.
	**Volume**	Exibe o ajuste do volume (0 ta100) de Security Desk. Clique para ajustar o volume usando a barra ou para tirar o volume.

Ícone	Nome	Descrição
	Mensagens do sistema	Exibe o número de mensagens do sistema atual (questões de saúde, advertências, mensagens e eventos de saúde) no seu sistema. Clique para abrir a caixa de diálogo de Mensagens do sistema para ler e revisar as mensagens. Se houver problemas de saúde, o ícone fica vermelho (). Se houver avisos, o ícone fica amarelo. Se houver apenas mensagens, o ícone fica azul. Para obter mais informações, consulte Visualizar mensagens do sistema na página 300.
	Atualização da versão do firmware	Aparece somente quando há atualizações do firmware da unidade atualmente em uso. A contagem de upgrade é exibida sobre o ícone. Clique no ícone para visualizar os detalhes.
	Atualizações de firmware	Aparece somente quando existem atualizações críticas de firmware necessárias. Clique no ícone para visualizar os detalhes.
	Ações do banco de dados	Aparece somente quando há atualizações do banco de dados atualmente em uso. A contagem de upgrade é exibida sobre o ícone. Clique no ícone para visualizar os detalhes.
	Adicionar status da unidade	Aparece somente quando há unidades recém-adicionadas no sistema. A unidade de contagem é exibida sobre o ícone. Clique no ícone para visualizar os detalhes.
	Processo em segundo plano	Indica que um processo está sendo executado em segundo plano, como a exportação de arquivos de vídeo. Clique no ícone para visualizar mais detalhes sobre o processo específico em execução.
	Solicitações de cartão	Exibe o número de solicitações pendentes para os cartões de credencial a serem impressos (). Clique para abrir a caixa de diálogo *Solicitações de cartão* e responda à solicitação. Para obter mais informações, consulte Responder a solicitações de cartão de credencial na página 687.
	Conversão de arquivo de vídeo	Exibe o número de arquivos G64 ou G64x atualmente sendo convertidos para o formato ASF ou MP4. Clique para abrir a caixa de diálogo Conversão e visualizar o status da conversão. Quando o ícone mudar para  , a conversão de arquivo está completa Para obter mais informações sobre como converter arquivos G64 para ASF ou para o formato MP4, consulte o *Guia do usuário Security Desk*.

Tópicos relacionados

Criar bancos de dados na página 144
Excluir bancos de dados na página 145
Fazer backup de bancos de dados na página 151
Restaurar bancos de dados na página 153

Mudar senhas

Após fazer logon no Security Center, você pode alterar a sua senha.

O que você deve saber

Como boa prática, é recomendável alterar a sua senha regularmente.

Para alterar sua senha:

1. Na página inicial, clicar em **Sobre**.
2. Na página *Sobre*, clique em **Alterar senha**.
3. Na caixa de diálogo **Alterar senha**, digite sua senha antiga e, em seguida, digite sua nova senha duas vezes.
4. Clique em **OK**.

Abrir o Security Desk pelo Config Tool

Você pode abrir o aplicativo do Security Desk na página *Ferramentas* no Config Tool.

O que você deve saber

Quando você abre o aplicativo do Security Desk pelo Config Tool, o seu logon é feito usando as mesmas credenciais com as quais você fez o logon atual.

Para abrir o Security Desk pelo Config Tool:

- Na página inicial do Config Tool, clique em **Ferramentas** > **Security Desk** ().

Enviar feedback

Você pode enviar feedback à Genetec Inc. se houver algo que você queira levar à nossa atenção, como um problema com a interface ou uma configuração que não está clara.

Para enviar feedback:

1 Na página inicial, clique em **Sobre** > **Enviar feedback**.
2 Na caixa de diálogo *Enviar feedback*, digite o seu feedback.
3 Para adicionar anexos, clique em **Anexos** e selecione entre as seguintes opções:
   - Para anexar informações do sistema, selecione **Informações do sistema**.
   - Para anexar arquivos, como um arquivo de registro, selecione **Arquivos**, clique em , selecione um arquivo e clique em **Abrir**.
   - Para anexar uma captura de sua tela atual, selecione **Capturas de tela** e clique em .

     DICA: Você pode mover a caixa de diálogo de feedback para a lateral e navegar para a tela relevante para tirar sua captura de tela enquanto ela ainda estiver aberta.
4 Clique em **Enviar**.

Coletando dados de diagnóstico

Para fins de solução de problemas, a *Ferramenta de Coleta de Dados de Diagnóstico* coleta e empacota convenientemente informações do sistema para que você possa enviá-las facilmente para o Centro de Assistência Técnica da Genetec™.

Antes de iniciar

Para executar a Ferramenta de Coleta de Dados de Diagnóstico:

- Você deve ter privilégios administrativo do Windows em seu computador.
- Você deve ter privilégios administrativos do Security Center.
- Todos os clientes e servidores devem estar na versão 5.3 SR1 ou superior.

O que você deve saber

- A ferramenta coleta diferentes tipos de informações do sistema (tipos de coleção), como informações do sistema da Genetec, coleção do Archiver e inventário de Vídeo. Veja as etapas abaixo para uma lista completa dessas coleções e o que elas podem conter.
- Executar a Ferramenta de Coleta de Dados de Diagnóstico pode ter impacto temporário sobre o desempenho do sistema.
- Se o seu sistema estiver executando o Windows XP ou 2003, os registros de eventos e os dados do monitor de desempenho não são coletados.

Para coletar informações de diagnóstico:

1 Na página inicial, clicar em **Ferramentas** > **Ferramenta de Coleta de Dados de Diagnóstico.**
2 Na caixa de diálogo, selecione um dos seguintes:
   - **Coleta de dados padrão em todos os servidores do Security Center:** Envia apenas um conjunto de coleções de dados pré-definidos (padrão)"
   - **Coleções de dados e servidores específicos:** Envia um conjunto de coleções de dados e informações do servidor que você tenha selecionado.
3 Se estiver selecionando **Coleções de dados e servidores específicos**, faça o seguinte:
   a) No painel esquerdo, selecione o(s) selecione o servidor(es) de onde precisa de informações.
   b) No painel direito, selecione os tipos de coleções específicos daquele servidor.

   Você pode escolher entre as seguintes coleções:
   - **Coleta de Informações do Sistema (padrão):** Uma coleta de dados usada para teste de diagnóstico que inclui registro de sistema e informações do sistema não específica a aplicativos Genetec. Essa coleta contém:
     - Registros de eventos Genetec
     - Registros de eventos do Sistema
     - Registros de eventos do Aplicativo
     - Registros de eventos de Segurança
     - Aplicativos instalados
     - Atualizações instaladas
     - Aplicativos rodando no momento
     - Conexões de rede ativas no momento
     - Conjuntos .NET CLR necessários para o debug

- **Coleta de Informações do Sistema Genetec (padrão):** Uma coleta de dados usada para teste de diagnóstico que inclui informações específicas de aplicativos Genetec. Contém:
  - Arquivos de configuração do Security Center.
  - Registros de traços do Security Center
  - Registro de erros do Security Desk e Config Tool (quando os clientes são selecionados)
  - Dados de monitoramento de desempenho
  - Informações de processos de execução
  - Informações de processos de execução do Security Center com conjuntos carregados
  - Dumps de memória
  - Chaves de Registro (somente as usadas ou criadas pela Genetec)
- **Coleta do Archiver:** Uma coleta de dados usada para o teste de diagnóstico que inclui informações específicas do Archiver da Genetec como o cachê e os registros do Archiver.
- **Coleta do Gerenciador de Acesso:** Uma coleta de dados usada para teste de diagnóstico que inclui informações específicas do Gerenciador de Acesso da Genetec. Inclui arquivos de configuração, conexões de rede atualmente ativas, cachê de arquivo VertX e arquivos temporários VertX.
- **Inventário da unidade de vídeo:** Uma coleta de dados usada para teste de diagnóstico que lista unidades de vídeo inscritas pelas câmeras federadas do sistema e Security Center.

4 Clique em **Iniciar**.

  As barras de status mostram o progresso para cada coleção de dados. As informações são salvas no computador de onde a ferramenta foi executada, na pasta: *C:\ProgramData\Genetec Security Center 5.7\Diagnostics*. Para o Windows XP e 2003, os dados estão salvos em: *C:\Documents and Settings\All Users \Application Data\Genetec Security Center 5.7\Diagnostics*.

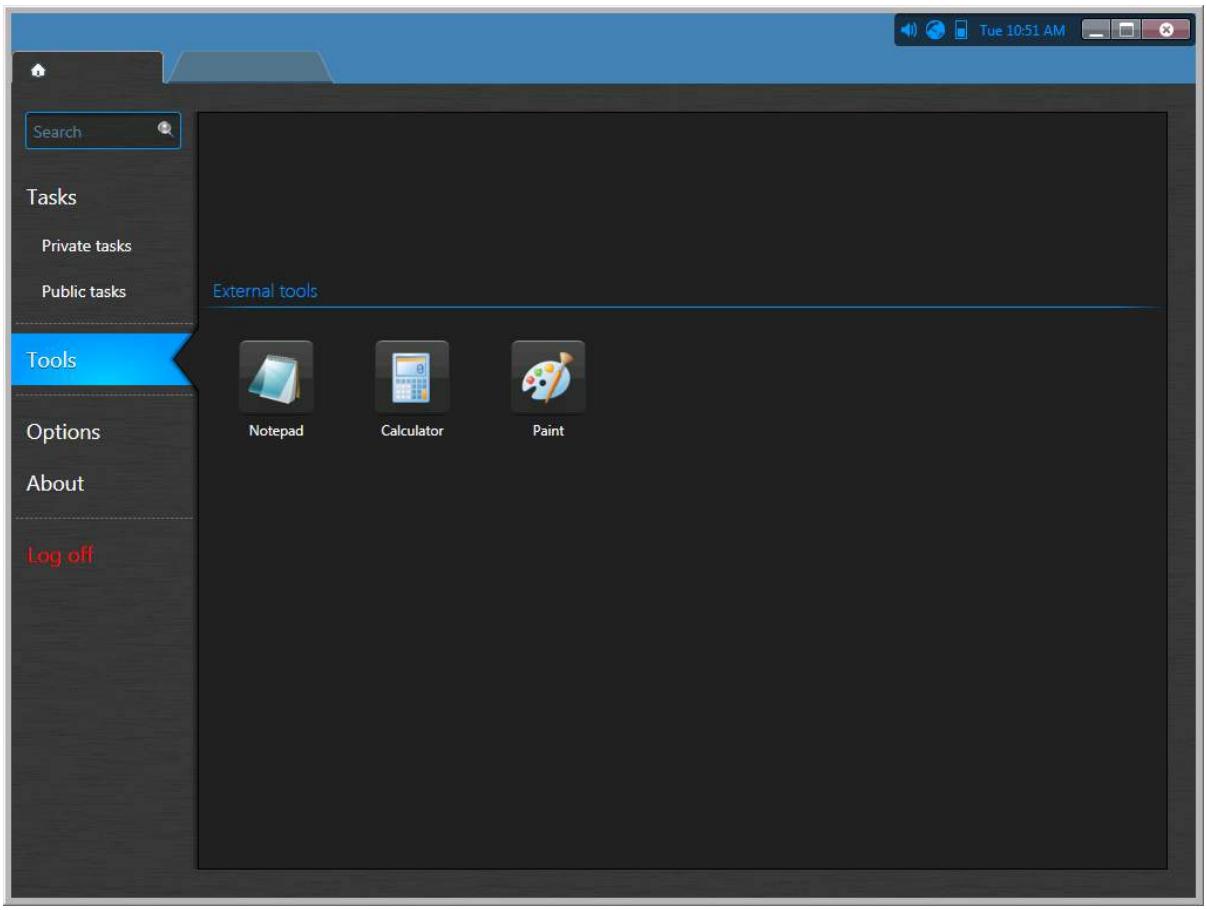
5 Para abrir a pasta, clique em **Abrir pasta de entrada**.

Você poderá então enviar as informações de diagnóstico para o Centro de Assistência Técnica da Genetec™.

Atalhos para ferramentas externas

Você pode adicionar atalhos para ferramentas e aplicativos externos usados frequentemente à página Ferramentas no Security Center modificando o arquivo *ToolsMenuExtensions.xml*.

Este arquivo está localizado em *C:\Program files (x86)\Genetec Security Center 5.7* em um computador de 64 bits e em *C:\Program files\Genetec Security Center 5.7* em um computador de 32 bits.



O conteúdo original desse arquivo tem a seguinte aparência:

```
<?xml version="1.0" encoding="utf-8"?>
<ArrayOfToolsMenuExtension xmlns:xsi="http://www.w3.org/2001/XMLSchema-...>
    <ToolsMenuExtension>
    </ToolsMenuExtension>
</ArrayOfToolsMenuExtension>
```

Cada atalho é definido por uma tag XML chamada `<ToolsMenuExtension>`. Cada tag `<ToolsMenuExtension>` pode conter quatro elementos XML:

- `<Name>` – Nome do comando exibido na página Ferramentas .
- `<FileName>` – Comando a ser executado (arquivo executável).
- `<Icon>` – (Opcional) Arquivo de ícone alternativo (.ico). Use este elemento para substituir o ícone padrão extraído do arquivo executável.
- `<Arguments>` – (Opcional) Argumentos de linha de comando, quando aplicáveis.

Todos os nomes de tags XML diferenciam maiúsculas e minúsculas. Você pode editar este arquivo XML com qualquer editor de texto. As alterações a este arquivo somente se tornarão efetivas na próxima vez que você lançar o Security Desk.

NOTA: Se um caminho não for fornecido na tag <FileName>, o aplicativo não será capaz de extrair o ícone associado ao executável. Nesse caso, forneça explicitamente um ícone com a tag <Icon>.

Exemplo

O seguinte arquivo de exemplo adiciona os três atalhos (*Bloco de notas*, *Calculadora* e *Paint*) à página Ferramentas . O atalho para o *Bloco de notas* está configurado para abrir o arquivo *C:\SafetyProcedures.txt* quando você clicar nele.

```
<?xml version="1.0" encoding="utf-8"?>
<ArrayOfToolsMenuExtension xmlns:xsi="http://www.w3.org/2001/XMLSchema-...>
    <ToolsMenuExtension>
        <Name>Notepad</Name>
        <FileName>c:\windows\notepad.exe</FileName>
        <Arguments>c:\SafetyProcedures.txt</Arguments>
    </ToolsMenuExtension>
    <ToolsMenuExtension>
        <Name>Calculator</Name>
        <FileName>c:\windows\system32\calc.exe</FileName>
    </ToolsMenuExtension>
    <ToolsMenuExtension>
        <Name>Paint</Name>
        <FileName>c:\windows\system32\mspaint.exe</FileName>
    </ToolsMenuExtension>
</ArrayOfToolsMenuExtension>
```

2

Tarefas

Esta seção inclui os seguintes tópicos:

- "Abrir tarefas" na página 39
- "Salvar tarefas" na página 40
- "Organização das tarefas salvas" na página 42
- "Adicionar tarefas em sua lista Favoritos lista" na página 43
- "Enviar tarefas " na página 44
- "Mover a barra de tarefas" na página 45
- "Personalizar comportamento de tarefas" na página 46

Abrir tarefas

Para executar a maioria das ações no Security Center, primeiro é preciso abrir as tarefas.

O que você deve saber

Algumas tarefas do Security Center podem ter apenas uma instância e as outras podem ter várias. Tarefas de instância única não podem ser renomeadas.

Para abrir uma tarefa:

1 Na página inicial, fazer uma das seguintes ações:
- Digite o nome da tarefa na caixa *Pesquisar* .
- Clicar na guia *Tarefas* e, depois, clicar **Pesquisar todas as tarefas**
- Para abrir uma tarefa salva, clique na aba **Tarefas privadas** ou **Tarefas públicas** .

2 Clique na tarefa.

Se somente uma instância é permitida, a nova tarefa é criada.

3 Se mais de uma instância da tarefa for permitida, digite o nome da tarefa e clique em **Criar**.

A nova tarefa abre e é adicionada a sua lista de tarefas.

4 (Somente tarefas administrativas) Se a tarefa contém mais de uma visualização de entidade, selecione uma visualização para configurar.

Tarefas que permitem que você configure mais de uma entidade são indicadas com um sinal de mais no ícone da tarefa.

Exemplo

Assista a este vídeo para saber mais. Clique no ícone **Legendas** (**CC**) para ligar a legenda do vídeo em um dos idiomas disponíveis. O vídeo pode não ser exibido no Internet Explorer. Para resolver isso, abra as **Configurações de compatibilidade de exibição** e limpe **Exibir sites da intranet em Visualizar compatibilidade**.

Tópicos relacionados

Visão geral da página inicial na página 13

Salvar tarefas

Você pode salvar suas tarefas em uma lista de tarefas privadas que somente você possa acessar ou em uma lista de tarefas públicas que possa ser acessada por qualquer um.

O que você deve saber

Quando você salva uma tarefa, o filtro de consulta, o layout da tarefa (ordem das colunas do painel do relatório, layout de tela e assim por diante) e as entidades exibidas em cada ladrilho também são salvos.

NOTA: Os resultados da consulta não são salvos. Eles são gerados novamente cada vez que você executa a consulta.

Os benefícios de salvar uma tarefa são os seguintes:

- Você pode fechar sua tarefa e recarregá-la com o mesmo layout quando precisar dela.
- Você pode compartilhar tarefas públicas com outros usuários.
- Você pode usar tarefas públicas como modelo de relatório com a ação *Enviar relatório por e-mail*.

Para salvar uma tarefa:

1 Clique com o botão direito na aba da tarefa e clique em **Salvar como**.

NOTA: O botão **Salvar como** só fica disponível se os filtros de consulta do relatório forem válidos. Você saberá que sua consulta é válida quando o botão **Gerar relatório** ficar ativado.

2 Na caixa de diálogo *Salvar tarefa*, selecione como você deseja salvar a tarefa:

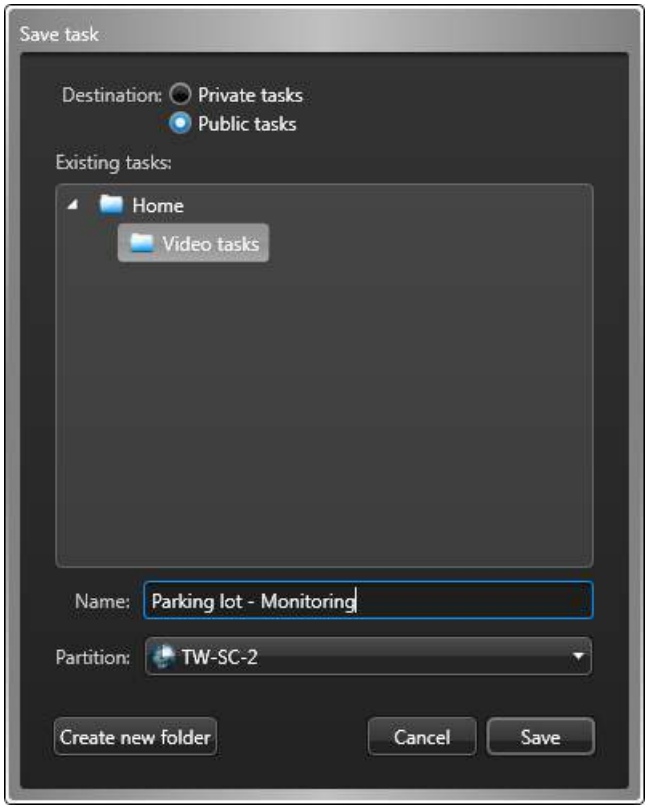
- **Tarefas privadas:** Uma tarefa privada é uma tarefa somente visível para o usuário que a criou.
- **Tarefas públicas:** Uma tarefa pública é uma tarefa salva que pode ser compartilhada e reutilizada entre vários usuários do Security Center.

3 (Opcional) Para salvar uma tarefa em uma pasta na página **Tarefas privadas** ou **Tarefas públicas**, clique em **Criar nova pasta**, digite um nome para a pasta e clique em **Criar**.

Se você selecionar a pasta **Início**, ou se você não selecionar uma pasta, a tarefa será salva na página principal da página **Tarefas privadas** ou **Tarefas públicas**.

4 Digite um nome para a tarefa salva ou selecione um existente para sobrescrevê-la.

Exemplo: Você pode salvar uma tarefa de Monitoramento que exibe suas câmeras em estacionamentos com o nome *Estacionamento - Monitoramento* ou salvar uma tarefa de investigação que pesquise marcadores de vídeo adicionados nas últimas 24 horas com o nome *Marcadores de hoje*.



5 (Somente para tarefas públicas) Selecione a *partição*à qual você quer que a tarefa pertença.
Somente usuários que sejam membros da partição poderão visualizar ou modificar esta tarefa pública.

6 Clique em **Salvar**.

Após terminar

- Para salvar alterações que você faça à tarefa, clique com o botão direito na aba da tarefa e clique em **Salvar**.
- Se você alterar o layout da tarefa (por exemplo, redimensionar ou ocultar colunas de relatório), você poderá reverter para o layout usado quando a tarefa foi salva clicando com o botão direito na aba da tarefa e clicando em **Recarregar**.

Tópicos relacionados

Visão geral da página inicial na página 13

Organização das tarefas salvas

Se você tiver muitas tarefas privadas salvas no Security Desk ou no Config Tool, você poderá organizá-las em pastas para encontrá-las facilmente.

O que você deve saber

Uma tarefa privada é uma tarefa somente visível para o usuário que a criou. Uma tarefa pública é uma tarefa salva que pode ser compartilhada e reutilizada entre vários usuários do Security Center.

Organização das tarefas salvas:

1. Na página inicial do Security Desk ou Config Tool, clique em **Tarefas privadas** ou **Tarefas públicas**.
2. Para criar uma nova pasta, clique com o botão direito na página **Tarefas privadas** ou **Tarefas públicas** e clique em **Criar pasta**.
3. Digite um nome para a pasta e, depois, clique em **Criar**.

   Para renomear a pasta, clique com o botão direito na pasta e clique em **Renomear**.
4. Para mover uma pasta faça um dos seguintes:
   - Arraste a pasta para dentro de outra pasta.
   - Clique com o botão direito sobre a pasta e clique em **Mover**. Na caixa de diálogo *Mover* para, selecione uma pasta existente ou clique em **Criar nova pasta** e, em seguida, clique em **Mover**.
5. Para classificar as tarefas, clique com o botão direito em uma pasta, clique em **Classificar** e então selecione uma das seguintes opções:
   - **Classificar por tipo:** Classificar as tarefas salvas que não estão em pastas por seus tipos de tarefa.
   - **Classificar por nome:** Classificar as pastas e as tarefas salvas em ordem alfabética.
6. Para excluir uma pasta, clique com o botão direito na pasta e clique em **Excluir**.

Adicionar tarefas em sua lista Favoritos lista

Você pode adicionar tarefas e ferramentas em sua Favoritos para que elas sejam listadas ao lado de Itens recentes na sua página inicial no lugar da lista completa de tarefas.

O que você deve saber

As tarefas que você adiciona na lista Favoritos são específicas da sua conta de usuário. As tarefas que aparecem na lista Favoritos não aparecem na lista Itens recentes .

Para adicionar uma tarefa em sua lista Favoritos :

1 Fazer um dos seguintes:

- Na página inicial, mova o ponteiro do mouse sobre uma tarefa e clique em **Adicionar a Favoritos** (☆).
- Na página inicial, arraste uma tarefa da lista *Itens recentes* para a lista Favoritos .
- Clique com o botão direito na aba da tarefa e clique em **Adicionar a Favoritos**.

2 Para remover uma tarefa da lista Favoritos , execute uma das seguintes ações:

- Na página inicial, mova o ponteiro do mouse sobre uma tarefa e clique em **Remover dos Favoritos** (★).
- Clique com o botão direito na aba da tarefa e clique em **Remover dos Favoritos**.

Ocultar as Favoritos e Itens recentes listas da sua página inicial

Você pode desativar a exibição de Favoritos e Itens recentes listas em sua página inicial para que a lista de tarefas completa seja sempre exibida em vez disso.

O que você deve saber

Quando você desativa a exibição das Favoritos e Itens recentes listas em sua página inicial, o sistema não esquece os itens que estão registrados nessas listas. Mesmo quando este recurso está desativado, o sistema continua a acompanhar os seus itens usados recentemente.

Para ocultar as Favoritos e Itens recentes listas da sua página inicial:

1 Na página inicial, clique em **Opções> Visual**.
2 Limpe a opção **Exibir itens recentes e favoritos na página inicial**.
3 Clique em **Salvar**.

A partir de agora, somente a lista de tarefas completa será exibida quando você clicar em **Tarefas** na página inicial.

Enviar tarefas

Se tiver selecionado entidades específicas para monitorar ou tiver configurado filtros de consulta específicos para uma tarefa de investigação, você pode compartilhar o layout da tarefa com outro usuário ou um monitor do Security Desk através do envio da tarefa.

Antes de iniciar

Por padrão, quando uma tarefa é recebida, uma janela de confirmação é exibida na estação de trabalho e um usuário deve aceitar a tarefa antes de ela ser carregada no Security Desk. Se você estiver enviando tarefas para um monitor do Security Desk e não desejar que a janela de confirmação seja exibida, desabilite a opção Solicitar confirmação ao abrir tarefas enviadas por outros usuários na caixa de diálogo *Opções* na estação de trabalho receptora.

O que você deve saber

Enviar tarefas para um monitor do Security Desk é tipicamente usado para estações de trabalho com vários monitores, como uma tela de vídeos. Com este recurso, você pode enviar uma tarefa diretamente para um monitor específico na tela sem a necessidade da intervenção de um operador.

Para enviar uma tarefa, os destinatários devem estar online. Se você estiver enviando uma tarefa para um monitor do Security Desk, um usuário deve estar conectado nessa estação de trabalho.

Para enviar uma tarefa:

1. Abra a tarefa que deseja enviar.
2. Configure a tarefa.

   Exemplo: Você pode modificar o layout de ladrilhos, exibir certas câmeras, configurar filtros de consulta, adicionar entidades a serem monitoradas e assim por diante.
3. Clique com o botão direito na aba da tarefa e clique em **Enviar**.
4. Na caixa de diálogo *Enviar tarefa*.
5. Selecione se a tarefa é enviada para um **Usuário** ou um **Monitoramento** do Security Desk.
6. Na lista **Selecionar destino**, selecione os usuários ou monitores aos quais enviar a tarefa.
7. (Opcional) Se estiver enviando a tarefa a um usuário, escreva uma mensagem no campo **Mensagem**.
8. Clique em **Enviar**.

Se a opção Solicitar confirmação ao abrir tarefas enviadas por outros usuários estiver habilitada na estação de trabalho receptora, a solicitação de confirmação é exibida e o destinatário deve aceitar a tarefa antes de ela ser carregada.

Mover a barra de tarefas

Você pode configurar a barra de tarefas para aparecer em qualquer borda da janela do aplicativo ou configurá-la para ocultar-se automaticamente, sendo apenas exibida ao passar seu mouse sobre o local da barra de tarefas.

O que você deve saber

Ao ocultar a barra de tarefas, a bandeja de notificação também é ocultada. Estas configurações são salvas como parte do seu perfil de usuário e se aplicam ao Security Desk e Config Tool.

Para mudar a posição da barra de tarefas:

1. Na página inicial, clique em **Opções** > **Visual**.
2. Na lista suspensa **Posição da barra de tarefas**, selecione a borda onde deseja que a barra de tarefas apareça.
3. Para ocultar automaticamente a barra de tarefas, selecione a opção **Auto-ocultar a barra de ferramentas**.
4. Para mostrar o nome da tarefa atual quando *ciclo de tarefas* estiver ativado e a barra de tarefas estiver oculta, selecione a opção **Exibir nome da tarefa em sobreposição**.
5. Clique em **Salvar**.

Personalizar comportamento de tarefas

Uma vez que você esteja familiarizado com o modo de trabalhar com tarefas no Security Center, você poderá personalizar a forma como o sistema lida com tarefas na caixa de diálogo *Opções*.

O que você deve saber

As configurações de tarefas são salvas como parte do seu perfil de usuário do Security Center e se aplicam ao Security Desk e ao Config Tool.

Para customizar o comportamento das tarefas:

1 Na página inicial, clicar em **Opções** > **Interação de usuários**.

2 Na seção **Mensagens do sistema**, configure as seguintes opções como desejado:

- **Solicitar um nome quando criar uma tarefa:** Selecione esta opção se quiser Security Desk perguntar um nome sempre que criar uma tarefa que aceita várias instâncias.
- **Solicitar confirmação antes de fechar uma tarefa:** Selecione esta opção se quiser Security Desk pedir uma confirmação sempre que remover uma tarefa da interface
- **Solicitar confirmação ao abrir tarefas enviadas por outros usuários:** Selecione esta opção se quiser Security Desk pedir uma confirmação sempre que abrir uma tarefa enviada por outro usuário.

3 Na seção **Recarregar tarefa**, especifique como deseja que o Security Desk se comporte quando alguém atualizar uma *tarefa pública* que atualmente está aberta:

- *Perguntar ao usuário*. Pergunta antes de carregar a definição de tarefa atualizada.
- *Sim*. Recarrega a tarefa sem perguntar.
- *Não*. Nunca recarrega a tarefa.

4 Clique em **Salvar**.

3

Relatórios

Esta seção inclui os seguintes tópicos:

- "Sobre os relatórios visuais " na página 48
- "Gerar relatórios" na página 53
- "Gerar relatórios visuais" na página 57
- "Gerando e salvando relatórios" na página 60
- "Personalizar o painel de relatório" na página 61
- "Personalizar o comportamento dos relatórios" na página 62
- "Sobre a função do Report Manager" na página 63
- "Configurar resultados máximos para relatórios automatizados" na página 64

Sobre os relatórios visuais

Os diagramas e gráficos dinâmicos do Security Desk oferecem dados visuais que podem ser usados para realizar buscas, investigar situações e identificar padrões de atividade.

Relatórios visuais podem exibir dados no formato de um gráfico ou diagrama junto com um eixo específico ao usar linhas ou barras para representar visualmente os dados do relatório. O eixo X representa todas as etiquetas (grupo por) e o eixo Y mostra o número total de instâncias relativas ao eixo X.

No eixo X, dois tipos de agrupamento podem ser realizados:

- **Valores nominais:** Pode separar os dados em diversas colunas no eixo X. Por exemplo, os valores do eixo X podem ser classificados pelo número de instâncias e o usuário pode escolher o agrupamento (**Top 3**, **Top 5**, ou **Top 10**).
- **Datas:** Pode separar o eixo X com base em uma linha do tempo. Por exemplo, o usuário pode mudar o agrupamento de intervalo da data (**Hora**, **Dia**, **Semana**, **Mês**, ou **Ano**).

Tipos de gráficos visuais

Os seguintes tipos de gráficos são suportados no Security Center 5.7 ao usar as funções **Gerar relatório** em Security Desk: **Linhas**, **Colunas**, **Colunas empilhadas**, **Barras**, **Barras empilhadas**, **Rosca**, e **Pizza**.

Gráfico de linhas

Use um gráfico de **Linhas** quando quiser acompanhar mudanças ao longo de um período de tempo curto ou longo. Por exemplo, o número total de instâncias do relatório de dados selecionado em relação a linha do tempo.

- Gráficos de linha podem representar os dados melhor do que gráficos de barra ou coluna quando a diferença nas mudanças é pequena.
- Gráficos de linha também podem ser usados para comparar mudanças no mesmo período para mais de um grupo.

O seguinte exemplo mostra um relatório de Eventos de titular de cartão, Dividido por: **Nome**, Exibir: **Top 5** e Eixo-X: **Marca temporal do evento**, Grupo por: **Dia** como um gráfico de **Linhas** .

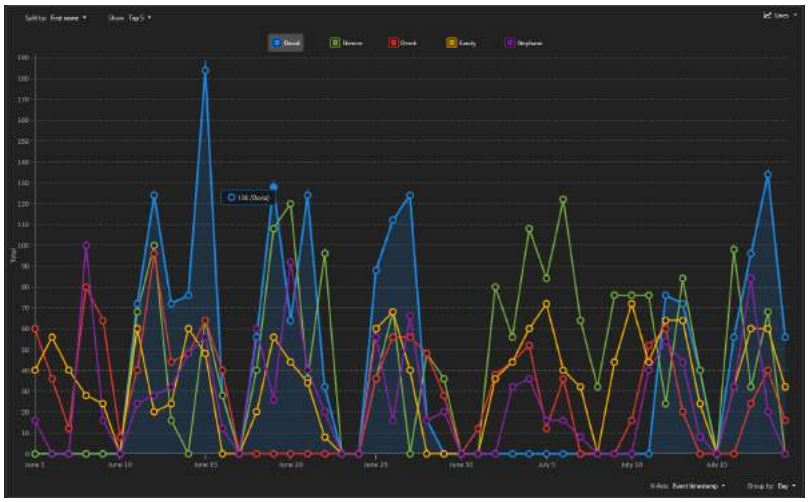
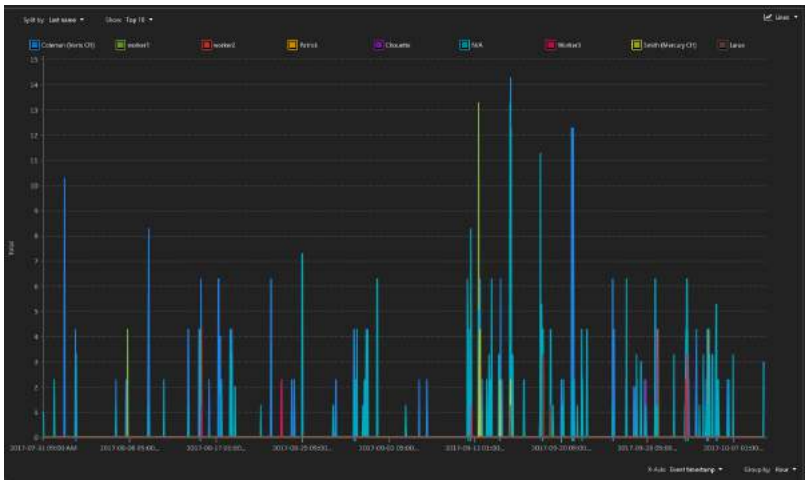


Gráfico de linhas (simplificado)

Quando o intervalo de tempo é muito amplo ou preciso, muitos dados precisam ser computados e exibidos na tela. Nessa situação, uma versão simplificada do gráfico de linhas é exibida.

O seguinte exemplo mostra uma versão simplificada de um gráfico de **Linhas** .

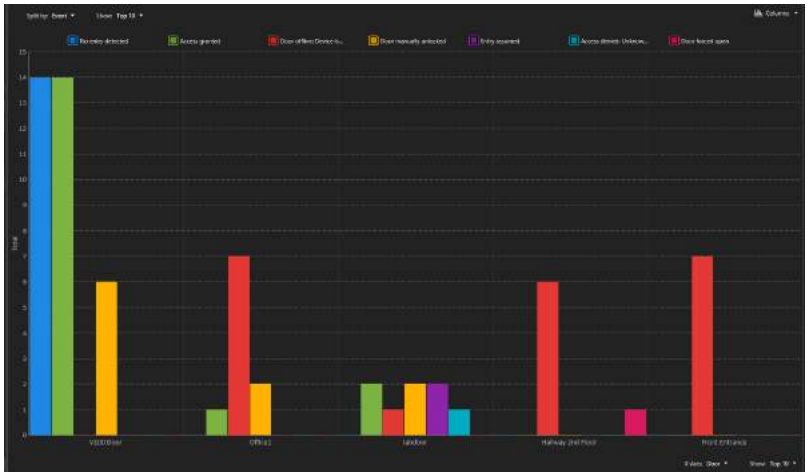


NOTA: A versão simplificada de um gráfico de linhas não tem suporte para interação com o mouse ou indicação de um valor Y para um ponto específico.

Gráfico de colunas

Use um gráfico de **Colunas** quando quiser agrupar os dados por categoria e exibir os resultados usando barras verticais.

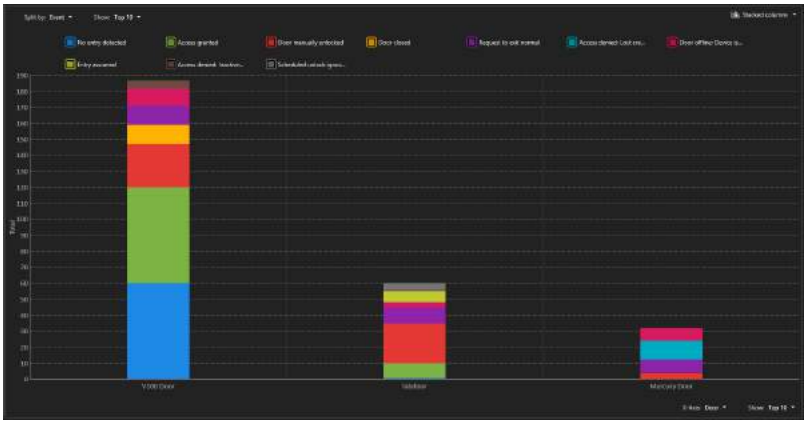
O seguinte exemplo mostra um Relatório de acesso da porta, Dividido por: **Evento**, Exibir: **Top 10** e Eixo-X: **Porta**, Exibir: **Top 10** como um gráfico **Colunas** .



Colunas empilhadas

Use um gráfico **Colunas empilhadas** quando quiser agrupar os dados por categoria e exibir os resultados usando barras verticais. O eixo Y pode ser usado para dividir os dados e ter informações mais precisas em relação ao valor de X.

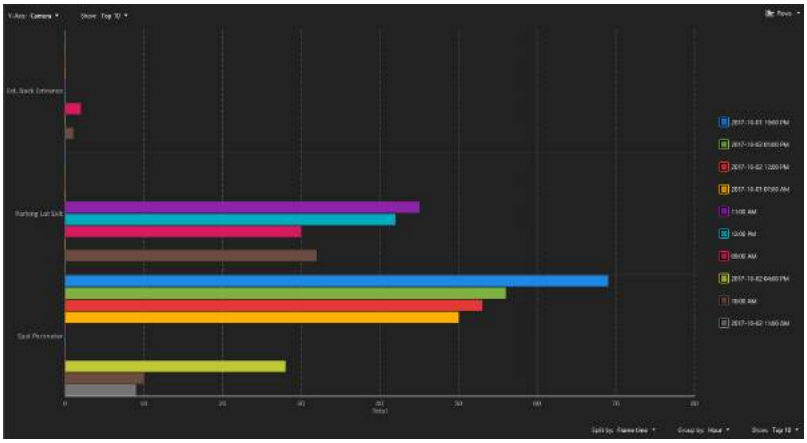
O seguinte exemplo mostra um relatório de Atividades da porta, Dividido por: **Evento**, Exibir: **Top 10** e Eixo-X: **Porta**, Exibir: **Top 10** como um gráfico de **Colunas empilhadas** .



Linhas

Use um gráfico de **Barras** quando quiser agrupar os dados por categoria e exibir os resultados usando barras horizontais.

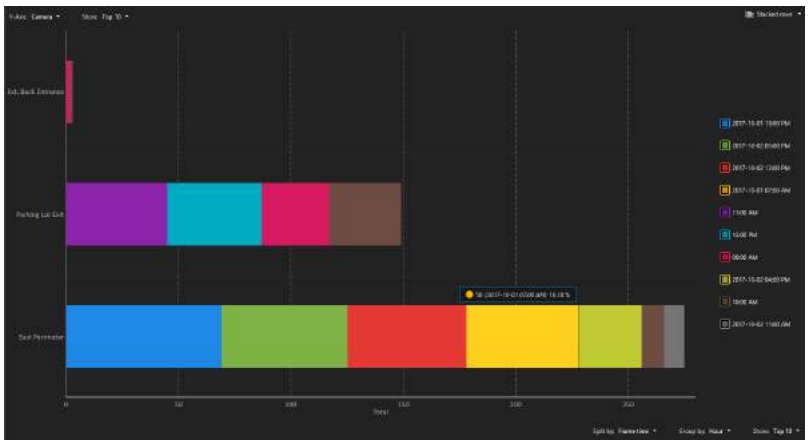
O seguinte exemplo mostra um relatório de Detector de intrusão, Eixo Y: **Câmera**, Exibir: **Top 10** e Dividido por: **Tempo do quadro**, Agrupado por: **Hora**, Exibir: **Top 10** como um gráfico **Barras** .



Barras empilhadas

Use um gráfico de **Barras empilhadas** quando quiser agrupar os dados por categoria e exibir os resultados usando barras horizontais. O eixo X pode ser usado para dividir os dados e ter informações mais precisas em relação ao valor de Y.

O seguinte exemplo mostra um relatório de Detector de intrusão, Eixo Y: **Câmera**, Exibir: **Top 10** e Dividido por: **Tempo do quadro**, Agrupado por: **Hora**, Exibir: **Top 10** como um gráfico de **Barras empilhadas** .



Gráficos de pizza e rosca

Use um gráfico Pizza ou Rosca quando quiser comparar os dados do relatório como um todo.

NOTA: Gráficos de Pizza ou Rosca não mostram mudanças ao longo do tempo.

Gráfico pizza

O seguinte exemplo mostra um relatório de movimento de Eventos de câmera, Dados: **Câmera**, Exibir: **Top 10** como um gráfico **Pizza** .

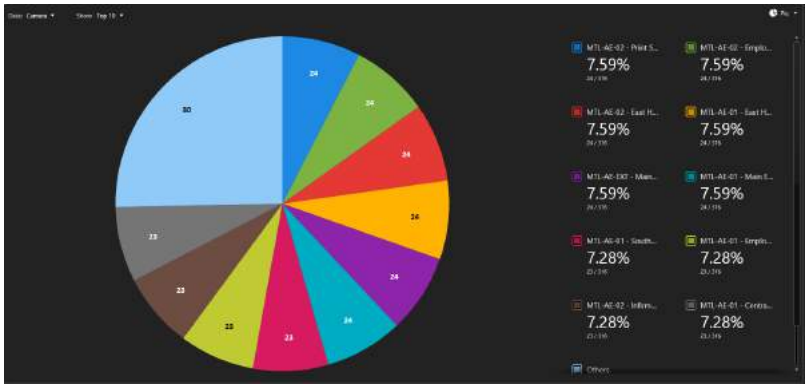
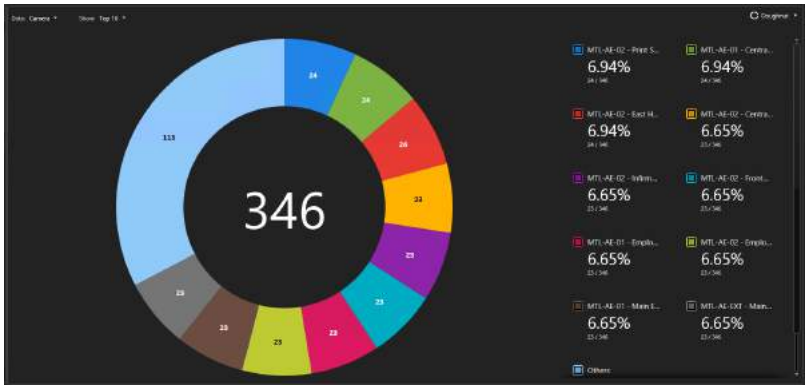


Gráfico rosca

O seguinte exemplo mostra um relatório de Eventos da câmera, Dados: **Câmera**, Exibir: **Top 10** como um gráfico **Rosca** .



Exemplo

Assista a este vídeo para saber mais. Clique no ícone **Legendas** (**CC**) para ligar a legenda do vídeo em um dos idiomas disponíveis. O vídeo pode não ser exibido no Internet Explorer. Para resolver isso, abra as **Configurações de compatibilidade de exibição** e limpe **Exibir sites da intranet em Visualizar compatibilidade**.

Tópicos relacionados

Gerar relatórios visuais na página 57

Gerar relatórios

Para gerar um relatório em qualquer tarefa de relatório, é necessário definir filtros de pesquisa e depois executar a pesquisa. Após gerar o relatório, é possível trabalhar com os resultados.

O que você deve saber

Tarefas de relatório estão onde você gera consultas personalizadas sobre as entidades, atividades e eventos no seu sistema Security Center para fins de investigação ou manutenção. A maioria das tarefas de investigação e manutenção são de relatório.

O número máximo de resultados de relatório que pode receber em Security Center é 10.000. Por padrão, o número máximo de resultados é 2.000. Esse valor pode ser alterado na seção de Desempenho da caixa de diálogo *Opções* em Security Center.

Se quiser gerar um relatório com mais de 10.000 resultados, use o comando **Gerar e salvar relatório** .

NOTA: Esses passos descrevem somente o processo geral para executar um relatório.

Para gerar um relatório:

1 Abra uma tarefa de relatório existente, ou crie uma nova.

2 Na aba *Filtros* , use os filtros de pesquisa para criar uma busca personalizada.

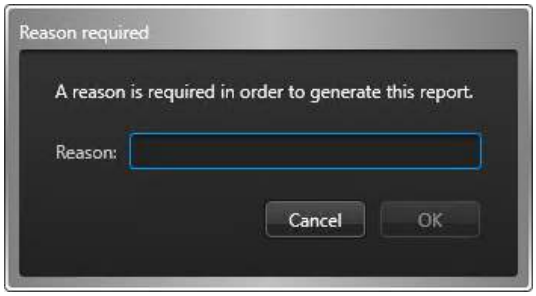
NOTA: Alguns desses filtros têm um botão **Selecionar Todos** . Esse botão não aparece se existir mais de 100 entidades a selecionar (por exemplo, se tiver uma lista de 1500 titulares de cartão), porque se pesquisar entidades em excesso, o relatório leva muito tempo para ser gerado.

3 Defina uma data e intervalo de tempo para o relatório.

4 Clique em **Gerar relatório**.

Se houver filtros inválidos, o botão **Gerar relatório** fica indisponível.

IMPORTANTE: O diálogo *Motivo necessário* é exibido ao gerar qualquer relatório que contenha dados LPR.



Isso garante que o motivo para a pesquisa LPR esteja registrado e incluído em registro de auditoria de trilha de atividade (relatório gerado) em conformidade com as leis estaduais.

Os resultados da pesquisa são exibidos no painel do relatório.

DICA: É possível classificar os resultados por coluna. Também é possível clicar com o botão direito na fileira de títulos para selecionar colunas, depois adicionar ou remover colunas conforme a necessidade.

5 Analise os resultados da pesquisa.

Os resultados de pesquisa dependem do tipo de tarefa de relatório. Quando as sequências de vídeo ou dados LPR estão relacionados aos resultados de pesquisa, é possível visualizá-los na tela ao arrastar um item do relatório a um ladrilho.

6 Trabalhe com os resultados da pesquisa.

Dependendo dos itens nos resultados de pesquisa, é possível imprimir o relatório, salvar o relatório como um documento Excel ou PDF, exportar as sequências de vídeo, etc.

7 (Opcional) Salvar o relatório como modelo.

Se salvar o layout do relatório (filtros de pesquisa e colunas de relatório) como um modelo, ele pode ser enviado a outro usuário ou estação de trabalho usando a ação *Enviar relatório por e-mail* .

Exemplo

Assista a este vídeo para saber mais. Clique no ícone **Legendas** (**CC**) para ligar a legenda do vídeo em um dos idiomas disponíveis. O vídeo pode não ser exibido no Internet Explorer. Para resolver isso, abra as **Configurações de compatibilidade de exibição** e limpe **Exibir sites da intranet em Visualizar compatibilidade**.

Tópicos relacionados

Personalizar o painel de relatório na página 61
Personalizar o comportamento dos relatórios na página 62
Gerar relatórios visuais na página 57
Tarefa LPR - Visualização de configurações gerais na página 1086

Exportar relatórios gerados

Em toda tarefa de relatório, é possível exportar seu relatório após gerado. Para exportar os dados do relatório como uma lista (formato CSV, Excel ou PDF), use a opção *Dados* . Para exportar os dados do relatório como um gráfico (JPEG ou PNG), use a opção *Gráfico* . Alternativamente, é possível selecionar as duas opções para gerar uma lista e gráfico de relatório.

O que você deve saber

O número máximo de resultados de relatório que podem ser exportados é 10.000.

Para exportar um relatório gerado:

1 Na parte superior do painel de relatório, clique em **Exportar relatório** ( ).

2 Na caixa de diálogo, selecione **Dados**, **Gráfico** ou ambos e defina as seguintes opções:

- **Formato de arquivo:** (Somente dados) Selecione o formato do arquivo (CSV, Excel ou PDF). (Somente gráficos) Selecione o formato do arquivo (JPEG ou PNG).
- **Arquivo de destino:** Selecione o nome do arquivo.
- **Orientação:** (Somente PDF) Selecione se o arquivo PDF deve estar no modo retrato ou paisagem.
- **Pasta de arquivos anexados:** (Somente CSV) Especificar quando os arquivos anexados, como fotos dos titulares do cartão ou das placas, são salvas.

NOTA: A caixa de diálogo de opções exibida pode variar consoante o relatório seja ou não compatível com Gráficos (Diagrama). A função Gráficos não é suportada para os seguintes relatórios: Resolução de Problemas da Porta, Explorador de Arquivos de Vídeo e Pesquisa de Movimento.

3 Clique em **Exportar**.

Imprimir relatórios gerados

Em toda tarefa de relatório, é possível imprimir seu relatório após ser gerado. Para imprimir os dados de relatório como uma lista, use a opção *Imprimir dados*. Para imprimir um relatório visual ou gráfico, use a opção *Imprimir gráfico*.

O que você deve saber

NOTA: No momento, NitroPdf não é suportado.

Para imprimir um relatório (Imprimir dados):

1 No topo do painel de relatórios, clique em **Imprimir relatório** (), depois clique em **Imprimir dados**.
2 Na Prévia do relatório janela, clique em **Imprimir** e selecione uma impressora.

DICA: Também é possível exportar () a visualização do relatório como documento Microsoft Excel, Word ou Adobe PDF.

Para imprimir um relatório visual (Imprimir gráfico):

1 No topo do painel de relatórios, clique em **Imprimir relatório** (), depois clique em **Imprimir gráfico**.
2 Na janela *Imprimir*, selecione uma impressora e clique em **Imprimir**.

Personalizar configurações de fuso horário

Se o seu sistema Security Center incluir dispositivos operando em diferentes fusos horários, você deverá selecionar se as consultas de relatórios são baseadas em um fuso horário fixo ou no fuso horário local de cada dispositivo.

O que você deve saber

As configurações de fuso horário afetam o modo como os filtros de intervalo de tempo no seu relatório funcionam. Se você selecionar um fuso horário fixo, os resultados que vierem de um dispositivo (como uma *unidade de controle de acesso* ou uma *unidade de vídeo*) em outro fuso horário serão ajustados para as diferenças de horário.

As configurações da fuso horário são salvas como parte do seu perfil de usuário e se aplicam ao Security Desk e ao Config Tool.

Para personalizar as configurações de fuso horário:

1 Na página inicial, clicar em **Opções** > **Data e hora**.
2 Para adicionar abreviaturas de fuso horário a todos os carimbo de data/hora no Security Center, selecione a opção **Exibir abreviaturas dos fusos horários**.
3 Selecione como os campos de data/hora são exibidos e interpretados no Security Center:

- Para exibir e interpretar a data/hora de acordo com o fuso horário local de cada dispositivo, selecione a opção **fuso horário de cada dispositivo**.

  Esta opção permite que cada dispositivo siga um fuso horário diferente. Selecione esta opção para exibir e interpretar o tempo de acordo com o fuso horário local de cada dispositivo.

- Para exibir e interpretar a data/hora de acordo com um fuso horário fixo, selecione a opção **fuso horário seguinte** e escolha um fuso horário na lista suspensa.

4 Clique em **Salvar**.

Exemplo

Se você criar um relatório com um intervalo de tempo entre 9:00 e 10:00. Horário da Costa Leste e dispositivos localizadas em Vancouver (horário do Pacífico) estiverem incluídos na pesquisa, um dos seguintes acontecerá com base em suas configurações de fuso horário:

- Fuso horário baseado no fuso horário local de cada dispositivo: Os resultados do relatório são de eventos que ocorreram entre as 9:00 e as 10:00 no Horário do Pacífico.

- Fuso horário fixo (definido para a hora de Leste): Os resultados do relatório são de eventos que ocorreram entre as 6:00 e as 7:00 no fuso horário do Pacífico, devido à diferença de três horas entre Montreal e Vancouver.

Gerar relatórios visuais

Para gerar um relatório visual em qualquer tarefa de relatório é necessário definir os filtros de pesquisa e depois executar a pesquisa. Após gerar o relatório, é possível trabalhar com os seus resultados usando diagramas e gráficos.

Antes de iniciar

- É necessário ter uma licença de relatório visual para usar a função de gráficos nos relatórios.
- Somente usuários com privilégios de *visualização de gráficos* podem acessar os relatórios visuais de gráficos.

O que você deve saber

Tarefas de relatório estão onde você gera consultas personalizadas sobre as entidades, atividades e eventos no seu sistema Security Center para fins de investigação ou manutenção. A maioria das tarefas de investigação e manutenção são de relatório.

Aqui estão alguns exemplos de casos de uso de *relatórios visuais*:

- Omnicast™ Tarefa de eventos de câmera: Visualizar relatórios de câmeras como gráficos para entender a atividade de múltiplas câmeras, durante um período de tempo específico.
- KiwiVision™ Relatório de detecção de intrusão: Executar relatórios visuais para obter uma visão global do seu ambiente de segurança.
- Synergis™ Atividades da porta: Visualizar eventos como gráficos e diagramas para obter informações sobre o seu sistema de controle de acesso.
- AutoVu™ leitura de tarefa: Use relatórios visuais para auxiliar na melhor compreensão dos relatórios ALPR para o tráfego de veículos no seu ambiente.

NOTA: A função Gráficos não é suportada para os seguintes relatórios: Resolução de Problemas da Porta, Explorador de Arquivos de Vídeo e Pesquisa de Movimento.

Para gerar um relatório visual:

1 Abra uma tarefa de relatório existente que suporte a função de gráficos ou crie uma nova.

2 Na aba *Filtros* , use os filtros de pesquisa para criar uma busca personalizada.

NOTA: Alguns desses filtros têm um botão **Selecionar Todos** . Esse botão não aparece se existir mais de 100 entidades a selecionar (por exemplo, se tiver uma lista de 1500 titulares de cartão), porque se pesquisar entidades em excesso, o relatório leva muito tempo para ser gerado.

3 Defina uma data e intervalo de tempo para o relatório.

4 Clique em **Gerar relatório**.

Se houver filtros inválidos, o botão **Gerar relatório** fica indisponível.

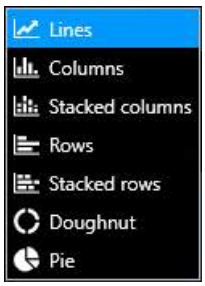
Os resultados da pesquisa são exibidos no painel do relatório.

DICA: É possível classificar os resultados por coluna. Também é possível clicar com o botão direito na fileira de títulos para selecionar colunas, depois adicionar ou remover colunas conforme a necessidade.

5 Fazer um dos seguintes:

- Se o relatório tiver suporte para ladrilhos, abra a visualização do gráfico usando o botão de alternar ( ) na parte superior direita da tarefa.
- Se o relatório não tiver suporte para ladrilhos, abra a visualização de gráfico usando o botão de Gráfico (Charts).

6 Selecione um tipo de Gráfico do menu suspenso no painel de Gráficos.

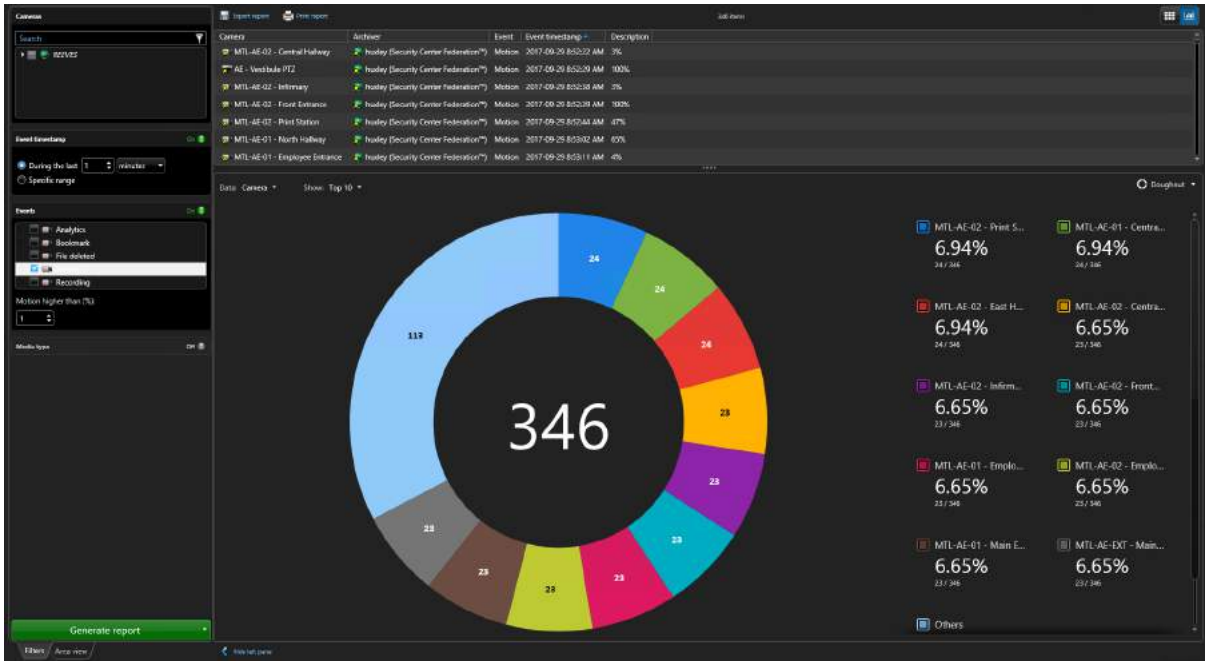


7 Selecione os dados que deseja exibir no relatório visual usando os menus suspensos no painel de Gráficos: **Dividido por**, **Exibir** (**Top 10**, **Top 5**ou **Top 3**), **Eixo X**, **Eixo Y**ou **Dados**.

NOTA: Somente os menus suspensos relevantes ao gráfico selecionado são exibidos. As escolhas disponíveis nos menus suspensos variam dependendo dos dados no painel de relatório.

Exemplo:

O exemplo seguinte mostra os Top 10 eventos de câmera como um gráfico **Rosca** .



Exemplo:

O exemplo seguinte mostra os Top 5 eventos de titulares de cartão divididos por Nome e Marca temporal de evento agrupado por Dia por um período de tempo especificado como um gráfico de **Linhas**.

8 (Opcional) Trabalhe com os dados no gráfico.

É possível passar sobre os elementos no gráfico ou diagrama para exibir informações adicionais, isso também destaca o item relacionado na legenda do gráfico.

DICA: É possível exibir ou ocultar rapidamente dados no gráfico ao selecionar (☐) ou limpar (☐) um item da legenda do gráfico.

9 Analise os resultados da pesquisa.

Os resultados da pesquisa variam dependendo do tipo de tarefa de relatório.

10 Trabalhe com os resultados da pesquisa.

Dependendo dos itens nos resultados da pesquisa, é possível exportar o relatório como dados (Excel, CSV ou PDF) ou como gráfico (PNG ou JPEG). Também é possível imprimir o relatório como dados ou gráfico.

11 (Opcional) Salvar o relatório como modelo.

Se salvar o layout do relatório (filtros de pesquisa e colunas de relatório) como um modelo, ele pode ser enviado a outro usuário ou estação de trabalho usando a ação *Enviar relatório por e-mail* .

Exemplo

Assista a este vídeo para saber mais. Clique no ícone **Legendas** (**CC**) para ligar a legenda do vídeo em um dos idiomas disponíveis. O vídeo pode não ser exibido no Internet Explorer. Para resolver isso, abra as **Configurações de compatibilidade de exibição** e limpe **Exibir sites da intranet em Visualizar compatibilidade**.

Tópicos relacionados

Gerar relatórios na página 53
Sobre os relatórios visuais na página 48
Exportar relatórios gerados na página 54
Imprimir relatórios gerados na página 54

Gerando e salvando relatórios

Em vez de esperar que um relatório seja gerado e então exportar os resultados, você pode gerar um relatório e salvá-lo diretamente em um local de arquivo.

O que você deve saber

Gerar e salvar um relatório é útil, pois você não precisará esperar em sua estação de trabalho para que o relatório seja gerado. Ele também é útil se a sua consulta tiver muitos resultados, pois você não estará limitado a 10.000 resultados como quando você gera um relatório normalmente.

NOTA: As tarefas que suportam este comando são aquelas em que os resultados são consultados a partir de um banco de dados da função, não do Directory.

Para gerar e salvar um relatório

1 Abra uma tarefa de relatório existente, ou crie uma nova.
2 Na aba *Filtros* , use os filtros de pesquisa para criar uma busca personalizada.

   NOTA: Alguns desses filtros têm um botão **Selecionar Todos** . Esse botão não aparece se existir mais de 100 entidades a selecionar (por exemplo, se tiver uma lista de 1500 titulares de cartão), porque se pesquisar entidades em excesso, o relatório leva muito tempo para ser gerado.

3 Clique com o botão direito em um cabeçalho de coluna no painel do relatório e clique em **Selecionar colunas** ( ).
4 Selecione quais colunas incluir no relatório salvo e clique em **Salvar**.
5 Clique na seta suspensa próxima ao **Gerar relatório** e clique em **Gerar e salvar relatório**.
6 Na caixa de diálogo, definir as seguintes opções:
   - **Formato de arquivo:** Selecione o formato do arquivo. Somente CSV é suportado.
   - **Arquivo de destino:** Selecione o nome do arquivo.
   - **Orientação:** (Somente PDF) Selecione se o arquivo PDF deve estar no modo retrato ou paisagem.
   - **Pasta de arquivos anexados:** Especifique onde estão salvos os arquivos anexados, tais como fotos do titular do cartão ou imagens de placas.
7 Clique em **Exportar**.

O relatório é salvo no local especificado.

Personalizar o painel de relatório

Uma vez que você tenha gerado o seu relatório, você poderá personalizar a forma como os resultados são exibidos no painel do relatório.

Para personalizar o painel de relatório:

1 Gerar o relatório.

2 Selecione quais colunas exibir, como segue:

a) No painel de relatório, clique com o botão direito em um cabeçalho de coluna e, em seguida, clique em **Selecionar colunas** ( ).

b) Selecione as colunas que deseja exibir e limpe as colunas que deseja ocultar.

c) Para alterar a ordem das colunas, use as setas e .

d) Clique em **OK**.

3 Para ajustar a largura de uma coluna, clique entre os dois cabeçalhos de coluna e arraste o separador para a direita ou a esquerda.

4 Para alterar a ordem de colunas, clique e segure em um cabeçalho de coluna no painel de relatório e arraste-o para a posição desejada.

5 Para classificar o relatório por uma das colunas, clique no cabeçalho da coluna. Clique no cabeçalho da coluna uma segunda vez para classificar o relatório na ordem inversa.

NOTA: Todas as colunas contendo marcas de tempo são classificadas de acordo com seu valor de horário UTC. Caso você opte por exibir os horários no Security Center de acordo com o fuso horário local de cada dispositivo em vez de um fuso horário fixo, os horários podem parecer desordenados se o relatório contiver dispositivos de fusos horários diferentes.

6 Para aumentar o tamanho do painel do relatório, arraste o separador entre o painel de relatório e a tela para a parte inferior da janela do aplicativo.

7 Salve o layout do seu relatório com as alterações que você fez ao painel de relatório como segue:

- Para salvar a tarefa como uma tarefa *privada* ou *pública*, clique com o botão direito na aba da tarefa e, em seguida, clique em **Salvar como**.
- Para salvar o espaço de trabalho para a próxima vez que abrir o aplicativo, clique com o botão direito na barra de tarefas e, em seguida, clique em **Salvar o espaço de trabalho**.

Tópicos relacionados

Personalizar configurações de fuso horário na página 55

Personalizar o comportamento dos relatórios

Você pode selecionar quantos resultados de relatórios receber, e quando você quer receber mensagens de erro sobre relatórios, na caixa de diálogo *Opções* .

O que você deve saber

Quando a consulta alcançar o limite especificado, ela automaticamente parará com uma mensagem de alerta. O valor máximo que pode ser configurado é 10.000. As configurações de relatório são salvas como parte do seu perfil de usuário e se aplicam ao Security Desk e ao Config Tool.

Para personalizar o comportamento dos relatórios:

1. Na página inicial, clicar em **Opções** > **Desempenho**.
2. Na seção **Relatórios**, defina o valor da opção **Número máximo de resultados**.

   Esta opção determina o número máximo de resultados que podem ser retornados por uma consulta usando uma tarefa de relatório. Esse limite ajuda a garantir o desempenho estável quando muitos resultados são retornados se a sua consulta for muito ampla.

3. Clique na aba **Interação de usuários**.
4. Se você quiser que o Security Center exiba uma mensagem de aviso cada vez que você estiver prestes a executar uma consulta que possa levar muito tempo, selecione a opção **Exibir advertência, caso uma consulta possa levar um longo tempo para executar**.
5. Clique em **Salvar**.

Sobre a função do Report Manager

O Gerenciador de relatórios é um tipo de função que automatiza o envio por e-mail e a impressão de relatórios com base em agendas.

Apenas uma instância dessa função é permitida por sistema.

Esta função é criada por padrão na instalação do sistema e hospedada em seu *servidor principal*.

Configurar resultados máximos para relatórios automatizados

Você pode selecionar o número máximo de resultados que podem ser gerados usando as ações *Enviar relatório por e-mail* ou *Exportar relatório* para evitar que a presença de muitos resultados em relatórios trave o seu computador.

O que você deve saber

O número máximo de resultados de relatório se aplica somente se você estiver salvando o relatório em formato PDF ou Excel. Não se aplica ao formato CSV.

As ações *Enviar relatório por e-mail* ou *Exportar relatório* podem ser acionadas com o uso de eventos causa-efeito ou acionadas como uma ação única ou ação instantânea no Security Desk.

Para configurar o número máximo de resultados de relatório:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.
2 Selecione a função Report Manager e clique na aba **Propriedades**.
3 Defina um valor na opção **Número máximo de resultados para relatórios em lote** e clique em **Aplicar**.

4

Atalhos de teclado

Esta seção inclui os seguintes tópicos:

- "Atalhos padrão no teclado" na página 66
- "Personalizar atalhos de teclado" na página 68

Atalhos padrão no teclado

Esse gráfico lista os atalhos padrão do teclado que podem ser usados para controlar tarefas, ladrilhos e entidades na sua estação de trabalho local. Essa lista é categorizada alfabeticamente pela categoria comando.

NOTA: É possível alterar os atalhos do teclado a partir da caixa de diálogo *Opções* .

Comando	Descrição	Atalho
Comandos gerais		
Aplicar alterações	Aplica as alterações feitas à sua aba de configurações atual.	Ctrl+S
Sair do aplicativo	Fechar o aplicativo .	Alt+F4
Tela cheia	Alterna entre exibir o aplicativo em tela cheia e modo de janela.	F11
Ir para a próxima página	Alterna para a próxima aba de tarefa.	Ctrl+Tab
Ir para a página anterior	Alterna para a aba de tarefas anterior.	Ctrl+Shift+Tab
Ajuda	Abre a ajuda online.	F1
Página inicial	Vai para a página inicial.	Ctrl+Acento grave (`)
Opções	Abre a Opções caixa de diálogo.	Ctrl+O
Selecionar colunas	Seleciona quais colunas exibir/ocultar no painel de relatório.	Ctrl+Shift+C
Menu de contexto de ladrilho	Abre o menu de contexto do ladrilho para o ladrilho selecionado na tela. **NOTA:** Este atalho no teclado não pode ser modificado pela caixa de diálogo *Opções* .	Shift+F10 ou Tecla do menu de contexto Pressione Tab para passar pelas opções do menu e em seguida pressione `Enter`.
Comandos da câmera		
Adicionar um marcador	Adiciona um marcador ao vídeo no ladrilho selecionado (somente para vídeo ao vivo).	B
Adicionar aos favoritos (tudo)	Adiciona marcadores ao vídeo em todos os ladrilhos selecionados (somente para vídeo ao vivo).	Ctrl + Shift + B
Copiar estatísticas da janela de vídeo atualmente selecionada	Copia as estatísticas do ladrilho selecionado.	Ctrl + Shift + X

Comando	Descrição	Atalho
Mostrar linha do tempo de diagnóstico	Exibe a linha do tempo do diagnóstico do fluxo do vídeo.	Ctrl + Shift + T
Mostrar diagnóstico do stream de vídeo	Exibe/oculta o diagnóstico do fluxo do vídeo, onde é possível resolver os problemas do fluxo do vídeo.	Ctrl + Shift + D
Mostrar estatísticas do stream de vídeo no ladrilho	Exibe/oculta o resumo das estatísticas do vídeo no ladrilho selecionado.	Ctrl + Shift + A
Mostrar status do stream de vídeo	Exibe/oculta o resumo das estatísticas das conexões do fluxo do vídeo e redireciona no ladrilho selecionado.	Ctrl+Shift+R.
Comandos de PTZ		
Vai para predefinição	Pula para uma predefinição PTZ selecionada.	<PTZ preset>+ Shift + Insert
Panorâmica à esquerda	Coloca a imagem da câmera PTZ em panorâmica na esquerda.	Seta para esquerda
Panorâmica à direita	Coloca a imagem da câmera PTZ em panorâmica na direita.	Seta para direita
Inclinação para baixo	Inclina a imagem da câmera PTZ para baixo.	Seta para baixo
Inclinação para cima	Inclina a imagem da câmera PTZ para cima.	Seta para cima
Aproximar zoom	Aproxima o zoom na imagem da câmera PTZ.	Mantenha o sinal de Mais (+) pressionado
Afastar zoom	Afasta o zoom da imagem da câmera PTZ.	Mantenha a tecla Hífen (-) pressionada
Comandos da tarefa		
Renomear tarefa	Renomeia a tarefa selecionada.	F2
Salvar como	Salva a tarefa com um nome e privacidade (privado ou público) diferente.	Ctrl + T
Salvar o espaço de trabalho	Salva a lista de tarefas para que seja automaticamente restaurada da próxima vez que você fizer logon no sistema com o mesmo nome de usuário.	Ctrl + Shift + S
Tarefas salvas	Abre a página *tarefas públicas* na página inicial.	Ctrl + N

Tópicos relacionados

Personalizar atalhos de teclado na página 68

Personalizar atalhos de teclado

É possível atribuir, modificar, importar ou exportar os atalhos de teclado mapeados para comandos frequentemente usados no Security Center.

O que você deve saber

Um atalho de teclado somente pode ser atribuído a um único comando. Atribuir um atalho de teclado existente a um novo comando remove o anterior. A configuração de atalhos de teclado é salva como parte do seu perfil de usuário e se aplica ao Security Desk e ao Config Tool. Se sua empresa usar um conjunto padrão de atalhos, você poderá exportar a configuração de atalhos de teclado para um arquivo XML e enviá-lo para outra estação de trabalho ou importar um para a sua estação de trabalho.

Para personalizar seus atalhos de teclado:

1 Na página inicial, clicar em **Opções** > **Atalhos de teclado**.
2 (Opcional) Importa uma configuração de atalhos de teclado, como segue:
   a) Clique em **Importar**.
   b) Na caixa de diálogo que aparecer, selecione um arquivo e clique em **Abrir**.
3 Na coluna *Comando*, selecione o comando ao qual deseja atribuir um atalho de teclado.
4 Clique em **Adicionar um item** () e pressione a combinação de teclas desejada.
   Se o atalho já estiver atribuído a um outro comando, uma mensagem pop-up aparecerá.
   - Clique em **Cancelar** para escolher outro atalho.
   - Clique em **Atribuir** para atribuir o atalho ao comando selecionado.
5 Clique em **Salvar**.
6 Caso você precise enviar sua configuração de atalhos para outro usuário, exporte a configuração como segue:
   a) Na página inicial, clicar em **Opções** > **Atalhos de teclado**.
   b) Clique em **Exportar**.
   c) Na caixa de diálogo que aparecer, selecione um nome de arquivo e clique em **Salvar**.
7 Para restaurar os atalhos de teclado padrão:
   a) Na página inicial, clicar em **Opções** > **Atalhos de teclado**.
   b) Clique em **Restaurar padrão** > **Salvar**.

Tópicos relacionados

Atalhos padrão no teclado na página 66

Administração comum do Security Center

Esta parte inclui as seguintes chapters:

- "Entidades" na página 70
- "Servidores e funções" na página 97
- "Bancos de dados e redes" na página 137
- "Alta disponibilidade" na página 160
- "Automação do sistema" na página 196
- "Federation" na página 223
- "Mapas" na página 235
- "Plug-ins" na página 284
- "Monitoramento da saúde do sistema" na página 289
- "Auditorias do sistema" na página 318
- "Web Client Server" na página 333

5

Entidades

Esta seção inclui os seguintes tópicos:

- "Sobre entidades" na página 71
- "Entidades criadas automaticamente no Security Center " na página 72
- "Alterar ícones de entidade" na página 73
- "Configuração de locais geográficos de entidades" na página 74
- "Pesquisar por entidades" na página 75
- "Copiar definições de configuração de uma entidade para a outra" na página 77
- "Atribuir IDs lógicos a entidades" na página 81
- "Customizar como as entidades são exibidas na tela" na página 82
- "Excluir entidades" na página 83
- "Estados de entidades" na página 84
- "Solução de problemas: entidades" na página 85
- "Sobre campos personalizados" na página 86
- "Criar tipos de dados personalizados para campos personalizados" na página 87
- "Criar campos personalizados" na página 88
- "Sobre a Ferramenta de registro de unidades" na página 90
- "Visualizar propriedades das unidades" na página 93
- "Personalizar o comportamento do Security Center ao renomear unidades de hardware" na página 96

Sobre entidades

Entidades são os blocos de construção básicos do Security Center. Tudo o que precisa de configuração é representado por uma entidade. Uma entidade pode representar um dispositivo físico, como uma câmera ou porta, ou um conceito abstrato, como um alarme, um cronograma, um usuário, uma função, um plugin ou add-on.

Entidades criadas automaticamente no Security Center

Embora a maioria das *entidades* seja criada manualmente no Security Center, algumas entidades também podem ser descobertas ou criadas automaticamente.

As entidades que são *descobertas* no Security Center são aquelas que representam dispositivos de hardware, como unidades de vídeo ou unidades de controle de acesso. Normalmente, o Security Center precisa de uma conexão ativa ao dispositivo de hardware antes que a entidade possa ser criada.

A tabela a seguir lista as entidades que são criadas automaticamente no Security Center:

Tipo da entidade	Criação automática	Criação manual
Servidores	Sempre.	Não suportado.
Redes	Adicionar um novo servidor automaticamente cria uma nova rede.	Suportado, mas geralmente não necessário.
Unidades de controle de acesso	Somente para unidades que suportam *descoberta automática*.	Suportado, mas exige uma conexão ativa com a unidade.
Unidades de vídeo	Somente para unidades que suportam *descoberta automática*.	Suportado, mas exige uma conexão ativa com a unidade.
Câmeras	Sempre. Entidades de câmera (ou codificador de vídeo) são criadas quando as unidades de codificação de vídeo são adicionadas ao seu sistema.	Não suportado.
Monitores analógicos	Sempre. Entidades de monitor analógico (ou codificador de vídeo) são criadas quando as unidades de decodificação de vídeo são adicionadas ao seu sistema.	Não suportado.
Unidades LPR	• Unidades LPR fixas são descobertas pelas funções do LPR Manager. • Unidades de LPR móveis (montadas em veículos de patrulha) são adicionadas quando entidades do Genetec Patroller™ são adicionadas.	Suportado para unidades LPR fixas, mas geralmente não são necessárias.
Patrulhas	Sempre.	Não suportado.
Unidades de detecção de invasão	Nunca.	Suportado, mas exige uma conexão ativa com o painel de intrusão.
Áreas de detecção de intrusão	Criadas pela função Intrusion Manager quando o painel de intrusão é inscrito.	Suportado apenas se o Intrusion Manager não puder ler as configurações de área da unidade.

Tópicos relacionados

Inscrição automática de unidades de controle de acesso na página 610
Descobrir unidades em sua rede na página 90

Alterar ícones de entidade

Os ícones de entidade representam graficamente as funções das entidades, funcionando como um rápido auxiliar visual ao interagir com a *árvore de entidades*.

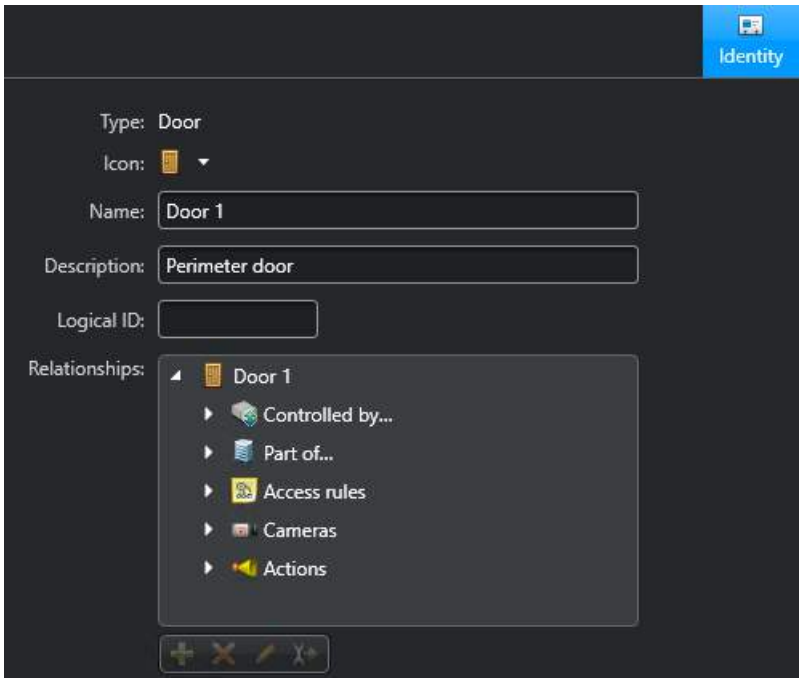
O que você deve saber

Você pode alterar o ícone de uma entidade para que ele corresponda ao propósito específico da entidade (por exemplo, uma entidade de porta que representa uma catraca ou o portão de um estacionamento).

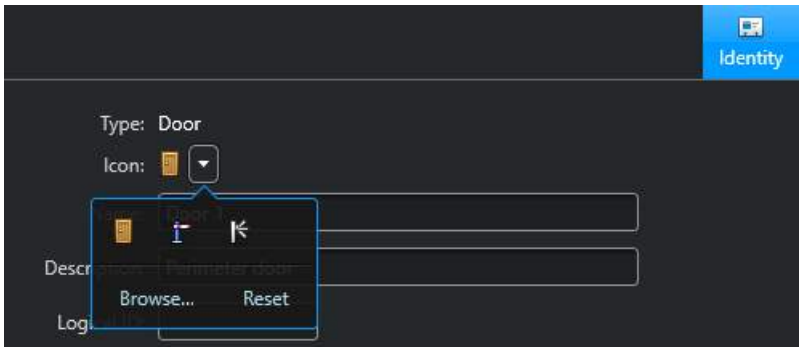
Para alterar o ícone de uma entidade:

1 Na página inicial do Config Tool, abra a tarefa *Exibição de área*.

2 No *navegador de entidades*, selecione a entidade e clique na aba **Identidade**.



3 Na lista **Ícone**, selecione um novo ícone.



NOTA: Você pode selecionar o ícone padrão que corresponde a função real da entidade ou executar uma das seguintes opções:

- Clique em **Procurar...** para navegar para ou selecionar seu próprio ícone personalizado favorito.
- Clique em **Redefinir** para restaurar o ícone padrão.

4 Clique em **Aplicar** (.

Configuração de locais geográficos de entidades

Para calcular o nascer e o pôr do sol para unidades de vídeo, ou para traçar um mapa de unidades LPR, você pode definir a latitude e a longitude daquela entidade.

O que você deve saber

A localização geográfica (latitude, longitude) de uma entidade tem dois usos diferentes:

- A localização geográfica das unidades de vídeo são usadas para calcular automaticamente a hora em que o sol nasce ou se põe em uma determinada data. Isso é útil se você quiser que o sistema somente grave vídeo durante o dia (para câmeras que sejam colocadas no lado de fora), ou ajustar o brilho de uma câmera com base na hora do dia.
- A localização geográfica das *Unidades LPR* fixas sem um receptor GPS é usada para traçar os eventos LPR (*leituras* e *ocorrências*) associados com a unidade LPR no mapa no Security Desk.

Para definir a localização geográfica de uma entidade:

1 Na aba **Localização** de uma entidade, clique em **Visualizar no mapa**.

Uma janela de mapa aparecerá.

2 Navegue até o local da sua entidade no mapa.

Você pode clicar e arrastar para aumentar o zoom, diminuir o zoom e fazer panorâmica.

3 Clique em **Selecionar** na janela do mapa.

O cursor muda para uma cruz.

4 Clique no local desejado no mapa.

Um alfinete aparece no mapa.

5 Clique em **OK**.

Os campos de latitude e longitude exibem as coordenadas da localização em que você clicou no mapa.

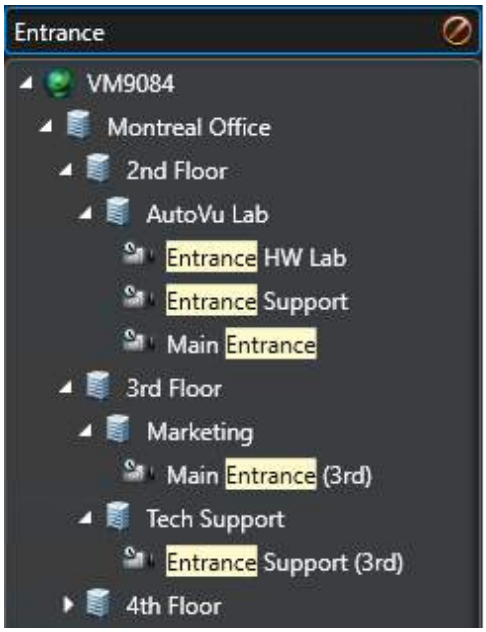
Pesquisar por entidades

Se não conseguir encontrar a entidade necessária em uma tarefa, é possível procurar pela entidade por nome.

Para pesquisar por uma entidade:

1 Na caixa *Pesquisar* no seletor, digite o nome da entidade que está buscando.

2 Clique em **Pesquisar** ( ).



Somente entidades com nomes contendo o texto digitado são exibidas.

3 Clique em **Apagar filtro** ( ) para parar de usar o filtro de pesquisa.

Pesquisando por entidades usando a ferramenta de pesquisa

É possível aplicar um conjunto de filtros para encontrar as entidades que precisa usando a ferramenta *Buscar* .

O que você deve saber

A ferramenta *Pesquisar* está disponível para muitas tarefas. Os filtros disponíveis dependem da tarefa que está usando. Por exemplo, é possível filtrar entidades por nome, descrição, tipo de entidade, partições, etc.

Para procurar por uma entidade usando a ferramenta Pesquisar:

1 Na caixa *Pesquisar* no seletor, clique em **Aplicar um filtro personalizado** ( ).

2 Na janela *Pesquisar* , use os filtros para especificar seus critérios de busca.

- Para ativar um filtro, clique no cabeçalho do filtro. Filtros ativos são exibidos com um LED verde ( ).
- Para desativar um filtro ( ), clique no cabeçalho do filtro.

NOTA: Filtros inválidos são exibidos em vermelho. Passe o cursor do mouse sobre o cabeçalho para verificar porque o filtro é inválido.

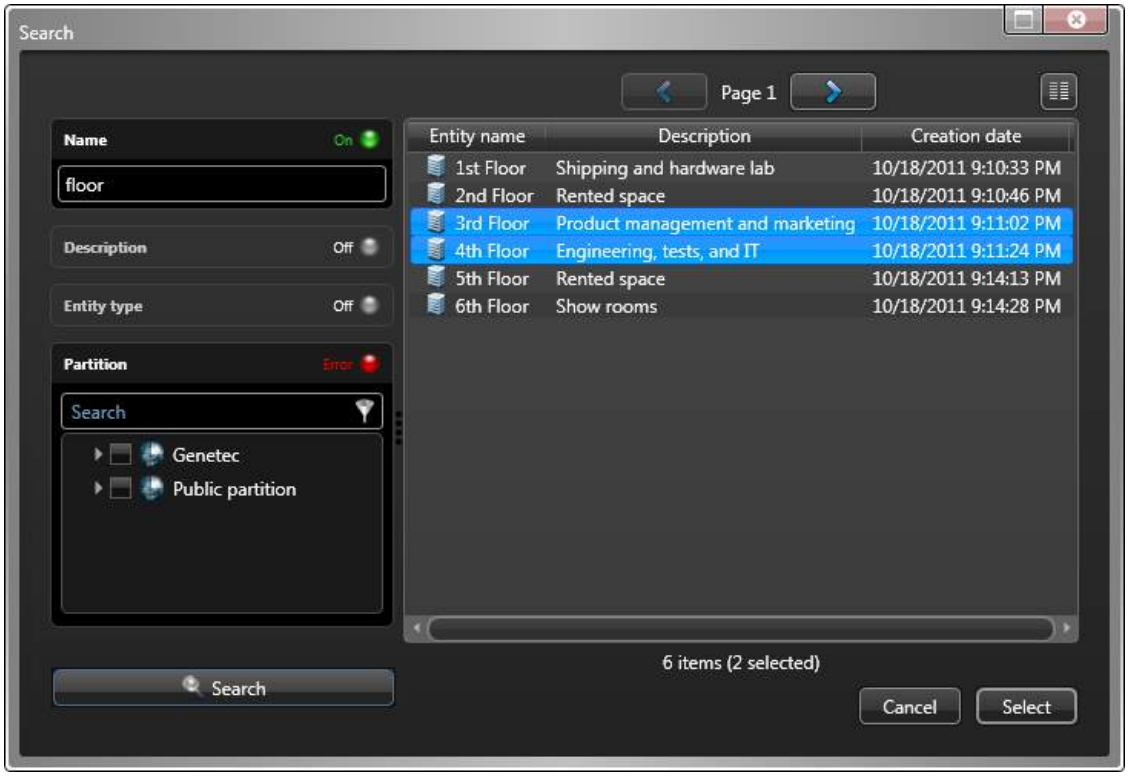
3 Clique em **Pesquisar** ( ).

Os resultados da pesquisa aparecem à direita. O número total de resultados é exibido na parte de baixo da lista.

4 Clique em **Selecionar colunas** ( ) para escolher quais colunas exibir na lista de resultados.

5 Selecione as entidades que deseja.

DICA: Segure a tecla Ctrl para fazer várias seleções. Clique em e para passar por múltiplas páginas de resultados.



6 Clique em **Selecionar**.

Somente as entidades selecionadas aparecem no seletor.

7 Clique em **Apagar filtro** ( ) para parar de usar o filtro de pesquisa.

Copiar definições de configuração de uma entidade para a outra

Quando você tiver muitas entidades similares para configurar, você poderá poupar tempo copiando as configurações de uma entidade para outras do mesmo tipo usando a Ferramenta de cópia de configuração.

Antes de iniciar

Se você estiver copiando configurações de câmeras, certifique-se de que as câmeras sejam da mesma marca e modelo para que as configurações correspondam.

O que você deve saber

(Apenas câmeras) Se você estiver copiando as configurações de rede da câmera, somente as configurações de transmissão serão copiadas (*Tipo de conexão* e *Porta UDP*). O endereço Multicast não é copiado.

Para copiar ajustes de configuração de uma entidade para a outra:

1 Abra a **Ferramenta de cópia de configuração** de uma das seguintes formas:
   - Na página inicial do Config Tool, clique em **Ferramentas** > **Ferramenta de cópia de configuração**.
   - No Config Tool, clique com o botão direito em uma árvore de entidades e, em seguida, clique em **Copiar** > **Ferramenta de cópia de configuração**.

2 Se você tiver aberto a **Ferramenta de cópia de configuração** a partir da página inicial, selecione um tipo de entidade e clique em **Próximo**.
3 Na página *Origem*, selecione de qual entidade você deseja copiar as configurações e clique **Próximo**.
4 Na página *Opções*, selecione os tipos de configurações que você deseja copiar e clique em **Próximo**.
   Para saber quais opções estão disponíveis para cada entidade, consulte a lista a seguir.
5 Na página *Destinos*, selecione as entidades para as quais você deseja copiar as configurações e clique em **Próximo**.
6 Quando o processo de cópia estiver concluído, clique em **Fechar**.

Após terminar

Se você tiver copiado configurações de câmera, teste as configurações que são dependentes da localização da câmera (por exemplo, detecção de movimento ou cor) na câmera para a qual você copiou a configuração. Você pode precisar ajustar as configurações, dependendo da câmera estar no interior ou no exterior, em um local tranquilo ou barulhento e assim por diante.

Tópicos relacionados

Teste de configurações de detecção de movimento na página 490
Ajustar configurações de cor da câmera na página 492
Atualizar firmware de unidade de controle de acesso na página 747
Substituir unidades Sharp fixas na página 821

Ajustar configurações copiadas para cada entidade usando a ferramenta de Copiar Configurações

Você pode determinar quais categorias de configurações são copiadas ao usar a ferramenta de Cópia de Configurações. As categorias disponíveis são diferentes para cada entidade.

A tabela a seguir lista as categorias de configurações que estão disponíveis para cada entidade ao usar a Ferramenta de Cópia de Configurações:

Tipo da entidade	Configuração de categorias disponíveis
Unidade de controle de acesso	• Ações • Propriedades (apenas HID) — Todas as configurações na aba **Propriedades**, exceto aquelas cobertas na categoria *Segurança*. • Segurança (apenas HID) — Inclui: **Modo de segurança** e **Senha de administrador**. • Sincronização • Fuso horário
Regra de acesso	• Entidades anexas • Membros • Propriedades
Alarme	• Ações • Entidades anexas • Propriedades • Destinatários
Área	• Mapas
Câmera	• Ações • Melhorar a qualidade • Cor • Codificação • Configurações específicas de hardware • Detecção de movimento • Rede • PTZ • Gravando • Uso do stream • Qualidade do vídeo • Rastreamento visual
Titular do cartão	• Regras de acesso • Ações • Opções • Grupos de titulares de cartão pais • Estado

Tipo da entidade	Configuração de categorias disponíveis
Grupo de titulares de cartão	• Regras de acesso • Membros • Grupos de titulares de cartão pais • Propriedades
Credencial	• Ações • Modelo do crachá • Estado
Porta	• Regras de acesso • Ações • Câmeras • Propriedades • Agendamentos de abertura
Lista de procurados	• Avançado • Atributos • Caminho • Propriedades
Unidade LPR	• Listas de procurados
Regra de estacionamento	• Propriedades
Zona de estacionamento	• Fiscalização • Câmeras LPR • Regras de estacionamento • Propriedades
Patroller	• Ações • Campos personalizados • Listas de procurados • Autorizações • Propriedades

Tipo da entidade	Configuração de categorias disponíveis
Autorização	• Avançado • Atributos • Vagas de estacionamento • Caminho • Propriedades
Usuário	• Permissões de acesso • Ações • Avançado • Alarmes • Privilégios • Propriedades • Configurações do Security Desk
Grupo de usuários	• Permissões de acesso • Avançado • Alarmes • Membros • Privilégios • Propriedades • Configurações do Security Desk
Unidade de vídeo	• Ações • Áudio • Configurações específicas de hardware • Detecção de movimento • Rede • Segurança • Fuso horário
Zona	• Ações

Atribuir IDs lógicos a entidades

Você pode atribuir um ID lógico (número exclusivo) a entidades, tarefas públicas e estações de trabalho em seu sistema para que você possa controlá-las usando os atalhos do teclado.

O que você deve saber

Se você quiser usar atalhos de teclado para alternar entre diferentes tarefas públicas, controlar outras estações de trabalho ou exibir entidades na tela do Security Desk, você deverá atribuir números exclusivos (IDs lógicos) às entidades. Os IDs lógicos podem então ser usados em um atalho de teclado. Para obter mais informações sobre o uso de atalhos de teclado no Security Desk, consulte o *Guia do Usuário do Security Desk*.

Há algumas entidades que costumam ser usadas em conjunto em um atalho de teclado. Essas entidades são agrupadas e não podem ter o mesmo ID lógico. Por exemplo, *câmeras* e *tarefas públicas* estão no mesmo grupo, pois costumam ser usadas em conjunto em um atalho de teclado para abrir uma tarefa salva e exibir uma câmera.

DICA: Você também pode alterar o ID lógico a partir da aba *Identidade* na página de configuração de cada entidade.

Para atribuir um ID lógico a uma entidade:

1. Abra a tarefa **Sistema**, clique na visualização **Configurações gerais** e, em seguida, clique na página **ID lógico**.
2. Na lista suspensa **Exibir ID lógico para**, selecione o grupo que lista a entidade, tarefa pública ou estação de trabalho que deseja usar.

   Se o item que desejar não estiver listado em um dos grupos, selecione **Todos os tipos**.
3. Próximo ao item ao qual deseja atribuir o ID lógico, digite um número na coluna **ID**.
4. Clique em **Aplicar**.

   Se o ID lógico já estiver atribuído, você receberá uma mensagem de erro. Selecione um ID diferente e tente novamente.

Modificar IDs lógicos

Se houver ID lógicos duplicados, ou se você quiser alterar um ID para um número que seja mais fácil de lembrar ao usar seus atalhos de teclado, você poderá modificar o ID lógico de uma entidade.

Para modificar um ID lógico:

1. Abra a tarefa **Sistema**, clique na visualização **Configurações gerais** e, em seguida, clique na página **ID lógico**.
2. Na lista suspensa **Exibir ID lógico**, selecione o grupo a ser configurado.
3. Se você tiver um sistema de grande dimensão, selecione a opção **Ocultar IDs lógicos não atribuídos** para exibir somente entidades, tarefas públicas e estações de trabalho que tenham um ID lógico.
4. Se ainda houver várias páginas, use os botões  e  para passar pelas páginas.
5. Junto à entidade, tarefa pública ou estação de trabalho que deseja modificar, digite um novo ID lógico na coluna **ID**.
6. Clique em **Aplicar**.

Customizar como as entidades são exibidas na tela

Você pode exibir a ID lógica (número de ID exclusivo) das entidades na visualização de área para ajudar a identificá-las. Você também pode exibir o nome do *Diretório ativo* do qual a entidade é importada.

O que você deve saber

Estas configurações são salvas como parte do seu perfil de usuário e são aplicadas ao Security Desk e Config Tool.

Para personalizar como as entidades são exibidas:

1. Na página inicial, clicar em **Opções** > **Interação de usuários**.
2. Para exibir a ID lógica entre colchetes após o nome da entidade, selecione a opção **Mostrar ID lógica**.
3. Para exibir o nome de usuário e o nome de domínio do Active Directory, selecione a opção **Exibir o nome de domínio de Directory Ativo onde for aplicável**.
4. Clique em **Salvar**.

Excluir entidades

Você pode excluir entidades que tenha criado manualmente e aquelas que foram descobertas automaticamente pelo sistema.

Antes de iniciar

Se a entidade tiver sido descoberta automaticamente, ela deverá estar desligada ou inativas (mostrada em vermelho) antes que você possa excluí-la.

O que você deve saber

Se você excluir uma entidade pai que tenha entidades abaixo dela na árvore de entidades, essas entidades também serão excluídas.

Para excluir uma entidade:

1. Na visualização de entidade de qualquer tarefa, selecione a entidade.
2. Na parte inferior da janela, clique em **Excluir** ( ).
3. Na caixa de diálogo de confirmação que aparece, clique em **Excluir**.
   Se existir mais de uma cópia da entidade, as outras cópias serão mantidas até serem excluídas.

Estados de entidades

As entidades podem aparecer na visualização de área em diversos estados diferentes, que são representados por diferentes cores.

A tabela a seguir lista os três estados de entidades:

Estado	Cor	Descrição
Online	Branco	O servidor pode se conectar à unidade.
Offline	Vermelho	O servidor não pode se conectar à entidade.
Alerta	Amarelo	O servidor pode se conectar à entidade, mas há problemas.

Os avisos da entidade normalmente aparecem por causa de configurações inválidas. Por exemplo, quando se trata de câmeras, as duas condições a seguir podem fazer com que a câmera entre em um estado amarelo de advertência:

- Vários agendamentos conflitantes de gravação foram aplicados à mesma câmera.
- Ocorreu um evento de *Transmissão interrompida*. Isso significa que o Archiver ainda está conectado à câmera, mas não recebeu nenhum pacote de vídeo por mais de 5 segundos.

Para realizar solucionar problemas de câmeras desligadas e em estados de alerta, faça um dos seguintes:

- Altere os agendamentos conflitantes.
- Solucione o problema da função do Archiver.

Tópicos relacionados

Solução de problemas: entidades na página 85
Sobre agendamentos na página 197

Solução de problemas: entidades

Você pode solucionar problemas de entidades e funções com a ferramenta *diagnóstico*.

O que você deve saber

Uma entidade ou função que não esteja adequadamente configurada é exibida em amarelo. Uma entidade que esteja desligada é exibida em vermelho. A ferramenta *diagnóstico* pode ajudar a solucionar problemas com a entidade.

Para solucionar problemas de uma entidade:

1 Abrir a tarefa **Status do sistema**.
2 Na lista suspensa **Monitor**, selecione o tipo de entidade que você deseja diagnosticar.
3 Se necessário, selecione uma área no *Seletor*.
4 Para incluir entidades dentro de áreas aninhadas, selecione a opção **Buscar entidades de membro**.

As entidades relacionadas são listadas no painel do relatório.

5 Selecione uma entidade com problema e clique em **Diagnosticar** ( ).

Abre-se uma janela de diagnóstico mostrando os resultados do teste executado na entidade selecionada.

6 Para salvar os resultados do teste, clique em **Salvar**.
7 Clique em **Fechar**.

Tópicos relacionados

Estados de entidades na página 84

Sobre campos personalizados

É uma propriedade definida pelo usuário que está associada a um tipo de entidade e é usada para armazenar informações adicionais que são úteis para sua organização.

Campos personalizados podem incluir quaisquer informações que você defina. Eles podem usar tipos de dados que ficam disponíveis por padrão no Security Center, ou você pode criar seus próprios tipos de dados. Uma vez que os campos personalizados sejam adicionados, eles estarão disponíveis em todos os relatórios de bancos de dados e consultas relacionados à entidade para a qual eles são definidos. Se um campo personalizado contiver informações privadas, você poderá restringir que certos grupos de usuários visualizem aquele campo.

Por exemplo, você pode adicionar *Gênero*, *Telefone residencial* e *Número de celular* como campos personalizados para entidades de titulares de cartões e permitir que apenas o grupo de usuários *Recursos Humanos* tenha acesso a essas informações.

Limitações de campos personalizados

Os campos personalizados são sempre locais para o sistema onde são definidos.

- Em um cenário de *Federação*, campos personalizados não são importados do sistema federado. Porém, você pode associar campos personalizados como atributos locais para *entidades federadas*.
- Em um cenário de integração do *Active Directory (AD)*, campos personalizados podem ser mapeados para atributos do AD para exibir seus valores em seu sistema local, mas não para atualizar o AD.

Tipos de dados padrão

O Security Center inclui os seguintes tipos de dados padrão para os campos personalizados:

- **Texto:** Texto alfanumérico.
- **Numérico:** Números inteiros no intervalo de -2147483648 a 2147483647.
- **Decimal:** Números reais de -1E28 a 1E28.
- **Data:** Data e hora do calendário gregoriano.
- **Booleanos:** Dados booleanos, representados por uma caixa de seleção.
- **Imagem:** Arquivo de imagem. Os formatos compatíveis são: bmp, jpg, gif e png.
- **Entidade:** Entidade Security Center.

Tópicos relacionados

Sobre entidades federadas na página 225
Mapear campos personalizados para sincronizar com o Active Directory na página 392

Criar tipos de dados personalizados para campos personalizados

Para usar algo diferente dos tipos de dados padrão ao criar campos personalizados, você pode criar seus próprios tipos de dados personalizados.

O que você deve saber

Tipos de dados personalizados definem uma lista de valores com base em um tipo de dados personalizado. Os tipos de dados personalizados aparecem em uma lista suspensa na aba *Campos personalizados* da página de configuração da entidade.

Para criar um tipo de dado personalizado para um campo personalizado:

1. Abra a tarefa **Sistema** e clique na visualização **Configurações gerais**.
2. Clique na página **Campos personalizados** e, em seguida, clique na aba **Tipos de dados personalizados**.
3. Clique em na parte inferior da lista de tipos de dados personalizados.
4. Na página **Editar tipo de dado personalizado**, digite **Nome**, **Descrição** e **Tipo** para o seu tipo de dado personalizado e clique em **Próximo**.
5. Na página **Entrada de dados**, digite um valor no campo **Valor** e clique em .

   O valor inserido é adicionado à lista enumerada.
6. Defina os outros valores possíveis para este tipo de dado.
7. Quando tiver terminado, clique em **Próximo**, **Próximo** e **Fechar**.

Editar tipos de dados personalizados

Você pode modificar tipos de dados personalizados (renomear, adicionar ou excluir valores e assim por diante) antes ou depois do tipo de dado personalizado estar em uso em um campo personalizado.

O que você deve saber

As seguintes limitações se aplicam ao modificar tipos de dados personalizados:

- Você não pode excluir um valor se ele estiver sendo usado como o valor padrão para um campo personalizado.
- Você não pode alterar o tipo de dados padrão no qual o tipo de dado personalizado é baseado.

Para editar um tipo de dado personalizado:

1. Abra a tarefa **Sistema** e clique na visualização **Configurações gerais**.
2. Clique na página **Campos personalizados** e, em seguida, clique na aba **Tipos de dados personalizados**.
3. Selecione o tipo de dado, clique em **Editar o item** () e siga o assistente.

Criar campos personalizados

Para adicionar mais informações às propriedades de entidades em seu sistema, você pode criar campos personalizados.

Antes de iniciar

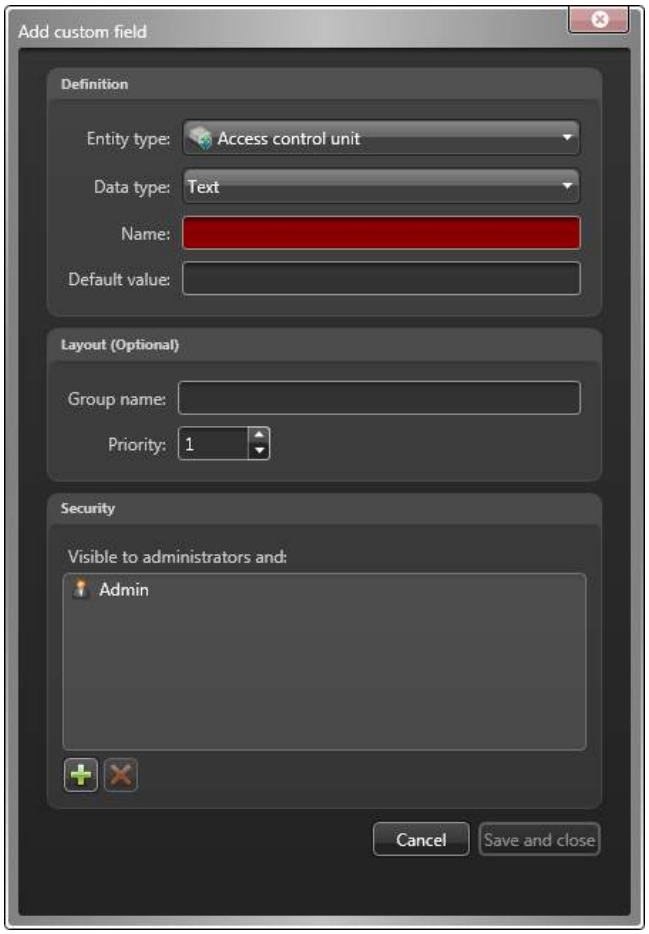
Se você quiser criar um campo personalizado usando o seu próprio tipo de dado personalizado, o tipo de dado já deve ter sido criado.

Para criar um campo personalizado:

1 Abra a tarefa **Sistema** e clique na visualização **Configurações gerais**.

2 Clique na página **Campos personalizados** e clique em na parte inferior da lista de campos personalizados.

3 Na lista suspensa **Tipo de entidade** na caixa de diálogo **Adicionar campo personalizado**, selecione o tipo de entidade ao qual este campo personalizado se aplica.



4 Na lista suspensa **Tipo de dado**, selecione um tipo de dado personalizado ou padrão para o campo personalizado.

5 No campo **Nome**, digite o nome para o campo personalizado.

6 (Opcional) No campo **Valor padrão**, digite ou selecione o valor padrão para este campo.

Este valor é exibido por padrão quando uma entidade que usa este campo personalizado é criada.

7 Dependendo do tipo de dado selecionado, as seguintes opções adicionais aparecerão:

- **Obrigatório:** Selecione-o se o campo personalizado não puder ficar vazio.

- **O valor deve ser único:** Selecione-o se o valor do campo personalizado dever ser exclusivo.

  NOTA: A opção de *valor exclusivo* somente pode ser aplicada após o campo ter sido criado. Para aplicar esta opção, você deve primeiro certificar-se de que todas as entidades no seu sistema tenham um valor distinto para este campo personalizado, em seguida, volte para esta aba para aplicar a opção de valor único a ela. Selecionar esta opção automaticamente seleciona a opção **Obrigatório**.

8 Na seção **Layout**, digite o **Nome do grupo** e selecione a **Prioridade** na lista suspensa.

  Esses dois atributos são usados ao exibir o campo na aba **Campos personalizados** da entidade associada. O nome do grupo é usado como o cabeçalho do grupo e a prioridade define a ordem de exibição do campo dentro do grupo.

9 Na seção **Segurança**, clique em para adicionar usuários e grupos de usuários que poderão visualizar este campo personalizado.

  Como padrão, somente administradores podem ver um campo personalizado.

10 Clique em **Salvar e fechar**.

O novo campo personalizado está agora disponível na aba **Campos personalizados** do tipo de entidade selecionado e pode ser usado para pesquisar esses tipos de entidade na ferramenta *Pesquisa*.

Tópicos relacionados

Sobre campos personalizados na página 86

Sobre a Ferramenta de registro de unidades

A Ferramenta de registro de unidades permite descobrir unidades IP (controle de acesso e vídeo) conectadas à sua rede, com base no fabricante e propriedades de rede (porta de descoberta, intervalo de endereços IP, senha e assim por diante). Uma vez detectadas, as unidades podem ser adicionadas ao seu sistema.

- A Ferramenta de registro de unidades abre automaticamente após o *assistente de instalação do Security Center*, a menos que você tenha desmarcado ao opção **Abrir a ferramenta de registro de unidades depois do assistente**.
- Ao adicionar unidades de controle de acesso, somente unidades HID e Synergis™ podem ser registradas com a Ferramenta de registro de unidades. Para obter detalhes completos sobre como registrar unidades Synergis™, consulte o *Guia de Configuração de Aparelhos Synergis™*.

Definir configurações de registro de unidades

Você pode usar o botão **Configurações e fabricantes** na ferramenta de *Registro de unidades* para especificar quais fabricantes incluir ao pesquisar novas unidades. Você também pode definir as configurações de descoberta para unidades e especificar nome de usuário e senhas para unidades para que elas possam ser registradas facilmente.

Para definir suas configurações de descoberta:

1 Na página inicial, clique em **Ferramentas** > **Registro de unidades**.

2 Na caixa de diálogo *Registro de unidades*, clique em **Configurações e fabricantes** ( ).

3 Configure as seguintes opções:

- **Sempre executar pesquisa ampla**. Acione esta opção se quiser que todas as unidades do sistema sejam descobertas.

  NOTA: As unidades de outros fabricantes também podem ser descobertas se UPnP e *Configuração Zero* também foram usados no processo de descoberta.

- **Recusar autenticação básica** (somente unidades de vídeo). Use esta opção para ativar ou desativar a autenticação básica. Isso é útil se você tiver desativado a autenticação básica no Security Center InstallShield, mas você precisará ativá-la novamente para realizar uma atualização de firmware ou registrar uma câmera que somente suporte a autenticação básica. Para ativar novamente a autenticação básica, você deve colocar a opção **Recusar autenticação básica** em **Desligado**.

  NOTA: Esta opção somente fica disponível para usuários com privilégios de Administrador.

4 Clique em **Adicionar fabricante** ( ) para adicionar um fabricante à lista de unidades que serão descobertas.

Para excluir um fabricante da lista, selecione-o e clique em .

5 Defina as configurações individuais para quaisquer fabricantes que você tiver adicionado. Para fazer isso, selecione o fabricante e clique em .

IMPORTANTE: Você deve inserir nome de usuário e senha corretos para a unidade ser inscrita adequadamente.

6 (Opcional) Remover unidades da lista de unidades ignoradas (ver Removendo unidades de listas de unidades ignoradas na página 92).

7 Clique em **Salvar**.

Descobrir unidades em sua rede

Se você não souber o endereço IP da unidade de vídeo ou de controle de acesso que deseja adicionar, você poderá encontrar a unidade em sua rede usando a *Ferramenta de registro de unidades*.

Antes de iniciar

Se quiser descobrir uma unidade controle de acesso, leia Adicionar extensões de unidades de controle de acesso na página 601.

Para descobrir unidades:

1 Na página inicial, clique em **Ferramentas** > **Registro de unidades**.
2 Configure as configurações de registro da unidade.
3 Clique em **Salvar** > **Iniciar descoberta** ( ).

As unidades descobertas em sua rede são listadas, usando as configurações de inscrição que você configurou para cada fabricante. Você pode interromper o processo de descoberta a qualquer momento.

Adicionar unidades

Assim que novas unidades tenham sido descobertas, você poderá usar a *Ferramenta de registro de unidades* para adicioná-las ao seu sistema.

Para adicionar uma unidade:

1 Na página inicial, clique em **Ferramentas** > **Registro de unidades**.
2 Há três maneiras para adicionar unidades recém-descobertas:

- Adicione todas as unidades recém-descobertas ao mesmo tempo clicando no botão **Adicionar tudo** ( ) na lateral direita inferior da caixa de diálogo.
- Clique em uma única unidade na lista e, em seguida, clique em **Adicionar** na coluna **Status**.
- Clique com o botão direito em uma única unidade da lista e clique em **Adicionar ou Adicionar Unidade**.

  Quando uma unidade de vídeo não tiver o nome de usuário e a senha corretos, o **Status** da unidade será listado como **Logon errado** e você será solicitado a inserir as informações corretas quando você adicionar a unidade. Se você quiser usar o mesmo nome de usuário e senha para todas as câmeras em seu sistema, selecione a opção **Salvar como autenticação padrão para todos os fabricantes**.

Você também pode adicionar uma unidade manualmente clicando no botão **Adição manual** na parte inferior da caixa de diálogo da **Ferramenta de registro de unidades**.

NOTA:

- Para unidades de vídeo, se a câmera adicionada for um codificador com várias transmissões disponíveis, cada transmissão será adicionado com a cadeia de caracteres *Câmera - n* anexa ao nome da câmera, onde *n* representa o número da transmissão. Para uma câmera IP com apenas um fluxo disponível, o nome da câmera não é modificado.
- Se você estiver registrando uma câmera Sharp executando o SharpOS 11.3 ou superior no Archiver, para acessar as transmissões de vídeo da câmera ou se for exigido controle de entrada/saída da unidade de processamento de LPR, você deve configurar a extensão AutoVu™ para permitir autenticação básica. No Config Tool, na aba **Extensões** do Archiver, selecione a extensão do Genetec™ AutoVu™ e desligue **Recusar Autenticação Básica**.

Tópicos relacionados

Adicionar unidades de vídeo manualmente na página 447
Adicionar unidades de controle de acesso na página 608

Limpar unidades adicionadas

Você pode limpar unidades que já tenham sido adicionada ao seu sistema para que elas não sejam exibidas toda vez que você usar a *Ferramenta de registro de unidades* para descobrir unidades em seu sistema.

O que você deve saber

A opção **Limpar concluídos** na *Ferramenta de registro de unidades* é permanente e não pode ser revertida.

Para limpar unidades adicionadas:

1 Adicione as unidades descobertas desejadas ao seu sistema; consulte Adicionar unidades na página 91.

2 Uma vez que as unidades tenham sido adicionadas, clique em **Limpar concluídos**.

Qualquer unidade que tenha **Adicionada** exibido na coluna **Status** será limpa da lista de unidades descobertas.

Ignorar unidades

Você pode optar por ignorar unidades para que elas não apareçam na lista de unidades descobertas da *Ferramenta de registro de unidades*.

Para ignorar uma unidade:

1 Na página inicial, clique em **Ferramentas** > **Registro de unidades**.

A ferramenta *Registro de unidades* é aberta com a lista de unidades que foram descobertas no sistema.

2 Clique com o botão direito na unidade que deseja ignorar e selecione **Ignorar**.

A unidade é removida da lista e será ignorada quando a ferramenta de *Registro de unidades* descobrir novas unidades. Para informações sobre como remover unidades da lista de unidades ignoradas, consulte Removendo unidades de listas de unidades ignoradas na página 92.

Removendo unidades de listas de unidades ignoradas

Você pode remover uma unidade da lista de unidades ignoradas para que ela não seja ignorada quando uma descoberta for realizada pela *Ferramenta de registro de unidades*.

O que você deve saber

Para remover uma unidade da lista de unidades ignoradas:

1 Na página inicial, clique em **Ferramentas** > **Registro de unidades**.

2 No canto superior direito da caixa de diálogo *Registro de unidades* clique em **Configurações e Fabricantes** ().

3 Clique em **Unidades ignoradas** e clique em **Remover todas as unidades ignoradas**, ou você pode selecionar uma única unidade e clicar no botão **Remover unidade ignorada** ().

Visualizar propriedades das unidades

Com uma simples olhada, você pode visualizar uma lista de todas as unidades locais que façam parte do seu sistema e ver suas informações, como tipo de unidade, fabricante, modelo, endereço IP e assim por diante, usando o relatório *Inventário de hardware*.

O que você deve saber

Como exemplo, você pode usar o relatório *Inventário de hardware* para ver qual versão de firmware uma unidade tem e determinar se ela precisa ser atualizada.

O relatório *Inventário de hardware* não inclui informações de unidades federadas.

Para visualizar as propriedades de unidades de seu sistema:

1 Na página inicial, abra a tarefa **Inventário de hardware**.

2 Definir os filtros de consulta para o seu relatório. Escolha um ou mais dos filtros abaixo:

- **Campos personalizados:** Restringir a busca a campo personalizado predefinido para a entidade. Este filtro aparece somente se os campos personalizados estiverem definidos para a entidade e estavam visíveis para você, quando foi criado ou configurado pela última vez.
- **Grupo de origem:** Grupo de entidade fonte do evento. Normalmente um papel ou uma unidade.
- **Unidades:** Selecionar o controle de acesso, vídeo, detecção de invasão e unidades LPR para investigar.

3 Clique em **Gerar relatório**.

As propriedades da unidade são listadas no painel de relatório.

Colunas do painel de relatórios para a tarefa Inventário de hardware

Após gerar um relatório, os resultados da sua pesquisa são listados em um painel de relatório. Esta seção lista as colunas disponíveis para a tarefa de relatório relevante.

- **Unidade:** Controle de acesso, vídeo, detecção de invasão ou unidade LPR envolvida.
- **Tipo de unidade:** Tipo ou modelo de unidade envolvido
- **Fabricante:** Fabricante da unidade.
- **Tipo de produto:** Modelo da unidade envolvida
- **Função:** Tipo de função que gerencia a entidade selecionada.
- **Versão do firmware:** Versão do firmware instalada na unidade que gerou o evento
- **Endereço IP:** Endereço de IP da unidade ou computador que gerou o evento
- **Endereço físico:** Endereço MAC da interface de rede do equipamento
- **Fuso horário:** Fuso horário da unidade
- **Usuário:** Nome do usuário usado para conectar a unidade.
- **Senha:** Força da senha da unidade Ao passar o mouse sobre o valor de força da senha, uma informação indica se a senha padrão do fabricante está sendo usada.
- **Esquema de autenticação:** Indica o tipo de autenticação sendo usado pela unidade da câmera, como básica, resumo, anônima ou de terceiro. Se a unidade solicitar repentinamente para conectar usando um esquema de autenticação menos seguro, o Archiver rejeita a comunicação e a câmera fica offline. Por exemplo, o Archiver espera que a câmera esteja usando autenticação resumo mas a câmera tenta se conectar usando autenticação básica. A conexão é rejeitada e a câmera fica offline.

- **Campos personalizados:** Os campos personalizados predefinidos para a entidade. As colunas aparecem somente se os campos personalizados estiverem definidos para a entidade e se estiver visível para você, quando forem criados ou configurados pela última vez.
- **Modo seguro:** (Somente unidades HID) Indica se o modo seguro está ativado ou desativado.
- **Status da atualização:** Status da atualização de firmware (Nenhuma, Agendada, Iniciada, Concluída ou Falha).
- **Próxima atualização:** A data para a próxima atualização com base na configuração **Retardar atualização até**.
- **Motivo para falha da atualização:** Motivo pelo qual a atualização de firmware falhou (por exemplo, Unidade offline ou Caminho da atualização do firmware não respeitada).
- **Versão proposta de firmware:** A versão recomendada necessária para a atualização.
- **Descrição proposta de firmware:** Descrição da atualização necessária.
  - **Atualizado:** Nenhuma atualização de firmware é necessária.
  - **Opcional:** A atualização de firmware é sugerida.
  - **Recomendado:** A atualização de firmware é recomendada.
  - **Crítico:** A atualização de firmware conserta um problema de vulnerabilidade de segurança e é altamente recomendada.

  NOTA: Essa informação está disponível somente se o Genetec™ Update Service estiver rodando.

Reativar a autenticação de acesso básica

Após instalar o Security Center usando configurações de segurança padrão, as câmeras que não sejam compatíveis com autenticação de acesso resumo poderão não funcionar. Para corrigir este problema, você pode reativar a autenticação de acesso básica por unidade de vídeo ou por fabricante.

O que você deve saber

Autenticação de acesso resumo é o esquema de autenticação que a maioria dos modelos de unidades de vídeo recentes suportam. Este esquema de autenticação é mais seguro do que a autenticação de acesso básica porque as senhas são transformadas em hash antes de serem enviadas pela rede. Por esse motivo, a autenticação de acesso básica é desabilitada por padrão na instalação. Após a instalação, se concluir que algumas das suas câmeras não são compatíveis com autenticação de acesso resumo, você pode revertê-las para autenticação de acesso padrão a partir do Config Tool.

Como segurança adicional, o Security Center memoriza se uma unidade de vídeo específica é compatível com o esquema de autenticação resumo. Uma vez que o sistema tenha sido autenticado com êxito para uma unidade de vídeo que use o esquema resumo, você não pode reverter para o esquema básico menos seguro. Você pode ver o esquema de autenticação usado para cada câmera no relatório *Inventário de hardware*.

Para reverter para o esquema de autenticação básico em uma unidade de vídeo específica:

1 Na Config Tool, abra a tarefa *Inventário de hardware*.
2 Execute o relatório nas unidades de vídeo que estão inativas (em vermelho) no seu sistema.
   Você poderá precisar rolar horizontalmente para a direita para ver a coluna **Esquema de autenticação**.
3 No painel de relatório, selecione as unidades de vídeo inativas e clique em **Redefinir esquema de autenticação**.
   O **Esquema de autenticação** muda para **Anônimo**. Após o Archiver se conectar com êxito à unidade de vídeo, o esquema de autenticação exato é exibido.

Para reverter para o esquema de autenticação básica para um fabricante específico:

1 Na Config Tool, abra a tarefa *Vídeo*.
2 Selecione a função Archiver que controla suas câmeras e clique em **Extensões**.

3 Selecione o fabricante desejado e defina **Recusar autenticação básica** como **Desligado**.
4 Clique em **Aplicar**.

Personalizar o comportamento do Security Center ao renomear unidades de hardware

Você pode configurar como o Config Tool se comporta ao renomear uma unidade de hardware, como uma *unidade de controle de acesso* ou uma *unidade de vídeo*.

O que você deve saber

Essas configurações são salvas como parte do seu perfil de usuário.

Para personalizar as opções ao renomear unidades de hardware:

1 Na página inicial, clique em **Opções** > **Interação do usuário**.

2 Na seção **Tarefas de administração**, selecione como o Config Tool se comporta ao renomear uma unidade na lista suspensa **Renomear todos os dispositivos dentro da unidade**:

- **Pergunte ao usuário:** Pergunta antes de renomear todos os dispositivos relacionados à unidade.
- **Sim:** Renomeia todos os dispositivos relacionados sem perguntar.
- **Não:** Nunca renomeia os dispositivos relacionados.

3 Clique em **Salvar**.

6

Servidores e funções

Esta seção inclui os seguintes tópicos:

- "Sobre servidores" na página 98
- "Abrir o Server Admin usando um navegador da Web" na página 99
- "Server Admin - Página de visão geral" na página 101
- "Server Admin - Página do servidor principal" na página 104
- "Server Admin - Página Servidor de expansão" na página 107
- "Adicionando Servidores de Expansão" na página 109
- "Converter o servidor principal em um servidor de expansão" na página 110
- "Converter um servidor de expansão em servidor principal:" na página 111
- "Conectar servidores de expansão ao servidor principal" na página 112
- "Ativar sua licença do Security Center usando a Web" na página 115
- "Ativar licenças do Security Center sem acesso à Internet" na página 118
- "Reaplicar sua licença do Security Center" na página 123
- "Substituir o servidor principal" na página 129
- "Sobre funções" na página 132
- "Mover funções para outros servidores" na página 133
- "Desativar e ativar funções" na página 134
- "Sobre a função Directory" na página 135
- "Sobre Web-based SDK" na página 136

Sobre servidores

Um servidor é um tipo de entidade que representa uma máquina de servidor em que o serviço Servidor Genetec™ está instalado.

IMPORTANTE: Nenhum nome de servidor pode ter mais que 15 caracteres. O Security Center trunca todos os nomes de servidores com mais de 15 caracteres, provocando erros quando o sistema tenta acessar esses servidores.

As entidades de servidor são criadas automaticamente quando o software do Security Center Server é instalado em um computador e esse computador está conectado ao *servidor principal* do seu sistema.

Servidor principal

O servidor principal é o computador que hospeda a função do *Directory*. Todos os outros servidores (de expansão) no sistema devem se conectar ao servidor principal para fazer parte do mesmo sistema.

É possível ter apenas um servidor principal em um sistema do Security Center.

Servidores de expansão

Um servidor de expansão é um computador que você adiciona ao seu sistema para aumentar a potência geral. Um servidor de expansão deve se conectar ao servidor principal e pode hospedar qualquer função no Security Center, exceto a de Directory.

É possível aumentar a potência do computador do seu sistema a qualquer momento, basta adicionar mais servidores de expansão ao seu grupo de recursos.

Serviço Servidor Genetec™

O serviço Servidor Genetec™ é um serviço do Windows que é instalado automaticamente ao instalar o Security Center Server em um computador.

O Security Center Server e o serviço *Servidor Genetec™* devem ser instalados em cada computador que você queira incluir no conjunto de servidores disponível para o Security Center. Após o serviço *Servidor Genetec™* estar instalado, você pode alterar sua senha e outras configurações usando o aplicativo Web *Server Admin*.

Tópicos relacionados

Adicionando Servidores de Expansão na página 109

Abrir o Server Admin usando um navegador da Web

Usando um navegador da Web, você pode abrir o Server Admin em qualquer servidor em seu sistema e então alterar as configurações de qualquer servidor em seu sistema.

Antes de iniciar

Para fazer logon em um servidor de seu sistema usando o Server Admin, você deve saber o nome de DNS ou endereço IP do servidor, a porta do servidor da Web e a senha do servidor. A senha do servidor é especificada durante a instalação do Security Center Server e é o mesmo para todos os servidores no seu sistema.

O que você deve saber

Independentemente de a qual servidor de expansão você tente se conectar, o Server Admin sempre o redirecionará para o servidor principal, se as seguintes condições forem cumpridas:

- O servidor de expansão está conectado ao servidor principal.
- O servidor de expansão e o servidor principal estão executando a mesma versão (X.Y) do Security Center.

Para abrir o Server Admin usando um navegador da Web:

1 Fazer um dos seguintes:

- Na barra de endereços do seu navegador, digite `http://computer:port/Genetec`, onde `computer` é o nome DNS ou o endereço IP do servidor e `port` é a porta do servidor Web especificada durante a instalação do Security Center Server.

  Pode omitir a porta do servidor da Web se está usando o valor padrão (80).

- Se estiver se conectando ao Server Admin a partir de um host local, clique duas vezes em **Genetec™Server Admin** () na pasta *Genetec Security Center* no menu Iniciar do Windows.

NOTA: Se você estiver se conectando a um servidor remoto, o Server Admin usa uma conexão segura (HTTPS). Se o seu servidor estiver usando um certificado autoassinado, o navegador avisa que sua conexão não é segura. Se você receber a mensagem de alerta, ignore-a e prossiga com a conexão sem segurança.

2 Digite a senha do servidor que definiu durante a instalação do servidor e clique em **Log on**.

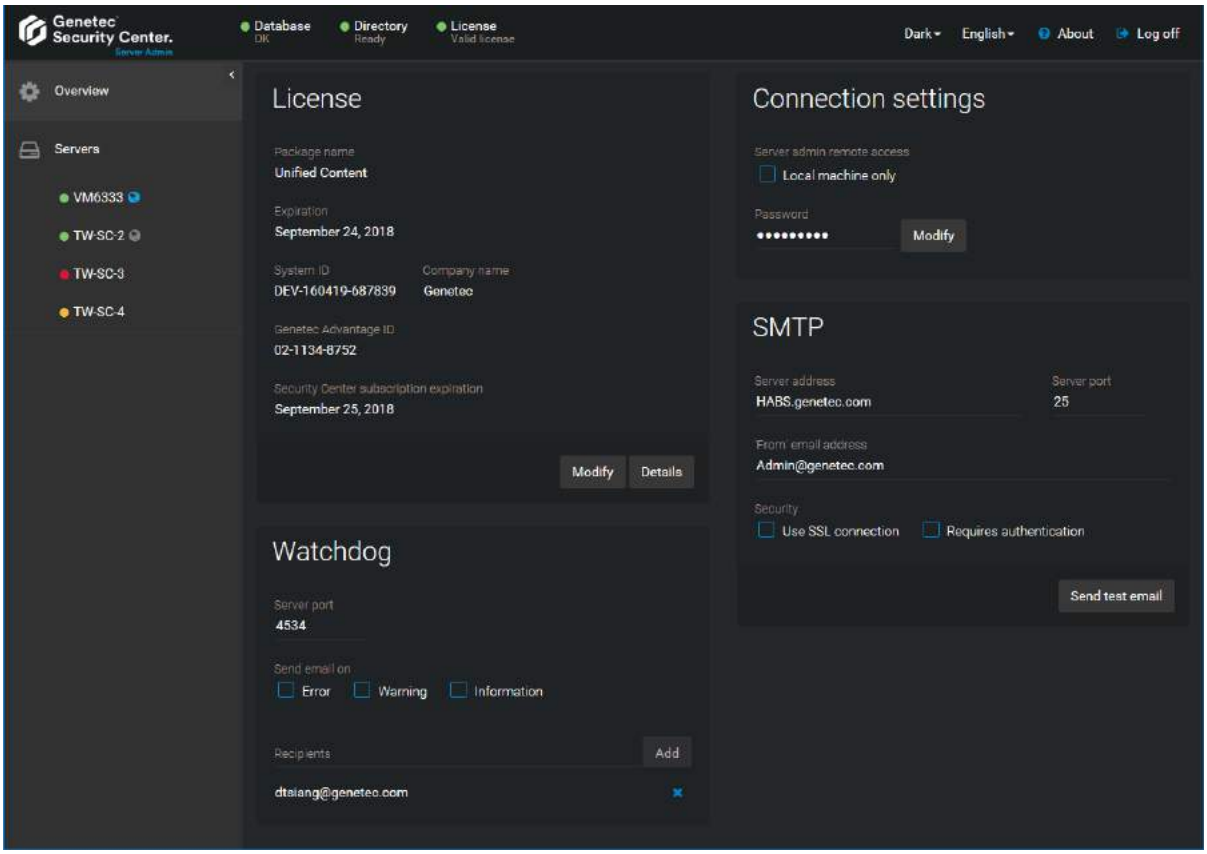
A página *Visão Geral* do Server Admin será exibida.

Tópicos relacionados

Server Admin - Página de visão geral na página 101
O que é o protocolo Transport Layer Security? na página 372

Server Admin - Página de visão geral

A página *Visão geral*do Server Admin mostra suas informações de licença do Security Center e as configurações comuns (Watchdog, Conexão, SMTP) que se aplicam a todos os servidores em seu sistema.



Painel (superior esquerdo)

O painel indica o status (●=preparado, ●=preparando, ●=não preparado) do seu sistema em todo o tempo, para os seguintes componentes:

- **Banco de dados:** Banco de dados do Directory. Clique para ir até a seção de configuração do banco de dados do Directory.
- **Diretório:** Função do diretório. Clique para iniciar, interromper ou reiniciar a função do Directory.
- **Licença:** Licença do Security Center. Clique para ativar a licença ou exibir os detalhes da licença.

Servidores (painel esquerdo)

Lista de todos os servidores encontrados em seu sistema (apenas se você estiver conectado ao servidor principal). Clique em um servidor da lista para exibir a página de configuração.

O status e a função de cada servidor são indicados como segue:

- **:** Servidor primário do Directory (servidor principal).
- **:** Servidor secundário do Directory.
- **Sem ícone:** Servidor de expansão.
- **:** O servidor está ativado.

- : O servidor está desativado.
- : O servidor tem problemas.

Licença

Status e informações da licença do Security Center.

- **Nome do pacote:** Nome do pacote do software.
- **Validade:** Data quando a sua licença expira.
- **ID do sistema:** O número de ID do seu sistema.
- **Nome da empresa:** Nome da sua empresa.
- **ID do Genetec Advantage:** ID do seu contrato Genetec™ Lifecycle Management (GLM). Se você não tiver adquirido um contrato GLM, este campo não estará definido.
- **Tempo de validade da assinatura do Security Center:** Data de vencimento do seu contrato Genetec™ Lifecycle Management (GLM).
- **Modificar:** Clique para ativar ou modificar sua licença do Security Center.
- **Detalhes:** Clique para visualizar detalhes da sua licença do Security Center.

Watchdog

Use esta seção para configurar o serviço *Genetec™ Watchdog*. A função do Watchdog é garantir que o serviço Servidor Genetec™ sempre esteja em execução.

- **Porta do servidor:** Porta de comunicação entre o Watchdog e o servidor.
- **Enviar e-mail ao:** Envia notificações de e-mail pelo Watchdog para uma lista de destinatários em caso de eventos de *Erro*, *Alerta* e *Informação*.
- **Destinatários:** Usuários do Security Center que recebem os e-mails do Watchdog.

Configurações de conexão

Use esta seção para definir as configurações de conexão do Server Admin.

- **Somente máquina local:** Ative esta opção para restringir as conexões do Server Admin à máquina local.
- **Senha:** Senha de login para o Server Admin.

SMTP

Use esta seção para configurar o servidor SMTP responsável por lidar com mensagens de e-mail no Security Center.

- **Endereço do servidor:** O nome DNS ou o endereço IP do servidor SMTP de e-mail.
- **Porta do servidor:** A porta do servidor normalmente é 25, embora seu servidor de e-mail possa usar uma porta diferente.
- **Endereço de e-mail "De":** Endereço de e-mail mostrado como o remetente do e-mail.
- **Usar conexão SSL:** Ativa a comunicação segura com o servidor de e-mail.
- **Exige autenticação:** Ative esta opção se o seu servidor de e-mail exige autenticação. Em caso positivo, você precisará inserir um nome de usuário e senha.
- **Enviar e-mail de teste:** Enviar um e-mail de teste para validar sua configuração SMTP.

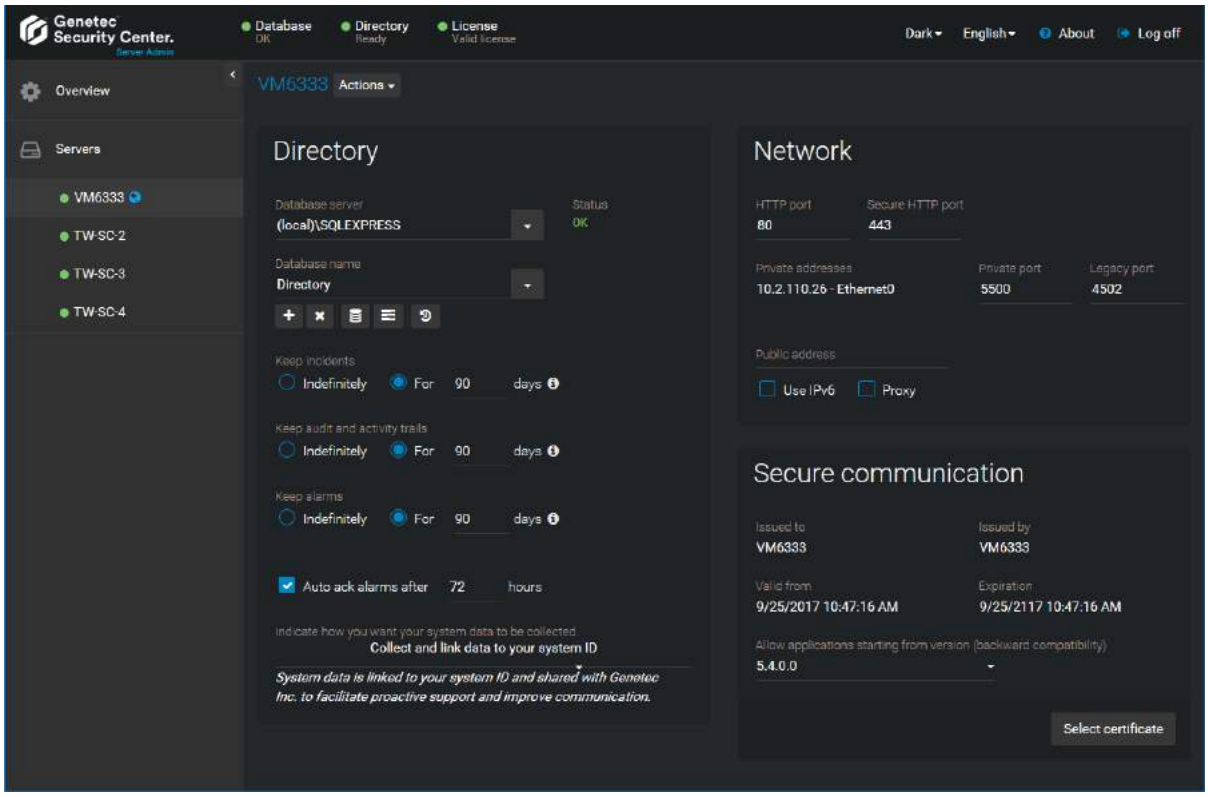
Tópicos relacionados

Server Admin - Página do servidor principal na página 104

Server Admin - Página Servidor de expansão na página 107
Ativar sua licença do Security Center usando a Web na página 115
Ativar licenças do Security Center sem acesso à Internet na página 118
Servidor - Aba Propriedades na página 1029

Server Admin - Página do servidor principal

A página Server Admin - *Servidor principal* permite que você configure seu banco de dados do Directory e as configurações referentes ao seu servidor principal.



Ações

Clique na lista suspensa **Ações** ao lado do nome do servidor para ver quais ações podem ser aplicadas ao servidor principal.

As ações disponíveis são:

- **Directory:**
  - **Iniciar/parar:** Iniciar ou parar o Directory.
  - **Reiniciar:** Reiniciar o Directory.
  - **Desativar:** Converter o servidor principal em um servidor de expansão.
- **Servidor Genetec™:**
  - **Console:** Abra a página *Console de depuração* (reservada para engenheiros de Suporte Técnico da Genetec™).
  - **Reiniciar:** Reinicie o serviço Servidor Genetec™. Esta ação deixa o servidor temporariamente indisponível.

Directory

A seção *Directory* mostra o status e as configurações de banco de dados do Directory. O banco de dados do Directory contém todas as configurações de sistema e de entidades, os relatórios de incidentes e o histórico de alarmes.

NOTA: Se você tiver acessado o Server Admin a partir de Config Tool em vez de um navegador da Web, você não verá os comandos do banco de dados (atualizar ou restaurar o banco de dados) porque você ainda estará conectado ao Directory. Você não poderá modificar o banco de dados do Directory enquanto ainda estiver conectado a ele.

- **Servidor de banco de dados:** Nome do serviço SQL Server (padrão=`(local)\SQLEXPRESS`).
- **Nome do banco de dados:** Nome da instância de banco de dados (padrão=`Directory`).
- **Ações:** Ações relacionadas à manutenção do banco de dados do Directory.
  - **Criar banco de dados ( ):** Crie um novo banco de dados.
  - **Excluir banco de dados ( ):** Exclua o banco de dados.
  - **Propriedades do banco de dados ( ):** Abre uma caixa de diálogo mostrando as informações do banco de dados e as configurações de backup automático e Notificação por e-mail.
  - **Mostrar progresso ( ):** Abre uma caixa de diálogo que exibe as ações atuais e anteriores sendo executadas no banco de dados.
  - **Atualizar banco de dados ( ):** Atualize o esquema do banco de dados para a versão atual.
  - **Resolver conflitos ( ):** Resolva conflitos de entidades importadas.
  - **Backup/restauração ( ):** Faça backup de ou restaure o banco de dados.
- **Manter incidentes:** Especifique por quanto tempo os relatórios de incidentes são mantidos no banco de dados do Directory.
- **Manter trilhas de auditoria e atividade:** Especifique por quanto tempo o histórico de configurações de entidades e o histórico de atividades são mantidos no banco de dados do Directory.
- **Manter alarmes:** Especifique por quanto tempo o histórico de alarmes é mantido no banco de dados do Directory.
- **Confirmar alarmes automaticamente após:** Ative esta opção para permitir que o sistema confirme automaticamente todos os alarmes ativos que não forem confirmados antes do tempo especificado (em horas). Quando ativada, esta opção substitui a opção **Confirmação automática** configurada para cada alarme individual. Quando a confirmação automática de alarmes está ativada em nível de alarme de sistema e individual, é o retardo mais curto que se aplica.
- **Indicar como você quer que os dados de seu sistema sejam coletados:** Você pode alterar sua preferência de coleta de dados selecionada na instalação do sistema. As opções são:
  - **Não coletar dados:** Nenhum dado é coletado para fins de melhoria do produto.
  - **Coletar dados anonimamente:** Os dados do sistema são coletados e compartilhados com a Genetec Inc., mas todos os dados que identifiquem sua empresa são removidos primeiro.
  - **Coletar e associar dados à ID do seu sistema:** Os dados do sistema são associados à ID do seu sistema e compartilhados com a Genetec Inc. para facilitar o suporte proativo e melhorar a comunicação.

Rede

Use esta seção para configurar a placa de rede e a porta TPC de escuta usada pelo serviço Servidor Genetec™.

- **Porta HTTP:** Porta usada pelo serviço Servidor Genetec™ para escuta de comandos recebidos de outros servidores do Security Center no endereço público.
- **Porta HTTP segura:** Porta usada pelo serviço Servidor Genetec™ para conexões HTTP seguras.
- **Endereço privado:** Lista de endereços privados correspondente às placas de interface de rede (NIC) instaladas neste servidor. Selecione somente as que são usadas para comunicação entre aplicativos do Security Center.

- **Porta privada:** Porta usada pelo servidor principal para escuta de solicitações de conexão de entrada e por todos os servidores para comunicação entre si, no endereço IP privado (padrão=5500).

  NOTA: Se você alterar esta porta no servidor principal, todos os usuários deverão especificar o novo número da porta após o nome do **Directory** na caixa de diálogo *Logon*, separado por dois pontos (:). Isso se aplica a todos os servidores de expansão. Você deve especificar o novo número da porta depois do nome do **Directory do Security Center** no Server Admin, na seção *Conexão do servidor principal*.
- **Porta legada:** Porta usada pelo serviço Servidor Genetec™ para escuta de comandos recebidos de servidores executando uma versão mais antiga do Security Center (padrão=4502).
- **Endereço público:** Endereço público do servidor.
  - **Usar IPv6:** Use *IPv6* para transmissão de vídeo e comunicação entre servidores (somente se a sua rede suportar).
  - **Proxy:** Selecione esta opção se o servidor for usado como servidor proxy para uma rede privada protegida por um firewall.

Comunicação segura

Use esta seção para visualizar a atual *certificado de identidade* usada pelo servidor para comunicar com outros servidores do Security Center.

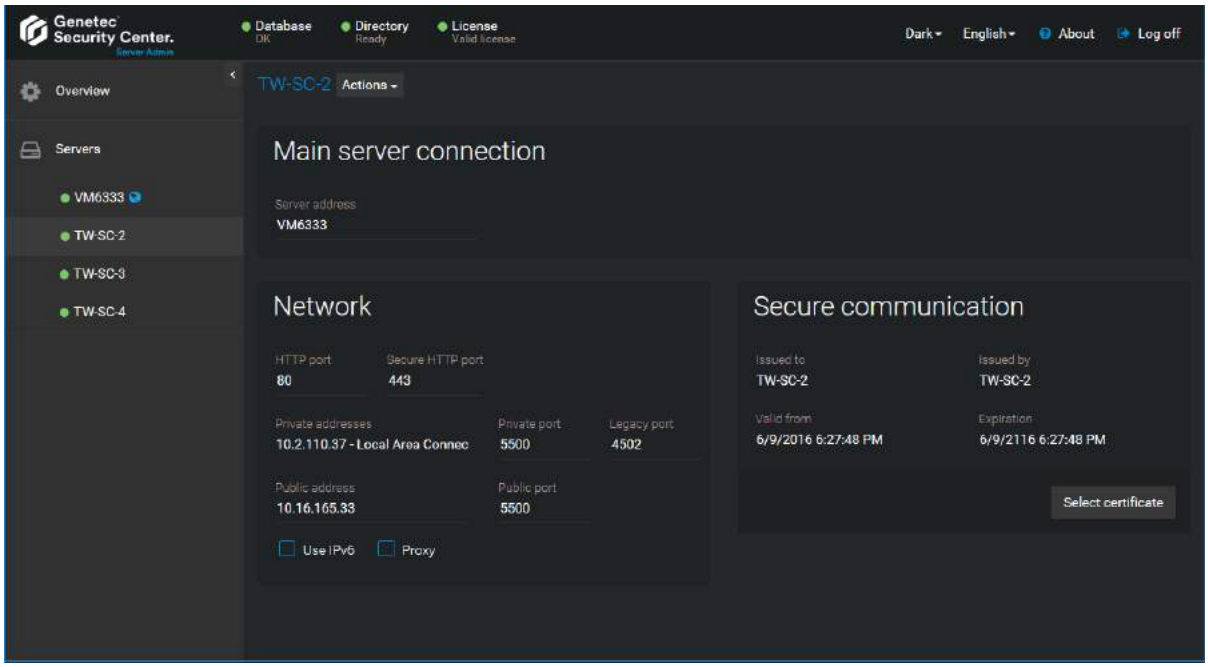
- **Emitido para:** Objeto do certificado atual. Um *certificado auto-assinado* criado na instalação do software aparece no formato *GenetecServer-{MachineName}*.
- **Emitido por:** Nome da *autoridade de certificação (CA — certificate authority)* que emitiu o certificado. O emissor e o objeto são os mesmos para certificados autoassinados.
- **Válido de/até:** Período de validade do certificado atual.
- **Selecionar certificado (botão):** Caixa de dialogo listando todos os certificados instalados nesta máquina. Você pode usar esta caixa de diálogo para alterar o certificado usado para este servidor.
- **Permitir conexões não autenticadas (5.3 e anteriores):** Para aumentar a segurança do sistema, desative essa opção (padrão=ativado). Desativar esta opção impede que clientes e servidores do Security Center mais antigos (5.3 e anteriores) se conectem ao servidor principal. Para mais informações, consulte Desabilitar compatibilidade com versões anteriores na página 377.

Tópicos relacionados

Server Admin - Página de visão geral na página 101
Servidor - Aba Propriedades na página 1029

Server Admin - Página Servidor de expansão

A página Server Admin - *Servidor de expansão* mostra todas as configurações relacionadas ao servidor de expansão selecionado.



Ações

Clique na lista suspensa **Ações** ao lado do nome do servidor para ver quais ações podem ser aplicadas ao servidor de expansão.

As ações disponíveis são:

- **Directory:**
  - **Ativar:** Converter o servidor de expansão em um servidor principal.
- **Servidor Genetec™:**
  - **Console:** Abra a página *Console de depuração* (reservada para engenheiros de Suporte Técnico da Genetec™).
  - **Reiniciar:** Reinicie o serviço Servidor Genetec™. Esta ação deixa o servidor temporariamente indisponível.

Conexão ao servidor principal

Esta seção identifica o servidor principal ao qual o servidor de expansão precisa se conectar.

- **Endereço do servidor:** O nome DNS ou o endereço IP do servidor principal.
- **Alterar senha:** Aparece apenas quando nenhuma conexão tiver sido estabelecida entre o servidor de expansão e o servidor principal. Clique para configurar a senha. Uma vez que o primeiro contato seja feito, o servidor de expansão enviará seu *certificado de identidade* para o servidor principal e a senha não é necessária novamente.

Rede

Use esta seção para configurar a placa de rede e a porta TPC de escuta usada pelo serviço Servidor Genetec™.

- **Porta HTTP:** Porta usada pelo serviço Servidor Genetec™ para escuta de comandos recebidos de outros servidores do Security Center no endereço público.
- **Porta HTTP segura:** Porta usada pelo serviço Servidor Genetec™ para conexões HTTP seguras.
- **Endereço privado:** Lista de endereços privados correspondente às placas de interface de rede (NIC) instaladas neste servidor. Selecione somente as que são usadas para comunicação entre aplicativos do Security Center.
- **Porta privada:** Porta usada pelo servidor principal para escuta de solicitações de conexão de entrada e por todos os servidores para comunicação entre si, no endereço IP privado (padrão=5500).

  NOTA: Se você alterar esta porta no servidor principal, todos os usuários deverão especificar o novo número da porta após o nome do **Directory** na caixa de diálogo *Logon*, separado por dois pontos (:). Isso se aplica a todos os servidores de expansão. Você deve especificar o novo número da porta depois do nome do **Directory do Security Center** no Server Admin, na seção *Conexão do servidor principal*.
- **Porta legada:** Porta usada pelo serviço Servidor Genetec™ para escuta de comandos recebidos de servidores executando uma versão mais antiga do Security Center (padrão=4502).
- **Endereço público:** Endereço público do servidor.
  - **Usar IPv6:** Use *IPv6* para transmissão de vídeo e comunicação entre servidores (somente se a sua rede suportar).
  - **Proxy:** Selecione esta opção se o servidor for usado como servidor proxy para uma rede privada protegida por um firewall.

Comunicação segura

Use esta seção para visualizar a atual *certificado de identidade* usada pelo servidor para comunicar com outros servidores do Security Center.

- **Emitido para:** Objeto do certificado atual. Um *certificado auto-assinado* criado na instalação do software aparece no formato *GenetecServer-{MachineName}*.
- **Emitido por:** Nome da *autoridade de certificação (CA — certificate authority)* que emitiu o certificado. O emissor e o objeto são os mesmos para certificados autoassinados.
- **Válido de/até:** Período de validade do certificado atual.
- **Selecionar certificado (botão):** Caixa de dialogo listando todos os certificados instalados nesta máquina. Você pode usar esta caixa de diálogo para alterar o certificado usado para este servidor.

Tópicos relacionados

Server Admin - Página de visão geral na página 101
Servidor - Aba Propriedades na página 1029

Adicionando Servidores de Expansão

Você pode adicionar servidores de expansão ao seu sistema a qualquer momento para aumentar o poder geral de processamento do seu sistema.

O que você deve saber

Um servidor de expansão é qualquer servidor em um sistema Security Center que não hospede a função de Directory. A finalidade do servidor de expansão é aumentar o poder de processamento do sistema.

Cada sistema do Security Center exige o seu próprio conjunto de servidores para executar as funções do sistema. Você deve garantir que hava poder de processamento suficiente disponível para executar suas funções necessárias.

Para adicionar um servidor de expansão:

1 Instale o Server Security Center no computador que deseja adicionar ao conjunto de servidores.

Para obter mais informações sobre como instalar o Server Security Center, consulte o *Guia de Instalação e Atualização do Security Center*.

2 Conecte aquele computador ao servidor principal do Security Center.

O servidor principal é o que abriga a função do Directory. Isto é feito com o Server Admin através de um navegador Web.

3 Abra o Config Tool em qualquer estação de trabalho.

4 Na página inicial, abra a tarefa **Exibição de rede**.

O servidor que você acabou de adicionar deve aparecer na estrutura da rede. O nome da entidade do servidor deve combinar com o nome do domínio do servidor.

5 Selecione a entidade do novo servidor e clique na aba **Propriedades**

Se o servidor for usado como proxy para uma rede privada protegida por um firewall, defina seu **Endereço público** e **Porta** conforme configurado por seu departamento de TI.

6 Clique em **Aplicar**.

Agora você pode atribuir funções ao servidor.

Tópicos relacionados

Visão geral da arquitetura do Security Center na página 5

Converter o servidor principal em um servidor de expansão

Você pode converter seu servidor principal em um servidor de expansão, se você quiser que uma máquina diferente assuma a função de servidor principal.

Antes de iniciar

- Prepara outro servidor para assumir como o novo servidor principal em seu sistema. Para obter mais informações sobre como instalar o Security Center em um servidor principal, consulte o *Guia de Instalação e Atualização do Security Center*.
- Se você precisar manter a configuração do seu sistema e se o banco de dados do Directory atualmente estiver hospedado em seu servidor principal, mova o banco de dados do Directory para um servidor diferente (este pode ser o novo servidor principal que você preparou).

O que você deve saber

Você converte um servidor principal em um servidor de expansão desativando a função Directory no seu servidor usando a função Server Admin.

CUIDADO: Essa operação reinicia o serviço Genetec™ Server, o que desativa temporariamente todas as funções hospedadas no seu servidor. É necessário realizar logon no Server Admin novamente para conectar seu servidor principal antigo (convertido para um servidor de expansão) ao novo servidor principal que você preparou.

Para converter o servidor principal em um servidor de expansão:

1 Faça logon no Server Admin em seu computador usando um navegador da Web.
2 Na lista de servidores, selecione o servidor principal ( ).
A página Server Admin - Servidor principal é exibida.
3 Ao lado do nome do servidor, clique em **Ações** > **Desativar**.
4 Na caixa de diálogo de confirmação que aparece, clique em **Continuar**.
O serviço Genetec™ Server é reiniciado. Você será desconectado temporariamente do Server Admin.
5 Redefina a ID de identificação do servidor.
a) Em um editor de texto, abra o arquivo *GenetecServer.gconfig* localizado na pasta *ConfigurationFiles*, na pasta de instalação do Security Center (*C:\Program Files (x86)\Genetec Security Center 5.7*\).
b) Encontre e exclua a seguinte frase `<serverIdentification id="<guid>" />`.
c) Salve as alterações e feche o arquivo.
6 Abra um navegador da Web e digite `http://machine/Genetec` na barra de endereços, onde `machine` é o nome de DNS ou o endereço IP do seu servidor.
7 Faça novamente logon no Server Admin.
A página Server Admin - Servidor de expansão é exibida.
8 Na seção *Conexão do servidor principal* digite o nome e a senha do servidor principal ao qual o servidor de expansão deve se conectar e clique em **Salvar**.
9 Na caixa de diálogo de confirmação que aparece, clique em **Sim**.
O serviço Genetec™ Server é reiniciado. Você será desconectado temporariamente do Server Admin.
10 Feche a página do seu navegador e abra uma nova página.
11 Faça logon novamente no Server Admin e verifique se você está conectado ao novo servidor principal.

Tópicos relacionados

Substituir o servidor principal na página 129

Converter um servidor de expansão em servidor principal:

Para substituir seu servidor principal existente ou começar um novo sistema, você pode converter um servidor de expansão em servidor principal.

Antes de iniciar

Se estiver substituindo um servidor principal antigo e se o banco de dados do Directory estava hospedado no seu antigo servidor principal, mova o banco de dados do Directory para o servidor que você deseja converter ou para um terceiro computador.

O que você deve saber

Você converte um servidor de expansão em um servidor principal ativando a função Directory do seu servidor usando a função Server Admin.

CUIDADO: Essa operação reinicia o serviço Genetec™ Server, o que desativa temporariamente todas as funções hospedadas no seu servidor. Você deve fazer logon novamente no Server Admin para ativar sua licença do software em seu novo servidor principal.

Para converter um servidor de expansão em servidor principal:

1. Faça logon no Server Admin em seu computador usando um navegador da Web.
2. Na lista de servidores, selecione o servidor de expansão que deseja converter.

   A página Server Admin - Servidor de expansão é exibida.
3. Ao lado do nome do servidor, clique em **Ações** > **Ativar**.
4. Na caixa de diálogo de confirmação que aparece, clique em **Continuar**.

   O serviço Genetec™ Server é reiniciado. Você será desconectado temporariamente do Server Admin.
5. Abra um navegador da Web e digite `http://machine/Genetec` na barra de endereços, onde `machine` é o nome de DNS ou o endereço IP do seu servidor.
6. Faça novamente logon no Server Admin.

   A página Server Admin - Visão geral é exibida.
7. Ative a licença de software no novo servidor principal.
8. Se você estiver substituindo um servidor principal antigo, defina as configurações do banco de dados na página Server Admin - Servidor principal para que este servidor se conecte ao banco de dados existente do Directory.

   Esta operação força o servidor de expansão (promovido a servidor principal) a assumir a identidade do antigo servidor principal. Isso significa que se havia funções hospedadas no servidor de expansão anteriormente, elas deverão ser movidas para o *novo* servidor principal, pois a ID do servidor de expansão foi alterada.
9. Na página inicial do Config Tool, abra a tarefa *Exibição de rede*.
10. Na visualização de rede, se você ver uma cópia offline do servidor de expansão que você acabou de converter ( ), exclua-o.

Após terminar

- (Opcional) Converter o servidor principal em um servidor de expansão.
- Conecte todos os servidores de expansão em seu sistema ao novo servidor principal.

Tópicos relacionados

Conectar servidores de expansão ao servidor principal na página 112
Substituir o servidor principal na página 129

Conectar servidores de expansão ao servidor principal

Sempre que migrar o servidor principal para um novo computador, você deve usar o Server Admin para reconectar todos os servidores de expansão no seu sistema ao novo computador.

Antes de iniciar

Depois de concluir uma instalação do servidor de expansão, o servidor de expansão se conecta automaticamente ao servidor principal. Só deve seguir as etapas de conectar o servidor de expansão ao servidor principal se:

- Inseriu os parâmetros de conexão errados ao servidor principal durante a instalação do servidor de expansão.
- Migrou o servidor principal para um computador diferente.
- Alterou a senha no servidor principal enquanto o servidor de expansão estava inativo.
- Habilitou a Autenticação no Directory no seu servidor de expansão, mas o seu certificado do Directory não está assinado por uma autoridade de certificação.

Para conectar um servidor de expansão ao servidor principal:

1 Abra a página da Web do Server Admin executando um dos seguintes procedimentos:

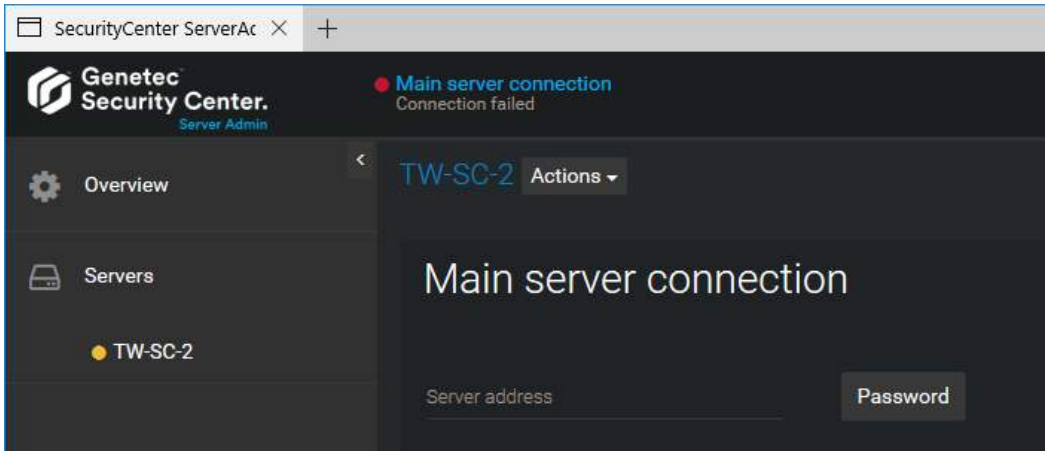
- Na barra de endereços do seu navegador, digite `http://computer:port/Genetec`, onde `computer` é o nome DNS ou o endereço IP do servidor e `port` é a porta do servidor Web especificada durante a instalação do Security Center Server.

  Pode omitir a porta do servidor da Web se está usando o valor padrão (80).
- Se estiver se conectando ao Server Admin a partir de um host local, clique duas vezes em **Genetec™Server Admin** ( ) na pasta *Genetec Security Center* no menu Iniciar do Windows.

2 Digite a senha do servidor que definiu durante a instalação do servidor e clique em **Log on**.

A página *Visão Geral* do Server Admin será exibida.

3 Se não estiver conectado ao servidor principal, clique em **Conexão ao servidor principal** na parte superior da janela Server Admin.

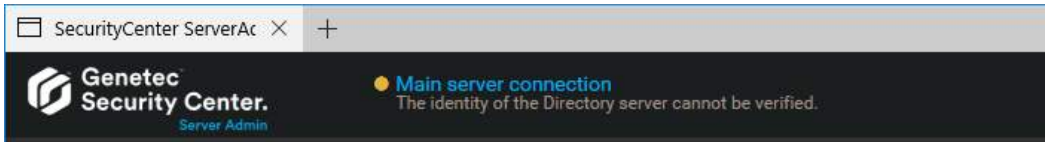


4 Digite o **Endereço do servidor** (nome DNS ou endereço IP do servidor principal) e **Senha** e, em seguida, clique em **Salvar**.

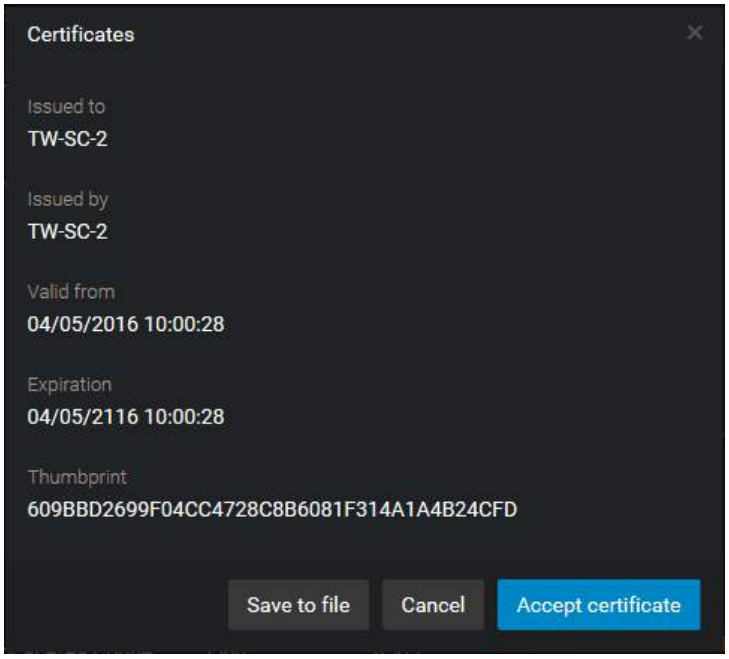
5 Quando for solicitado a reiniciar o serviço, clique em **Sim**.

Enquanto o serviço *Genetec™ Server* for reiniciado, você ficará temporariamente desconectado do Server Admin.

6 Depois de efetuar logon novamente no Server Admin, se receber a mensagem de que a identidade do Directory não pode ser verificada, clique em **Conexão ao servidor principal**.



7 Na caixa de diálogo exibida, verifique se o certificado do servidor principal está conforme o esperado e clique em **Aceitar certificado**.



IMPORTANTE: Uma vez aceito, o certificado é armazenado em uma lista de permissões local e não será necessário aceitá-lo novamente. Se receber esse pedido, deve notificar imediatamente seu departamento de TI.

MELHOR PRÁTICA: Para evitar o desgaste de ter que aceitar o certificado do servidor principal sempre que alguém tentar se conectar a ele a partir de uma nova máquina, use somente certificados assinados por uma autoridade de certificação designada como confiável pelo departamento de TI da empresa.

8 Clique em **Salvar**.

9 Quando for solicitado a reiniciar o serviço, clique em **Sim**.

Enquanto o serviço *Genetec™ Server* for reiniciado, você ficará temporariamente desconectado do Server Admin.

O servidor de expansão agora está conectado ao servidor principal. Os dois servidores permanecerão conectados, mesmo quando alterar o certificado, em um ou ambos os servidores, desde que os dois servidores estejam conectados enquanto a alteração está sendo feita.

Tópicos relacionados

O que é a autenticação do diretório? na página 373

Ativar sua licença do Security Center usando a Web

A licença do Security Center é ativada no servidor principal. Você deve ativar sua licença do Security Center depois de instalar o Security Center no servidor principal, e quando instaurar um servidor de expansão para um servidor principal. Se você tiver acesso à Internet, você pode ativar a sua licença do Security Center utilizando uma ligação Web através do Server Admin.

Antes de iniciar

Para ativar sua licença usando a web, precisa do seguinte:

- **Conexão à internet:** Se o seu servidor não tiver acesso à Internet, consulte Ativar licenças do Security Center sem acesso à Internet na página 118.
- **ID do sistema e senha:** O ID e a senha do Sistema encontram-se no documento *Informações de Licença do Security Center*. O Serviço de Atendimento ao Cliente Genetec™ envia este documento quando o cliente compra o produto.
- **Senha do servidor:** A senha do servidor é usada para fazer logon no Server Admin. A senha do servidor é definida durante a instalação.

Para ativar sua licença do Security Center usando a Web:

1 Abra a página da Web do Server Admin executando um dos seguintes procedimentos:

- Na barra de endereços do seu navegador, digite `http://computer:port/Genetec`, onde `computer` é o nome DNS ou o endereço IP do servidor e `port` é a porta do servidor Web especificada durante a instalação do Security Center Server.

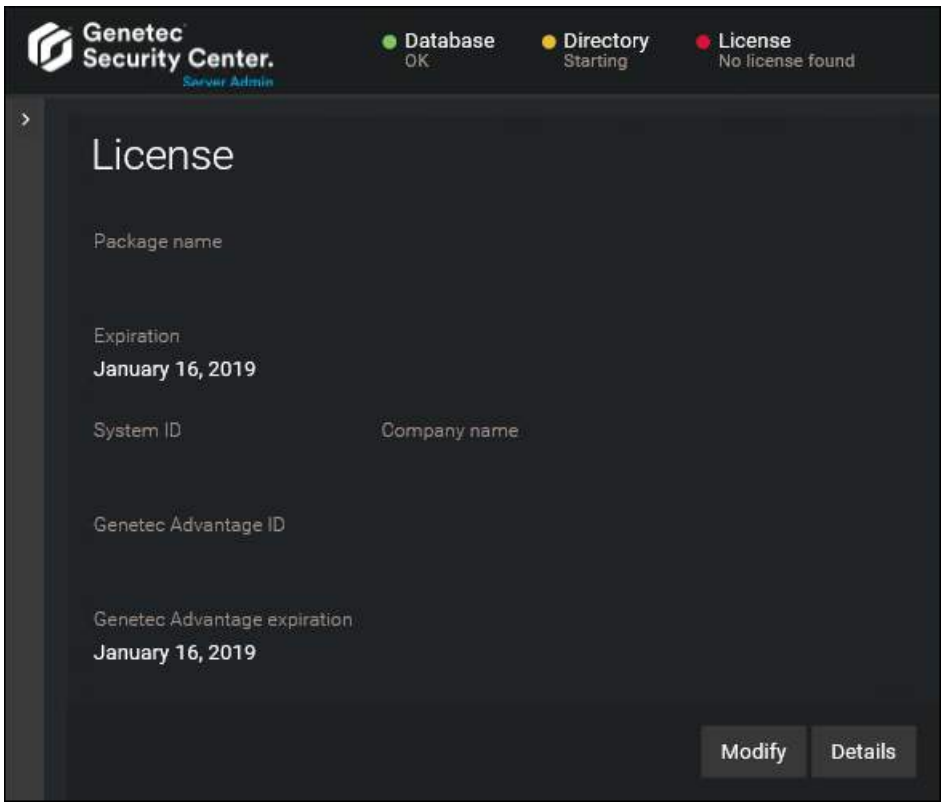
  Pode omitir a porta do servidor da Web se está usando o valor padrão (80).
- Se estiver se conectando ao Server Admin a partir de um host local, clique duas vezes em **Genetec™Server Admin** () na pasta *Genetec Security Center* no menu Iniciar do Windows.

2 Digite a senha do servidor que definiu durante a instalação do servidor e clique em **Log on**.

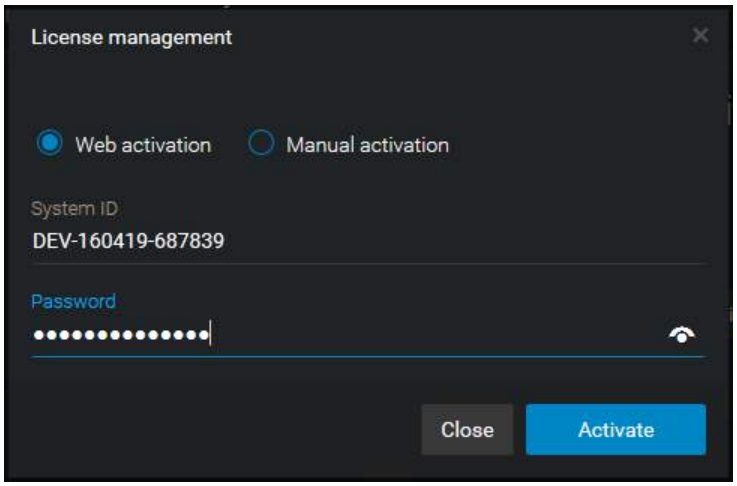
A página *Visão Geral* do Server Admin será exibida.

3 Fazer um dos seguintes:

- Clique em **Licença** na parte superior da janela do navegador do Server Admin.
- Clique em **Modificar** na seção *Licença* da página *Visão Geral* do Server Admin.

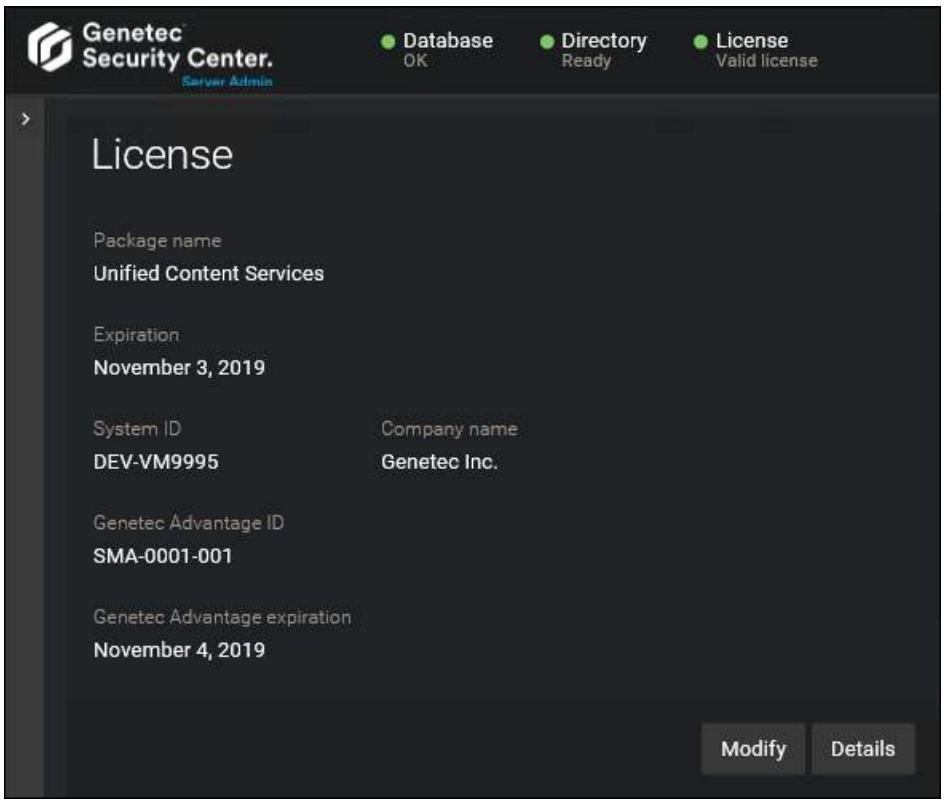


4 Na caixa de diálogo *Gerenciamento de licenças*, clique em **Ativação Web** e digite o **ID do Sistema** e a **Senha** conforme especificado no documento de *Informações de Licença do Security Center* que recebeu quando adquiriu sua licença.

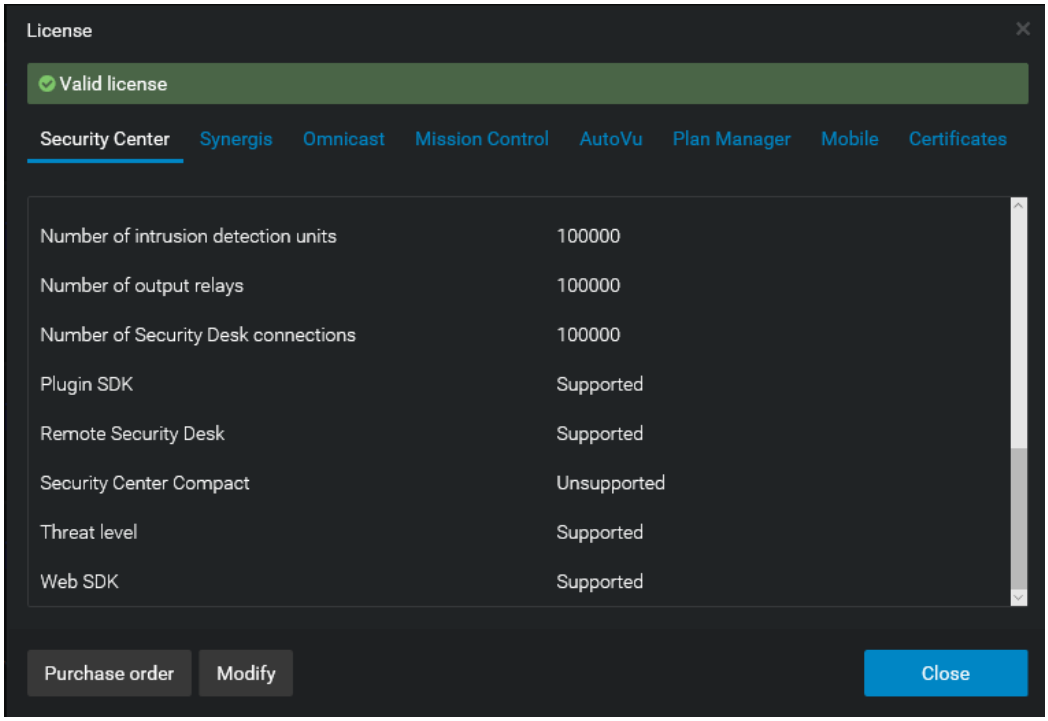


5 Clique em **Ativar**.

As informações da licença são exibidas na seção *Licença* da página *Visão Geral* do Server Admin.



6 Clique em **Detalhes** para exibir suas opções de licença em uma caixa de diálogo.



Suas opções de licença estão divididas em várias abas. Para mais informações, consulte o *Security Center Guia do Administrador*.

7 Clique em **Fechar** e, em seguida, feche a janela do navegador.

Ativar licenças do Security Center sem acesso à Internet

A licença do Security Center é ativada no servidor principal. Você deve ativar sua licença do Security Center depois de instalar o Security Center no servidor principal, e quando instaurar um servidor de expansão para um servidor principal. Se não tiver acesso à Internet, você pode ativar a sua licença do Security Center manualmente usando uma combinação de Server Admin e GTAP.

Antes de iniciar

Para ativar sua licença, precisa do seguinte:

- **ID do sistema e senha:** O ID e a senha do Sistema encontram-se no documento *Informações de Licença do Security Center*. O Serviço de Atendimento ao Cliente Genetec™ envia este documento quando o cliente compra o produto.
- **Senha do servidor:** A senha do servidor é usada para fazer logon no Server Admin. A senha do servidor é definida durante a instalação.

Para ativar a licença do Security Center sem acesso à Internet:

1 Abra a página da Web do Server Admin executando um dos seguintes procedimentos:

- Na barra de endereços do seu navegador, digite `http://computer:port/Genetec`, onde `computer` é o nome DNS ou o endereço IP do servidor e `port` é a porta do servidor Web especificada durante a instalação do Security Center Server.

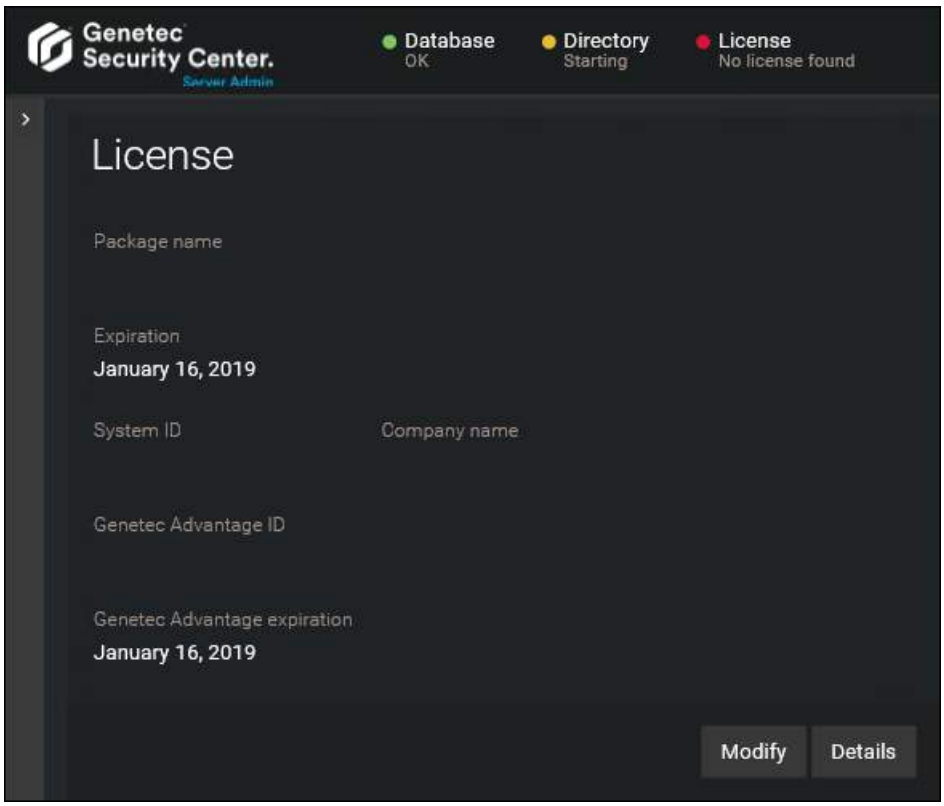
  Pode omitir a porta do servidor da Web se está usando o valor padrão (80).
- Se estiver se conectando ao Server Admin a partir de um host local, clique duas vezes em **Genetec™Server Admin** ( ) na pasta *Genetec Security Center* no menu Iniciar do Windows.

2 Digite a senha do servidor que definiu durante a instalação do servidor e clique em **Log on**.

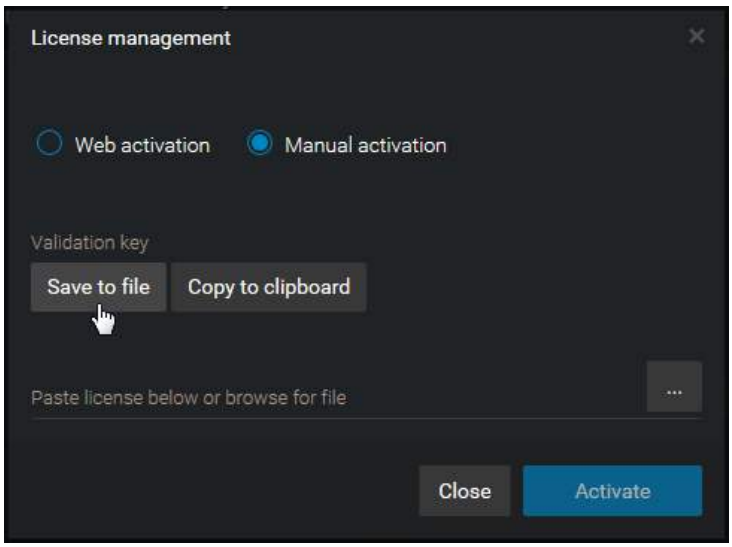
A página *Visão Geral* do Server Admin será exibida.

3 Fazer um dos seguintes:

- Clique em **Licença** na parte superior da janela do navegador do Server Admin.
- Clique em **Modificar** na seção *Licença* da página *Visão Geral* do Server Admin.



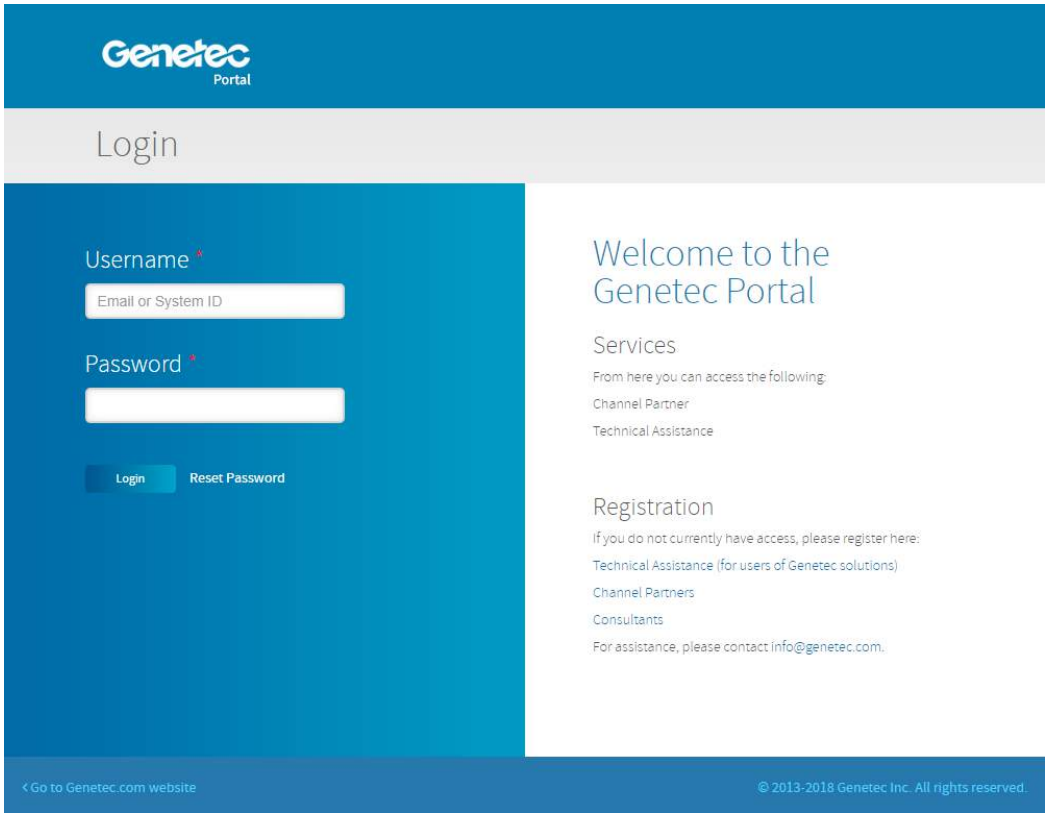
4 Na caixa de diálogo *Gerenciamento de licenças*, clique em **Ativação manual** e, em *Chave de validação*, clique em **Salvar para arquivo**.



A chave de validação é uma sequência de números (em formato de texto hexadecimal) gerada pelo Security Center que identifica o servidor de forma exclusiva. A chave de validação é usada para gerar a chave de licença que desbloqueia o software Security Center. Ela só pode ser aplicada ao servidor previamente identificado pela chave de validação.

Um arquivo de texto chamado *validation.vk* é salvo em sua pasta de *Downloads* padrão. Certifique-se de copiar este arquivo para um local (isso pode ser uma chave USB) que possa acessar de outro computador que tenha acesso à Internet.

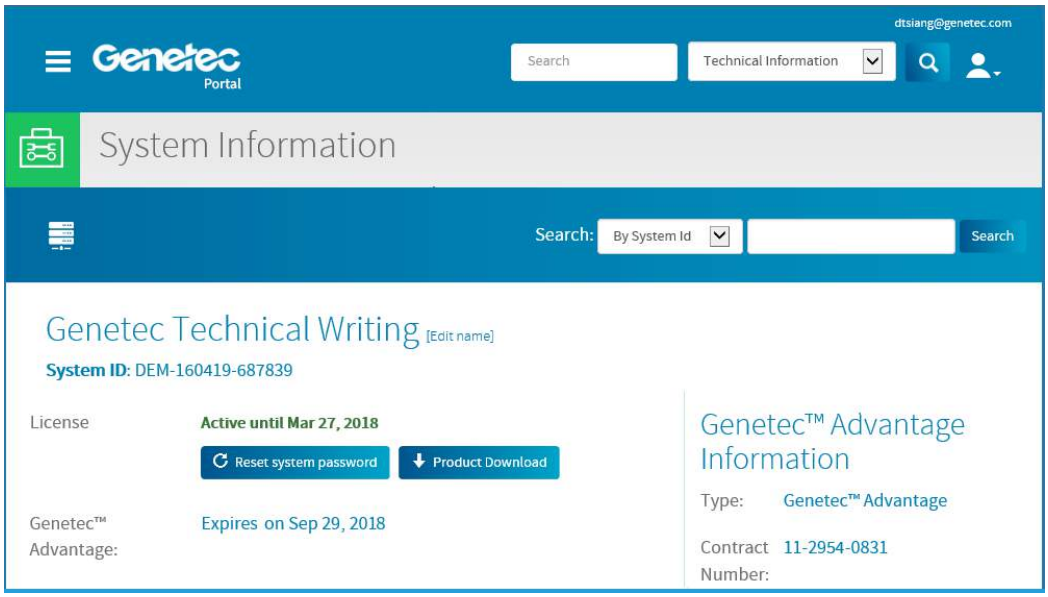
5 De outro computador com acesso à Internet, faça logon no GTAP em: https://gtap.genetec.com.



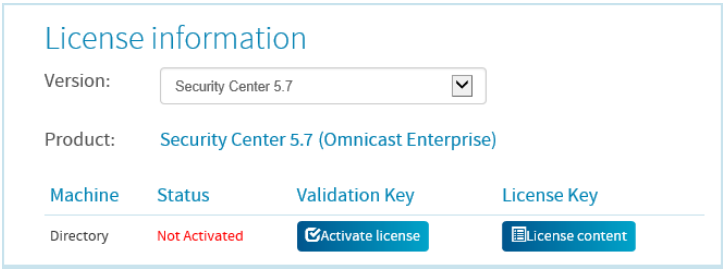
6 Na página de Login do GTAP, faça uma das seguintes opções:

- Digite o ID do sistema e a senha especificada no documento *Informações de Licença do Security Center* e clique em **Login**.
- Digite sua conta de usuário GTAP (seu endereço de e-mail) e senha e clique em **Login**.
  1 Na página *Genetec™ Portal - Portais*, clique em **Página Inicial de Assistência Técnica** > **Ativar novo sistema**.
  2 Na lista suspensa **ID do sistema**, selecione seu sistema e clique em **Enviar**.

O navegador é aberto na página *Informações do Sistema*.



7 Role para baixo até a seção *Informações de licença* e clique em **Ativar licença**.



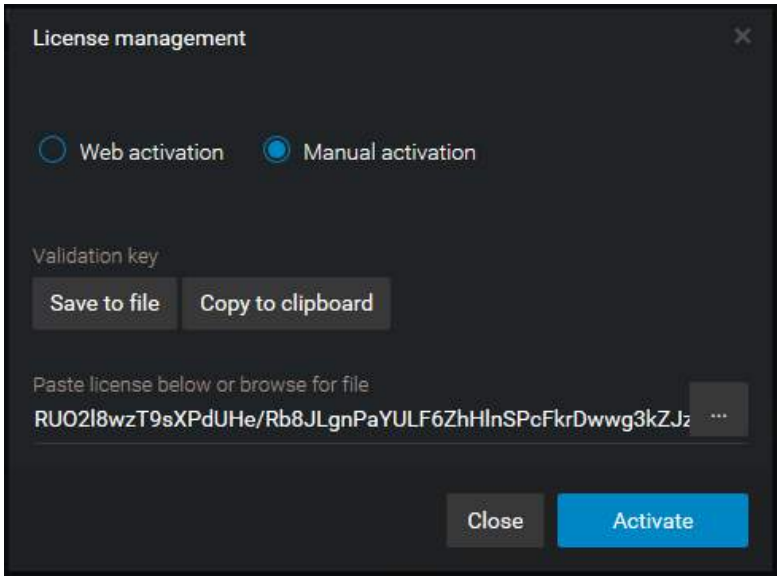
8 Na caixa de diálogo que abre, procure a sua chave de validação (arquivo .vk) e clique em **Enviar**.
A mensagem *Ativação de licença bem-sucedida* é exibida.

9 Clique em **Baixar licença** e salve a chave de licença em um arquivo.
O nome padrão é o ID do sistema seguido de *_Directory_License.lic*.

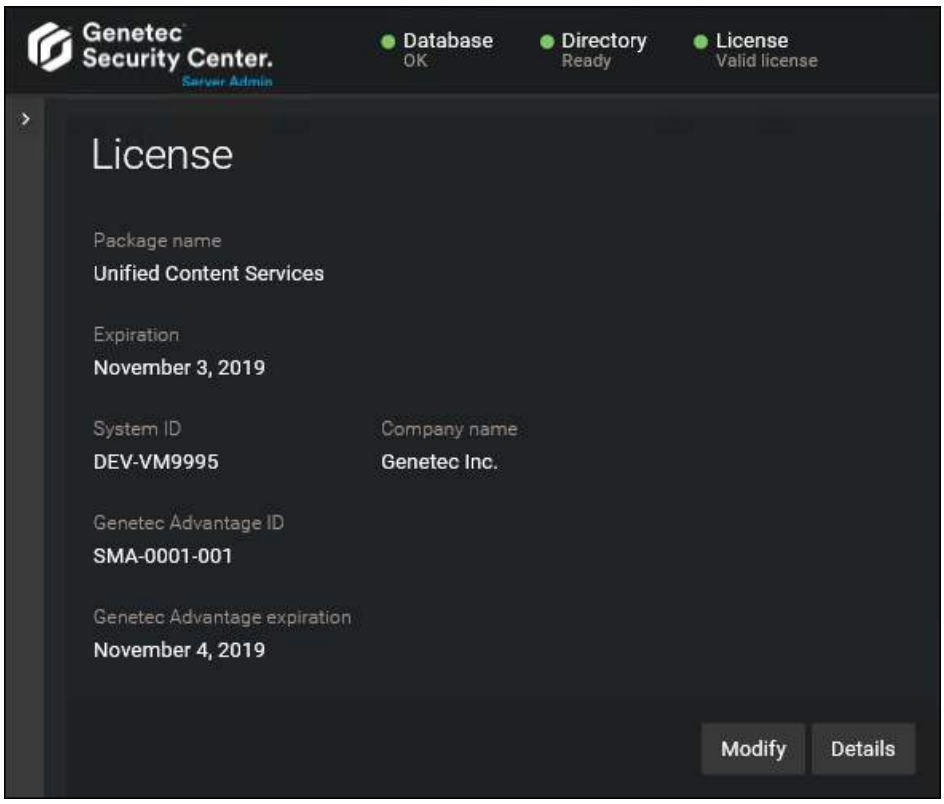
10 Retorne ao Server Admin que está conectado ao seu servidor principal do Security Center.

11 Na caixa de diálogo *Gerenciamento de licenças*, tome uma das seguintes opções:

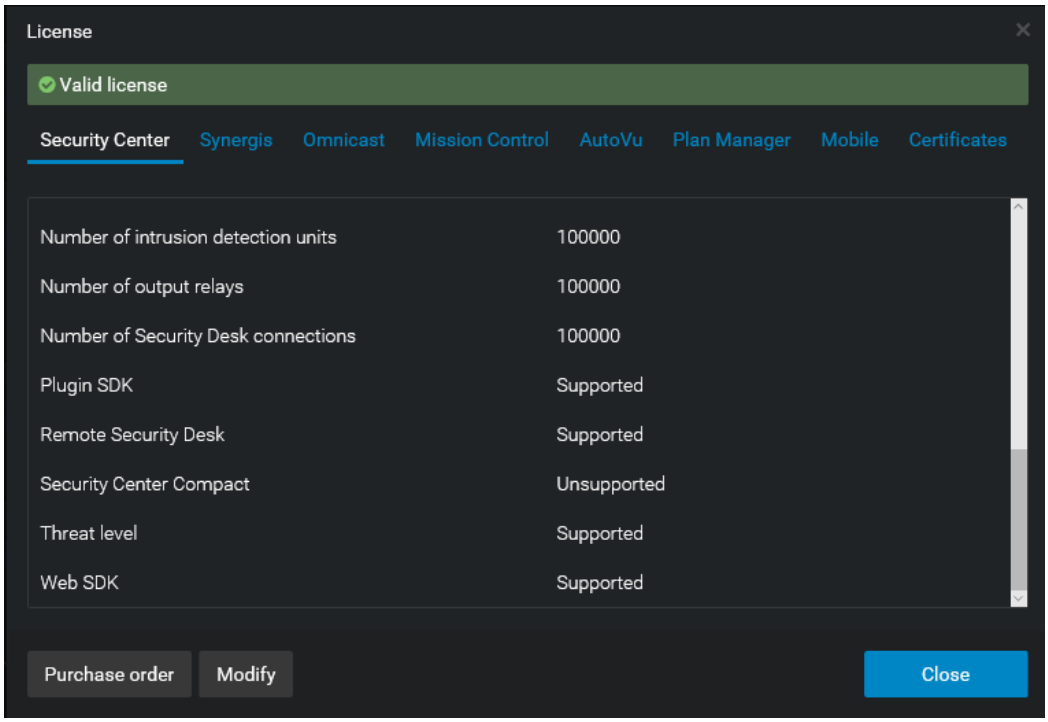
- Cole suas informações de licença a partir do arquivo de chave de licença (abra com um editor de texto).
- Procure a chave de licença (arquivo .lic) e clique em **Abrir**.



12 Clique em **Ativar**.
As informações da licença são exibidas na seção *Licença* da página *Visão Geral* do Server Admin.



13 Clique em **Detalhes** para exibir suas opções de licença em uma caixa de diálogo.



Suas opções de licença estão divididas em várias abas. Para mais informações, consulte o *Security Center Guia do Administrador*.

14 Clique em **Fechar** e, em seguida, feche a janela do navegador.

Reaplicar sua licença do Security Center

Cada vez que sua licença do Security Center é atualizada (novas conexões de câmeras adicionadas, data de vigor prorrogada e assim por diante), você deverá reaplicá-la ao seu servidor principal para que as alterações tenham efeito.

Antes de iniciar

Para reaplicar sua licença, você precisa do seguinte:

- **ID do sistema e senha:** O ID e a senha do Sistema encontram-se no documento *Informações de Licença do Security Center*. O Serviço de Atendimento ao Cliente Genetec™ envia este documento quando o cliente compra o produto.
- **Senha do servidor:** A senha do servidor é usada para fazer logon no Server Admin. A senha do servidor é definida durante a instalação.

O que você deve saber

Se você substituir seu servidor principal por uma nova máquina, você precisará ativar sua licença na nova máquina. Você não precisa reativar sua licença se o seu servidor principal permanecer o mesmo.

IMPORTANTE: Se você tiver uma configuração com vários servidores do Directory, você deverá reativar sua licença a partir do Config Tool.

Para reaplicar sua licença do Security Center:

1 Abra a página da Web do Server Admin executando um dos seguintes procedimentos:

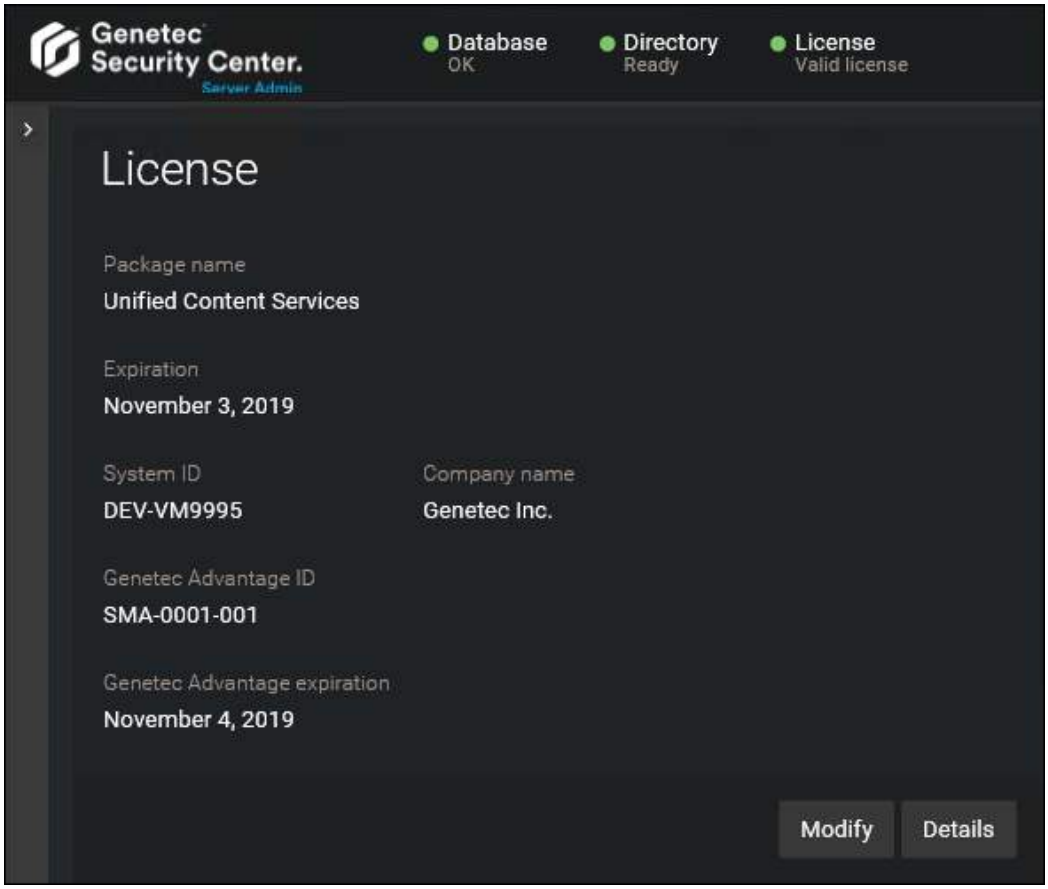
- Na barra de endereços do seu navegador, digite `http://computer:port/Genetec`, onde `computer` é o nome DNS ou o endereço IP do servidor e `port` é a porta do servidor Web especificada durante a instalação do Security Center Server.

  Pode omitir a porta do servidor da Web se está usando o valor padrão (80).
- Se estiver se conectando ao Server Admin a partir de um host local, clique duas vezes em **Genetec™Server Admin** () na pasta *Genetec Security Center* no menu Iniciar do Windows.

2 Digite a senha do servidor que definiu durante a instalação do servidor e clique em **Log on**.

A página *Visão Geral* do Server Admin será exibida.

3 Na seção *Licença*, clique em **Modificar**.



4 Na caixa de diálogo *Gerenciamento de licença*, ative sua licença de uma das seguintes maneiras:

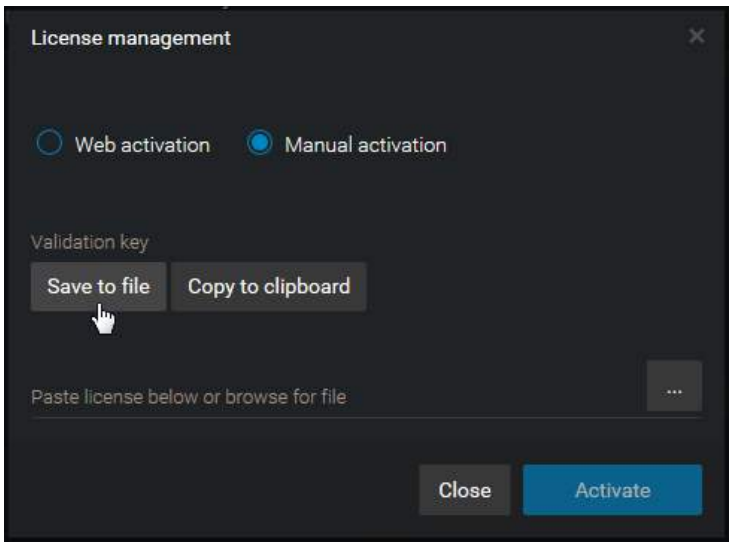
- **Ativação pela Internet:** (Recomendável) Ative a sua licença pela Internet.

  Na caixa de diálogo que aparece, digite seu *ID do sistema* e *Senha* e clique em **Ativar**. O processo estará concluído.

- **Ativação Manual:** Atualize sua licença do Security Center manualmente usando um arquivo de licença e continue com a próxima etapa.

5 Se o seu servidor principal continuar sendo o mesmo computador, vá para a etapa 7.

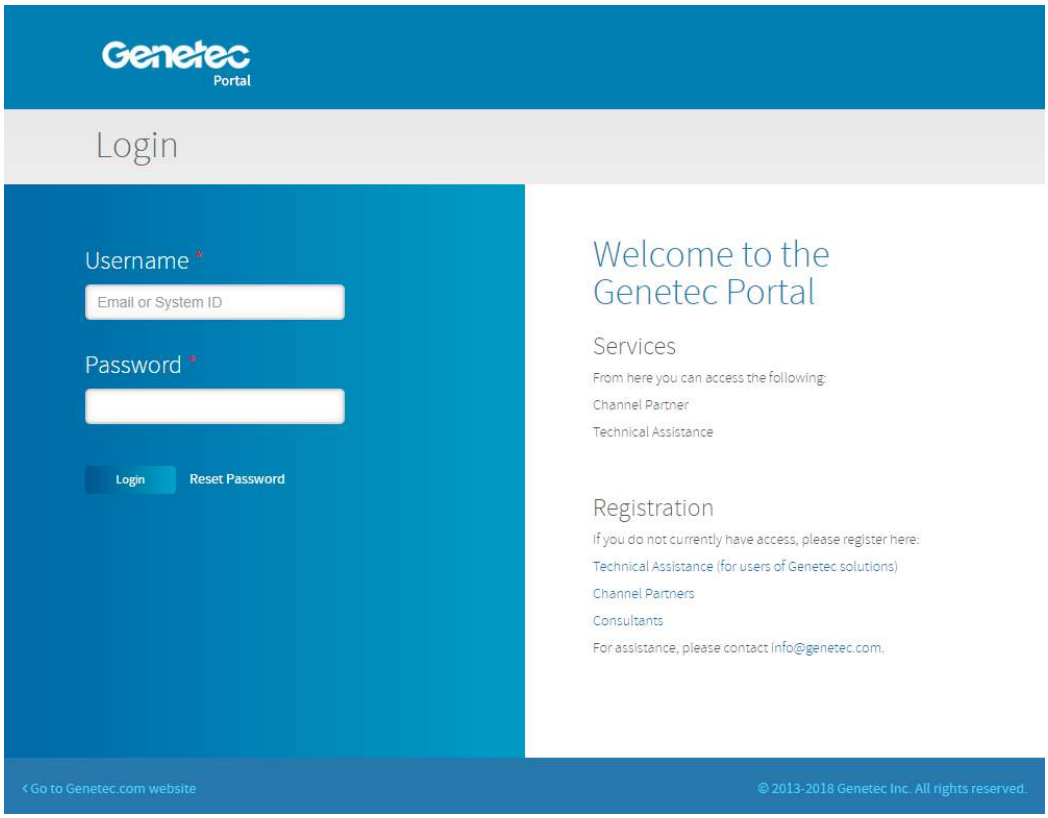
6 Na caixa de diálogo *Gerenciamento de licenças*, clique em **Ativação manual** e, em *Chave de validação*, clique em **Salvar para arquivo**.



A chave de validação é uma sequência de números (em formato de texto hexadecimal) gerada pelo Security Center que identifica o servidor de forma exclusiva. A chave de validação é usada para gerar a chave de licença que desbloqueia o software Security Center. Ela só pode ser aplicada ao servidor previamente identificado pela chave de validação.

Um arquivo de texto chamado *validation.vk* é salvo em sua pasta de *Downloads* padrão. Certifique-se de copiar este arquivo para um local (isso pode ser uma chave USB) que possa acessar de outro computador que tenha acesso à Internet.

7 De outro computador com acesso à Internet, faça logon no GTAP em: https://gtap.genetec.com.

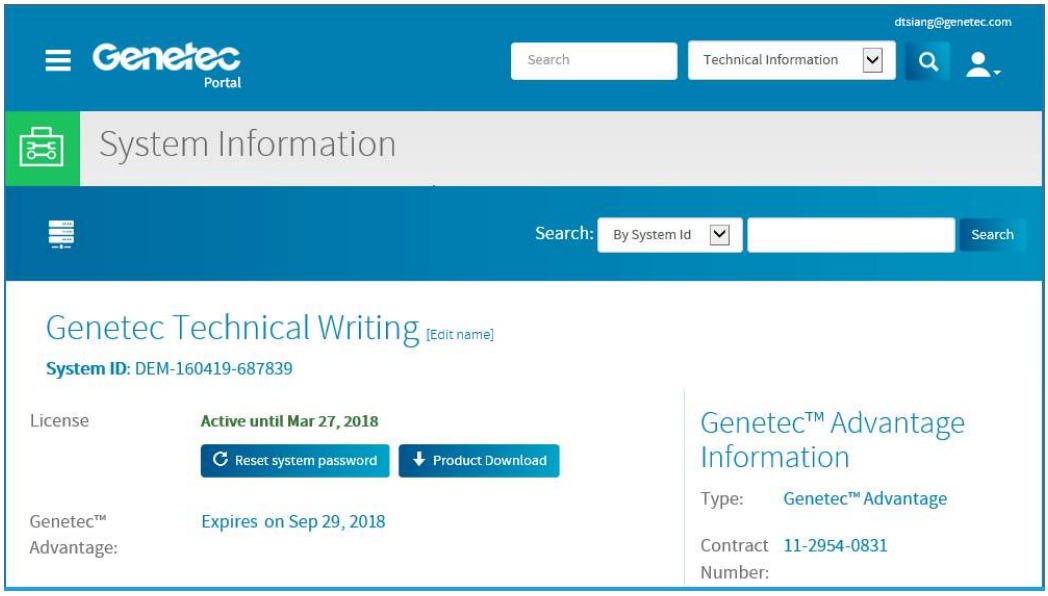


8 Na página de Login do GTAP, faça uma das seguintes opções:

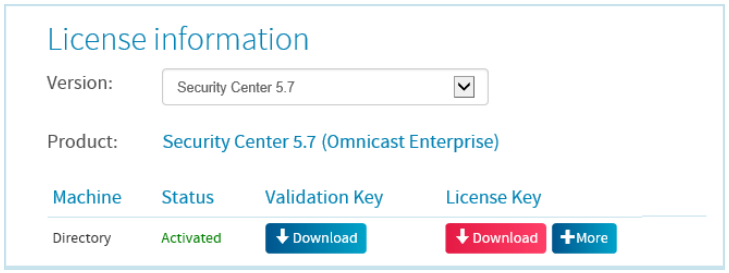
- Digite o ID do sistema e a senha especificada no documento *Informações de Licença do Security Center* e clique em **Login**.

- Digite sua conta de usuário GTAP (seu endereço de e-mail) e senha e clique em **Login**.
  1. Na página *Genetec™ Portal - Portais*, clique em **Página Inicial de Assistência Técnica** > **Ativar novo sistema**.
  2. Na lista suspensa **ID do sistema**, selecione seu sistema e clique em **Enviar**.

O navegador é aberto na página *Informações do Sistema*.



9 Role até a seção *Informações da licença* e faça um dos seguintes:

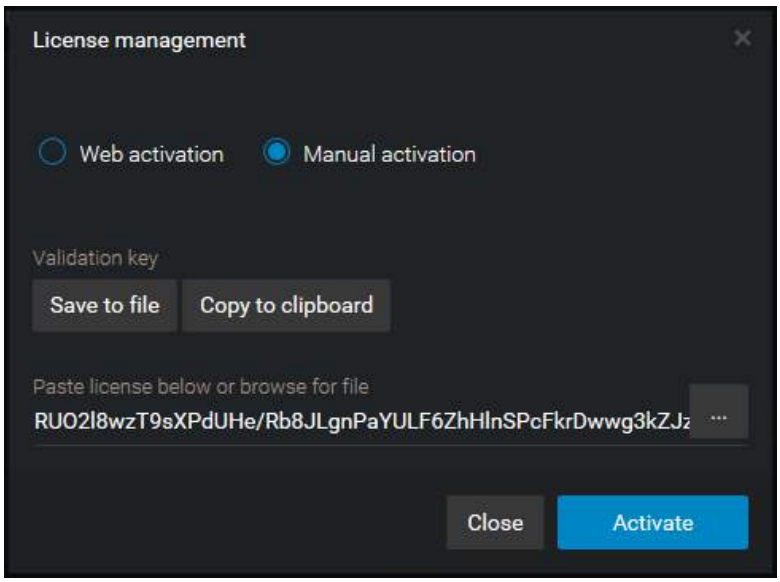


- Abaixo de **Chave de licença**, clique em **Download** e salve a chave de licença em um arquivo.
- Clique em **+Mais** > **Enviar por e-mail** , digite seu endereço de e-mail e clique em **OK** para que o arquivo da chave de licença (.lic file) seja enviado para o seu e-mail.

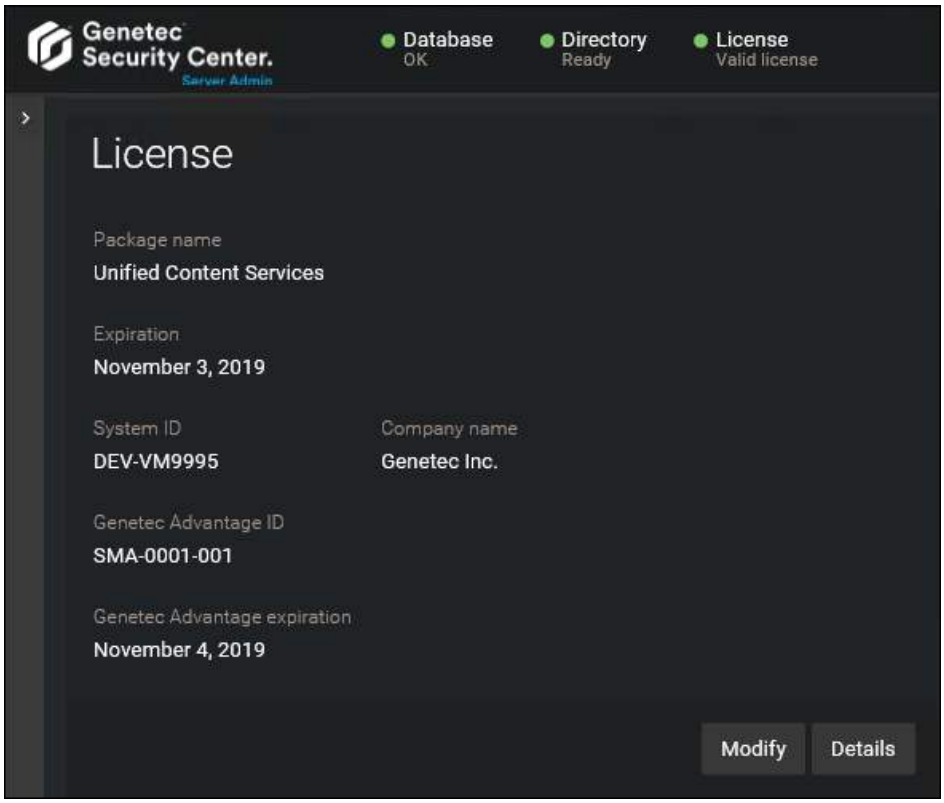
10 Retorne ao Server Admin que está conectado ao seu servidor principal do Security Center.

11 Na caixa de diálogo *Gerenciamento de licenças*, tome uma das seguintes opções:

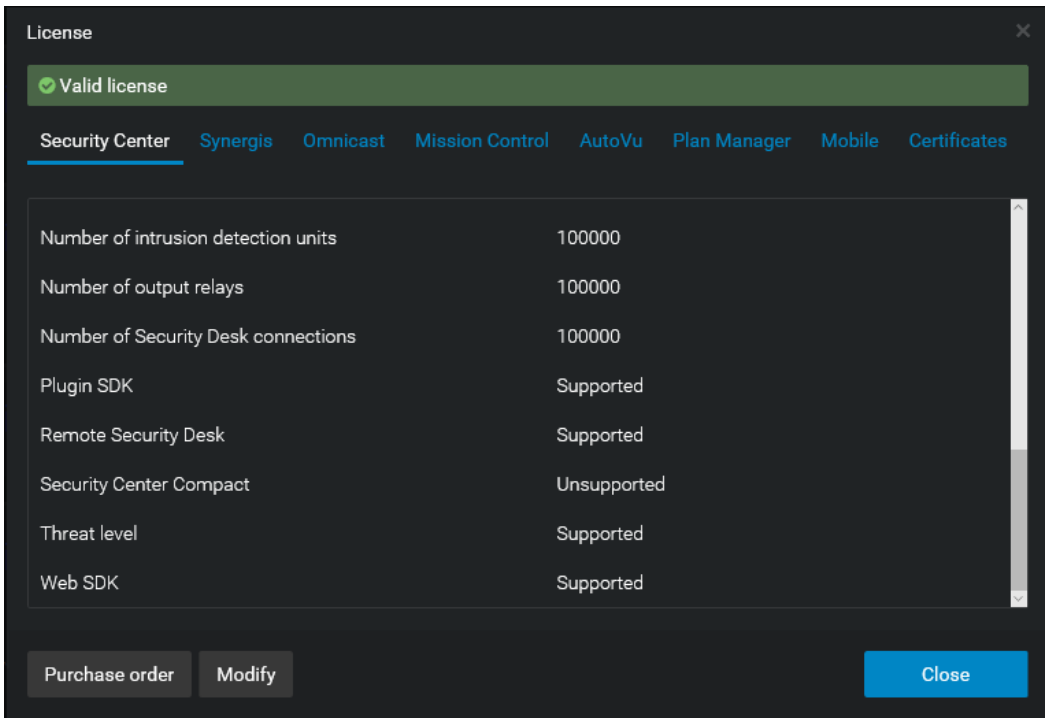
- Cole suas informações de licença a partir do arquivo de chave de licença (abra com um editor de texto).
- Procure a chave de licença (arquivo .lic) e clique em **Abrir**.



12 Clique em **Ativar**.
As informações da licença são exibidas na seção *Licença* da página *Visão Geral* do Server Admin.



13 Clique em **Detalhes** para exibir suas opções de licença em uma caixa de diálogo.



Suas opções de licença estão divididas em várias abas. Para mais informações, consulte o *Security Center Guia do Administrador*.

14 Clique em **Fechar** e, em seguida, feche a janela do navegador.

Substituir o servidor principal

Quando o seu servidor principal deixar de ser adequado, você pode substituí-lo por um novo servidor, ativar sua licença do Security Center no novo servidor e conectar todos os servidores de expansão ao novo servidor.

Antes de iniciar

A substituição do servidor principal implica uma interrupção do serviço de até 3 horas. Quanto maior o sistema, mais tempo demora a fazer backup e restaurar o banco de dados do Directory e a reconectar os servidores de expansão. Regra geral, você pode estimar meia hora para backup e restauro e uma hora extra por cada 25 servidores de expansão que precise reconectar ao novo servidor. Agende sua janela de manutenção para um momento que seja o menos prejudicial para as suas operações. Você pode prosseguir com este procedimento até ao ponto em que seja solicitado a esperar pela janela de manutenção agendada.

O que você deve saber

Este cenário de migração implica os seguintes pressupostos:

- Você tem um único sistema de Directory (nenhuma configuração de failover de Directory).
- O banco de dados de Directory reside no servidor principal (nenhum acesso a bancos de dados remotos necessário).
- O SQL Server em execução no novo servidor é uma versão igual ou mais recente do SQL Server em execução no antigo servidor.

  Isto é para garantir que você pode restaurar o antigo banco de dados na nova máquina. Você sempre pode fazer backup de um banco de dados numa versão mais antiga do SQL Server e restaurá-lo numa versão mais recente do SQL Server, mas o contrário não é necessariamente verdade.
- O antigo servidor principal ainda está em execução.
- Os servidores principais antigo e novo estão no mesmo domínio de rede.

NOTA: Essa operação reinicia o serviço Genetec™ Server, o que desativa temporariamente todas as funções hospedadas no seu servidor. Recomendamos reservar uma janela de manutenção de 4 horas para esta operação.

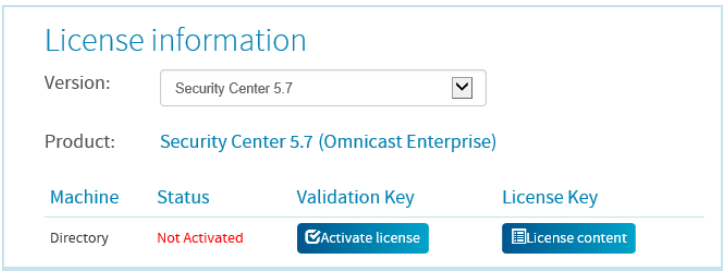
Para substituir o servidor principal:

1 Instale o Security Center na nova máquina usando a configuração *Servidor principal*, mas não ative a licença.

Para obter mais informações, consulte o *Guia de Instalação e Atualização do Security Center*.

2 Contacte os Serviços de Atenção ao Cliente da Genetec™ para redefinir sua licença do Security Center e poder ativá-la no novo servidor.

No GTAP (https://gtap.genetec.com), verifique se o botão **Ativar licença** está habilitado para o seu sistema.



3 Ative a licença do Security Center no novo servidor.

Para obter mais informações, consulte o *Guia de Instalação e Atualização do Security Center*.

NOTA: O novo servidor ainda não faz parte do seu sistema. É um sistema independente.

4 Se você tiver outras funções para além do Directory que sejam executadas no servidor principal e precisem de seu próprio banco de dados, como a função Health Monitor, faça backup dos respectivos bancos de dados.

5 Espere até que a manutenção agendada seja iniciada antes de prosseguir com a etapa seguinte.

A partir da próxima etapa, o seu sistema estará offline até ao final do processo.

6 Faça backup do banco de dados do Directory.

a) Abra o Server Admin e se conecte ao antigo servidor principal.

b) Na parte superior da janela do navegador, clique em **Directory** > **Parar**.

Isto garante que o banco de dados não esteja sendo acessado enquanto faz backup do mesmo.

c) Clique em **Banco de dados** > **Propriedades (** **)** , defina a **Pasta de destino** do backup do banco de dados e clique em **OK**.

Certifique-se de que a pasta de backup possa ser acessada do novo servidor.

d) Clique em **Backup/Restauração (** **)** > **Fazer backup agora** .

e) Clique em **Fechar**.

7 Restaure o banco de dados de Directory (arquivo .bak) no novo servidor principal.

a) Abra o Server Admin e se conecte ao novo servidor principal.

b) Clique em **Banco de dados** > **Backup/Restauração (** **)** , selecione o arquivo de backup que deseja restaurar e clique em **Restaurar agora**.

c) Clique em **Fechar**.

8 Conecte todos os servidores de expansão ao novo servidor principal.

9 Fazer um dos seguintes:

- Converta o antigo servidor principal em um servidor de expansão.
- Descomissione o antigo servidor principal.

  Recomendamos fazer isso em duas etapas. Por agora, desabilite o serviço Genetec™ Server no antigo servidor para evitar que o serviço seja iniciado por acidente. Quando o novo servidor estiver totalmente operacional, desinstale o Security Center no antigo servidor.

10 Abra o Config Tool e conecte-o ao novo servidor principal usando suas antigas credenciais de *Admin*.

11 Abra a tarefa *Exibição de rede* e confirme que todos os servidores de expansão estejam online ( ).

Você também deverá ver uma cópia offline ( ) de cada servidor. Não as exclua já.

12 Abra a tarefa *Sistema* e clique na visualização **Funções**.

13 Recrie o banco de dados da função Media Router.

a) Selecione Media Router na lista de funções e clique em **Recursos**.

b) Clique em **Criar um banco de dados** ( ).

c) Na janela que abrir, clique em **Sobrescrever banco de dados existente** > **OK**.

14 Para as restantes funções na lista que estejam no estado de aviso (amarelo) ou problema (vermelho), faça o seguinte:

a) Selecione a função e clique em **Recursos**.

b) Na lista **Servidores**, se o antigo servidor principal estiver listado, substitua-o pelo novo.

c) Se a função tinha um banco de dados hospedado no servidor antigo, crie um banco de dados no novo servidor e restaure o backup.

15 Abra a tarefa *Exibição de rede* e exclua as cópias offline dos seus servidores ( ).

O seu sistema já está novamente online. Se você optar por descomissionar o antigo servidor principal, desinstale o Security Center nele.

Após terminar

Informe seus usuários do nome DNS e endereço IP do novo servidor principal.

Tópicos relacionados

Converter um servidor de expansão em servidor principal: na página 111
Converter o servidor principal em um servidor de expansão na página 110

Sobre funções

Uma função é um componente de software que realiza um trabalho específico no Security Center. Para executar uma função, você deve atribuir um ou mais servidores para hospedá-la. Você pode atribuir funções para arquivamento de vídeo, para controlar um grupo de unidades, para sincronizar usuários do Security Center com seu serviço de diretório corporativo e assim por diante.

No Security Center, as entidades de função podem ser definidas como segue:

- **Tipo de função:** Determina o conjunto de funções específicas que devem ser realizadas pela função, como gerenciar unidades de vídeo e arquivos de vídeo associados.
- **Configurações de função:** Defina o conjunto específico de parâmetros dentro dos quais a função deve funcionar, como um período de retenção para os dados coletados, ou qual banco de dados o sistema deve usar.
- **Servidores:** Os *servidores* que devem estar hospedando (executando) esta função. Você pode atribuir uma ou mais funções ao mesmo servidor ou atribuir múltiplos servidores à mesma função para proporcionar balanceamento de carga e failover.

Após uma função estar configurada, você poderá movê-la para qualquer servidor em seu sistema Security Center (por exemplo, um com um processador mais rápido ou com mais espaço em disco) sem precisar instalar qualquer software adicional naquele servidor. Mover uma função para outro servidor pode causar uma breve pausa nas operações da função. Adicionalmente, algumas funções podem gerar subprocessos (chamados *agentes*) e executá-los simultaneamente em vários servidores para maior escalabilidade.

Mover funções para outros servidores

Você pode mover uma função para outro servidor sem instalar nenhum software adicional, por exemplo, se o servidor no qual a função está instalada for lento ou tiver espaço em disco limitado.

Antes de iniciar

Certifique-se de que você tenha outro servidor configurado e pronto para aceitar uma nova função.

O que você deve saber

Mover uma função para outro servidor pode causar uma breve pausa nas operações da função.

NOTA: Esse procedimento não se aplica a funções Archiver. Para mover funções Archiver, consulte Mover a função Archiver para outro servidor na página 444.

Para mover uma função para outro servidor:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.
2 Selecione a função que deseja modificar e clique na aba **Recursos**.
3 Se a função exigir um banco de dados, faça um dos seguintes:
- Se o banco de dados estiver em um terceiro computador, você não terá nada a alterar.
- Se o banco de dados estiver vazio, você poderá criá-lo em qualquer local que quiser.
- Se o banco de dados contiver dados e estiver residindo no servidor atual, mova o banco de dados para o novo servidor ou para um terceiro computador.

4 Na lista **Servidores**, clique em **Adicionar um item** ().

Uma caixa de diálogo aparecerá com todos os servidores disponíveis em seu sistema.

5 Selecione o servidor substituto e clique em **Adicionar**.
6 Selecione o servidor atual na lista **Servidores** e clique em **Excluir** ().
7 Clique em **Aplicar**.

Tópicos relacionados

Adicionando Servidores de Expansão na página 109

Desativar e ativar funções

Para fins de manutenção ou solução de problemas, você pode desativar uma função sem afetar nenhuma de suas configurações e então reativá-la posteriormente

O que você deve saber

Se você estiver tendo problemas com seu sistema, às vezes é útil reiniciar uma função. As funções também são desativadas para que suas propriedades possam ser modificadas. .

Você deve ser um administrador do sistema para desativar ou ativar uma função.

Para desativar uma função:

1 Na página inicial, abra a tarefa **Status do sistema** .

2 Na lista suspensa **Monitor**, selecione **Funções**.

As funções que são parte do seu sistema são listados no painel de relatório.

3 Selecione a função que você deseja desativar e clique em **Desativar função** ( ).

A função fica vermelha (inativa) no painel de relatório.

4 Para reativar a função, selecione a função e clique em **Ativar função** ( ).

Sobre a função Directory

A função Directory identifica um sistema Security Center. Ela gerencia as configurações de todas as entidades e de todo o sistema no

Como a função Directory funciona

O seu sistema pode ter apenas uma instância dessa função. O servidor que hospeda a função do Diretório é chamado de *servidor principal* e deve ser configurado primeiro. Todos os outros servidores adicionados ao Security Center são chamados *servidores de expansão* e devem ser conectados ao servidor principal para fazerem parte do mesmo sistema.

As funções principais da função Directory são:

- Autenticação de conexão do aplicativo cliente
- Fiscalização da licença do software
- Gerenciamento de configuração central
- Gerenciamento de eventos e roteamento
- Gerenciamento de trilhas de auditoria e trilhas de atividade
- Gerenciamento de alarmes e roteamento
- Gestão de incidente
- Execução de tarefa agendada
- Execução de macros

Configuração da função Directory

Como a função Directory é responsável pela autenticação de todas as conexões de clientes, ela não pode ser configurada no aplicativo cliente do Config Tool. Para configurar a função Directory, você deve fazer login no *Server Admin* a partir de um navegador da Web.

Usando o Server Admin, você pode realizar as seguintes tarefas administrativas:

- Iniciar/interromper a função Directory
- Gerenciar o banco de dados do Directory e alterar os períodos de retenção de dados
- Visualizar e modificar sua licença do Security Center
- Visualizar e modificar a senha do servidor principal e as portas de comunicação
- Converter o servidor principal em um servidor de expansão

Em uma configuração com vários servidores do Directory, o *failover* e o *balanceamento de carga* do Directory são gerenciados pela função *Directory Manager*.

Tópicos relacionados

Failover e balanceamento de carga de Directory na página 167

Sobre Web-based SDK

Esta função expõe os métodos SDK do Security Center e os objetos como serviços Web para dar suporte ao desenvolvimento da plataforma cruzada.

Permite que desenvolvedores em plataformas diferentes do Windows (por exemplo, Linux) escrevam programas personalizados que podem interagir com o Security Center.

Esta função existe principalmente para clientes que precisam de desenvolvimento personalizado. Os Genetec™ Professional Services pode ajudar você a desenvolver a solução personalizada de que você precisa. Para descobrir mais, entre em contato com seu representante de vendas ou ligue para um de nossos escritórios regionais ao redor do mundo. Para entrar em contato conosco, visite nosso site em www.genetec.com.

7

Bancos de dados e redes

Esta seção inclui os seguintes tópicos:

- "Bancos de dados" na página 138
- "Mover bancos de dados para outros computadores" na página 139
- "Conectar funções a servidores de bancos de dados remotos" na página 140
- "Garantindo as permissões do SQL Server" na página 142
- "Restringir a memória alocada a servidores de bancos de dados" na página 143
- "Criar bancos de dados" na página 144
- "Excluir bancos de dados" na página 145
- "Atualizar o banco de dados do Security Center Directory" na página 146
- "Compactar bancos de dados do Security Center após uma atualização" na página 148
- "Visualizar informações do banco de dados" na página 149
- "Receber notificações quando os bancos de dados estão quase cheios" na página 150
- "Fazer backup de bancos de dados" na página 151
- "Restaurar bancos de dados" na página 153
- "Sobre redes" na página 154
- "Sobre a exibição de rede" na página 156
- "Adicionar redes" na página 157
- "Personalizando opções de rede" na página 159

Bancos de dados

Um banco de dados é uma coleção de dados que é organizada para que seu conteúdo possa ser facilmente acessado, gerenciado e atualizado.

Como a hospedagem de banco de dados funciona no Security Center

Por padrão, o banco de dados de uma função é hospedado no mesmo servidor que hospeda a função. Isso é mostrado na aba **Recursos** da função pelo valor `(local)\SQLEXPRESS` no campo **Servidor de banco de dados**, onde "(local)" é o servidor em que a função está em execução.

Se você planeja alterar a hospedagem do servidor ou adicionar servidores secundários para failover, o banco de dados deverá estar hospedado em um computador diferente.

Adicionalmente, o computador que hospeda o servidor de banco de dados não precisa ser um servidor do Security Center (o que significa um computador no qual o serviço do *Genetec Server* esteja instalado), a menos que você esteja configurando o failover do banco de dados do Directory usando o método de backup e restauração.

Como o SQL Server usa a memória

Se você estiver usando uma edição licenciada do SQL Server (como SQL Server Standard, SQL Server Business Intelligence ou SQL Server Enterprise), tenha em mente que todos os bancos de dados são gerenciados pelo Microsoft SQL Server no Security Center. Como padrão o SQL Server é configurado para usar tanta memória quanto esteja disponível no sistema. Isso pode causar problemas de memória se você estiver hospedando o SQL Server e muitas funções no mesmo servidor, especialmente em uma máquina virtual com poucos recursos de memória. Se você estiver ficando com pouca memória em um de seus servidores, você pode resolver o problema configurando um limite máximo na quantidade de memória que o SQL Server tem permissão para usar.

Tópicos relacionados

Mover bancos de dados para outros computadores na página 139
Conectar funções a servidores de bancos de dados remotos na página 140
Restringir a memória alocada a servidores de bancos de dados na página 143

Mover bancos de dados para outros computadores

Se você quiser alterar o servidor que hospeda uma função ou adicionar servidores secundários para failover, você deverá hospedar o banco de dados da função em um computador diferente.

O que você deve saber

Esse procedimento não é necessário para a função do Archiver. Para funções do Archiver, é recomendável hospedar o banco de dados localmente.

Para mover um banco de dados para outro computador:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.

2 Selecione a função cujo banco de dados você deseja mover e clique em **Manutenção** > **Desativar função** ( ) na barra de ferramenta na parte inferior do espaço de trabalho.

3 Clique na aba **Recursos**.

4 Faça um backup do banco de dados atual.

DICA: Como a pasta de backup é relativa ao servidor atual, pode ser uma boa ideia selecionar um local de rede que possa ser alcançado por qualquer servidor em seu sistema.

5 (Opcional) Exclua o banco de dados atual.

6 Crie o banco de dados na nova máquina.

7 Restaure o conteúdo que você possa ter em backup no novo banco de dados.

8 Clique em **Aplicar**.

9 Na barra de ferramentas na parte inferior da área de trabalho, clique em **Ativar** ( ).

Conectar funções a servidores de bancos de dados remotos

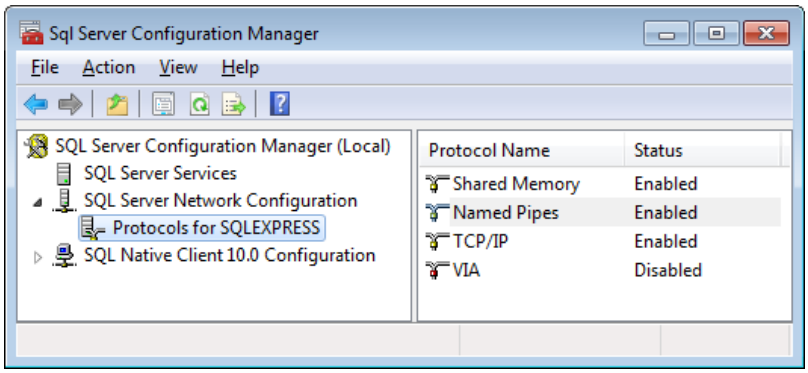
Se o banco de dados de uma função estiver hospedado em um computador diferente daquele da função, você deverá configurar o servidor de banco de dados remoto (SQL Server) para aceitar solicitações de conexão da função.

Antes de iniciar

No computador que hospeda o SQL Server, abra as portas TCP 1433 e 1434 do Firewall do Windows.

Para conectar uma função a um servidor de bancos de dados remoto:

1 Permita a conexão remota na sua instância do SQL Server.
   a) No servidor que hospeda o banco de dados, abra o *Microsoft SQL Server Management Studio* e conecte ao *servidor de banco de dados* usado pelo Security Center.
   b) Na janela do **Microsoft SQL Server Management Studio**, clique com o botão direito no nome do servidor de banco de dados ( ), no **Pesquisador de Objetos**, e selecione **Propriedades**.
   c) Na janela **Propriedades do Servidor**, selecione a página **Conexões**.
   d) Na seção **Conexões remotas ao servidor**, selecione a opção **Permitir conexões remotas a este servidor**.
   e) Clique em **OK** e feche o *Microsoft SQL Server Management Studio*.
2 Ative os protocolos **Pipes nomeados** e **TCP/IP** em sua instância do SQL Server.
   a) No servidor que hospeda o banco de dados, abra o *SQL Server Configuration Manager*.
   b) Expanda a seção **SQL Server Network Configuration** e selecione os protocolos para sua instância de servidor de banco de dados (por exemplo, **Protocolos para SQLEXPRESS**).
   c) Clique com o botão direito nos protocolos **Pipes nomeados** e **TCP/IP** e coloque seus status em **Habilitado**.



   d) Feche o *SQL Server Configuration Manager*.
3 Certifique-se de que sua instância do SQL Server seja visível de outros computadores em sua rede.
   a) No servidor que hospeda o bancos de dados, abra o *Microsoft Management Console Services* (`services.msc`).
   b) Inicie o serviço chamado **SQL Server Browser**.
   c) Clique com o botão direito no serviço SQL Server Broswer e clique em **Propriedades**.
   d) Na aba **Geral**, na lista suspensa **Tipo de inicialização**, selecione **Automática**.

      A instância do SQL Server fica disponível na lista suspensa **Servidor de banco de dados** da aba **Recursos** de qualquer função no Config Tool.

4 Reinicie sua instância do SQL Server para ativar as configurações que você alterou.
   a) No servidor que hospeda o bancos de dados, abra o *Microsoft Management Console Services* (`services.msc`).

b) Clique com o botão direito no serviço da instância de SQL Server (por exemplo, `SQL Server (SQLEXPRESS)`) e clique em **Reiniciar**.

5 Em cada servidor que hospede suas funções do Security Center, altere o usuário de logon do serviço **Genetec Server** para uma conta de administrador do Windows que também tenha as permissões para acessar a instância do SQL Server que você acabou de modificar.

A conta de administrador do Windows normalmente é uma conta de domínio usada para se conectar a todos os servidores.

a) No servidor que hospeda a função, abra o *Microsoft Management Console Services* (`services.msc`).
b) Clique com o botão direito no serviço **Genetec Server** e clique em **Propriedades**.
c) Na aba **Logon**, selecione a opção **Esta conta** e digite um **Nome de conta** e uma **Senha** de administrador.
d) Clique em **Aplicar** > **OK**.
e) Repita essas etapas em cada servidor que esteja hospedando uma função do Security Center que se conectará ao servidor de banco de dados remoto.

6 Selecione a função na aba **Recursos** > **Config Tool** e modifique o caminho do banco de dados para apontar para o banco de dados remoto.

Garantindo as permissões do SQL Server

Para que a função de Directory Security Center seja executada, os usuários de serviço que não são administradores do Windows (nome de login SYSADMIN) devem receber a permissão de Servidor SQL *Visualizar estado do servidor*.

O que você deve saber

A *função mínima de nível de servidor* SQL suportada pelo Security Center é *dbcreator*, e a *função de nível mínimo de banco de dados* do SQL é *db_owner*. Portanto, deve assegurar-se de que os membros da função de servidor *dbcreator* e os membros da função de banco de dados *db_owner* tenham a permissão *Visualização do estado do servidor* concedida.

Para mais informações sobre funções de Servidor SQL e seus recursos, consulte a documentação da Microsoft.

NOTA: O procedimento a seguir é para o SQL Server 2014 Express. Se está usando uma versão diferente do SQL Server, consulte a documentação da Microsoft para obter informações sobre como conceder permissões.

Para garantir as permissões do SQL Server:

- No SQL Server Management Studio, siga um destes procedimentos:
  - Execute a seguinte consulta: `CONCEDER VISUALIZAR ESTADO DO SERVIDOR PARA [nome de logon]`.
  - Modifique manualmente as permissões de utilizador da seguinte forma:
    1. Clique com o botão direito do mouse na instância apropriada do SQL Server e selecione **Propriedades**.
    2. Clique na página *Permissões*.
    3. Em **Logins ou funções**, selecione o usuário ou função que deseja modificar.
    4. Na seção **Permissões**, clique na aba **Explícitas** e selecione a caixa de seleção **Conceder** ao lado da permissão de **Visualização do estado do servidor**.
    5. Clique em **OK**.

Após terminar

Para usuários que recebem a permissão localmente no servidor do Security Center, deve adicioná-los como usuários no SQL Server.

Restringir a memória alocada a servidores de bancos de dados

O servidor de banco de dados (SQL Server) é configurado para usar tanta memória quanto esteja disponível no sistema. Se você tiver passando por problemas de memória insuficiente, você pode resolver o problema configurando um limite máximo na quantidade de memória que o SQL Server tem permissão para usar.

Para restringir a memória usada pelo SQL Server:

1. No servidor que hospeda o banco de dados, abra o *Microsoft SQL Server Management Studio*.
2. Na janela do **Microsoft SQL Server Management Studio**, clique com o botão direito no nome do servidor de banco de dados (), no **Pesquisador de Objetos**, e selecione **Propriedades**.
3. Na janela **Propriedades do Servidor**, selecione a página **Memória**.
4. No campo **Memória máxima do servidor (em MB)**, digite a memória máxima que o SQL Server tem permissão para usar.

   A Microsoft recomenda as seguintes diretrizes:

   - RAM = 2 GB, Máximo de memória do servidor = 1000 MB
   - RAM = 4 GB, Máximo de memória do servidor = 2200 MB
   - RAM = 6 GB, Máximo de memória do servidor = 3800 MB
   - RAM = 8 GB, Máximo de memória do servidor = 5400 MB
   - RAM = 12 GB, Máximo de memória do servidor = 8000 MB
   - RAM = 16 GB, Máximo de memória do servidor = 13500 MB
   - RAM = 24 GB, Máximo de memória do servidor = 21500 MB

5. Clique em **OK** e feche o *Microsoft SQL Server Management Studio*.

O serviço do SQL Server ajusta automaticamente sua ocupação de memória.

Criar bancos de dados

Sob certas circunstâncias, você pode precisar criar um novo banco de dados, sobrescrever o banco de dados padrão atribuído a uma função ou atribuir um banco de dados diferente que esteja preparado por seu Departamento de TI se você planejar usar um servidor de banco de dados dedicado.

Antes de iniciar

Se você planejar sobrescrever o banco de dados existente com o novo, você deverá fazer backup do banco de dados existente.

O que você deve saber

Todos os bancos de dados de funções são criados no Config Tool, exceto o banco de dados do Directory, que deve ser criado a partir da página Server Admin - Servidor Principal. Os procedimentos são muito semelhantes em ambos os casos. Assim, apenas se descreve a criação a partir de Config Tool.

Para criar um banco de dados:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.

2 Selecione uma função e clique na aba **Recursos**.

3 Na lista suspensa **Servidor de banco de dados**, digite ou selecione o nome do servidor de banco de dados.

O valor `(local)\SQLEXPRESS` corresponde ao *Microsoft SQL Server 2014 Express Edition* que foi instalado por padrão com o *Genetec™ Security Center*. Para especificar um servidor de banco de dados em um servidor diferente daquele que hospeda a função, digite o nome desse servidor remoto.

4 Na lista suspensa **Banco de dados**, digite ou selecione o nome do banco de dados.

O mesmo servidor de banco de dados pode gerenciar várias instâncias de bancos de dados.

5 Clique em **Criar um banco de dados**.

6 Especifique as opções de criação do banco de dados.

CUIDADO: Se você selecionar a opção **Sobrescrever banco de dados existente**, todo o conteúdo atual do banco de dados selecionado será perdido.

7 Clique em **OK**.

A criação do banco de dados será iniciada. Uma janela é aberta mostrando o progresso desta ação. Você pode fechar esta janela e revisar o histórico de todas as ações do banco de dados clicando em **Ações do banco de dados** na bandeja de notificação.

8 Aguarde até que você veja o **Status do banco de dados** indicar **Conectado**.

Tópicos relacionados

Fazer backup de bancos de dados na página 151
Receber notificações quando os bancos de dados estão quase cheios na página 150

Excluir bancos de dados

Para liberar espaço em disco, você pode excluir bancos de dados que não estejam mais em uso.

O que você deve saber

Todos os bancos de dados de funções são excluídos no Config Tool, exceto o banco de dados do Directory, que deve ser excluído a partir da página Server Admin - Servidor Principal. Os procedimentos são muito semelhantes em ambos os casos. Assim, somente a exclusão a partir do Config Tool é descrita aqui.

Para excluir um banco de dados:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.

2 Selecione uma função e clique na aba **Recursos**.

3 A partir da lista suspensa **Banco de dados** na aba **Recursos** de uma função, selecione o banco de dados que você deseja excluir.

NOTA: Ele não precisa ser o seu banco de dados atual.

4 Clique em **Excluir o banco de dados** ( ).

CUIDADO: Uma caixa de diálogo de confirmação aparecerá. Se você continuar, o banco de dados será excluído permanentemente.

5 Clique em **Excluir** na caixa de diálogo de confirmação.

A exclusão do banco de dados será iniciada. Uma janela aparecerá mostrando o progresso desta ação. Você pode fechar esta janela e revisar posteriormente o histórico de todas as ações do banco de dados clicando em **Ações do banco de dados** na bandeja de notificação.

6 Crie um novo banco de dados para a função.

Após terminar

Conecte a função a um banco de dados existente ou crie um novo banco de dados.

Tópicos relacionados

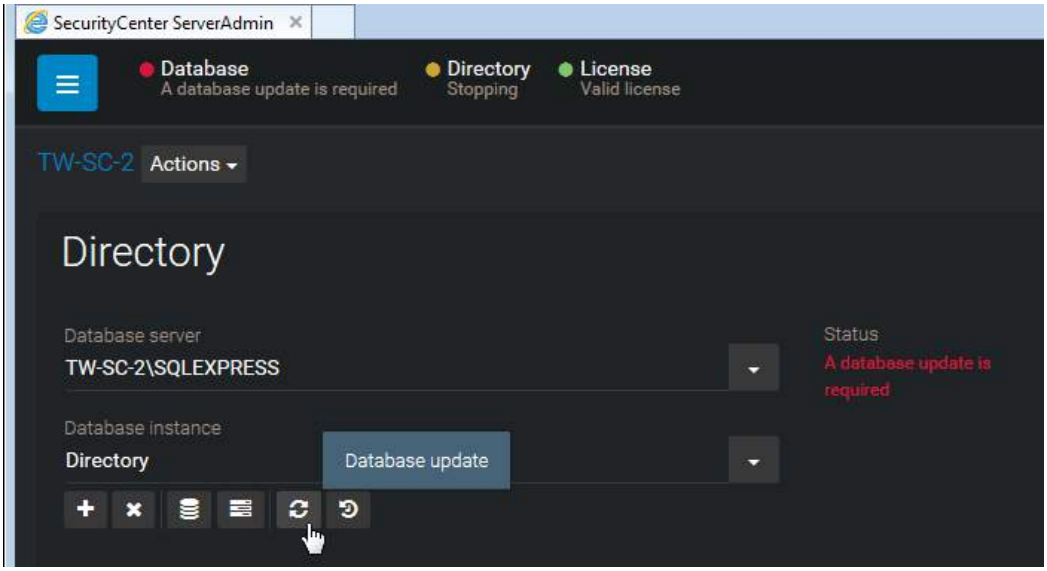
Criar bancos de dados na página 144

Atualizar o banco de dados do Security Center Directory

O Instalador do Security Center 5.7 atualiza o banco de dados do Directory como parte da atualização do servidor principal. Você só precisa atualizar o banco de dados do Directory manualmente se restaurou uma versão mais antiga do banco de dados.

O que você deve saber

Após restaurar uma versão mais antiga do banco de dados do Directory, o Server Admin notifica você de que é necessária uma atualização do banco de dados. *Para obter informações sobre como restaurar bancos de dados, consulte o Security CenterGuia do Administrador do Security Center.*



Para atualizar o banco de dados do Directory:

1 Fazer um dos seguintes:

- Clique no **Banco de dados** com o LED pulsante em vermelho.
- Clique em **Atualização do banco de dados** ( ) na seção *Directory*.

A atualização do banco de dados do Directory é iniciada e o status do servidor de banco de dados é exibido como **Atualizando**.

2 Enquanto o banco de dados estiver sendo atualizado, clique em **Mostrar progresso** ( ) para visualizar o andamento da atualização.

Quando a atualização estiver concluída, o **Status** mostra **OK**.

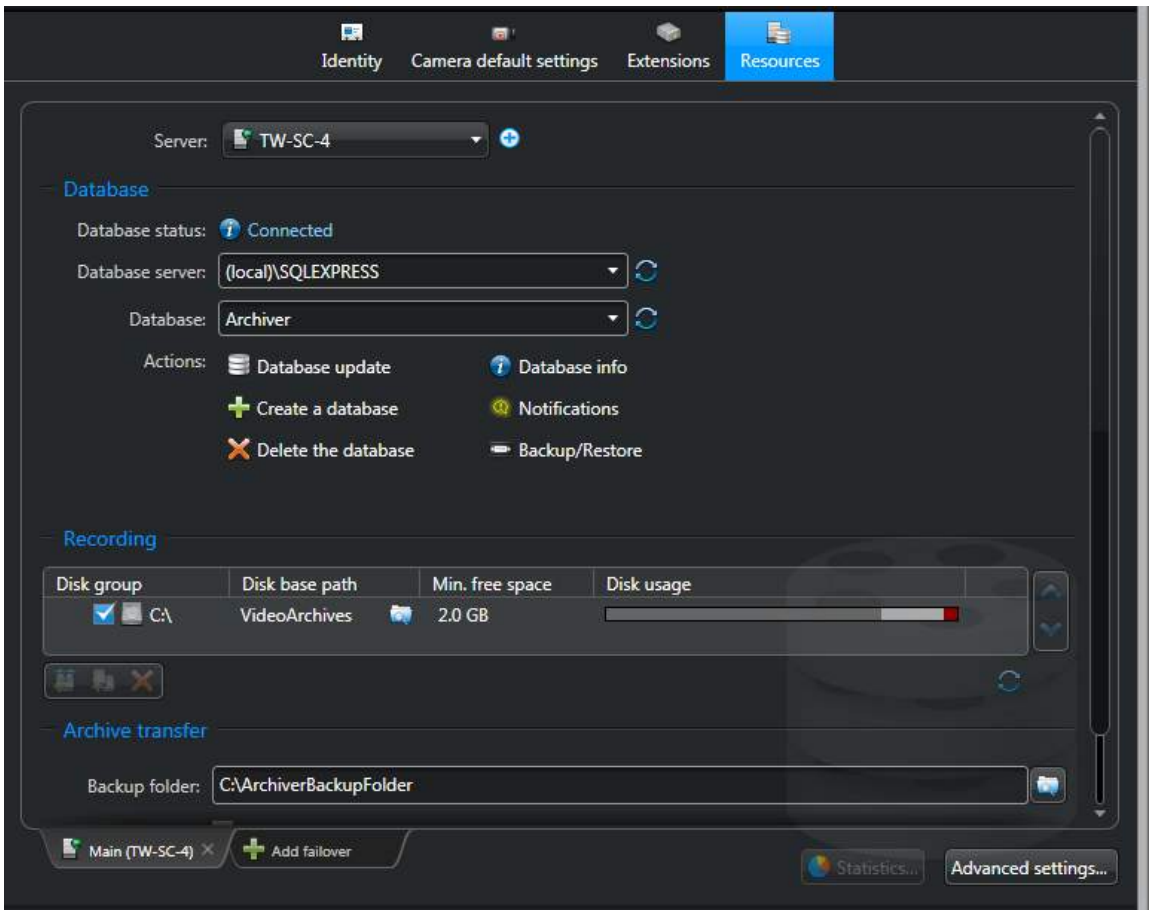
3 Clique em **Propriedades do banco de dados** ( ) para confirmar a versão do banco de dados e o número de entidades no banco de dados.

4 Termine sessão no Server Admin e faça logon no Config Tool.

5 Abra a tarefa **Sistema** e selecione **Funções**.

6 Selecione a função Archiver e clique em **Recursos**.

7 Na seção **Ações**, clique em **Atualização do banco de dados** ( ) .



Depois que a atualização esteja concluída, o **Status do banco de dados** indica *Conectado*.

8 Repita as etapas para cada função que exige a atualização do banco de dados. As funções no seu sistema variam dependendo das suas opções de licença.

Após terminar

Compacte o bancos de dados do Archiver e, se necessário, outros bancos de dados que tiverem sido atualizados.

Compactar bancos de dados do Security Center após uma atualização

Após uma atualização do banco de dados, seu uso de disco pode aumentar significativamente devido ao armazenamento temporário necessário para executar as transações de atualização. O espaço em disco usado durante a atualização não é liberado automaticamente após a atualização ser concluída. Para recuperar o espaço em disco não utilizado, deve compactar o banco de dados.

Antes de iniciar

Nem todas as atualizações de banco de dados fazem com que o banco de dados cresça em tamanho. No entanto, no caso da atualização do banco de dados do Archiver de 5.3 para 5.7, recomendamos compactar o banco de dados após a atualização. Se não tem certeza quanto à necessidade de compactar o banco de dados após uma atualização, verifique o uso de disco com o SQL Server Management Studio.

O que você deve saber

Dependendo do modelo de recuperação do seu bancos de dados, um backup de logs de transação pode ser necessário para recuperar o espaço em disco não utilizado. Para obter mais informações, consulte os seguintes artigos online: Modelos de recuperação (SQL Server) e Truncamento de logs de transação.

Para compactar um banco de dados:

1 Siga o procedimento Compactar um banco de dados publicado online pela Microsoft.
2 Aplique o mesmo procedimento para todos os bancos de dados que exigem compactação.

Visualizar informações do banco de dados

Você pode visualizar as informações sobre o banco de dados de uma função, como as versões do servidor de banco de dados e do banco de dados, quanto espaço em disco está disponível e um resumo dos dados que ele possui.

O que você deve saber

As informações fornecidas pelo banco de dados variam dependendo da função. Você pode ser solicitado a fornecer informações sobre o banco de dados de uma função ao entrar em contato com a Assistência Técnica da Genetec™.

Todas as informações de bancos de dados de função são visualizadas a partir do Config Tool, exceto o banco de dados do Directory, que deve ser visualizado a partir da página Server Admin - Servidor principal. Os procedimentos são muito semelhantes em ambos os casos. Portanto, somente a visualização a partir do Config Tool é descrita aqui.

Para visualizar as informações do banco de dados de uma função:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.

2 Selecione uma função e clique na aba **Recursos**.

3 Clique em **Informações do banco de dados** ( ).

As informações a seguir podem ser exibidas, dependendo da função.

- **Versão do servidor do banco de dados:** Versão do software do servidor de banco de dados.
- **Versão do banco de dados:** Versão esquemática do banco de dados da função.
- **Número aproximado de eventos:** (Também chamado de *Número aproximado de eventos arquivados* e *Contagem de eventos*) Número de eventos que são armazenados no banco de dados da função.
- **Contagem da origem (Somente Archiver e Auxiliary Archiver):** Número de origens de vídeo (câmeras) que têm arquivos.
- **Contagem de arquivos de vídeo (Somente Archiver e Auxiliary Archiver):** Número de arquivos de vídeo.
- **Tamanho no disco:** Tamanho dos arquivos de banco de dados.
- **Número aproximado de entidades (Somente Directory):** Número de entidades (áreas, câmeras, portas, agendamentos e assim por diante) no sistema.
- **Número aproximado de alarmes ativos (Somente Directory):** Número de alarmes ativos (ainda não confirmados) no sistema.
- **Número aproximado de alarmes arquivados (Somente Directory):** Número de alarmes anteriores disponíveis para relatórios, exceto os ativos.

Receber notificações quando os bancos de dados estão quase cheios

Você pode configurar funções diferentes para enviar uma notificação por e-mail quando seus espaços no banco de dados estiver se esgotando.

Antes de iniciar

Para confirmar que a notificação por e-mail seja enviada, defina as configurações de **SMTP** e **Watchdog** no servidor que hospeda a função.

O que você deve saber

Todas as notificações de banco de dados de função são configurados do Config Tool, exceto pelo banco de dados do Directory, que deve ser configurado a partir da Server Adminpágina Servidor principal. Os procedimentos são muito semelhantes em ambos os casos. Portanto, somente a configuração do Config Tool é descrita aqui.

Para receber uma notificação quando o banco de dados de uma função estiver quase cheio:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.

2 Selecione uma função e clique na aba **Recursos**.

3 Clique **Notificações** ( ).

4 Na caixa de diálogo que se abrirá, defina as seguintes opções:

- **Espaço do disco:** Envia uma notificação quando o espaço livre restante no disco fica abaixo de determinado limiar (em GB).
- **Uso do banco de dados:** Envia uma notificação quando o espaço usado pelo banco de dados da função alcança determinada porcentagem. Esta opção é apenas para a edição Express do SQL Server, cujo tamanho do banco de dados é limitado a 10 GB. Se você estiver usando uma edição completa do SQL Server, esta opção não terá efeito.

5 Clique em **OK**.

Tópicos relacionados

Server Admin - Página do servidor principal na página 104

Fazer backup de bancos de dados

Pode proteger os dados no banco de dados de uma função fazendo backup do banco de dados periodicamente. Além disso, é sempre melhor fazer o backup de seus bancos de dados antes de uma atualização.

O que você deve saber

ADVERTÊNCIA: Não use instantâneos de máquina virtual para backup dos seus bancos de dados Security Center . Durante o processo dos instantâneos, todos os I/Os na máquina virtual são suspensos, o que pode afetar a estabilidade e desempenho de seu sistema.Recomendamos vivamente que você siga o procedimento descrito abaixo.

Todos os bancos de dados de função são copiados do Config Tool, exceto o banco de dados do Directory, cujo backup deve ser feito a partir da página do servidor principal Server Admin. Os procedimentos são semelhantes em ambos os casos. Portanto, apenas o backup do Config Tool é descrito aqui.

NOTA: Os seguintes casos são exceções:

- Para fazer o backup dos bancos de dados de função Archiver e Archiver auxiliar com seus arquivos de vídeo associados, você deve usar a tarefa Transferência de arquivos.
- Para fazer backup do banco de dados do Directory enquanto o modo de failover *Backup e restauração* está ativado, o backup deve ser feito na aba **Failover de banco de dados** da função Directory Manager no Config Tool.
- Há restrições em relação ao backup e restauração do banco de dados de Directory quando o modo de failover *Espelhamento* está habilitado. Para obter mais informações, consulte a documentação do Microsoft SQL Server Database Mirroring.

Para fazer o backup do banco de dados de uma função:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.
2 Selecione uma função e clique na aba **Recursos**.
3 Clique em **Backup/Restauração** ( ).
4 Na caixa de diálogo *Backup/Restauração*, ao lado do campo **Pasta de backup**, clique em **Selecionar pasta** ( ) e selecione a pasta onde deseja salvar o arquivo de backup.

   NOTA: O caminho é relativo ao servidor que hospeda a função, não à estação de trabalho onde está executando o Config Tool. Para selecionar uma unidade de rede, digite o caminho manualmente e verifique se o usuário do serviço tem acesso de gravação a essa pasta.

5 (Opcional) Coloque a opção **Comprimir arquivo de backup** em **Ligado** para criar um arquivo ZIP ao invés de um arquivo BAK.

   Se selecionar esta opção, precisará descompactar o arquivo de backup antes de restaurá-lo.

   IMPORTANTE: A opção **Comprimir arquivo de backup** somente funciona se o banco de dados for local no mesmo servidor.

6 Clique em **Fazer backup agora**.

Um arquivo de backup é criado na pasta de backup com a extensão de arquivo BAK. O nome do arquivo é o nome do banco de dados, seguido por "_ManualBackup_" e a data atual (mm-dd-aaaa).

Tópicos relacionados

Transferir arquivos de vídeos sob demanda na página 534
Gerando backup completo do banco de dados do Directory na página 182

Fazer backup de bancos de dados segundo uma agenda

Para proteção adicional dos seus dados, você pode configurar os backups do banco de dados para serem realizados periodicamente.

Para fazer o backup do banco de dados de uma função em um cronograma:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.
2 Selecione uma função e clique na aba **Recursos**.
3 Clique em **Backup/Restauração** ( ).
4 Na caixa de diálogo **Backup/Restauração**, altere a opção **Habilitar backup automático** para **Ligado**.
5 Selecione o dia e a hora para realizar o backup (diariamente ou uma vez por semana).

   DICA: É uma boa ideia alternar operações de backup se diversos bancos de dados diferentes precisarem ter o backup feito na mesma máquina.

6 Especifique quantos arquivos de backup você deseja manter.

   NOTA: Os arquivos de backup que você criar manualmente não serão contados nesse número.

7 Clique em **OK** > **Aplicar**.

O backup automático começará na próxima data e hora agendadas.

Restaurar bancos de dados

Se você tiver acabado de restaurar um servidor de banco de dados, mover um servidor para outro computador, reinstalado ou atualizado o SQL Server ou feito algum engano de configuração que deseje desfazer, você poderá restaurar o banco de dados antigo.

Antes de iniciar

Faça backup do banco de dados atual antes de restaurar um banco de dados antigo. Se a opção **Comprimir arquivo de backup** tiver sido selecionada durante o backup, você primeiro precisará descomprimir o arquivo de backup antes de poder restaurá-lo.

O que você deve saber

Todos os bancos de dados de funções são restaurados do Config Tool, exceto o banco de dados do Directory, que deve ser restaurado a partir da página Server Admin - Servidor Principal. Os procedimentos são muito semelhantes em ambos os casos. Portanto, apenas a restauração de bancos de dados a partir do Config Tool é descrita aqui.

NOTA: Os seguintes casos são exceções:

- Para restaurar o backup de um banco de dados de uma função Archiver ou Archiver auxiliar usando a tarefa *Transferência de arquivos*, consulte Restaurar arquivos de vídeo na página 535.
- Não é possível restaurar o banco de dados do Directory a partir do Server Admin quando o modo de failover *Espelhamento* estiver ativado. Para obter mais informações sobre as restrições referentes a backup e restauração enquanto a *sessão de espelhamento do banco de dados* estiver ativa, consulte a documentação sobre Database Mirroring do Microsoft SQL Server.

Para restaurar o banco de dados de uma função:

1. Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.
2. Selecione uma função e clique na aba **Recursos**.
3. Clique em **Backup/Restauração** ( ).
4. Na caixa de diálogo **Backup/Restauração**, ao lado do campo **Pasta de restauração**, clique em **Selecionar pasta** ( ) e selecione o arquivo de backup que deseja restaurar.

   NOTA: O caminho é relativo ao servidor que hospeda a função, não à estação de trabalho onde está executando o Config Tool.

5. Clique em **Restaurar agora**.

O conteúdo atual do banco de dados é substituído pelo conteúdo restaurado do arquivo de backup.

Sobre redes

A entidade de rede é usada para captar as características das redes usadas pelo seu sistema, para que possam ser tomadas as decisões adequadas de roteamento de stream.

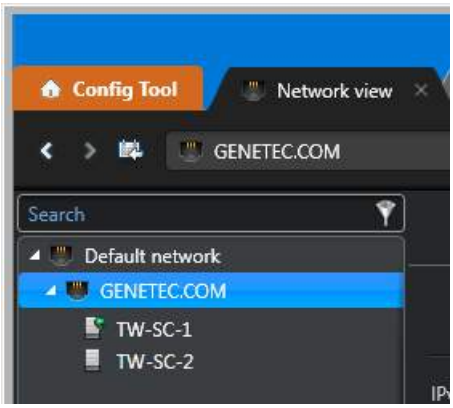
A menos que todo o seu sistema seja executado a partir de uma única rede privada sem comunicação com o mundo exterior, você deverá configurar pelo menos uma entidade de rede além da *Rede padrão* para descrever o seu ambiente de rede.

Como as entidades de rede são criadas

As entidades de rede são criadas automaticamente pelo sistema.

Após instalar o Security Center em seu servidor principal, você terá as duas entidades de rede seguintes em seu sistema:

- A *Rede padrão* é o nó raiz da árvore de redes. Suas capacidades de transmissão de vídeo são configuradas como *Unicast TCP*, que é a característica compartilhada por todas as redes IP. Você não pode excluir a entidade *Rede padrão*.
- Uma segunda entidade de rede é anexada à *Rede padrão*, que corresponde à rede da sua empresa (onde seu servidor principal está localizado).



Após isso, mais entidades de rede são adicionadas ao seu sistema quando você adiciona novos servidores de redes diferentes.

Quando um servidor com várias placas de interface de rede (NIC) é adicionado ao sistema, somente o primeiro endereço definido no sistema operacional é representado por padrão como uma entidade de rede. Porém, você pode adicionar as outras entidade de rede manualmente se, posteriormente, você precisar de ter um melhor controle das capacidades de roteamento.

Uma rede federada ( ) é criada para cada sistema federado. Isso permite que você controle como a mídia daquele sistema é acessada pelo sistema local, para forçar o redirecionamento da mídia e para configurar as capacidades de roteamento.

Roteamentos de rede

Entre cada duas redes no seu sistema há uma rota. As capacidades de transmissão de dados da rota estão limitadas ao menor conjunto de capacidades dos dois pontos de extremidade.

Por exemplo, se uma extremidade tiver capacidade multicast e a outra somente tiver capacidade unicast UDP, as capacidades da rota entre esses dois pontos de extremidades não poderão ser superiores a unicast UDP.

Se a conexão entre os dois pontos de extremidade (por exemplo, VPN) somente suportar unicast TCP, você poderá precisar limitar mais as capacidades de uma rota.

Tópicos relacionados

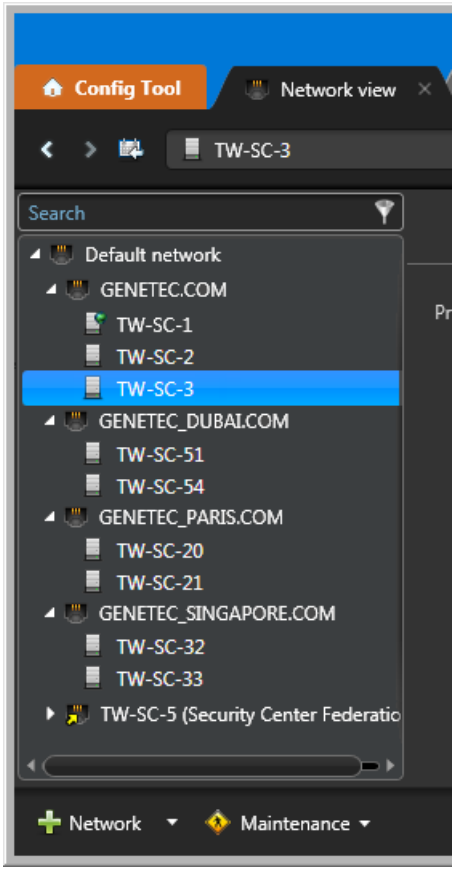
Adicionar redes na página 157

Sobre a exibição de rede

A visualização de rede é um navegador que ilustra seu ambiente de rede ao mostrar cada servidor na rede a que pertence.

Você pode gerenciar esta exibição através da tarefa *Exibição de rede*. A hierarquia na tarefa *Exibição de rede* exibe as redes ( ) e os *servidores* ( ) encontrados em seu sistema e permite que você os configure. O *servidor principal* que hospeda a função *Directory* é exibido com um ícone diferente ( ).

Ter uma representação precisa na Exibição de rede ajuda a visualizar a configuração atual do seu sistema.



Uma rede federada ( ) é criada para cada sistema federado. Isso permite que você controle como a mídia daquele sistema é acessada pelo sistema local, para forçar o redirecionamento da mídia e para configurar as capacidades de roteamento.

Adicionar redes

Se o seu sistema se espalhar por várias redes ou se você permitir que seus usuários se conectem ao servidor principal pela Internet, você deverá configurar a visualização de rede e adicionar redes adicionais.

Para adicionar uma rede:

1 Abra a tarefa **exibição de rede**.

2 Se estiver criando uma sub-rede, selecione a rede pai na estrutura da rede. Caso contrário, selecione a *Rede padrão*.

3 Clique em **Rede** (), e digite o nome da entidade de rede.

Você será colocado automaticamente na aba**Propriedades**.

4 Na lista suspensa **Capacidades**, selecione o tipo de transmissão de dados para a transmissão de vídeo ao vivo na rede.

DICA: Sempre selecione o maior conjunto de capacidades que sua rede suporte.

- **TCP Unicast:** Comunicação (individual) Unicast usando protocolo TCP é o modo de comunicação mais comum de comunicação. É suportado por todas as redes de IP, mas também é o método menos eficiente de transmitir vídeo.
- **UDP Unicast:** Comunicação Unicast (individual) usando protocolo UDP. Devido ao fato de o UDP ser um protocolo sem conexão, funciona muito melhor para transmissão de vídeo ao vivo. Quando o tráfego de rede está ocupado, o UDP tem muito menos probabilidade de causar vídeos intermitentes do que o TCP. Uma rede que suporta UDP unicast necessariamente suporta TCP unicast.
- **Multicast:** Multicast é o método de transmissão mais eficiente para vídeo ao vivo. Permite que a transmissão de vídeo seja transmitida uma vez pela rede para ser recebida por quantos destinos forem necessários. O ganho pode ser muito significativo se houverem muitos destinos. Uma rede que suporta multicast necessariamente suporta UDP unicast e TCP unicast.

  NOTA: Multicast necessita de roteadores e interruptores especializados. Certifique-se de confirmar isso com seu departamento de TI antes de definir as capacidades para multicast.

5 Na seção **Rotas**, verifique se todas as rotas criadas por padrão são válidas.

- Você pode precisar alterar as capacidades padrão ou forçar o uso de endereço privado quando endereços públicos não puderem ser usados entre servidores dentro da mesma subrede. Para editar uma rota, selecione-a na lista e clique em **Editar o item** ().
- Se não houver conexão entre esta rede e outra rede no sistema, selecione a rota e clique em **Excluir** ().
- Você pode querer adicionar uma rota direta entre esta rede e outra rede secundária, ignorando sua rede principal.

6 Clique em **Aplicar**.

Tópicos relacionados

Configurar a função Media Router na página 463
Rede - Aba Propriedades na página 1019

Criar conexões diretas entre redes

Você pode criar uma nova rota entre duas redes em seu sistema se sua configuração de rede o permitir.

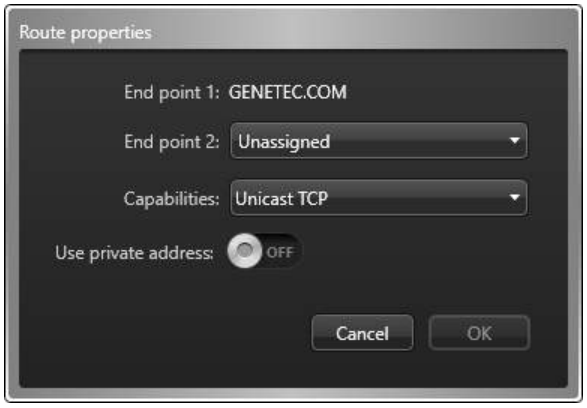
O que você deve saber

Por padrão, o Security Center cria uma rota entre uma rede e sua rede principal e entre duas redes sujeitas à mesma rede principal.

Para adicionar uma rota entre duas redes:

1 Abra a tarefa **exibição de rede**.
2 Selecione a rede a partir da qual deseja estabelecer a rota e clique na aba **Propriedades**.
3 Na seção **Rotas**, clique em **Adicionar um item** ( ).

A caixa de diálogo *Propriedades da rota* abre.



4 A partir da lista suspensa **Extremidade 2**, selecione outra rede com a qual queira estabelecer a rota.
5 Na lista suspensa **Capacidades**, selecione o menor conjunto de capacidades.
6 Se endereços públicos não puderem ser usados entre essas duas redes, alterne a opção **Usar endereço privado** para **Ligado**.
7 Clique em **OK** e, em seguida, clique em **Aplicar**.

Personalizando opções de rede

Você pode personalizar sua placa de rede, o modo como sua rede é selecionada e seu intervalo da porta para garantir a melhor comunicação de entrada e saída de sua estação de trabalho.

O que você deve saber

As configurações de rede se aplicam à estação de trabalho local e afetam o Security Desk e o Config Tool para todos os usuários.

Para personalizar opções de rede:

1 Na página inicial, clicar em **Opções** > **Geral**.
2 Se o seu computador for equipado com mais de uma placa de rede, selecione aquela usada para se comunicar com os aplicativos do Security Center na lista suspensa **Placa de rede**.
3 Escolha como selecionar a **Rede**:
   - **Detecção automática:** O Security Center detecta automaticamente a rede na qual a sua estação de trabalho está conectada.
   - **Específico:** Selecione manualmente a rede em que você está na lista suspensa. Essa opção é útil se você tiver problema em obter feeds de vídeo.
4 Na opção **Intervalo de portas UDP de entrada**, selecione o intervalo de porta usado para transmitir vídeo para a sua estação de trabalho usando o *multicast* ou unicast *UDP*.
5 Clique em **Salvar**.

Exemplo

Consideremos o seguinte caso de uso. Você tem uma rede 10.1.x.x com uma rota para 10.2.x.x. Mas, por algum motivo, uma estação de trabalho específica no endereço 10.1.2.3 não pode acessar 10.2.x.x. Especificar uma rede manualmente naquela estação de trabalho permite que o Media Router saiba que deve redirecionar a mídia de 10.2.x.x para aquela estação de trabalho em vez de fazê-la se conectar diretamente a 10.2.x.x e falhar.

8

Alta disponibilidade

Esta seção inclui os seguintes tópicos:

- "Sobre os recursos de alta disponibilidade no Security Center" na página 161
- "Failover de função" na página 162
- "Configurar failover de função" na página 165
- "Failover e balanceamento de carga de Directory" na página 167
- "Preparar failover e balanceamento de carga do Directory" na página 168
- "Configurar failover e balanceamento de carga do Directory" na página 169
- "Reativar a licença do Security Center para sistemas com failover do Directory" na página 172
- "Removendo servidores da lista de failover do Directory." na página 177
- "Ignorar o balanceamento de carga em estações de trabalho" na página 178
- "Failover de banco de dados do Directory" na página 179
- "Configurar failover do banco de dados do Directory por backup e restauração" na página 181
- "Configurar failover do banco de dados do Directory por espelhamento" na página 183
- "Configurar failover de banco de dados do Directory através do SQL AlwaysOn" na página 185
- "Failover do Archiver" na página 186
- "Configurar failover do Archiver" na página 188
- "Configurar um período de retenção diferente para o servidor de Archiver secundário" na página 191
- "Consolidar arquivos de vídeo após failover do Archiver" na página 193
- "Solução de problemas do failover" na página 195

Sobre os recursos de alta disponibilidade no Security Center

A alta disponibilidade é uma abordagem que permite que um sistema funcione em um nível operacional mais alto que o normal. Muitas vezes, isso envolve failover e balanceamento de carga.

Para garantir que haja acesso e proteção de dados ininterruptos para o seu sistema, o Security Center oferece os seguintes recursos de disponibilidade:

- **Failover do diretório:** Certifique-se de que a função Directory permaneça disponível quando seu servidor primário falhar. A função Directory lida com o failover para todas as outras funções, portanto é importante que ela permaneça disponível em todos os momentos.
- **Equilíbrio de carga do diretório:** Benefício adicional do failover do Directory. Até 5 servidores podem ser atribuídos para a função Directory para compartilhar sua carga de trabalho. Todos os servidores que sejam configurados para failover do Directory são usados automaticamente para o balanceamento de carga.
- **Failover de banco de dados (somente para a função Directory):** Protege o banco de dados do Directory, usando um dos seguintes métodos:
  - **Backup e restauração:** Faz backup regular do seu banco de dados e o restaura se ocorrer um failover.
  - **Espelhamento do Microsoft SQL Server Database:** As instâncias de banco de dados são mantidas em sincronia pelo Microsoft SQL Server.
- **Failover do Archiver:** Certifique-se que a função Archiver e as capacidades de arquivamento de vídeo permaneçam disponíveis quando o servidor principal do Archiver falhar.
- **Failover de outra função:** Certifique-se de que outras funções em seu sistema permaneçam disponíveis quando seu servidor principal falhar. Se for necessário proteger o banco de dados da função, você deverá considerar uma das seguintes soluções de terceiros: *Clustering de SQL Server* ou *Espelhamento de Banco de Dados*.
- **NEC ExpressCluster X LAN:** Solução de terceiros para funções que não suportam failover. Para obter mais informações, consulte o *Guia de Instalação Security Center para Cluster NEC*. Clique aqui para obter a versão mais recente desse documento.
- **Cluster de failover do Windows Server 2008:** Solução de terceiros para funções que não suportam failover. Para obter mais informações, consulte o *Guia de Instalação Security Center para Cluster Windows*. Clique aqui para obter a versão mais recente desse documento.

Outras maneiras como você pode garantir alta disponibilidade são detectar os problemas antecipadamente e evitar que esses problemas ocorram novamente.

Tópicos relacionados

Sobre monitoramento da saúde do sistema na página 290

Failover de função

Failover é um modo operacional de backup em que uma função (do sistema) é automaticamente transferida do seu servidor primário para um secundário que está em espera. Esta transferência entre servidores ocorre somente quando o primeiro servidor está indisponível, seja por falha ou por inatividade programada. O failover de função é gerenciado pela função Directory.

Como o failover de função funciona no Security Center

Para que o failover funcione no Security Center, você precisará definir os dois seguintes tipos de servidores:

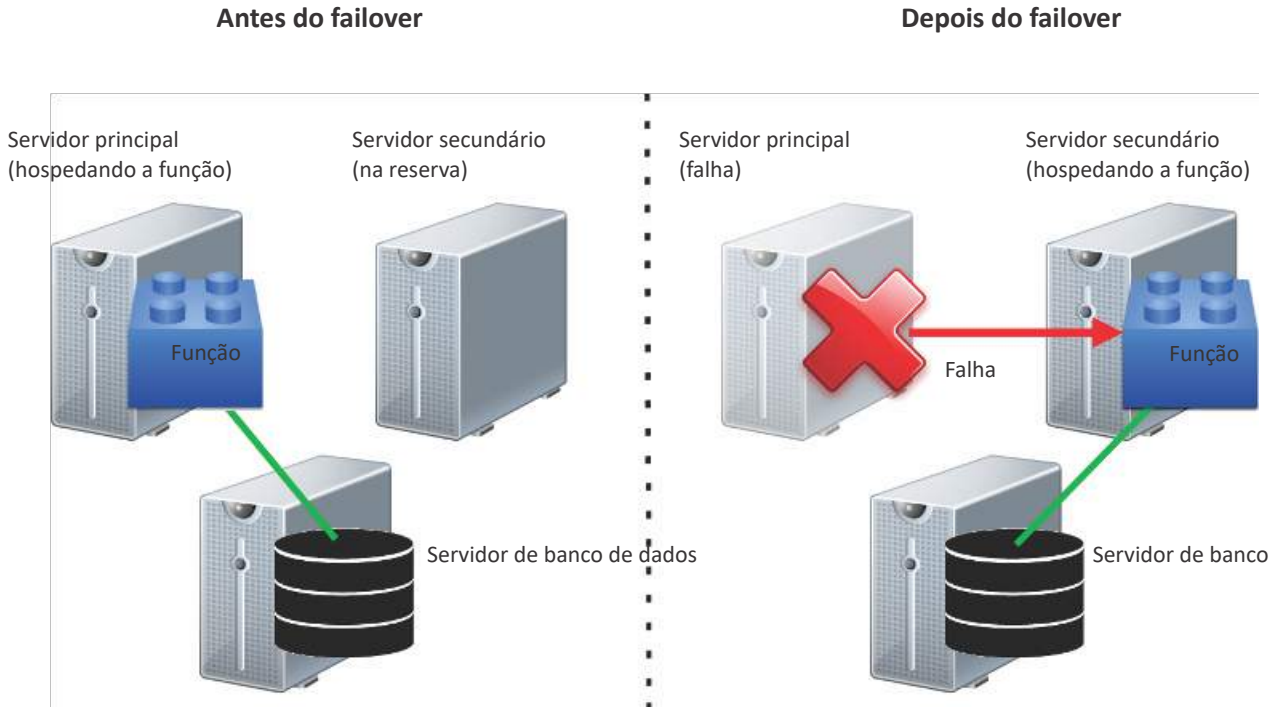
- **Servidor principal:** Servidor que normalmente hospeda uma função para funcionar no sistema.
- **Servidor secundário:** Servidores em espera que são atribuídos a uma função para mantê-la em funcionamento caso o servidor principal fique indisponível.

Não há limite para o número de servidores secundários (ou em espera) que você pode atribuir à maioria das funções. Porém, quanto mais servidores você adicionar, menor poderá ser o custo-benefício para você.

O servidor secundário de uma função pode ser o servidor principal de outra função, desde que ambos os servidores tenham recursos suficientes (CPU, memória, espaço em disco e largura de banda de rede) para lidar com a carga combinada de ambas as funções em caso de failover.

IMPORTANTE: O Security Center não processa o failover de bancos de dados de função. Para proteger os seus dados, faça backups regulares dos banco de dados de função.

Antes do failover, uma função é hospedada no *servidor primário* e se conecta a um *servidor do banco de dados* hospedado em um terceiro computador. Quando o *servidor primário* falha, a função falhada é transferida automaticamente para o *servidor secundário* e se reconecta ao **mesmo** *servidor de banco de dados*.



Funções com suporte a failover

Algumas funções no Security Center não suportam failover e outras suportam o failover somente sob certas condições.

A tabela a seguir lista quais funções do Security Center suportam failover, a abordagem de failover que elas usam e quaisquer requisitos especiais que possam ter.

Função	Suporta failover	Comentários e exceções
Gestor de Acesso	Sim	
Diretório ativo	Sim	
Serviços de Federação do Active Directory (ADFS)	Sim	A função ADFS é executada no mesmo servidor da função Directory. Se o failover do Directory estiver configurado, então a URL de todos os servidores do Directory no seu sistema devem ser adicionados como pontos de extremidade à parte confiável Security Center do servidor ao qual o ADFS está conectado.
Archiver	Sim	Pode ter até dois servidores secundários atribuídos a uma função de Archiver. Cada servidor exige o seu próprio banco de dados separado, hospedado localmente ou em um computador separado.
Archiver Auxiliar	Não se aplica	A função do Archiver auxiliar é garantir que arquivo de vídeos continuem disponíveis quando o Archiver falhar.
Diretório	Sim	Pode ser executado simultaneamente em até cinco servidores. Também suporta o failover do banco de dados do Directory.
Gerenciador do diretório	Não se aplica	A função do Directory Manager is é gerenciar o failover e balanceamento de carga do Directory.
Sincronizador do Titular do Cartão Global	Sim	
Monitor de Integridade	Sim	
Gerenciador de invasão	Sim	Somente quando os *painéis de intrusão* são conectados usando o IP. O failover não é suportado se os painéis de intrusão forem conectados usando portas seriais.

Função	Suporta failover	Comentários e exceções
LPR Manager	Sim	Devem ser compartilhados recursos extras entre os servidores atribuídos à função. A pasta *Raiz* da função deve seguir a convenção UNC e ser acessível a todos os servidores. Os caminhos para a lista de procurados e entidades de autorização devem também seguir a convenção UNC e estar acessível a todos os servidores. O arquivo *WatermarkEncryptionParameters.xml* encontrado na pasta de instalação do servidor principal deve ser copiado para todos os servidores secundários.
Gerenciador de mapas	Sim	**MELHOR PRÁTICA:** É melhor definir o cache do mapa em um local que pode ser atingido por todos os servidores atribuídos à função.
Gateway de mídia	Sim	
Roteador de mídia	Sim	Os servidores principal e secundário podem ter, cada um, um banco de dados separado, hospedado localmente ou em outro computador.
Omnicast™ Federation™	Sim	
Plug-in	Sim	
Gerenciador de Relatório	Sim	
Security Center Federation™	Sim	
SDK baseado na web	Sim	
Servidor Web Client	Sim	O Web Client deve se reconectar a uma URL diferente quando a função falhar e é transferida para um servidor diferente.
Gerenciador de Zona	Sim	

Tópicos relacionados

Adicionar uma parte confiável para o Security Center na página 406

Configurar failover de função

Para configurar o failover para funções no seu sistema, você deve selecionar servidores secundários para ficarem em espera caso o servidor principal que hospeda a função fique indisponível.

Antes de iniciar

Para funções que exijam um banco de dados (com exceção da função Archiver), o banco de dados deve ser hospedado em um computador diferente de quaisquer servidores atribuídos à função. Todos os servidores atribuídos à função devem ter capacidade de conexão ao servidor que gerencia o banco de dados da função.

IMPORTANTE: Todos os servidores atribuídos à mesma função devem executar a mesma versão do Security Center.

O que você deve saber

Para configurar o failover para uma função Archiver, consulte Failover do Archiver na página 186.

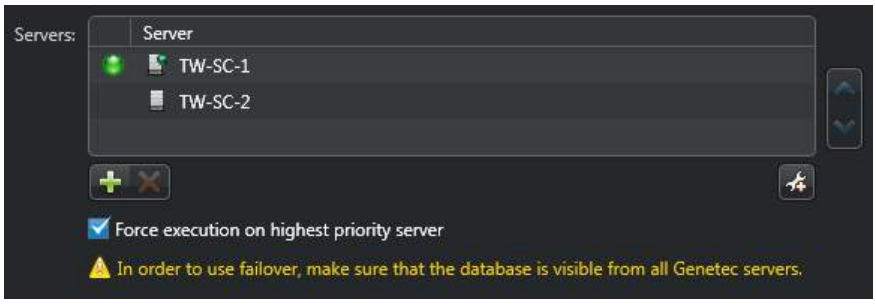
Para configurar o failover de função:

1. Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.
2. Selecione a função para a qual deseja configurar failover e clique na aba **Recursos** onde o servidor principal da função está listado.
3. Na lista **Servidores**, clique em **Adicionar um item** ( ).

   Aparece uma caixa de diálogo listando todos os servidores restantes em seu sistema que ainda não tenham sido atribuídos à função.
4. Selecione o servidor que deseja adicionar como servidor secundário e clique em **Adicionar**.

   O servidor secundário é adicionado abaixo do servidor principal. O LED verde indica qual servidor está hospedando a função.

   NOTA: Os servidores são listados na ordem em que são escolhidos se um failover ocorrer. Quando o servidor principal falha, a função é alternada automaticamente para o próximo servidor na lista.

5. Para alterar a prioridade de um servidor, selecione-o na lista e clique no botão ou para movê-lo para cima ou para baixo na lista.
6. Se você quiser que o servidor primário retome o controle uma vez que ele seja restaurado de um failover, selecione a opção **Forçar a execução no servidor com prioridade mais alta**.

   Por padrão, para minimizar perturbações no sistema, a função permanece no servidor secundário após a ocorrência de um failover.
7. Clique em **Aplicar**.

Alterar a prioridade do servidor para failover de funções

Você pode tornar servidores secundários em servidores primários ou assegurar que um servidor primário é sempre o que hospeda a função desde que esteja em execução.

O que você deve saber

Por padrão, para minimizar perturbações no sistema, a função permanece no servidor secundário após a ocorrência de um failover. Você pode alterar a prioridade dos servidores e fazer com que o servidor com maior prioridade seja o que sempre hospeda a função.

Para alterar a prioridade do servidor para o failover:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.

2 Selecione a função e clique na aba **Recursos** onde o servidor principal da função está listado.

3 Selecione um servidor na lista e clique nos botões ou para alterar a prioridade dos servidores.

Quanto mais acima na lista, maior prioridade tem o servidor.

4 Selecione a opção **Forçar execução no servidor de prioridade mais alta** e clique em **Aplicar**.

Esta opção faz com que o servidor de maior prioridade (no topo da lista) seja o que sempre hospeda a função, desde que esteja online. Se o primeiro servidor estiver offline, a prioridade passa para o segundo servidor na lista e assim sucessivamente.

Após alguns segundos, o LED verde se move para o servidor que está no topo da lista, indicando que agora ele é o que hospeda a função.

IMPORTANTE: Os servidores são exibidos para que eles sejam escolhidos se um failover ocorrer. Quando o servidor principal falha, a função é alternada automaticamente para o próximo servidor na lista.

Failover e balanceamento de carga de Directory

Como o Directory é a função principal que gerencia toda a configuração de entidades no seu sistema, você deve garantir que o serviço do Directory sempre esteja disponível e não fique sobrecarregado.

O serviço do Directory fica disponível enquanto seus dois componentes estiverem disponíveis:

- **Função do diretório:** Gerencia a configuração do seu sistema e lida com o failover para todas as outras funções.
- **Banco de dados do Directory:** Armazena sua configuração do sistema.

A função *Directory Manager* lida com o *failover* e o *balanceamento de carga* do Directory para o seu sistema. Ela gerencia o failover para a função Directory e o banco de dados do Directory independentemente, permitindo que você tenha listas separadas de *servidores* atribuídos para hospedar os dois componentes. Essas duas listas de servidores podem ser sobrepostas ou ser completamente separadas.

NOTA: Somente pode haver uma função do Directory Manager em seu sistema. Ela é criada automaticamente quando sua licença de software suporta vários servidores do Directory.

Diferenças entre servidores do Directory e o servidor principal

Para configurar o failover do Directory e o balanceamento de carga, você deve saber a diferença entre servidores do Directory e o servidor principal.

- **servidor do Directory:** Servidores atribuídos para hospedar a função do Directory. A função Directory pode ser executada em cinco servidores do Directory simultaneamente para o *balanceamento de carga*. Eles distribuem a carga de trabalho para autenticação de credenciais, fiscalização de licença de software, consultas de relatório do banco de dados do Directory e assim por diante.

  Os usuários podem fazer logon no Security Center através de qualquer um dos servidores do Directory. Por padrão, o Directory Manager redireciona as solicitações de conexão entre todos os servidores do Directory de modo alternado, mas você pode ignorar o balanceamento de carga em estações de trabalho específicas conforme necessário.
- **Servidor principal:** O servidor principal do Directory em seu sistema (). Ele possui acesso de gravação/leitura completo para o banco de dados do Directory. Se o seu sistema estiver configurado para failover do Directory e balanceamento de carga, os servidores do Directory adicionais () têm somente acesso de leitura no banco de dados.

Quando um servidor do Directory falha, apenas os aplicativos clientes conectados ao Security Center por aquele servidor deverão se reconectar. Se o servidor principal falhar, então *todos* os clientes no sistema devem se reconectar e a responsabilidade de *servidor principal* é passada para o servidor do Directory seguinte na lista de failover.

Preparar failover e balanceamento de carga do Directory

Antes que você possa configurar o Directory para failover e balanceamento de carga, são necessárias algumas etapas pré-configuração.

Antes de configurar o failover e balanceamento de carga do Directory:

1 Certifique-se de que sua licença do Security Center suporta vários *Servidores do Directory*.

NOTA: A função *Directory Manager* ( ) é criada automaticamente em Config Tool quando sua licença suporta múltiplos servidores do Directory.

a) Na página inicial, clique em **Sobre** > **Security Center**.
b) Na opção **Número de servidores do Directory adicionais**, observe o número de servidores suportados.

Caso precise atualizar sua licença, consulte o *Guia de Instalação e Atualização do Security Center*.

2 Tenha em mãos seu *ID do sistema* e sua *Senha*, encontrados no documento *Informações de Licença do Security Center*.

A Assistência Técnica da Genetec™ envia este documento quando o cliente compra o produto.

3 Certifique-se de que todos os servidores que você planeja usar como *servidores* do Directory estão ativos e em execução como servidores de expansão.

Para mais informações sobre como instalar servidores de expansão, consulte o *Guia de Instalação e Atualização do Security Center*.

4 Para todos os servidores de expansão que você planeja usar como servidores do Directory, certifique-se de que suas propriedades gerais configuradas no Server Admin são as mesmas do servidor principal.

Isso garante que seus dados, como o período de retenção do alarme e assim por diante, seja armazenado pelo mesmo período de tempo.

5 Hospede o banco de dados do Directory em um computador remotos dos servidores do Directory.
6 Certifique-se de que o servidor de banco de dados seja acessível de todos os servidores do Directory.

Tópicos relacionados

Server Admin - Página do servidor principal na página 104

Configurar failover e balanceamento de carga do Directory

Para proteger suas informações caso o servidor principal falhe, você pode configurar o failover do Directory e o balanceamento de carga atribuindo os servidor de expansão como servidores do Directory.

Antes de iniciar

Prepare o failover e o balanceamento de carga do Directory.

O que você deve saber

- Você pode converter até cinco servidores de expansão como *Servidores do Directory* para serem usados para balanceamento de carga e failover. A ordem de aparição dos servidores na lista corresponde à ordem em que eles são selecionados se um failover ocorrer. Se o servidor principal falhar, a função alterna para o próximo servidor da lista e aquele servidor se torna o servidor principal.

  IMPORTANTE: Não tente adicionar um servidor à lista de failover do Directory ativando o Directory naquele servidor de expansão com o Server Admin. Essa ação desconecta o servidor do seu sistema atual e o transforma no *servidor principal* de um novo sistema.

- Se você quiser excluir um servidor do Directory do balanceamento de carga porque o servidor ou a conexão entre o cliente e o servidor é lenta, você pode ativar a opção **Recuperação de desastre**. Isso remove o servidor de participar do balanceamento de carga, mas o servidor ainda estará disponível para assumir como servidor principal em caso de failover do Directory.

Para configurar o failover e balanceamento de carga do Directory:

1. Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.
2. Selecione a função **Directory Manager** ( ) e clique na aba **Servidores do Directory**.
3. Clique em **Adicionar um item** ( ).
4. Na caixa de diálogo que aparece, selecione o servidor que você deseja adicionar, sua porta de conexão (padrão=5500) e clique em **Adicionar**.

   O servidor é adicionado à lista de failover.
5. Adicione mais servidores do Directory, se necessário.
6. Atualize sua licença para incluir os servidores que você acabou de promover a servidores do Directory.
7. Clique em **Aplicar**.

Os servidores de expansão são convertidos em servidores do Directory e a licença atualizada é aplicada a todos os servidores do Directory na lista. Os aplicativos clientes e as funções nos servidores de expansão podem se conectar ao Security Center usando qualquer um dos servidores do Directory.

Tópicos relacionados

Configurar um servidor do Directory para recuperação de desastres na página 170

Forçando um servidor do Directory a sempre ser o servidor principal

Se um dos *Servidores do Directory* for sua escolha preferida para ser o *servidor principal*, você pode forçá-lo a sempre ser o servidor principal quando estiver disponível.

O que você deve saber

O primeiro servidor na lista de servidores do Directory é o seu servidor principal *padrão*. Quando um failover do Directory ocorre, o próximo servidor da fila se torna o novo servidor principal ( ). Quando o primeiro servidos fica online novamente após um failover, o comportamento padrão é manter o servidor atual e não mudar de volta para o servidor principal. Esse comportamento minimiza as disrupções do sistema

causadas por aplicativos tendo que se desconectar e reconectar ao servidor principal. Se esse não for o comportamento que você deseja para o seu sistema, você pode alterá-lo na aba **Servidores do Directory**.

Para alterar a prioridade dos servidores na lista de failover do Directory:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.
2 Selecione a função **Directory Manager** ( ) e clique na aba **Servidores do Directory**.
3 Selecione um servidor na lista e clique em **Para cima** ( ) ou **Para baixo** ( ) para mover os servidores do Directory para cima ou para baixo na lista.
4 Para forçar o primeiro servidor na lista de failover a ser o servidor principal sempre que estiver disponível, selecione a opção **Forçar o primeiro servidor na lista a ser o servidor principal**.
5 Clique em **Aplicar**.

Configurar um servidor do Directory para recuperação de desastres

Configurar um servidor do Directory para ser um servidor de *recuperação de desastres* exclui o servidor do balanceamento de carga. Um servidor de recuperação de desastre somente é ativado se ele assumir como servidor principal durante um failover do Directory.

Antes de iniciar

Configure o failover e balanceamento de carga do Directory.

O que você deve saber

- Se um *servidor do Directory* estiver localizado remotamente ou tiver uma conexão lenta, você poderá ativar a opção de recuperação de desastres para que ele não deixe o sistema lento participando no balanceamento de carga.
- Um servidor de recuperação de desastres não aceita conexões de clientes a menos que se torne o *servidor principal* durante um failover do Directory.
- Funções como Media Router, Health Monitor e Report Manager são frequentemente hospedadas em servidores do Directory. Se você estiver ativando a recuperação de desastres, você deverá ativar a opção **Forçar execução no servidor de prioridade mais alta** em todas as funções que sejam hospedadas em servidores do Directory. Isto garante que essas tarefas não continuam a ser executadas no servidor de recuperação de desastres depois de o servidor principal do Directory ficar novamente online. Para mais informações, veja Failover de função na página 162.

Para configurar um servidor de recuperação de desastre:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.
2 Selecione a função **Directory Manager** ( ) e clique na aba **Servidores do Directory**.
3 Na parte inferior da lista de servidores, clique em **Avançado** ( ).
Uma coluna adicional, **Recuperação de desastres**, exibida na lista.
4 Selecione **Recuperação de desastres** para um ou mais servidores do Directory.
NOTA: A opção de **Recuperação de desastre** aplica-se somente aos servidores do Directory, não a Gateways.
5 Clique em **Aplicar**.

O servidor é excluído do balanceamento de carga e somente aceita conexões de cliente se ele se tornar o servidor principal durante um failover do Directory.

Tópicos relacionados

Configurar failover e balanceamento de carga do Directory na página 169

Alternar o servidor principal

Se necessário, você pode atribuir qualquer servidor na lista de failover do Directory para ser o servidor principal. Por exemplo, quando trabalho de manutenção precisa ser feito no servidor principal atual.

Para alternar o servidor principal:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.

2 Selecione a função **Directory Manager** ( ) e clique na aba **Servidores do Directory**.

3 Selecione um servidor e clique em **Ativar Directory** ( ).

4 Clique em **Continuar**.

Todos os aplicativos clientes e funções são desconectados, o servidor principal alterna para o servidor do Directory que você selecionou e todos os aplicativos e função se reconectam.

Reativar a licença do Security Center para sistemas com failover do Directory

Deve reativar sua licença do Security Center com uma nova chave de validação, sempre que adicionar ou remover servidores da lista de servidores do Directory.

Antes de iniciar

Para atualizar sua licença, precisa do seguinte:

- **ID do sistema e senha:** O ID e a senha do Sistema encontram-se no documento *Informações de Licença do Security Center*. O Serviço de Atendimento ao Cliente Genetec™ envia este documento quando o cliente compra o produto.

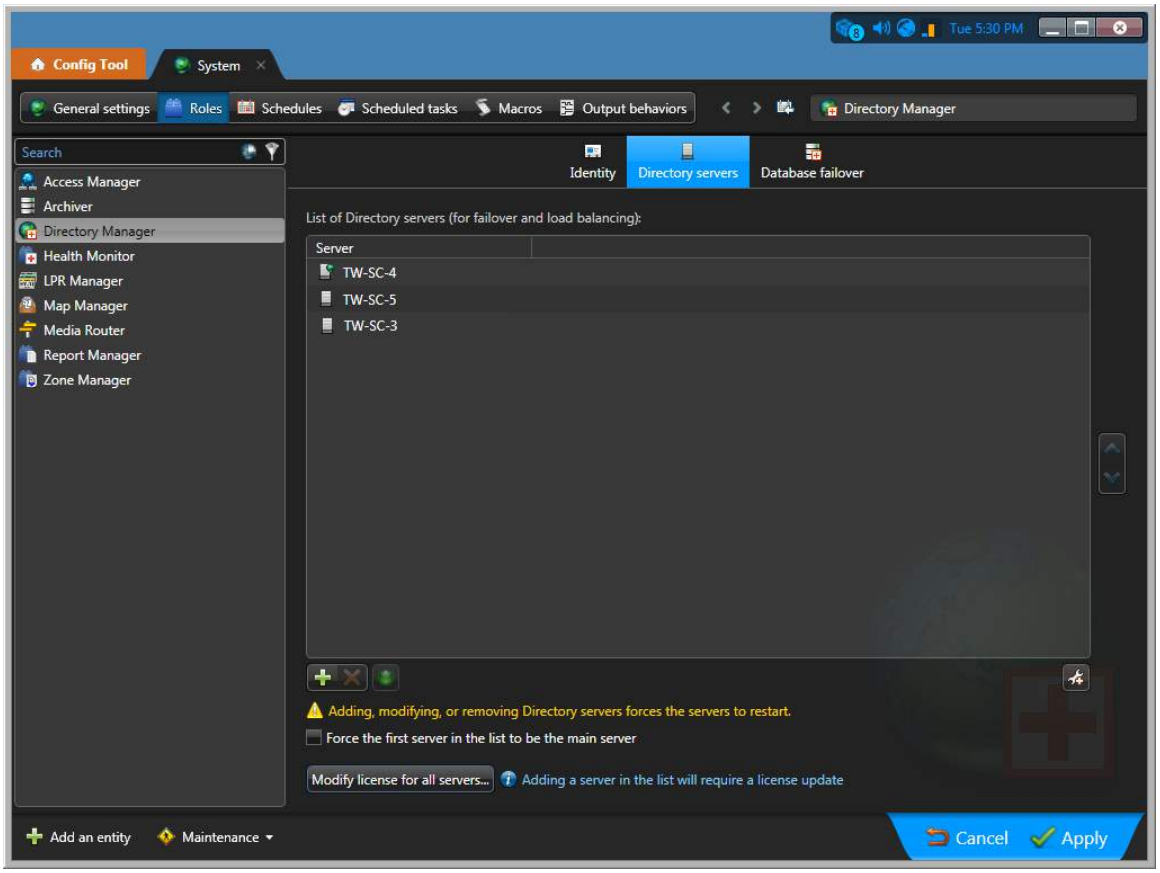
O que você deve saber

IMPORTANTE: O Server Admin só pode ser usado para ativar uma licença de servidor único. Se você tiver uma configuração de servidores múltiplos do Directory, tanto a geração da chave de validação quanto a aplicação da chave de licença devem ser executadas pelo Config Tool. Todos os servidores do Directory devem estar em execução para atualizar a licença a partir do Config Tool.

Para ativar a licença do Security Center para um sistema de servidores múltiplos do Directory:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.

2 Selecione a função **Directory Manager** ( ) e clique na aba **Servidores do Directory**.



3 Clique em **Modificar a licença para todos os servidores**.

4 Na caixa de diálogo **Gerenciamento de licença**, ative sua licença de uma das seguintes maneiras:

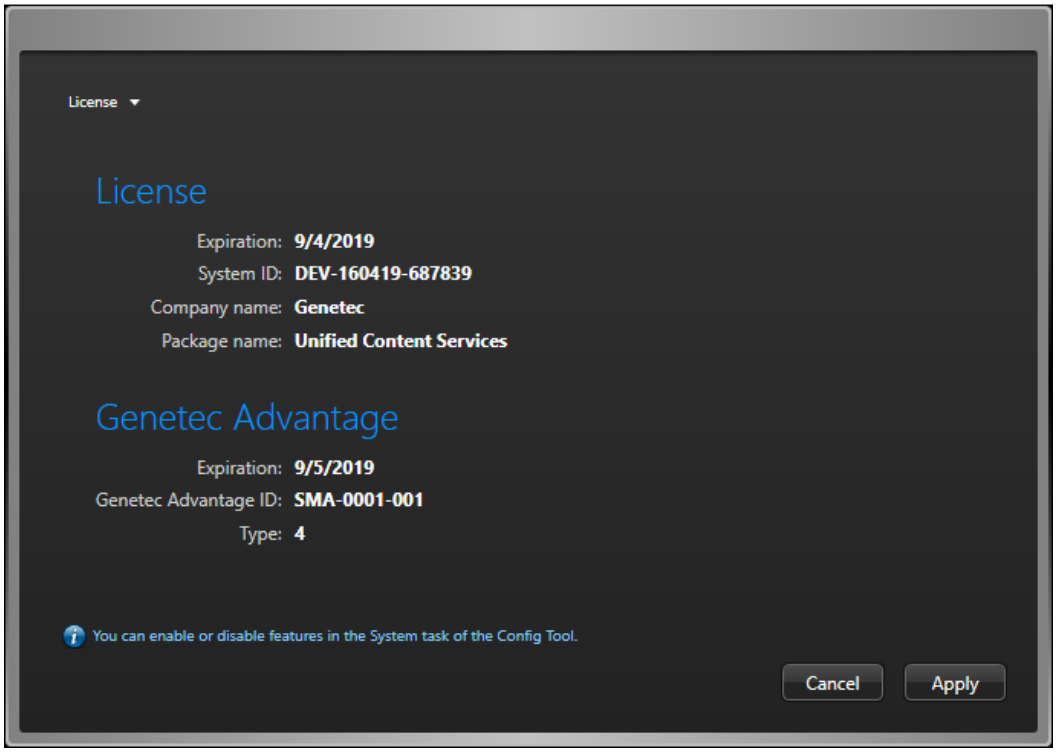
- **Ativação pela Internet:** (Recomendável) Reative a sua licença pela Internet.

  Na caixa de diálogo que aparece, digite seu *ID do sistema* e *Senha* e clique em **Ativar**.

- **Ativação Manual:** Se a sua estação de trabalho do Config Tool não possuir acesso à Internet, reative manualmente a sua licença do Security Center usando um arquivo de licença.

IMPORTANTE: Envie a chave de validação composta (compreendendo todos os servidores do Directory); caso contrário, a reativação da licença falhará silenciosamente e o failover do Directory não funcionará.

Uma caixa de diálogo mostrando suas informações de licença será exibida.



Na lista suspensa **Licença**, você pode selecionar uma opção para visualizar o que está incluído na sua licença.

5 Clique em **Aplicar** para fechar a caixa de diálogo e, em seguida, clique em **Aplicar** na parte inferior da janela do Config Tool para salvar suas alterações.

Reativar a licença do Security Center usando um arquivo de licença

Para reativar a sua licença do Security Center para as alterações feitas na lista de servidores do Directory enquanto a estação de trabalho do Config Tool não possui acesso à Internet, use uma segunda estação de trabalho para baixar o arquivo de licença do GTAP e, em seguida, aplique o arquivo da licença usando a sua primeira estação de trabalho.

O que você deve saber

Esse procedimento encaixa no contexto de reativar a sua licença do Security Center em um sistema com failover do Directory.

Para atualizar sua licença usando um arquivo de licença:

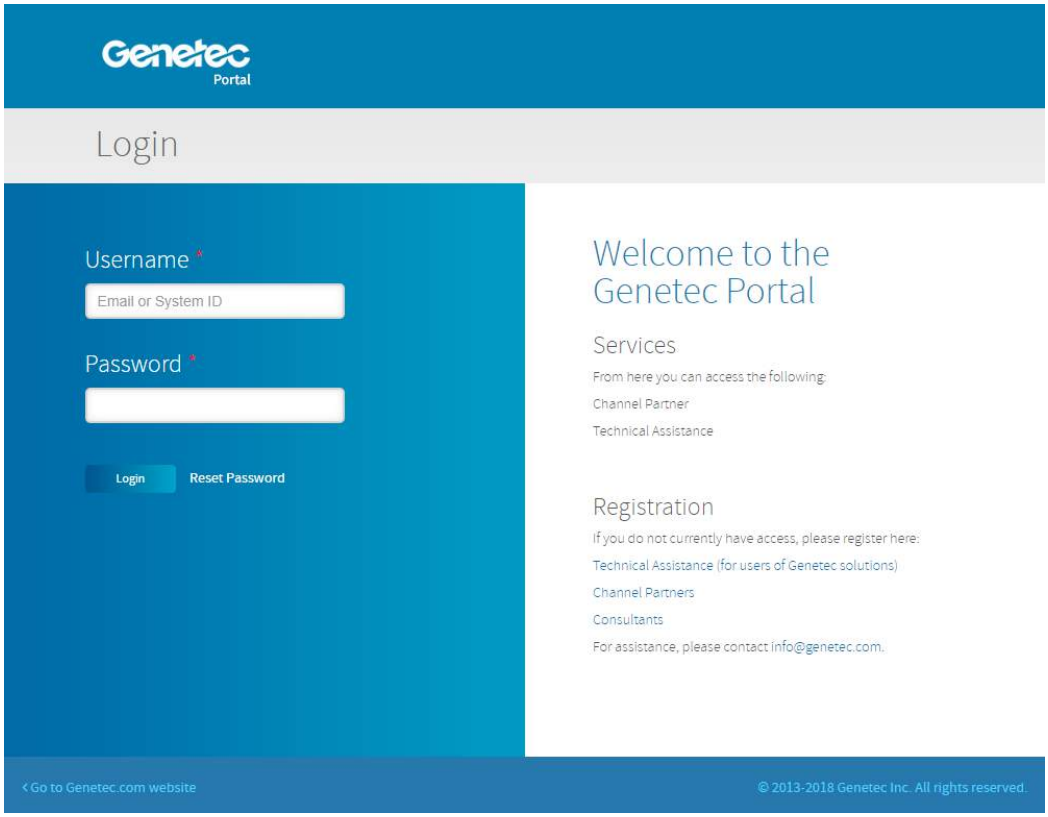
1 Na caixa de diálogo *Gerenciamento de licenças*, clique em **Salvar no arquivo** para salvar a chave de validação composta em um arquivo.

A chave de validação é uma sequência de números (em formato de texto hexadecimal) gerada pelo Security Center que identifica todos os servidores do Directory de forma exclusiva. A chave de validação é usada para gerar a chave de licença que desbloqueia o software Security Center. A chave de licença que é gerada só pode ser aplicada aos servidores identificados pela chave de validação.

Um arquivo de texto chamado *validation.vk* é salvo em sua pasta de *Downloads* padrão. Certifique-se de copiar este arquivo para um local (isso pode ser uma chave USB) que possa acessar de outro computador que tenha acesso à Internet.

2 Passe para o computador que tem acesso à Internet.

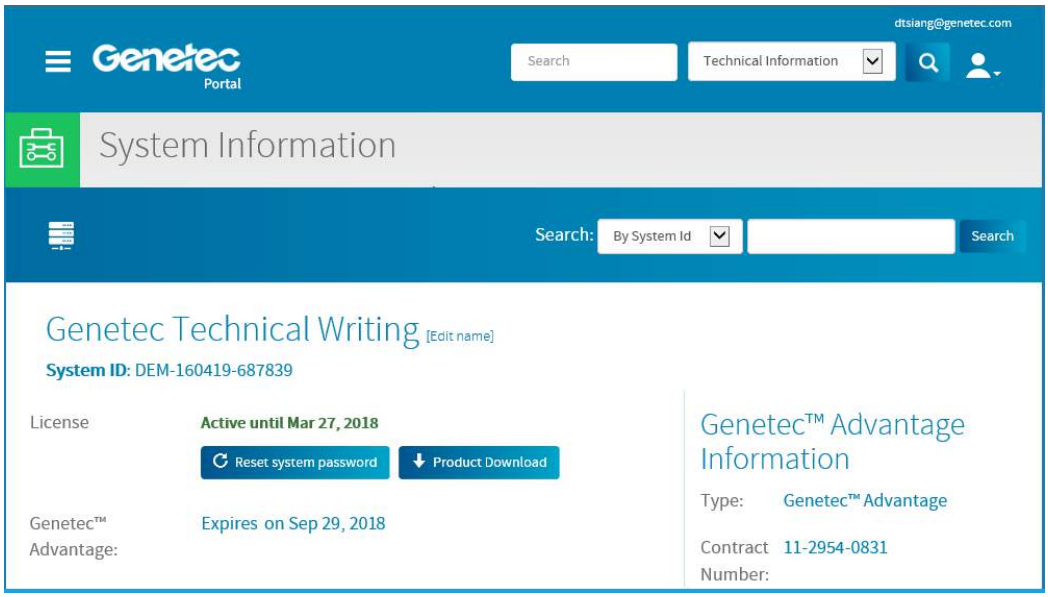
3 De outro computador com acesso à Internet, faça logon no GTAP em: https://gtap.genetec.com.



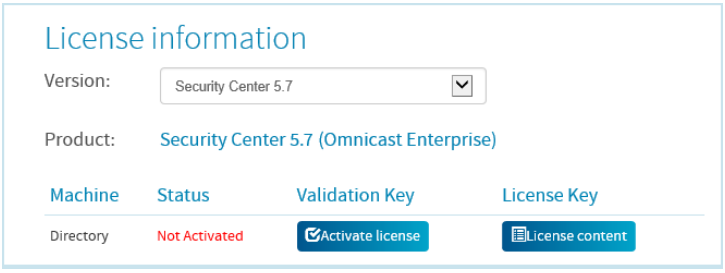
4 Na página de Login do GTAP, faça uma das seguintes opções:

- Digite o ID do sistema e a senha especificada no documento *Informações de Licença do Security Center* e clique em **Login**.
- Digite sua conta de usuário GTAP (seu endereço de e-mail) e senha e clique em **Login**.
  1 Na página *Genetec™ Portal - Portais*, clique em **Página Inicial de Assistência Técnica** > **Ativar novo sistema**.
  2 Na lista suspensa **ID do sistema**, selecione seu sistema e clique em **Enviar**.

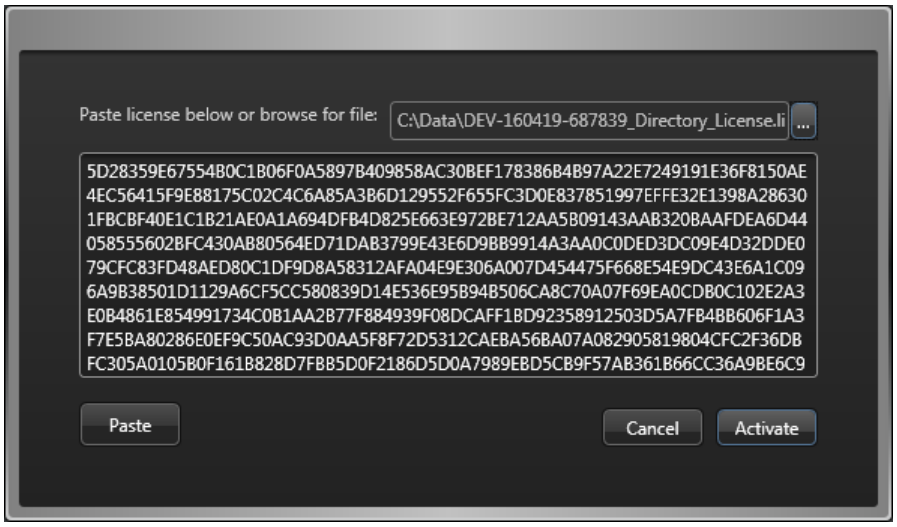
O navegador é aberto na página *Informações do Sistema*.



5 Role para baixo até a seção *Informações de licença* e clique em **Ativar licença**.



6 Na caixa de diálogo que abre, procure a sua chave de validação (arquivo .vk) e clique em **Enviar**.
A mensagem *Ativação de licença bem-sucedida* é exibida.
7 Clique em **Baixar licença** e salve a chave de licença em um arquivo.
O nome padrão é o ID do sistema seguido de *_Directory_License.lic*.
8 Retorne para a estação de trabalho do Config Tool.
9 Na caixa de diálogo *Gerenciamento de licenças*, clique em **Ativação manual**.
10 Na caixa de diálogo *Ativação manual*, procure o arquivo de chave de licença e clique em **Abrir**.



11 Clique em **Ativar**.

Removendo servidores da lista de failover do Directory.

Se você não precisar mais de um servidor como servidor do Directory para o failover do Directory ou balanceamento de carga, você pode removê-lo da lista de failover do Directory.

O que você deve saber

Não tente remover um servidor da lista de failover do Directory desativando o Directory naquele servidor do Server Admin. Sua alteração não será permanente, porque o Directory Manager fará com que ele volte a ser um servidor do Directory.

Para remover um servidor da lista de failover do Directory:

1. Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.
2. Selecione a função **Directory Manager** ( ) e clique na aba **Servidores do Directory**.
3. Selecione os servidores que você deseja remover e clique em **Remover o item** ( ).
4. Atualize sua licença para excluir os servidores que você acabou de remover.
5. Clique em **Aplicar**.

Os servidores removidos se tornam servidores de expansão e a licença atualizada é aplicada para todos os servidores do Directory restantes. Os usuários não podem mais se conectar ao sistema usando os servidores que foram removidos. Clientes conectados ao Security Center através desses servidores são desconectados e reconectados aos servidores do Directory restantes.

Exemplo

Você acaba de adicionar um novo computador ao seu sistema e deseja usar o servidor naquele computador como um servidor do Directory; porém, você já está usando cinco servidores do Directory. Você pode remover um dos servidores existentes da lista de failover do Directory para dar espaço para o novo servidor.

Ignorar o balanceamento de carga em estações de trabalho

Se você tiver mais de um servidor do Directory em seu sistema, mas não quiser que os usuários sejam redirecionados para outro servidor quando eles fizerem logon no Security Center, você poderá ignorar o balanceamento de carga.

O que você deve saber

Quando você tem mais de um servidor do Directory em seu sistema, o balanceamento de carga automaticamente fica em efeito. Isso significa que cada vez que um usuário faz logon no Security Center, o Directory Manager redireciona sua solicitação de logon para o próximo servidor do Directory na lista, com base no servidor ao qual o usuário anterior se conectou.

Você pode ignorar o balanceamento de carga em estações de trabalho específicas (aplicadas para o Config Tool e o Security Desk), o que é útil quando um cliente está em uma LAN remota.

Para ignorar o balanceamento de carga em uma estação de trabalho:

1 Na página inicial, clique em **Opções** > **Geral**.
2 Selecione a opção **Evitar redirecionamento da conexão para servidores do Directory diferentes**.
3 Clique em **Salvar**.

Failover de banco de dados do Directory

Você pode realizar o failover do banco de dados do Directory usando o modo de failover de backup e restauração no modo de failover de espelhamento.

Três modos de failover do banco de dados são suportados para o Directory:

- **Backup e restauração:** O Directory Manager protege o banco de dados do Directory fazendo backup regular da instância principal do banco de dados mestre (cópia de origem). Durante um failover, os backups mais recentes são restaurados para o banco de dados de reserva que for o próximo da fila. Podem ser definidas duas agendas: uma para backups completos e outro para backups diferenciais.
- **Espelhando:** O failover de banco de dados é tratado pelo Microsoft SQL Server e é transparente para o Security Center. As instâncias *Principal* e *Espelho* do banco de dados do Directory são sempre mantidas em sincronia. Não há perda de dados durante o failover.
- **SQL AlwaysOn:** Use este modo de failover se você estiver usando o recurso do Windows SQL AlwaysOn como sua solução de alta disponibilidade e recuperação de desastres.

Limitações do modo de failover de backup e restauração

- Para preservar as alterações feitas à configuração do seu sistema enquanto você estava operando a partir do bancos de dados de backup, você deve restaurar o mais recente backup de contingência (criado na subpasta *ContingencyBackups* na pasta de restauração) para o seu banco de dados mestre antes de reativá-lo.
- Para evitar perder as alterações de configuração feitas enquanto você estava operando a partir do banco de dados reserva, você pode alterar o banco de dados reserva para ser o seu banco de dados mestre. Para fazer isso, selecione-o na lista de failover do banco de dados para movê-lo para o alto da lista. Porém, tenha em mente que o seu banco de dados reserva é apenas atualizado até a data do backup mais recente antes da ocorrência do failover.

Diferenças entre o modo de backup e restauração e o modo de espelhamento

A tabela a seguir compara as diferenças entre os dois modos de failover do banco de dados.

Backup e restauração (Directory Manager)	Espelhamento (Microsoft SQL Server)
Várias instâncias de backup do banco de dados do Directory são mantidas relativamente em sincronismo com sua instância mestre por meio de backups regulares executados pela função do Directory Manager.	Uma única cópia (a instância espelho) do banco de dados do Directory é mantida perfeitamente em sincronismo com a cópia mestre (ou instância principal) usando o espelhamento de banco de dados do SQL Server.
O banco de dados de failover somente pode ser tão atualizado quanto o backup mais recente.	O banco de dados do failover é uma cópia exata do banco de dados principal.
Alterações feitas enquanto o Directory está conectado ao banco de dados reserva são perdidas quando o Directory muda de volta para o banco de dados mestre.	Alterações podem ser feitas ao banco de dados do Directory a qualquer momento sem nunca perder dados.
Os bancos de dados mestre e de backup devem ser hospedados nos *servidores* do Security Center.	As instâncias de banco de dados principal e espelho podem ser hospedadas em qualquer computador.

Backup e restauração (Directory Manager)	Espelhamento (Microsoft SQL Server)
Pode funcionar com o SQL Server Express edition, que é gratuito.	Exige o SQL Server 2008 Standard Edition ou superior, que suporta espelhamento.
Recomendado quando as configurações da entidade não são atualizadas frequentemente.	Recomendado quando as configurações da entidade são atualizadas frequentemente, como para gerenciamento de titulares de cartão e de visitantes.
Causa uma desconexão temporária de todos os aplicativos e funções cliente enquanto o failover do banco de dados está em progresso.	Faz com que o Directory seja reiniciado se o servidor principal estiver indisponível por mais de alguns segundos.
O failover do banco de dados é gerenciado pela função Directory Manager.	O failover do banco de dados é executado por um *Servidor testemunha* separado que é executado no SQL Server Express (opcional, mas altamente recomendável) ou ele deve ser detectado e executado manualmente pelo administrador do banco de dados.

Tópicos relacionados

Configurar failover do banco de dados do Directory por backup e restauração na página 181
Configurar failover do banco de dados do Directory por espelhamento na página 183
Configurar failover de banco de dados do Directory através do SQL AlwaysOn na página 185

Configurar failover do banco de dados do Directory por backup e restauração

Para proteger o banco de dados do Directory por meio de backup regular da instância mestre do banco de dados, você pode configurar o failover do banco de dados do Directory usando o método de backup e restauração.

Antes de iniciar

- Sua licença do Security Center deve suportar múltiplos *servidores do Directory*. Caso precise atualizar sua licença, consulte o *Guia de Instalação e Atualização do Security Center*.

  NOTA: A função *Directory Manager* ( ) é criada automaticamente em Config Tool quando sua licença suporta múltiplos servidores do Directory.
- Todos os servidores de banco de dados devem ser acessíveis a partir de todos os servidores de Directory. Você deve configurar o servidor remoto do banco de dados (SQL Server) para aceitar solicitações de conexão das funções.
- Todas as instâncias do banco de dados devem ser da mesma versão e um servidor de expansão deve ser instalado em cada servidor de banco de dados. Para mais informações sobre como instalar servidores de expansão, consulte o *Guia de Instalação e Atualização do Security Center*.

O que você deve saber

Uma vez que o modo de failover de *Backup e restauração* seja ativado, você não precisará mais fazer backup do banco de dados do Directory a partir do Server Admin, mas sim a partir do Config Tool.

Alterações feitas à configuração do sistema enquanto você operava a partir do bancos de dados de backup não são restauradas automaticamente para o banco de dados mestre quando ele é restaurado para o serviço ativo.

Para usar backup e restauração como sua solução de failover do banco de dados do Directory

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.
2 Selecione a função Directory Manager ( ) e clique na aba **Failover de banco de dados**.
3 Alterne a opção **Usar failover de banco de dados** para **Ligado**.
4 Selecione **Backup e restauração** para **Modo de failover**.
5 Clique em **Adicionar um item** ( ).
6 Na caixa de diálogo que aparecerá, especifique o *servidor* Security Center, o *servidor do banco de dados*, a instância do banco de dados e a pasta para onde os arquivos de backup deverão ser copiados.

É possível atribuir quantos bancos de dados de backup quiser. Porém, quanto mais bancos de dados de backup você tiver, mais tempo levará para fazer o backup do conteúdo do banco de dados do Directory.

7 Clique em **OK**.

A nova instância do banco de dados é adicionada.

NOTA: O servidor identificado como **(Mestre)** é o que atualmente hospeda o banco de dados. O LED verde ( ) indica o bancos de dados atualmente ativo (não necessariamente o *mestre*).

8 Para forçar todos os servidores do Directory a se reconectar ao banco de dados mestre assim que ele voltar a ficar online após um failover, selecione a opção **Reconectar automaticamente ao banco de dados mestre**.

CUIDADO: Alterar o banco de dados ativo causa uma breve interrupção do serviço, e todas as alterações feitas à configuração do sistema enquanto o banco de dados mestre estava offline são perdidas. Use esta opção somente se você estiver pronto para perder as alterações feitas na configuração do sistema enquanto você operava pelo banco de dados de backup.

9 Em **Backup mestre**, especifique a frequência na qual o *backup completo* e o *backup diferencial* devem ser gerados.

Um backup diferencial contém apenas as transações do banco de dados feitas desde o backup anterior, portanto ele é muito mais rápido de gerar do que um backup completo. Backups diferenciais frequentes garantem que o banco de dados de backup esteja atualizado quando ocorrer um failover, mas podem levar mais tempo para serem restaurados.

10 Clique em **Aplicar**.

Após terminar

CUIDADO: Assim que o modo de failover de *Backup e restauração* esteja habilitado, todas as alterações subsequentes ao banco de dados mestre a partir do Server Admin (restaurar um backup anterior, por exemplo) deverão ser imediatamente seguidas por um backup manual completo executado a partir de Config Tool. Deixar de fazer isso fará com que os seus bancos de dados mestre e de backup percam o sincronismo e o mecanismo de failover do banco de dados deixe de funcionar.

Tópicos relacionados

Failover de banco de dados do Directory na página 179

Gerando backup completo do banco de dados do Directory

Uma vez que o modo de failover de *Backup e restauração* esteja ativado, todos os backups manuais do banco de dados do Directory devem ser realizados a partir da aba **Failover do banco de dados**do Directory Manager no Config Tool.

O que você deve saber

Se o modo de failover de *Backup e restauração* não estiver ativado, realize o backup do banco de dados do Directory a partir do Server Admin.

Para gerar um backup completo do banco de dados do Directory:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.

2 Selecione a função Directory Manager ( ) e clique na aba **Failover de banco de dados**.

3 Na seção *Backup mestre*, clique em **Gerar backup completo**.

Um backup completo do Directory é gerado na pasta de backup do Security Center (padrão=*C:\SecurityCenterBackup\Backups*). Todos os arquivos de configuração (arquivos *config*, *gconfig* e *xml*) também são incluídos no backup.

Configurar failover do banco de dados do Directory por espelhamento

Para proteger o banco de dados do Directory de modo que você não perca dados caso ocorra um failover, você pode configurar o failover de banco de dados do Directory para usar o Espelhamento de Banco de Dados do Microsoft SQL Server.

Antes de iniciar

- O Espelhamento de Banco de Dados da Microsoft está sendo descontinuado. Para novas instalações, é recomendado utilizar o SQL AlwaysOn.
- O servidor de banco de dados *Principal*, o servidor de banco de dados *Espelho* e o servidor *Testemunha* (O servidor *Testemunha* é opcional, mas altamente recomendado) devem ser configurados. Para configurar o SQL Server para espelhamento, consulte a documentação sobre Espelhamento de Banco de Dados do Microsoft SQL Server.
- Sua licença do Security Center deve suportar múltiplos *servidores do Directory*. Caso precise atualizar sua licença, consulte o *Guia de Instalação e Atualização do Security Center*.

  NOTA: A função *Directory Manager* ( ) é criada automaticamente em Config Tool quando sua licença suporta múltiplos servidores do Directory.
- Os servidores de banco de dados devem ser executados em computadores independentes dos servidores de Directory. Mova os bancos de dados para outros computadores.
- Todos os servidores de banco de dados devem ser acessíveis a partir de todos os servidores de Directory. Você deve configurar o servidor remoto de banco de dados (SQL Server) para aceitar solicitações de conexão das funções.
- Os bancos de dados *Principal* e *Espelho* devem ser da mesma versão. Para obter mais informações sobre espelhamento de bancos de dados, como orientações para realizar backup e restauração manual, consulte a documentação sobre Espelhamento de Banco de Dados do Microsoft SQL Server.

O que você deve saber

Com o espelhamento de bancos de dados, o failover de banco de dados é controlado pelo Microsoft SQL Server. As instâncias *Principal* e *Espelho* do banco de dados do Directory são sempre mantidos em sincronia. Não há perda de dados durante o failover.

NOTA: Após um failover de banco de dados, a primeira consulta a bancos de dados realizada por aplicativos clientes do Security Center provavelmente falhará. Quando uma consulta falha, a mensagem "A transação de banco de dados falhou" aparece na tela. Feche a janela da mensagem e tente retomar a operação normal novamente.

Para usar o Espelhamento de Banco de Dados como sua solução de failover de banco de dados do Directory:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.
2 Selecione a função Directory Manager ( ) e clique na aba **Failover de banco de dados**.
3 Alterne a opção **Usar failover de banco de dados** para **Ligado** e selecione a opção **Espelhamento**.

  O banco de dados ao qual você está conectado atualmente é o banco de dados *Principal*.

4 Em **Banco de dados espelho**, digite o nome do servidor de banco de dados para o banco de dados *Espelho*.
5 Clique em **Aplicar**.

Tópicos relacionados

Failover de banco de dados do Directory na página 179

Configurar failover de banco de dados do Directory através do SQL AlwaysOn

Se você estiver usando o recurso do Windows *SQL AlwaysOn* como sua solução de failover de banco de dados do Directory, você deverá configurar o Directory Manager para usar o SQL AlwaysOn no Config Tool.

Antes de iniciar

Todos os servidores de banco de dados devem ser acessíveis a partir de todos os servidores de Directory. Você deve configurar o servidor remoto de banco de dados (SQL Server) para aceitar solicitações de conexão das funções.

Para usar o SQL AlwaysOn como sua solução de failover de banco de dados do Directory:

1. Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.
2. Selecione a função Directory Manager () e clique na aba **Failover de banco de dados**.
3. Alterne a opção **Usar failover de banco de dados** para **Ligado** e selecione a opção **SQL AlwaysOn**.
4. Clique em **Aplicar**.

Tópicos relacionados

Failover de banco de dados do Directory na página 179

Failover do Archiver

Adicionar um servidor em espera à sua função Archiver minimiza o tempo ocioso de seu vídeo ao vivo caso ocorra uma falha de hardware.

Como o failover do Archiver funciona

Se o servidor que hospeda a função *Archiver* falhar, você perderá o acesso a vídeo ao vivo e a vídeo arquivado. O vídeo ao vivo fica desativado porque o Archiver controla as *unidades de vídeo*. O acesso a vídeo arquivado fica desativado porque seus arquivos somente podem ser acessados por meio do Archiver que os criou (mesmo que o seu *servidor do banco de dados* não seja o computador que falhou).

Para o failover do Archiver, as seguintes condições se aplicam:

- Você pode atribuir um servidor primário, um servidor secundário e um servidor terciário a uma função Archiver. Isso é especialmente útil em sistemas em vários locais, uma vez que você pode proteger os servidores primário e secundário em uma instalação local com um servidor terciário em uma instalação remota.
- Os servidores primário, secundário e terciário devem ter, cada um, seu próprio banco de dados, hospedado localmente ou em outro computador.
- Para garantir que o vídeo arquivado pelo *servidor primário* ainda esteja disponível se ele falhar para um servidor secundário ou terciário, você deverá ativar o *arquivamento redundante*. Isso garante que todos os servidores possam arquivar vídeo ao mesmo tempo e que cada um deles gerencie sua própria cópia do arquivo de vídeos. Você pode configurar o arquivamento redundante em todas as câmeras gerenciadas pela função Archiver ou proteger apenas algumas câmeras importantes

Planejamento de carga cuidadoso para failover

Se o failover ocorrer, o desempenho de um servidor em espera pode ser afetado pela carga adicional de arquivamento (número de câmeras, qualidade de vídeo e assim por diante) da nova função Archiver. Se o servidor em espera hospedar outras funções, isso também afetará a capacidade de arquivamento.

Ao selecionar um servidor como um servidor em espera para uma função Archiver, considere o seguinte:

- Se o servidor tiver outras funções, ele pode não ser capaz de absorver a carga total de outro servidor.

  DICA: Para reduzir a carga de failover em um servidor, crie várias funções Archiver, cada uma com menos unidades de vídeo. Além disso, configure todos os Archivers para compartilhar o mesmo servidor primário, mas para falharem para servidores secundários ou terciários diferentes.
- Quanto tempo se espera que um failover típico dure? Quanto mais um failover durar, mais espaço em disco adicional deverá ser reservado para arquivamento.
- Um servidor pode lidar com mais unidades de vídeo quando somente as funcionalidades de comando e controle são necessárias. Se o arquivamento de vídeo não for importante para todas as câmeras, você poderá associar todas as câmaras importantes a uma função Archiver e dar a ela uma *prioridade de arquivamento* maior do que o resto. Desse modo, se várias funções Archiver falharem para o mesmo servidor ao mesmo tempo, o arquivamento será mantido para as câmeras importantes.

Limitações para failover do Archiver

O processo de failover pode fazer com que demore 15–30 segundos até que as câmeras fiquem online novamente. Durante este tempo, não é possível exibir vídeo ao vivo e as funções de Archiver auxiliar não gravam. No entanto, a falha de vídeo gravado é mais curta: não mais que 5 segundos.

Se uma função Archiver (A) for configurada com um servidor secundário e um terciário, e o servidor secundário for compartilhado com outra função Archiver (B) que tenha maior prioridade de arquivamento, então, se ambos os servidores principais do Archiver falharem ao mesmo tempo, o servidor secundário

começará a arquivar para o Archiver com prioridade mais alta (B). Porém, esta configuração impede que a função Archiver (A) arquive nos servidores secundário ou terciário.

MELHOR PRÁTICA: Se houver uma configuração de servidor terciário para failover do Archiver, não compartilhe o servidor secundário se a função Archiver não tiver a prioridade de arquivamento mais alta. Se for necessário compartilhar um servidor em espera, compartilhe o terciário.

Tópicos relacionados

Criar Archivers auxiliares na página 458
Sobre arquivos de vídeos na página 520

Configurar failover do Archiver

Você pode configurar o failover da função Archiver para um servidor secundário se o servidor primário falhar, e para um servidor terciário se os servidores primário e secundário falharem. Isso permite manter o controle das unidades de vídeo, acessar vídeo ao vivo e minimizar potencial tempo ocioso.

Antes de iniciar

É necessária uma licença para atribuir um servidor terciário para o failover da função Archiver. Consulte Opções de licença no Security Center na página 1132 para maiores detalhes.

O que você deve saber

Os servidores atribuídos ao Archiver devem ser configurados separadamente e devem ter seu próprio sistema de banco de dados e armazenamento para o arquivo de vídeos.

Para configurar o failover da função Archiver:

1 Abra a tarefa **Vídeo** e selecione a função Archiver a configurar.

2 Clique na aba **Recursos** e, em seguida, clique em **Adicionar failover** ( ).

3 Na caixa de diálogo que aparecer, selecione um servidor e clique em **Adicionar**.

O servidor que você adicionou para failover se torna a aba do servidor secundário.

4 Na aba do servidor secundário, defina as configurações de banco de dados de arquivos e armazenamento de arquivos.

5 (Opcional) Se o servidor secundário também estiver em espera para outras funções Archiver, você poderá precisar ajustar as prioridades de arquivamento para servidores em espera.

6 (Opcional) Adicionar um servidor terciário no caso do servidor primário e do secundário falharem:

a) Clique na aba **Adicionar failover**.

b) Selecione um servidor terciário e clique em **Adicionar**.

O servidor que você adicionou para failover se torna a aba do servidor terciário.

c) Na aba do servidor terciário, defina as configurações de banco de dados de arquivos e armazenamento de arquivos.

d) (Opcional) Se o servidor terciário também estiver em espera para outras funções Archiver, você poderá precisar ajustar as prioridades de arquivamento para servidores em espera.

7 Clique em **Aplicar**.

8 Para que os servidores primário e de espera arquivem vídeo ao mesmo tempo, clique na aba **Configurações padrão de câmeras**, clique em **Exibir configurações avançadas** e alterne a opção **Arquivamento redundante** para **Ligado**.

Isso garante que o vídeo gravado seja armazenado em três locais, para garantir proteção adicional.

Tópicos relacionados

Failover do Archiver na página 186
Bancos de dados na página 138
Sobre arquivos de vídeos na página 520

Alterar a prioridade dos servidores para failover do Archiver

Você pode decidir qual Archiver é o servidor primário, qual é o secundário e qual é o terciário para failover.

Antes de iniciar

Você precisa ter pelo menos dois servidores atribuídos para a função Archiver.

O que você deve saber

CUIDADO: Para evitar perder vídeo, você deve alterar a prioridade do servidor para failover do Archiver em um momento em que o Archiver não estiver arquivando.

Para alterar a prioridade do servidor para o failover do Archiver:

1 Clique em **Failover** ( ) na parte inferior da aba **Recursos**.

Uma caixa de diálogo aparecerá, mostrando os servidores atribuídos a essa função Archiver.

2 Selecione um dos servidores na lista e clique em ou para movê-lo para cima ou para baixo na lista.

3 Clique em **OK** para fechar a caixa de diálogo **Failover**.

As abas dos servidores mudam de lugar.

4 Quando um servidor em espera hospeda outras funções Archiver, você pode precisar ajustar as prioridades de arquivamento para o servidor em espera.

5 Clique em **Aplicar**.

Atribuir prioridades de arquivamento para servidores em espera

Se todas as funções Archiver falharem ao mesmo tempo para o mesmo servidor em espera, você poderá atribuir prioridades de arquivamento às funções para evitar a sobrecarga do servidor.

O que você deve saber

O mesmo servidor pode ser designado como o servidor em espera para as várias funções Archiver. Se todas as funções Archiver falharem para o mesmo servidor ao mesmo tempo, sua carga combinada pode ser demais para o servidor lidar. Uma forma de evitar a sobrecarga de um servidor é atribuir uma prioridade de arquivamento mais baixa para as funções de menor importância para que elas não tenham que competir por recursos de computação.

NOTA: Em qualquer momento em um determinado servidor, apenas as funções Archiver com a prioridade de arquivamento mais alta serão capazes de arquivar. A prioridade de arquivamento afeta somente o arquivamento. Ter uma prioridade de arquivamento mais baixa não impede que uma função Archiver em falha execute suas funções de comando e controle.

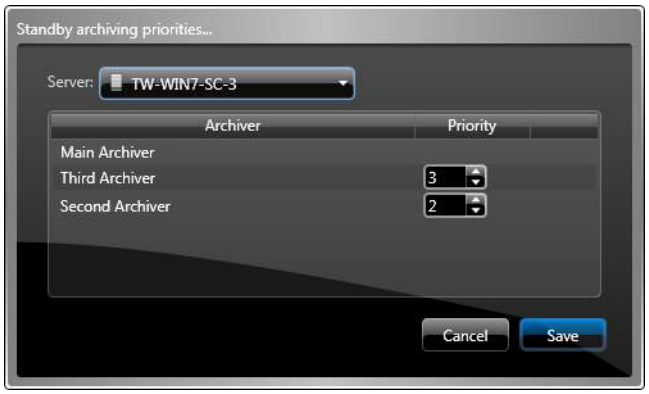
Para atribuir prioridades de arquivamento para servidores em espera:

1 Abra a tarefa **Vídeo** e selecione a função Archiver a configurar.

2 Clique na aba **Recursos** e, em seguida, clique em **Failover** ( ).

3 Na caixa de diálogo **Failover**, clique em **Prioridades de arquivamento em espera**.

4 Selecione um servidor na lista suspensa **Servidor**.



Todas as funções Archiver que dependem deste servidor como seu servidor primário ou *servidor secundário* são listadas. A prioridade de arquivamento somente pode ser definida quando o servidor é usado em espera. Para funções que dependam do servidor como seu *servidor primário*, a prioridade de arquivamento é implicitamente bloqueada para 1 (a mais alta).

5 Configure a prioridade das funções e clique em **Salvar**.

NOTA: A prioridade de arquivamento é específica de cada função Archiver em cada servidor. Quando a prioridade de arquivamento nunca tiver sido definida, seu valor padrão será 1.

6 Repita as etapas para configurar todos os servidores que hospedam funções Archiver em seu sistema.

Configurar um período de retenção diferente para o servidor de Archiver secundário

Você pode configurar um período de retenção diferente para o servidor secundário do Archiver (usado para failover ou redundância) para gerenciar mais precisamente a quantidade de armazenamento de dados. Você pode definir esta configuração no arquivo *Archiver.gconfig*.

O que você deve saber

- Um servidor redundante ou secundário do Archiver pode ter um período de retenção maior ou menor do que o servidor primário do Archiver.
- Se nenhum valor for especificado para o servidor secundário do Archiver, ou se o valor for igual a zero, o período de retenção do servidor primário do Archiver será aplicado.
- Se um período de retenção personalizado for configurado para determinada câmera, a configuração do Archiver é ignorada para aquela câmera.
- A configuração para o período de retenção redundante não se aplica a backups de arquivos.
- O novo período de retenção padrão do Archiver secundário é uma configuração da função. Os computadores com arquivamento primário e secundário devem ter o mesmo arquivo de configuração.

Para configurar um período de retenção diferente para o servidor do Archiver:

1. Abra o arquivo \<*Pasta de instalação*>*Configuration Files**Archiver.gconfig*.

   A pasta de instalação do Security Center encontra-se (por padrão) na seguinte localização: *C:\Program Files (x86)\Genetec Security Center 5.x*.
2. Configure o valor de *DefaultRetentionPeriodForSecondaryArchver* para o número de dias durante os quais deseja reter as gravações secundárias.

   Por exemplo: *<ArchiverRole DefaultRetentionPeriodForSecondaryArchiver="1" />* define o período de retenção secundário para um dia.
3. Salve o arquivo.
4. Reinicie o processo do Archiver para aplicar as alterações.

Gerar o arquivo Archiver.gconfig

Para modificar as configurações avançadas do Archiver que não estão definidas em Security Center do Config Tool, você deve gerar o *Archiver.gconfig*a partir do console Genetec™ Server.

Antes de iniciar

Se o arquivo *Archiver.gconfig* já existir, faça uma cópia de backup antes de gerar um novo arquivo. O novo arquivo *Archiver.gconfig* contém as configurações padrão do Archiver e sobrescreve o arquivo existente.

O que você deve saber

O arquivo *Archiver.gconfig* é criado no servidor que está hospedando a função Archiver. O arquivo é salvo no diretório de instalação do Security Center. A localização padrão é *C:\Program Files (x86)\Genetec Security Center 5.x\ConfigurationFiles*\ em um computador de 64 bits e em *C:\Program Files\Genetec Security Center 5.x \ConfigurationFiles*\ em um computador de 32 bits.

As configurações no arquivo *Archiver.gconfig* aplicam-se a todas as funções Archiver hospedadas no servidor.

CUIDADO: Você deve apenas gerar o *Archiver.gconfig* se souber que configuração deve alterar ou adicionar. Se a sintaxe neste arquivo estiver incorreta, as funções Archiver que estão hospedadas neste servidor não serão iniciadas.

Para gerar um arquivo *Archiver.gconfig*:

1 Abra o Server Admin usando um navegador da Web e faça login.
2 Na seção *Servidores* da página *Visão Geral*, selecione o servidor da função Archiver.
3 Junto ao nome do servidor, clique em **Ações** > **Console**.
4 Clique na aba **Comandos**.
5 Expanda **Comandos da Função Archiver** e, em seguida, clique em **GenerateConfigFile**.

Consolidar arquivos de vídeo após failover do Archiver

Se o seu servidor Archiver principal ficar offline e o failover ocorrer, depois que o servidor seja reiniciado, você pode consolidar arquivos de vídeo do período em que esteve offline. Para isso, use o recurso *consolidação de arquivos* para duplicar os arquivos de vídeo do Archiver secundário ou terciário para o Archiver principal.

Antes de iniciar

O failover de Archivers deve ser configurado.

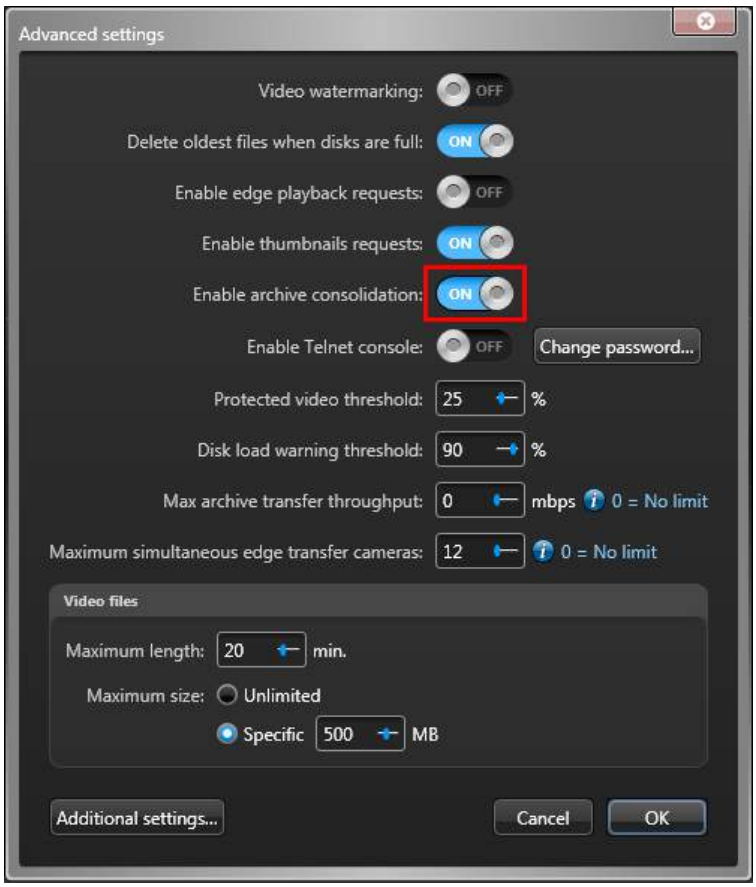
O que você deve saber

Por padrão, o servidor de Archiver primário verifica a cada hora se existem arquivos de vídeos que possam ser consolidados dos servidores secundário e terciário. A consolidação de arquivos é executada em todas as câmeras controladas pelo Archiver.

Se a consolidação de arquivos estiver habilitada e você alterar o servidor Archiver principal, os arquivos que estejam ausentes da linha de tempo do novo servidor principal são copiados dos servidores secundário e terciário, se os arquivos estiverem disponíveis.

Para consolidar arquivos de vídeo após um failover do Archiver:

1. Na página inicial do Config Tool, abra a tarefa **Vídeo** e selecione o Archiver que deseja configurar.
2. Clique na aba **Recursos** e, em seguida, clique em **Configurações avançadas**.
3. Na caixa de diálogo *Configurações avançadas*, coloque a opção **Habilitar consolidação de arquivos** em **Ligado**.



4 Clique em **OK** > **Aplicar**.

O recurso de consolidação de arquivos é habilitado e um *Grupo de transferência de consolidação padrão* é criado. Se o servidor Archiver principal falhar ou reiniciar, os arquivos de vídeo dos servidores em espera são transferidos para preencher as falhas a cada hora, se houver arquivos disponíveis.

5 (Opcional) Para ver o *Grupo de transferência de consolidação padrão* e suas configurações de transferência no Config Tool, faça o seguinte:

a) Abra o arquivo *GeneralSettings.gconfig* localizado na pasta de instalação do Security Center.

A localização padrão é *C:\Program Files (x86)\Genetec Security Center 5.7* em um computador de 64 bits e *C:\Program Files\Genetec Security Center 5.7* em um computador de 32 bits

b) Adicione a linha de código a seguir:

```
<archiveTransfer ViewArchiveConsolidationTransfer="true" />
```

c) Salve o arquivo.

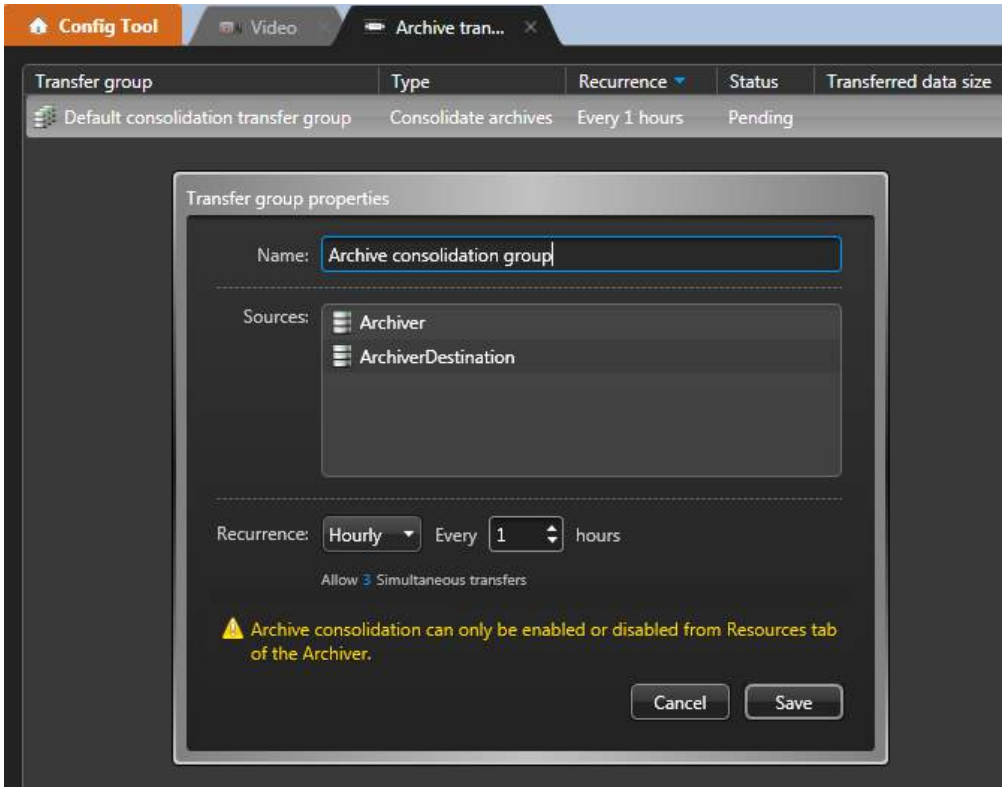
Você pode agora visualizar o *Grupo de transferência de consolidação padrão* na tarefa *Transferência de arquivos* no Config Tool.

6 (Opcional) Se você desejar alterar as configurações de transferência de vídeo, faça o seguinte:

a) Abra a tarefa *Transferência de arquivos*.

b) Clique duas vezes em **Grupo de transferência de consolidação padrão**.

c) Na caixa de diálogo *Propriedades do grupo de transferência*, digite um novo nome para o grupo no campo **Nome**.



d) Na opção **Recorrência**, selecione com que frequência você deseja que a transferência ocorra:

e) Na opção **Permitir n transferências simultâneas**, selecione o número de câmeras das quais transferir vídeo simultaneamente.

f) Clique em **Salvar**.

Tópicos relacionados

Transferir arquivos de vídeo na página 527

Solução de problemas do failover

Se tiver problemas ao configurar o failover para o seu sistema, há algumas coisas que você pode verificar para resolver os problemas.

Solução de problemas do failover:

1. Certifique-se de que as portas corretas estejam abertas na sua rede (ver Portas usadas por aplicativos principais no Security Center na página 1137).
2. Certifique-se de que suas conexões a bancos de dados estejam devidamente configuradas e que os servidores sendo usados para failover possam se comunicar com o servidor de banco de dados (ver Conectar funções a servidores de bancos de dados remotos na página 140).
3. Certifique-se de que o caminho do banco de dados esteja correto na página Server Admin - Servidor principal.
4. Certifique-se de que os serviços do Genetec™ Server e do Microsoft SQL Server estejam em execução em uma conta de administrador local do Windows (ver Conectar funções a servidores de bancos de dados remotos na página 140).
5. (Somente failover de banco de dados do Directory usando o método de Backup/Restauração) Certifique-se de que a conta de usuário tenha acesso para gravação/leitura na pasta de backup.
6. (Somente failover de banco de dados do Directory usando o método de Backup/Restauração) Certifique-se de que o Server Security Center esteja instalado no servidor remoto do banco de dados.

   Para mais informações sobre como instalar servidores de expansão, consulte o *Guia de Instalação e Atualização do Security Center*.

9

Automação do sistema

Esta seção inclui os seguintes tópicos:

- "Sobre agendamentos" na página 197
- "Criando agendamentos" na página 199
- "Sobre eventos" na página 205
- "Atribuir cores a eventos" na página 206
- "Criar eventos personalizados" na página 207
- "Criar eventos causa-efeito" na página 208
- "Adicionar condições ao criar eventos causa-efeito para eventos de análise de vídeo" na página 209
- "Elementos usados em condições de evento causa-efeito para eventos de análise de vídeo" na página 211
- "Adicionar condições ao criar eventos causa-efeito para reconhecimento de placas de veículos" na página 213
- "Elementos usados em condições de evento causa-efeito para leituras de placas de veículos" na página 215
- "Modificar eventos causa-efeito" na página 217
- "Tarefas agendadas" na página 218
- "Agendar tarefa" na página 219
- "Adicionar arquivos de áudio" na página 220
- "Sobre macros" na página 221
- "Criar macros" na página 222

Sobre agendamentos

Uma agenda é um tipo de entidade que define um conjunto de restrições de tempo que pode ser aplicado a várias situações no sistema. Cada restrição de tempo é definida por uma cobertura de datas (diária, semanal, ordinal ou específica) e uma cobertura de horário (todo o dia, intervalo fixo, durante o dia e durante a noite).

Cada restrição de tempo é caracterizada por uma cobertura de datas (padrão de datas ou datas específicas cobertas por um agendamento) e uma cobertura do tempo (períodos de tempo que se aplicam durante um dia de 24 horas).

Quando o Directory Security Center está instalado, o agendamento *Sempre* é criado por padrão. Esse agendamento tem uma cobertura de 24 horas/7 dias por semana. Não pode ser renomeado, modificado ou excluído e tem a menor prioridade em relação a resolução de conflitos de agendamento.

Fuso horário para agendamentos

A hora do dia para um agendamento se baseia no fuso horário local definido em cada contexto individual onde é aplicado. Por exemplo, se o agendamento é usado para definir uma gravação contínua de vídeo das 9:00 às 17:00, quer a *unidade de vídeo* esteja em Tóquio ou em Londres, a gravação ocorrerá no agendamento de acordo com o horário local. Isso ocorre porque cada unidade de vídeo tem uma configuração de fuso horário para controlar as configurações de vídeo e gravações relativas ao horário local da unidade.

Quando um agendamento é aplicado a uma entidade que não tenha configurações de fuso horário, como o agendamento de logon para um usuário, o horário local é tirado do *servidor* que hospeda a função Directory.

Conflitos de agendamento

É possível ter um conflito de agendamento quando dois agendamentos que se sobrepõem são aplicados à mesma função. Por exemplo, se dois agendamentos se aplicarem à gravação da mesma *câmera*.

Security Center pode resolver alguns desses conflitos dando prioridade ao agendamento mais específico (ou restritivo). A especificidade de um agendamento é determinada por sua opção de cobertura de datas.

Segue uma lista de opções de cobertura de data em ordem decrescente de prioridade:

1 Específico (Executado apenas uma vez. Prioridade mais alta)
2 Ordinal (Repetição mensal ou anual)
3 Semanal (Repetição semanal)
4 Diário (Repetição todos os dias)
5 Sempre (Agendamento padrão. Tem a menor prioridade)

IMPORTANTE: Quando dois agendamentos que se sobrepõem com o mesmo nível de prioridade são aplicados à mesma função, ocorre um conflito não resolvido. Se dois agendamentos tiverem sido aplicados a uma entidade, um *Aviso de entidade* ocorrerá e a entidade com a configuração conflitante é exibida em amarelo no navegador de entidades.

Tópicos relacionados

Personalizar configurações de fuso horário na página 55

Sobre agendas vespertinas

É um tipo de entidade de agendamento que suporta coberturas durante o dia e a noite. Esse cronograma não pode ser usado em todas as situações. Sua utilidade principal é controlar comportamentos relacionados a vídeo.

Benefícios de agendamentos vespertinos

Agendamentos vespertinos são feitos para situações em que a luz do sol tenha um impacto sobre a operação do sistema, como configurações de vídeo e gravação. Alguns usos típicos dos agendamentos vespertinos são os seguintes:

- Gravar vídeos apenas durante o dia.
- Aumentar a sensibilidade do *codificador de vídeo* depois do pôr do sol.
- Desativar a *detecção de movimento* durante o período noturno.

Limitações de agendamentos vespertinos

Os agendamentos vespertinos têm as seguintes limitações:

- Eles não podem ser usados em nenhuma situação envolvendo entidades de controle de acesso.
- A entidade à qual a agenda se aplica deve ter uma configuração de localização geográfica, como unidades de vídeo e *unidades de LPR*.
- A opção *Semanalmente* para cobertura de data não está disponível.
- As opções *Dia inteiro* e *Intervalo* para cobertura de tempo não estão disponíveis.
- Eles não ficam visíveis em contextos onde não são aplicáveis.

Tópicos relacionados

Configuração de locais geográficos de entidades na página 74

Criando agendamentos

Para definir um conjunto de restrições de tempo para uma infinidade de situações, como quando um usuário pode fazer logon no sistema ou quando o vídeo de uma câmera de vigilância pode ser gravado, você pode criar agendamentos e, em seguida, aplicá-los a entidades específicas.

O que você deve saber

Quando o Directory Security Center está instalado, o agendamento *Sempre* é criado por padrão. Esse agendamento tem uma cobertura de 24 horas/7 dias por semana. Não pode ser renomeado, modificado ou excluído e tem a menor prioridade em relação a resolução de conflitos de agendamento.

Se você quiser usar agendamentos para qualquer uma das suas configurações no Security Center, deverá criar os agendamentos com antecedência.

Para criar um agendamento:

1 Abra a tarefa **Sistema** e clique na visualização **Agendamentos**.
2 Clique em **Agendamento** (), digite um nome para o agendamento e em seguida pressione **ENTER**.
3 Na aba **Identidade**, digite as propriedades básicas do agendamento e clique em **Aplicar.**
4 Clique na guia **Propriedades.**
5 Na lista suspensa **Cobertura de data**, escolha um dos seguintes:
   - **Diariamente:** Define um padrão que se repete diariamente.
   - **Semanalmente:** Define um padrão que se repete semanalmente. Cada dia da semana pode ter uma cobertura de tempo diferente. Esta opção não está disponível para agendamentos de crepúsculo.
   - **Ordinal:** Define uma série de padrões que se repetem mensalmente ou anualmente. Cada padrão de data pode ter uma cobertura de tempo diferente. Por exemplo, no dia 1° de julho de cada ano, no primeiro domingo de cada mês, ou na última sexta-feira de outubro de cada ano.
   - **Específico:** Define uma lista de datas específicas no futuro. Cada data pode ter uma cobertura de tempo diferente. Esta opção é ideal para eventos especiais que ocorrem apenas uma vez.

   NOTA: Os agendamentos *Diário*, *Ordinal* e *Específico* permitem que você defina configurações vespertinas.
6 Clique em **Aplicar**.

Definir agendas diárias

Para definir um conjunto de restrições de tempo para situações que ocorrem diariamente, você pode definir agendamentos diários e, em seguida, aplicá-los a entidades.

O que você deve saber

Os intervalos de tempo são mostrados como blocos coloridos em uma grade de tempo. Cada bloco representa 30 minutos. Ao clicar e manter pressionado o botão esquerdo do mouse, aparece uma janela de pop-up. Cada bloco na grade representa um minuto.

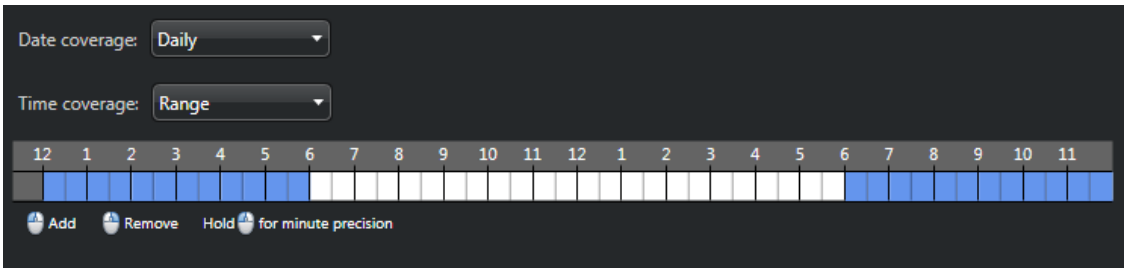
Para definir um agendamento diário:

1 Abra a tarefa **Sistema** e clique na visualização **Agendamentos**.
2 Clique em **Agendamento** (), digite um nome para o agendamento e em seguida pressione **ENTER**.
3 Na aba **Identidade**, digite as propriedades básicas do agendamento e clique em **Aplicar.**
4 Clique na guia **Propriedades.**
5 Na lista suspensa **Cobertura de data**, selecione **Diariamente**.
6 Na lista suspensa **Cobertura de tempo**, selecione **Dia inteiro** ou **Intervalo**.

7 Usando a grade de tempo, ajuste a cobertura de tempo como segue:
   - Para selecionar blocos de tempo, clique com o botão esquerdo do mouse.
   - Para remover blocos de tempo, clique com o botão direito do mouse.
   - Para selecionar ou remover um bloco de tempo sucessivo, clique e arraste com o mouse.
   - Para ampliar a grade de tempo e selecionar minutos específicos, clique e mantenha pressionado o botão esquerdo do mouse.
8 Clique em **Aplicar**.

Exemplo

O exemplo seguinte mostra uma agenda diária das 18:00 às 6:00. A grade de tempo mostra um dia com 24 horas em blocos de 30 minutos.



Definir agendas semanais

Para definir um conjunto de restrições de tempo para situações que ocorrem semanalmente, você pode definir agendamentos semanais e, em seguida, aplicá-los a entidades.

O que você deve saber

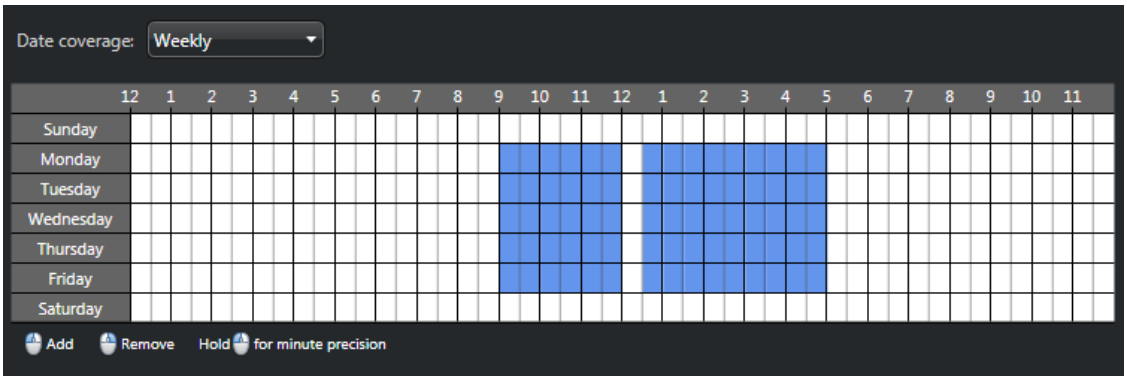
Os intervalos de tempo são mostrados como blocos coloridos em uma grade de tempo. Cada bloco representa 30 minutos. Ao clicar e manter pressionado o botão esquerdo do mouse, aparece uma janela de pop-up. Cada bloco na grade representa um minuto.

Para definir um agendamento semanal:

1 Abra a tarefa **Sistema** e clique na visualização **Agendamentos**.
2 Clique em **Agendamento** ( ), digite um nome para o agendamento e em seguida pressione **ENTER**.
3 Na aba **Identidade**, digite as propriedades básicas do agendamento e clique em **Aplicar.**
4 Clique na guia **Propriedades.**
5 Na lista suspensa **Cobertura de data**, selecione **Semanal**.
6 Usando a grade de tempo, ajuste a cobertura de tempo como segue:
   - Para selecionar blocos de tempo, clique com o botão esquerdo do mouse.
   - Para remover blocos de tempo, clique com o botão direito do mouse.
   - Para selecionar ou remover um bloco de tempo sucessivo, clique e arraste com o mouse.
   - Para ampliar a grade de tempo e selecionar minutos específicos, clique e mantenha pressionado o botão esquerdo do mouse.
7 Clique em **Aplicar**.

Exemplo

O exemplo a seguir mostra uma agenda semanal das 9:00 às 17:00, de segunda a sexta-feira, com uma pausa de meia hora entre 12:00 e 12:30.



Definir agendas ordinais

Para definir um conjunto de restrições de tempo para situações que incluem um série de padrões repetitivos, cada um com uma cobertura de tempo diferente, você pode definir agendamentos ordinais e, em seguida, aplicá-los a entidades.

O que você deve saber

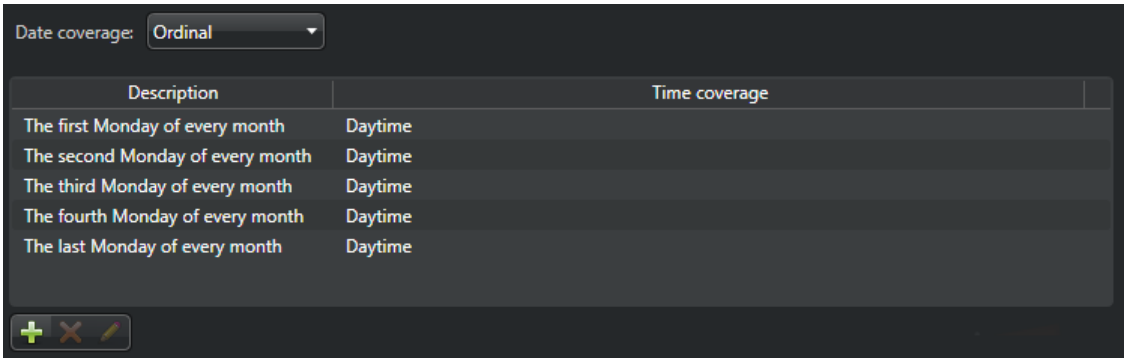
Agendamentos ordinais são ideais para eventos que se repetem. Você pode definir quantas datas forem necessárias dentro de uma única entidade de agendamento.

Para definir um agendamento ordinal:

1 Abra a tarefa **Sistema** e clique na visualização **Agendamentos**.
2 Clique em **Agendamento** (), digite um nome para o agendamento e em seguida pressione **ENTER**.
3 Na aba **Identidade**, digite as propriedades básicas do agendamento e clique em **Aplicar.**
4 Clique na guia **Propriedades.**
5 Na lista suspensa **Cobertura de data**, selecione **Ordinal** e, em seguida, clique em **Adicionar um item** ().
6 Selecione um dia e um mês.
7 Na lista suspensa **Cobertura de tempo**, selecione **Dia inteiro**, **Intervalo**, **Diurno** ou **Noturno** (consulte Definir agendas vespertinas para obter informações sobre coberturas diurnas e noturnas).
8 Clique em **OK** e, em seguida, clique em **Aplicar**.

Exemplo

Você pode configurar algo similar ao padrão *Semanal* usando o padrão *Ordinal*. O exemplo a seguir mostra um agendamento que cobre o período diurno de cada segunda-feira do ano.



Definir agendas com datas específicas

Para definir um conjunto de restrições de tempo para situações que ocorrerão em datas específicas, onde cada data pode ter uma cobertura de tempo diferente, você pode definir agendamentos com datas específicas e, em seguida, aplicá-los a entidades.

O que você deve saber

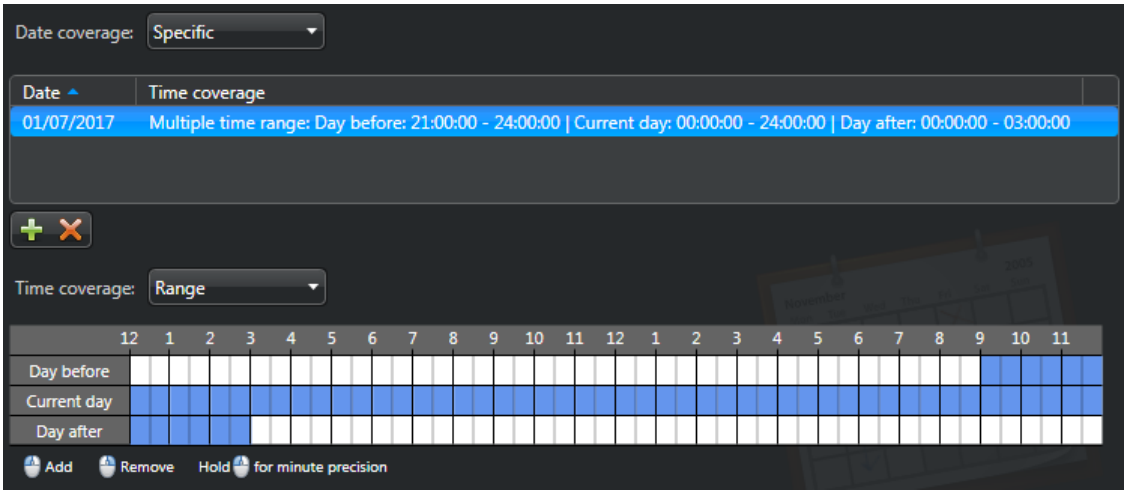
Você pode definir um intervalo de tempo diferente para cada data no agendamento.

Para definir um agendamento com data específica:

1 Abra a tarefa **Sistema** e clique na visualização **Agendamentos**.
2 Clique em **Agendamento** (), digite um nome para o agendamento e em seguida pressione **ENTER**.
3 Na aba **Identidade**, digite as propriedades básicas do agendamento e clique em **Aplicar.**
4 Clique na guia **Propriedades.**
5 Na lista suspensa **Cobertura de data**, selecione **Específica** e, em seguida, clique em **Adicionar um item** ().
6 Selecione datas no calendário e clique em **Fechar**.
7 Selecione uma entrada e, na lista suspensa **Cobertura de tempo**, faça um dos seguintes:
   - Selecione **Dia inteiro**.
   - Selecione **Intervalo** e, em seguida, selecione horários específicos na grade para o *Dia anterior*, o *Dia atual* ou o *Dia seguinte*.
   - Selecione **Diurno** ou **Noturno** (consulte Definir agendas vespertinas para obter informações sobre coberturas diurnas e noturnas).
8 Clique em **Aplicar**.

Exemplo

O exemplo a seguir mostra uma agenda específica que abrange 1 de julho de 2017 das 9:00 do dia anterior às 3:00 do dia seguinte.



Definir agendas vespertinas

Para definir um conjunto de restrições de tempo para situações que cobrem o período diurno ou noturno, onde o cálculo de exatamente quando o sol nasce e se põe se baseia em uma localização geográfica (latitude e longitude), você pode definir agendamentos vespertinos.

O que você deve saber

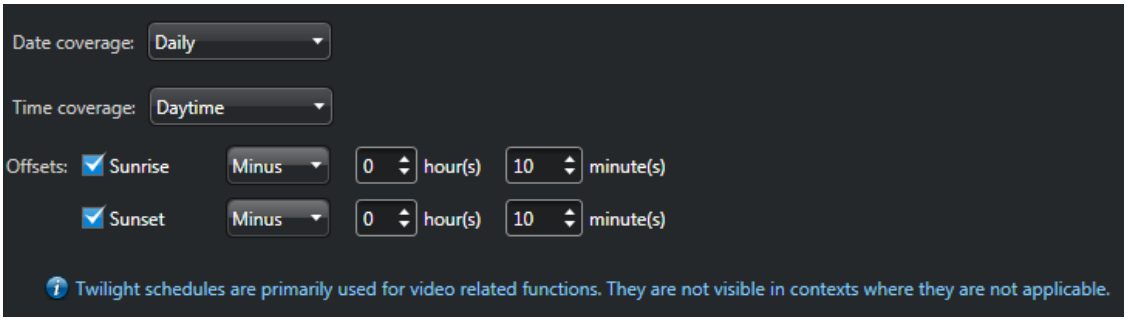
Agendamentos vespertinos são feitos para situações em que a luz do sol tenha um impacto sobre a operação do sistema, como configurações de vídeo e gravação.

Para definir um agendamento vespertino:

1 Abra a tarefa **Sistema** e clique na visualização **Agendamentos**.
2 Clique em **Agendamento** ( ), digite um nome para o agendamento e em seguida pressione **ENTER**.
3 Na aba **Identidade**, digite as propriedades básicas do agendamento e clique em **Aplicar.**
4 Clique na guia **Propriedades.**
5 Na lista suspensa **Cobertura de data**, selecione **Diária**, **Específica** ou **Ordinal**.
6 Se você selecionar **Específica** ou **Ordinal**, defina a cobertura de data.
7 Na lista suspensa **Cobertura de tempo**, selecione **Diurno** ou **Noturno**.
8 Selecione as opções **Nascer do sol** ou **Pôr do sol** e selecione a quantidade de tempo para compensar o horário do nascer do sol ou do pôr do sol (até 2 horas antes ou depois).

Exemplo

O exemplo a seguir mostra uma agenda diária usando uma cobertura *Diurno*. A cobertura de tempo começa 10 minutos após o nascer do sol e termina 10 minutos antes do sol se por.


Date coverage:
Daily
Time coverage:
Daytime
Offsets:
Sunrise
Minus
0
hour(s)
10
minute(s)
Sunset
Minus
0
hour(s)
10
minute(s)
Twilight schedules are primarily used for video related functions. They are not visible in contexts where they are not applicable.

Sobre eventos

Um evento indica a ocorrência de uma atividade ou um incidente, como acesso negado a um titular de cartão ou movimento detectado em uma câmera. Os eventos são automaticamente registrados no Centro de Segurança e podem ser programados para disparar ações. Todo evento foca, principalmente, em uma entidade, chamada origem do evento.

Os eventos podem surgir de muitas fontes, como gravação iniciada por um usuário em uma câmera, uma porta sendo deixada aberta por muito tempo, ou uma tentativa de usar uma credencial roubada. Os tipos de eventos gerados pelo Security Center variam em função da entidade. Por exemplo, eventos de *Acesso negado* se relacionam a *titulares de cartão*, eventos de *Sinal perdido* se relacionam a câmeras, eventos de *Ocorrência de placa de veículo* se relacionam a *listas de procurados* e assim por diante.

Alguns dos modos como você pode utilizar os *eventos do sistema* são os seguintes:

- Visualizá-los no *Security Desk* em tempo real.
- Fazer com que o sistema os grave em registros de eventos para visualização e análise posteriormente.
- Configurar o sistema para agir automaticamente associando *ações* a vários tipos de eventos, como acionar um *alarme* ou enviar uma mensagem. Isso é chamado de *evento causa-efeito*. Este é o método mais poderoso para lidar com eventos.

Eventos personalizados

Além dos tipos de eventos predefinidos, você também pode definir eventos personalizados para representar cada uma das várias combinações de sinais de entrada recebidos de diferentes unidades em seu sistema.

Tópicos relacionados

Tipos de evento na página 1101
Criar eventos causa-efeito na página 208
Criar eventos personalizados na página 207

Atribuir cores a eventos

Para que os usuários avaliem e respondam rapidamente aos eventos quando são recebidos no Security Desk, você pode atribuir cores diferentes a eventos do Security Center.

O que você deve saber

As cores de eventos são usadas como pistas visuais no Security Desk. Quando um *evento do sistema* é gerado, a cor do evento é indicada na lista de eventos e no ladrilho da tela.

Se você tem um sistema grande, isso ajuda a se concentrar em eventos que são mais importantes. Por exemplo, você pode usar vermelho para indicar um evento crítico (alguém tentou usar uma credencial roubada) e azul para indicar um evento menos crítico (*Acesso concedido*).

Atribuir uma cor para um evento:

1 Abra a tarefa **Sistema**, clique na visualização **Configurações gerais** e, em seguida, clique na página **Eventos**.
2 Próximo a um evento na aba **Cores de eventos**, selecione uma cor na lista suspensa **Cor**.
3 Clique em **Aplicar**.

Criar eventos personalizados

Você pode criar seus próprios eventos personalizados do Security Center que você pode usar para eventos para ações.

O que você deve saber

Eventos personalizados permitem que você forneça nomes descritivos a eventos padrão gerados por sinais de entrada de zonas, painéis de intrusão, e assim por diante. Eles são usados para configurar evento para ações personalizados.

Por exemplo, você pode associar um estado de entrada (normal, ativo, problema) de uma entidade de zona a um evento personalizado que descreve o que está acontecendo, como *Entrada ilegal* ou *Porta aberta por muito tempo para essa zona*. Quando esse evento personalizado é recebido no Security Desk, ele pode acionar uma ação, usando eventos causa-efeito.

Para criar um evento personalizado:

1. Abra a tarefa **Sistema**, clique na visualização **Configurações gerais** e, em seguida, clique na página **Eventos**.
2. Clique em **Adicionar um item** ().
3. Na caixa de diálogo **Criar evento personalizado**, digite um **Nome** para o novo evento.
4. Na lista suspensa **Tipo de entidade**, selecione o tipo de entidade que dispara este evento.
5. No campo **Valor**, digite um número exclusivo para diferenciar o evento personalizado de outros eventos personalizados.

   Esses valores não estão relacionados à IDs lógicas das entidades.
6. Clique em **Salvar** > **Aplicar**.

Criar eventos causa-efeito

Se você quiser que certos eventos que ocorrem no seu sistema desencadeiem automaticamente uma ação, como soar um alarme ou gravar uma câmera, você pode criar eventos causa-efeito.

O que você deve saber

Um evento causa-efeito vincula uma *ação* a um *evento* específico. Por exemplo, é possível configurar o Security Center para acionar um alarme quando uma porta é forçada.

Para criar um evento causa-efeito:

1 Abra a tarefa **Sistema** e clique na visualização **Configurações gerais**.

2 Clique na página **Ações** e, em seguida, clique em **Adicionar um item** ( ).

3 Na lista suspensa **Quando** na caixa de diálogo *Evento causa-efeito*, selecione um tipo de evento.

a) (Opcional: somente eventos de câmera) Se selecionar eventos de análise de vídeo de câmeras, você pode especificar uma condição para eventos de análise de câmera. Por exemplo, *Face detectada* ou *Face reconhecida*.

b) (Opcional: somente LPR) Se selecionar **Reconhecimento de placas de veículos**, você pode especificar uma condição para eventos LicensePlateRead.

c) (Opcional: somente eventos personalizados) Se selecionar um evento personalizado, você pode especificar uma cadeia de texto no campo **and** a ser incluída na macro que aciona o evento causa-efeito.

4 Na opção **De**, clique em **Qualquer entidade** e, em seguida, selecione uma entidade que aciona o evento.

Como padrão, o evento causa-efeito ocorre quando qualquer entidade aciona o tipo de evento selecionado. Caso você selecione uma entidade específica, você poderá precisar configurar outros parâmetros (por exemplo, se você selecionar uma porta, você também deverá selecionar um lado da porta).

5 Na lista suspensa **Ação**, selecione um tipo de ação e configure seus parâmetros.

Por exemplo, se selecionar a ação *Enviar um e-mail*, você pode criar uma mensagem de e-mail modelo que pode incluir campos relacionados ao relatório ou evento. Neste caso, usando o campo `{CardholderName}`, você poderia criar a mensagem: *Tentativa de acesso não autorizado por* `{CardholderName}`.

6 Na opção **Efetivo**, clique em **Sempre** e selecione uma agenda de quando este evento causa-efeito está ativo.

Se o evento ocorrer fora da agenda definida, a ação não será acionada. Por exemplo, você pode querer soar um alarme apenas quando uma janela for aberta durante o fim de semana. Por padrão, **Sempre** fica selecionado.

7 Clique em **Salvar**.

O botão **Salvar** somente fica disponível quando todos os argumentos exigidos pelo tipo de evento causa-efeito são especificados.

O novo evento causa-efeito é adicionado à lista de ações do sistema.

Tópicos relacionados

Tipos de evento na página 1101
Tipos de ação na página 1120
Configurar alarmes usando eventos de causa-efeito na página 924

Adicionar condições ao criar eventos causa-efeito para eventos de análise de vídeo

Ao criar eventos causa-efeito para eventos de análise de vídeo, você pode especificar condições adicionais baseadas em análises de câmera para desencadear uma ação. Por exemplo, você pode especificar que uma ação somente ocorre quando a direção de passagem é para a *direita* ou o veículo passa a uma determinada velocidade.

Antes de iniciar

- Certifique-se de ter análise de vídeo habilitada e configurada para suas câmeras.
- Familiarize-se com os tipos de evento de análise de vídeo.

O que você deve saber

- As condições devem ser digitadas como uma expressão que contém um identificador, um operador e um valor (não diferenciar maiúsculas de minúsculas). Por exemplo, `[RuleName] = "RuleA"`. Para saber mais sobre os operadores e identificadores que podem ser usados, consulte Elementos usados em condições de evento causa-efeito para eventos de análise de vídeo na página 211.
- Os identificadores devem ser digitados entre colchetes: `[RuleName]`.
- Os valores de texto devem ser digitados entre aspas: `"ABC123"`.
- Você pode usar AND e OR para combinar várias expressões. Ao fazer isso, use parênteses para forçar a ordem da avaliação. Por exemplo, se você digitar `([Count] > 20 AND [Update] = "Punctual") OR ([Count] > 50 AND [Direction] = "right")`, o operador AND tem precedência.
- Você pode usar o ponto de exclamação (!) para excluir uma expressão. Por exemplo, se você digitar `[RuleName] contains "RuleA" AND !([Update] = "punctual")`, qualquer câmera com um nome de regra que contenha o valor "RuleA" e um valor de "Update" diferente de "punctual" desencadeará uma ação.
- As análises de câmera não são geradas 100% do tempo. Um evento causa-efeito poderá não ser processado se a câmera não for capaz de gerar a análise especificada na condição. Por exemplo, se a condição for `[Count] > 50` e a câmera não puder produzir um valor para a contagem, o Security Center avaliará a condição como sendo falsa e a ação não será processada.

Para adicionar uma condição ao criar um evento causa-efeito para um evento de análise de vídeo:

1. Abra a tarefa **Sistema** e clique na visualização **Configurações gerais**.
2. Clique na aba **Ações** e clique em **Adicionar um item** ().
3. Na lista suspensa **Quando** na caixa de diálogo *Evento causa-efeito*, selecione um evento de análise de vídeo na lista de eventos.
4. Clique em **Especificar uma condição** e digite a expressão.

   DICA: Passe o mouse sobre o campo para obter exemplos de expressões válidas. O campo será exibido em vermelho se a expressão inserida for inválida.

5. Na lista suspensa **De**, mantenha o padrão **Qualquer entidade** inalterado.
6. Na lista suspensa **Ação**, selecione um tipo de ação e configure seus parâmetros.

   Por exemplo, se você selecionar a ação *Enviar um e-mail*, você também deverá selecionar os destinatários do e-mail.

7. Na opção **Efetivo**, clique em **Sempre** e selecione uma agenda para quando este evento causa-efeito esteja ativo.

   Se o evento ocorrer fora do agendamento definido, ação não será disparada.

8 Clique em **Salvar**.

O botão **Salvar** somente fica disponível quando todos os argumentos exigidos pelo tipo de evento causa-efeito são especificados.

Elementos usados em condições de evento causa-efeito para eventos de análise de vídeo

Se você adicionar uma condição ao criar um evento causa-efeito para um evento de análise de vídeo, a condição deve conter um identificador, um operador e um valor (textual ou numérico).

Operadores

A tabela a seguir lista operadores que podem ser usados e os tipos de valores correspondentes, descrições e exemplos.

Operador	Descrição	Tipo de valor	Exemplo
>	Maior do que o valor especificado.	Numérico	[Count] > 80
<	Menor do que o valor especificado.	Numérico	[Count] < 75
>=	Maior do que ou igual ao valor especificado.	Numérico	[Count] >= 80
<=	Menor do que ou igual ao valor especificado.	Numérico	[Count] <= 75
=	Igual ao valor especificado.	Numérico	[Count] = 80
		Texto	[Direction] = "left"
startsWith	Começa com o valor especificado.	Texto	[RuleName] startsWith "X"
endsWith	Termina com o valor especificado.	Texto	[RuleName] endsWith "C"
contém	Contém o valor especificado.	Texto	[RuleName] contém "Rule123"
corresponde	Respeita a expressão regular.	Texto	[RuleName] corresponde a "regularExpression" expression1 OR expression2 AND expression3

Identificadores

A tabela a seguir lista os identificadores comuns que podem ser usados e os tipos de valores correspondentes, descrições e exemplos.

IMPORTANTE: Estes identificadores somente são suportados para eventos de contagem de pessoas (**A contagem de objetos atingiu** e **A contagem de objetos mudou**).

Identificador	Descrição	Tipo de valor	Exemplo
RuleName	O nome da regra configurado no dispositivo.	Texto	[RuleName] contém "RuleA"
Atualizar	Os valores de atualização são punctual ou summary.	Texto	[Update] = "punctual'

Identificador	Descrição	Tipo de valor	Exemplo
Direção	Os valores de direção são in, out, left ou right.	Texto	[Direction] = "right"
Contagem	Valor numérico.	Numérico	[Count] > 2

Para obter mais informações sobre como especificar condições ao criar eventos causa-efeito para eventos de análise de câmera, consulte Adicionar condições ao criar eventos causa-efeito para eventos de análise de vídeo na página 209

Adicionar condições ao criar eventos causa-efeito para reconhecimento de placas de veículos

Ao criar eventos causa-efeito para reconhecimento de placas de veículos, você pode especificar condições adicionais baseadas em análises Sharp para desencadear uma ação. Por exemplo, você pode especificar que uma ação ocorra somente quando o número da placa contém "123", ou o veículo está viajando a uma determinada velocidade.

Antes de iniciar

- Habilite e configure a análise para seus Sharps. Para mais informações, consulte o *Guia do Administrador do Sharp* e o *Guia do Administrador do Genetec Patroller™*.

O que você deve saber

- As condições devem ser digitadas como uma expressão que contém um identificador, operador e um valor (não diferenciar maiúsculas de minúsculas). Por exemplo, `[PlateNumber] = "ABC123"`. Para saber mais sobre os operadores e identificadores que podem ser usados, consulte Elementos usados em condições de evento causa-efeito para leituras de placas de veículos na página 215.
- Os identificadores devem ser digitados entre colchetes: `[PlateNumber]`.
- Os valores de texto devem ser digitados entre aspas: `"ABC123"`.
- Você pode usar AND e OR para combinar várias expressões. Ao fazer isso, é preferível usar parênteses para forçar a ordem da avaliação. Por exemplo, se você digitar `([Speed] > 20 AND [Speed.unit] = "mph") OR ([Speed] > 50 AND [Speed.Unit] = "km/h")` o operador AND tem precedência.
- Você pode usar o ponto de exclamação (!) para excluir uma expressão. Por exemplo, se você digitar `[PlateNumber] contains "123" AND !([PlateState] = "QC")`, qualquer leitura de um número de placa de veículo que contenha o valor "123" e um estado de placa diferente de "QC" desencadeará uma ação.
- As análises Sharp não são geradas 100% do tempo. Um evento para ação pode não ser executado se o Sharp não for capaz de gerar a análise especificada na condição. Por exemplo, se a condição for **[Speed] > 50** e o Sharp não puder produzir um valor para a velocidade, o Security Center avaliará a condição como sendo falsa e a ação não será executada.
- Quando as saídas de uma Unidade de Processamento LPR são usadas para controlar o acesso a edifícios através de eventos causa-efeito no Security Center, reinicializar a Unidade de Processamento LPR faz com que as saídas sejam ativadas, o que pode levar à abertura do ponto de acesso. Este comportamento de saída não é ideal para controle de acesso, mas é necessário para alimentar o computador no veículo na partida do veículo. Crie um evento causa-efeito no Security Center que enviará um estado "Normal" para as saídas após um evento "Unidade Conectada". Os pontos de acesso continuarão abertos, mas fecharão pouco depois.

Para adicionar uma condição ao criar um evento para ação para uma leitura de placa de licença:

1 Abra a tarefa **Sistema** e clique na visualização **Configurações gerais**.
2 Clique na aba **Ações** e clique em **Adicionar um item** ().
3 Na lista suspensa **Quando**, na caixa de diálogo *Evento causa-efeito*, selecione **Reconhecimento de placas de veículos**.
4 Clique em **Especificar uma condição** e digite a expressão.

DICA: Passe o mouse sobre o campo para obter exemplos de expressões válidas. O campo será exibido em vermelho se a expressão inserida for inválida.

5 Na lista suspensa **De**, selecione a unidade de LPR que aciona o evento.
6 Na lista suspensa **Para**, selecione a entidade desejada.

7 Na lista suspensa **Ação**, selecione um tipo de ação e configure seus parâmetros.

Por exemplo, se você selecionar a ação *Enviar um e-mail*, você também deverá selecionar os destinatários do e-mail.

8 Na opção **Efetivo**, clique em **Sempre** e selecione uma agenda para quando este evento causa-efeito esteja ativo.

Se o evento ocorrer fora do agendamento definido, ação não será disparada.

9 Clique em **Salvar**.

O botão **Salvar** somente fica disponível quando todos os argumentos exigidos pelo tipo de evento causa-efeito são especificados.

Elementos usados em condições de evento causa-efeito para leituras de placas de veículos

Se você adicionar uma condição ao criar um evento para ação para uma leitura de placa de licença, a condição deve conter um identificador, um operador e um valor (texto ou numérico).

Operadores

A tabela a seguir lista operadores que podem ser usados e os tipos de valores correspondentes, bem como descrições e exemplos.

Operador	Descrição	Tipo de valor	Exemplo
>	Maior do que o valor especificado.	Numérico	[Pontuação de confiança] > 80
<	Menor do que o valor especificado.	Numérico	[Pontuação de confiança] < 75
=	Igual ao valor especificado.	Numérico	[Pontuação de confiança] = 80
		Texto	[Marca do veículo] = "Toyota"
contém	Contém o valor especificado.	Texto	[PlateNumber] contém "123"
startsWith	Começa com o valor especificado.	Texto	[PlateNumber] startsWith "X"
endsWith	Termina com o valor especificado.	Texto	[State Name] endsWith "C"
corresponde	Respeita a expressão regular.	Texto	[PlateNumber] corresponde a "[02468]$"

Identificadores

A tabela a seguir lista os identificadores comuns que podem ser usados e os tipos de valores correspondentes, bem como descrições e exemplos.

Identificador	Descrição	Tipo de valor	Exemplo
PlateNumber	Placa de licença como lida pelo Sharp.	Numérico	[PlateNumber] contém "123"
Nome do estado	Nome do estado lido pelo Sharp.	Texto	[Nome do estado] = "QC"
Tipo do veículo	Certas placas de licença incluem símbolos de caracteres que identificam tipos de veículos específicos (por exemplo, táxi, transporte e assim por diante). O Sharp pode ler esses símbolos e exibir o tipo de veículo.	Texto	[Tipo de veículo] = "Táxi"

Identificador	Descrição	Tipo de valor	Exemplo
Movimento relativo	O Sharp pode detectar se o veículo está se aproximando ou se afastando do Sharp.	Texto	[Movimento relativo] = "Mais perto"
Contexto	Tipo de contexto LPR para uma região específica.	Texto	[Contexto] = "Brasil"
Altura dos caracteres	Altura em pixels dos caracteres de contexto.	Numérico	[Altura dos caracteres] = 26
Marca do veículo	As câmeras Sharp podem reconhecer a marca de certos veículos.	Texto	[Marca do veículo] = "Toyota"
Pontuação de confiança	O Sharp atribui um valor numérico (de 0 a 100) para cada leitura de placa de licença. Este valor mostra o nível de precisão da leitura.	Numérico	[Pontuação de confiança] = 80
Velocidade	As câmeras Sharp são capazes de estimar a velocidade aproximada de um veículo.	Numérico	[Velocidade] > 50
Speed.Unit	Dependendo do contexto em que o Sharp é utilizado, a unidade de velocidade é medida em *km/h* ou *mph*. Para o contexto dos EUA, a velocidade é medida em *mph*.	Texto	[Unidade.Velocidade] = "mph"
Prefixo	Dígitos mais à esquerda e mais acima em placas dos Emirados Árabes Unidos.	Texto	[Prefixo] = 10

Para obter mais informações sobre como especificar condições ao criar eventos para ações para leituras de placas de licença, consulte Adicionar condições ao criar eventos causa-efeito para reconhecimento de placas de veículos na página 213

Modificar eventos causa-efeito

Se você precisar modificar um evento causa-efeito, mas tiver uma lista longa deles no Security Center, você pode pesquisá-los usando uma combinação de entidade de origem (nome e tipo), tipo de evento e tipo de ação.

Para modificar um evento para ação:

1 Abra a tarefa **Sistema** e clique na visualização **Configurações gerais**.

2 Clique na página **Ações** e em **Pesquisa avançada** (⊕) para mostrar os filtros de pesquisa e filtrar os eventos causa-efeito como segue:

- **Nome da entidade:** Pesquisa por nomes de entidades de origem começando com a sequência de pesquisa.
- **Tipo da entidade:** Selecione um tipo específico de entidade de origem (padrão = Todos).
- **Evento:** Selecione um tipo específico de evento de origem (padrão = Todos).
- **Ação:** Selecione um tipo específico de ação (padrão = Todos).

3 Selecione um evento causa-efeito e clique em **Editar o item** (✎).

4 Na lista suspensa **Quando** na caixa de diálogo *Evento causa-efeito*, selecione um tipo de evento.

a) (Opcional: somente eventos de câmera) Se selecionar eventos de análise de vídeo de câmeras, você pode especificar uma condição para eventos de análise de câmera. Por exemplo, *Face detectada* ou *Face reconhecida*.

b) (Opcional: somente LPR) Se selecionar **Reconhecimento de placas de veículos**, você pode especificar uma condição para eventos LicensePlateRead.

c) (Opcional: somente eventos personalizados) Se selecionar um evento personalizado, você pode especificar uma cadeia de texto no campo **and** a ser incluída na macro que aciona o evento causa-efeito.

5 Na opção **De**, clique em **Qualquer entidade** e, em seguida, selecione uma entidade que aciona o evento.

Como padrão, o evento causa-efeito ocorre quando qualquer entidade aciona o tipo de evento selecionado. Caso você selecione uma entidade específica, você poderá precisar configurar outros parâmetros (por exemplo, se você selecionar uma porta, você também deverá selecionar um lado da porta).

6 Na lista suspensa **Ação**, selecione um tipo de ação e configure seus parâmetros.

Por exemplo, se selecionar a ação *Enviar um e-mail*, você pode criar uma mensagem de e-mail modelo que pode incluir campos relacionados ao relatório ou evento. Neste caso, usando o campo `{CardholderName}`, você poderia criar a mensagem: *Tentativa de acesso não autorizado por* `{CardholderName}`.

7 Na opção **Efetivo**, clique em **Sempre** e selecione uma agenda de quando este evento causa-efeito está ativo.

Se o evento ocorrer fora da agenda definida, a ação não será acionada. Por exemplo, você pode querer soar um alarme apenas quando uma janela for aberta durante o fim de semana. Por padrão, **Sempre** fica selecionado.

8 Clique em **Salvar**.

O botão **Salvar** somente fica disponível quando todos os argumentos exigidos pelo tipo de evento causa-efeito são especificados.

9 Para excluir um evento causa-efeito, selecione o item e clique em **Excluir** (✖).

10 Clique em **Aplicar**.

Tarefas agendadas

Uma tarefa agendada é um tipo de entidade que define uma ação que é executada automaticamente em data e hora específicas ou de acordo com uma agenda recorrente.

Semelhanças entre tarefas agendadas e evento para ações

As semelhanças entre os dois conceitos são:

- Ambos têm acesso ao mesmo conjunto de ações.
- Ambos são agendamentos recorrentes.

Diferenças entre tarefas agendadas e evento para ações

As diferenças entre os dois conceitos são:

- Uma tarefa agendada é salva como uma *entidade*, um evento causa-efeito não.
- Uma tarefa agendada é disparada pelo agendamento, não pelo evento.
- Uma tarefa agendada pode ser ativada e desativada.
- As opções de agendamento são diferentes:
  - **Uma vez:** Executado uma vez em uma data e horário específicos.
  - **A cada minuto:** Executado a cada minuto.
  - **A cada hora:** Executado em um minuto específico de cada hora.
  - **Diariamente:** Executado em uma hora específica a cada dia.
  - **Semanalmente:** Executado em um horário específico em dias selecionados na semana.
  - **Na inicialização:** Executado na inicialização do sistema.
  - **Intervalo:** Executado em intervalos regulares que podem ser dias, horas, minutos ou segundos.

Agendar tarefa

Você pode configurar uma ação para executar automaticamente na inicialização do sistema ou de acordo com uma tarefa agendada criando uma *tarefa agendada*.

Para configurar uma ação para ser disparada em um agendamento:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Tarefas agendadas**.
2 Clique em **Tarefa agendada** ( ).

Uma nova entidade de tarefa agendada aparece na lista de entidades.

3 Digite um nome para a tarefa agendada e pressione **ENTER**.
4 Clique na aba **Propriedades** e altere a opção **Status**para **Ativo**.
5 Na opção **Recorrência**, selecione com que frequência você deseja que a tarefa ocorra:

- **Uma vez:** Executado uma vez em uma data e horário específicos.
- **A cada minuto:** Executado a cada minuto.
- **A cada hora:** Executado em um minuto específico de cada hora.
- **Diariamente:** Executado em uma hora específica a cada dia.
- **Semanalmente:** Executado em um horário específico em dias selecionados na semana.
- **Na inicialização:** Executado na inicialização do sistema.
- **Intervalo:** Executado em intervalos regulares que podem ser dias, horas, minutos ou segundos.

6 Selecione o tipo de ação a ser executada:
7 Se necessário, defina os parâmetros adicionais para a ação selecionada.

Por exemplo, se você selecionar *Sincronizar função* como a ação, você deve selecionar qual função é sincronizada.

8 Clique em **Aplicar**.

Tópicos relacionados

Tipos de ação na página 1120

Adicionar arquivos de áudio

Você pode adicionar novos arquivos de áudio que podem ser reproduzidos quando os usuários recebem um alarme no Security Desk ou que são usados com a ação *Reproduzir um som*.

O que você deve saber

O Security Center suporta os formatos de arquivo .mid, .rmi, .midi, .wav, .snd, .au, .aif, .aifc, .aiff, .mp3 e .ogg.

Como prática recomendada, não adicione arquivos de áudio maiores do que 100 KB.

Para adicionar um arquivo de áudio:

1. Abra a tarefa **Sistema**, clique na visualização **Configurações gerais** e, em seguida, clique na página **Áudio**.
2. Clique em **Adicionar um item** ( ).
3. No navegador do Windows, selecione um arquivo de áudio e clique em **Abrir**.

   O arquivo de áudio é adicionado à lista.
4. Para alterar o nome de arquivo de áudio, clique em **Editar o item** ( ), digite um nome e clique em **OK**.
5. Para ouvir o arquivo de áudio, clique em **Reproduzir** ( ).
6. Clique em **Aplicar**.

Sobre macros

É um tipo de entidade que envolve um programa C# que adiciona funcionalidades personalizadas ao Security Center.

As macros podem ser executadas manualmente ou automaticamente. Quando automatizada, ela é carregada como um processo em segundo plano e é executada quando um conjunto de condições são atendidas.

Você cria macros escrevendo um programa em C# usando o *SDK* Security Center e, em seguida, carregando o programa no Security Center. Se precisar de ajuda para desenvolver macros personalizadas, entre em contato com os Genetec™ através de seu representante de vendas para uma cotação ou ligue para um de nossos escritórios regionais em todo o mundo. Para entrar em contato conosco, visite nosso site em www.genetec.com.

Contexto de execução de macro

Você pode fornecer parâmetros de entrada para sua macro declarando modificadores. Esses modificadores devem ser públicos. Seu tipo deve ser um dos seguintes:

- System.Boolean
- System.String
- System.Int32
- System.Guid

Ao declarar modificadores, sua macro terá um contexto de execução que pode ser configurado na aba *Contexto de execução padrão*. Se uma macro é executada sem especificar um contexto de execução, o contexto de execução padrão é usado. Este é sempre o caso quando uma macro é iniciada a partir da barra de ferramentas na parte inferior do Config Tool.

O contexto de execução padrão pode ser substituído especificando seu próprio contexto.

Criar macros

Para criar uma macro que você possa executar no Security Center, você deve escrever um programa em C# usando um editor de texto externo ou o editor de texto do Config Tool e, em seguida, carregar o programa no Security Center.

O que você deve saber

O Security Center impede que uma macro que tenha erros seja salva. Se uma macro tiver erros e você alternar entre abas, ela será revertida para a última versão sem erro.

Para criar uma macro:

1 Na página inicial de Config Tool, abra a tarefa *Sistema* e clique na visualização **Macros**.

2 Clique em **Macro** ( ) e digite o nome da macro.

3 Clique em **Propriedades** e tome uma das seguintes ações:

- Para importar o código-fonte de um arquivo, clique em **Importar de arquivo**, selecione o arquivo que contém o código C# e, em seguida, clique em **Abrir**.
- Escreva seu próprio programa na aba **Propriedades**.

4 Clique em **Aplicar**.

5 Se você tiver adicionado parâmetros de entrada ao programa, clique na aba **Contexto de execução padrão** e defina as configurações.

6 Clique em **Aplicar**.

10

Federation™

Esta seção inclui os seguintes tópicos:

- "Sobre o recurso Federation" na página 224
- "Sobre entidades federadas" na página 225
- "Configurar uma Security Center Federation" na página 228
- "Configurar uma Omnicast Federation" na página 229
- "Usar configurações padrão do Security Desk para exibir câmeras federadas" na página 231
- "Exigências para grandes sistemas Federation" na página 232
- "Adicionar grupos de funções Federation" na página 234

Sobre o recurso Federation™

O recurso Federation™ associa múltiplos sistemas de segurança IP Genetec™ independentes em um único sistema virtual. Com essa função, os usuários do Security Center podem controlar entidades que pertencem a sistemas remotos diretamente pelo sistema local do Security Center.

O Security Center pode unir (ou federar) outros sistemas Security Center e sistemas Omnicast™ em uma grande Federation™ de sistemas de segurança IP Genetec™. O sistema que une outros sistemas é chamado *Host de Federation™*. O Security Center faz isso criando uma função Federation™ específica para cada sistema que é necessário unificar.

Para obter uma lista das versões do Security Center e do Omnicast™ que você pode federar nesta versão, consulte as *Notas de Versão do Security Center.*

Security Center Federation™

A função Security Center Federation™ conecta um sistema Security Center remoto e independente ao seu Security Center local. Desse modo, as entidades e eventos do sistema remoto podem ser usados no seu sistema local.

A função Security CenterFederation™ atua como um proxy entre seus clientes locais e o sistema remoto do Security Center com o qual eles precisam se conectar.

Múltiplas instâncias da função Security CenterFederation™ podem ser criadas no sistema.

Para obter uma lista de eventos federados disponíveis, consulte a página *Propriedades* da função Federation™ correspondente no Config Tool.

Omnicast™ Federation™

A função Omnicast™ Federation™ conecta um sistema Omnicast™ 4.x ao Security Center. Desse modo, as entidades e eventos do Omnicast™ podem ser usados no seu sistema do Security Center.

A função Omnicast™ Federation™ atua como um proxy entre seus clientes locais e o sistema remoto do Omnicast™ com o qual eles precisam se conectar.

Múltiplas instâncias da função Omnicast™ Federation™ podem ser criadas no sistema.

Limitações com o Omnicast™ Federation™

A federação de um sistema Omnicast™ tem as seguintes limitações:

- Alguns recursos de reprodução não são suportados em câmeras federadas. A reprodução inversa suave não está disponível e a velocidade de rebobinamento é limitada a -10x, -20x, -40x e -100x.
- As sequências de câmeras são federadas, mas elas se comportam como uma única câmera no host do Federation™. Isso significa que os usuários no host do Federation™ não podem desempacotar nem interromper o ciclo das câmeras em sequências de câmeras ( ) federadas do Omnicast™.
- Os locais ( ) são federados como áreas ( ) no Security Center.
- Locais com uma propriedade de Mapa (URL) ( ) são federados como áreas ( ) com um plug-in de ladrilho de página da Web anexado.

Tópicos relacionados

Diferenças entre Federation e GCM na página 702

Sobre entidades federadas

As entidades federadas são entidades importadas de sistemas remotos independentes do Security Center ou Omnicast™.

As entidades federadas não pertencem ao seu sistema local. Você pode exibi-las e manipulá-las no sistema local, mas não é possível alterar suas configurações nativas. Você pode facilmente identificar entidades federadas pela seta amarela que é sobreposta ao seu ícone de entidade (por exemplo, aqui está uma entidade de alarme federada —).

As seguintes entidades federadas só se aplicam a um tipo de Federation™:

- – Entidade de porta federada (somente Security Center Federation™)
- – Entidade de elevador federada (somente Security Center Federation™)
- – Entidade de titular do cartão federada (somente Security Center Federation™)
- – Entidade de credencial federada (somente Security Center Federation™)
- – Entidade de câmera virtual federada (somente Omnicast™ Federation™)

Quais entidades são federadas no Security Center

As seguintes entidades podem ser federadas a partir de um sistema remoto do Security Center:

Componente	Entidades
Vídeo	Câmeras e sequências de câmeras.
Controle de acesso	Unidades de controle de acesso, portas, elevadores, titulares de cartões, grupos de titulares de cartões, credenciais, unidades de detecção de intrusão e áreas de detecção de intrusão.
LPR	Unidades de LPR e unidades Genetec Patroller™.
Geral	Alarmes, caixas registradoras, redes, áreas e mapas, zonas, comportamentos de saída e eventos personalizados. **Limitation:** Mapas ArcGIS são federados apenas na versão 5.7 e mais recente. Se você federar um sistema mais antigo (5.6 em diante) isso torna o sistema federado com um mapa ArcGIS, você não poderá ver o mapa ArcGIS no seu sistema.

Funções, servidores, partições e outras entidades não listadas na lista precedente não serão federadas.

NOTA: Visitantes e grupos de visitantes são diferentes dos titulares de cartões e grupos de titulares de cartão e não são federados.

O que você pode fazer com entidades federadas no Security Desk

Você pode executar as seguintes operações em entidades federadas no Security Desk:

- Visualizar vídeo ao vivo e de reprodução de câmeras federadas.
- Adicionar marcadores, iniciar e parar gravações e exportar vídeos a partir de câmeras federadas.
- Controlar câmeras PTZ federadas (exceto o bloqueio PTZ).
- Ligar câmeras em matrizes CCTV usando *câmeras virtuais* federadas do Omnicast™ 4.x.

- Visualizar, iniciar e interromper ciclo, empacotar e desempacotar sequências de câmeras federadas.
- Receber, confirmar, adiar, encaminhar, iniciar e interromper ciclo, empacotar e desempacotar alarmes federados.
- Visualizar e controlar plugins de ladrilhos federados.
- Bloquear e desbloquear portas federadas.
- Armar e desarmar áreas de detecção de intrusão federadas.
- Armar e desarmar zonas federadas.

O que você pode configurar com entidades federadas

Você pode fazer as seguintes alterações em entidades federadas em seu sistema local:

- Você pode atribuir IDs lógicas a entidades federadas. A ID lógica é um atributo local associado à entidade federada para identificá-la exclusivamente dentro do Federation™.
- Você pode atribuir nomes de entidades locais a entidades federadas. Os nomes de entidade originais permanecem visíveis no Config Tool a fim de solucionar problemas.
- Você pode atualizar os campos personalizados associados a entidades federadas. Campos personalizados são locais para o host do Federation™.
- Você pode escolher quais eventos você deseja receber do sistema federado. Com base nesses eventos, você pode definir *eventos causa-efeito* para entidades federadas. As ações podem ser executadas no host do Federation™ ou no sistema federado.
- Você pode visualizar seus relatórios de atividade e de trilha de auditoria no painel *Relatórios*.
- Você pode controlar a visibilidade das entidades federadas para seus usuários locais usando partições.
- Você pode configurar rastreamento visual para câmeras federadas de sistemas Omnicast™.
- Você pode usar entidades federadas para configurar entidades locais, como anexar câmeras federadas a entidades locais ou usá-las para definir alarmes locais e sequências de câmera.

Limitações de entidades federadas

Não é possível fazer o seguinte com entidades federadas:

- Você não pode alterar as propriedades de entidades federadas no sistema remoto. Você pode apenas sobrescrever certas propriedades, tais como o nome da entidade e o ID lógico, localmente no seu sistema.
- Não é possível visualizar os campos personalizados definidos no sistema remoto. Os campos personalizados não são federados.
- Ações realizadas em entidades federadas, tais como a armação de uma zona ou adicionar uma marcação a uma câmera, não estão registradas nas trilhas de atividades do sistema federado.

  NOTA: Existe uma exceção a essa limitação. As ações de *Exportar vídeo* estão registradas em ambas as trilhas de atividades. No host Federation™ (sistema local), o usuário que realizou a atividade está conectado como *iniciador*. No sistema federado (sistema remoto), o *iniciador* é o usuário Federation™ e o usuário que realizou a atividade no host Federation™ está conectado como o *iniciador original*. O registro de atividade remoto só funciona se o sistema federado estiver executando uma versão Security Center 5.7 ou mais recente.

Exceções para alarmes federados

Nem todas as propriedades de alarme são federadas. A maioria das propriedades pertencentes à exibição de alarme no Security Desk deve ser configurada localmente no host do Federation™.

As exceções para alarmes federados são as seguintes:

- O *agendamento* do alarme segue a configuração original do sistema remoto. Como as entidades de agendamento não são federadas, o agendamento padrão *Sempre* é exibido em vez delas.
- Prioridade do alarme:
  - Omnicast™: o valor original não é federado. Você pode configurá-lo (padrão=1) localmente no host do Federation™.
  - Security Center: o valor original é federado e não pode ser modificado.
- O limiar de reativação é uma propriedade inerente ao alarme e não pode ser modificado.
- O ciclo da entidade é uma propriedade local para o host do Federation™. É possível alterar sua configuração e isso não afetará o sistema federado.
- O limiar de confirmação automática é uma propriedade inerente ao alarme e não pode ser modificado.
- Criar um incidente na confirmação é uma propriedade local para o host do Federation™. É possível alterar sua configuração e isso não afetará o sistema federado.
- O limiar de gravação de vídeo automática é uma propriedade inerente ao alarme e não pode ser modificado.
- O vídeo gravado protegido é uma propriedade inerente ao alarme e não pode ser modificado.
- A exibição de vídeo é uma propriedade local para o host do Federation™. É possível alterar sua configuração e isso não afetará o sistema federado.
- Procedimento de alarme (*URL*):
  - Omnicast™: o valor original não é federado. Você pode configurá-lo localmente no host do Federation™.
  - Security Center: o valor original é federado e não pode ser modificado.
- As entidades associadas ao alarme federado (câmeras, portas etc.) são propriedades inerentes ao alarme e não podem ser modificadas.
- Os destinatários de alarmes devem sempre ser configurados localmente para o host do Federation™.

Tópicos relacionados

Formatos de cartão personalizados na página 689
Importar grupos de segurança de um Active Directory na página 389

Configurar uma Security Center Federation™

Para configurar uma Security Center Federation™, você deve criar uma função Security Center Federation™, conectá-la ao sistema Security Center remoto e decidir quais eventos você deseja federar.

Para configurar uma Security Center Federation™:

1 Abra a tarefa *Sistema* e clique na visualização **Funções**.

2 Clique em **Adicionar uma entidade** ( ) e, em seguida, clique em **Security Center Federation™**.

3 No campo **Directory**, digite o nome do Security Center Directory remoto.

4 Nos dois campos seguintes, digite o nome de usuário e a senha que a função Federation™ vai usar para efetuar logon no sistema Security Center remoto e clique em **Próximo**.

Os direitos e privilégios daquele usuário determinam o que seus usuários locais serão capazes de ver e fazer no sistema federado.

5 Na página **Informações básicas**, insira um nome e uma descrição para a função.

6 Selecione uma **Partição** da qual esta função seja membro e clique em **Próximo**.

Todas as entidades federadas são criadas na partição que você selecionar. Somente usuários que sejam parte da partição poderão visualizar ou modificar essas entidades.

7 Clique em **Próximo** > **Criar** > **Fechar**.

A nova função Federation™ ( ) é criada.

8 Se você pretende hospedar mais de 100 funções Security Center Federation™ no mesmo servidor, será necessário atribuir um *grupo de funções* diferente para cada 100 funções que você criar.

9 Clique na guia **Propriedades.**

O status da conexão deve ser **Sincronizando entidades** ou **Conectado**.

10 Decida o que acontece se a conexão entre a função Security Center Federation™ e o Security Center Directory federado for interrompida configurando as seguintes opções:

- **Conexão resiliente:** Quando essa opção é ativada, se a conexão entre a função Federation™ e o servidor do Security Center Directory federado for temporariamente interrompida, a função Federation™ tentará reconectar-se ao Directory remoto por um período de tempo definido antes que a conexão seja considerada perdida e a função entre em um estado de aviso.
- **Tempo limite de reconexão expirado:** Especifique o número de segundos durante os quais a função Federation™ tenta se reconectar ao Directory antes da conexão ser considerada perdida.

11 Na lista suspensa **Transmissão ao vivo padrão**, selecione o *stream de vídeo* padrão usado para exibir vídeo ao vivo de câmeras Security Center federadas (padrão=**Remoto**).

Se souber que uma estação de trabalho não precisa seguir as configurações padrão da função Federation™, você pode alterar a sua configuração para usar as configurações padrão do Security Desk.

12 Para impedir que os usuários visualizem vídeo de reprodução de câmeras federadas, coloque a opção **Ativar solicitações de reprodução** em **Desligado**.

13 Caso não queira receber alarmes do sistema federado, altere a opção **Federar alarmes** para **Desligado**.

14 Na seção **Eventos federados**, selecione os eventos que deseja receber do sistema federado e clique em **Aplicar**.

Os eventos são necessários se você planeja monitorar as entidades federadas no Security Desk ou configurar eventos causa-efeito para as entidades federadas.

15 Abra a tarefa **Exibição de área**.

16 Expanda a nova função Security Center Federation™ ( ) na exibição de área e verifique se todas as entidades federadas foram importadas pela função.

A hierarquia de entidades corresponde à exibição da área no sistema federado remoto.

Tópicos relacionados

Exigências para grandes sistemas Federation na página 232
Usar configurações padrão do Security Desk para exibir câmeras federadas na página 231

Configurar uma Omnicast™ Federation™

Para configurar uma Omnicast™ Federation™, você deve criar uma função Omnicast™ Federation™, conectá-la ao sistema Omnicast™ remoto e decidir quais eventos você deseja federar.

Antes de iniciar

Instale o pacote de compatibilidade do Omnicast™ correspondente à versão do sistema Omnicast™ que você planeja federar nos servidores e nas estações de trabalho a seguir:

- No servidor no qual a função Federation™ deve ser hospedada.
- Na estação de trabalho cliente onde o Config Tool está em execução.
- Em todos os servidores secundários que deseja atribuir à função Federation™ role.
- Em todas as estações de trabalho do Security Desk visualizando as câmeras federadas.

Para configurar uma Omnicast™ Federation™:

1 Abra a tarefa *Sistema* e clique na visualização **Funções**.

2 Clique em **Adicionar uma entidade** () e, em seguida, clique em **Omnicast™ Federation™**.

3 No campo **Directory**, digite o nome do Gateway Omnicast™ que conecta você ao sistema Omnicast™ remoto.

4 Nos dois campos seguintes, digite o nome de usuário e a senha que a função Federation™ vai usar para efetuar logon no sistema Omnicast™ remoto.

Os direitos e privilégios daquele usuário determinam o que seus usuários locais serão capazes de ver e fazer no sistema federado remoto.

5 Na lista suspensa **Versão**, selecione a versão do sistema Omnicast™ remoto e clique em **Próximo**.

Esta lista suspensa mostra apenas as versões do Omnicast™ para as quais um pacote de compatibilidade está instalado.

6 Na seção **Eventos federados**, selecione os eventos que deseja receber do sistema federado e clique em **Próximo**.

Os eventos são necessários se você planeja monitorar as entidades federadas no Security Desk ou configurar eventos causa-efeito para as entidades federadas.

7 Na página **Informações básicas**, insira um nome e uma descrição para a função.

8 Selecione uma **Partição** da qual esta função seja membro e clique em **Próximo**.

Todas as entidades federadas são criadas na partição que você selecionar. Somente usuários que sejam parte da partição poderão visualizar ou modificar essas entidades.

9 Clique em **Próximo** > **Criar** > **Fechar**.

A nova função Federation™ () é criada.

10 Se você pretende hospedar mais de 40 funções Omnicast™ Federation™ no mesmo servidor, será necessário atribuir um *grupo de funções* diferente para cada 40 funções que você criar.

11 Clique na guia **Propriedades.**

O status da conexão deve ser **Sincronizando entidades** ou **Conectado**.

12 Na lista suspensa **Transmissão ao vivo padrão**, selecione a transmissão de vídeo padrão usada para exibir vídeo ao vivo de câmeras Omnicast™ federadas (padrão=**Remoto**).

Se souber que uma estação de trabalho não precisa seguir as configurações padrão da função Federation™, você pode alterar a sua configuração para usar as configurações padrão do Security Desk.

13 Para impedir que os usuários visualizem vídeo de reprodução de câmeras federadas, coloque a opção **Ativar solicitações de reprodução** em **Desligado**.

14 Caso não queira receber alarmes do sistema federado, altere a opção **Federar alarmes** para **Desligado**.

15 Abra a tarefa **Exibição de área**.

16 Expanda a nova função Omnicast™ Federation™ () na exibição de área e verifique se todas as entidades federadas foram importadas pela função.

A hierarquia da entidade corresponde à visualização da área no sistema federado remoto.

Tópicos relacionados

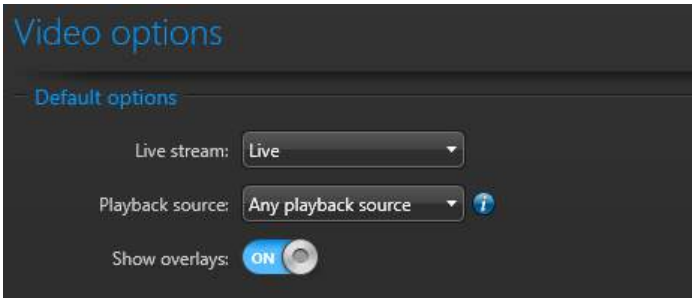
Exigências para grandes sistemas Federation na página 232
Usar configurações padrão do Security Desk para exibir câmeras federadas na página 231

Usar configurações padrão do Security Desk para exibir câmeras federadas

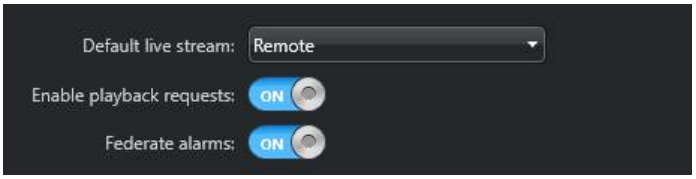
Ao solicitar vídeo ao vivo de câmeras federadas, ao invés de usar as configurações padrão da tarefa Federation™, você pode configurar uma estação de trabalho para usar as configurações padrão do Security Desk.

O que você deve saber

Quando os usuários solicitam vídeo ao vivo de uma câmera local, a configuração de transmissão padrão é obtida das opções de vídeo padrão no Security Desk (padrão=**Ao vivo**).



No entanto, quando os usuários solicitam vídeo ao vivo de uma câmera federada, a configuração de transmissão padrão é obtida das propriedades da função Federation™ (padrão=**Remoto**).



Isto acontece porque as câmeras federadas são frequentemente usadas em um segmento de baixa largura de banda da rede. Se souber que uma estação de trabalho não precisa seguir as configurações padrão da função Federation™, você pode alterar a sua configuração para usar as configurações padrão do Security Desk.

Para sobrescrever as configurações da função Federation™ com as configurações do Security Desk para câmeras federadas:

1 Na estação de trabalho onde você deseja alterar o comportamento padrão, abra o arquivo *GeneralSettings.gconfig* com um editor de texto.

Você pode encontrar este arquivo na pasta *ConfigurationFiles*, na pasta de instalação do Security Center (*C:\Program Files (x86)\Genetec Security Center 5.7*).

2 Localize a linha que contém `<configuration>` e adicione a seguinte linha imediatamente abaixo dela:

```
<streamUsage bypassFederationDefaultStream="true"/>
```

3 Salve suas alterações e reinicie o Security Desk.

Exigências para grandes sistemas Federation™

Em uma implantação em larga escala, o Security Center pode federar milhares de sistemas remotos independentes. Porém, há limitações de hardware e software que você deve considerar.

O número de funções Federation™ que você pode hospedar em um único servidor depende do seguinte:

- Tipo de funções Federation™ que você está hospedando.
- Número de funções Federation™ que você está hospedando.
- Tipo de computador que executa o serviço Genetec™ Server.
  - Capacidade baixa: Intel Core 2 Duo 3,0 GHz, 2 GB de RAM
  - Capacidade média: Dual Core Intel Xeon 2,66 GHz, 4 GB de RAM
  - Capacidade alta: Quad Core Intel® Xeon® 2.00 GHz 4 GB de RAM

Grupo de funções Federation™

Quando um grande número de funções Federation™ são hospedadas no mesmo servidor, elas devem ser divididas em vários *grupos de funções*. Todas as funções pertencentes ao mesmo grupo de funções são executadas pelo mesmo processo na mesma máquina. Existe um limite para o número de funções com as quais um único processo pode lidar.

A tabela a seguir ajuda a determinar quantos grupos de funções você precisa no seu servidor.

NOTA: Esses cálculos pressupõem que cada sistema federado (sistema Omnicast™ ou Security Center) possui 150 câmeras.

Tipo de função	Número de funções Federation™ suportadas em um único servidor		
	Grupo de funções único (Qualquer perfil de hardware)	**Vários grupos de funções (Perfis de hardware de baixa e média capacidade)**	**Vários grupos de funções (Perfil de hardware de alta capacidade)**
Omnicast™ Federation™	40	Entre em contato com a Assistência Técnica da Genetec™.	100
Security Center Federation™	100	Entre em contato com a Assistência Técnica da Genetec™.	500

Se um único grupo de funções pode ter até 40 funções Omnicast™Federation™, um computador de alta capacidade com 100 funções Omnicast™Federation™ requer três grupos de funções separados. Um computador de alta capacidade que hospeda 500 funções do Security Center Federation™ requer cinco grupos de funções separados.

Exemplo

Você deseja federar 250 locais Omnicast™, usando uma função Omnicast™ Federation™ por local. Você pode dividir seus locais como segue:

- **Servidor A:** 40 locais Omnicast™ (*grupo de função 1*) + 40 locais Omnicast™ (*grupo de função 2*) + 20 locais Omnicast™ (*grupo de função 3*) = 100 locais Omnicast™
- **Servidor B:** 40 locais Omnicast™ (*grupo de função 1*) + 40 locais Omnicast™ (*grupo de função 2*) + 20 locais Omnicast™ (*grupo de função 3*) = 100 locais Omnicast™

- **Servidor C:** 40 locais Omnicast™ (*grupo de função 1*) + 10 locais Omnicast™ (*grupo de função 2*) = 50 locais Omnicast™.

Adicionar grupos de funções Federation™

Se você precisa hospedar um grande número de funções Federation™ no mesmo servidor, configure um grupo de funções Federation™.

Antes de iniciar

Determinar quantos grupos de funções você precisa para a sua implantação.

Para adicionar um grupo de função Federation™:

1. Abra a tarefa **Sistema** e clique na **visualização Funções**.
2. Selecione a entidade de função Federation™ (Security Center ou Omnicast™) que deseja configurar e clique na aba **Identidade**.
3. No campo **Nome**, digite **Ctrl+Shift+A**.

   A seção **Configurações avançadas** aparece na parte inferior da aba.
4. Altere o nome do **Grupo de função**, se necessário.
5. Clique em **Aplicar**.

11

Mapas

Esta seção inclui os seguintes tópicos:

- "Como trabalhar com mapas no Security Center" na página 237
- "Instalar a solução de mapeamento BeNomad" na página 238
- "Configurar a função Map Manager" na página 239
- "Conectar a função Map Manager ao provedor de mapas ESRI ArcGIS" na página 240
- "Conectar a função Map Manager a provedores de mapas baseados na Web" na página 241
- "Criar mapas" na página 244
- "Criar mapas a partir de arquivos de imagem" na página 248
- "Criar mapas por conexão a um GIS" na página 253
- "Visão geral da tarefa Map designer" na página 255
- "Objetos de mapa suportados" na página 257
- "Adicionar objetos de mapa aos seus mapas" na página 263
- "Adicionar unidades de controle de acesso aos seus mapas" na página 264
- "Adicionar áreas aos seus mapas" na página 265
- "Adicionar texto, imagens e formas aos seus mapas" na página 267
- "Adicionar portas aos seus mapas" na página 268
- "Adicionar câmeras aos seus mapas" na página 269
- "Adicionar sequências de câmeras aos seus mapas" na página 272
- "Adicionar layouts aos seus mapas" na página 273
- "Adicionar câmeras LPR aos seus mapas" na página 274
- "Adicionar alarmes aos seus mapas" na página 275
- "Adicionar áreas de detecção de intrusão em seus mapas" na página 276
- "Adicionar unidades de detecção de intrusão e entidades relacionadas em seus mapas" na página 277
- "Adicionar zonas aos seus mapas" na página 278
- "Adicionar pinos de entrada aos seus mapas" na página 279
- "Adicionar relés de saída aos seus mapas" na página 280
- "Adicionar objetos KML aos seus mapas" na página 281
- "Adicionar macros aos seus mapas" na página 282

- "Configurar opções de agrupamento de mapas no Security Center" na página 283

Como trabalhar com mapas no Security Center

Para melhorar a sua percepção situacional e aumentar a segurança do sistema, você pode utilizar mapas no Security Center para visualizar e navegar em suas instalações em tempo real, bem como gerir as suas câmaras, portas e outros sistemas de segurança.

Para usar mapas no Security Center, você deve ter o *Gestor de planos* habilitado em sua licença. Para trabalhar com seus mapas no Security Desk, você pode usar a tarefa *Mapas*, que é dedicada ao trabalho com mapas, ou a tarefa genérica *Monitoramento*.

Usando mapas, você pode fazer o seguinte:

- Aplicar panorâmica e zoom em mapas
- Navegar por mapas diferentes
- Estender um único mapa por vários monitores
- Gerir seu equipamento de segurança (câmeras, portas, zonas e assim por diante) em mapas
- Monitorar e responder a notificações em tempo real de alarmes e eventos em mapas
- Adicionar entidades locais e federadas em mapas
- Mostrar ou ocultar informações específicas (*objetos de mapa*) exibidas em mapas
- Apontar para ou clicar em objetos de mapa para visualizar informações relacionadas exibidas em um balão de texto
- Localizar dispositivos em mapas para poder ver quais outros dispositivos estão perto deles
- Marcar e pontos de interesse (saídas de incêndio, kits de primeiros socorros etc.) em mapas
- Monitorar e controlar câmeras, portas, áreas de detecção de intrusão e zonas em mapas
- Monitorar objetos em movimento (como veículos de patrulha) em mapas
- Visualizar leituras de placa de veículo e ocorrências de câmeras de LPR fixas em mapas
- Monitorar o estado dos pinos de entrada (ativos, inativos) diretamente nos mapas
- Controlar o comportamento de relês de saída diretamente em mapas
- Executar macros diretamente em mapas

Assista a este vídeo para saber mais. Clique no ícone **Legendas** (**CC**) para ligar a legenda do vídeo em um dos idiomas disponíveis. O vídeo pode não ser exibido no Internet Explorer. Para resolver isso, abra as **Configurações de compatibilidade de exibição** e limpe **Exibir sites da intranet em Visualizar compatibilidade**.

Instalar a solução de mapeamento BeNomad

Se a sua licença do Security Center suportar mapas, você pode usar a solução de mapeamento padrão *BeNomad* para fornecer mapas e informações de geocodificação reversa.

O que você deve saber

Quando a sua licença é criada, você recebe um e-mail com um arquivo compactado contendo os mapas BeNomad para sua localização geográfica e um arquivo *.glic* exclusivo que contém as informações da licença. Você precisará desses dois arquivos para instalar o BeNomad.

O BeNomad deve ser instalado em todas as máquinas cliente que executam o Security Desk.

Para instalar o BeNomad:

1. Descompacte o conteúdo do arquivo compactado BeNomad para o seu computador.
   Uma pasta chamada *BeNomad* é criada.
2. Copie a pasta *BeNomad* para a pasta do programa principal onde o Security Center está instalado.
   Em uma instalação padrão do Security Center, esta pasta é: *C:\Program Files (x86)\Genetec Security Center 5.7*.
3. Copie o arquivo de licença *.glic* do e-mail recebido para a pasta *BeNomad*.
   Os mapas BeNomad são ativados quando você inicia o Security Center.

Configurar a função Map Manager

O Map Manager é a função central que gerencia todos os recursos de mapeamento no Security Center, inclusive arquivos de mapas importados, provedores externos de mapas e objetos KML. Ele funciona como o servidor de mapas para todos os aplicativos clientes que exigem mapas. Você deve configurar essa função antes de começar a usar mapas no seu sistema.

O que você deve saber

A função Map Manager é criada por padrão na instalação do software e atribuída ao servidor principal.

Para configurar a função Map Manager:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.

2 Selecione a função Map Manager e clique na aba **Propriedades**.

3 Na seção **Provedores de mapas**, conecte o Map Manager aos provedores de mapas de terceiros.

Os provedores de mapas são sistemas *GIS*. A maioria deles exige uma licença para usar. Uma vez configurados, eles aparecem na lista de opções disponíveis ao criar mapas geográficos.

Exemplo: Você pode conectar a função Map Manager a um provedor de mapas baseado na web. Se você tiver uma licença ESRI ArcGIS, você pode conectar a função Map Manager ao provedor de mapas ESRI ArcGIS.

4 (Opcional) Na seção **Camadas de mapas**, importe os objetos KML que deseja exibir em seus mapas.

5 Configure o **Local do cache** para os seus mapas.

O cache é uma pasta onde os ladrilhos de mapas são salvos. Quando você cria mapas a partir de arquivos de imagens, a função gera um conjunto de pequenas imagens, chamadas de *ladrilhos do mapa*, para cada nível de zoom no qual você precisa visualizar o mapa. Quanto maior a escala do mapa, mais ladrilhos de mapa precisam ser gerados pela função. A pasta padrão é *C:\ProgramData\Security Center\Maps.*.

MELHOR PRÁTICA: Se você estiver configurando o failover de função, configure o cache em um local que possa ser alcançado por todos os servidores atribuídos à função. Se a função não puder alcançar a localização de cache configurada, ela irá regenerar os ladrilhos do mapa a partir dos arquivos de origem armazenados no banco de dados do Directory e salvá-los no local de cache padrão.

6 Clique em **Mapa padrão** e selecione o mapa padrão para o seu sistema.

O mapa padrão do sistema, também conhecido como *mapa padrão global*, é usado quando um usuário não tem um mapa padrão personalizado configurado. Você só pode definir o mapa padrão global depois de ter criado seu primeiro mapa.

7 Clique em **Aplicar**.

Conectar a função Map Manager ao provedor de mapas ESRI ArcGIS

Antes de criar mapas usando o provedor de mapas ArcGIS ESRI, você deve conectar a função Map Manager ao provedor de mapas.

Antes de iniciar

- Adquira uma licença ERSI *Básica* ou *Padrão* válida e certifique-se de que você conheça seu ID de cliente.
- Se você tiver uma licença ESRI *Padrão*, certifique-se de que você conheça seu código da licença. Entre em contato com a ESRI para adquirir seu código de licença.
- No site ESRI ArcGIS, baixe e instale o ArcGIS Runtime SDK para .NET versão 10.2.X.

Para obter mais informações sobre como solicitar uma licença ESRI, consulte o site ESRI ArcGIS.

O que você deve saber

O Map Manager é a função central que gerencia todos os recursos de mapeamento no Security Center, inclusive arquivos de mapas importados, provedores externos de mapas e objetos KML. Ele funciona como o servidor de mapas para todos os aplicativos clientes que exigem mapas.

Para conectar a função Map Manager ao provedor de mapas ESRI:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.
2 Selecione a função Map Manager e clique na aba **Propriedades**.
3 Na seção *Provedores de mapas*, clique em **Adicionar um item** ( ).
4 Na lista suspensa **Provedor**, na caixa de diálogo *Provedores de mapas*, selecione **ESRI**.
5 Na opção **ID de cliente**, digite o ID de cliente da sua licença ESRI.
6 Se você tiver uma licença ESRI *Padrão*, digite as seguintes informações:
   a) Na opção **Código da licença**, digite o código de licença fornecido pela ESRI.
   b) Se você estiver usando extensões de servidor local para obter funcionalidades adicionais, digite as licenças de extensões de servidor local na opção **Parâmetros da licença**.
7 Clique em **Validar**.
   Se você tiver inserido as informações corretas, o status da licença muda para **Válido**.
8 Adicione um servidor ESRI ArcGIS, da seguinte forma:
   a) Na caixa de diálogo *Provedores de mapas*, clique em **Adicionar um item** ( ).
   b) Na caixa de diálogo *Adicionar servidor*, digite o **Nome** do servidor ArcGIS.
   c) No campo **URL do servidor**, digite a URL do servidor ArcGIS.
      Use um dos seguintes formatos de URL, dependendo do tipo de servidor que você está usando:
      - Servidor de portais Web: *https://<PortalName>.maps.arcgis.com/sharing/rest*
      - Servidor de mapas online: *http://services.arcgisonline.com/arcgis/rest/services/<MapName>/MapServer*
      - Servidor online ou nas instalações: *http://<ServerName>:<PortNumber>/arcgis/rest/services*
   d) Se o servidor exigir autenticação, coloque a opção **Usar autenticação** em **Ligado** e digite o nome de usuário e a senha.
   e) Clique em **Adicionar**
9 Conforme exigido, adicione mais servidores ArcGIS para visualizar mais camadas em seu mapa.
10 Clique em **Salvar** > **Aplicar**.

Conectar a função Map Manager a provedores de mapas baseados na Web

Antes de criar mapas baseados na Web no Security Center, é necessário conectar a função Map Manager a um GIS que suporte um protocolo de serviço em ladrilhos baseado na web.

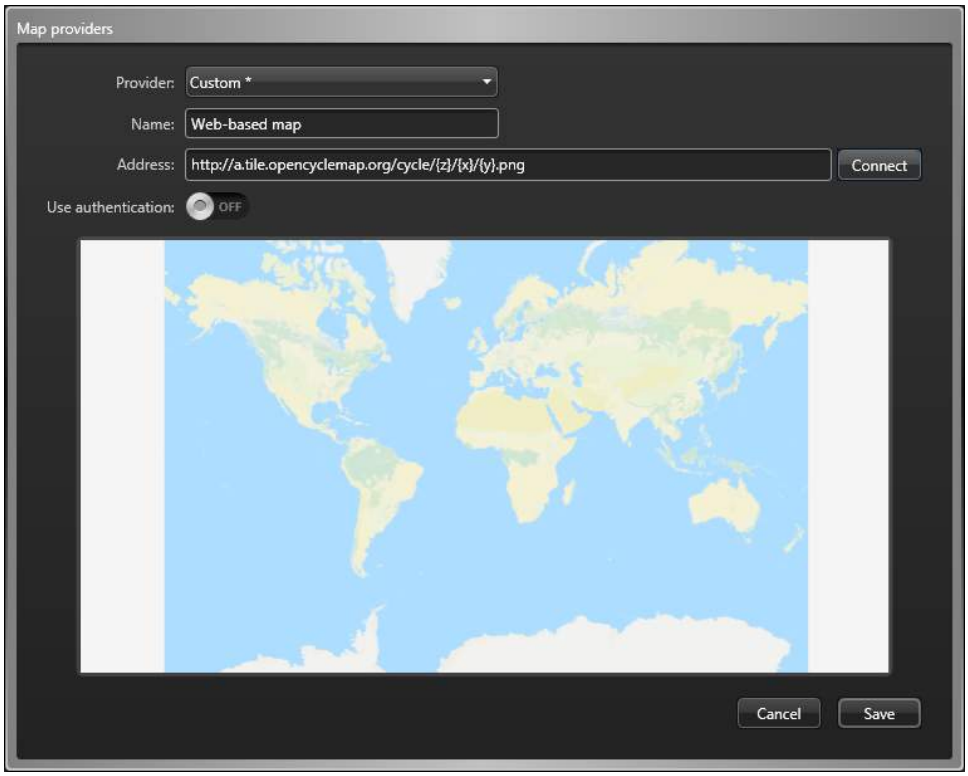
O que você deve saber

Por exemplo, você pode conectar o Map Manager a um servidor de mapas que suporte o Padrão de Implementação WMTS (Open Map Web Map Tile Service) do OpenGIS. Usando o padrão WMTS, você pode definir os limites e a escala das camadas de mapa em ladrilhos que deseja solicitar. Para obter mais informações sobre o padrão WMTS, consulte o site do Consórcio Geoespacial Aberto (OGC).

Você também pode conectar o Map Manager a mapas fornecidos pela Fundação OpenStreetMap (OSM), que usa o padrão WMTS.

Para conectar a função Map Manager a provedores de mapas baseados na Web:

1. Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.
2. Selecione a função Map Manager e clique na aba **Propriedades**.
3. Na seção **Provedores de mapas**, clique em **Adicionar um item** ( ).
4. Na lista suspensa **Provedor**, na caixa de diálogo *Provedores de mapas*, selecione **Personalizado**.
5. Na opção **Nome**, digite um nome para o provedor de mapas.
6. Na opção **Endereço**, digite a URL do servidor de mapas.
7. Clique em **Conectar**.
   Se você tiver inserido uma URL válida, o mapa será exibido.



8. Se o servidor exigir autenticação, coloque a opção **Usar autenticação** em **Ligado** e digite o nome de usuário e a senha.
9. Clique em **Salvar** > **Aplicar**.

Exemplos de formatos de URL para provedores de mapas baseados na Web

Quando você conecta a função Map Manager a um provedor de mapas baseado na Web no Security Center, o formato da URL do servidor difere em função do provedor de mapas que você está usando.

Formato de URL para servidores de mapas WMTS

Se você estiver conectando o Map Manager a um servidor de mapas que suporte o padrão WMST (Web Map Tile Service), utilize o seguinte formato de URL:

```
http://<Server>/tile/<Version>/<Layer>/<Style>/<TileMatrixSet>/{z}/{x}/{y}.<FileType>
```

Os componentes da URL são os seguintes:

Elemento da URL	Descrição
`Servidor`	A URL raiz do recurso WMTS.
`Versão`	A versão do padrão WMTS (por exemplo, `1.0.0`).
`Camada`	A camada do mapa. Para obter uma lista dos valores suportados, consulte o *documento de capacidades* do servidor.
`Estilo`	O estilo da camada de mapa (normalmente `default`). Para obter uma lista dos valores suportados, consulte o *documento de capacidades* do servidor.
`TileMatrixSet`	O conjunto de parâmetros para a camada de mapa em ladrilho. O conjunto de matriz de ladrilhos define a escala dos ladrilhos (tamanho do pixel de renderização), a largura e a altura de cada ladrilho, os limites da camada, o número de ladrilhos e assim por diante. Para obter uma lista dos valores suportados, consulte o *documento de capacidades* do servidor.
`PixelCoordParams`	As variáveis de fator de zoom {z} ou {zoom}, posição X {x} e posição Y {y} que fazem parte do padrão WMTS. Estes valores são calculados automaticamente quando você visualiza o mapa no Security Center.
`Tipo de arquivo`	O formato do arquivo (normalmente formato JPEG ou PNG). Para obter uma lista dos valores suportados, consulte o *documento de capacidades* do servidor.

Exemplo

```
http://sampleserver6.arcgisonline.com/arcgis/rest/services/WorldTimeZones/MapServer/
WMTS/tile/1.0.0/WorldTimeZones/default/default028mm/{z}/{y}/{x}.png
```

Formato de URL para OpenStreetMaps

Se você estiver conectando o Map Manager a um mapa fornecido pela OpenStreetMap Foundation, utilize o seguinte formato de URL:

```
http://<Server>/{z}/{x}/{y}.png
```

`Server` é a URL do servidor OpenStreetMap. Não são necessários outros componentes da URL.

Exemplo

```
http://a.tile.opencyclemap.org/cycle/{z}/{x}/{y}.png
```

Criar mapas

Um mapa no Security Center é um diagrama bidimensional que o ajuda a visualizar as localizações físicas de seu equipamento de segurança em uma área geográfica ou em um espaço de construção. Você pode criar mapas usando a tarefa Map designer.

Antes de iniciar

Todos os mapas devem estar anexados a uma área no Security Center. A área e o mapa anexo formam uma única entidade. É recomendável definir sua hierarquia de áreas antes de anexar os mapas.

O que você deve saber

Um mapa é composto por uma imagem de fundo estática com várias camadas de informação sobrepostas, chamadas de *objetos de mapa*. Os usuários do Security Desk podem controlar a quantidade de informação exibida em um mapa mostrando ou ocultando qualquer uma dessas camadas (objetos de mapa).

Para criar um mapa:

1 Na página inicial de Config Tool, abra a tarefa *Exibição de área*.
2 Na árvore de entidades, clique na área à qual deseja anexar o mapa.
3 Clique na aba **Identidade** e, em seguida, clique em **Criar mapa**.
A tarefa *Map designer* é aberta.
4 Selecione um dos seguintes métodos para criar o plano de fundo do mapa.
- Importe o fundo do mapa de um arquivo de imagem.
- Estabeleça conexão com um provedor de mapas.
5 Configure a visualização de mapa padrão e outras predefinições.
6 Configure as informações padrão a serem exibidas quando alguém abrir este mapa.
7 Clique em **Aplicar**.

Exemplo

Assista a este vídeo para saber mais. Clique no ícone **Legendas** (**CC**) para ligar a legenda do vídeo em um dos idiomas disponíveis. O vídeo pode não ser exibido no Internet Explorer. Para resolver isso, abra as **Configurações de compatibilidade de exibição** e limpe **Exibir sites da intranet em Visualizar compatibilidade**.

Após terminar

Adicione objetos de mapa ao seu mapa.

Tópicos relacionados
Visão geral da tarefa Map designer na página 255

Configurar predefinição de mapa

Você pode salvar exibições de mapa frequentemente usadas como predefinições de mapa para que outros usuários possam usá-las rapidamente quando precisarem.

O que você deve saber

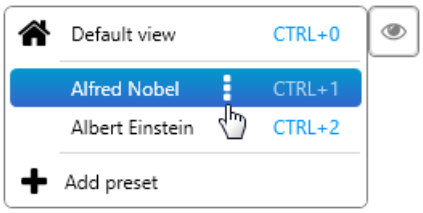
Uma visualização de mapa é uma seção definida de um mapa. Uma predefinição de mapa é uma exibição de mapa salva. Cada mapa tem pelo menos uma predefinição, chamada *exibição padrão*. É a predefinição que é exibida por padrão quando um usuário abre o mapa. Quando um usuário seleciona uma predefinição de mapa, Security Desk tenta o máximo possível encaixar a exibição de mapa na janela do mapa ajustando o nível de zoom.

Para configurar uma exibição de mapa:

1 Na tarefa *Map designer*, crie a exibição de mapa que deseja salvar.

- Arraste para mover o mapa.
- Role a roda do mouse para clicar nos botões (➕) e (➖) para aumentar ou diminuir o zoom.

2 Clique em **Selecionar predefinição** (👁).



3 Fazer um dos seguintes:

- Clique em ⋮ to anular, renomear ou excluir uma predefinição de mapa existente.
- Clique em **Adicionar predefinição** (➕) para salvar a sua exibição de mapa como uma nova predefinição.

4 Na barra de ferramentas *Map designer*, clique em **Salvar** (💾).

Para reverter as suas alterações, clique em **Cancelar** (↩) ao invés disso.

As suas alterações estão imediatamente disponíveis para usuários Security Desk.

Configurando informações padrão para exibição em mapas

Você pode definir informações padrão para exibir em seus mapas. Estas informações são sempre exibidas quando alguém abre os mapas.

O que você deve saber

Os usuários do Security Desk sempre podem definir as camadas (*objetos de mapa*) que desejam ver em seus mapas, independentemente de quais camadas são exibidas por padrão.

Para configurar as camadas a serem exibidas por padrão em um mapa:

1 No menu *Map designer*, clique em **Mapa** > **Camadas**.

É exibida uma caixa de diálogo que lista todas as camadas disponíveis para o seu mapa.

2 Selecione as camadas que deseja exibir por padrão.

Você pode optar por mostrar ou ocultar quaisquer tipos de objetos de mapa no mapa, incluindo entidades Security Center (câmeras, portas etc.), objetos KML, objetos ESRI, objetos personalizados, ocorrências e leituras de LPR e assim por diante.

3 Selecione a opção **Ocultar camadas vazias** para exibir somente as camadas que tem objetos de mapas no mapa atual.

4 Para classificar as camadas, selecione uma camada e use as setas para cima (🔼) e para baixo (🔽).

5 Na barra de ferramentas *Map designer*, clique em **Salvar** (💾).

Ajustar a opacidade das informações exibidas em mapas

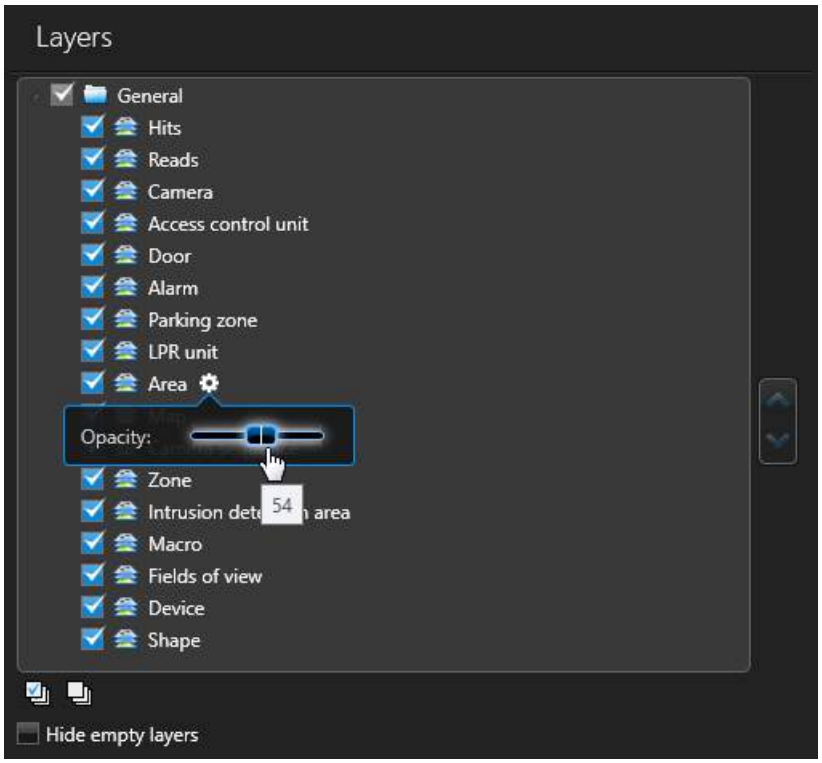
Para não obstruir informações valiosas no mapa, você pode ajustar a opacidade de uma camada de mapa. Por exemplo, uma camada que exibe padrões meteorológicos pode bloquear a visualização do nome de uma rua ou de um ponto de interesse no mapa.

O que você deve saber

Os usuários do Security Desk não podem alterar a opacidade de uma camada de mapa porque isso só pode ser feito no Config Tool.

Para ajustar a opacidade de camadas de mapa:

1 No menu *Map designer*, clique em **Mapa** > **Camadas**.
É exibida uma caixa de diálogo que lista todas as camadas disponíveis para o seu mapa.
2 Aponte para a camada que deseja alterar e clique na roda de engrenagem ( ).



3 No widget que for aberto, arraste o controle deslizante de **Opacidade** até conseguir o efeito desejado no mapa.
4 Repita com outras camadas conforme necessário.
5 Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

Configurar objetos de mapa que se movem

Para representar objetos que se movem em um mapa, você pode configurar uma camada de mapa ESRI para que seja atualizada periodicamente.

O que você deve saber

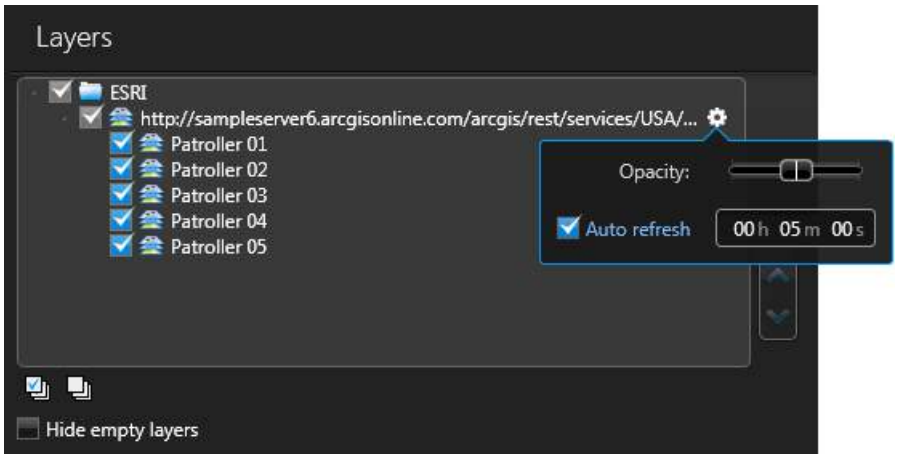
Se você tiver um objeto ESRI que seja atualizado em tempo real, você pode definir a camada de mapa correspondente para que seja atualizada periodicamente, para que essas atualizações sejam aplicadas. Por

exemplo, se tiver um objeto ESRI que rastreie a posição de um veículo em tempo real, você pode definir a camada de mapa para que seja atualizada a cada 5 minutos para mostrar o movimento desse veículo no Security Desk.

Para configurar um objeto de mapa em movimento:

1 No menu *Map designer*, clique em **Mapa** > **Camadas**.
É exibida uma caixa de diálogo que lista todas as camadas disponíveis para o seu mapa.

2 Aponte para a camada que deseja alterar e clique na roda de engrenagem ( ).



3 No widget que abrir, selecione **Atualizar automaticamente** e, em seguida, defina a taxa de atualização.

4 Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

Criar mapas a partir de arquivos de imagem

Você pode criar mapas personalizados de seu local e plantas de seus prédios, importando sua imagem de fundo a partir de arquivos de imagem.

O que você deve saber

Todos os mapas devem estar anexados a uma área.

Para criar um mapa a partir de um arquivo de imagem:

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.

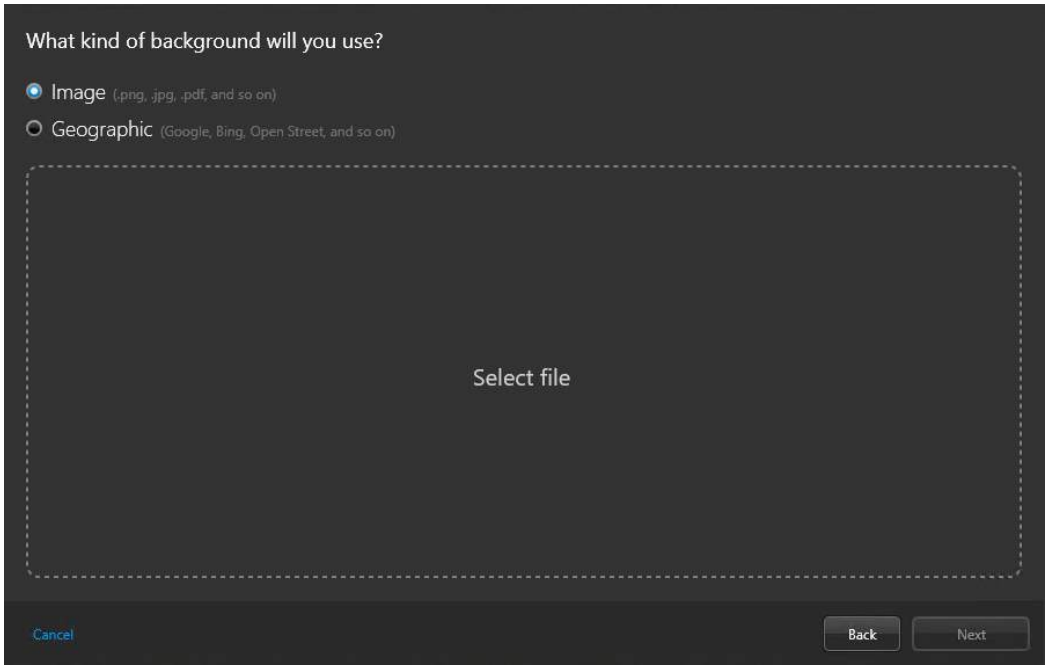
2 Clique em **Criar** ( ).

3 Na árvore de áreas, selecione a área à qual deseja anexar seu mapa ou clique em **Nova área** ( ) para criar uma nova.

4 (Opcional) Selecione o ícone para representar a sua área com um mapa (Padrão =).

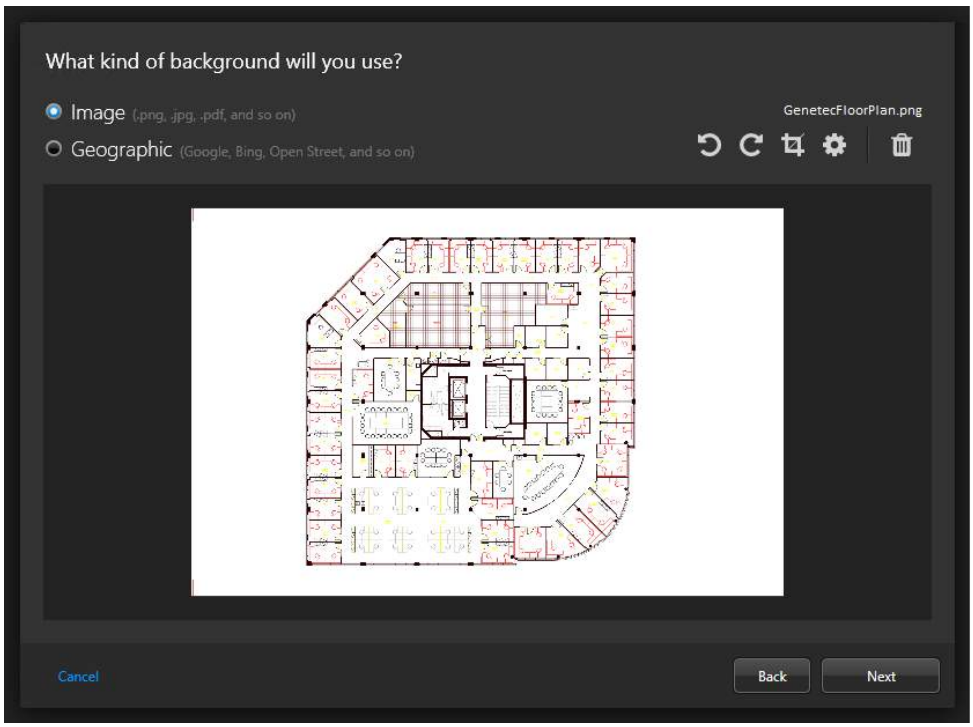
5 Clique em **Próximo**.

6 Para o tipo de plano de fundo do mapa, selecione a opção **Imagem** e clique em **Selecionar arquivo**.



7 No navegador de arquivos que aparece, selecione um arquivo de imagem (.png, .jpg, .pdf e assim por diante) e clique em **Abrir**.

A imagem selecionada aparece na janela de visualização.



8 Se necessário, mova para a página desejada e, em seguida, gire e recorte a imagem.

9 Clique em **Configurações avançadas** ( ) e configura as opções a seguir:

- **Resolução:** A resolução da imagem.
- **Fundo:** A cor do fundo da imagem.

10 Clique em **Próximo**.

11 Defina sua escala de mapa usando uma das seguintes opções:

NOTA: Como alternativa à configuração da escala do mapa, você pode georreferenciar o mapa.

- **Sala:** Planta de uma pequena área, como um refeitório ou um auditório.
- **Edifício:** Planta de uma grande área, como um andar de um prédio, um estádio ou um armazém.
- **Campus:** Mapa de local para um aeroporto, um shopping ou um campus universitário.
- **Cidade:** Mapa de cidade. Por exemplo: Montreal, Nova York, Paris, Londres, Tóquio.
- **Escala específica:** Desenhe uma linha no mapa e especifique seu comprimento exato, da seguinte forma:
  1 Na lista suspensa no topo da tela, selecione as unidades a usar para a medição (por exemplo, metros ou pés) e defina o número de unidades para corresponder à sua medida conhecida.
  2 Clique em **Desenhar linha**.
  3 Clique e arraste o mouse pelo mapa para desenhar a linha.
  4 Mova as extremidades da linha até que correspondam aos dois pontos conhecidos da sua medição.

12 Clique em **Criar** para gerar o mapa.

O mapa criado é exibido no espaço de trabalho do Map designer.

13 Configure a visualização de mapa padrão e outras predefinições.

14 Configure as informações padrão a serem exibidas quando alguém abrir este mapa.

15 Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

Após terminar

Adicione objetos de mapa ao seu mapa.

Georreferenciar uma imagem de mapa

Para garantir que todos os mapas importados respeitem a mesma escala, você pode georreferenciar cada mapa adicionando pelo menos três marcadores com coordenadas geográficas ao mapa.

Antes de iniciar

Crie um mapa partir de um arquivo de imagem.

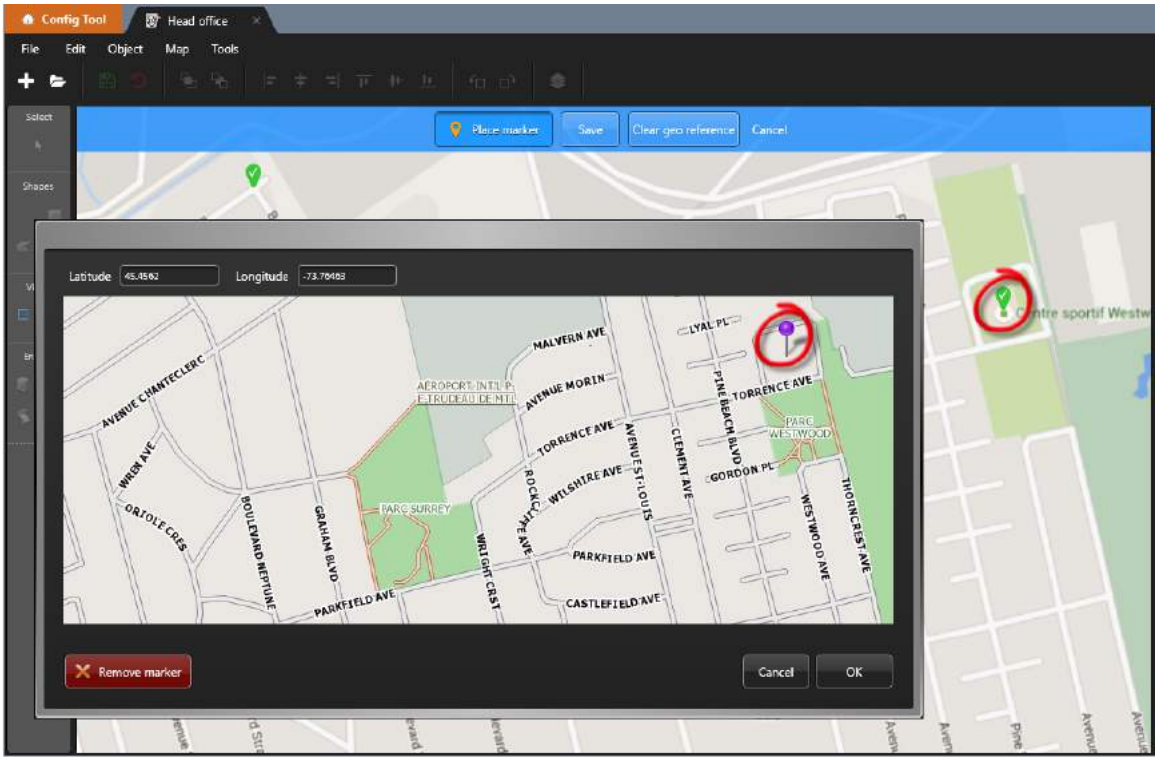
O que você deve saber

IMPORTANTE: O georreferenciamento de um mapa remove todos os objetos que foram previamente adicionados ao mapa. Os objetos precisam ser adicionados novamente depois de georreferenciar o mapa.

Para georreferenciar de uma imagem de mapa:

1 Abra a tarefa *Map Designer* e selecione o mapa que deseja georreferenciar.
2 Clique em **Mapa** > **Calibrar georreferenciamento**.
3 Clique em **Colocar marcador** e clique em um local no mapa.
Uma janela é aberta com um segundo mapa.
4 Amplie e clique no mesmo local que o marcador definido na etapa anterior.

NOTA: Se você já sabe as coordenadas exatas do local, você pode inserir a latitude e a longitude nos campos fornecidos.

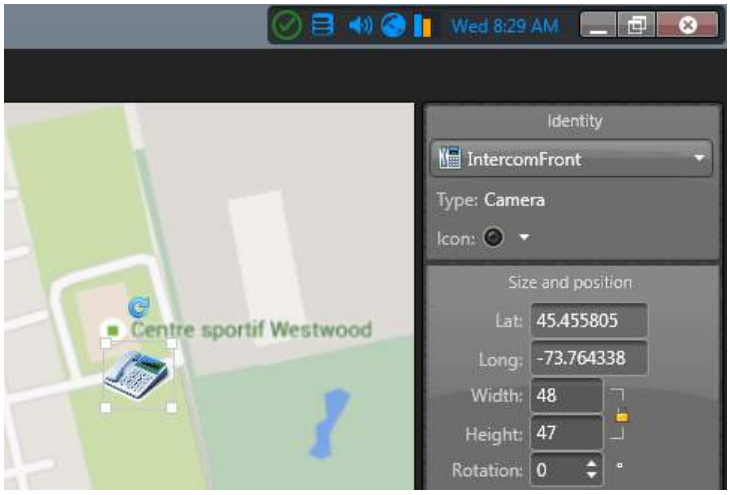


5 Para aceitar a posição do pino, clique em **OK**.
6 Repita o mesmo processo até ter georreferenciado pelo menos três posições.

DICA: A adição de marcadores adicionais aumenta a precisão de georreferenciamento.

7 Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).
8 Para verificar se o georreferenciamento está ativado no mapa, adicione um objeto ao mapa.

Se o widget *Tamanho e posição* mostrar a latitude e longitude do objeto, o mapa está georreferenciado.



Tópicos relacionados

Configurar a escala de uma imagem de mapa importada na página 251
Adicionar câmeras aos seus mapas na página 269

Configurar a escala de uma imagem de mapa importada

Para garantir que a escala do mapa corresponda à distância do campo de visão definida para as câmeras no mapa, você pode definir uma escala específica para a imagem de mapa importada após a criação do mapa.

Antes de iniciar

- Crie um mapa partir de um arquivo de imagem.
- Adicionar uma câmara ao mapa
- Conheça a distância exata entre dois pontos que aparecem no mapa.

O que você deve saber

Como alternativa para configuração da escala do mapa, você pode aplicar georreferência ao mapa.

NOTA: A escala de mapa e o georreferenciamento não podem ser definidos ao mesmo tempo.

Para configurar a escala de uma imagem de mapa importada:

1 Abra a tarefa *Map Designer* e selecione o mapa que deseja colocar em escala.
2 Clique em **Mapa** > **Editar escala**.
3 Na lista suspensa **Escala**, selecione **Escala específica**.
4 Na lista suspensa no topo da tela, selecione as unidades a usar para a medição (por exemplo, metros ou pés) e defina o número de unidades para corresponder à sua medida conhecida.
5 Clique em **Desenhar linha**.
6 Clique e arraste o mouse pelo mapa para desenhar a linha.
7 Mova as extremidades da linha até que correspondam aos dois pontos conhecidos da sua medição.
8 Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

O campo de visão da câmera e o nível de aproximação do mapa são ajustados automaticamente à escala que você definiu.

Tópicos relacionados

Adicionar câmeras aos seus mapas na página 269
Georreferenciar uma imagem de mapa na página 250

Criar mapas por conexão a um GIS

Você pode criar mapas de estradas e mapas de grande área detalhados conectando-se a um fornecedor de GIS de terceiros, também conhecido como provedor de mapas.

Antes de iniciar

Você deve conectar seu Map Manager a pelo menos um provedor de mapa externo.

Por exemplo, você pode conectar a função Map Manager ao fornecedor de mapas ArcGIS ESRI ou conectar a função Map Manager a um provedor de mapas baseado na Web.

O que você deve saber

Todos os mapas devem estar conectados a uma área.

Para criar um mapa conectando-se a um provedor de mapas:

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.

2 Clique em **Criar** ( ).

3 Na árvore de áreas, selecione a área à qual deseja anexar seu mapa ou clique em **Nova área** ( ) para criar uma nova.

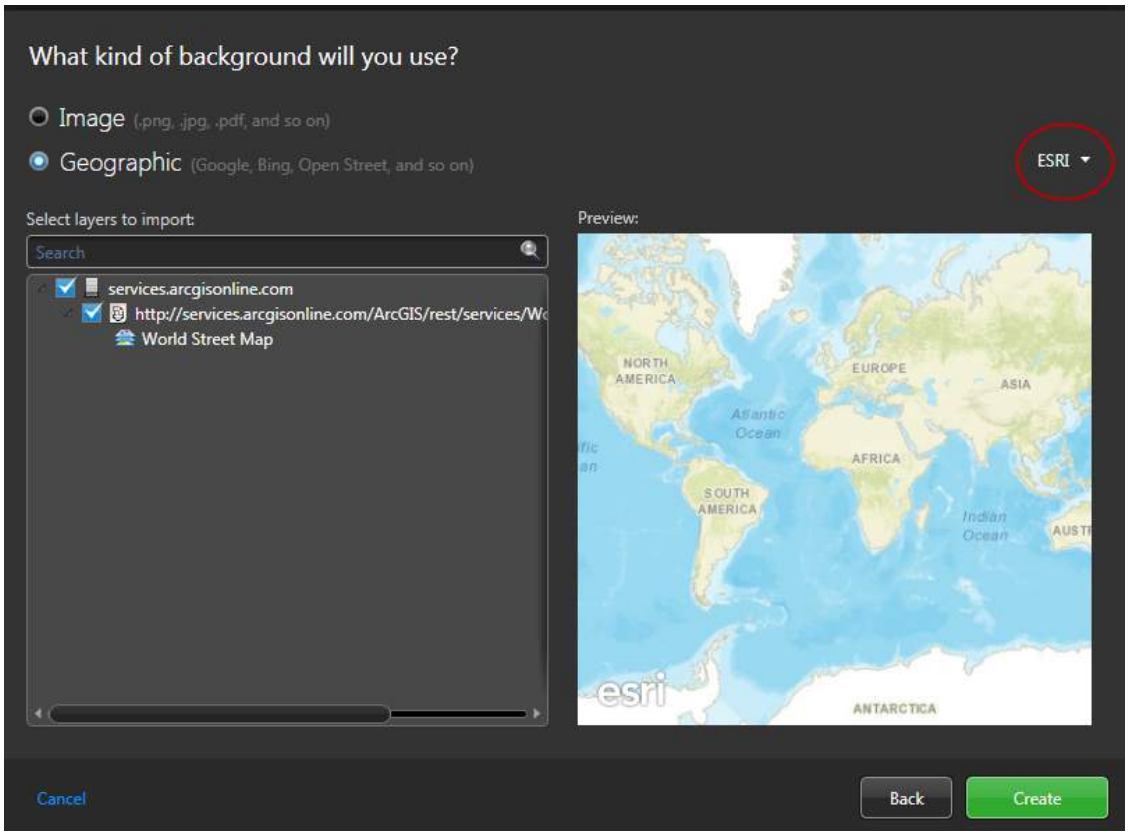
4 (Opcional) Selecione o ícone para representar a sua área com um mapa (Padrão =).

5 Clique em **Próximo**.

6 Para o tipo de plano de fundo do mapa, selecione a opção **Geográfica**.

7 Clique na lista suspensa à direita e selecione o provedor de mapa desejado.

Exemplo: Se você conectou a função Map Manager ao provedor de mapas do ESRI ArcGIS, selecione **ESRI**.



8 Dependendo do provedor de mapa selecionado, talvez seja necessário selecionar quais mapas e camadas você deseja importar.

NOTA: Se você importar vários mapas da web do ESRI ArcGIS que compartilham as mesmas camadas de mapa, você poderá ter problemas com a exibição, ocultação ou classificação de camadas de mapa. Para evitar esse problema, importe apenas um mapa da web ESRI.

9 Clique em **Criar**.

O mapa criado é exibido no espaço de trabalho do Map designer.

10 Configure a visualização de mapa padrão e outras predefinições.

11 Configure as informações padrão a serem exibidas quando alguém abrir este mapa.

12 Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

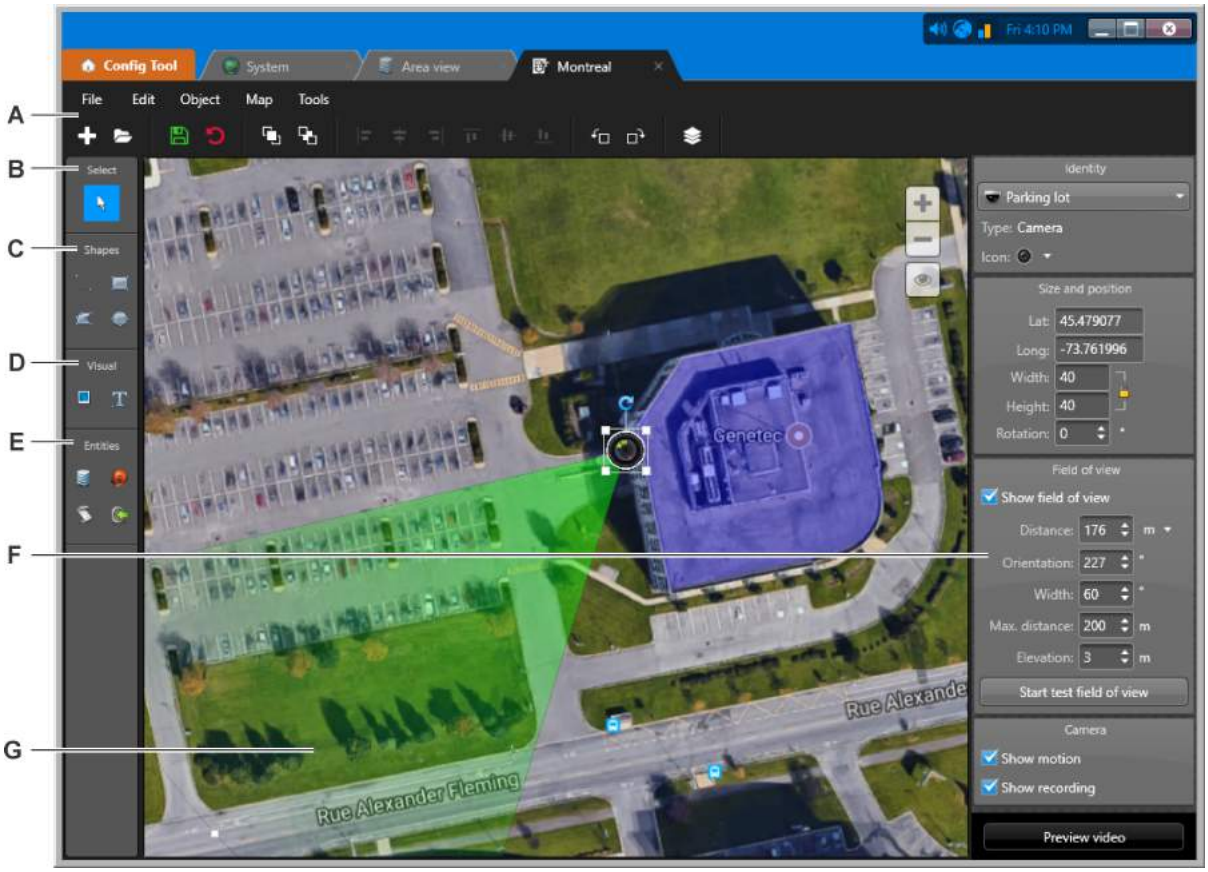
Após terminar

Adicione objetos de mapa ao seu mapa.

Visão geral da tarefa Map designer

Use a tarefa Map designer para criar e editar mapas que representam as localizações físicas do seu equipamento para usuários do Security Desk.

Um mapa no Security Center é um diagrama bidimensional que o ajuda a visualizar as localizações físicas de seu equipamento de segurança em uma área geográfica ou em um espaço de construção. A figura a seguir mostra a tarefa *Map designer* editando um mapa chamado "Montreal" em um sistema de monitoramento de vídeo.



A	Use o menu e a barra de ferramentas de *Map designer* para criar, editar e excluir os mapas em seu sistema, bem como organizar os *objetos de mapa* no seu mapa.
B	**Ferramenta de seleção** ( ): Clique em um objeto de mapa para selecioná-lo. Você também pode escolher entre as seguintes opções: • Clique e mantenha clicado o fundo do mapa para movê-lo. • Amplie uma área do mapa mantendo pressionada a tecla Ctrl e, em seguida, clicando e arrastando. • Selecione vários objetos de mapa com um retângulo mantendo pressionada a tecla Alt e, em seguida, clicando e arrastando. • Selecione todos os objetos de mapa do mesmo tipo que estão em exibição mantendo pressionada a tecla Alt e, em seguida, clicando em um objeto de mapa.

C	Desenhar objetos de vetor: • **Desenhar linha:** Clique e arraste para desenhar um único segmento de linha para representar uma parede. • **Desenhar retângulo:** Clique e arraste para desenhar um retângulo. Arraste uma alça para alterar o tamanho. Observe que não é possível alterar um retângulo para um tipo de polígono diferente. • **Desenhar polígono:** Clique uma vez para cada extremidade e clique na primeira extremidade para fechar o polígono. Use Shift+clique para adicionar ou remover um ponto entre dois pontos. Clique duas vezes em um ponto para completar um polígono sem fechá-lo. • **Desenhar elipse:** Clique e arraste para desenhar uma elipse. Arraste uma alça para alterar o tamanho.
D	Inserir imagens e texto: • **Inserir imagem:** Abre um navegador para selecionar um arquivo de imagem e clicar para posicioná-lo no mapa. • **Inserir texto:** Clique para colocar uma caixa de texto no mapa. Clique duas vezes na caixa de texto para digitar o texto. Use os widgets para ajustar a aparência do texto.
E	Criar objetos de mapa que representam entidades: • **Exibição de área:** Clique na exibição de área para criar objetos de mapa que representam áreas, áreas de detecção de intrusão, câmeras, sequências de câmera, layouts de monitoramento, portas, câmeras LPR e zonas. • **Alarmes:** Clique, selecione e arraste uma alarme até o mapa. • **Macros:** Clique, selecione e arraste macros até o mapa. • **Entradas/Saídas:** Clique, selecione e arraste um pino de entrada, um relê de saída ou uma unidade até o mapa. **NOTA:** É possível selecionar Entradas/Saídas federadas e câmeras locais.
F	Use os widgets para configurar o objeto de mapa selecionado. Quando vários objetos de mapa são selecionados, somente os widgets comuns são exibidos.
G	Clique e arraste o FOV para posicioná-lo no mapa.

Objetos de mapa suportados

Os objetos de mapa são representações gráficas de entidades do Security Center ou qualquer característica geográfica (cidades, estradas, rios e assim por diante) nos seus mapas. Com objetos de mapa, você pode interagir com seu sistema sem sair do mapa.

Os objetos de mapa são exibidos no mapa como ícones dinâmicos ou como formas coloridas às quais você pode apontar e clicar. A aparência da maioria dos objetos de mapa pode ser configurada.

Os seguintes objetos de mapa da tabela são suportados:

Objeto mapa	Aparência nos mapas	Aplicação e ações específicas
Unidade de controle de acesso	 - Unidade de controle de acesso A cor indica o estado da unidade de controle de acesso: *On-line*, *Off-line* ou *Aviso*.	Monitore o estado da unidade de controle de acesso.
Área	• Miniatura do mapa (sempre ligada ao mapa que é representado pela miniatura) • Polígono semi-transparente colorido ou elipse (pode ou não ser ligado a um mapa)	• Aponte para mostrar a contagem de pessoas ou a presença de pessoas (se ativado). • Remova os titulares do cartão selecionados da área. • Clique para exibir a área ou o mapa em uma bolha de ladrilho ou para alternar para o mapa vinculado, se um estiver definido.
Porta	•  - Porta aberta •  - Porta fechada (sem tranca configurada) •  - Porta fechada e trancada •  - Porta fechada e destrancada •  Porta aberta com força •  - Porta destravada e em modo de manutenção • Os eventos são exibidos em balões de notificação de eventos. A cor do balão corresponde à cor atribuída ao evento.	• Monitorar alarmes e estados de porta e eventos. • Coloque o ponteiro para conhecer mais detalhes. • Clique no balão de notificação para transformá-lo em um balão de ladrilho. • Desbloqueie a porta, substitua o cronograma de desbloqueio e desvie o leitor do widget da porta, ou clique com o botão direito do mouse na porta do mapa.

Objeto mapa	Aparência nos mapas	Aplicação e ações específicas
Câmera	•  - A câmera não está gravando •  - A câmera está gravando •  - A câmera detecta movimento (com efeito de ondulação verde) •  - A câmera está em modo de manutenção • Câmeras fixas são mostradas com um FOV azul (campo de visão). • Câmeras PTZ são mostradas com um FOV verde.	• Monitorar alarmes e eventos da câmera. • Clique para ver o vídeo ao vivo ou de reprodução em uma bolha de ladrilho. • Clique e arraste o FOV para ajuste horizontal e vertical (somente se a câmera suportar retorno de posição). • Use o widget PTZ para ampliar e reduzir. • Clique em um local no mapa enquanto mantém pressionada a tecla CTRL para apontar todas as câmeras disponíveis para esse local.
Sequência de câmera	•  - Sequência de câmera	• Exibir várias câmeras ao mesmo tempo. • Aponte várias câmeras PTZ para um local específico. • Clique duas vezes na sequência da câmera para exibir todas as câmeras em blocos separados na tarefa de *Monitoramento*. Se o mapa for exibido em um ladrilho, ele não será substituído se os ladrilhos estiverem cheios. **NOTA:** Ao usar o controle de mapa **Localize-me**, você obterá resultados para câmeras individuais que fazem parte da sequência. A sequência da câmera não é encontrada pelo controle **Localize-me**.
Layout	•  - Layout • Um objeto de mapa vinculado a um layout de tarefa de monitoramento salvo previamente.	• Clique para exibir as câmeras monitoradas como uma sequência em uma balão de ladrilho. • Clique duas vezes para exibir todas as câmeras em blocos separados na tarefa de *Monitoramento*. Se o mapa for exibido em um ladrilho, ele não será substituído se os ladrilhos estiverem cheios.
Câmera LPR	•  - Câmera LPR fixa •  - A câmera LPR está em modo de manutenção • Leituras e alertas são mostrados em bolhas de notificação.	• Leituras e alertas do monitor a partir das câmeras LPR. • Clique para ver o vídeo ao vivo da câmera de contexto associada.

Objeto mapa	Aparência nos mapas	Aplicação e ações específicas
Alarme	•  - O alarme está inativo •  - O alarme está ativo • Polígono semi-transparente ou elipse que transforma a cor do alarme e pisca se o alarme estiver ativo. • Um objeto do mapa conectado a um alarme ativo é marcado com um balão de notificação de alarme. A cor da bolha corresponde à cor atribuída ao evento.	• Mostra alarmes em mapas (útil quando nenhuma entidade anexada ao alarme é representada nos mapas). • Coloque o ponteiro para conhecer mais detalhes. • Clique no balão de notificação para transformá-lo em um balão de ladrilho. • (Inativo) Clique para disparar o alarme manualmente. • (Ativo) Clique para exibir o alarme em uma bolha de ladrilho.
Área de detecção de intrusão	•  - Área de detecção de intrusão • Os diferentes estados são: *Desarmado (não preparado)*, *Desarmado (pronto para armar)*, *Armando*, *Perímetro armado*, *Mestre armado* e *Alarme ativo*. • As cores dos estados são configuráveis e o ícone pode ser exibido ou escondido dependendo do estado.	• Monitorar alarmes e estado de área de detecção de intrusão. • Arme ou desarmar a área de detecção de intrusão a partir do widget ou clicando com o botão direito do mouse no objeto de mapa. • Ativar, silenciar ou reconhecer um alarme de intrusão a partir do widget de área de detecção de intrusão ou clicando com o botão direito do mouse no objeto de mapa.

Objeto mapa	Aparência nos mapas	Aplicação e ações específicas
Pino de entrada	• - Entrada em estado *Normal* • - Entrada em estado *Ativo* • - Entrada em estado *Problema* • Os diferentes estados são: *Normal*, *Ativo*, *Problema (curto-circuito)*, *Problema(circuito aberto)* e *Indisponível*. • As cores dos estados são configuráveis e o ícone pode ser exibido ou escondido dependendo do estado.	• Monitorar o estado de entrada. • Monitoramento da área de detecção de intrusão. As entradas usadas para a detecção de intrusão possuem indicadores visuais adicionais: • O estado *Desvio* é indicado com um 'X' sobreposto ao ícone de entrada. Com o privilégio *propriedades Modificar unidade de detecção de intrusão*, você pode desconsiderar uma entrada ou limpar um desvio clicando com o botão direito no ícone da entrada e selecionando a partir do menu de contexto. • O estado *Alarme ativo* é indicado por um halo vermelho pulsante ao redor do ícone da entrada. • Clicar com o botão esquerdo em um pino da entrada de intrusão exibirá um pop-up com o nome, código de cores dos estados, estado do alarme, estado do desvio e áreas relacionadas da entidade.
Zona	• - Zona • - Zona virtual • - Zona de E/S • Os diferentes estados são: *Desarmado*, *Normal*, *Ativo* e *Problema*. • As cores dos estados são configuráveis e o ícone pode ser exibido ou escondido dependendo do estado.	• Monitorar alarmes e o estado da zona. • Armar e desarmar a zona do widget.

Objeto mapa	Aparência nos mapas	Aplicação e ações específicas

Relé de saída	•  - Relé de saída (normal)
	•  - Relé de saída (ativo)
		• Acionar comportamentos de saída em relês de saída diretamente de mapas.
		• Clique com o botão esquerdo para exibir uma lista de comportamentos de saída que você pode acionar.
		• Para saídas de intrusões:
		  • Com o privilégio *Acionar saída*, clique com o botão direito no ícone de saída para alterar o estado de saída de normal para ativo, ativo para normal ou desconhecido para normal ou ativo a partir de um menu de contexto.
		  • Clique com o botão esquerdo para exibir um pop-up com o nome, estado e comportamentos de saída atribuídos da etidade.

Objeto KML	• Pode ser qualquer coisa exibida como uma camada transparente em um mapa georreferenciado.	• Sobreponha informações úteis em mapas, como limites de cidades, estradas e recursos hidrográficos. Clique para exibir esta informação.
Objeto ESRI	• Objetos clicáveis que vêm como parte dos mapas ESRI (similar em função aos objetos KML).	• Sobreponha informações úteis em mapas, como limites de cidades, estradas e recursos hidrográficos. Clique para exibir esta informação. • Pode representar objetos em movimento, tais como veículos de patrulha, atualizando a sua posição no mapa em intervalos regulares.
Macro	•  - Macro	• Executar macros diretamente em mapas. • Substitua o contexto de execução padrão em mapas. • Clique em uma macro para executá-la.
Link de mapa	Um link de mapa é um objeto que leva você a outro mapa com um simples clique. Os links de mapa podem ser representados como miniaturas de mapa, ou quaisquer textos, ícones, imagens ou formas geométricas coloridas.	• Navegação de mapas sem usar a barra de ferramentas de Mapas. • Útil quando o mapa é exibido na tarefa *Monitoramento*. • Clique para mudar para o mapa associado.

Objeto mapa	Aparência nos mapas	Aplicação e ações específicas
Texto, imagens e formas geométricas	Texto, ícones, imagens e formas geométricas coloridas (polígonos e elipses) podem ser adicionados aos mapas para fornecer informações adicionais, indicar a localização de pontos de interesse ou servir como links de mapas ou alarmes.	Um aplicativo de exemplo pode ser para indicar a localização dos scanners montados na parede de um piso de loja de departamento.
Objeto personalizado	Os objetos personalizados podem ser adicionados ao mapa como ícones ou polígonos para adicionar comportamento personalizado ao mapa.	Os exemplos de objetos personalizados incluem: solução de intercomunicação personalizada, rastreador GPS para unidades móveis. Entre em contato com o seu representante da Genetec Inc. para obter informações sobre Genetec™ Custom Solutions.
Bolha de cluster	Um grupo de três ou mais objetos de mapa próximos uns dos outros são representados por uma bolha de cluster azul.	Clique para aumentar a vista do mapa e visualizar os objetos de mapa individuais.

Adicionar objetos de mapa aos seus mapas

Você deve adicionar objetos de mapa aos seus mapas para que seus mapas sejam interativos.

Antes de iniciar

Crie onde você deseja adicionar os objetos do mapa.

O que você deve saber

- Os objetos de mapa são representações gráficas de entidades do Security Center ou qualquer característica geográfica (cidades, estradas, rios e assim por diante) nos seus mapas. Com objetos de mapa, você pode interagir com seu sistema sem sair do mapa.
- Se estiver criando um mapa que compartilha câmeras ou outras entidades com outro mapa, você pode copiar e colar as entidades e suas configurações de um mapa para outro.

Para adicionar um objeto de mapa ao seu mapa:

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.
2 Selecione um dos **Mapas recentes** ou clique em **Explorar todos os mapas** para abrir um mapa existente.
O mapa selecionado preenche o espaço de trabalho do Map designer.
3 Fazer um dos seguintes:
   - Adicione uma unidade de controle de acesso.
   - Adicionar área.
   - Adicionar porta.
   - Adicionar uma câmera.
   - Adicionar sequência de câmera.
   - Adicionar layout.
   - Adicionar uma câmera fixa de LPR.
   - Adicionar um alarme.
   - Adicionar uma área de detecção de intrusão.
   - Adicionar unidades de detecção de intrusão e entidades relacionadas em seus mapas na página 277
   - Adicionar uma zona.
   - Adicionar um pino de entrada.
   - Adicionar um relé de saída.
   - Adicionar um objeto KML.
   - Adicionar uma macro.
   - Adicionar um ponto de interesse.

Após terminar

Visualize e teste seus objetos de mapa no Security Desk com a tarefa *Mapas*.

Tópicos relacionados

Visão geral da tarefa Map designer na página 255

Adicionar unidades de controle de acesso aos seus mapas

Você pode adicionar unidades de controle de acesso aos seus mapas para permitir que os operadores do Security Desk monitorem controle de acesso e estados de unidades dos mapas.

Antes de iniciar

- Crie o mapa para o qual você deseja adicionar sua unidade de controle de acesso.
- Certifique-se de ter unidades de controle de acesso em seu sistema.

Para adicionar uma unidade de controle de acesso ao seu mapa

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.

2 Selecione um dos **Mapas recentes** ou clique em **Explorar todos os mapas** para abrir um mapa existente.

O mapa selecionado preenche o espaço de trabalho do Map designer.

3 Na barra de ferramentas, clique em **I/Os** (), selecione a unidade de controle de acesso () que deseja vincular e arraste-a para onde desejar que ela esteja no mapa.

Os widgets para configurar o objeto de mapa aparecem no painel da direita. O objeto de mapa sempre assume a identidade da entidade que representa.

4 Na barra de ferramentas *Map designer*, clique em **Salvar** ().

Adicionar áreas aos seus mapas

Você pode adicionar áreas aos seus mapas para permitir que os operadores do Security Desk as usem como links para mapas, monitorem a contagem de pessoas, exibam a presença de pessoas ou tudo o que foi mencionado antes.

Antes de iniciar

Crie o mapa onde você deseja adicionar suas áreas.

O que você deve saber

- As áreas que têm um mapa anexado são representadas como miniaturas de mapa por padrão. As miniaturas de mapa servem para ser usadas como *links para mapas*.
- As áreas que não têm um mapa anexado são representadas como tetrágonos por padrão. Você pode alterá-los mais tarde para qualquer tipo de polígono.
- Você também pode usar qualquer ícone, imagem ou forma geométrica para representar áreas no mapa.

Para adicionar uma área ao seu mapa:

1 Tome uma das seguintes ações:
   - Adicione uma área como uma miniatura de mapa.
   - Adicione uma área para monitorar contagens de pessoas.
   - Adicione uma área como uma forma ou imagem personalizada.
2 Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

Tópicos relacionados

Visão geral da tarefa Map designer na página 255

Adicionar áreas como miniaturas de mapa em seus mapas

Você pode adicionar áreas com um mapa anexado, como miniaturas de mapa a um mapa, e usá-las como links de mapa.

Antes de iniciar

- Crie o mapa onde você deseja adicionar suas miniaturas de mapa.
- Certifique-se de ter outros mapas aos quais você deseja vincular a partir do seu mapa atual.

Para adicionar uma área como uma miniatura de mapa ao seu mapa:

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.
2 Selecione um dos **Mapas recentes** ou clique em **Explorar todos os mapas** para abrir um mapa existente.
   O mapa selecionado preenche o espaço de trabalho do Map designer.
3 Na barra de ferramentas, clique em **Exibição de área** ( ), selecione o mapa ( ) ao qual deseja vincular e arraste-o para onde deseja que sua miniatura esteja no mapa atual.
   Uma grande miniatura do mapa de destino é exibida no seu mapa atual.
4 Redimensione e posicione a miniatura no local desejado usando o mouse.
5 Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

Adicionar áreas para contagem de pessoas em seus mapas

Você pode adicionar áreas protegidas aos seus mapas para ver contagens de pessoas nos mapas.

Antes de iniciar

- Crie o mapa onde você deseja adicionar suas áreas.
- Certifique-se de ter áreas protegidas configuradas para contagem de pessoas em seu sistema.

Para adicionar uma área para contagem de pessoas em seu mapa.

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.

2 Selecione um dos **Mapas recentes** ou clique em **Explorar todos os mapas** para abrir um mapa existente.
O mapa selecionado preenche o espaço de trabalho do Map designer.

3 Na barra de ferramentas, clique em **Exibição de área** (), selecione a área protegida () que deseja adicionar e arraste-a para onde desejar que ela esteja no mapa.
Um tetrágono aparece no mapa.

4 Arraste os cantos do tetrágono para cobrir o espaço físico que a área protegida representa no mapa
Use Shift+clique para adicionar ou remover um ponto entre dois pontos.

5 Use o widget **Cor e borda** para alterar os atributos de exibição do objeto de mapa.
Selecione **Bloquear campo de visão** se o perímetro da área protegida corresponder às paredes reais.

6 (Opcional) Clique em **Não atribuído** no widget **Links** para transformar o objeto de mapa em um *link de mapa*.

NOTA: Se você adicionar múltiplos links ao objeto de mapa, o operador terá que clicar três vezes para chegar a um link. O primeiro clique exibe a entidade que identifica o objeto de mapa. O segundo clique exibe as escolhas de links. O terceiro clique seleciona um link.

7 Na barra de ferramentas *Map designer*, clique em **Salvar** ().

Adicionar texto, imagens e formas aos seus mapas

Você pode adicionar texto, imagens e formas aos seus mapas para indicar pontos de interesse ou para representar entidades no mapa com algo diferente do aspecto padrão. Esses objetos de mapa também podem ser duplicados como links de mapas.

Antes de iniciar

Crie o mapa onde você deseja adicionar seus objetos gráficos

O que você deve saber

Entidades normalmente representadas por polígonos, como áreas, áreas de detecção de intrusão e zonas, podem ser atribuídas a objetos gráficos personalizados. Os alarmes também podem ser atribuídos a objetos gráficos personalizados.

Para adicionar um texto ou uma imagem ao seu mapa:

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.

2 Selecione um dos **Mapas recentes** ou clique em **Explorar todos os mapas** para abrir um mapa existente.

O mapa selecionado preenche o espaço de trabalho do Map designer.

3 Na barra de ferramentas, clique em uma das seguintes ferramentas para inserir um objeto gráfico:

- **Desenhar retângulo:** Clique e arraste para desenhar um retângulo. Arraste uma alça para alterar o tamanho. Observe que não é possível alterar um retângulo para um tipo de polígono diferente.
- **Desenhar polígono:** Clique uma vez para cada extremidade e clique na primeira extremidade para fechar o polígono. Use Shift+clique para adicionar ou remover um ponto entre dois pontos. Clique duas vezes em um ponto para completar um polígono sem fechá-lo.
- **Desenhar elipse:** Clique e arraste para desenhar uma elipse. Arraste uma alça para alterar o tamanho.
- **Inserir imagem:** Abre um navegador para selecionar um arquivo de imagem e clicar para posicioná-lo no mapa.
- **Inserir texto:** Clique para colocar uma caixa de texto no mapa. Clique duas vezes na caixa de texto para digitar o texto. Use os widgets para ajustar a aparência do texto.

4 (Opcional) No widget **Físico**, selecione **Bloquear campo de visão** para usar os objetos para bloquear FOVs de câmeras no mapa.

NOTA: A opção **Bloquear campo de visão** não está disponível para elipses.

5 (Opcional) Clique em **Não atribuído** no widget **Identidade** para atribuir uma entidade ao seu objeto de mapa.

Os objetos de mapa herdam sua identidade da entidade que eles representam. Você não precisa atribuir uma entidade ao objeto de mapa se você estiver usando apenas para indicar um ponto de interesse. Os objetos de mapa que não são atribuídos a uma entidade não têm nome.

6 (Opcional) Clique em **Não atribuído** no widget **Links** para transformar o objeto de mapa em um *link de mapa*.

NOTA: Se você adicionar múltiplos links ao objeto de mapa, o operador terá que clicar três vezes para chegar a um link. O primeiro clique exibe a entidade que identifica o objeto de mapa. O segundo clique exibe as escolhas de links. O terceiro clique seleciona um link.

7 Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

Adicionar portas aos seus mapas

Você pode adicionar portas aos seus mapas para permitir que os operadores do Security Desk monitorem eventos de portas, gerenciem alarmes e controlem fechaduras e leitores de mapas.

Antes de iniciar

- Crie o mapa onde você deseja adicionar suas portas.
- Certifique-se de que você tem porta no sistema do Security Center.

Adicionar uma porta ao seu mapa:

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.
2 Selecione um dos **Mapas recentes** ou clique em **Explorar todos os mapas** para abrir um mapa existente.
O mapa selecionado preenche o espaço de trabalho do Map designer.
3 Na barra de ferramentas, clique em **Vista de área** ( ), selecione a porta que deseja adicionar e arraste-a para onde desejar que ela esteja no mapa.
Os widgets para configurar o objeto de mapa aparecem no painel da direita. O objeto de mapa sempre assume a identidade da entidade que representa.
4 Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

Tópicos relacionados

Visão geral da tarefa Map designer na página 255

Adicionar câmeras aos seus mapas

Você pode adicionar câmeras aos seus mapas para permitir que os operadores do Security Desk monitorem vídeo ao vivo e eventos de câmeras, gerenciem alarmes e controlem câmeras PTZ e gravações a partir de mapas.

Antes de iniciar

- Crie o mapa onde você deseja adicionar suas câmeras.
- Certifique-se de ter câmeras no seu sistema Security Center.

O que você deve saber

Para criar um efeito mais realista quando o mapa é exibido na tarefa Mapas ou na tarefa Monitoramento no Security Desk, você pode bloquear o campo de visão de suas câmeras ao desenhar paredes e outros obstáculos em seu mapa..

Para adicionar uma câmera ao seu mapa:

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.

2 Selecione um dos **Mapas recentes** ou clique em **Explorar todos os mapas** para abrir um mapa existente.

O mapa selecionado preenche o espaço de trabalho do Map designer.

3 Na barra de ferramentas, clique em **Exibição de área** (), selecione a câmera que deseja adicionar e arraste-a para onde desejar que ela esteja no mapa.

Os widgets para configurar o objeto de mapa aparecem no painel da direita. O objeto de mapa sempre assume a identidade da entidade que representa.

4 Clique em **Visualizar vídeo** para mostrar uma visualização do vídeo ao vivo em um balão de ladrilho.

5 Selecione **Mostrar campo de visão** e defina as propriedades de FOV.

IMPORTANTE: Você deve definir as propriedades de FOV mesmo que você não pretenda mostrar o FOV no mapa. A orientação, a largura e a distância máxima do FOV são necessárias para que o recurso *Clique inteligente* funcione corretamente.

DICA: Alternativamente, você pode ajustar a orientação e o comprimento do FOV com o mouse.

NOTA: Se o mapa ao qual você está adicionando a câmera for um arquivo de imagem importado, você deve definir a escala do mapa para dar significado às distâncias nas propriedades do campo de visão. Você pode fazer isso georreferenciando o mapa ou definindo a escala do mapa.

- **Distância:** Comprimento do FOV como ele aparece no mapa.
- **Orientação:** Direção que a câmera está apontando.
- **Largura:** Largura do FOV como ele aparece no mapa.
- **Distância máxima:** Até que distância a câmera pode ver. Principalmente para cálculos de *Clique inteligente*.
- **Elevação:** Distância da câmera ao chão.

  DICA: Clicar em **Iniciar campo de visão de teste** mostra pontos cegos criados por outros objetos no mapa.

6 Selecione os eventos de câmeras que deseja monitorar no mapa.

- **Mostrar o movimento:** Mostra o ícone da câmera com um efeito de ondulação verde () no evento *Movimento ativo*.
- **Mostrar gravação:** Mostra o ícone da câmera com um botão vermelho () quando a gravação está ativada.

7 Na barra de ferramentas *Map designer*, clique em **Salvar** ().

Tópicos relacionados

Configurar a escala de uma imagem de mapa importada na página 251
Georreferenciar uma imagem de mapa na página 250
Visão geral da tarefa Map designer na página 255
Desenhar paredes para bloquear o campo de visão de suas câmeras na página 270

Desenhar paredes para bloquear o campo de visão de suas câmeras

Para criar um efeito mais realista quando o mapa é exibido na tarefa Mapas ou na tarefa de Monitoramento no Security Desk, você pode bloquear o campo de visão de suas câmeras ao desenhar paredes e outros obstáculos em seu mapa.

O que você deve saber

Somente linhas, retângulos e polígonos podem ser usados para bloquear o campo de visão (FOV) das câmeras. Texto, imagens e formas elípticas não podem ser usados para o bloqueio.

Para desenhar um objeto para bloquear o FOV das câmeras:

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.

2 Selecione um dos **Mapas recentes** ou clique em **Explorar todos os mapas** para abrir um mapa existente.
O mapa selecionado preenche o espaço de trabalho do Map designer.

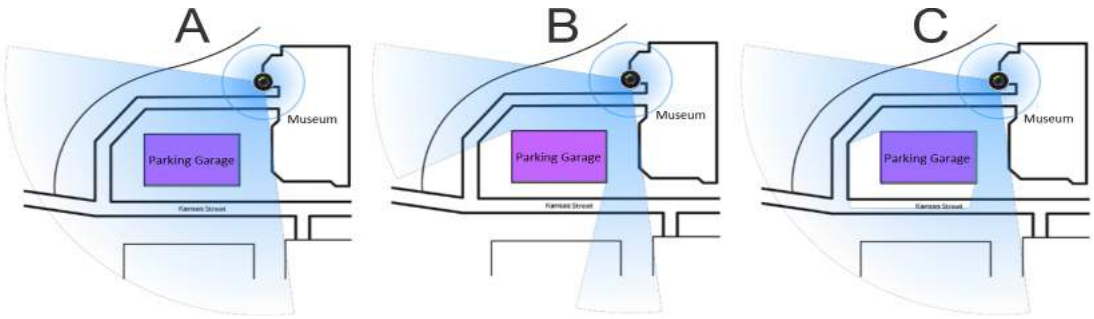
3 Na barra de ferramentas, clique em uma das seguintes ferramentas para inserir um objeto gráfico:

- **Desenhar linha:** Clique e arraste para desenhar um único segmento de linha para representar uma parede.
- **Desenhar retângulo:** Clique e arraste para desenhar um retângulo. Arraste uma alça para alterar o tamanho. Observe que não é possível alterar um retângulo para um tipo de polígono diferente.
- **Desenhar polígono:** Clique uma vez para cada extremidade e clique na primeira extremidade para fechar o polígono. Use Shift+clique para adicionar ou remover um ponto entre dois pontos. Clique duas vezes em um ponto para completar um polígono sem fechá-lo.

Os widgets para configurar o objeto de mapa aparecem no painel da direita. O objeto de mapa sempre assume a identidade da entidade que representa.

4 No widget **Físico**, selecione **Bloquear campo de visão** e defina a **Elevação** da parede. Usando esta elevação em conjunto com a elevação configurada no widget **Campo de visão** da câmera, forneça uma representação visual no mapa do ponto cego criado pela parede.

5 Teste o ponto cego criado pelo objeto selecionando a câmera e clicando em **Iniciar teste de campo de visão** no widget da câmera.



Exemplo	Configuração
A	**Bloquear campo de visão** não está selecionado para o retângulo que representa a garagem de estacionamento.

Exemplo	Configuração
B	**Bloquear campo de visão** está selecionado para o retângulo que representa a garagem de estacionamento.
C	**Bloquear campo de visão** está selecionado para o retângulo que representa a garagem de estacionamento e a **Elevação** está definida para a garagem de estacionamento e a câmera.

6 Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

Tópicos relacionados

Adicionar câmeras aos seus mapas na página 269

Adicionar sequências de câmeras aos seus mapas

Para permitir que os operadores do Security Desk se concentrem em um ponto de interesse, você pode adicionar sequências de câmeras aos seus mapas para que várias câmeras sejam exibidas ao clicar em um único objeto de mapa.

Antes de iniciar

- Crie o mapa onde você deseja adicionar suas sequências de câmeras.
- Certifique-se de ter câmeras no seu sistema Security Center.

O que você deve saber

Uma sequência de câmeras marca um local no mapa que requer atenção especial ou monitoramento atento. Você pode configurar uma sequência de câmeras para que, quando ela for exibida, aponte todas as câmeras PTZ que fazem parte dela para um local específico (posição predefinida).

Para adicionar uma sequência de câmeras ao seu mapa:

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.

2 Selecione um dos **Mapas recentes** ou clique em **Explorar todos os mapas** para abrir um mapa existente.

O mapa selecionado preenche o espaço de trabalho do Map designer.

3 Na barra de ferramentas, clique em **Exibição de área** (), selecione a sequência de câmeras que deseja adicionar e arraste-a para onde desejar que ela esteja no mapa.

Os widgets para configurar o objeto de mapa aparecem no painel da direita. O objeto de mapa sempre assume a identidade da entidade que representa.

4 Na barra de ferramentas *Map designer*, clique em **Salvar** ().

Tópicos relacionados

Visão geral da tarefa Map designer na página 255

Adicionar layouts aos seus mapas

Para permitir que os operadores do Security Desk visualizem várias câmeras enquanto se focam no mapa, você pode adicionar layouts aos seus mapas para que todas as câmeras associadas ao layout sejam exibidas em uma bolha de ladrilhos (como uma sequência de câmeras) ao clicar em um único objeto de mapa.

Antes de iniciar

- Crie o mapa onde você deseja adicionar o seu *layout*.
- Certifique-se de ter layouts no seu sistema Security Center.

O que você deve saber

Um operador do Security Desk pode clicar duas vezes em um layout no mapa para abrir uma tarefa de *Monitoramento* com esse layout.

Para adicionar um layout ao seu mapa:

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.

2 Selecione um dos **Mapas recentes** ou clique em **Explorar todos os mapas** para abrir um mapa existente.

O mapa selecionado preenche o espaço de trabalho do Map designer.

3 Na barra de ferramentas, clique em **Exibição de área** (), selecione o layout () que deseja adicionar e arraste-o para onde desejar que ele esteja no mapa.

Os widgets para configurar o objeto de mapa aparecem no painel da direita. O objeto de mapa sempre assume a identidade da entidade que representa.

4 Na barra de ferramentas *Map designer*, clique em **Salvar** ().

Tópicos relacionados

Visão geral da tarefa Map designer na página 255

Adicionar câmeras LPR aos seus mapas

Você pode adicionar câmeras LPR fixas aos seus mapas para permitir que os operadores do Security Desk monitorem leituras e acessos de mapas.

Antes de iniciar

- Crie o mapa onde você deseja adicionar suas câmeras LPR fixas.
- Certifique-se de ter câmeras LPR fixas no seu sistema Security Center.

O que você deve saber

Para adicionar uma câmera de LPR ao seu mapa:

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.
2 Selecione um dos **Mapas recentes** ou clique em **Explorar todos os mapas** para abrir um mapa existente.
O mapa selecionado preenche o espaço de trabalho do Map designer.
3 Na barra de ferramentas, clique em **Vista de área** ( ), selecione a câmera de contexto ( ) anexada à câmera de LPR fixa que você deseja e arraste-a para onde desejar que ela esteja no mapa.

NOTA: Se você arrastar a unidade de LPR ( ) ou a câmera de LPR ( ) para o mapa, o sistema exibirá ocorrências e leituras LPR ao invés do feed de vídeo da câmera.

Os widgets para configurar o objeto de mapa aparecem no painel da direita. O objeto de mapa sempre assume a identidade da entidade que representa.
4 No widget de **regras LPR**, selecione uma lista de procurados.
5 Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

Tópicos relacionados
Visão geral da tarefa Map designer na página 255

Adicionar alarmes aos seus mapas

Você pode adicionar alarmes aos seus mapas para permitir que os operadores do Security Desk monitorem e administrem alarmes dos mapas.

Antes de iniciar

- Crie o mapa onde você deseja adicionar seus alarmes.
- Certifique-se de ter alarmes no seu sistema Security Center.

O que você deve saber

As bolhas de notificação de alarme são exibidas acima de todos os objetos de mapa que representam uma entidade anexada a um alarme ativo. Se nenhuma entidade conectada a um alarme ativo for representada em um mapa, nenhuma notificação de alarme será exibida nesse mapa, a menos que o alarme ativo em si seja representado nesse mapa.

Você também pode vincular um alarme a uma forma personalizada.

Para adicionar um alarme ao seu mapa:

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.

2 Selecione um dos **Mapas recentes** ou clique em **Explorar todos os mapas** para abrir um mapa existente.

O mapa selecionado preenche o espaço de trabalho do Map designer.

3 Na barra de ferramentas, clique em **Alarmes** (), selecione o alarme que deseja vincular e arraste-o para onde desejar que ele esteja no mapa.

Os widgets para configurar o objeto de mapa aparecem no painel da direita. O objeto de mapa sempre assume a identidade da entidade que representa.

4 Na barra de ferramentas *Map designer*, clique em **Salvar** ().

Tópicos relacionados

Visão geral da tarefa Map designer na página 255

Adicionar áreas de detecção de intrusão em seus mapas

Você pode adicionar áreas de detecção de intrusão aos seus mapas para permitir que os operadores do Security Desk monitorem e controlem as áreas de detecção de intrusão dos mapas.

Antes de iniciar

- Crie o mapa onde você deseja adicionar suas áreas de detecção de intrusão.
- Certifique-se de ter áreas de detecção de intrusão em seu sistema.

Para adicionar uma área de detecção de intrusão em seus mapa:

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.

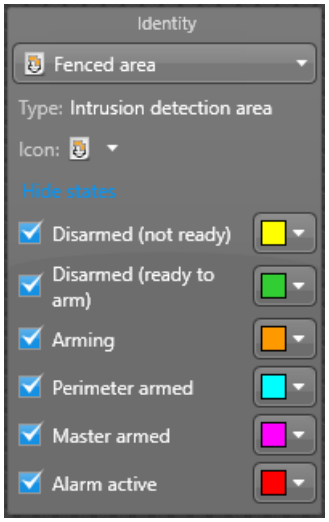
2 Selecione um dos **Mapas recentes** ou clique em **Explorar todos os mapas** para abrir um mapa existente.

O mapa selecionado preenche o espaço de trabalho do Map designer.

3 Na barra de ferramentas, clique em **Exibição de área** ( ), selecione a área de detecção de intrusão ( ) que deseja vincular e arraste-a para onde desejar que ela esteja no mapa.

Os widgets para configurar o objeto de mapa aparecem no painel da direita. O objeto de mapa sempre assume a identidade da entidade que representa.

4 No widget **Identidade**, clique em **Mostrar estados**, e, em seguida, atribua cores para os diferentes estados de área de detecção de intrusão.



DICA: Para evitar sobrecarregar o mapa, você pode ocultar objetos do mapa quando a entidade for encontrada em certos estados. Limpe os estados que deseja ocultar.

Quando o estado da área de detecção de intrusão muda, o objeto de mapa muda para a cor configurada para esse estado ou fica oculto.

5 Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

Tópicos relacionados

Visão geral da tarefa Map designer na página 255

Adicionar unidades de detecção de intrusão e entidades relacionadas em seus mapas

Você pode adicionar unidades de detecção de intrusão, o que inclui receptor de alarmes, e os seus dispositivos relacionados, painéis, áreas, sensores e entradas para os seus mapas permitirem que operadores Security Desk monitorem o estado dessas entidades dos mapas.

Antes de iniciar

- Crie o mapa pra o qual você deseja adicionar sua unidade de detecção de intrusão.
- Certifique-se de que tem unidades de detecção de intrusão adicionadas à função de Intrusion Manager no Config Tool.

Para adicionar uma entidade de unidade de detecção de intrusão ao seu mapa:

1. Na página inicial do Config Tool, abra a tarefa *Map designer*.
2. Selecione um dos **Mapas recentes** ou clique em **Explorar todos os mapas** para abrir um mapa existente.
   O mapa selecionado preenche o espaço de trabalho do Map designer.
3. Na barra de ferramentas, clique em **Vista de área** ( ), localize e selecione a entidade que deseja adicionar e arraste-a para onde desejar no mapa.
   Os widgets para configurar o objeto de mapa aparecem no painel da direita. O objeto de mapa sempre assume a identidade da entidade que representa.
4. Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

Adicionar zonas aos seus mapas

Você pode adicionar zonas de hardware e zonas virtuais aos seus mapas para permitir que os operadores do Security Desk monitorem e controlem zonas a partir dos mapas.

Antes de iniciar

- Crie o mapa onde você deseja adicionar suas zonas.
- Certifique-se de ter zonas no seu sistema.

Para adicionar uma zona ao seu mapa:

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.

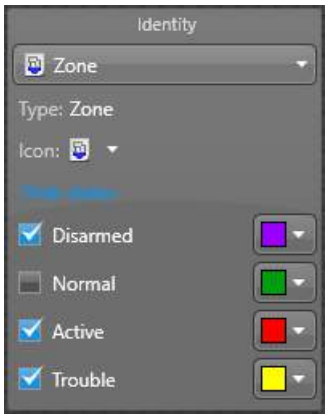
2 Selecione um dos **Mapas recentes** ou clique em **Explorar todos os mapas** para abrir um mapa existente.

O mapa selecionado preenche o espaço de trabalho do Map designer.

3 Na barra de ferramentas, clique em **Exibição de área** ( ), selecione a zona de hardware ( ), zona virtual ( ) ou zona de E/S ( ) que deseja adicionar e arraste-a para onde desejar que ela esteja no mapa.

Os widgets para configurar o objeto de mapa aparecem no painel da direita. O objeto de mapa sempre assume a identidade da entidade que representa.

4 No widget **Identidade**, clique em **Mostrar estados** e, em seguida, atribua cores aos diferentes estados de zona.



DICA: Para evitar sobrecarregar o mapa, você pode ocultar objetos do mapa quando a entidade for encontrada em certos estados. Limpe os estados que deseja ocultar.

Quando o estado da zona muda, o objeto de mapa muda para a cor configurada para esse estado ou fica oculto.

5 Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

Tópicos relacionados

Visão geral da tarefa Map designer na página 255

Adicionar pinos de entrada aos seus mapas

Você pode adicionar pinos de entrada aos seus mapas para permitir que os operadores do Security Desk monitorem os estados dos pinos de entrada dos mapas.

Antes de iniciar

- Crie o mapa onde você deseja adicionar seus pinos de entrada.
- Certifique-se de que você tem pinos de entrada no seu sistema do Security Center.

Para adicionar um pino de entrada ao seu mapa:

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.

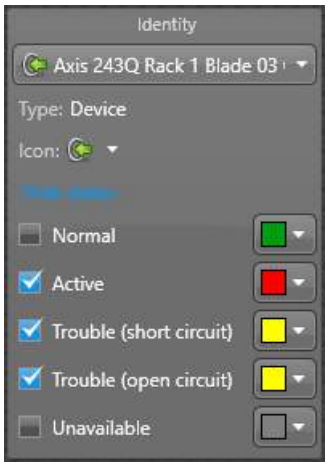
2 Selecione um dos **Mapas recentes** ou clique em **Explorar todos os mapas** para abrir um mapa existente.

O mapa selecionado preenche o espaço de trabalho do Map designer.

3 Na barra de ferramentas, clique em **E/S** ( ), selecione o pino de entrada ( ) que deseja adicionar e arraste-o para onde desejar que esteja no mapa.

Os widgets para configurar o objeto de mapa aparecem no painel da direita. O objeto de mapa sempre assume a identidade da entidade que representa.

4 No widget **Identidade**, clique em **Mostrar estados** e, em seguida, atribua cores aos diferentes estados de entrada.



DICA: Para evitar sobrecarregar o mapa, você pode ocultar objetos do mapa quando a entidade for encontrada em certos estados. Limpe os estados que deseja ocultar.

NOTA: Caso use o ícone de entrada padrão ( ), o objeto de mapa é exibido como LED colorido ( ). Caso altere o ícone, o objeto do mapa será representado pelo ícone que você selecionou com um pequeno ícone de LED sobreposto.

Quando o estado da entrada muda, o objeto de mapa muda para a cor configurada para esse estado ou fica oculto.

5 Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

Tópicos relacionados

Visão geral da tarefa Map designer na página 255

Adicionar relés de saída aos seus mapas

Você pode adicionar relés de saída aos seus mapas para permitir que os operadores do Security Desk acionem comportamentos de saída em relés de saída a partir dos mapas.

Antes de iniciar

- Crie o mapa onde você deseja adicionar seus relés de saída.
- Certifique-se de que você tenha relés de saída no seu sistema Security Center.

Para adicionar um relé de saída ao seu mapa:

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.

2 Selecione um dos **Mapas recentes** ou clique em **Explorar todos os mapas** para abrir um mapa existente.

O mapa selecionado preenche o espaço de trabalho do Map designer.

3 Na barra de ferramentas, clique em **E/S** (), selecione o relé de saída () que deseja adicionar e arraste-o para onde desejar que ele esteja no mapa.

Os widgets para configurar o objeto de mapa aparecem no painel da direita. O objeto de mapa sempre assume a identidade da entidade que representa.

4 No widget **Comportamentos de saída**, clique em **Adicionar ação** (), selecione um comportamento de saída e atribua a ele um nome.

Você pode configurar vários comportamentos de saída. Quando um operador clica em um relé de saída no mapa, os comportamentos de saída disponíveis aparecem em uma bolha de menu.

5 Na barra de ferramentas *Map designer*, clique em **Salvar** ().

Tópicos relacionados

Visão geral da tarefa Map designer na página 255

Adicionar objetos KML aos seus mapas

Você pode adicionar recursos, como estradas, parques, prédios e assim por diante aos seus mapas, importando objetos KML (Keyhole Markup Language) a partir de arquivos KML através da função Gerenciador de mapas.

Antes de iniciar

Você deve criar pelo menos um mapa georreferenciado.

O que você deve saber

Keyhole Markup Language (KML) é um formato de arquivo usado para exibir dados geográficos em um navegador da Terra, como Google Earth e o Google Maps. Os objetos KML são tipicamente usados para representar objetos estáticos, como estradas, rios, parques, prédios e assim por diante. Eles só podem ser usados com mapas georreferenciados.

Para adicionar objetos KML ao seu mapa:

1. Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.
2. Selecione a função *Map Manager* e clique na aba **Propriedades**.
3. Na seção *Camadas de mapas*, clique em **Adicionar um item** ().
4. Na caixa de diálogo *Selecionar camadas a importar*, digite o caminho para seu arquivo `.kml`
   Uma visualização do objeto KML aparece na caixa de diálogo.
5. Clique em **Importar** e, em seguida, clique em **Aplicar**.

Após terminar

Os objetos KML recém-importados serão exibidos por padrão em todos os mapas existentes que você criou. Se você não quiser mostrá-los em alguns mapas, você deve alterar esses mapas e remover essa camada KML de suas camadas padrão.

Adicionar macros aos seus mapas

Você pode adicionar macros aos seus mapas para permitir que os operadores do Security Desk executem as macros a partir dos mapas.

Antes de iniciar

- Crie o mapa onde você deseja adicionar suas macros.
- Certifique-se de que você tem a macro no sistema do Security Center.

Para adicionar uma macro ao seu mapa:

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.
2 Selecione um dos **Mapas recentes** ou clique em **Explorar todos os mapas** para abrir um mapa existente.
O mapa selecionado preenche o espaço de trabalho do Map designer.
3 Na barra de ferramentas, clique em **Macros** ( ), selecione a macro ( ) que deseja vincular e arraste-a para onde desejar que ele esteja no mapa.
Os widgets para configurar o objeto de mapa aparecem no painel da direita. O objeto de mapa sempre assume a identidade da entidade que representa.
4 (Opcional) No widget **Propriedades de Macro**, clique em **Substituir contexto padrão** para definir um contexto de execução diferente do padrão.
Clique em **Limpar** para reverter para o contexto de execução padrão.
5 Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

Tópicos relacionados

Visão geral da tarefa Map designer na página 255
Sobre macros na página 221

Configurar opções de agrupamento de mapas no Security Center

Por padrão, grupos de três ou mais objetos de mapa que estão localizados próximos uns dos outros são representados por bolhas de cluster azul em um mapa. Se você tiver um pequeno número de câmeras ou outros objetos de mapa em seu mapa, você pode reconfigurar ou desativar esse recurso do arquivo *LnkMaps.config*.

Para configurar opções de agrupamento de mapa no Security Center:

1 Abra o arquivo *LnkMaps.config*, localizado na pasta *ConfigurationFiles* da sua pasta de instalação do Security Center.

2 Para desativar o agrupamento, adicione o seguinte código à linha <Maps>:

```
EnableClustering="False"
```

3 Para desabilitar o agrupamento somente se houver menos de *x* número de objetos de mapa no seu mapa, adicione o seguinte código à linha <Maps> e especifique o número desejado de objetos de mapa:

```
ClusterMinObjectCount="500"
```

4 Para alterar o número padrão de objetos de mapa que devem estar próximos uns dos outros para que as bolhas de cluster apareçam, adicione o seguinte código à linha <Maps> e altere o número de 3 para o número desejado:

```
ClusterDensity="3"
```

5 Salve o arquivo *LnkMaps.config* e, em seguida, reinicie a Config Tool e o Security Desk.

Da próxima vez que você abrir a Config Toolou o Security Desk, as alterações de cluster de mapa serão feitas.

12

Plug-ins

Esta seção inclui os seguintes tópicos:

- "Sobre plug-ins" na página 285
- "Sobre plug-ins de ladrilho" na página 286
- "Criar plug-ins de ladrilho ligados a um website" na página 287
- "Criar plugins de janela ligados a um arquivo executável" na página 288

Sobre plug-ins

Uma função de plug-in adiciona recursos opcionais ao Security Center. Uma função de plug-in é criada usando o modelo de função *Plug-in*. Por padrão, é representada por uma peça de quebra-cabeça laranja na visualização *Funções* da tarefa *Sistema*.

Modelo do plug-in ()

Plug-in (com uma maiúscula, no singular) é o modelo de função que serve para criar funções de plug-in específicas.

Sobre a criação de plug-ins ()

Antes de você poder criar uma função de plug-in, o pacote de software específico para essa função deve ser instalado no seu sistema. É preciso certificar-se também de que a sua licença Security Center possui uma *certificado* válida para o plug-in que deseja usar.

Para obter mais informações, consulte o *Guia de Plug-in* individual para o plug-in que você está usando. Os Guias de Plug-ins estão disponíveis para download a partir do TechDoc Hub. Será necessário ter um nome de usuário e uma senha para ingressar no Hub.

Sobre plug-ins de ladrilho

Um plug-in de ladrilho é um componente de software que é executado dentro de um ladrilho do Security Desk. Por padrão, é representado por uma peça de quebra-cabeça verde na exibição de área.

A entidade de plug-in de ladrilho () representa um site () ou um arquivo *.dll* ou *.xaml* interativo.

Quando um plug-in de ladrilho é exibido no Security Desk, você pode visualizar e interagir com o site ou o arquivo de plug-in interativo. Quando um plug-in de ladrilho é anexado a uma entidade de área, ele é exibido automaticamente no Security Desk no lugar do ícone de área, quando a área é arrastada para um ladrilho.

Criar plug-ins de ladrilho ligados a um website

Você pode criar um plug-in de ladrilho que se associa a um site que contém um mapa, com o qual você pode interagir quando o plug-in de ladrilho for exibido no Security Desk.

O que você deve saber

Certifique-se de que a URL à qual você vincula o plug-in do ladrilho pode ser alcançada a partir de todas as estações de trabalho do Security Desk ou alguns usuários podem não conseguir visualizar o mapa ou outro conteúdo da URL.

Para criar um plug-ins de ladrilho que se associa a um website:

1. Abra a tarefa **Exibição de área**.
2. Clique em **Adicionar uma entidade** () > **Plug-in de ladrilho**.
3. No assistente *Criando um plug-in de ladrilho*, digite o nome e descrição da entidade.
4. Se houver partições no seu sistema, selecione a partição da qual o plug-in de ladrilho faz parte e clique em **Próximo**.

   As partições determinam quais usuários do Security Center têm acesso a essa entidade. Somente usuários que receberam acesso à partição podem ver o plug-in de ladrilho.
5. Na página *Informações do plug-in de ladrilho*, selecione **Website**.
6. Clique em**Próximo** > **Fechar**.

   O plug-in do ladrilho é exibido na visualização de área com um ícone do site ().
7. Selecione o plug-in de ladrilho e clique na aba **Propriedades**.
8. Na opção **Página da web**, digite um endereço da web.
9. Clique em **Aplicar**.

Tópicos relacionados

Sobre plug-ins de ladrilho na página 286

Criar plugins de janela ligados a um arquivo executável

Você pode criar um plug-in de ladrilho que se associa a um arquivo .dll ou .xmal que contém um arquivo executável, com o qual você pode interagir quando o plug-in de ladrilho for exibido no Security Desk.

Antes de iniciar

O arquivo executável deve ser criado e localizado em seu computador local.

Para criar um plugin de ladrilho que se liga a um arquivo executável:

1. Abra a tarefa **Exibição de área**.
2. Clique em **Adicionar uma entidade** ( ) > **Plug-in de ladrilho**.
3. No assistente *Criando um plug-in de ladrilho*, digite o nome e descrição da entidade.
4. Se houver partições no seu sistema, selecione a partição da qual o plug-in de ladrilho faz parte e clique em **Próximo**.

   As partições determinam quais usuários do Security Center têm acesso a essa entidade. Somente usuários que receberam acesso à partição podem ver o plug-in de ladrilho.
5. Na página de *Informações do plug-in do ladrilho*, selecione **Plug-in do ladrilho**.
6. No Windows, selecione o arquivo .dll ao qual o plug-in de ladrilho será vinculado e clique em **Abrir**.
7. Clique em**Próximo** > **Fechar**.

   O plug-in do ladrilho é exibido na visualização de área com o ícone padrão ( ).
8. Selecione o plug-in de ladrilho e clique na aba **Propriedades**.
9. Para selecionar outro arquivo executável, clique em **Modificar** e selecione outro arquivo .dll.
10. Clique em **Aplicar**.

Tópicos relacionados

Sobre plug-ins de ladrilho na página 286

13

Monitoramento da saúde do sistema

Esta seção inclui os seguintes tópicos:

- "Sobre monitoramento da saúde do sistema" na página 290
- "Sobre a função do Monitor de Saúde" na página 293
- "Redefinir o banco de dados do Health Monitor." na página 294
- "Selecionar eventos de saúde a serem monitorados" na página 295
- "Definir entidades para modo de manutenção" na página 296
- "Habilitar eventos para câmeras em modo de manutenção" na página 297
- "Definir aplicativos clientes Security Center para o modo de manutenção" na página 299
- "Visualizar mensagens do sistema" na página 300
- "Visualizar eventos de saúde do sistema" na página 302
- "Visualizar o estado de saúde e a disponibilidade de entidades" na página 304
- "Monitorar recursos do seu computador" na página 306
- "Visão Geral da tarefa de Status do sistema 264" na página 310
- "Monitorar o status do seu sistema Security Center" na página 316

Sobre monitoramento da saúde do sistema

Monitoramento de saúde se refere a um conjunto de ferramentas para monitorar a saúde de seu sistema Security Center. O objetivo é detectar problemas de saúde suficientemente cedo para evitar problemas mais sérios no futuro. O monitoramento de saúde também fornece a você as informações para identificar a causa raiz de vários problemas de saúde para que possam ser impedidos de ocorrer novamente.

Eventos de saúde

A tabela abaixo lista os eventos de integridade por seu número de erro e indica seu nível de gravidade, informações (), aviso () ou erro (). Os eventos no seu sistema variam dependendo das suas opções de licença.

Número do erro	Evento de saúde	Severidade
1	Arquivamento iniciado	Informações
2	Arquivamento interrompido	Erro
3	Aplicativo conectado	Informações
4	Aplicativo desconectado por usuário	Informações
5	Aplicativo desconectado inesperadamente	Alerta
6	Aplicativo iniciado	Informações
7	Aplicativo interrompido por usuário	Informações
8	Aplicativo interrompido inesperadamente	Alerta
9	Conexão restaurada	Informações
10	Falha na conexão	Erro
11	A conexão com a unidade foi estabelecida	Informações
12	Conexão com a unidade interrompida inesperadamente	Erro
13	Conexão com a unidade interrompida pelo usuário	Informações
14	O backup automático do banco de dados foi restaurado	Informações
15	O backup automático do banco de dados falhou	Erro
16	Banco de dados recuperado	Informações
17	Perda do banco de dados	Erro
18	Uso normal da CPU	Informações
19	Uso elevado da CPU	Alerta
20	Uso normal da memória	Informações

Número do erro	Evento de saúde	Severidade
21	Uso elevado da memória	Alerta
22	Espaço no banco de dados normal	Informações
23	Espaço no banco de dados baixo	Alerta
24	Descarregamento do Genetec Patroller™ restaurado	Informações
25	Descarregamento do Genetec Patroller™ falhou	Erro
26	Genetec Patroller™ online	Informações
27	Genetec Patroller™ offline	Informações
28	Banco de dados de *Ponto de venda* recuperado	Informações
29	Banco de dados de *Ponto de venda* perdido	Erro
30	Função iniciada	Informações
31	Função interrompida inesperadamente	Erro
32	Função interrompida por usuário	Informações
33	Perda de pacote RTP normal	Informações
34	Perda de pacote RTP elevada	Alerta
35	Servidor iniciado	Informações
36	Servidor interrompido por usuário	Informações
37	Servidor interrompido inesperadamente	Erro
38	A sincronização foi recuperada	Informações
39	A sincronização falhou	Alerta
40	Sinal de vídeo recuperado	Informações
41	Perda do sinal de vídeo	Erro
42	Acesso a disco restaurado	Informações
43	Acesso a disco não autorizado	Alerta
44	Taxa de disparo de alarmes normal	Informações
45	Taxa de disparo de alarmes elevada	Alerta
46	Directory iniciado	Informações
47	Directory interrompido inesperadamente	Erro

Número do erro	Evento de saúde	Severidade
48	Directory interrompido por usuário	Informações
49	Espaço restante em disco de repositório normal	Informações
50	Espaço restante em disco de repositório baixo	Alerta
51	Monitoração de servidor ao vivo foi recuperada	Informações
52	Monitoração de servidor ao vivo falhou	Erro
53	Failover do Directory: Banco de dados principal recuperado	Informações
54	Failover do Directory: Banco de dados principal perdido	Erro
55	A restauração do banco de dados foi bem sucedida	Informações
56	A restauração do banco de dados falhou	Erro
57	Sucesso na recuperação de arquivos das unidades	Informações
58	Falha na recuperação de arquivos das unidades	Erro
59	Falha parcial na recuperação de repositórios das unidades	Erro
60	Sucesso na duplicação de repositórios	Informações
61	Falha na duplicação de repositórios	Erro
62	Falha parcial na duplicação de repositórios	Erro
63	Sucesso na transferência de arquivo	Informações
64	Falha na transferência de arquivo	Erro
73	Conexão estabelecida com a câmera	Informações
74	Conexão com a câmera interrompida inesperadamente	Erro
75	Conexão com a câmera interrompida pelo usuário	Informações

Sobre a função do Monitor de Saúde

A função Health Monitor monitora entidades do sistema como servidores, funções, unidades e aplicativos cliente em busca de problemas de saúde do sistema.

Eventos de saúde são registrados em um banco de dados com a finalidade de relatórios e análise estatística. Os erros atuais do sistema são relatados em tempo real na bandeja de notificação do aplicativo.

Apenas uma instância dessa função é permitida por sistema. Ele é criado na instalação do sistema e não pode ser excluído.

A partir da função do Monitor de Saúde, você pode escolher quais eventos de saúde a monitorar.

Redefinir o banco de dados do Health Monitor.

Depois de inicialmente configurar o sistema, você deve redefinir o banco de dados de monitoramento de integridade para seu estado original.

O que você deve saber

O processo de configuração e configuração de um sistema pode gerar muitos eventos de saúde. É normal que erros de saúde e avisos sejam produzidos durante este período. É por isso que é importante restaurar o banco de dados para seu estado original e limpo, para que as estatísticas de integridade do sistema sejam redefinidas.

Para redefinir o banco de dados do Health Monitor para seu estado original:

1. Abra a tarefa **Sistema** e clique na visualização **Funções**.
2. Selecione a função **Health Monitor** e clique na aba **Recursos**.
3. Clique em **Excluir o banco de dados** ( ).
4. Quando solicitado a excluir este banco de dados, clique em **Excluir**.

   A janela **Ações do banco de dados** é aberta.
5. Quando você vir a confirmação de que o banco de dados foi excluído, clique em **Limpar concluído** e, em seguida, clique em **Fechar**.
6. Na barra de ferramentas na parte inferior da área de trabalho, clique em **Desativar função** ( ).
7. Clique em **Ativar função** ( ).

   Após 15 a 30 segundos, um novo banco de dados *HealthMonitor* deverá ser criado na aba **Recursos** da função Health Monitor.

Os erros e avisos de saúde gerados durante a configuração são excluídos e todas as estatísticas de saúde são redefinidas.

Selecionar eventos de saúde a serem monitorados

Você pode configurar a função *Health Monitor* para ignorar determinados eventos de saúde e alterar como ele gera alguns eventos de saúde.

O que você deve saber

Se você quiser ignorar todos os eventos de saúde, desative a função Health Monitor completamente. Se você quiser ignorar temporariamente os eventos de saúde de uma entidade porque está executando um trabalho de manutenção nela, defina-a para o modo de manutenção.

IMPORTANTE: Limpar um evento de saúde na lista de monitoramento não o remove do filtro de consulta *Histórico de saúde do sistema*, mas pode tornar impossíveis alguns dos cálculos de estatísticas de saúde.

Selecionar quais eventos de saúde a monitorar:

1. Abra a tarefa **Sistema** e clique na visualização **Funções**.
2. Selecione a função **Health Monitor** e clique na aba **Propriedades**.
3. Em **Eventos a serem monitorados**, selecione ou desmarque os eventos desejados.

   A maioria dos eventos de saúde vem aos pares, como *Perda do banco de dados* e *Banco de dados recuperado*. Eles só podem ser selecionados ou ignorados juntos.

4. Adicione critérios para gerar os eventos, da seguinte forma:

   Os critérios só são suportados para alguns eventos. Por exemplo, você pode configurar o evento de saúde *Uso elevado da CPU* para apenas ser gerado em servidores cuja carga da CPU é superior a 80% por um período de 10 segundos.

   a) Selecione o evento a ser modificado e clique em **Editar** (✎) na parte inferior da lista.
   b) Na janela de **detalhes** do evento, ajuste os valores conforme necessário e clique em **Salvar**.
5. Clique em **Aplicar**.

Tópicos relacionados

Visualizar eventos de saúde do sistema na página 302

Definir entidades para modo de manutenção

Se estiver alterando as definições de configuração de uma entidade, como uma função, ou tiver de trabalhar na contraparte física da entidade (manutenção em uma unidade de vídeo, unidade de detecção de intrusão, unidade de controle de acesso ou unidade de LPR), pode definir a entidade para o *modo de manutenção* para que as estatísticas de saúde dessa entidade não sejam afetadas.

O que você deve saber

- Tempo de inatividade inesperado (quando uma entidade não está disponível) afeta as estatísticas de saúde dessa entidade. No entanto, quando uma entidade está em *modo de manutenção*, o tempo de inatividade é considerado um tempo de inatividade *esperado* e não é usado no cálculo da disponibilidade dessa entidade.

  NOTA: Definir uma entidade no modo de manutenção não interrompe os eventos de saúde, mas relata todos os eventos de saúde como somente informações.
- Você pode colocar as seguintes entidades em modo de manutenção: funções, unidades de vídeo, câmeras, unidades de controle de acesso, unidades de detecção de intrusão, zonas de hardware, veículos de patrulha e unidades de LPR.
- Você também pode destrancar uma porta para fins de manutenção na aba **Propriedades** da porta.

Para definir uma entidade no modo de manutenção:

1. Abra a tarefa apropriada no Config Tool.
2. Clique com o botão direito do mouse na entidade na árvore de entidades e clique em **Manutenção** ( ) > **Modo de manutenção** ( ).
3. Na caixa de diálogo *Modo de manutenção*, clique em **Ativar**.
4. Selecione por quanto tempo você quer definir a entidade no modo manutenção, a partir de uma das seguintes opções:
   - **Indeterminado:** Sem data de término. Você deve desativar manualmente o modo de manutenção.
   - **Duração:** O modo de manutenção é ligado pelo número de dias que você selecionar.
   - **Horário específico de término:** O modo de manutenção é ligado até a data selecionada.

   Você pode modificar a duração enquanto a entidade estiver no modo de manutenção.
5. No campo **Motivo**, digite a razão pela qual você está definindo a entidade para o modo de manutenção.
6. Clique em **Salvar**.

   Às vezes, os ícones de função Federation™ não são atualizados imediatamente. Pressione **F5** para atualizar a árvore de entidades.

   A entidade é definida para o modo de manutenção pela duração especificada. Enquanto a entidade está no modo de manutenção, o ícone de *Modo de manutenção* ( ) é exibido no ícone de entidade na exibição de área no Config Tool e no Security Desk, bem como nos ladrilhos do Security Desk e em mapas, quando aplicável. A razão pela qual a entidade está no modo de manutenção é mostrada quando você passa o mouse sobre o ícone de entidade na visualização da área e nos mapas.

Tópicos relacionados

Habilitar eventos para câmeras em modo de manutenção na página 297

Habilitar eventos para câmeras em modo de manutenção

Por padrão, o Security Center suprime eventos de unidades de câmera e vídeo enquanto os dispositivos estão em *modo de manutenção*. Se você deseja que os eventos causa-efeito relacionados continuem funcionando quando os dispositivos estão em modo de manutenção, você pode desativar a supressão de eventos modificando o arquivo de configuração.

O que você deve saber

- Quando uma câmera está em modo de manutenção, eventos de câmera como *gravação iniciada* ou *sinal perdido* não são gerados. Quando uma unidade de vídeo está em modo de manutenção, os eventos associados à unidade de vídeo ou a câmeras conectadas à unidade de vídeo não são gerados, como, por exemplo, *unidade perdida* ou *estado de entrada alterado*. Se não forem gerados eventos, os eventos causa-efeito relacionados são efetivamente desabilitados.
- As configurações no arquivo *Archiver.gconfig* aplicam-se a todas as funções Archiver hospedadas no servidor.
- Você deve executar as seguintes etapas em cada servidor que hospede uma função Archiver.

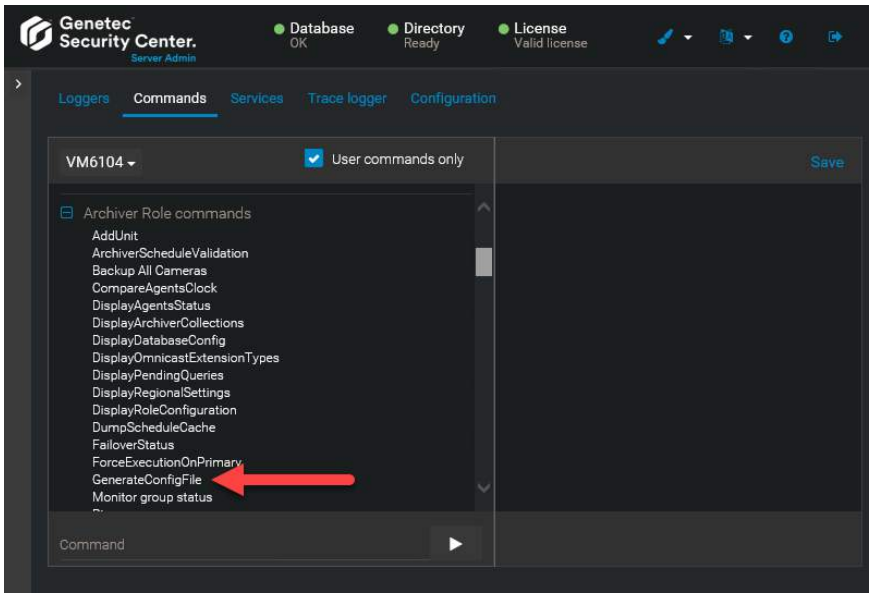
Para habilitar eventos para câmeras em modo de manutenção:

1 Abra o Server Admin usando um navegador da Web e faça logon.

2 Gere o arquivo *Archiver.config*.

IMPORTANTE: Se o arquivo *Archiver.gconfig* já existir, faça uma cópia de backup antes de gerar um novo arquivo. O novo arquivo *Archiver.gconfig* contém as configurações padrão do Archiver e sobrescreve o arquivo existente. A localização padrão é *C:\Program Files (x86)\Genetec Security Center 5.x \ConfigurationFiles*

a) Na seção *Servidores* da página *Visão Geral* , selecione o servidor da função Archiver.
b) Junto ao nome do servidor, clique em **Ações** > **Console**.
c) Clique na aba **Comandos**.
d) Expanda **Comandos da Função Archiver** e, em seguida, clique em **GenerateConfigFile**.



3 Abra a pasta *ConfigurationFiles* do servidor em: *C:\Program Files (x86)\Genetec Security Center 5.x \ConfigurationFiles*.

4 Abra o arquivo *Archiver.gconfig* usando um editor de texto.

5 Localize a configuração *suppressUnitEventsInMaintenanceMode* e defina o valor como *falso*.

6 Salve o arquivo.
7 Reinicie a função Archiver reinicializando o serviço ou desabilitando e habilitando a função Archiver.
8 Repita o procedimento para outros servidores que hospedem uma função Archiver, conforme necessário.

Tópicos relacionados

Definir entidades para modo de manutenção na página 296

Definir aplicativos clientes Security Center para o modo de manutenção

Se estiver alterando as definições de configuração do seu sistema, você pode definir todos os aplicativos clientes Security Center (Security Desk, Config Tool e Web Client) para o *modo de manutenção*, para que as estatísticas de saúde de seus aplicativos não sejam afetados.

O que você deve saber

O tempo de inatividade inesperado (quando uma entidade não estiver disponível) afeta as estatísticas de saúde dessa entidade. No entanto, quando um aplicativo está em *modo de manutenção*, o tempo de inatividade é considerado um tempo de inatividade *esperado* e não é usado no cálculo da disponibilidade desse aplicativo.

NOTA: Definir um aplicativo no modo de manutenção não interrompe os eventos de saúde, mas relata todos os eventos de saúde somente como informações.

Para definir um aplicativo cliente Security Center para o modo de manutenção:

1 Abra a tarefa **Sistema** e clique na visualização **Funções**.
2 Selecione o Health Monitor e, em seguida, clique na aba **Propriedades**.
3 Alterne a opção **Modo de manutenção de aplicativo cliente** para **Ligado** e clique em **Aplicar**.

Visualizar mensagens do sistema

Se receber mensagens do sistema, pode analisá-las a partir da área de notificação e diagnosticar as entidades problemáticas.

O que você deve saber

Você pode receber três tipos de mensagens do sistema:

- Problemas de saúde
- Advertências
- Mensagens

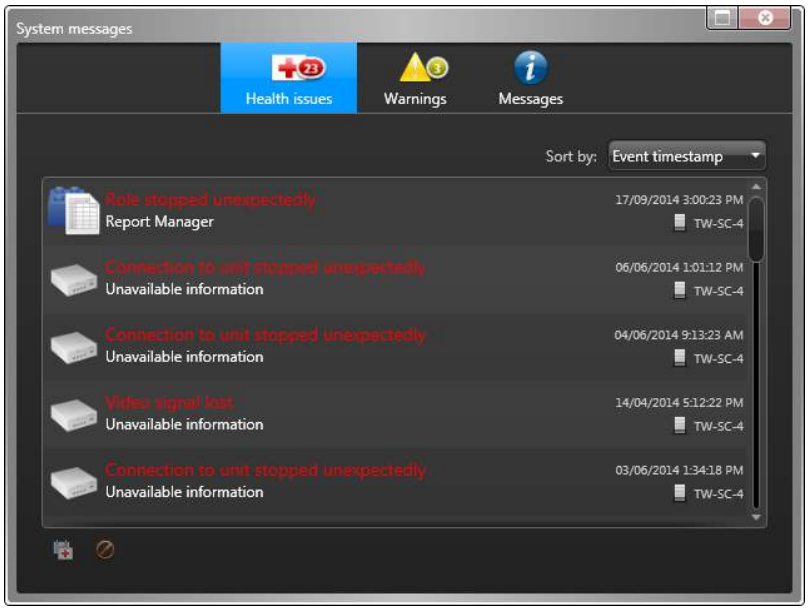
NOTA: As mensagens do sistema não são iguais aos eventos de integridade relacionados às entidades. Os ventos de saúde podem ser problemas de saúde, mas problemas de saúde não são necessariamente eventos de saúde.

Para ver as mensagens do sistema:

1 Na bandeja de notificação, clique duas vezes no ícone **Mensagens do sistema** ( ).

2 Na aba *Problemas de saúde* da caixa de diálogo *Notificações*, execute uma das seguintes opções:

- Na lista suspensa **Classificar por**, selecione como exibir os problemas de saúde. Você pode classificá-los em ordem alfabética pelo tipo de evento de saúde, data e hora do evento, máquina (nome do computador) ou fonte (nome da entidade).
- Clique em uma entidade para abrir suas páginas de configuração, para diagnosticar a entidade.
- Clique em em uma linha para iniciar uma tarefa de *Histórico de saúde do sistema* e exibir eventos de saúde do sistema.
- Clique em **Atualizar** para atualizar o conteúdo exibido na guia *Problemas de saúde* .



3 Na guia *Advertências* ( ), execute uma das seguintes opções:

- Clique em uma entidade para abrir suas páginas de configuração. .
- Clique em **Detalhes** ( ) para abrir a janela de diagnóstico, que fornece detalhes adicionais sobre o aviso.

A partir desta janela, você pode salvar o aviso como um arquivo de texto ou clicar em **Atualizar** para executar novamente os testes de diagnóstico.

4 Na guia *Mensagens* (), selecione uma mensagem e siga um destes procedimentos:

- Clique em **Copiar para a área de transferência** para copiar a mensagem selecionada para a área de transferência.
- Clique em **Limpar todos** para excluir as mensagens selecionadas.
- Clique em **Limpar todos** para excluir todas as mensagens.

5 Clique em para fechar a caixa de diálogo *Notificações* .

Tópicos relacionados

Visualizar eventos de saúde do sistema na página 302
Solução de problemas: entidades na página 85

Visualizar eventos de saúde do sistema

Você pode visualizar eventos de saúde do sistema relacionados a entidades selecionadas dentro de um período de tempo específico usando o relatório *Histórico de saúde do sistema*.

O que você deve saber

Existem três níveis de gravidade de eventos de saúde:

- Erro
- Alerta
- Informações

Quase todas as entidades do seu sistema podem gerar eventos de saúde. Você pode escolher os eventos de saúde a serem monitorados configurando a função *Health Monitor*. .

Por exemplo, se uma entidade estiver tendo problemas, você pode procurar eventos de saúde passados que ocorreram em relação a essa entidade. Se você quiser pesquisar se houve erros críticos que aconteceram no sistema durante a última semana, você pode filtrar a pesquisa somente para erros e definir um intervalo de tempo.

NOTA: Eventos de saúde também aparecem na bandeja de notificação como mensagens de sistema () como elas ocorrem em tempo real.

Para visualizar eventos de saúde do sistema relativos a uma entidade.

1 Na página inicial, abra a tarefa **Histórico de saúde do sistema** .

2 Defina os filtros de consulta para o relatório. Escolha um ou mais dos filtros abaixo:

- **Campos personalizados:** Restringir a busca a campo personalizado predefinido para a entidade. Este filtro aparece somente se os campos personalizados estiverem definidos para a entidade e estavam visíveis para você, quando foi criado ou configurado pela última vez.
- **Carimbo de tempo do evento:** Definir o intervalo de tempo para consulta O intervalo pode ser definido para um período específico ou para unidades de tempo globais, como a semana ou mês anteriores.
- **Evento de saúde:** Nome do evento de saúde.
- **Gravidade da saúde:**

  Nível de gravidade do evento de saúde:

  - Informações
  - Aviso
  - Erro
- **Máquina:** Selecionar um computador que estava com problema de saúde para investigar.
- **Entidade de origem:** Entidade fonte do evento.
- **Grupo de origem:** Grupo de entidade fonte do evento. Normalmente um papel ou uma unidade.

3 Para restringir a pesquisa a eventos de saúde atuais, clique no título **Exibir eventos de saúde atuais**.

Quando o cabeçalho está habilitado, ele aparece como **Ligado** .

4 Clique em **Gerar relatório**.

Os eventos de saúde das entidades selecionadas estão listadas no painel do relatório.

Tópicos relacionados

Selecionar eventos de saúde a serem monitorados na página 295
Visualizar mensagens do sistema na página 300

Colunas do painel de relatório para a tarefa Histórico de saúde do sistema

Após gerar um relatório, os resultados da sua pesquisa são listados em um painel de relatório. Esta seção lista as colunas disponíveis para a tarefa de relatório relevante.

- **Campos personalizados:** Os campos personalizados predefinidos para a entidade. As colunas aparecem somente se os campos personalizados estiverem definidos para a entidade e se estiver visível para você, quando forem criados ou configurados pela última vez.
- **Descrição:** Descrição do evento, atividade, entidade ou incidente.

  IMPORTANTE: Para cumprir com as leis estaduais, se a opção **Relatório gerado** é usada para um relatório de Trilha de atividade que contém dados LPR, o motivo da pesquisa LPR é incluído no campo **Descrição** .
- **Número do erro:** Número de identificação do erro de saúde.
- **Carimbo de tempo do evento:** Data e hora em que o evento ocorreu.
- **Evento de saúde:** Nome do evento de saúde.
- **Endereço IP:** Endereço de IP da unidade ou computador que gerou o evento
- **Máquina:** Computador onde ocorreu o evento de saúde
- **Contagem de ocorrências:** Número de vezes que este evento de saúde ocorreu na entidade selecionada.
- **Endereço físico:** Endereço MAC da interface de rede do equipamento
- **Severidade:**

  Nível de gravidade do evento de saúde:

  - Informações
  - Aviso
  - Erro
- **Fonte:** Entidade fonte associada ao alarme ou evento.

Visualizar o estado de saúde e a disponibilidade de entidades

Você pode monitorar o estado de saúde geral do sistema usando o relatório *Estatísticas de saúde do sistema*.

O que você deve saber

Ao monitorar a saúde e a disponibilidade de certos recursos, como funções de servidor, unidades de vídeo, controladores de portas, painéis de detecção de intrusão, etc., você pode identificar instabilidades e até mesmo evitar falhas críticas do sistema.

Um dos campos importantes no relatório Estatísticas de saúde do sistema é a *Disponibilidade* de uma dada entidade. A disponibilidade é expressa em percentagem.

Para visualizar o status de saúde e a disponibilidade de uma entidade:

1 Abrir a tarefa **Estatísticas de saúde do sistema**.

2 Defina os filtros de consulta para o relatório. Escolha um ou mais dos filtros abaixo:

- **Campos personalizados:** Restringir a busca a campo personalizado predefinido para a entidade. Este filtro aparece somente se os campos personalizados estiverem definidos para a entidade e estavam visíveis para você, quando foi criado ou configurado pela última vez.
- **Carimbo de tempo do evento:** Definir o intervalo de tempo para consulta O intervalo pode ser definido para um período específico ou para unidades de tempo globais, como a semana ou mês anteriores.
- **Entidade de origem:** Entidade fonte do evento.
- **Grupo de origem:** Grupo de entidade fonte do evento. Normalmente um papel ou uma unidade.

3 Clique em **Gerar relatório**.

As estatísticas de saúde para as entidades selecionadas estão listadas no painel do relatório. Se as estatísticas de saúde não puderem ser calculadas para uma determinada função ou entidade, a razão será exibida na coluna *Status do cálculo* do painel de relatório:

- **Um ou mais eventos utilizados para calcular a disponibilidade estão atualmente desativados:** O administrador do sistema precisa selecionar os eventos de saúde a serem monitorados ao configurar a função Monitor de função. .
- **Um ou mais servidores do sistema estão offline.:** O servidor que hospeda a função selecionada está offline, portanto, as estatísticas de saúde não podem ser calculadas para a função.

Exemplo

Um controlador de porta chamado *Gym* falhou quatro vezes na última semana, produzindo uma disponibilidade de 90,72%. A partir dos resultados do relatório, você pode verificar se este controlador de porta é uma preocupação em potencial, e pedir para que uma equipe de manutenção examine a porta.

Colunas do painel de relatório para a tarefa Estatísticas de saúde do sistema

Após gerar um relatório, os resultados da sua pesquisa são listados em um painel de relatório. Esta seção lista as colunas disponíveis para a tarefa de relatório relevante.

- **Disponibilidade:** A porcentagem do tempo disponível para determinada entidade.
- **Status de cálculo:** Se uma estatística de saúde estiver indisponível, a razão é exibida aqui.

- **Campos personalizados:** Os campos personalizados predefinidos para a entidade. As colunas aparecem somente se os campos personalizados estiverem definidos para a entidade e se estiver visível para você, quando forem criados ou configurados pela última vez.
- **Tempo parado esperado:** Quantos dias/horas/minutos a entidade esteve offline ou indisponível pela intenção do usuário ou modo de *Manutenção*. Por exemplo, desativar a função de um servidor ou desconectar um aplicativo de cliente causa inatividade esperada. A inatividade esperada nunca é usada no cálculo de porcentagem de *Disponibilidade*.
- **Falhas:** Quantas falhas ocorreram
- **MTBF:** Tempo médio entre as falhas (em horas)
- **MTTR:** Tempo médio para recuperação (em horas)
- **Pacote de RTP perdido:** Número de pacotes de *Protocolo de Transporte em Tempo Real* perdidos.
- **Fonte:** Entidade fonte associada ao alarme ou evento.
- **Inatividade inesperada:** Quantos dias/horas/minutos a entidade esteve offline ou indisponível depois de não ter sido ajustada no *Modo de manutenção*. A inatividade inesperada não é causada pela intenção do usuário.
- **Tempo de funcionamento:** Quantos dias/horas/minutos a entidade ficou online e disponível.

Monitorar recursos do seu computador

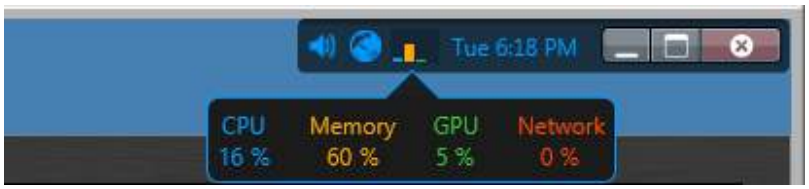
Você pode monitorar a porcentagem de uso dos recursos do computador ao passar o ponteiro do mouse sobre o ícone do **Medidor de recursos** na bandeja de notificação. Clique no mesmo ícone para exibir um resumo do hardware instalado no computador e seu uso atual em uma caixa de diálogo.

O que você deve saber

Se você não vir o ícone **Medidor de recursos** ( ) na bandeja de notificação, defina sua propriedade de exibição como **Mostrar**.

Para monitorar os recursos em seu computador:

1 Passe o ponteiro do mouse sobre o ícone do **Medidor de recursos** na bandeja de notificação para exibir o uso atual dos recursos do computador em porcentagens.



A utilização dos recursos do computador é apresentada em quatro categorias:

- CPU (azul)
- Memória (laranja)
- GPU (verde)
- Rede (vermelho)

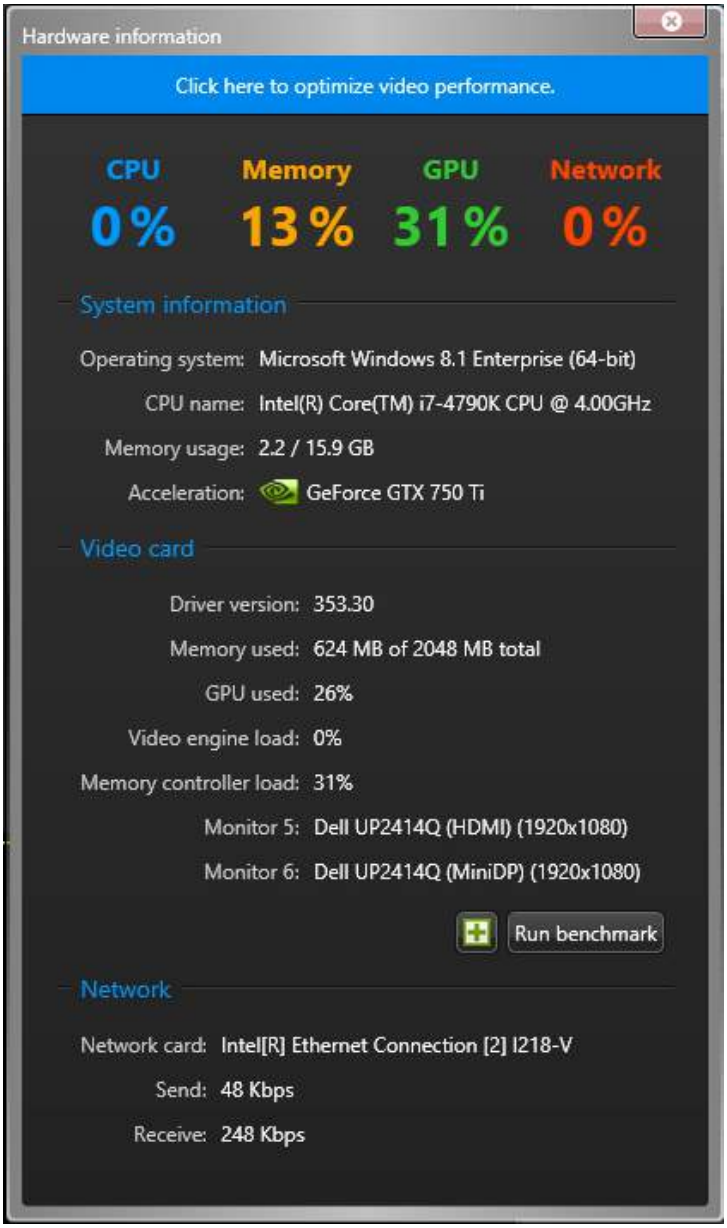
NOTA: A GPU (Unidade de Processamento Gráfico) é mostrada somente se sua placa de vídeo suportar aceleração de hardware e se esse recurso estiver ativado nas opções de vídeo do Security Desk. Consulte *Opções de vídeo* no *Guia do Usuário do Security Desk*.

2 Clique no ícone **Medidor de recursos** na bandeja de notificação para exibir informações detalhadas sobre os recursos do computador na caixa de diálogo Informações de hardware.

Caixa de diálogo Informações de hardware

A caixa de diálogo Informações de hardware fornece um resumo dos componentes de hardware detectados no seu computador, bem como a respectiva percentagem de utilização atual. Você também pode executar a ferramenta de referência de hardware a partir da caixa de diálogo Informações de hardware.

Quando o desempenho não corresponde à sua expectativa, use essas informações para descobrir qual aspecto do seu sistema está causando o estrangulamento. Se sua placa de vídeo atingiu seus limites, exibir menos fluxos de vídeo.



As informações do cartão de vídeo não estão disponíveis se você estiver conectado ao computador por meio da área de trabalho remota.

A porcentagem de uso da GPU (Unidade de Processamento Gráfico) é mostrada somente se sua placa de vídeo suportar aceleração de hardware e se esse recurso estiver ativado nas opções de vídeo do Security Desk. Se o computador tiver várias placas de vídeo, clique na lista suspensa **Aceleração** para escolher a que deseja monitorar. Para obter informações sobre como ativar o recurso de *Aceleração de hardware*, consulte o *Guia do Usuário do Security Desk*.

Para mais informações sobre a execução da ferramenta de diagnóstico de hardware, consulte Utilizar a ferramenta de parâmetro de comparação de hardware na página 308.

Tópicos relacionados

Optimizar o desempenho do decodificador de vídeo no seu computador na página 557

Utilizar a ferramenta de parâmetro de comparação de hardware

A ferramenta de parâmetro de comparação de hardware permite que você calibre suas configurações para otimizar o desempenho de suas placas de vídeo instaladas. Você pode executar a ferramenta de parâmetro de comparação de hardware no Config Tool ou no Security Desk.

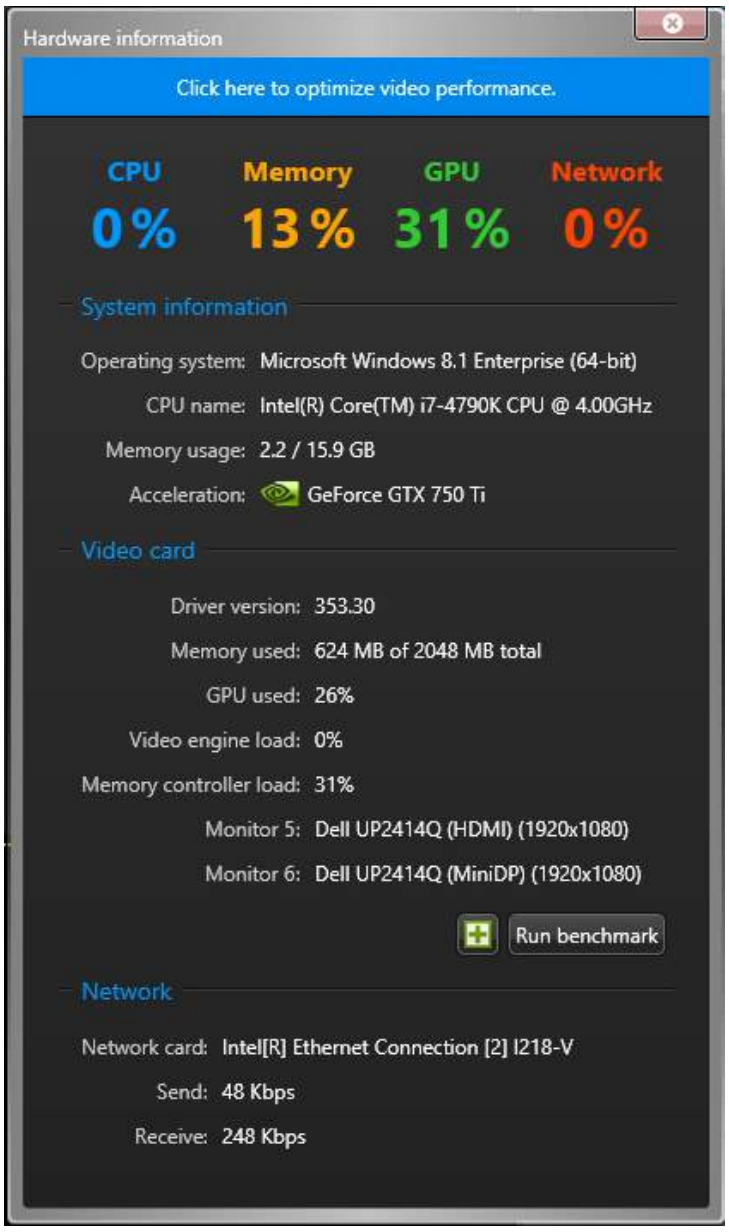
O que você deve saber

- Será solicitado que você execute a ferramenta de parâmetro de comparação de hardware na primeira vez que iniciar o Security Desk. Há também um ícone de aviso amarelo que aparece na bandeja de notificação sempre que você alterar a configuração da placa de vídeo. Não existem avisos no Config Tool.
- A execução da ferramenta de parâmetro de comparação é exigente para a GPU. Feche todas as outras tarefas e aplicativos ao executar um teste de parâmetro de comparação para garantir que você obtenha resultados válidos.
- Para obter melhores resultados, verifique se os drivers da GPU estão atualizados antes de executar a ferramenta de parâmetro de comparação de hardware.

Para utilizar a ferramenta de parâmetro de comparação de hardware:

1 Na bandeja de notificação, clique no ícone da **Medidor de recursos** ( ).

A caixa de dialogo **Informações de hardware** se abrirá.



2 Na lista suspensa **Aceleração**, selecione a placa de vídeo na qual deseja executar o teste de parâmetro de comparação.

3 Clique em **Executar parâmetro de comparação**.

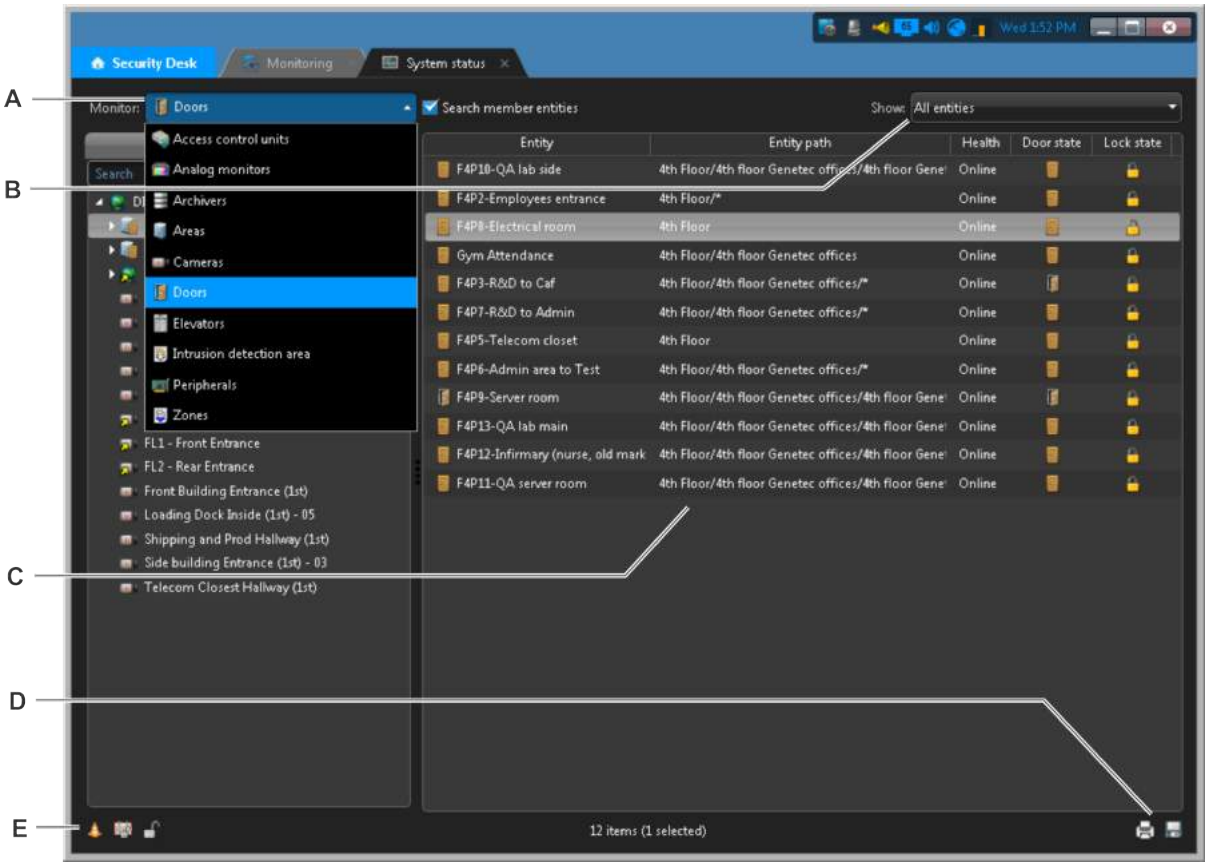
Assim que o teste de parâmetro de comparação estiver concluído, a capacidade de **Taxa de quadros** da placa selecionada é listada.

4 Clique em **Fechar**.

Visão Geral da tarefa de Status do sistema 264

Use a tarefa Status do sistema para monitorar o status atual de diferentes tipos de entidades e investigar os problemas de saúde que eles possam ter.

A figura a seguir mostra a tarefa Status do sistema.



A	Tipos de entidades que você pode monitorar.
B	Tipo de problemas que você pode monitorar.
C	Os status da entidade são listados no painel de relatório.
D	Imprimir ou Exportar o relatório.
E	Comandos específicos da entidade.

Colunas da tarefa Status do sistema

Na tarefa *Status do sistema*, você pode monitorar o status atual de diferentes tipos de entidades e investigar os problemas de saúde que elas possam ter.

A tabela a seguir lista as colunas exibidas para cada tipo de entidade na lista suspensa **Monitor**.

Entidade	Coluna	Descrição
Unidades de controle de acesso	Entidade	Nome da unidade
	Saúde	Online, Offline, ou Alerta
	Endereço de IP	Endereço IP da unidade
	Sincr.	Status da sincronização
	Falha de CA	Sim (#) ou Não (vazio)
	Falha de bateria	Sim (#) ou Não (vazio)
	Firmware	Versão de firmware da unidade
	Adulterado	Indica se a unidade foi adulterada Sim (#) ou Não (vazio)
	Manutenção	Indica se a unidade de controle de acesso atualmente está em modo de manutenção e declara a duração do modo de manutenção
Monitores analógicos	Entidade	Nome do monitor analógico
	Caminho de entidade	Lista de todas as áreas relacionadas, começando pela entidade do sistema. Se o monitor analógico tiver várias áreas pai, "*\" é mostrado como o caminho.
	Saúde	Online, Offline, ou Alerta
	Entidade conectada	Nome das câmeras atualmente exibidas no monitor
Aplicações	Entidade	Tipo de aplicativo (Config Tool ou Security Desk)
	Origem	A máquina em que está sendo executado
	Nome do usuário	Nome do usuário conectado
	Versão	Versão de software do aplicativo cliente
Áreas	Entidade	Nome da área
	Caminho de entidade	Lista de todas as áreas relacionadas, começando pela entidade do sistema.
	Saúde	Online, Offline, ou Alerta
	Nível de ameaça	Indica se um nível de ameaça está ativado atualmente na área selecionada, juntamente com o nome do nível de ameaça. Se nenhum nível de ameaça for definido, a coluna fica em branco

Entidade	Coluna	Descrição
	Folga de segurança	(Visível apenas para usuários administrativo) Indica a autorização de segurança mínima exigida dos titulares em áreas específicas, além das restrições impostas pelas regras de acesso.
	Número de pessoas	Funcionando (#) ou Não funcionando (em branco)
	Anti-passback	Físico, Eletrônico ou Nenhum (sem *anti-passback*)
	Intertravamento	Funcionando (#) ou Não funcionando (em branco)
	Prioridade	Prioridade de entradas de *Intertravamento*: Bloqueio ou Sobreposição
Archivers	Entidade	Nome do Archiver
	Servidores	Lista de servidores atribuídos para hospedar esta função
	Câmeras ativas	Número de câmeras atualmente ativas
	Arquivando câmeras	Número de câmeras que têm o arquivamento ativo
	Espaço usado	Quantidade de espaço usado no disco
	Uso do espaço em disco de arquivamento	Percentual de espaço usado no disco
	Taxa de recepção do Archiver:	Taxa em que o Archiver está recebendo dados
	Taxa de gravação do Archiver	Taxa em que o Archiver está gravando no disco
	Manutenção	Indica se o Archiver atualmente está em modo de manutenção e declara a duração do modo de manutenção
Câmeras	Entidade	Nome de câmera
	Caminho de entidade	Lista de todas as áreas relacionadas, começando pela entidade do sistema. Se uma câmera tiver várias áreas pai, “*\” é mostrado como o caminho.
	Saúde	Online, Offline, ou Alerta
	Gravando	Estado da gravação
	Sinal analógico	Perdido, Disponível ou Desconhecido (*câmeras IP*)
	Bloqueado	Indica se a câmera está atualmente bloqueada de alguns Bloqueado (#), ou não bloqueado (em branco)

Entidade	Coluna	Descrição
	Manutenção	Indica se a câmera atualmente está em modo de manutenção e declara a duração do modo de manutenção
Portas	Entidade	Nome da porta
	Caminho de entidade	Lista de todas as áreas relacionadas, começando pela entidade do sistema.
	Saúde	Online, Offline, ou Alerta
	Estado da porta	Aberta () ou fechada ()
	Estado da fechadura	Trancada () ou destrancada ()
Elevadores	Entidade	Nome do elevador
	Caminho de entidade	Lista de todas as áreas relacionadas, começando pela entidade do sistema.
	Saúde	Online, Offline, ou Alerta
Problemas de saúde	Tipo da entidade	Ícone que representa o tipo de entidade
	Entidade	Nome da entidade
	Origem	Para uma entidade local, mostra o servidor no qual ele está sendo executado. Para uma *entidade federada*, mostra o nome da função Federation™.
	Caminho de entidade	Lista de todas as áreas relacionadas, começando pela entidade do sistema.
	Saúde	Online, Offline, ou Alerta
	Manutenção	Indica se a câmera atualmente está em modo de manutenção e declara a duração do modo de manutenção
Áreas de detecção de intrusão	Entidade	Nome da área de detecção de intrusão
	Caminho de entidade	Lista de todas as áreas relacionadas, começando pela entidade do sistema.
	Saúde	Online, Offline, ou Alerta
	Estado de alarme	Alarme ativo, Alarme silenciado, Retardo de entrada ou Normal
	Estado de colocação em atenção	Armado, Desarmado (não preparado), Desarmado (pronto a armar), *Mestre armado* ou *Perímetro armado*.
	Desvio	Ativo / inativo (representado por um ícone)

Entidade	Coluna	Descrição
	Problema	Sim (#) ou Não (vazio)
Unidades de detecção de invasão	Entidade	Nome da unidade de detecção de intrusão
	Saúde	Online, Offline, ou Alerta
	Falha de CA	Sim (#) ou Não (vazio)
	Falha de bateria	Sim (#) ou Não (vazio)
	Violação	Sim (#) ou Não (vazio)
	Manutenção	Indica se a unidade de detecção de intrusão atualmente está em modo de manutenção e declara a duração do modo de manutenção
Macros	Entidade	Nome da macro
	Horário de início	Hora em que a macro foi iniciada
	Iniciador	Nome do usuário que disparou a macro
Periféricos	Nome	Nome do periférico
	Tipo	Entrada, Saída, Leitor.
	Estado	Normal, Ativo, ou Desviado (entradas e leitores)
	Informações adicionais	Configurações específicas do tipo de periférico
	Controlando	Entidade controlada pelo periférico.
	Saúde	Online, Offline, ou Alerta
	ID lógico	ID Lógico designado para o periférico
	Nome físico	Nome do periférico designado pelo sistema
Funções	Entidade	Nome da função
	Saúde	Online, Offline, ou Alerta
	Servidor atual	Nome do servidor que atualmente hospeda a função
	Servidores	Lista de servidores atribuídos para hospedar esta função
	Versão	Versão do software da função
	Status	Status Ativado ( ) ou Desativado ( )

Entidade	Coluna	Descrição
	Manutenção	Indica se a função atualmente está em modo de manutenção e declara a duração do modo de manutenção
Rotas	Rota	Nome da rota, mostrando as duas redes que ela une
	Configuração atual	*Unicast TCP*, Unicast *UDP* ou *Multicast*
	Possibilidades detectadas	Unicast TCP, Unicast UDP ou Multicast **NOTA:** É necessário um *Redirecionador* em cada rede para poder detectar as capacidades.
	Status	OK ou mensagem de aviso informando o motivo do problema **NOTA:** É necessário um *Redirecionador* em cada rede para poder exibir o status.
Servidores	Entidade	Nome do servidor
	Saúde	Online, Offline, ou Alerta
	Funções	Funções atribuídas a este servidor
	Certificado	Indica se o servidor tem um *certificado de identidade* atual e o período de validade do certificado atual
	Manutenção	Indica se o servidor atualmente está em modo de manutenção e declara a duração do modo de manutenção
Zonas	Entidade	Nome da zona
	Caminho de entidade	Lista de todas as áreas relacionadas, começando pela entidade do sistema.
	Saúde	Online, Offline, ou Alerta
	Estado	Normal, Ativo ou Problema
	Atenta	Indica se a zona está armada ou não
	Manutenção	Indica se a zona de hardware atualmente está em modo de manutenção e declara a duração do modo de manutenção

Monitorar o status do seu sistema Security Center

Você pode monitorar o status atual de diferentes tipos de entidades e investigar problemas de saúde que eles possam ter usando o relatório de *Status do sistema*.

O que você deve saber

Use o relatório de status do Sistema para monitorar seu sistema. Por exemplo, se você tiver uma câmera que não está funcionando, você pode selecionar a entidade de câmera na tarefa *Status do sistema* e, em seguida, diagnosticar por que está offline. A partir da tarefa *Status do sistema*, você também pode iniciar a tarefa *Histórico de saúde do sistema* e gerar um relatório de saúde para investigar mais.

Ao monitorar *Rotas*, um *Redirecionador* deve ser configurado em cada rede para poder detectar os recursos de rede e exibir o status atual.

Para monitorar o status do seu sistema:

1 Abra a tarefa *Status do sistema*.
2 Na lista suspensa **Monitoramento**, selecione um dos seguintes itens:
   - Unidades de controle de acesso
   - Monitores analógicos
   - Aplicativos (somente se você for um administrador)
   - Áreas
   - Archivers
   - Câmeras
   - Caixas registradoras
   - Portas
   - Elevadores
   - Problemas de saúde
   - Área de detecção de intrusão
   - Unidades de detecção de invasão
   - Macros
   - Periféricos
   - Funções
   - Rotas
   - Servidores
   - Zonas
3 Se necessário, selecione uma área no *Seletor*.
4 Para buscar entidades dentro de áreas aninhadas, selecione a opção **Buscar entidades de membro**.

   As entidades, funções, aplicações e itens relacionados são listados no painel do relatório.
5 (Opcional) Siga um destes procedimentos, dependendo da entidade selecionada:
   - Para iniciar um relatório de *Histórico de saúde do sistema*, clique em .
   - Para solucionar problemas da entidade selecionada, clique em .
   - Para imprimir o relatório, clicar em .
   - Para alterar a configuração de uma entidade, clique com o botão direito do mouse na entidade no painel de relatórios e clique em **Configurar entidade** ().
   - Para salvar o relatório, clique em .

Tópicos relacionados

Colunas da tarefa Status do sistema na página 310
Visualizar eventos de saúde do sistema na página 302
Solução de problemas: entidades na página 85

14

Auditorias do sistema

Esta seção inclui os seguintes tópicos:

- "Investigar atividades relacionadas a usuários no seu sistema Security Center" na página 319
- "Configurar registro de eventos para sequências de vídeos" na página 323
- "Descobrindo quais mudanças foram feitas na configuração do sistema" na página 324
- "Alterações de configuração registradas pelo sistema Security Center" na página 325
- "Alterações de propriedades registradas com os valores antes e depois" na página 327

Investigar atividades relacionadas a usuários no seu sistema Security Center

É possível visualizar todas as atividades de usuários relacionada a vídeos, controle de acesso e LPR usando o relatório *Trilhas de atividade*.

Antes de iniciar

Para receber resultados no relatório Trilhas de atividades, você já deve estar monitorando a atividade do usuário. Você pode selecionar quais atividades monitorar e gravar no banco de dados a partir da tarefa Sistema

O que você deve saber

Por exemplo, você pode usar a tarefa *Trilhas de atividades* para descobrir quem reproduziu quais gravações de vídeo, quem bloqueou uma câmera, quem ativou um nível de ameaça, quem solicitou um crachá de credencial para ser impresso, que usou a tarefa *Editor de listas de procurados e autorizações* ou quem ativou a filtragem de listas de procurados.

Para investigar a atividade relacionada ao usuário no sistema:

1 A partir da página inicial, abrir a tarefa *Trilhas de atividades*.
2 No filtro **Atividades**, selecione qual das seguintes atividades você deseja investigar:
   - Controle de acesso:
     - **Unidade de controle de acesso reiniciada (manualmente):** Quem reiniciou uma unidade de controle de acesso manualmente.
     - **A sincronização da unidade de controle de acesso foi iniciada (manualmente):** Quem iniciou uma unidade de controle de acesso manualmente.
     - **Violação de anti-passback perdoada:** Quem perdoou uma violação de anti-passback.
     - **Crachá impresso:** Quem imprimiu um crachá de credencial.
     - **Titular do cartão removido da área:** Quem removeu um titular de cartão e de qual área.
     - **Solicitação de credencial cancelada/ concluída:** Solicitação de impressão de quem completou ou cancelou uma solicitação de impressão.
     - **Solicitação de credencial:** Quem solicitou um crachá de credencial para ser impresso, e por quê.
     - **Desabilitação de dispositivo:** Quem desabilitou (desligou) um dispositivo de controle de acesso.
     - **Modo de manutenção da porta cancelado:** Quem cancelou o modo de manutenção em uma porta.
     - **Porta mantida no modo de manutenção:** Quem destrancou uma porta configurando-a no modo de manutenção.
     - **Programação de desbloqueio da porta substituída (bloqueio/desbloqueio):** Quem substituiu o agendamento de bloqueio ou desbloqueio de uma porta.
     - **Sobreposição de agendamento de abertura cancelada:** Quem cancelou a sobreposição do agendamento de desbloqueio de uma porta.
     - **Porta desbloqueada (explicitamente):** Quem desbloqueou uma porta no Security Desk usando um evento causa-efeito de ação instantânea ou alarme.
     - **Porta desbloqueada (manualmente):** Quem desbloqueou manualmente uma porta a partir do widget *Porta* do Security Desk.
     - **Atualização de firmware para unidade de controle de acesso agendada:** A atualização da unidade está agendada para iniciar imediatamente ou depois, se a configuração **Retardar atualização até** for usada.

- **Atualização de firmware agendada para unidade de controle de acesso cancelada:** A atualização agendada da unidade foi cancelada

- Geral:
  - **Alarme confirmado/confirmado forçadamente:** Quem confirmou ou confirmou forçadamente um alarme ativo.
  - **Alarme encaminhado/em espera:** Quem encaminhou ou adiou um alarme ativo.
  - **Alarme disparado (manualmente):** Quem disparou manualmente um alarme.
  - **Todos os alarmes confirmados forçadamente:** Quem reconheceu à força todos os alarmes ativos.
  - **Conectado a Security Desk remoto:** Quem se conectou a uma estação de trabalho remota do Security Desk.
  - **Desconectado de Security Desk remoto:** Quem se desconectou de uma estação de trabalho remota do Security Desk.
  - **Alarme de intrusão confirmado:** Quem confirmou um alarme de intrusão.
  - **Alarme de intrusão silenciado:** Quem silenciou um alarme de intrusão.
  - **Alarme de intrusão disparado:** Quem disparou manualmente um alarme de intrusão.
  - **Área de detecção de intrusão colocada fora de atenção:** Quem desarmou uma área de detecção de intrusão.
  - **Desvio de entrada da área de detecção de intrusão ativado:** Quem ativou o bypass de um sensor em uma área de detecção de intrusão.
  - **Desvio de entrada da área de detecção de intrusão desativado:** Quem desativou o bypass de um sensor em uma área de detecção de intrusão.
  - **Master da área de detecção de intrusão colocado em atenção:** Quem armou o mestre de uma área de detecção de intrusão.
  - **Perímetro da área de detecção de intrusão colocado em atenção:** Quem armou o perímetro de uma área de detecção de intrusão.
  - **Saída disparada (manualmente):** Quem disparou um pino de saída (por exemplo, usando uma ação instantânea).
  - **Relatório exportado/gerado/impresso:** Quem exportou, gerou ou imprimiu um relatório.

    IMPORTANTE: Para cumprir com as leis estaduais, se a opção **Relatório gerado** é usada para um relatório de Trilha de atividade que contém dados LPR, o motivo da pesquisa LPR é incluído no campo **Descrição** .
  - **Nível da ameaça definido/apagado:** Quem definiu ou limpou um nível de ameaça, e em qual área ou sistema.
  - **Usuário conectado/desconectado:** Quem se conectou ou desconectou de qual aplicativo cliente do Security Center.
  - **Zona armada/desarmada:** Quem armou ou desarmou uma zona.
- LPR:
  - **Aplicativo atualizado:** Quem atualizou uma unidade Genetec Patroller™ ou Sharp.
  - **Forçar violação no estacionamento acionado:** Quem forçou uma violação no estacionamento em uma zona de estacionamento.
  - **Acerto excluído:** Quem excluiu um alerta.
  - **Lista de procurados ou lista de autorização editada:** Quem carregou uma lista de procurados ou de autorização ou adicionou, modificou, ou excluiu placas de licença da lista.
  - **Correspondência de leituras passadas acionada:** Quem executou a correspondência de leituras passadas no Genetec Patroller™.
  - **Relatório de evidência fotográfica impresso (Alertas/Leituras):** Quem imprimiu um relatório de evidências de alertas/leituras.

- **Filtragem de placas ativada:** Qual função do LPR Manager tem a filtragem de placas ativada.
- **Leitura editada/disparada:** Quem editou/disparou uma leitura de placa de licença.
- **Ler/ocultar protegido:** Quem protegeu uma leitura ou alerta de placa de licença.
- **Ler/ocultar desprotegido:** Quem desprotegeu uma leitura ou alerta de placa de licença.
- **Redefinir inventário da área de estacionamento:** Quem redefiniu o inventário de uma zona de estacionamento.
- **Definir a ocupação da zona de estacionamento:** Quem modificou a ocupação de uma zona de estacionamento.

- Vídeo:
  - **Backup de arquivo iniciado/interrompido (manualmente):** Quem iniciou ou parou manualmente o backup do vídeo de um Archiver.
  - **Duplicação de arquivo iniciada/interrompida (manualmente):** Quem iniciou ou impediu que o vídeo fosse duplicado de um Archiver para outro.
  - **Restauração do arquivo iniciada/parada (manualmente):** Quem iniciou ou parou a restauração de um arquivo de vídeo para um Archiver.
  - **Recuperação de arquivos de unidades iniciada/parada (manualmente):** Quem iniciou ou parou a transferência de vídeos de unidades de vídeo para um Archiver.
  - **Limite de largura de banda excedido:** Quem solicitou um fluxo de vídeo que não pôde se conectar porque o limite de largura de banda para o vídeo redirecionado foi atingido Ou, quem perdeu uma conexão de fluxo de vídeo redirecionada porque o limite de largura de banda foi atingido e um usuário com um nível de usuário mais alto solicitou um fluxo
  - **Marcador excluído/modificado:** Quem excluiu ou modificou um marcador.
  - **Câmera bloqueada/desbloqueada:** Quem bloqueou ou desbloqueou uma câmera.
  - **Vídeo confidencial solicitado:** Quem solicitou a visualização de uma transmissão de vídeo confidencial.
  - **Conectado a um monitor analógico:** Quem se conectou a um monitor analógico.
  - **Desconectado de monitor analógico:** Quem se desconectou de um monitor analógico.
  - **Fluxo de vídeo ao vivo iniciado/interrompido:** Qual câmera foi exibida ou removida.
  - **Reprodução de fluxo de vídeo iniciada:** Qual gravação foi reproduzida.
  - **Comando PTZ enviado:** O que o usuário fez com o PTZ.
  - **Gravação iniciada (manualmente):** Quem iniciou a gravação de vídeo manualmente.
  - **Gravação interrompida (manualmente):** Quem interrompeu a gravação de vídeo manualmente.
  - **Instantâneo impresso/salvo:** Quem imprimiu ou salvou um instantâneo.
  - **Vídeo exportado:** O que o usuário exportou e onde o salvou.
  - **Arquivo de vídeo excluído (manualmente):** Quem excluiu um arquivo de vídeo do sistema.
  - **Arquivo de vídeo protegido/desprotegido:** Quem iniciou ou parou a proteção em um arquivo de vídeo.
  - **Stream de vídeo não reproduzido:** Cuja solicitação de vídeo foi encerrada sem ter um único quadro renderizado.
  - **Unidade de vídeo identificada/reinicializada/reconectada:** Quem identificou/reiniciou/reconectou uma unidade de vídeo.
  - **Rastreamento visual ativado/desativado:** Quem ativou ou desativou o *rastreamento visual* em um ladrilho.

3 Definir os outros filtros de consulta para o relatório. Escolha de um ou mais dos filtros abaixo:

- **Aplicativo:** Qual aplicação do cliente foi usada para a atividade.

- **Carimbo de tempo do evento:** Definir o intervalo de tempo para consulta O intervalo pode ser definido para um período específico ou para unidades de tempo globais, como a semana ou mês anteriores.
- **Eventos:** Selecionar os eventos de interesse. Os tipos de evento disponíveis dependem da tarefa que está usando.
- **Impactadas:** Entidades que sofreram impacto por esta atividade.
- **Iniciador:** Usuário ou função responsável pela atividade.

4 Clique em **Gerar relatório**.
Os resultados da atividade são listados no painel do relatório.

Colunas de relatório para a tarefa Rastreio de atividades

Após gerar um relatório, os resultados da sua pesquisa são listados em um painel de relatório. Esta seção lista as colunas disponíveis para a tarefa de relatório relevante.

- **Iniciador:** Quem e qual função realizou a atividade.
- **Tipo de iniciador:** Tipo de entidade que iniciou a atividade.
- **Nome da atividade:** Tipo de atividade
- **Descrição:** Descrição do evento, atividade, entidade ou incidente.

  IMPORTANTE: Para cumprir com as leis estaduais, se a opção **Relatório gerado** é usada para um relatório de Trilha de atividade que contém dados LPR, o motivo da pesquisa LPR é incluído no campo **Descrição** .
- **Entidade afetada:** Quais entidades sofreram impacto por esta atividade.
- **Tipo de entidade que sofreu impacto:** Tipo de entidade que sofreu impacto por esta atividade.
- **Máquina do iniciador:** Em qual computador a atividade foi realizada.
- **Aplicativo do iniciador:** Aplicativo usado para esta atividade
- **Carimbo de tempo do evento:** Data e hora em que o evento ocorreu.
- **Versão da entidade afetada:** Número da versão da entidade que sofreu impacto por esta atividade. Este campo está vazio se a entidade que sofreu o impacto não for uma função.
- **Versão do aplicativo do iniciador:** Número da versão do aplicativo. Este campo está vazio se a atividade for iniciada pela entidade de uma função.
- **Versão do iniciador:** Número da versão do iniciador. Este campo está vazio se a atividade for iniciada por um usuário.
- **Iniciador original:** (Usado para fazer login remoto em sistemas federados) Quem ou qual função foi executada no host Federation™. Nesse caso, o *Iniciador* corresponde ao usuário Federation™.

Configurar registro de eventos para sequências de vídeos

Para os sistemas com muitas sequências de vídeos configuradas, o relatório *Trilhas de atividades* pode ser imenso devido ao número de conexões e desconexões de câmera. Você pode reduzir o tamanho do relatório configurando o sistema para registrar somente as conexões e desconexões de sequências de câmeras.

O que você deve saber

- Como padrão, o registro está habilitado para todas as conexões e desconexões de todas as câmeras e sequências de câmeras. Se o relatório de *Trilhas de atividades* for gerenciável usando este padrão, então não é necessário modificar esta configuração.
- Se você desabilitar *Trilhas de atividades* em sequências, as alterações da conexão da câmera dentro de uma sequência não são registradas; somente as conexões e desconexões da sequência de câmeras são registradas.
- Essa alteração na configuração aplica-se somente à estação de trabalho onde o arquivo é modificado.

Configurar registro de eventos para sequências de vídeos:

1 Em um editor de texto, abra o arquivo *GeneralSettings.gconfig* encontrado na pasta *ConfigurationFiles* na pasta de instalação do Security Center (*C:\Program Files (x86)\Genetec Security Center 5.7*).

2 Encontre o nó `<mediaPlayer>` e modifique-o para `<mediaPlayer IsActivityTrailEnabledOnSequence="false">` ou `<mediaPlayer IsActivityTrailEnabledOnSequence="true">`, como necessário.

3 Salve as alterações e feche o arquivo.

A nova configuração tem efeito imediato.

4 Repita o procedimento para outras estações de trabalho, como necessário.

Descobrindo quais mudanças foram feitas na configuração do sistema

Você pode descobrir quais alterações de configuração foram feitas no sistema, quem as fez, quando e em quais configurações de entidade (valores antes e depois), usando o relatório *Trilhas de auditoria*.

O que você deve saber

O relatório de trilhas de auditoria é útil se você ver que as propriedades de uma entidade foram alteradas e você deve descobrir quem fez essas alterações e quando (por exemplo, se o modo de gravação de uma câmera foi modificado). Além disso, se você solicitou uma atualização para uma entidade (por exemplo, os privilégios para um usuário), você pode verificar se as alterações foram feitas a partir do Config Tool.

Para descobrir quais mudanças foram feitas na configuração do sistema:

1 Na página inicial, abrir a tarefa *Trilhas de auditoria*.

2 Definir os filtros de consulta para o relatório. Escolha de um ou mais dos filtros abaixo:

- **Aplicativo:** Qual aplicação do cliente foi usada para a atividade.
- **Entidades:** Selecionar as entidades que deseja investigar. É possível filtrar as entidades por nome e por tipo.
- **Horário da modificação:** Entidades modificadas no intervalo especificado.
- **Modificado por:** Usuário ou função responsável pela modificação da entidade.

3 Clique em **Gerar relatório**.

A descrição das alterações (valores antes e depois) para as entidades selecionadas, bem como quem fez essas modificações e quando, estão listadas no painel de relatório.

Colunas de relatório para a tarefa Rastreio de auditoria

Após gerar um relatório, os resultados da sua pesquisa são listados em um painel de relatório. Esta seção lista as colunas disponíveis para a tarefa de relatório relevante.

- **Entidade:** Nome da entidade afetada pela modificação
- **Tipo da entidade:** Tipo da entidade afetada pela modificação
- **Descrição:** Descrição da modificação da entidade.
- **Iniciador:** Quem ou qual função fez a modificação da entidade.
- **Tipo de iniciador:** Tipo da entidade que iniciou as modificações.
- **Máquina do iniciador:** Computador usado para fazer a alteração
- **Aplicativo do iniciador:** Aplicativo usado para fazer a alteração
- **Versão do aplicativo do iniciador:** Número da versão do aplicativo. Este campo está vazio se a atividade for iniciada pela entidade de uma função.
- **Horário da modificação:** Horário em que a entidade foi modificada pela última vez

Alterações de configuração registradas pelo sistema Security Center

Todas as alterações de configuração são registradas pelo sistema. Você pode investigar essas alterações com o relatório *Trilhas de auditoria*.

A tabela a seguir apresenta as descrições de alterações que você pode esperar do relatório *Trilhas de auditoria*.

Tipo de modificação	Descrição
Criações de entidades	Entidade criada: <*Nome da entidade na criação*>.
Exclusões de entidades	Entidade excluída: <*Nome da entidade na exclusão*>.
Modificações de membros	• <*Entidade*> é agora membro de <*Entidade de grupo*>. • <*Entidade*> não é mais membro de <*Entidade de grupo*>. **NOTA:** <Entidade de grupo> pode ser uma área, uma partição, um grupo de portadores de cartões ou um grupo de usuários.
Modificações de permissões de acesso	• <*Usuário ou grupo de usuários*> ganhou direitos de acesso a <*Partição*>. • <*Usuário ou grupo de usuários*> perdeu direitos de acesso a <*Partição*>.
Modificações de privilégios	O valor de <*Privilégio*> foi alterado de <*Valor antigo*> para <*Valor novo*>.
Modificações de propriedades	O valor de <*Propriedade*> foi alterado de <*Valor antigo*> para <*Valor novo*>. **NOTA:** Nem todas as modificações de propriedades são descritas com valores anteriores e posteriores. Para obter a lista exata das propriedades que mostram este nível de detalhe, consulte Alterações de propriedades registradas com os valores antes e depois na página 327.

Tipo de modificação	Descrição
Ativações/desativações de funções	O valor do estado Ativo foi alterado de <*Valor antigo*> para <*Novo valor*>.
Modificações de mapas	• <*Entidade*> foi adicionado como um link ao mapa <*Map entity*>. • <*Entidade*> foi removido como um link do mapa <*Map entity*>. • Configuração de <*Entidade*> modificada. • Configuração de <*Entidade de câmera*> modificada para Movimento ativo/inativo. • Configuração de <*Entidade de câmera*> modificada para Gravação ligada/desligada. • Configurações de estado de <*Entidade de zona*> modificadas. • Camadas de mapa adicionadas/removidas (<*camada(s)*>) • Georreferência modificada. • Visualização padrão modificada. • Plano de fundo modificado.

Alterações de propriedades registradas com os valores antes e depois

A maioria das modificações de propriedades registradas pelo sistema são descritas com valores antes e depois.

A tabela a seguir lista todas as modificações de propriedade registradas com os valores antes e depois, ordenados por tipo de entidade. As alterações que não estão explicitamente listadas nesta tabela são registadas com a descrição genérica *Propriedades modificadas*.

Tipo da entidade	Aba de configurações	Alterações descritas com valores anteriores e atuais
Todos os tipos de entidades	Identidade	Nome Descrição ID lógico Relacionamentos • Ações • Associação de partição • Todos os outros relacionamentos específicos
Todos os tipos de unidade	Localização	Todas as propriedades
Unidade de controle de acesso	Todas as abas	Todas as propriedades (exceto configurações periféricas)
Access Manager (função)	Todas as abas	Todas as propriedades
Regra de acesso	Todas as abas	Todas as propriedades
Active Directory (função)	Todas as abas	Todas as propriedades
Active Directory Federation Service (função)	Todas as abas	Todas as propriedades
Alarme	Todas as abas	Todas as propriedades
Área	Propriedades	Todas as propriedades
	Avançado	Todas as propriedades (exceto configurações de portas: perímetro ou cativas)

Tipo da entidade	Aba de configurações	Alterações descritas com valores anteriores e atuais
Archiver (função)	Configurações padrão da câmera	Gravando • Modos de gravação (agendamento e modo) • Gravar áudio • Gravar metadados • Arquivamento redundante • Limpeza automática • Período de retenção • Tempo de gravação anterior a um evento • Tempo para gravar após um movimento • Duração inicial de gravação manual Codificação • Ligada/desligada • Certificados

	Recursos	Configurações avançadas
		• Marca d'água em vídeos
		• Apagar arquivos mais antigos quando os discos estiverem cheios
		• Habilitar solicitações de reprodução na unidade
		• Habilitar solicitações de instantâneos
		• Limiar de vídeo protegido
		• Limiar de advertência de carga de disco
		• Capacidade máxima de processamento de transferência de arquivo
		• Arquivos de vídeo
		  • Duração máxima
		  • Tamanho máximo

Modelo do crachá	Todas as abas	Todas as propriedades

Tipo da entidade	Aba de configurações	Alterações descritas com valores anteriores e atuais
Câmera	Vídeo	Qualidade do vídeo • Cronograma • Resolução • Taxa de transf. de bits constante • Taxa de transferência de bits • Taxa máxima permitida de transferência de bits • Qualidade da imagem • Taxa de quadros • Intervalo do quadro-chave • Medição de intervalo chave de quadros (segundos/ imagens) • Prioridade de taxa de bits • Velocidade de quadro de gravação • Todas as configurações de compressão específicas dos fabricantes Uso do stream Configurações de rede • Tipo de conexão • Endereço e porta de Multicast Melhorar a qualidade na gravação manual • Ligada/desligada • Configurações de compressão para gravação manual (igual a qualidade de vídeo) Melhorar a qualidade na gravação de evento • Ligada/desligada • Configurações de compressão para gravação manual (igual a qualidade de vídeo)

Tipo da entidade	Aba de configurações	Alterações descritas com valores anteriores e atuais
	Gravando	Gravando • Herdar do Archiver/Configurações personalizadas • Modos de gravação (agendamento e modo) • Gravar áudio • Gravar metadados • Arquivamento redundante • Limpeza automática • Período de retenção • Tempo de gravação anterior a um evento • Tempo para gravar após um movimento • Duração inicial de gravação manual Codificação • Ligada/desligada • Certificados
	Detecção de movimento	Cronograma Ligada/desligada Detecção de movimento por software/hardware Sensibilidade Detecções em quadros consecutivos Zonas de movimento • Adicionar/remover • Máscara de movimento • Limiar de movimento ativo • Evento de movimento ativo • Movimento do limiar • Evento de movimentação inativa • Sensibilidade • Máscara de movimento
Titular do cartão	Todas as abas	Todas as propriedades
Credencial	Todas as abas	Todas as propriedades
Directory Manager (função)	Todas as abas	Todas as propriedades
Federação (funções)	Todas as abas	Todas as propriedades
Monitor de Saúde (função)	Todas as abas	Todas as propriedades

Tipo da entidade	Aba de configurações	Alterações descritas com valores anteriores e atuais
Lista de procurados	Propriedades	Prioridade Caminho da lista de procurados
	Avançado	Todas as propriedades
LPR (tarefa)	Configurações gerais	Todas as configurações
LPR Manager (função)	Propriedades	Configurações gerais - Todas as configurações Ao vivo - Todas as configurações Associação de arquivos - Todas as configurações Correspondência - Todas as configurações Geocodificação - Todas as configurações Filtragem de placas - Todas as configurações Notificação por e-mail - Todas as configurações Importação de XML - Todas as configurações Exportação de XML - Todas as configurações Provedor de atualizações - Todas as configurações AutoVu™ Free-Flow - Todas as configurações
Gerenciador de mapas (função)	Recursos	Todas as propriedades
Media Router (função)	Propriedades	Configurações do redirecionador • Capacidade de vídeo ao vivo • Capacidade de reprodução • Controle de largura de banda
Regra para horas extras	Propriedades	Todas as propriedades
Estacionamento	Propriedades	Todas as propriedades
Partição	Propriedades	Todas as propriedades
Patroller	Propriedades	Todas as propriedades
Autorização	Propriedades	Caminho da autorização
	Avançado	Todas as propriedades
Restrições de autorização	Propriedades	Todas as propriedades
Gerenciador de relatório (função)	Todas as abas	Todas as propriedades

Tipo da entidade	Aba de configurações	Alterações descritas com valores anteriores e atuais
Usuário	Propriedades	Status Informações pessoais - Todas as configurações Configurações de senha • Expiração (em dias) • Alterar no próximo logon Nível de usuário Sobreposição de PTZ
	Avançado	Configurações de logon - Todas as configurações Configurações de Security Desk - Todas as configurações Limitar visualização de arquivo
Grupo de usuários	Propriedades	• Endereço de e-mail • Nível de usuário • Sobreposição de PTZ • Membros
	Avançado	Configurações de logon - Todas as configurações Configurações de Security Desk - Todas as configurações Limitar visualização de arquivo
Gerenciador de zona (função)	Todas as abas	Todas as propriedades
Visitante	Todas as abas	Todas as propriedades

15

Web Client Server

Esta seção inclui os seguintes tópicos:

- "Sobre Web Client Servers" na página 334
- "Criar Web Client Servers" na página 335
- "Configurar Web Client Servers" na página 337

Sobre Web Client Servers

O Web Client Server é a função usada para configurar o Security Center Web Client, um aplicativo da Web que oferece aos usuários acesso remoto ao Security Center. Cada função criada define um endereço da Web exclusivo (URL) que os usuários inserem no navegador da Web da Internet para fazer logon no Web Client e acessar informações do Security Center.

São permitidas várias instâncias da função Web Client Server. Você pode criar uma função para usuários locais e uma função diferente para usuários remotos, que acessam a rede do Security Center pela Internet.

Recomenda-se instalar funções em servidores de expansão separados.

Cada função deve ter uma URL exclusiva. O formato da URL é *https://nome de host ou endereço IP do computador:port/webAddress*.

Se várias funções forem criadas no mesmo servidor, cada uma delas deverá usar uma porta HTTPS ou um endereço da Web diferente. Caso contrário, a entidade da função fica em amarelo e um evento de *Aviso de entidade* é gerado.

Os padrões são a porta HTTP 80 e a porta HTTPS 443.

Criar Web Client Servers

Criar uma função Web Client Server para hospedar um Web Client e definir o endereço da web (URL) que os usuários entram nos seus navegadores para acessar o Security Center Web Client.

O que você deve saber

- Se o seu sistema só terá um único Web Client Server, você pode então criar a função usando as configurações padrão. Contudo, se tiver um sistema complexo que envolva várias redes privadas, você pode escolher implementar diversas funções Web Client Server, nesse caso, pode precisar alterar as configurações padrão de cada função.
- Quando um Web Client Server é criado, ele é implantado para o servidor principal do Security Center. Caso tenha diversas funções Web Client Server, mova cada um das funções para um servidor de expansão para que as cargas de tráfego sejam bem distribuídas.
- Uma função Media Gateway é criada automaticamente e hospedada no mesmo servidor Security Center que a função Web Client Server.
- Se você implantar vários Web Clients no mesmo servidor, certifique-se de que a URL para cada um seja única. Caso contrário, a entidade da função fica em amarelo e um evento de *Aviso de entidade* é gerado.
- Se os usuários finais forem monitorar vídeo no Web Client usando os navegadores Mozilla Firefox ou Microsoft Edge, certifique-se de que **uma** das seguintes condições sejam satisfeitas:
  - Um certificado SSL válido instalado no Web Client Server.
  - Caso esteja usando o certificado SSL auto-assinado padrão, certifique-se de que as portas REST na função Media Gateway e nas configurações de porta do Web Client Server correspondam; os padrões são porta 80 para HTTP e porta 443 para HTTPS.

Para criar um Web Client Server:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.

2 Clique em **Adicionar uma entidade** () e clique em **Web Client Server** ().

3 (Opcional) Defina **Tempo de sessão ilimitado** para **Ligado** para que os usuários permaneçam conectados ao Web Client enquanto mantiverem sua janela do navegador aberta.

Defina **Tempo de sessão ilimitado** para **Desligado** para que os usuários terminem sessão no Web Client automaticamente após 12 horas de inatividade.

4 Na página *Informações básicas*, insira um nome e uma descrição para a função.

5 Selecione a **Partição** da qual esta função seja membro e clique em **Próximo**.

Somente usuários que sejam membros da partição poderão visualizar ou modificar essas entidades.

6 Clique em **Próximo** > **Criar** > **Fechar**.

A nova função do Web Client Server está criada.

7 Na página do Web Client Server, clique na aba **Propriedades**.

8 Se você tiver várias funções de Web Client Server, verifique se a URL padrão em **Configurações de comunicação** não corresponde à URL de outros Web Client Servers no seu sistema. Se corresponder, mude o endereço da web e/ou as configurações de porta para que a URL deste Web Client seja única.

A URL padrão de um Web Client é *https://host:443/SecurityCenter*, onde o host é o endereço de IP ou o nome de host do computador do servidor que hospeda o Web Client Server.

9 Clique em **Aplicar**.

Após terminar

- Se esta for uma de várias funções de Web Client Server, mova a função para o seu próprio servidor.

- Para configurar o failover para essa função, adicione um servidor em espera.
- Se as configurações de porta padrão entrarem em conflito com outros aplicativos no seu sistema, é possível alterar as portas usadas pelo Web Client e o Media Gateway. Na função Servidor Web Client, na página *Propriedades*, deslize o controle deslizante **Usar portas da web padrão do servidor** para **DESLIGADO**, depois altere as portas HTTP e HTTPS. As configurações padrão são a porta HTTP 80 e a porta HTTPS 443. Clique em **Aplicar** para salvar as suas alterações. Depois faça as mesmas alterações às configurações de porta REST na função Media Gateway.

Configurar Web Client Servers

Após ter criado um Web Client Server, você pode configurar o tempo de sessão do usuário, estatísticas de uso, a URL, configurações de porta e o certificado SSL.

O que você deve saber

- Por padrão, um Web Client Server é implantado para o servidor principal do Security Center. Se você tiver vários Web Client Servers, atribua cada função a um servidor de expansão diferente.
- A URL de cada Web Client deve ser exclusiva.
- Você pode configurar balanceamento de carga adicionando vários servidores na aba **Recursos**. O Security Center usa automaticamente o servidor que tenha o menor número de conexões.
- Se os usuários finais forem monitorar vídeo no Web Client usando os navegadores Mozilla Firefox ou Microsoft Edge, certifique-se de que **uma** das seguintes condições sejam satisfeitas:
  - Um certificado SSL válido instalado no Web Client Server.
  - Caso esteja usando o certificado SSL auto-assinado padrão, certifique-se de que as portas REST na função Media Gateway e nas configurações de porta do Web Client Server correspondam; os padrões são porta 80 para HTTP e porta 443 para HTTPS.

Para modificar uma função Web Client Server:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.
2 Clique no **Web Client Server** que deseja alterar.
3 Na aba **Identidade**, você pode:
   a) Altere o nome da função de acordo com o que aparece no Config Tool.
   b) Atribua a função a uma partição diferente.
4 Clique na guia **Propriedades.**
5 Configure o comportamento de uma sessão de usuário selecionando uma das seguintes opções:
   a) Defina **Tempo de sessão ilimitado** para **Ligado** para que os usuários permaneçam conectados ao Web Client enquanto mantiverem sua janela do navegador aberta.
   b) Defina **Tempo de sessão ilimitado** para **Desligado** para que os usuários terminem sessão no Web Client automaticamente após 12 horas de inatividade.
6 Se as configurações de portas padrão entrarem em conflito com outras funções ou aplicativos em seu sistema, defina **Usar as portas Web padrão do servidor** como **Desligado** e altere as portas.

   Por padrão, a porta HTTP é 80 e a porta HTTPS é 443.
7 Para alterar a URL usada para acessar este Web Client, altere o **endereço Web**.

   Para ver a URL, procure em *Configurações de comunicação*.
8 Clique em **Aplicar**.
9 Verifique se a URL abre o Security Center Web Client clicando na URL em *Configurações de comunicação* na aba **Propriedades**.

   Se estiver usando o certificado autoassinado padrão e ele não estiver instalado no seu computador, o seu navegador exibe uma mensagem de erro. Prossiga para a página de logon executando o seguinte:
   - No Google Chrome, clique em **Mostrar avançadas** e, em seguida, clique em **Prosseguir para *ComputerName* (não seguro)**
   - No Internet Explorer, clique em **Continuar neste site (não recomendado)**.

   A página de logon do Security Center Web Client é exibida.
10 Se você tiver vários Web Client Servers, mova esta função para o seu próprio servidor de expansão.
11 Para adicionar balanceamento de carga e failover para o Web Client Server, adicione um servidor em espera.

Segurança do sistema

Esta parte inclui as seguintes chapters:

- "Introdução à segurança do sistema" na página 339
- "Partições" na página 343
- "Usuários e Grupos de usuários" na página 349
- "TLS e Autenticação no Directory" na página 371
- "Integração do Active Directory" na página 383
- "Autenticação baseada em declarações" na página 397
- "Criptografia de transmissão de fusão" na página 416

16

Introdução à segurança do sistema

Esta seção inclui os seguintes tópicos:

- "Definir quem pode acessar o Security Center " na página 340
- "Proteger seu data center contra ameaças externas" na página 341

Definir quem pode acessar o Security Center

Ao definir quem pode acessar o Security Center, você deve definir primeiro as partições de segurança (limites de responsabilidade) e, em seguida, selecionar os grupos de usuários e usuários individuais que podem acessar essas partições.

O que você deve saber

Embora o Security Center proteja os ativos da sua empresa (edifícios, equipamentos, dados importantes coletados em campo e assim por diante), seu trabalho como administrador é proteger o software do Security Center contra acesso ilegal.

Ao garantir o acesso ao seu software, você deve fazer as três seguintes perguntas:

- Quem precisa usar o sistema? – Quais *usuários* e *grupos de usuários* podem fazer logon?
- Para quê eles vão usá-lo? – Quais *privilégios* eles devem ter?
- Sobre quais partes do sistema eles são responsáveis? – Quais *partições* eles devem acessar?

MELHOR PRÁTICA: É mais fácil definir partições de segurança quando você configura seu sistema pela primeira vez. Dessa forma, à medida que você cria entidades no seu sistema, você pode colocá-las diretamente nas partições às quais pertencem. Se você começar criando usuários primeiro, poderá acabar tendo que revisitar seus direitos de acesso toda vez que adicionar uma nova partição ao seu sistema.

Para definir quem pode acessar o Security Center:

1 Decida se as partições são úteis na sua situação.

2 Se as partições forem úteis, identifique as partes do seu sistema que são relativamente independentes umas das outras e crie uma partição para cada parte.

Exemplo: Se seu sistema abrange vários locais e se a equipe de segurança em cada local funciona independentemente das equipes de segurança em outros locais, crie uma partição para cada local.

3 Identifique os grupos de usuários que compartilham as mesmas funções e responsabilidades e crie um grupo de usuários para cada um.

Exemplo: Todos os operadores de segurança podem formar um grupo e todos os investigadores podem formar outro grupo.

4 Se você tiver grupos de pessoal trabalhando em diferentes partições, defina um grupo de usuários para cada um deles, adicione-os como membros do maior grupo de usuários e conceda a eles acesso às respectivas partições.

Cada subgrupo individual deve ter permissão para acessar uma partição diferente. Com esta organização, o objetivo dos grupos de usuários pai é separar os usuários de acordo com suas funções e responsabilidades (operadores, investigadores, supervisores e assim por diante). O objetivo dos grupos de usuários filho é separar os usuários de acordo com suas áreas de responsabilidade.

Consoante você deseje que o gerenciamento de usuários seja centralizado ou descentralizado, cada subgrupo individual pode pertencer à mesma partição do seu grupo de usuários pai, gerenciada pelo mesmo administrador, ou pertencer a partições diferentes, gerenciadas por diferentes administradores.

5 Defina os usuários individuais e adicione-os como membros dos grupos de usuários.

MELHOR PRÁTICA: Tente adicionar os usuários como membros do menor grupo. Permita que cada usuário herde tudo do grupo de usuários principal e somente recorra a configurá-los individualmente para exceções.

Proteger seu data center contra ameaças externas

Se a política de segurança da sua empresa exigir que todos os bancos de dados corporativos residam em uma rede protegida, você deve criar Gateways do Directory para permitir que os aplicativos do Security Center localizados fora da rede protegida façam logon no sistema.

Antes de iniciar

Verifique se o *Número de servidores adicionais do Directory* suportado por sua licença do Security Center permite que você adicione os *gateways do Directory* que você precisa criar. Os gateways do Directory são contados como *Servidores do Directory* na sua licença do Security Center.

O que você deve saber

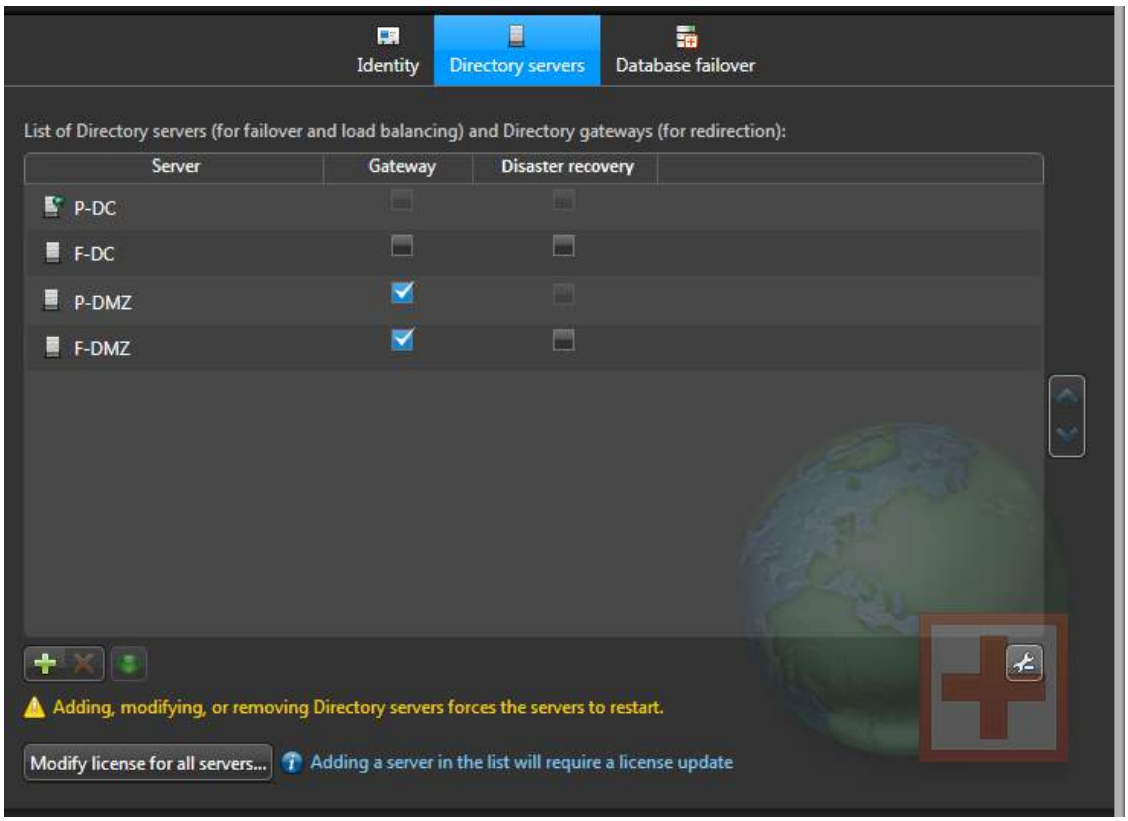
Todos os aplicativos do Security Center (funções e aplicativos cliente) devem se conectar a um servidor do Directory para fazer logon no sistema. Todos os servidores do Directory devem acessar o banco de dados do Directory onde a configuração do sistema é armazenada. Se o banco de dados do Directory residir em uma rede protegida, nenhum aplicativo localizado fora da rede protegida terá a permissão para acessá-lo. Para evitar violar a política de segurança, você deve criar gateways de Directory na rede não protegida.

Para criar gateways do Directory:

1. Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.
2. Selecione a função **Directory Manager** ( ) e clique na aba **Servidores do Directory**.
3. Na parte inferior da lista de servidores, clique em **Avançado** ( ).
   Uma coluna extra, **Gateway**, aparecerá na lista.
4. No fim da lista, clique em **Adicionar um item** ( ).
5. Na caixa de diálogo que aparecer, selecione o servidor que deseja adicionar e clique em **Adicionar**.
6. Adicione mais servidores à lista, se necessário.
7. Selecione a opção **Gateway** nos servidores que você deseja usar como gateways do Directory.
   Um gateway do Directory deve estar localizado na rede não protegida. Ele não precisa acessar o banco de dados do Directory, mas precisa se conectar ao servidor principal. O exemplo a seguir mostra um sistema com dois servidores do Directory (um dos quais é o servidor principal) e dois gateways do Directory.

   NOTA:

   - *O balanceamento de carga* ocorre somente entre servidores do mesmo tipo. Todos os servidores do Directory pertencem a um conjunto de balanceamento de carga e todos os gateways do Directory diretório pertencem a outro. Um usuário tentando se conectar a um gateway do Directory não será redirecionado para um servidor do Directory e vice-versa.
   - A opção de **Recuperação de desastre** aplica-se somente aos servidores do Directory, não a Gateways.



8 Atualize sua licença para incluir os servidores que você acabou de promover a gateways do Directory.
9 Clique em **Aplicar**.

Após terminar

Se você tiver estações de trabalho de cliente que são forçadas a se conectar a um Directory específico, atualize suas configurações para que elas se conectem a um dos gateways do Directory em vez disso.

Tópicos relacionados

Preparar failover e balanceamento de carga do Directory na página 168

17

Partições

Esta seção inclui os seguintes tópicos:

- "Sobre partições" na página 344
- "Criar partições" na página 345
- "Atualizar o conteúdo das partições" na página 346
- "Conceder direitos de acesso para as partições" na página 348

Sobre partições

É um tipo de entidade que define um conjunto de entidades que são visíveis apenas para um grupo específico de usuários. Por exemplo, uma divisão poderia incluir todas as áreas, portas, câmeras e zonas em um edifício.

As partições eliminam a tediosa tarefa de criar relações um a um entre os usuários e as entidades que eles podem ver no sistema. Se um usuário não tiver direitos a uma partição, essa partição e tudo o que ela contém ficarão ocultos daquele usuário.

Cada partição é definida pelos seguintes parâmetros:

- **Lista de membros.:** Entidades que pertencem à partição (áreas, portas, câmeras, portadores de cartão, usuários, e assim por diante).
- **Lista de usuários aceitos:** Usuários e grupos de usuários que têm direito de acesso às entidades contidas na partição. O tipo de acesso que cada usuário tem (visualizar, adicionar, modificar e excluir) é determinado pelos *privilégios* de cada usuário individual. Exceções aos privilégios básicos de um usuário podem ser configuradas para cada partição à qual o usuário tenha acesso.

  NOTA: Um usuário autorizado de uma partição não é necessariamente membro dessa partição, nem um usuário que seja membro de uma partição necessariamente é um usuário autorizado.

Benefícios de partições

Dividir seu sistema em partes menores tem os seguintes benefícios:

- Reduz o escopo do que um usuário pode acessar por questões de segurança. Por exemplo, em um sistema em vários locais, pode ser indesejável que a equipe de segurança de um local seja capaz de ver ou interferir com as atividades da equipe de segurança de outro local.
- Reduz o escopo do trabalho de um usuário para torná-lo mais gerenciável. Se um usuário é responsável apenas por uma parte do sistema (um local em um sistema em vários locais), é melhor não distrair o usuário com as entidades pelas quais o usuário não é responsável.

Partições criadas pelo sistema

Por padrão, duas partições são criadas no Security Center. Eles são invisíveis, a menos que você tenha criado explicitamente outras partições em seu sistema. A ideia é que, se você não precisa dividir seu sistema em partições, você não precisa ver nenhuma partição.

- **Partição raiz:** A partição *raiz* () é a partição que contém tudo o que você criar no seu sistema. Ela tem o nome de seu *servidor principal*. Quando não há partições criadas pelo usuário no sistema, todas as entidades criadas pertencem à partição raiz e todos os usuários são usuários autorizados da partição raiz.
- **Partição do sistema:** A partição *Sistema* () é uma partição gerenciada exclusivamente pelo sistema, com a finalidade de manter certas entidades do sistema sempre acessíveis a todos os usuários, como o agendamento *Sempre*, a entidade *rede Padrão*, a entidade principal do servidor, a função Monitor de Saúde, a função Gerente de Relatórios e assim por diante. Ninguém pode alterar a partição do Sistema, nem mesmo os administradores do sistema.

NOTA: A partição raiz e a partição do sistema são as duas únicas partições de nível superior no sistema. Todas as partições criadas são subordinadas à partição raiz.

Criar partições

Para dividir seu sistema em partes menores e gerenciáveis e ocultar algumas dessas partes de determinados usuários, você pode criar partições.

O que você deve saber

A primeira partição que você criar sempre será adicionada à partição raiz. As partições subsequentes criadas são adicionadas à partição selecionada na árvore de entidades. Se nenhuma estiver selecionada, o sistema solicitará que você especifique em qual partição você deseja criar a nova.

Para criar uma partição:

1 Na página inicial do Config Tool, execute uma das seguintes opções:

- Abra a tarefa *Gerenciamento de usuários*, clique em **Adicionar uma entidade** ( ) e clique em **Partição**.
- Abra qualquer tarefa de administração, clique em **Adicionar uma entidade > Mostrar tudo > Partição**, ou clique em **Mais** ( )ao lado do botão **Adicionar** ( ) e clique em **Partição**.

2 Se uma partição estiver selecionada na árvore de entidade antes de clicar em **Adicionar**, então a nova partição será criada imediatamente sob a partição selecionada.
   a) Introduza o nome da **Nova partição**.
   b) Na aba **Identidade**, digite a descrição da partição.

3 Se nenhuma partição foi selecionada na árvore de entidades antes de clicar em **Adicionar**, o Assistente de *Criação de partição* abrirá.
   a) Na página *Informações básicas*, insira o nome e a descrição da nova partição.
   b) Na lista suspensa **Partição**, selecione a partição principal à qual esta nova partição deve pertencer.

   A nova partição é criada.

4 Se você já tiver entidades prontas para serem adicionadas à nova partição, adicione-as agora.

5 Se os usuários e grupos de usuários já estiverem criados em seu sistema, conceda os direitos de acesso para a nova partição a quem precisa deles.

A partição é criada. Novas entidades que você criar podem ser adicionadas diretamente à partição.

Tópicos relacionados

Sobre partições na página 344

Atualizar o conteúdo das partições

Você pode controlar a visibilidade das entidades para os usuários em seu sistema adicionando ou removendo entidades das partições que esses usuários estão autorizados a acessar.

O que você deve saber

Quando você coloca entidades relacionadas, como portadores de cartão e credenciais, em partições diferentes, os usuários que não estão autorizados a acessar todas as partições envolvidas podem não ter todos os direitos de acesso de que precisam para realizar suas tarefas. Para simplificar o processo de configuração de partições, quando você adiciona ou remove entidades de uma partição, o sistema adiciona ou remove automaticamente suas entidades relacionadas dessa partição. As regras de senso comum aplicadas pelo sistema são as seguintes:

- Adicionando um grupo de usuários ou um grupo de portadores de cartão também adiciona seus membros.
- Adicionar um usuário ou um titular de cartão não adiciona automaticamente seus grupos principais.
- Remover um grupo de usuários ou um grupo de portadores de cartão também remove seus membros.
- Remover um usuário ou um titular de cartão não remove automaticamente seus grupos principais.
- Adicionar um titular de cartão também adiciona suas credenciais associadas.
- Remover um titular de cartão também remove suas credenciais associadas.
- Adicionar uma credencial não adiciona automaticamente o titular de cartão associado.
- Remover uma credencial não remove automaticamente o titular de cartão associado.
- Ao adicionar uma entidade que tenha entidades subordinadas anexadas (como uma área ou uma função), você precisa especificar se deseja ou não adicionar suas entidades subordinadas também (o que inclui tudo o que está abaixo da hierarquia dessa entidade).
- Ao remover uma entidade que tenha entidades subordinadas anexadas (como uma área ou uma função), você precisa especificar se deseja ou não remover suas entidades subordinadas também (o que inclui tudo o que está abaixo da hierarquia dessa entidade).
- Adicionar uma entidade a uma partição não a remove das outras partições a que pertence. Não há limite para o número de partições a que uma entidade pode pertencer.
- A remoção de uma entidade de uma partição a adiciona automaticamente à partição raiz se essa entidade não pertencer a nenhuma outra partição criada pelo usuário.
- Não é possível remover uma entidade da partição raiz se essa entidade não pertencer a nenhuma outra partição.

Para atualizar o conteúdo de uma partição:

1. Na página inicial do Config Tool, abra qualquer tarefa de administração e selecione uma aba que mostre uma árvore de entidades.

   Se as partições não estiverem visíveis, clique em **Mostrar partições** ( ) na caixa **Pesquisar** ou pressione **F4**.
2. Selecione a partição que deseja modificar e clique na aba **Propriedades**.

   O conteúdo atual da partição é exibido na lista **Membros**.
3. Faça um dos seguintes:
   - Para adicionar entidades à partição, clique em **Adicionar** ( ), selecione as entidades na caixa de diálogo *Pesquisar* e, em seguida, clique em **Selecionar**.
   - Para remover entidades da partição, selecione as entidades na lista **Membros** e, em seguida, clique em **Remover** ( ).

DICA: Como alternativa, você pode alterar o conteúdo das partições diretamente a partir da árvore de entidades, utilizando arrastar e soltar para mover entidades e Ctrl+arrastar e soltar para copiar entidades.

Todas as alterações são imediatamente aplicadas.

Conceder direitos de acesso para as partições

Para permitir que os usuários acessem as entidades contidas em uma partição, você deve conceder direitos de acesso para essa partição aos usuários e grupos de usuários em questão.

O que você deve saber

Os direitos de acesso para partições são regidos pelas seguintes regras:

- Os direitos de acesso a partições são herdados dos grupos de usuários principais.
- Os direitos de acesso herdados não podem ser revogados.
- Os direitos de acesso não concedidos a um grupo de usuários podem ser concedidos aos membros do grupo de usuários.
- Conceder direitos de acesso para uma partição a um usuário ou grupo de usuários também concede direitos de acesso para suas partições subordinadas ao mesmo usuário ou grupo de usuários.
- Revogar direitos de acesso para uma partição principal de um usuário ou grupo de usuários também revoga direitos de acesso para suas partições subordinadas desse usuário ou grupo de usuários, exceto quando esses direitos de acesso são herdados dos grupos de usuários principais.
- Revogar direitos de acesso para uma partição subordinada a um usuário ou grupo de usuários também revoga direitos de acesso para sua partição principal ao mesmo usuário ou grupo de usuários.

Para conceder direitos de acesso para uma partição a um usuário:

1. Na página inicial do Config Tool, abra a tarefa *Gerenciamento de usuários*, selecione um usuário e então clique na aba **Direitos de acesso**.
2. Marque a caixa de seleção ao lado da partição para a qual deseja conceder direitos de acesso.

   Esta ação concede automaticamente direitos de acesso para todas as suas partições subordinadas também.
3. Para revogar direitos de acesso para algumas das partições subordinadas, desmarque a caixa de seleção ao lado das partições subordinadas selecionadas.
4. Clique em **Aplicar**.
5. Se necessário, sobrescreva os privilégios básicos que este usuário tem na partição.
6. Clique em **Aplicar**.

18

Usuários e Grupos de usuários

Esta seção inclui os seguintes tópicos:

- "Sobre grupos de usuários" na página 350
- "Criando grupos de usuários" na página 351
- "Sobre usuários" na página 353
- "Criando usuários" na página 355
- "Definir configurações de usuários" na página 356
- "Alterar configurações de senhas para usuários" na página 358
- "Sobre privilégios" na página 359
- "Modelos de privilégios" na página 361
- "Atribuir privilégios a usuários" na página 362
- "Personalizar opções de logon de usuário" na página 365
- "Forçando o Security Desk a ser executado no modo de tela cheia" na página 367
- "Selecionar quais estações de trabalho os usuários podem controlar remotamente" na página 369
- "Selecionar quais atividades de usuários registrar" na página 370

Sobre grupos de usuários

É um tipo de entidade que define um grupo de usuários que compartilham as propriedades e privilégios comuns. Ao se tornar membro de um grupo, um usuário automaticamente herda todas as propriedades do grupo. Um usuário pode ser membro de vários grupos. Os grupos de usuários também podem ser aninhados.

Benefícios de grupos de usuários

Como todos os usuários que fazem parte do grupo de usuários herdam automaticamente todas as propriedades desse grupo, isso simplifica a configuração de usuários em sistemas grandes.

Grupo de usuários administradores

O grupo de usuários *Administradores* é uma entidade de sistema que é criada durante a instalação. Ele não pode ser excluído ou renomeado. Os membros desse grupo de usuários também são conhecidos como *administradores do sistema*. Eles têm os mesmos direitos administrativos que o usuário *Admin* e seus direitos não podem ser revogados.

MELHOR PRÁTICA: Por razões de rastreabilidade, em vez de permitir que todos usem a mesma conta *Admin*, é melhor criar uma conta de usuário separada para cada administrador.

Criando grupos de usuários

Para agrupar usuários que compartilham propriedades e privilégios comuns, você pode criar grupos de usuários.

O que você deve saber

Você também pode importar grupos de usuários de seu serviço de diretório corporativo.

Para criar um grupo de usuários:

1 Na página inicial Config Tool, abra a tarefa *Gerenciamento de usuários*.
2 Clique em **Adicionar uma entidade** ( ) e clique em **Grupo de usuários** ( ).
3 Na página **Informações do grupo de usuários**, insira um nome e uma descrição para o grupo de usuários.
4 Na lista suspensa **Grupo de usuários**, selecione o grupo principal para o novo grupo de usuários.
O grupo de usuários herda automaticamente as propriedades de seu grupo de usuários principal.

NOTA: Sobre a participação na partição do grupo de usuários:

- Se você selecionar **Não atribuído**, o novo grupo de usuários será adicionado à partição raiz.
- Se você selecionar um grupo de usuários principal, o novo grupo de usuários será adicionado à mesma partição que o grupo de usuários principal pertence.

5 Para conceder ao grupo de usuários um conjunto predefinido de privilégios, selecione um **Modelo de privilégios** na lista suspensa.

NOTA: Se você não tiver certeza de quais privilégios o grupo de usuários precisa, você pode adiar essa decisão para mais tarde. O modelo de privilégios pode ser aplicado a qualquer momento.

6 Clique em **Próximo**.
7 (Somente se partições estiverem em uso) Na página **Direitos de acesso**, selecione as partições para as quais os direitos de acesso devem ser concedidos para este grupo de usuários.
8 Clique em **Próximo**.
9 Na página **Resumo de criação**, verifique se a partição ao qual o grupo de usuários pertence e as que o grupo de usuários está autorizado a acessar são as que você pretende.
10 Clique em **Criar > Fechar**.
O novo grupo de usuários é criado.
11 (Opcional) Tornar esse grupo de usuários um subordinado de outro grupo de usuários.

Tópicos relacionados

Modelos de privilégios na página 361

Adicionar grupos de usuários subordinados

Para economizar tempo na configuração do seu sistema, você pode criar subgrupos de usuários que herdam todos os atributos de seu grupo principal.

O que você deve saber

A adição de grupos de subgrupos de usuários é útil se você tiver vários níveis na equipe de gerenciamento e os subgrupos compartilharem quase todas as mesmas propriedades e privilégios (por exemplo, um grupo de usuários do turno diurno e um grupo de usuários do turno da noite em sua equipe de segurança).

Para adicionar um grupo de usuários subordinado:

1 Abra a tarefa **Segurança** e clique na visualização **Grupos de usuários**.

2 Selecione o grupo de usuários a ser configurado.
3 Na seção **Relacionamentos** da aba **Identidade**, selecione **Grupos de usuários pai** e clique em **Inserir um item** ( ).
4 Selecione um ou mais grupos de usuários pai e clique em **Selecionar** > **Aplicar**.

Adicionar usuários como membros de grupos de usuários

Para simplificar a configuração do seu sistema, você pode adicionar usuários como membros de um grupo de usuários para que herdem todas as propriedades desse grupo.

Para adicionar um usuário como membro de um grupo de usuários:

1 Na página inicial Config Tool, abra a tarefa *Gerenciamento de usuários*.
2 Selecione o grupo de usuários a configurar e clique na aba **Propriedades**.
3 Na seção **Membros,** clique em **Adicionar** ( ).
4 Selecione um ou mais usuários e clique em **Selecionar** > **Aplicar**.

DICA: Como alternativa, pode alterar a associação dos grupos de usuários diretamente na árvore de entidades, utilizando a função de arrastar e soltar para mover e Ctrl+arrastar e soltar para copiar.

Sobre usuários

É um tipo de entidade que identifica uma pessoa usa os aplicativos do Security Center e define os direitos e os privilégios que a pessoa tem no sistema. Os usuários podem ser criados manualmente ou importados de um Active Directory.

A cada usuário é atribuído um nome de usuário e uma senha, que são as credenciais necessárias para efetuar logon no sistema.

O que uma pessoa pode fazer no sistema é restrito por seus atributos de usuário:

- **Privilégios:** Limita os tipos de atividades que o usuário pode realizar no sistema.
- **Direitos de acesso às partições:** Limita as entidades nas quais o usuário pode exercer seus privilégios.

Um usuário pode ser membro de um ou mais *grupos de usuários*. Os usuários podem herdar os privilégios e os direitos de acesso de seus grupos de usuários principais.

Usuário administrador

O usuário *Admin* é um usuário criado por padrão e não pode ser excluído ou renomeado. Ele direitos administrativos totais para configurar o Security Center. Uma pessoa conectada como *Admin* pode adicionar, modificar e excluir qualquer entidade no Security Center.

MELHOR PRÁTICA: O usuário *Admin* é criado com uma senha em branco na instalação do software. Por questões de segurança, você deve alterar a senha do usuário *Admin* imediatamente após a instalação do software.

Níveis de usuários

É um valor numérico atribuído aos usuários para restringir sua capacidade de realizar certas operações, como controlar uma câmera PTZ, visualizar a alimentação de vídeo de uma câmera ou ficar registrado quando é definido um nível de ameaça. O nível 1 é o nível de usuário mais alto, com mais privilégios. Os níveis de usuários vão de 1 a 254. O nível de usuário pode ser herdado de um grupo pai. Se o usuário tiver vários pais, o nível de usuário mais alto será herdado. Se o usuário não tiver um grupo pai, o nível de usuário mais baixo (254) será herdado.

Os níveis de usuário afetam quatro coisas no Security Center:

- Eles determinam quais usuários são desconectados do sistema quando um nível de ameaça é definido. Por exemplo, se você configurar um nível de ameaça para desencadear a ação *Definir nível mínimo de usuário* quando o nível de ameaça é definido, os usuários com um nível de usuário inferior ao especificado são desconectados.
- Eles determinam quais usuários podem continuar visualizando uma transmissão de vídeo quando uma câmera é bloqueada no Security Desk. Quando você bloqueia uma câmera, os usuários que têm um nível de usuário inferior ao especificado não podem mais visualizar o fluxo de vídeo.
- Eles determinam quais usuários perdem suas conexões de fluxo de vídeo se um limite máximo de largura de banda é configurado para fluxos de vídeo que são redirecionados de um site remoto e o limite de largura de banda é excedido. Quando o limite de largura de banda é alcançado e um usuário com um alto nível de usuário solicitar uma transmissão, o usuários com o nível de usuário mais baixo que estiver visualizando o vídeo atualmente que está sendo redirecionado desse redirecionador perde sua conexão de transmissão de vídeo. Se vários usuários com o mesmo nível de usuário estiverem exibindo fluxos de vídeo daquele redirecionador, o usuário que solicitou o fluxo de vídeo por último perde a conexão.
- Eles determinam qual usuário tem prioridade sobre os controles PTZ de uma câmera quando dois ou mais usuários estão tentando assumir o controle de uma câmera ao mesmo tempo.

  Os usuários podem receber níveis de usuário diferentes para controles PTZ que substituem seu nível geral de usuário. A prioridade é dada sempre ao usuário com o nível o mais elevado (1 = o mais elevado).

Se dois usuários concorrentes tiverem o mesmo nível de usuário, o usuário que solicitou o fluxo primeiro receberá prioridade.

Uma vez que um usuário ganha controle sobre uma câmera PTZ, ela é bloqueada por esse usuário. Isso significa que nenhum outro usuário pode assumir o controle dessa câmera, a menos que tenha um nível de usuário mais elevado. O controle sobre a câmera PTZ é liberado automaticamente após um período de inatividade (configurado na aba **Hardware** da câmera).

Tópicos relacionados

Sobre privilégios na página 359
Sobre partições na página 344

Criando usuários

Para permitir que alguém inicie sessão no Security Center, é necessário criar uma entidade de usuário com credenciais de logon.

O que você deve saber

Você também pode importar usuários de seu serviço de diretório corporativo.

Por razões de segurança, o *Nome da entidade* para este usuário deve ser exclusivo, porque é também o nome de usuário usado para fazer logon no Security Center.

Para criar um usuário:

1 Na página inicial Config Tool, abra a tarefa *Gerenciamento de usuários*.
2 Clique em **Adicionar uma entidade** () e clique em **Usuário** ().
3 Na página **Informações do usuário**, digite um nome de usuário que ainda não exista.
4 Digite uma senha para que este usuário faça logon no Security Center e confirme a senha.
5 Digite o nome e sobrenome do usuário.
6 Na lista suspensa **Grupo de usuários**, selecione o grupo principal para o novo usuário.
O usuário herda automaticamente as propriedades de seu grupo de usuários principal.

NOTA: Sobre a participação na partição do usuário:

- Se você selecionar **Não atribuído**, o novo usuário será adicionado à partição raiz.
- Se você selecionar um grupo de usuários principal, o novo usuário será adicionado à mesma partição que o grupo de usuários principal pertence.

7 Para conceder ao usuário um conjunto predefinido de privilégios, selecione um **Modelo de privilégios** na lista suspensa.

NOTA: Se você não tiver certeza de quais privilégios o usuário precisa, você pode adiar essa decisão para mais tarde. O modelo de privilégios pode ser aplicado a qualquer momento.

8 (Somente se partições estiverem em uso) Na página **Direitos de acesso**, selecione as partições para as quais os direitos de acesso devem ser concedidos para este usuário..
9 Clique em **Próximo**.
10 Na página **Resumo de criação**, verifique se a partição ao qual o usuário pertence e as que o usuário está autorizado a acessar são as que você pretende.
11 Clique em **Criar > Fechar**.

A nova conta de usuário está criada.

Após terminar

Configure o usuário.

Tópicos relacionados

Modelos de privilégios na página 361

Definir configurações de usuários

Depois que um usuário é criado no Security Center, você pode configurar suas propriedades e limitar o que ele tem permissão para fazer no sistema.

Antes de iniciar

Crie o usuário.

O que você deve saber

Em vez de configurar as propriedades de um usuário individual, você pode adicionar o usuário como membro de um grupo de usuários para que ele herde todas as propriedades do grupo.

Para definir as configurações de um usuário:

1. Na página inicial Config Tool, abra a tarefa *Gerenciamento de usuários*.
2. Selecione o usuário a configurar e clique na aba **Propriedades**.
3. Para impedir temporariamente que o usuário faça logon no Security Center, desative o perfil de usuário.
4. Se pretender enviar e-mails ou mensagens para este usuário, escreva um endereço de e-mail no campo **Endereço de e-mail** e clique em **Aplicar**.

   Você pode enviar e-mails para usuários usando as ações *Enviar um e-mail* e *Enviar relatório por e-mail*.
5. Altere a senha do usuário ou suas configurações de senha.
6. Na opção **Nível de usuário**, especifique se o usuário herda seu nível de usuário de seu grupo de usuários pai, ou defina um nível específico, e clique em **Aplicar**.

   É um valor numérico atribuído aos usuários para restringir sua capacidade de realizar certas operações, como controlar uma câmera PTZ, visualizar a alimentação de vídeo de uma câmera ou ficar registrado quando é definido um nível de ameaça. O nível 1 é o nível de usuário mais alto, com mais privilégios.
7. (Opcional) Configure um nível de usuário diferente para controlar motores PTZ.
8. Conceda direitos de acesso a partições ao usuário.
9. Atribua privilégios ao usuário.
10. Personalize como o usuário pode fazer logon.
11. Para permitir que o usuário controle remotamente estações de trabalho do Security Desk, você deve selecionar as estações de trabalho que ele pode controlar.
12. Clique na aba **Avançado**.
13. Para mostrar as tarefas abertas do usuário quando ele faz logon no Security Desk, coloque a opção **Iniciar ciclo de tarefas no logon** em **Ligado** e clique em **Aplicar**.

    DICA: Para impedir que o usuário interrompa o ciclo de tarefas uma vez que o Security Desk seja aberto, negue a ele o privilégio *Iniciar/interromper ciclo de tarefas*.
14. Quando o usuário exporta um vídeo (G64x) ou instantâneos, o sistema pode incluir metadados (por exemplo, nome da câmera, data de criação, coordenadas da câmera) que podem ser úteis na investigação de incidentes. Para ativar metadados com arquivos exportados, coloque a opção **Incluir propriedades adicionais em exportação/instantâneo** em **Ligado** e clique em **Aplicar**.

Tópicos relacionados

Sobre usuários na página 353

Desativar perfis de usuários

Você pode desativar o perfil dos usuários que não devem mais ser autorizados a fazer logon no Security Center.

O que você deve saber

Um usuário não pode iniciar sessão quando seu perfil estiver desativado. Desativar o perfil de um usuário enquanto ele estiver conectado efetuará imediatamente o seu logoff.

Para desativar o perfil de um usuário:

1 Na página inicial Config Tool, abra a tarefa *Gerenciamento de usuários*.
2 Selecione o usuário a configurar e clique na aba **Propriedades**.
3 Coloque a opção **Status** em **Inativo** e clique em **Aplicar**.

Alterar configurações de senhas para usuários

Você pode definir a senha de um usuário para expirar após um determinado período de tempo, forçar o usuário a alterar sua senha no próximo logon ou impor uma complexidade mínima para todas as senhas de usuário.

O que você deve saber

Os requisitos de complexidade de palavra-passe aplicam-se a todas as novas senhas e entram em vigor quando um usuário altera a respectiva senha atual.

Somente usuários que tenham o privilégio de usuário *Alterar a própria senha* podem alterar sua própria senha. Caso contrário, eles devem entrar em contato com seu administrador para alterar sua senha.

Para alterar as configurações de senhas para um usuário:

1 Na página inicial Config Tool, abra a tarefa *Gerenciamento de usuários*.

2 Selecione o usuário a configurar e clique na aba **Propriedades**.

3 Para alterar a senha do usuário, clique em **Alterar senha**, digite uma senha, confirme a senha e clique em **OK**.

4 Para definir uma data de expiração para a senha do usuário, coloque a opção **Expira** em **Ligado** e selecione o número de dias.

O sistema avisa automaticamente os usuários se as suas senhas estão para expirar em breve e lhes dá a oportunidade de definir uma nova senha imediatamente. Você pode definir o período de notificação de expiração de senha entre 0 e 30 dias na tarefa Sistema.

5 Para exigir que o usuário altere sua senha na próxima vez que fizer logon no Genetec Patroller™ ou no Security Desk, coloque a opção **Alterar no próximo logon** em **Ligado**.

6 Clique em **Aplicar**.

7 Para adicionar requisitos de complexidade às senhas de usuário, abra a tarefa **Sistema**, clique na visualização **Configurações gerais** e clique na página **Configurações de senha do usuário**.

8 Na seção **Impor número mínimo de**, selecione entre os seguintes requisitos e digite um valor:

- **Caracteres:** Número mínimo de caracteres.
- **Letras maiúsculas:** Número mínimo de letras maiúsculas.
- **Letras minúsculas:** Número mínimo de letras minúsculas.
- **Caracteres numéricos:** Quantidade mínima de números.
- **Caracteres especiais:** Número mínimo de caracteres especiais.

9 Clique em **Aplicar**.

Sobre privilégios

Os privilégios definem o que os usuários podem fazer, como as zonas de armamento, bloqueio de câmeras e desbloqueio de portas, em parte do sistema que têm direito de acesso.

Os privilégios de usuário no Security Center estão divididos nos seguintes grupos:

- **Privilégios de aplicativos:** Concede acesso a aplicativos do Security Center.
- **Privilégios gerais:** Concede acesso aos recursos genéricos do Security Center.
- **Privilégios administrativos:** Concede acesso à configuração de entidades no Config Tool.
- **Privilégios de tarefas:** Controla a acessibilidade às várias tarefas do Security Center.
- **Privilégios de ação:** Controla as *ações* que podem ser realizadas nas entidades do sistema.

Para obter uma lista dos privilégios disponíveis, consulte Privilégios Security Center 5.7 no Hub TechDoc da Genetec™.

Você também pode consultar a página *Privilégios* de um usuário ou grupo de usuários na tarefa *Gerenciamento de usuários* do Config Tool.

Hierarquia de privilégios

Os privilégios são organizados em uma hierarquia, com o seguinte comportamento:

- Para que um privilégio filho seja permitido, o privilégio pai deve ser permitido.
- Se um privilégio pai for negado, todos os privilégios filhos são negados.
- Um privilégio filho pode ser negado quando o privilégio pai é permitido.

Herança de privilégios

As configurações de privilégio podem ser herdadas de grupos de usuários e substituídas no nível de membro (usuário ou grupo de usuários) de acordo com as seguintes regras:

- Um privilégio que é indefinido no nível de grupo pode ser permitido ou negado no nível de membro.
- Um privilégio que é permitido no nível de grupo pode ser negado no nível de membro.
- Um privilégio que é negado no nível de grupo é negado automaticamente no nível de membro.
- Quando um usuário é membro de vários grupos de usuários, o usuário herda as configurações de privilégios mais restritivas de seus grupos pais. Isso significa que *Negar* tem prioridade sobre *Permitir* e *Permitir* tem prioridade sobre *Indefinido*.

Exceções para regras de privilégio

As exceções a seguir se aplicam às regras de privilégios:

- **Usuários administrativos:** Os membros do grupo de usuários *Administradores* (que inclui o usuário *Admin*) têm direitos administrativos totais sobre o sistema. Eles podem configurar o Security Center conforme julguem necessário. O usuário *Admin* e o grupo de usuários *Administradores* são criados na instalação do sistema. Eles têm todos os privilégios e não podem ser modificados nem excluídos.
- **Ações reservadas para usuários administrativos:** São ações que somente os usuários administrativos podem executar porque elas podem afetar todo o sistema. Estas ações não estão associadas a qualquer privilégio.
  - Adicionar, modificar e excluir macros.
  - Visualizar, adicionar, modificar e excluir níveis de ameaça.

- Criar eventos causa-efeito genéricos (sem uma entidade de origem específica).
- Configurar transferências de arquivos (usando a tarefa *Transferência de arquivos*).
- Definir as configurações gerais a partir da tarefa *Controle de acesso* (motivos de solicitação de cartão, formato de cartão personalizado e assim por diante).
- Executar a *Ferramenta de importação*.
- Executar a *Ferramenta de Coleta de Dados de Diagnóstico*.

Exceções de privilégios para partições

Um usuário (ou grupo de usuários) tem um conjunto de *privilégios básicos* que é o resultado dos privilégios herdados de seus grupos de usuários pai, mais os explicitamente permitidos ou negados ao usuário.

Quando um usuário recebe acesso a uma partição, seus privilégios básicos são aplicados por padrão à partição. Enquanto administrador do sistema, você pode sobrescrever os privilégios que um usuário tem sobre uma partição específica. Por exemplo, um usuário pode ter permissão para configurar *alarmes* na partição A, mas não na partição B. Isso significa que um usuário pode ter um conjunto diferente de privilégios para cada partição a que tiver acesso. Somente os privilégios *Administrativo* e *Ação*, mais os privilégios sobre *tarefas públicas*, podem ser sobrescritos no nível de partição.

Modelos de privilégios

Modelos de privilégios são configurações de privilégios predefinidas, com base em perfis de segurança padrão, que você pode aplicar a usuários e grupos de usuários para simplificar o processo de criação. Uma vez aplicados, você pode ajustar os privilégios manualmente.

Você não pode renomear, modificar, criar ou excluir modelos de privilégios, mas pode aplicá-los a qualquer momento. Você pode modificar livremente as configurações de privilégios após um modelo de privilégio ser aplicado a um usuário ou grupo de usuários.

MELHOR PRÁTICA: Crie um grupo de usuários para cada modelo de privilégio, se necessário. Depois que seus grupos de usuários de modelo são criados, os usuários podem herdar privilégios deles.

Tipos de modelos de privilégios

O Security Center fornece os seguintes modelos de privilégios:

- **Geração de relatórios:** Este modelo só concede privilégios para executar o Security Desk e para executar as tarefas de relatório mais básicas, excluindo as do AutoVu™ LPR. Um usuário com apenas esse conjunto de privilégios não pode visualizar nenhum vídeo, controlar dispositivos físicos ou relatar incidentes.
- **Operador:** Este modelo é para operadores de segurança que precisam monitorar eventos em tempo real no sistema. Concede os privilégios de usar a tarefa Monitoração, visualizar vídeo, gerenciar visitantes, credenciais e modelos de crachá, adicionar marcadores e incidentes, salvar instantâneos, destrancar portas e assim por diante.
- **Investigador:** Este modelo é para os investigadores. Concede os privilégios de usar a tarefa Monitoração, visualizar vídeo, controlar câmeras PTZ, gravar e exportar vídeo, adicionar marcadores e incidentes, usar tarefas de investigação, gerenciar alarmes e visitantes, sobrepor os agendamentos de destrancar portas, salvar tarefas e assim por diante.
- **Supervisor:** Este modelo é para pessoas que têm responsabilidades de supervisão. Ele concede os mesmos privilégios do modelo *Investigador*, mais os privilégios de usar tarefas de manutenção, gerenciar titulares de cartão e credenciais, modificar campos personalizados, definir níveis de ameaça, bloquear câmeras e realizar contagem de pessoas.
- **Provisionamento:** Este modelo é para o instalador do sistema. Ele concede quase todos os privilégios de configuração, com apenas algumas exceções (gerenciamento de papéis, macros, usuários, grupos de usuários, eventos personalizados, trilhas de atividade, níveis de ameaça e arquivos de áudio).
- **Operador do Basic AutoVu™:** Este modelo é para operadores de segurança que usam o AutoVu™ LPR. Ele concede privilégios para usar tarefas LPR, configurar entidades LPR, criar regras LPR, monitorar eventos LPR e assim por diante.
- **Usuário do Patroller:** Este modelo é para usuários Genetec Patroller™.

Atribuir privilégios a usuários

Você deve conceder privilégios aos usuários para que eles façam alguma coisa no Security Center, incluindo logon, usar o Security Desk e assim por diante.

O que você deve saber

Os usuários têm um conjunto de privilégios básicos, que são privilégios concedidos explicitamente a eles ou herdados de seus grupos de usuários pai, além de um conjunto de privilégios para cada partição para a qual eles são usuários autorizados. Os privilégios concedidos ou negados no nível de partição substituem os privilégios básicos.

Você pode conceder privilégios específicos a usuários individuais ou permitir que os usuários herdem privilégios de seus grupos de usuários pai.

Para atribuir privilégios a um usuário:

1 Na página inicial Config Tool, abra a tarefa *Gerenciamento de usuários*.

2 Selecione o usuário a configurar e clique na aba **Privilégios**.

3 Usa uma das configurações de privilégios predefinidas como ponto de partida.

Na parte inferior da página, clique em (⚙) e selecione uma das seguintes opções:

- **Aplicar modelo:** Selecione um dos modelos de privilégios para aplicar.

  Os modelos de privilégios podem ser combinados. Isto significa que, quando aplica um modelo de privilégio, você sempre adiciona privilégios. Os privilégios existentes nunca poderão ser removidos como resultado da aplicação de um modelo de privilégio. Para começar do zero, vá até ao topo da hierarquia de privilégios (**Todos os privilégios**) e clique em **Indefinido**.

- **Definir configuração para apenas leitura:** Defina todos os privilégios de configuração de entidade encontrados no grupo de *Privilégios administrativos* para *Visualizar propriedades* com *Modificar propriedades* negado.

- **Definir configuração para leitura e gravação:** Define todos os privilégios de configuração de entidade encontrados no grupo de *Privilégios administrativos* para *Visualizar*, *Modificar*, *Adicionar* e *Excluir*.

4 Ajuste os privilégios de usuário alterando as configurações de privilégios individuais, se necessário.

Observe que, se o seu usuário tiver um grupo de usuários pai, as regras de herança de privilégios são aplicáveis.

- **Permitir:** Conceder o privilégio ao usuário. Você não pode selecionar esta opção se o privilégio for negado ao grupo de usuários pai.
- **Negar:** Negar o privilégio ao usuário.
- **Indefinido:** Herdar este privilégio do grupo de usuários pai. Se não existir um grupo de usuários pai, este privilégio é negado.

5 Se necessário, configure as exceções de privilégios para cada partição à qual o usuário tenha acesso.

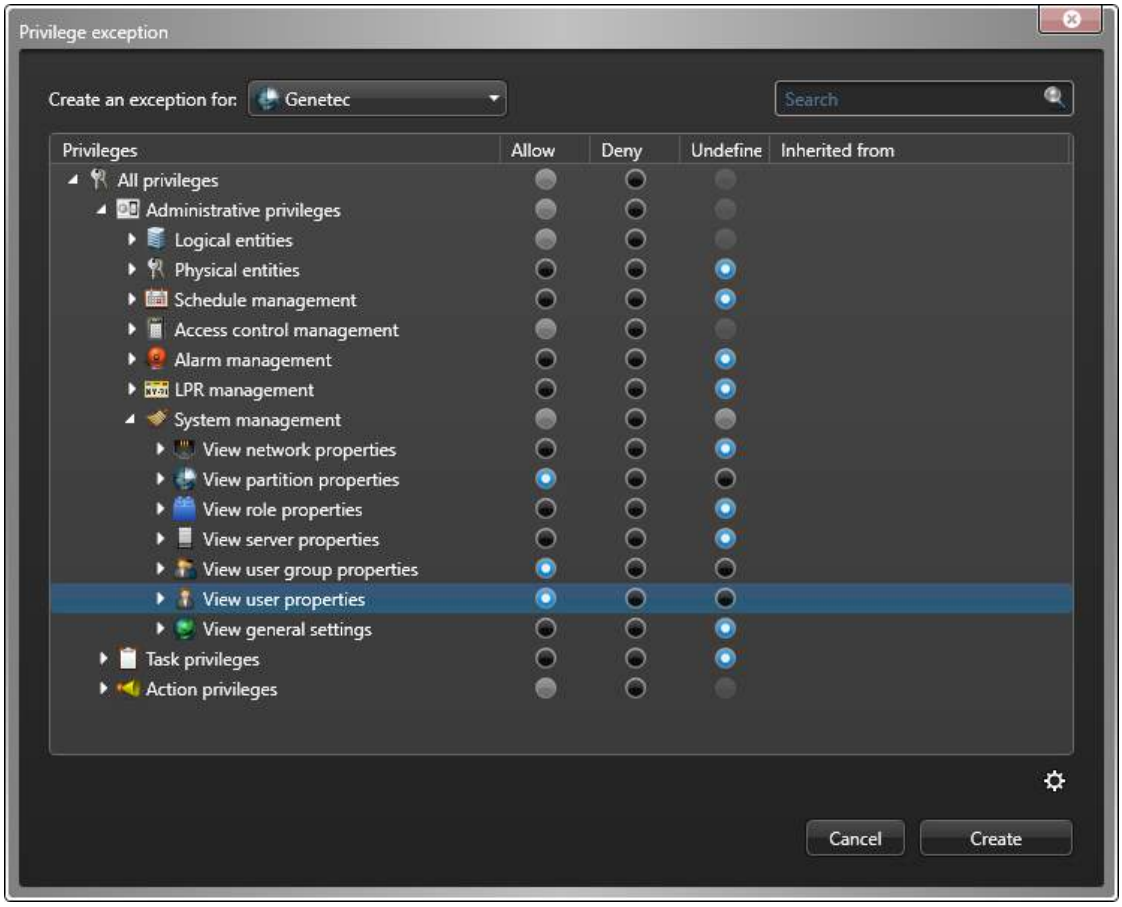
Quando um usuário recebe acesso a uma partição, seus privilégios básicos são aplicados por padrão à partição. Enquanto administrador do sistema, você pode sobrescrever os privilégios que um usuário tem sobre uma partição específica. Por exemplo, um usuário pode ter permissão para configurar *alarmes* na partição A, mas não na partição B. Isso significa que um usuário pode ter um conjunto diferente de privilégios para cada partição a que tiver acesso. Somente os privilégios *Administrativo* e *Ação*, mais os privilégios sobre *tarefas públicas*, podem ser sobrescritos no nível de partição.

a) Na parte inferior da página, clique em **Exceções** (➕).

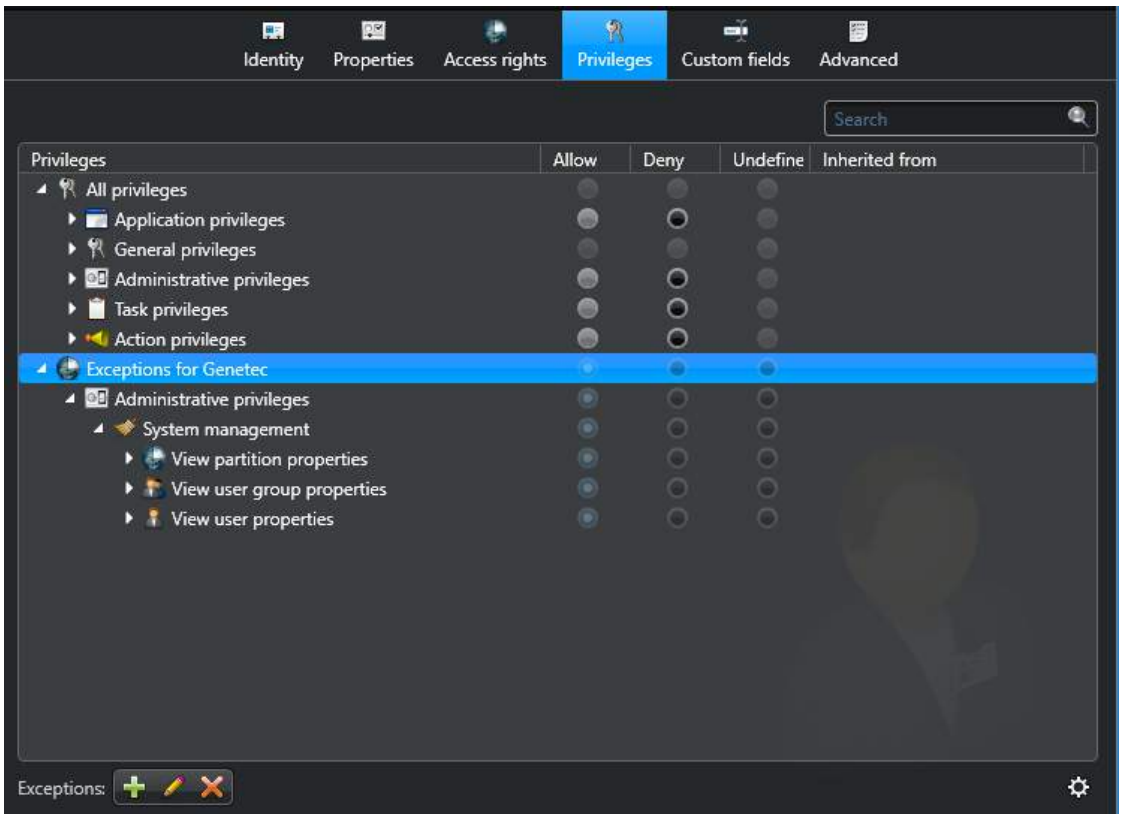
A caixa de diálogo *Exceção de privilégio* é aberta.

b) Na lista suspensa **Criar uma exceção para**, selecione uma partição.

c) Altere os privilégios básicos do usuário conforme necessário.



d) Clique em **Criar**.
As exceções de privilégios são adicionadas na parte inferior da lista de privilégios.



6 Clique em **Aplicar**.

Tópicos relacionados

Sobre privilégios na página 359
Modelos de privilégios na página 361

Personalizar opções de logon de usuário

Você pode selecionar como e quando os usuários podem fazer logon no Security Center.

O que você deve saber

As configurações se aplicam à estação de trabalho local e afetam o Security Desk e o Config Tool para todos os usuários. As alterações só entram em vigor na próxima vez em que um usuário iniciar o Security Desk ou o Config Tool.

NOTA: Se **Usar as credenciais do Windows** estiver definido como **Sempre** ou a opção **Forçar diretório a** estiver selecionada e um usuário ficar preso e não conseguir fazer logon, segure Ctrl+Shift e clique em **Fazer logon**. Isso permite que o usuário faça logon usando suas credenciais do Security Center ou força o campo **Diretório** a ser exibido.

Personalização de opções de logon de usuário

1 Na página inicial do Config Tool, clique em **Opções** > **Geral**.

2 Para forçar os usuários a fazer logon usando credenciais do Windows, configure a opção **Usar as credenciais do Windows** como **Sempre**.

Para que esta opção funcione, os usuários que devem fazer logon usando este computador devem ser importados de um *Active Directory*.

3 Para restringir o acesso de todos os usuários a um Directory específico, selecione a opção **Forçar diretório a** e digite o nome do Directory.

Com essa opção, os usuários não podem escolher o Directory ao qual desejam se conectar; o campo **Diretório** não é exibido na janela *Logon*. No entanto, eles podem ser redirecionados automaticamente para outro Directory quando o balanceamento de carga é usado.

NOTA: Se houver um erro no nome do Directory (por exemplo, um erro de digitação), a próxima vez que os usuários tentarem fazer logon, eles não poderão se conectar.

4 Para ignorar o balanceamento de carga do Directory, selecione a opção **Evitar o redirecionamento da conexão para servidores de diretórios diferentes**.

Os usuários se conectarão ao Directory padrão ou ao Directory que especificarem ao fazer logon e não serão redirecionados automaticamente para outro servidor. Esta opção só é significativa se o *balanceamento de carga* do Directory estiver configurado.

5 Clique em **Salvar**.

6 Para limitar o número de estações de trabalho nas quais um usuário pode fazer logon ao mesmo tempo, faça o seguinte:

a) Abra a tarefa de **Gerenciamento de usuários**.

b) Selecione o usuário que deseja configurar e clique na aba **Avançado**.

c) Coloque a opção **Limitar logons simultâneos** em **Ligado** e selecione o número de estações de trabalho.

7 Para selecionar quando um usuário pode fazer logon, clique em **Adicionar um item** () na seção **Agenda de logon do usuário**.

8 Selecione agendas predefinidas e clique em **Selecionar**.

Se você selecionar vários agendamentos, as regras de conflito de agendamento se aplicarão. Quando dois agendamentos com o mesmo nível de prioridade se sobrepõem, o agendamento de bloqueio tem prioridade sobre o agendamento de permissão.

9 Para bloquear a sessão de um usuário após um período de inatividade, coloque a opção **Bloqueio automático** em **Ligado** e selecione quanto tempo a sessão deve permanecer inativa antes da desconexão.

Esta opção se aplica apenas a ao Security Desk. Antes de ser bloqueado, a mensagem `Sessão prestes a ser bloqueada` é exibida para o usuário. Depois do aplicativo ser bloqueado o usuário deve fazer logon de novo para retomar a sessão atual.

NOTA: Se o usuário for autenticado através de ADFS com autenticação passiva, o usuário será desconectado e a sua sessão atual fechada ao invés de ficar bloqueada.

10 Clique em **Aplicar**.

11 Para exigir que o usuário faça logon no Security Center com um supervisor de logon, na tarefa **Gerenciamento de usuários**, selecione o usuário que será o supervisor e clique na aba **Avançado**.

12 Na seção **Supervisor de logon de**, clique em **Adicionar um item** (), selecione o usuário a ser supervisionado e clique em **OK**.

13 Clique em **Aplicar**.

Tópicos relacionados

Importar grupos de segurança de um Active Directory na página 389
Fazer logon no Security Center através do Config Tool na página 7

Forçando o Security Desk a ser executado no modo de tela cheia

Se o trabalho de um usuário for se concentrar no monitoramento de vídeo ao vivo, você poderá forçar o Security Desk a ser executado em modo de tela cheia para impedir que o usuário passe para o modo do Windows.

O que você deve saber

Você também pode definir o Security Desk para iniciar no modo de tela cheia em uma estação de trabalho específica.

Para forçar o Security Desk a ser executado no modo de tela cheia para um usuário:

1. Na página inicial Config Tool, abra a tarefa *Gerenciamento de usuários*.
2. Selecione um usuário e clique na aba **Privilégios**.
3. Expanda **Privilégios de aplicativo** e os privilégios do **Security Desk**.
4. Negue o privilégio **Alterar visualizações de cliente** para aquele usuário.
5. Clique em **Aplicar**.

O Security Desk passará a ser executado sempre em tela cheia para aquele usuário. O comando *Restaurar* e a tecla **F11** (alternar entre tela cheia e modo em janela) ficam desabilitados.

Configurar o Security Desk para iniciar no modo de tela cheia em estações de trabalho

Se uma estação de trabalho for usada principalmente para monitorar vídeo ao vivo, você pode configurar o Security Desk para iniciar sempre no modo de tela cheia naquela estação de trabalho.

O que você deve saber

Configurar o Security Desk para iniciar no modo de tela cheia não impede que o usuário minimize a janela do Security Desk com Alt+ESC ou alterne para outro aplicativo com Alt+TAB.

Para definir o Security Desk para iniciar no modo de tela cheia em uma estação de trabalho:

1. Na estação de trabalho, abra a caixa de diálogo **Propriedades do Security Desk**.
2. Selecione a aba **Atalho** e adicione a opção `/forcefullscreen` (ou `/ff`) no final da cadeia de caracteres em **Destino**.

3 Clique em **Aplicar**.

Da próxima vez que um usuário iniciar o Security Desk usando o atalho, o aplicativo será iniciado em modo de tela cheia. Os comandos *Restaurar* e a tecla F11 (alternar entre tela cheia e modo em janela) ficam desabilitados.

Selecionar quais estações de trabalho os usuários podem controlar remotamente

Você pode selecionar quais estações de trabalho e monitores do Security Desk um usuário tem permissão para controlar remotamente usando um teclado CCTV ou com a tarefa *Remoto* no Security Desk.

O que você deve saber

A cada monitor controlado pelo Security Desk é atribuído um *ID de monitor* exclusivo (exibido na bandeja de notificação e encontrado na página *Configurações gerais - ID Lógico* na tarefa *Sistema*). Usando um teclado de CCTV, você pode exibir uma entidade em uma estação de trabalho remota do Security Desk especificando seu ID de monitor, *ID de ladrilho* e o *ID lógico* da entidade.

IMPORTANTE: Para além de ter os *direitos de controle remoto* sobre usuários e estações de trabalho do Security Desk, as seguintes condições devem também ser atendidas para que um usuário local possa conectar-se a uma estação de trabalho remota do Security Desk:

- Tanto o Security Desk local como o remoto devem estar em execução e conectados ao mesmo Directory do Security Center.
- O usuário local deve ter os mesmos ou mais privilégios de usuário do que o usuário conectado no Security Desk remoto.
- O usuário local deve ser membro de todas as partições das quais o usuário conectado no Security Desk remoto seja membro.

Para selecionar quais estações de trabalho um usuário pode controlar remotamente:

1. Na página inicial Config Tool, abra a tarefa *Gerenciamento de usuários*.
2. Selecione o usuário a configurar e clique na aba **Avançado**.
3. Na seção **Permitir controle remoto sobre**, clique em **Adicionar um item** ( ).
4. Na lista suspensa, selecionar um dos seguintes tipos de entidades:
   - **Usuário:** Qualquer estação de trabalho do Security Desk onde esse usuário esteja conectado pode ser controlada remotamente.
   - **Grupo de usuários:** Qualquer estação de trabalho do Security Desk onde um membro desse grupo de usuários esteja conectado pode ser controlada remotamente.
   - **Aplicativo:** A estação de trabalho especificada (*COMPUTER - SecurityDesk*) pode ser controlada remotamente independentemente de quem está conectado.
5. Selecione as entidades associadas e clique em **OK** > **Aplicar**.

Selecionar quais atividades de usuários registrar

Você pode selecionar quais tipos de atividades relacionadas ao usuário são registradas no banco de dados e disponibilizadas para relatórios na tarefa *Trilhas de atividades*.

O que você deve saber

As atividades que você pode registrar são eventos gerados por usuários que se conectaram ao Security Center.

Para selecionar quais atividades monitorar:

1 Na página inicial do Config Tool, abra a tarefa **Sistema**.
2 Clique na visualização **Configurações gerais** e, em seguida, clique na página **Trilhas de atividades**.
3 Na lista, selecione os eventos a serem monitorados.

   Você pode selecionar eventos gerais, ou eventos especificamente relacionados ao vídeo, controle de acesso ou LPR.

4 Clique em **Aplicar**.

Agora, você pode procurar eventos no seu sistema que foram disparados pelos usuários, usando a tarefa Trilhas de atividades.

Tópicos relacionados

Tipos de evento na página 1101
Investigar atividades relacionadas a usuários no seu sistema Security Center na página 319

19

TLS e Autenticação no Directory

Esta seção inclui os seguintes tópicos:

- "O que é o protocolo Transport Layer Security?" na página 372
- "O que é a autenticação do diretório?" na página 373
- "Alterar a configuração de autenticação no Directory" na página 376
- "Desabilitar compatibilidade com versões anteriores" na página 377
- "Substituir certificados padrão" na página 378
- "Criar solicitações de certificados personalizadas para o Security Center" na página 379

O que é o protocolo Transport Layer Security?

Transport Layer Security (TLS) é um protocolo que fornece privacidade de comunicações e integridade de dados entre dois aplicativos que se comunicam através de uma rede. Quando um servidor e um cliente se comunicam, o TLS garante que nenhum terceiro possa interceptar ou modificar nenhuma mensagem. TLS é o sucessor do Secure Sockets Layer (SSL).

O que você deve saber

A partir do Security Center 5.4, o TLS é utilizado para conexões ao Directory a partir de estações de trabalho clientes e servidores de expansão. Com o TLS, você tem a opção de forçar a Autenticação no Directory em estações de trabalho clientes e servidores durante a instalação do software.

Quais são os benefícios do TLS?

O TLS oferece inúmeros benefícios aos clientes e servidores em relação a outros métodos de autenticação, incluindo:

- **Autenticação forte:** Autentica o Directory para aplicativos cliente, provando a identidade do servidor antes de se conectar a ele. Protege contra ataques *man-in-the-middle*.
- **Integridade dos dados:** Todos os dados são transmitidos com um valor de verificação de integridade.
- **Privacidade de mensagens:** Protege contra espionagem.

  NOTA: O potencial de tais ameaças está presente somente se você permitir conexões da WAN (ao contrário de através de uma VPN segura) ou quando sua rede corporativa estiver fisicamente comprometida.
- **Flexibilidade do algoritmo:** Fornece opções para os mecanismos de autenticação, algoritmos de criptografia e algoritmos de hash que são usados durante a sessão segura.
- **Fácil de usar:** A maioria de suas operações são completamente invisíveis ao cliente. Isso permite que o cliente tenha pouco ou nenhum conhecimento da segurança das comunicações e ainda seja protegido contra invasores.

Limitações

- A proteção contra man-in-the-middle só é aplicada se você optar por ativar a Autenticação do Directory em cada máquina (Cliente ou Servidor).
- As máquinas que executam o Security Center 5.3 e anteriores e o Mobile Server 4.0 só podem se conectar ao Directory do Security Center 5.7 usando o protocolo de comunicação antigo.
- Certificados de cliente ainda não são suportados para o Config Tool e o Security Desk.

Compatibilidade retroativa

A compatibilidade com versões anteriores é ativada por padrão na instalação do sistema. Quando o Directory 5.7 recebe uma solicitação de conexão do Security Center 5.3 e anteriores, ele alterna automaticamente para o antigo protocolo de comunicação (menos robusto contra ataques de rede). Se a vulnerabilidade da rede for um problema para sua organização, você pode desativar a compatibilidade com versões anteriores e forçar todas as máquinas a serem atualizadas antes que elas possam se conectar ao seu sistema.

Tópicos relacionados

Servidor - Aba Propriedades na página 1029

O que é a autenticação do diretório?

A autenticação do Directory é uma opção do Security Center que força todas as aplicações do cliente e do servidor em determinada máquina a validar o certificado de identidade do Directory antes de se conectar a ele. Esta medida impede ataques man-in-the-middle.

Quando preciso de autenticação do Directory?

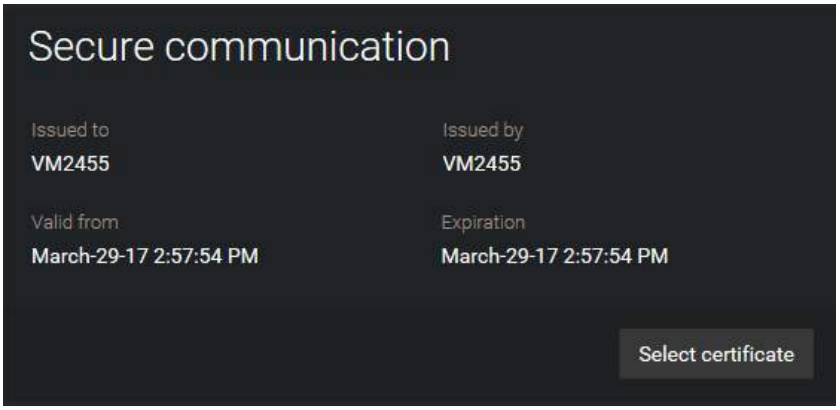
A finalidade da autenticação no Directory é proteger contra ataques *man-in-the-middle*. Se você não tiver aplicativos conectados ao seu sistema pela Internet (ou por qualquer rede não confiável), o potencial desse tipo de ataque é muito baixo. Nesse caso, você provavelmente está seguro sem ativar esta opção.

O que é um certificado de identidade?

Um certificado de identidade, também conhecido como *certificado digital* ou *certificado de chave pública*, é um documento digitalmente assinado que permite que um computador ou organização troquem informações de modo seguro em uma rede pública. O certificado inclui informações sobre a identidade do proprietário, a *chave pública* usada para criptografar futuras mensagens enviadas ao proprietário e a assinatura digital da autoridade de certificação (CA).

Como funciona

Ao instalar os componentes do servidor do Security Center, um *certificado auto-assinado*chamado *GenetecServer-{MachineName}* é automaticamente criado no Local Computer Certificate Store. Você pode ver o certificado atual na Server Admin, na seção *Comunicação segura com o servidor*.



Os certificados auto-assinados são usados para identificar os *servidores de expansão* para o *servidor principal* para que a senha usada para se conectar ao servidor principal não precise ser armazenada localmente nos servidores de expansão.

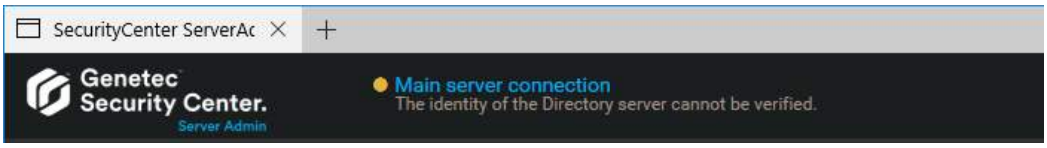
Autenticação no Directory está habilitada na instalação do Security Center quando você escolhe as configurações recomendadas de segurança ou selecionando **Sempre validar o certificado do Directory** ao escolher as configurações personalizadas de segurança. Para obter mais informações, consulte o *Guia de Instalação e Atualização do Security Center*.

MELHOR PRÁTICA: Se optar por ativar a autenticação do Directory, recomendamos que substitua o certificado autoassinado no servidor principal por um emitido por uma confiável *autoridade de certificação (CA — certificate authority)*. A CA pode ser interna ou de um terceiro. Isso permite que você implante um sistema altamente seguro sem forçar seus usuários a estar cientes do mecanismo subjacente.

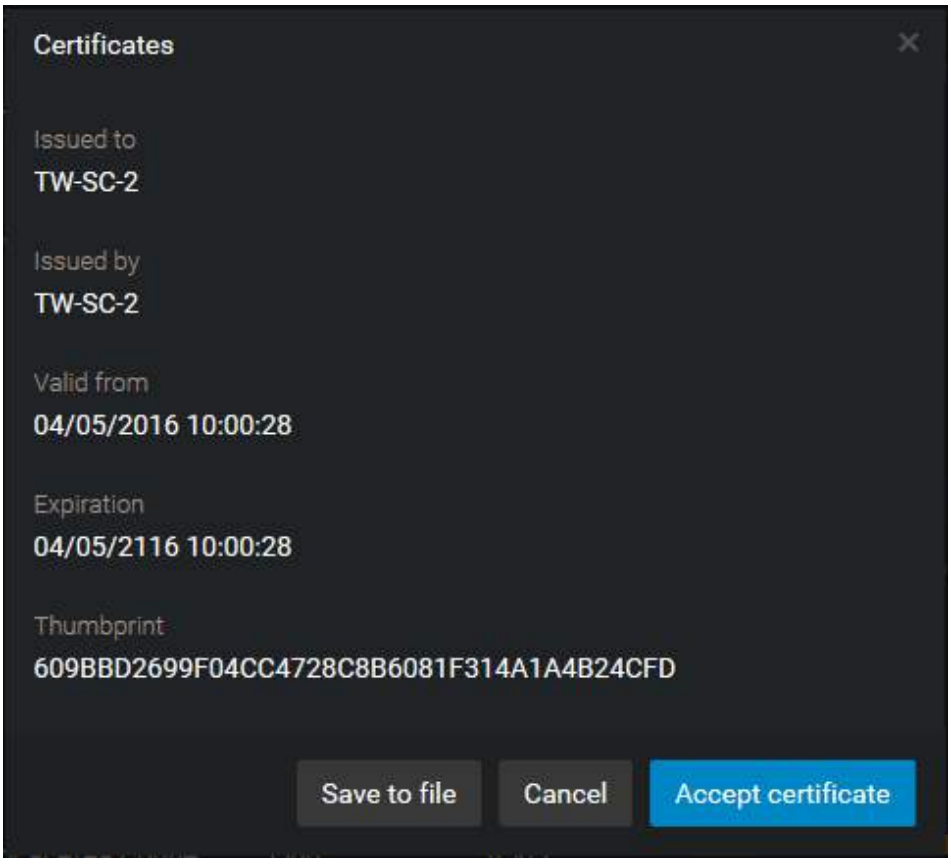
Se você optar por manter o certificado autoassinado no servidor principal, a primeira vez que uma estação de trabalho for usada para se conectar ao Directory, o usuário será solicitado a confirmar se o servidor do Directory pode ser confiável.

Uma vez que um usuário confirma que o servidor principal pode ser confiável, o certificado fica na lista de permissões, e a caixa de diálogo não aparecerá novamente.

A mesma confirmação é necessária nos servidores de expansão. Na primeira vez que você fizer logon no servidor de expansão com o Server Admin, você verá esta mensagem no painel.



Você deve clicar em **Conexão ao servidor principal** e então em **Aceitar certificado** na caixa de diálogo que aparecerá.



Depois que o servidor principal for confirmado, você poderá alterar a senha ou o certificado no servidor principal ou no servidor de expansão e nunca mais terá que confirmar sua confiança, desde que os dois servidores permaneçam conectados enquanto faz a alteração.

Exigências

Para que a autenticação do Directory funcione, as seguintes condições devem ser atendidas:

- O DNS deve ser configurado na rede. Servidores e estações de trabalho de cliente devem ser capazes de resolver o nome do servidor principal.
- O nome do servidor principal deve ser resolvido pelo DNS para o nome comum no certificado do Directory.
- As estações de trabalho do cliente e os servidores de expansão devem ser capazes de confiar no certificado fornecido pelo servidor principal. Caso contrário, uma intervenção do usuário é sempre necessária para aceitar o certificado na primeira vez que uma máquina é usada para se conectar ao servidor principal.

Como altero essa configuração após a instalação?

Para alterar a configuração de autenticação do Directory após a instalação do software, é necessário editar o arquivo *GeneralSettings.gconfig* em cada computador onde você queira a alteração.

Alterar a configuração de autenticação no Directory

Você pode optar por ativar ou desativar a autenticação no Directory em cada computador, alterando a configuração da política do canal TLS em seus respectivos arquivos *GeneralSettings.gconfig*.

O que você deve saber

Autenticação no Directory está habilitada na instalação do Security Center quando você escolhe as configurações recomendadas de segurança ou selecionando **Sempre validar o certificado do Directory** ao escolher as configurações personalizadas de segurança. Para obter mais informações, consulte o *Guia de Instalação e Atualização do Security Center*.

Depois que o Security Center esteja instalado, se você quiser alterar essa configuração, será necessário editar o arquivo *GeneralSettings.gconfig* em cada computador.

Para alterar a configuração de autenticação do Directory após a instalação do software:

1. Abra o arquivo *GeneralSettings.gconfig* na pasta de configuração com um editor de texto.

   A pasta de configuração encontra-se na pasta de instalação do Security Center (padrão = *C:\Program Files (x86)\Genetec Security Center 5.7*\ConfigurationFiles).
2. Edite a marca `<tlsChannel policy="value">`.

   Altere o valor para `"AllowAll"` para desativar a autenticação no Directory ou para `"TrustedOnly"` para ativá-la.
3. Salve suas alterações e reinicie o serviço *Genetec Server*.

Desabilitar compatibilidade com versões anteriores

Versões anteriores do Security Center (anteriores a 5.4) não suportam o protocolo *Transport Layer Security (TLS)* . Portanto, apoiá-los torna seu sistema mais vulnerável a ataques de rede. Para aumentar a segurança do seu sistema, você deve desativar a compatibilidade com versões anteriores.

O que você deve saber

A compatibilidade com versões anteriores é ativada por padrão na instalação do sistema. Esta opção aplica-se a todo o sistema.

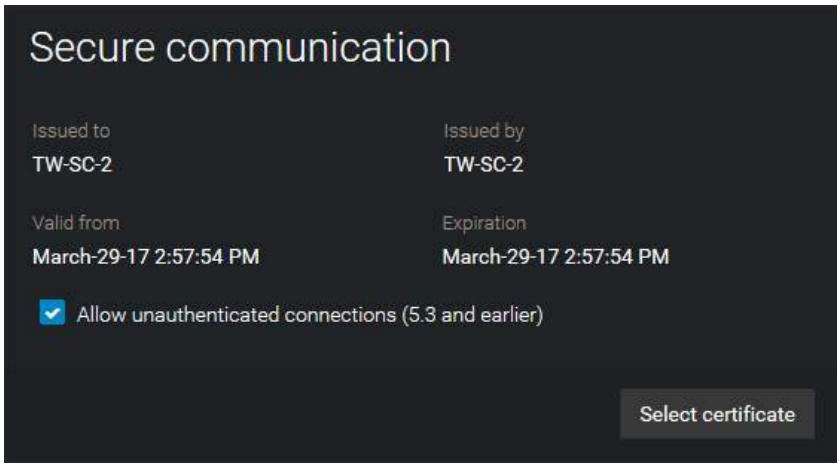
CUIDADO: O Mobile Server 4.0 não suporta TLS. A desativação da compatibilidade com versões anteriores significa que os aplicativos para dispositivos móveis e os Web Clients 4.0 não poderão mais se conectar ao Security Center. Todos os servidores de expansão que ainda não foram atualizados para a versão 5.4 ou posterior também pararão de funcionar. Tanto o Web Client 4.1 como o Web Client 5.6 baseado em funções e posteriores suportam TLS.

Para desabilitar a compatibilidade com versões anteriores:

1 Conecte-se ao Server Admin de seu servidor principal com um navegador da Web.

2 Clique no servidor principal ( ) na lista de servidores.

3 Em *Comunicação segura*, desmarque a opção **Permitir conexões não autenticadas (5.3 e anteriores)**.



4 Clique em **Salvar**.

IMPORTANTE: Na próxima vez que alguém tentar se conectar ao seu sistema com uma aplicação do Security Center mais antiga, aparecerá o erro *As versões cliente-servidor são incompatíveis*.

Substituir certificados padrão

Para substituir o *certificado auto-assinado* em um servidor por um certificado de uma origem confiável, é necessário importar o novo certificado para o Local Computer Certificate Store do seu servidor antes de poder selecioná-lo no Server Admin.

Antes de iniciar

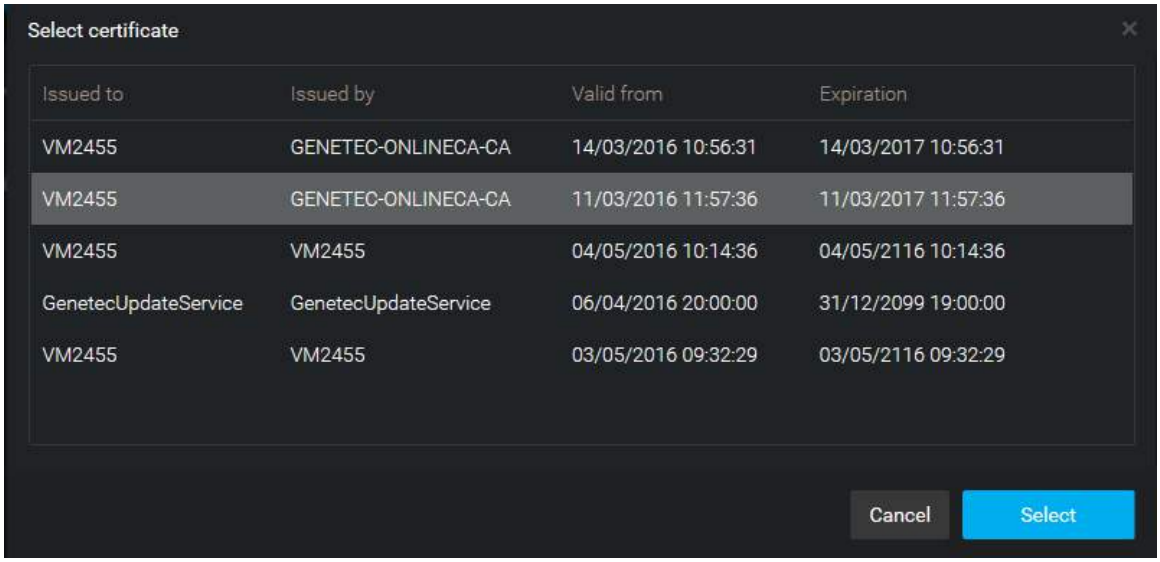
Siga o procedimento da sua empresa quanto à inscrição de certificados. Se sua situação requer que você crie uma solicitação personalizada, certifique-se de seguir as recomendações exigidas para o Security Center.

O que você deve saber

Para melhorar a segurança do seu sistema, você só precisa substituir o certificado auto-ssinado no servidor principal (ou em todos os servidores do Directory, se você tiver o failover do Directory configurado). Não é necessário alterar o certificado em todos os servidores de expansão.

Para importar um certificado confiável para o Local Computer Certificate Store do seu servidor principal:

1. No seu servidor principal, inicie o Microsoft Management Console (mmc.exe).
2. Na janela *Console*, expanda **Certificados**.
3. Em **Certificados (Computador local)**, clique com o botão direito em **Pessoal** e clique em**Todas as tarefas** > **Importar**.
4. Siga as instruções no *Assistente de importação de certificado* para importar o certificado.
5. Abra o Server Admin no seu servidor.
6. Clique na aba **Genetec Server**.
7. Em *Comunicação segura*, clique em **Selecionar certificado**.
8. Na caixa de diálogo que abrir, selecione o novo certificado que você importou e clique em **Selecionar**.



NOTA: Se o certificado selecionado não for válido (sem usar a chave Legacy por exemplo), uma mensagem de erro será exibida e você não poderá aplicá-lo.

9. Clique em **Salvar** e reinicie o serviço do Genetec™ Server.

Criar solicitações de certificados personalizadas para o Security Center

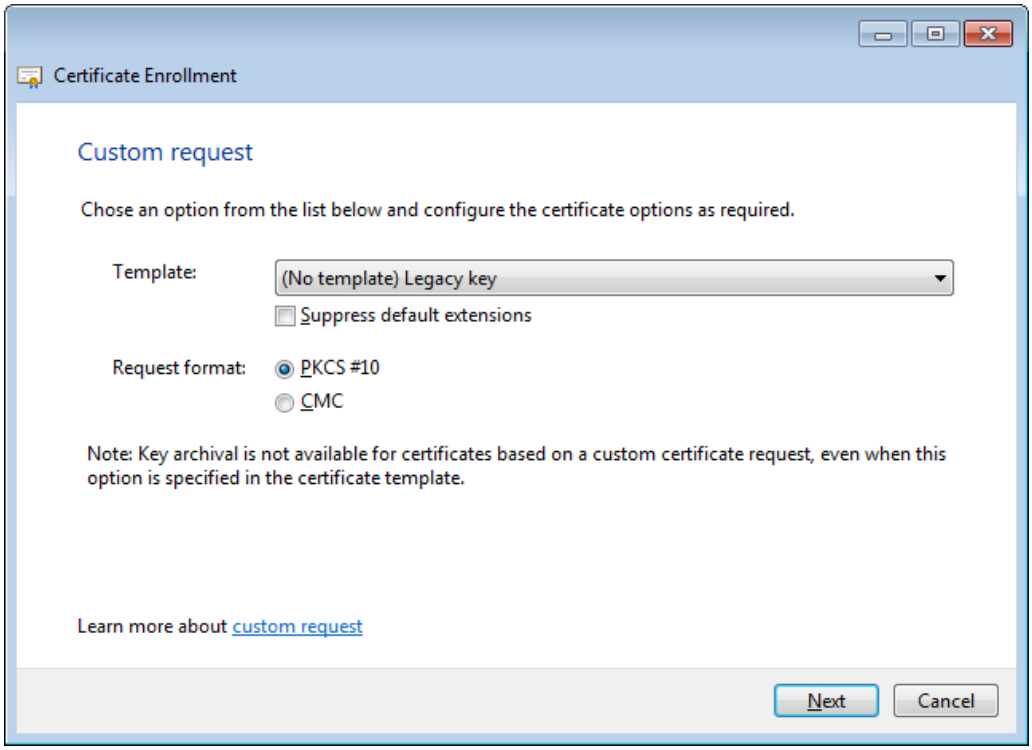
Solicitações de certificados personalizadas devem ser criadas com parâmetros específicos para funcionar com o Security Center. Todas as solicitações de certificado devem ser feitas a partir do servidor em que o certificado será aplicado.

O que você deve saber

A criação de solicitações de certificado personalizadas deve ser o último recurso. Existem muitas alternativas mais simples para solicitar um certificado para o servidor. Por exemplo, você pode registrar um certificado de um modelo de certificado do domínio Active Directory da sua empresa. Para obter mais informações, consulte Solicitar certificados usando o Assistente de Solicitação de Certificados na biblioteca Technet da Microsoft.

Para criar uma solicitação de certificado personalizada para o Security Center:

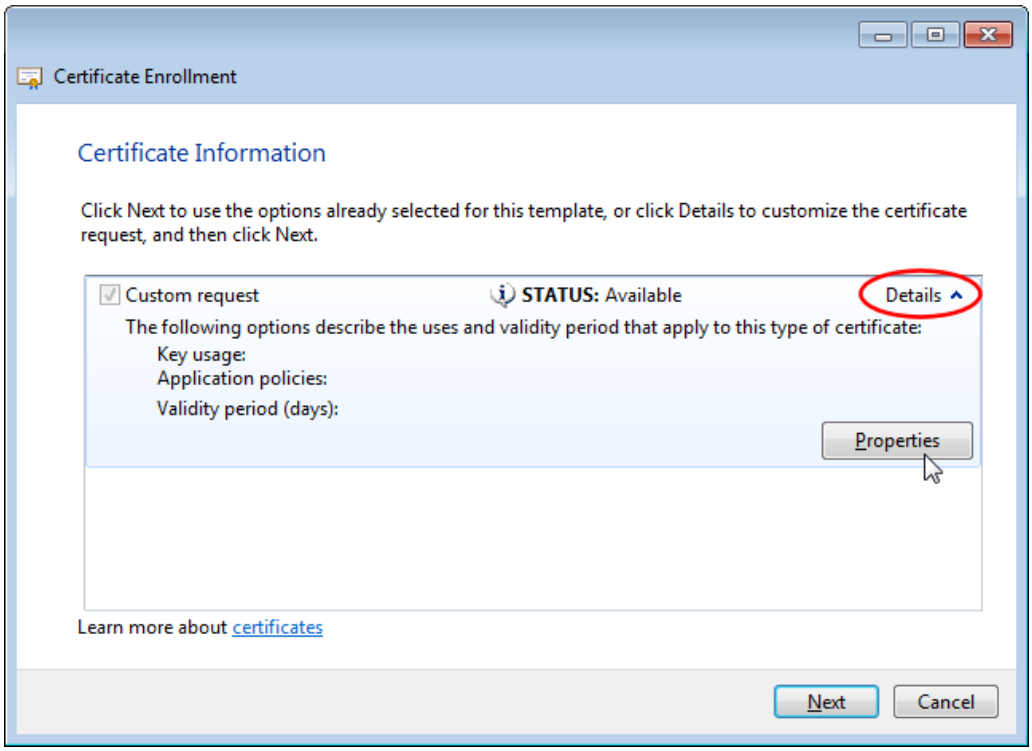
1 No seu servidor principal, inicie o Microsoft Management Console (mmc.exe) e adicione o snap-in Certificados.
   a) Na janela *Console*, clique em **Arquivo** > **Adicionar/Remover Snap-in**.
   b) Na caixa de diálogo *Adicionar ou remover snap-ins* que aparecerá, clique em **Certificados** e, em seguida, clique em **Adicionar >**.
   c) Na caixa de diálogo *Snap-in Certificados*, clique em **Conta do computador** > **Próximo** > **Concluir** > **OK**.
2 Na janela *Console*, expanda **Certificados**.
3 Em **Certificados (Computador local)**, clique com o botão direito em **Pessoal** e, em seguida, clique em **Todas as tarefas** > **Operações avançadas** > **Criar solicitação pessoal**.
4 Na caixa de diálogo *Registro de certificados*, clique em **Próximo** > **Continuar sem política de registro** > **Próximo**.
5 Na página *Solicitação personalizada*, selecione as opções conforme mostrado abaixo.



IMPORTANTE: Para **Modelo**, selecione **Chave herdade**. A opção padrão, **Chave CNG**, não é suportada pelo .NET Framework 4.5, que é usado pelo Security Center.

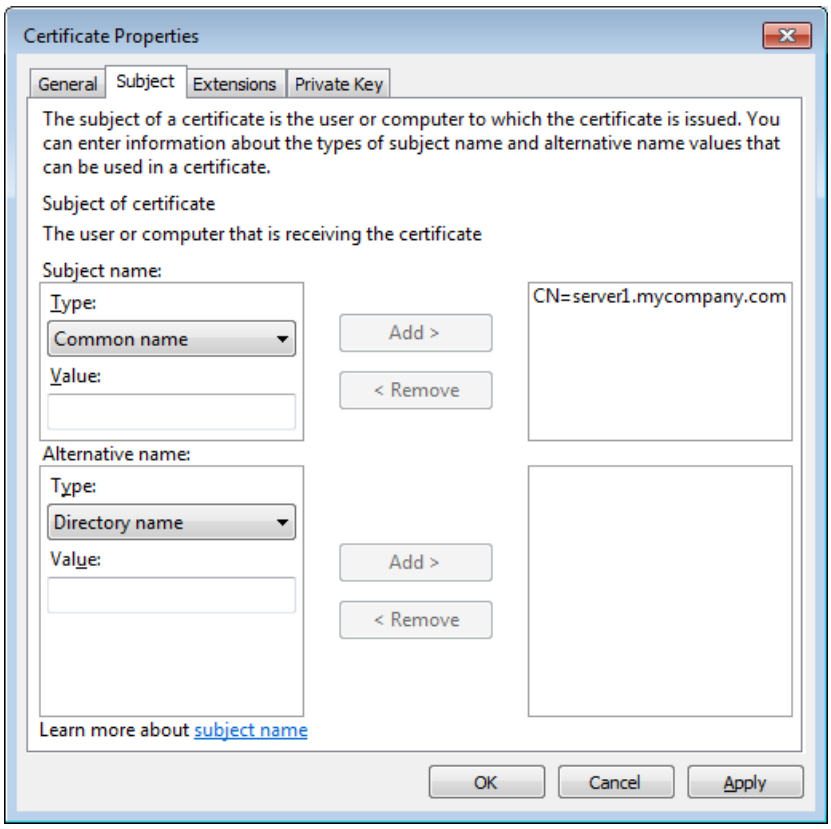
6 Clique em **Próximo**

7 Na página *Informações do certificado*, expanda **Detalhes** e clique em **Propriedades**.



8 Na caixa de diálogo *Propriedades do certificado*, clique na aba **Entidade** e digite o valor de **Nome comum** em **Nome da entidade**.

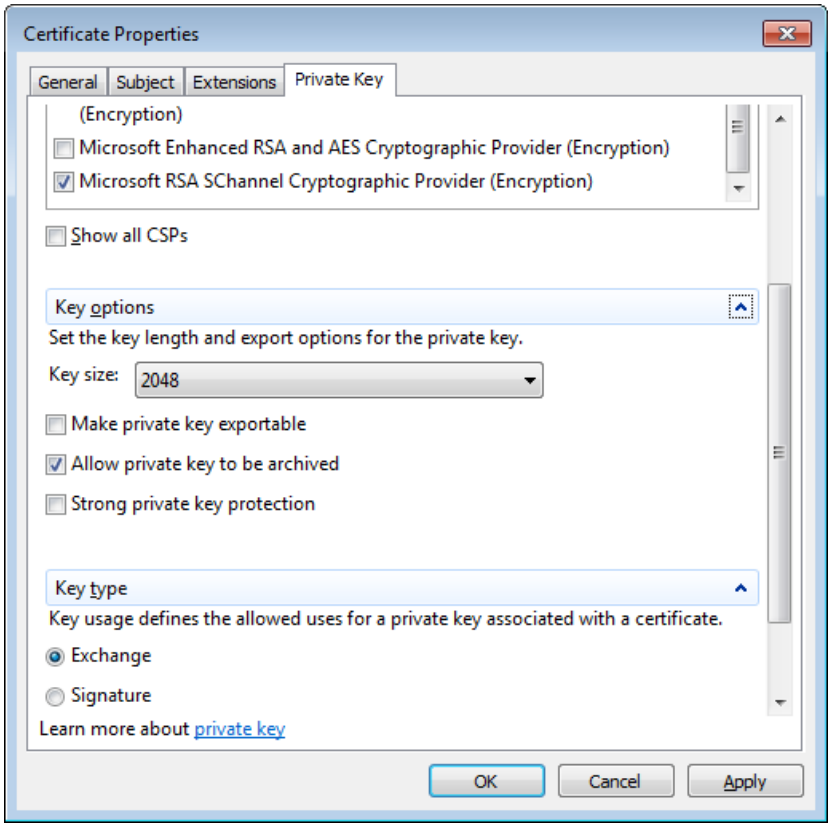
IMPORTANTE: O **Nome comum** deve corresponder ao nome de domínio completamente qualificado do servidor. Por exemplo, se o nome de host do seu servidor for *server1* e o seu domínio for *mycompany.com*, o nome de domínio completamente qualificado para o seu servidor será *server1.mycompany.com*.



9 Clique na aba **Extensões** e configure as propriedades a seguir.

- **Uso de chaves:** Adicione **Assinatura digital** e **Acordo de chaves**.
- **Uso de chave ampliado:** Adicione **Autenticação do servidor** e **Autenticação do cliente**.

10 Clique na aba **Chave privada** e configure as propriedades a seguir.



- **Tipo de chave:** Selecione **Trocar**. Isso deve ser configurado primeiro.
- **Provedor de Serviço de Criptografia:** Selecione somente **Provedor de Criptografia Microsoft RSA SChannel (Criptografia)**. É a última opção da lista.
- **Opções de chave:** O **Tamanho da chave** deve ser pelo menos 2048.

11 Clique em **Aplicar** > **OK** > **Próximo**.

12 Digite o **Nome do arquivo** e clique em **Concluir**.

Após terminar

Envie a solicitação (.csr) para o seu departamento de TI ou para a autoridade certificadora externa*autoridade de certificação* para processamento. Uma vez que o certificado tenha sido gerado, importe-o e aplique-o ao seu servidor.

20

Integração do Active Directory

Esta seção inclui os seguintes tópicos:

- "Integração com o Active Directory do Windows" na página 384
- "Sincronização do Active Directory" na página 386
- "Sobre grupos Universais e catálogos globais" na página 388
- "Importar grupos de segurança de um Active Directory" na página 389
- "Mapear campos personalizados para sincronizar com o Active Directory" na página 392
- "Resolver conflitos causados por entidades importadas" na página 393
- "Desativar usuários importados de um Active Directory" na página 394
- "Atributos de catálogo global" na página 395

Integração com o Active Directory do Windows

A integração de um Active Directory (AD) do Windows no Security Center permite gerenciar todas as informações de segurança e de pessoal em um único local, seja para segurança lógica (TI) ou para segurança física (controle de acesso a locais físicos).

Com a integração do AD, você pode importar grupos de segurança de um AD para o Security Center como grupos de usuários, grupos de titulares de cartão ou ambos. Os membros podem ser importados como usuários ou portadores de cartão. Ambos os atributos padrão e personalizados podem ser importados do AD. A maioria dos campos importados só podem ser modificados dentro do AD e são somente leitura no Security Center.

Você pode importar entidades de mais de um AD, se necessário. Por exemplo, a partir do Security Center, é possível gerenciar o acesso a um recurso compartilhado por várias empresas, como um prédio de escritórios. Como administrador do sistema, você pode importar usuários e/ou titulares de cartão de seus Active Directories individuais e gerenciá-los em partições separadas.

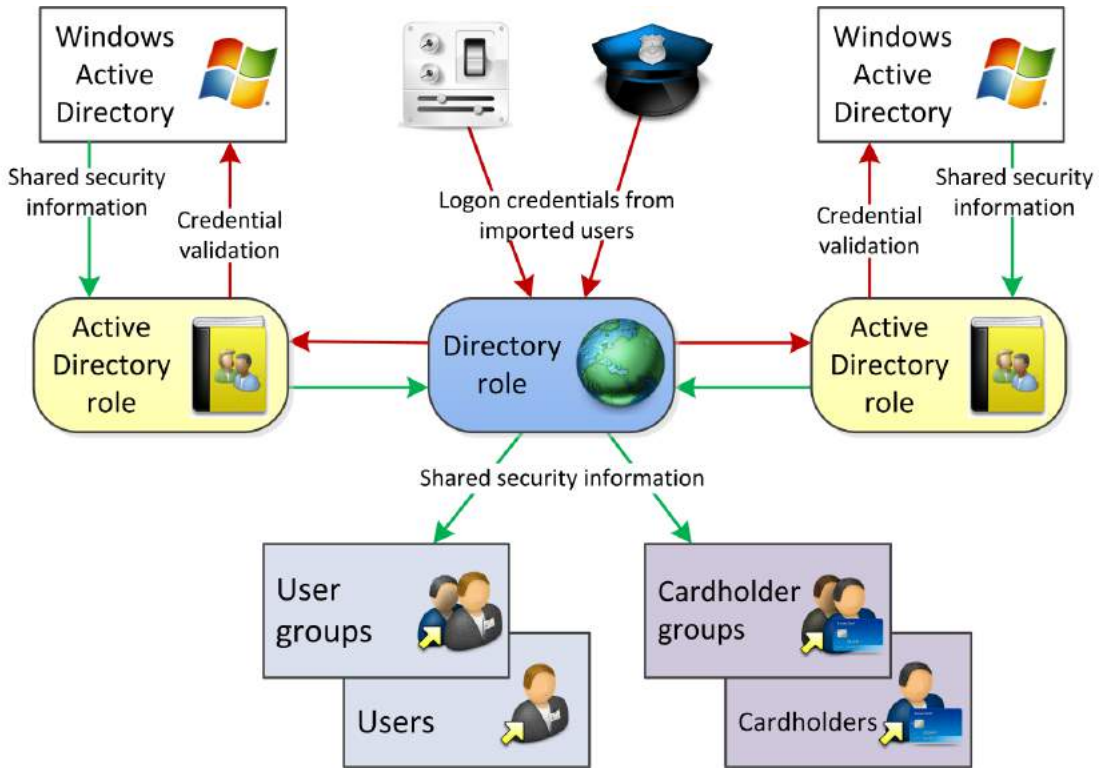
Para configurações de AD maiores que tenham muitos domínios que façam parte de uma floresta de AD, o Security Center oferece suporte à sincronização de grupos universais e à conexão a um catálogo global. Uma só função *Active Directory* pode ser usada para sincronizar um grupo universal. Para obter mais informações sobre como usar grupos universais e catálogos globais com o Security Center, consulte Sobre grupos universais e catálogos globais.

NOTA: Certifique-se de que o servidor que esteja executando a função Active Directory faça parte do domínio que você está tentando sincronizar.

Como a integração do AD funciona

Para importar usuários e/ou titulares de cartão de um AD, você deve criar uma função *Active Directory* para o AD que deseja importar. A função Active Directory conecta o sistema Security Center a um servidor do Active Directory e importa usuários e/ou titulares de cartão de grupos de segurança selecionados. As entidades importadas são identificadas no Security Center por uma seta amarela ( ) sobreposta ao habitual ícone de entidade.

A função Active Directory sincroniza todas as alterações feitas no AD com as entidades importadas no Security Center. Ela também envia as credenciais de logon de usuários importadas para o serviço do AD para validação.



Benefícios da integração do AD

Ter um sistema centralizado de gerenciamento de informações de segurança oferece muitos benefícios:

- Menos entradas de dados significam menos erros e melhor controle durante a configuração inicial do Security Center, pois os usuários e os titulares de cartão podem ser importados de um AD existente.
- Consistência e melhor segurança porque todas as informações compartilhadas são inseridas apenas uma vez.
  - Uma nova conta de usuário adicionada a um grupo de segurança importado adiciona automaticamente um novo usuário e/ou titular de cartão no Security Center.
  - Uma conta de usuário que está desabilitada no AD desativa automaticamente o usuário e/ou titular de cartão correspondente no Security Center.
- Capacidade de logon único para usuários sincronizados do Security Center. Os usuários conectados ao Windows não precisam fazer logon no Security Center.

Sincronização do Active Directory

Através de um processo chamado de *sincronização*, a função *Active Directory* também mantém todas as entidades importadas atualizadas com as alterações feitas no AD.

Todas as entidades importadas são sincronizadas com sua origem pela função Active Directory. A maioria dos atributos importados do AD são somente leitura no Security Center, exceto algumas propriedades de titular de cartão. As entidades importadas não podem ser excluídas a menos que sejam excluídas do AD.

CUIDADO: Se você mover uma conta de segurança de um grupo de segurança sincronizado do AD para um que não seja sincronizado, é como se a conta deixasse de existir no Security Center. A função Active Directory exclui as entidades correspondentes (usuários e/ou titulares de cartão) do Security Center na próxima sincronização com o AD.

A sincronização é sempre iniciada a partir do Security Center. Existem duas maneiras de iniciar a sincronização:

- **Manualmente:** A sincronização é executada quando você a solicita explicitamente. Esta é a configuração padrão. A vantagem dessa abordagem é que você tem controle perfeito sobre quando deseja que a sincronização seja feita.
- **Por agendamento:** Os grupos importados são sincronizados usando uma tarefa agendada.

Informações que podem ser sincronizadas com o AD

Ambos os campos padrão e personalizados do Security Center podem ser importados do AD e mantidos sincronizados com o AD. Você pode escolher o grupo de usuários, o usuário, o grupo de titulares de cartão e os campos de titular de cartão a importar do AD na aba *Links* da função Active Directory.

Os atributos padrão que você pode importar do AD são:

- Grupo de usuários
  - Nome
  - Descrição
  - Endereço de e-mail
  - Todos os membros do grupo (usuários)
- Usuário
  - Associação no grupo de usuários importados
  - Nome do usuário
  - Senha
  - Descrição
  - Nome
  - Sobrenome
  - Endereço de e-mail
  - Status: *Ativo* ou *Inativo*
- Grupo de titulares de cartão
  - Nome
  - Descrição
  - Endereço de e-mail
  - Todos os membros do grupo (titulares de cartão)

- Titular do cartão
  - Associação no grupo de titulares de cartão importados
  - Nome do titular do cartão
  - Descrição
  - Nome
  - Sobrenome
  - Endereço de e-mail
  - Status: *Ativo* ou *Inativo*
  - Imagem (opcional pela aba *Links*)
  - Partição (opcional pela aba *Links*)
- Credencial
  - Associação ao titular do cartão importado
  - Nome da credencial
  - Dados do cartão
  - Formato do cartão
  - Código da instalação
  - Número do cartão
  - Status: *Ativo* ou *Inativo*
  - Partição (opcional pela aba *Links*)

Atributos adicionais são importados do AD mapeando-os para os *campos personalizados* do Security Center. A função Active Directory mantém todos os campos importados *sincronizados* com o AD.

Tópicos relacionados

Agendar tarefa na página 219
Mapear campos personalizados para sincronizar com o Active Directory na página 392

Sobre grupos Universais e catálogos globais

O Security Center suporta a sincronização de grupos Universais que pertencem a um catálogo global. Usuários de domínios diferentes em uma floresta do AD podem acessar o Security Center usando uma função do Active Directory conectada a um controlador de domínio (catálogo global). Há algumas coisas que você deve saber antes de sincronizar um grupo Universal que pertence a um catálogo global.

Observe o seguinte ao importar um grupo Universal que pertence a um catálogo global:

- Deve haver uma relação de confiança configurada entre todos os domínios na floresta de AD.
- Grupos primários não são suportados.
- Para recuperar os diretórios dentro de uma floresta, o usuário da função *Active Directory* deve ser capaz de ler a pasta *CN=Partitions, CN=Configuration, DC=ROOTDOMAIN, DC=COM*.
- Se você estiver importando um grupo Universal que não pertence a um catálogo global:
  - A função *Active Directory* entra em contato com vários ADs. O usuário da função *Active Directory* deve ter as permissões necessárias para acessar os diferentes ADs dentro de uma floresta.
  - A porta padrão usada para contato com o AD é 389. Se estiver a utilizar uma porta diferente, deve anexá-la ao nome do servidor AD definido no campo **Active Directory** na aba *Propriedades*, por exemplo: **ADServer.Genetec.com:3393**.
- Se você estiver importando um grupo Universal que pertence a um catálogo global:
  - O catálogo global deve ser atualizado para incluir os atributos necessários para informações de usuários e titulares de cartão do Security Center. Para obter a lista de atributos necessários, consulte Atributos do catálogo global.
  - A porta padrão usada para contato com o AD é 3268. Se estiver a utilizar uma porta diferente, deve anexá-la ao nome do servidor AD definido no campo **Active Directory** na aba *Propriedades*. O nome e o número da porta devem ser separados por dois pontos, por exemplo: **ADServer.Genetec.com:3295**.

Benefícios da utilização de um catálogo global

Um catálogo global armazena uma cópia de todos os objetos AD em uma floresta, o que oferece muitos benefícios:

- A necessidade de consultar vários domínios para informações é eliminada, pois tudo é armazenado no catálogo global.
- Menos tempo para processar informações.
- Menor largura de banda usada.
- Menos repetição de informações.
- Exige apenas uma conexão à função *Active Directory*. Todos os usuários podem acessar o Security Center usando o catálogo global.

Importar grupos de segurança de um Active Directory

Para ter um sistema de gerenciamento de pessoal centralizado, você pode importar grupos de segurança do AD para o Security Center como grupos de usuários ou grupos de titulares de cartão.

Antes de iniciar

Se estiver importando um grupo universal de um catálogo global, leia Sobre grupos universais e catálogos globais.

O que você deve saber

- Ao importar um grupo de segurança do AD, você deve importar todos os membros desse grupo, incluindo os subgrupos. Se você quiser importar apenas um subconjunto de seus membros, por exemplo, apenas usuários do Security Center, você deve definir um novo grupo de segurança do AD apenas com os membros que deseja importar.
- Se você estiver integrando vários ADs no Security Center, cada um deles deve pertencer a um domínio diferente.
- Se você tiver servidores em seu sistema que estão executando uma versão anterior do Security Center, você deve atualizar os servidores para a versão atual antes de usá-los para hospedar uma nova função do Active Directory.
- Um grupo de segurança AD pode ser importado como grupo de usuários, grupo de titulares de cartão ou ambos.

Para importar um grupo de segurança:

1 Abra a tarefa **Sistema** e clique na visualização **Funções**.
2 Clique em **Adicionar uma entidade** () e selecione **Active Directory**.
3 Na página **Informações específicas**, faça o seguinte:
   a) (Se você tiver vários servidores no seu sistema) Na lista suspensa **Servidor**, selecione o *servidor* no qual deseja hospedar a função.
   b) No campo **Active Directory**, digite o Nome de Domínio Totalmente Qualificado (FQDN) do AD, nome do host ou endereço IP do servidor do AD.

      Se você não estiver usando uma porta padrão, deverá anexar o número da porta que está usando ao nome do servidor AD, separado por dois pontos. Por exemplo, **ADServer.Genetec.com:123**. As portas padrão são as seguintes:

      - Active Directory sem SSL: 389
      - Active Directory com SSL: 636
      - Catálogo global sem SSL: 3268
      - Catálogo global com SSL: 3269

   c) Especifique como deseja que a função se conecte ao servidor AD.

      Você deve ter acesso de leitura ao serviço AD selecionado.

      - Use as credenciais do Windows atribuídas ao serviço Genetec™ Server que está sendo executado no servidor que hospeda a função Active Directory.
      - Especifique um conjunto diferente de credenciais do Windows (nome de usuário, senha).

4 Na página *Informações básicas*, digite o nome, a descrição e a partição onde deseja criar a função Active Directory.
5 Clique em **Seguinte**, **Criar** e **Fechar**

   Uma nova função Active Directory () é criada. Aguarde alguns segundos para que a função se conecte ao servidor AD.

6 (Opcional) Se estiver importando um grupo universal que se conecta a um catálogo global, ative a opção **Usar catálogo global**.

7 Na aba **Propriedades**, selecione os grupos de segurança do AD que deseja importar.

NOTA: Existem dois tipos de grupos no Active Directory do Windows: *grupos de distribuição* e *grupos de segurança*. O Security Center somente pode sincronizar com grupos de segurança.

a) Clique em **Adicionar um item** ( ).

b) Selecione os grupos de segurança que você deseja adicionar à sua função Active Directory.

Use um dos seguintes métodos:

- (Recomendado) Digite o nome do grupo em **Encontrar grupos do Active Directory** e clique em .

  Se o texto digitado corresponder a um único grupo, ele será automaticamente adicionado à lista **Grupos selecionados**.

  Se o texto digitado corresponder a vários nomes de grupo, uma segunda caixa de diálogo aparecerá listando todos os nomes de grupos que correspondem ao texto inserido.

  Selecione os que desejar e clique em **OK** para adicioná-los à lista **Grupos selecionados**.

- Na lista **Grupos selecionados**, clique em ( ).

  A caixa de diálogo *Membros do Active Directory* aparece.

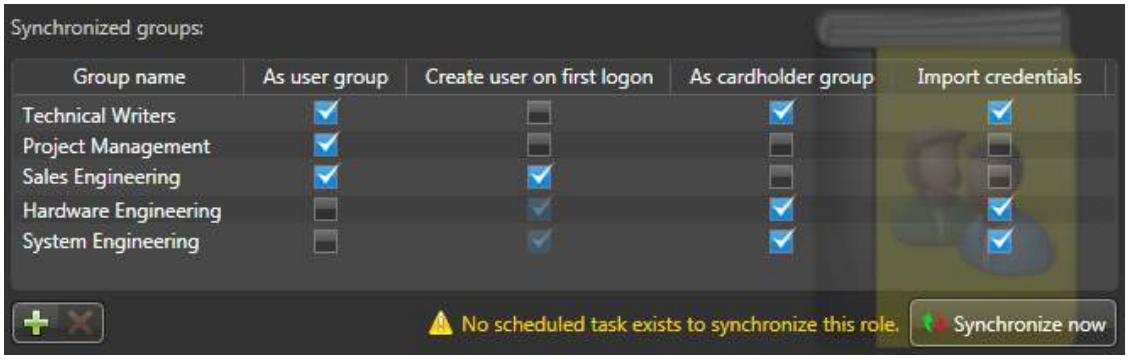
  Selecione um grupo de segurança e clique em **OK**. Somente grupos de segurança podem ser sincronizados. Se você selecionar um item que não é um grupo de segurança, o botão **OK** permanece desativado.

NOTA: Os nomes apresentados na caixa de diálogo são nomes de exibição. O Security Center somente sincroniza os nomes de contas porque eles são garantidamente únicos. Normalmente, os nomes de exibição e os nomes de conta são os mesmos. A única maneira de diferenciá-los é que os nomes de exibição contêm espaços.

c) Repita a etapa anterior com a frequência necessária até que todos os grupos de segurança que você deseja sincronizar com o AD sejam listados em **Grupos selecionados** e, em seguida, clique em **OK**.

Os grupos selecionados são listados em **Grupos sincronizados** na aba **Propriedades**.

8 Para cada um dos grupos sincronizados, especifique como você deseja importá-los.



Estão disponíveis as seguintes opções:

- **Como grupo de usuários:** Selecione esta opção para importar o grupo sincronizado como *grupo de usuários* e os membros do grupo como *usuários*.
- **Criar usuário no primeiro logon:** Essa é a opção padrão e cria um grupo de usuários vazio. As entidades de usuário só são criadas quando alguém tenta fazer logon na primeira vez. Essa opção evita ter que criar todas as entidades de usuário em simultâneo, o que pode travar o sistema. Se você desmarcar essa opção, todas as entidades de usuário serão criadas ao mesmo tempo que um grupo de usuários.

- **Como grupo de titulares de cartão:** Selecione esta opção para importar o grupo sincronizado como *grupo de titulares de cartão* e os membros do grupo como *titulares de cartão*. Todos os titulares de cartão sincronizados são criados em simultâneo.
- **Importar credenciais:** Selecione esta opção para importar as informações de credencial dos portadores de cartão sincronizados.

9 Se você estiver importando o grupo de segurança do AD como grupo de titulares de cartão, selecione quais campos de titular de cartão você deseja sincronizar com o AD.

10 (Opcional) Mapeie campos personalizados para sincronizar com o AD.

11 Clique em **Aplicar** e, em seguida, clique em **Sincronizar agora** ( ).

Todos os grupos sincronizados e seus membros são importados como entidades do Security Center de acordo com suas especificações, com uma seta amarela ( ) sobreposta ao seu ícone.

Após terminar

Alguma configuração adicional pode ser necessária, dependendo do que você sincronizou com o AD:

- Se você já tinha entidades configuradas no seu sistema, talvez seja necessário resolver certos conflitos causados pela importação.
- (Opcional) Configure os grupos de usuários importados com privilégios e opções de segurança apropriados, de modo que quando novas entidades de usuário forem criadas, elas possam herdar essas propriedades automaticamente de seu grupo de usuários pai.
- (Opcional) Configure os titulares de cartão e os grupos de titulares de cartão importados.
- (Opcional) Crie uma tarefa agendada para sincronizar entidades importadas com o AD regularmente.

Depois de criar uma tarefa agendada, a mensagem de aviso **Não existe nenhuma tarefa agendada para sincronizar esta função** desaparece da aba **Propriedades**.

Tópicos relacionados

Integração com o Active Directory do Windows na página 384
Formatos de cartão personalizados na página 689
Sobre entidades federadas na página 225

Mapear campos personalizados para sincronizar com o Active Directory

Além dos atributos padrão, você pode importar outros atributos do AD mapeando-os para campos personalizados do Security Center. O mapeamento de campos personalizados pode ser diferente para cada função do Active Directory no seu sistema.

Antes de iniciar

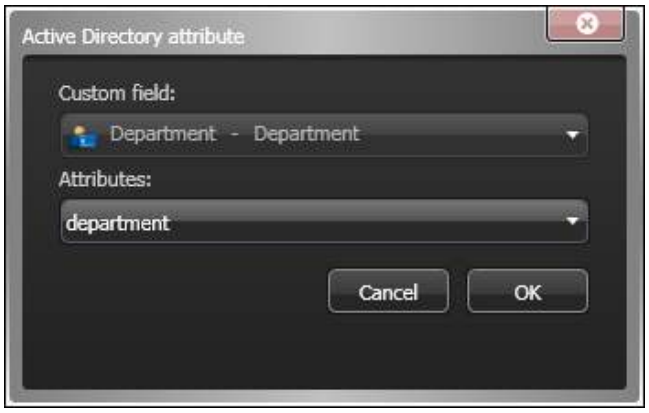
- Certifique-se de que a estação de trabalho em que o Config Tool está sendo executado esteja no mesmo domínio de rede que o servidor AD.
- Defina os campos personalizados que receberão dados do AD.

O que você deve saber

Não mais de 32 campos personalizados podem ser mapeados para o AD.

Para mapear campos personalizados para sincronizar com o Active Directory:

1 Na aba **Links** da função Active Directory, em **Campos personalizados**, clique em **Adicionar um item** ( ).



2 Selecione o campo personalizado e o atributo do AD e clique em **OK**.

IMPORTANTE: O tipo de dado do campo personalizado deve corresponder ao do atributo do AD: texto com texto, decimal com decimal, data com data etc. O tipo de dado de imagem do Security Center deve ser mapeado para o tipo de dado binário do AD, e o atributo do AD mapeado deve conter uma imagem JPEG válida.

O novo mapeamento aparece na aba **Links**.

3 Repita os passos anteriores conforme necessário.

4 Clique em **Aplicar**.

Os campos personalizados mapeados são exibidos na aba **Links**. Quando você sincroniza com o AD, eles são somente leitura.

Resolver conflitos causados por entidades importadas

A resolução de conflitos pode ser necessária se você tiver entidades existentes (usuários ou titulares de cartão) em seu banco de dados antes de importar entidades do AD.

O que você deve saber

Quando uma entidade sincronizada tem o mesmo nome de uma entidade local, a função do Active Directory a vê como um potencial conflito. Você pode usar a ferramenta *Resolução de conflitos* para visualizar ( ) e resolver potenciais conflitos excluindo as entidades conflituantes na tarefa Gerenciamento de titulares de cartões.

Para resolver conflitos causados por entidades importadas:

1 Abra a tarefa **Sistema** e clique na visualização **Funções**.

2 Selecione a função Active Directory ( ) e clique em **Resolução de conflitos** ( ).

A caixa de diálogo **Resolução de conflitos do Active Directory** aparece. Todas as entidades sincronizadas são listadas à esquerda. As que entram em conflito com uma entidade local são sinalizadas em verde.

3 Resolva cada conflito de titular de cartão:
   a) Abra a tarefa **Gerenciamento de titulares de cartão** e localize os dois registros de titular de cartão que estão em conflito.
   b) Selecione um dos registros de titular de cartão conflituante e clique em **Modificar**.
   c) Adicione quaisquer informações ausentes que estejam disponíveis no registro de titular de cartão duplicado.
   d) Salve e feche o registro de titular de cartão.
   e) Selecione o registro de titular de cartão duplicado e clique em **Excluir titular de cartão**.

4 Resolva cada conflito de usuário:
   a) Abra a tarefa de **Gerenciamento de usuários**.
   b) No navegador de entidades, localize os dois registros de usuário que estão em conflito.
   c) Abra um dos registros de usuário conflituantes.
   d) Adicione quaisquer informações ausentes que estejam disponíveis no registro de usuário duplicado.
   e) Clique em **Aplicar**.
   f) Selecione o registro de usuário duplicado e clique em **Excluir**.

5 Retorne para a visualização **Funções** na tarefa **Sistema**.

6 Na caixa de diálogo **Resolução de conflitos do Active Directory**, selecione as entidades que estão assinaladas como conflituantes e pressione **Excluir**.

7 Em **Resolução de conflitos do Active Directory**, clique em **Concluir**.

O processo irá gerar um arquivo com o nome *Conflict_Manifest.data* que documenta os conflitos resolvidos. Ele pode ser salvo para referência futura.

Desativar usuários importados de um Active Directory

Se você tiver usuários importados de um Active Directory, você pode definir o status do usuário como inativo. O usuário fica dessincronizado do AD até que você ative-o novamente.

Para desativar um usuário importado de um Active Directory:

1. Abra a tarefa **Segurança**.
2. Selecione um usuário importado ( ) e clique na aba **Propriedades**.
3. Coloque a opção **Status do usuário** como **Inativo**.
4. Clique em **Aplicar**.

O usuário não está mais sincronizado com o AD. Ele só será sincronizado novamente depois de definir o status do usuário como **Ativo**.

Atributos de catálogo global

Para que a função *Active Directory* se conecte com êxito a um catálogo global e sincronize usuários e titulares de cartão no Security Center, o catálogo global deve ser atualizado para incluir atributos específicos.

Atributos de usuário

O catálogo global deve ser atualizado com os seguintes atributos de usuário:

- distinguishedName
- objectGUID
- objectClass
- cn
- objectSid
- sAMAccountName
- displayName
- nome
- endereço
- descrição
- userPrincipalName
- userAccountControl
- accountExpires
- givenName
- sn
- tokenGroup
- memberof (Somente para o SDK)
- quaisquer atributos a serem usados na aba Links

Atributos de grupo

O catálogo global deve ser atualizado com os seguintes atributos de grupo:

- distinguishedName
- objectGUID
- objectClass
- cn
- objectSid
- sAMAccountName
- nome
- endereço
- descrição
- groupType
- membro

Atributos de contêiner, domínio e unidade organizacional

O catálogo global deve ser atualizado com os seguintes atributos de contêiner, domínio e unidade organizacional:

- distinguishedName
- objectGUID
- objectClass
- objectSid
- displayName
- nome
- membro

21

Autenticação baseada em declarações

Esta seção inclui os seguintes tópicos:

- "O que é a autenticação baseada em declarações?" na página 398
- "Implementar autenticação baseada em declarações pelo ADFS" na página 400
- "Adicionando confiança a um provedor de reivindicações para um ADFS de terceiros" na página 403
- "Configuração de regras de reivindicações para um provedor de reivindicações de terceiros" na página 405
- "Adicionar uma parte confiável para o Security Center" na página 406
- "Configurar regras de declaração para o Security Center" na página 411
- "Mapear grupos ADFS remotos para o Security Center" na página 412
- "Criar Active Directory Federation Services" na página 413

O que é a autenticação baseada em declarações?

A autenticação baseada em reivindicações é o processo de autenticação de um usuário com base em um conjunto de reivindicações sobre sua identidade contidas em um token confiável. Esse token é freqüentemente emitido e assinado por uma entidade que é capaz de autenticar o usuário por outros meios e que é confiável pela entidade que faz a autenticação baseada em reivindicações.

O que é uma reivindicação?

Uma *declaração* é uma afirmação que um sujeito faz sobre ele próprio ou outro sujeito. A afirmação pode ser sobre um nome, identidade, chave, grupo, privilégio ou capacidade, por exemplo. As declarações são emitidas por um provedor, recebem um ou mais valores e, em seguida, são empacotadas em tokens de segurança emitidos por um *emitente*, geralmente conhecido como *serviço de token de segurança* (STS).

Quais são os benefícios das reivindicações?

Reivindicações separam o processo de *autenticação* (verificar que uma entidade é o que declara ser) do processo de *autorização* (estabelecer os direitos que uma entidade tem sobre as características e recursos de um sistema). O benefício desta dissociação é que ela permite o *logon único* (o uso de uma autenticação de usuário única para vários sistemas de TI ou até mesmo organizações). Reivindicações também dão contexto à identidade do usuário, permitindo-o configurar políticas de acesso mais flexíveis.

No contexto do Security Center, o processo de autenticação é tratado por um *STS* personalizado ou um *Serviços de Federação do Active Directory (ADFS)* servidor, e o processo de autorização é tratado pelo próprio Security Center, através de partições e privilégios.

Quais métodos de autenticação de usuário o Security Center suporta?

Security Center oferece suporte aos seguintes métodos de autenticação do usuário:

- **Autenticação Security Center nativa:** O usuário fornece um nome de usuário e uma senha para o aplicativo cliente para fazer o logon no Security Center.
- **Autenticação ativa no Directory:** O usuário clica em **Usar credenciais do Windows** e faz o logon usando a sua conta de usuário do Windows (exige a integração do Active Directory configurada).
- **Autenticação ativa ADFS:** (Protocolo WS-Trust) A aplicação cliente envia o nome de usuário e senha para um provedor de identidade confiável (servidor ADFS) para autenticação.
- **Autenticação passiva ADFS (ou autenticação com base na web):** (Protocolo WS-Federation) A aplicação cliente redireciona o usuário para um formulário da web gerenciado por um provedor de identidade confiável (servidor ADFS). O provedor de identidade pode solicitar diversas credenciais para autenticar o usuário sem passar pelo aplicativo cliente. *Autenticação Multifator (MFA)* pode ser implementado através desse método.

NOTA: Os usuários federados por meio do ADFS são criados no Security Center apenas no primeiro logon. Ao contrário do Active Directory, você não tem a opção de criar todos os usuários importados no Security Center quando a função ADFS conecta-se ao servidor ADFS.

Exigências

Para usar o ADFS para autenticação, as seguintes condições devem ser cumpridas:

- A estação de trabalho cliente deve ser capaz de alcançar o servidor ADFS.
- O certificado de criptografia HTTPS do serviço ADFS deve ser confiável pela estação de trabalho cliente.

Impacto sobre o desempenho

- A escalabilidade do Directory não é afetada por esse recurso.
- Os logons de usuário que usam credenciais do ADFS devem levar um pouco mais de tempo que logons regulares, porque exigem que as estações de trabalho clientes se conectem a um ou mais servidores ADFS remotos antes de se conectarem ao Directory.

Compatibilidade retroativa

A opção **Usar credenciais do Windows** na caixa de diálogo *Logon* funciona somente para versão 5.4 e mais recente.

A autenticação ativa ADFS é suportada para estações de trabalho clientes que executam uma versão mais antiga do Security Desk ou SDK, mas apenas se a senha for inserida pelo usuário.

A autenticação ADFS passiva ou com base em web funciona somente para 5.7 SR2 e mais recentes.

Tópicos relacionados

Fazer logon no Security Center através do Config Tool na página 7

Implementar autenticação baseada em declarações pelo ADFS

Você pode usar um servidor de Active Directory Federation Services (ADFS) como o provedor de declarações para o Security Center e permitir que usuários externos à sua empresa façam logon no seu sistema estabelecendo uma cadeia de confiança de servidores ADFS de terceiros para o servidor principal do Security Center da empresa.

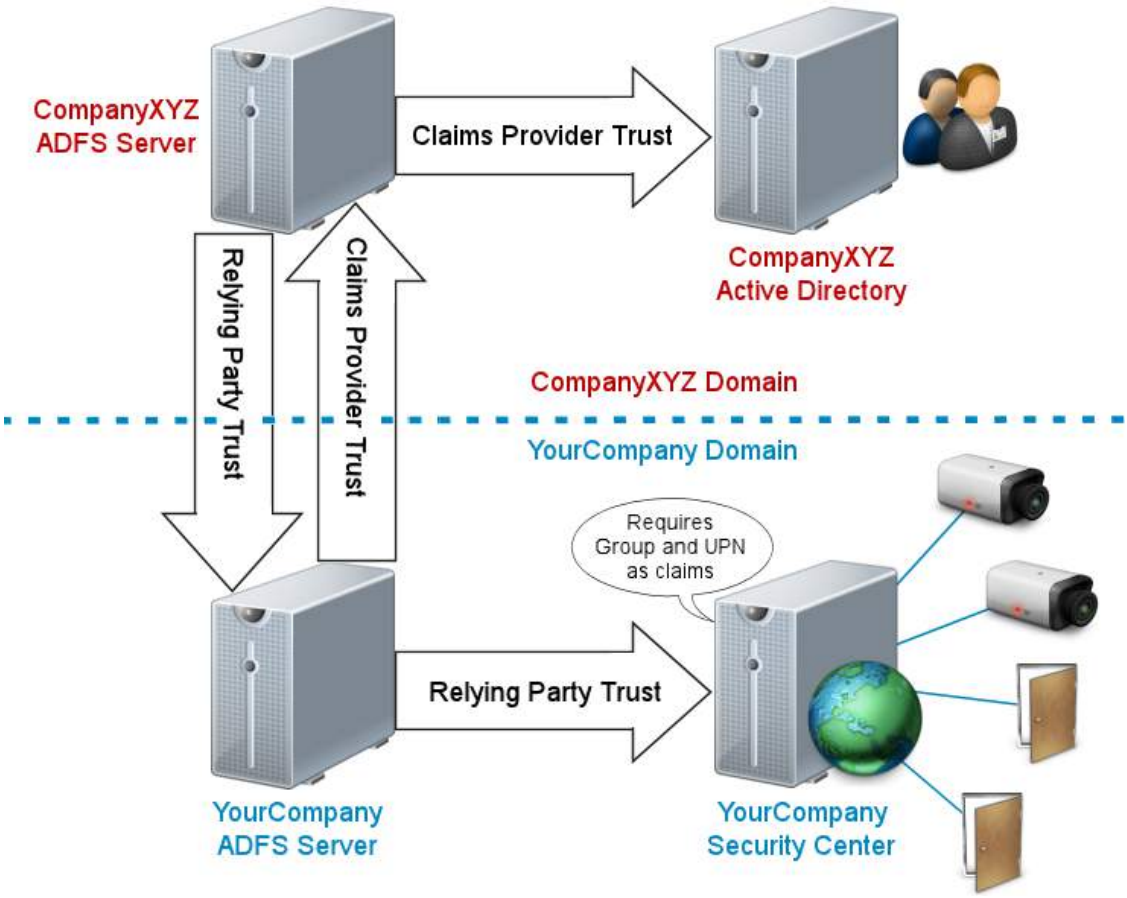
Antes de iniciar

Presume-se que você esteja familiarizado com os conceitos de autenticação baseada em declarações e que o servidor *ADFS* da sua empresa esteja operacional. Para obter informações gerais sobre a instalação e configuração do ADFS, consulte a documentação fornecida pela Microsoft.

O que você deve saber

Para fins ilustrativos, vamos supor que você deseje permitir que usuários externos da empresa XYZ acessem o sistema Security Center da sua empresa. A empresa XYZ tem seu próprio servidor ADFS que depende de seu próprio Active Directory como *provedor de reivindicações*. Os servidores da empresa XYZ não estão no mesmo domínio que os servidores da sua empresa. O servidor ADFS da sua empresa depende do servidor ADFS da empresa XYZ como provedor de declarações e, por sua vez, atua como provedor de declarações no sistema Security Center da sua empresa. Portanto, uma cadeia de confianças deve ser estabelecida a partir do Active Directory da empresa XYZ para o servidor principal do sistema Security Center da sua empresa.

NOTA: O Security Center requer atributos específicos como *declarações*: *Grupo* e *UPN (Nome Principal do Usuário)*.



MELHOR PRÁTICA: Se pretender aceitar grupos de segurança a partir do seu Active Directory local como grupos de utilizadores do Security Center, não faça a sua federação através da função ADFS, mas importe-os através da função Active Directory em vez disso. A última abordagem oferece mais funcionalidades, como a sincronização de todos os campos padrão (primeiro nome, sobrenome, endereço de e-mail e assim por diante), mapeamento de campos personalizados e a opção de criar todos os usuários no momento de sincronização de funções.

Para implantar autenticação baseada em reivindicações pelo ADFS:

1 Configure a cadeia de confiança fora do domínio da sua empresa.

Certifique-se de que as seguintes tarefas sejam executadas pelo pessoal de TI da Empresa XYZ.

a) Adicione um provedor de reivindicações ao servidor ADFS da Empresa XYZ para o Active Directory da Empresa XYZ.
b) Adicione uma parte confiável do servidor ADFS da Empresa XYZ para o servidor ADFS da sua empresa.

2 Configure o servidor ADFS local como o provedor de declarações para o sistema Security Center.

a) No servidor ADFS da sua empresa, abra o snap-in Gerenciamento de ADFS.
b) Adicione um provedor de declarações confiável ao seu ADFS para o servidor ADFS de terceiros.
c) Configure as regras de declaração para o provedor de declarações de terceiros.
d) Adicione uma parte confiável ao seu ADFS para o Security Center.
e) Configure as regras de declaração para o Security Center, a parte confiável que você adicionou.

3 Configure o sistema Security Center para receber declarações do seu servidor ADFS local.

a) Conecte ao seu sistema Security Center com o Config Tool.
b) Crie um grupo de usuários para cada grupo do ADFS que você aceitar como grupos de usuários do Security Center.
c) Crie a função Active Directory Federation Services.

Todos os usuários autenticados pelo ADFS devem fazer logon usando nomes de usuário totalmente qualificados, o que significa que eles devem adicionar seu nome de domínio aos seus nomes de usuário, como `Username@CompanyXYZ.com`.

IMPORTANTE: Há atualmente um problema conhecido sobre o uso de um Active Directory e ADFS locais. Quando você tiver usuários externos autenticados pelo ADFS no sistema, todos os usuários importados do Active Directory local também devem usar nomes de usuário totalmente qualificados, mesmo que pertençam ao mesmo domínio do sistema Security Center.

Adicionando confiança a um provedor de reivindicações para um ADFS de terceiros

Para permitir que os usuários de uma organização externa (Empresa XYZ) se conectem ao sistema do Security Center, o servidor ADFS da empresa deve confiar nas declarações fornecidas pelo servidor ADFS da Empresa XYZ.

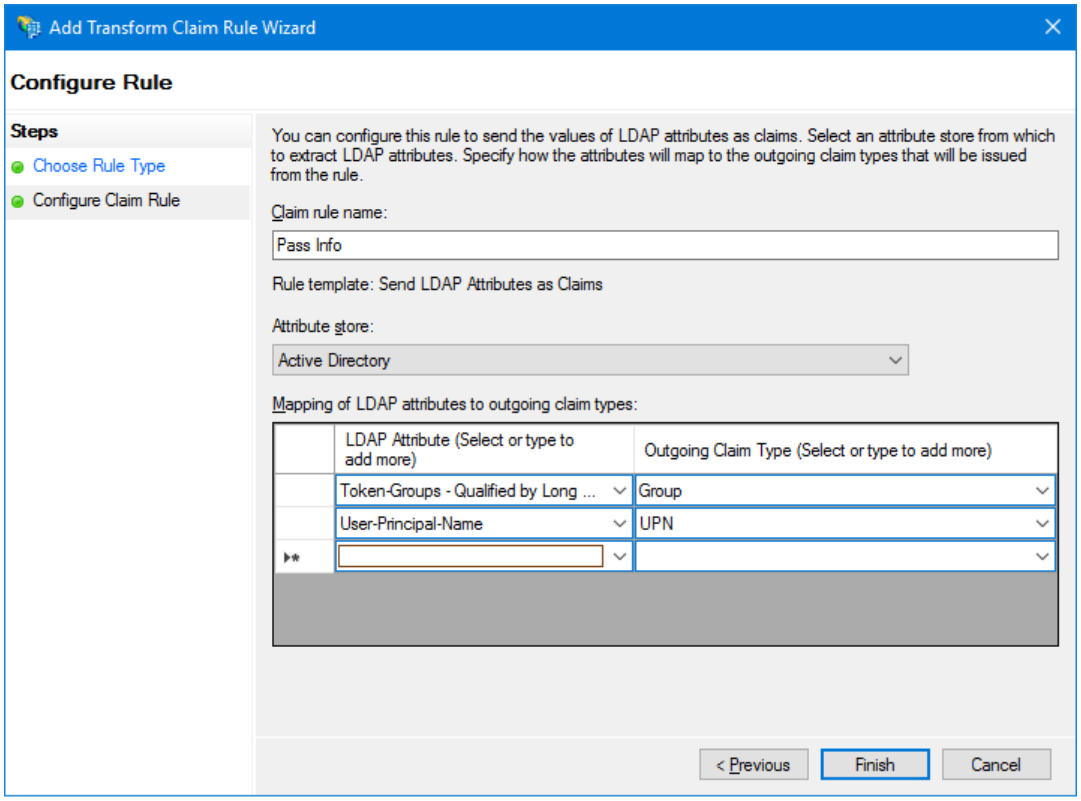
Antes de iniciar

Certifique-se de que a Empresa XYZ tenha feito o seguinte:

- Adicione um provedor de reivindicações ao servidor ADFS da Empresa XYZ para o Active Directory da Empresa XYZ.
- Adicione uma parte confiável do servidor ADFS da Empresa XYZ para o servidor ADFS da sua empresa.

NOTA: O Security Center requer atributos específicos como *declarações*: *Grupo* e *UPN (Nome Principal do Usuário)*.

A seguinte captura de tela ilustra a regra de declaração da parte confiável no servidor ADFS na EmpresaXYZ para SuaEmpresa.com.



O que você deve saber

Esta tarefa é parte do processo de implementação para autenticação baseada em reivindicações usando ADFS com base em um exemplo de cenário. As capturas de tela de exemplo foram tiradas a partir do Windows Server 2016. Caso esteja usando uma versão diferente, as suas capturas de tela podem parecer diferentes.

Adicionar confiança a um provedor de reivindicações ao servidor ADFS da sua empresa está fora do escopo deste documento. Para obter informações sobre esses tópicos, consulte a documentação do ADFS da Microsoft.

Configuração de regras de reivindicações para um provedor de reivindicações de terceiros

Depois de criar a confiança do provedor de reivindicações em seu servidor ADFS para o servidor ADFS de terceiros, você deve configurar as reivindicações que o último deve encaminhar ao seu servidor ADFS.

Antes de iniciar

A janela *Gerenciamento de ADFS* deve estar aberta no servidor ADFS e a confiança do provedor de reivindicações deve ser criada para o servidor ADFS de terceiros.

O que você deve saber

Esta tarefa é parte do processo de implementação para autenticação baseada em reivindicações usando ADFS com base em um exemplo de cenário.

Para configurar regras de reivindicações para um provedor de reivindicações de terceiros:

1. Na janela *ADFS*, clique em **Relacionamentos de confiança > Confianças de Provedor de Reivindicações**, selecione o provedor de reivindicações que corresponde ao ADFS de terceiro e clique em **Editar Regras de Reivindicações** no painel *Ações*.

   A janela *Editar Regras de Reivindicações* será aberta.
2. Se não existir nenhuma regra de reivindicação para **UPN**, adicione uma.
   a) Clique em **Adicionar regra**.
   b) Na lista suspensa **Modelo de regra de reivindicação**, selecione **Passagem ou filtrar uma reivindicação recebida** e clique em **Próximo**.
   c) Configure a regra e clique em **Concluir**.
      - **Nome da regra de reivindicação:** Digite um nome que ajude a lembrar da regra.
      - **Tipo de reivindicação de entrada:** Selecione **UPN**.
      - **Passar apenas os valores de reivindicação que correspondem a um valor de sufixo de e-mail específico:** Selecione esta opção e digite um valor de sufixo de e-mail. Por exemplo: `EmpresaXYZ.com`.

        MELHOR PRÁTICA: Recomenda-se filtrar as reivindicações provenientes de um provedor de reivindicações de terceiros como medida de segurança, para que o provedor de reivindicações de terceiros não possa enviar valores inesperados. Isso é feito, por exemplo, para evitar que a empresa XYZ finja que seus usuários são da sua empresa e obter privilégios elevados. **Passar todos os valores de reivindicação** deve ser evitado ao lidar com provedores de reivindicações de terceiros.
3. Se não existir nenhuma regra de reivindicação para **Grupo**, adicione uma.
   a) Clique em **Adicionar regra**.
   b) Na lista suspensa **Modelo de regra de reivindicação**, selecione **Passagem ou filtrar uma reivindicação recebida** e clique em **Próximo**.
   c) Configure a regra e clique em **Concluir**.
      - **Nome da regra de reivindicação:** Digite um nome que ajude a lembrar da regra.
      - **Tipo de reivindicação de entrada:** Selecione **Grupo**.
      - **Passar apenas os valores de reivindicação que comecem com um valor específico:** Selecione esta opção e digite um valor inicial. Por exemplo: `EmpresaXYZ\` ou `EmpresaXYZ.com\`. Consulte seu departamento de TI sobre qual deve ser usado.
4. Clique em **Aplicar**.

Adicionar uma parte confiável para o Security Center

Para que um servidor ADFS funcione como o provedor de declarações para o seu sistema Security Center, você deve adicionar o seu sistema Security Center às partes confiáveis do servidor ADFS.

Antes de iniciar

A janela do snap-in *Gerenciamento de ADFS* deve estar aberta no seu servidor ADFS. Se o failover do Directory estiver configurado no seu sistema, tenha consigo o nome de host de cada servidor do Directory.

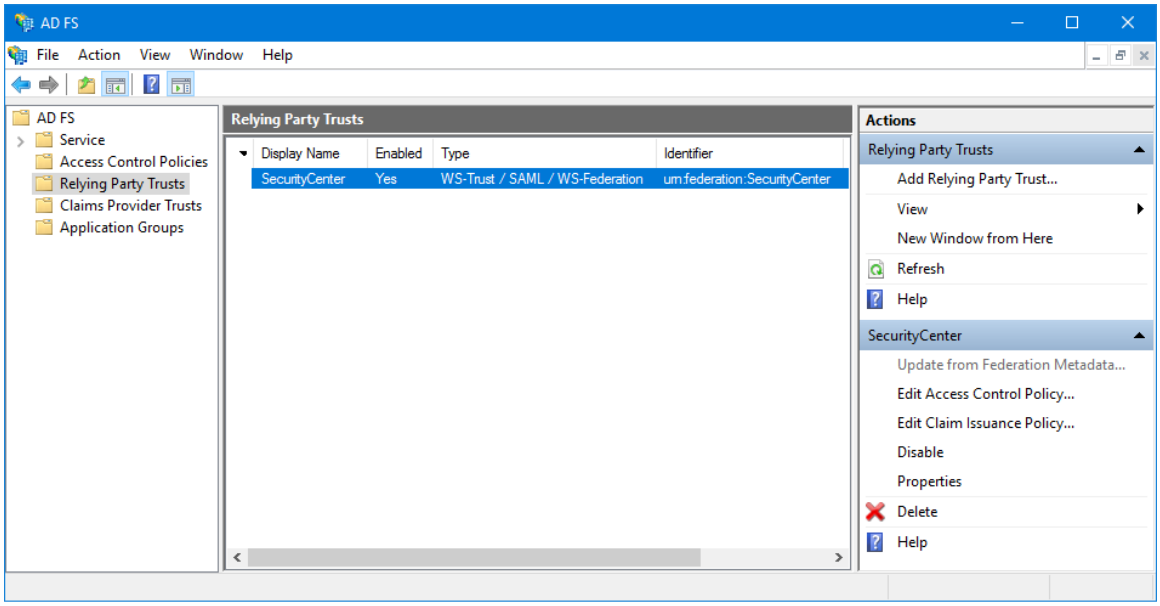
O que você deve saber

Esta tarefa é parte do processo de implementação para autenticação baseada em reivindicações usando ADFS com base em um exemplo de cenário. As capturas de tela de exemplo foram tiradas a partir do Windows Server 2016. Caso esteja usando uma versão diferente, as suas capturas de tela podem parecer diferentes.

NOTA: Se não estiver habilitando o *autenticação passiva*, clique em **Próximo** ao invés de executar as etapas que estão marcadas como "(Somente PA)".

Para adicionar uma parte confiável ao seu servidor ADFS para o Security Center:

1 Na janela *ADFS*, clique em **Partes confiáveis** > **Adicionar parte confiável**.



A janela *Assistente de adição de parte confiável* é aberta.

2 Na página de *Boas-vindas*, clique em **Iniciar** > **Inserir dados sobre a parte confiável manualmente** > **Próximo**.

Pode deixar **Conhecimento de declarações** selecionado.

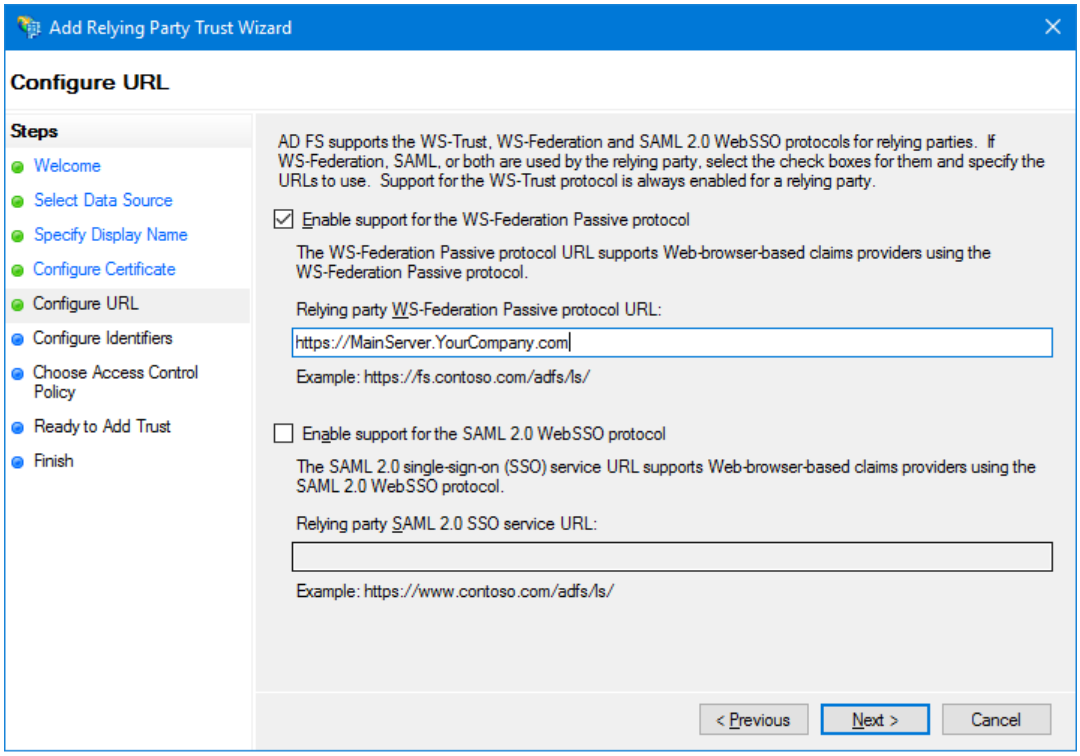
3 Na página *Especificar nome de exibição*, no campo **Nome de exibição**, digite um nome que represente o sistema Security Center da sua empresa e clique em **Próximo**.

Por exemplo, `YourCompany Security Center`.

4 (Opcional) Na página *Configurar certificado*, especifique um certificado de criptografia de token e clique em **Próximo**.

5 (Somente PA) Na página *Configurar URL*, selecione **Habilitar suporte para o protocolo passivo WS-Federation**, digite a URL do seu Security Center *servidor principal* e, em seguida, clique em **Próximo**.

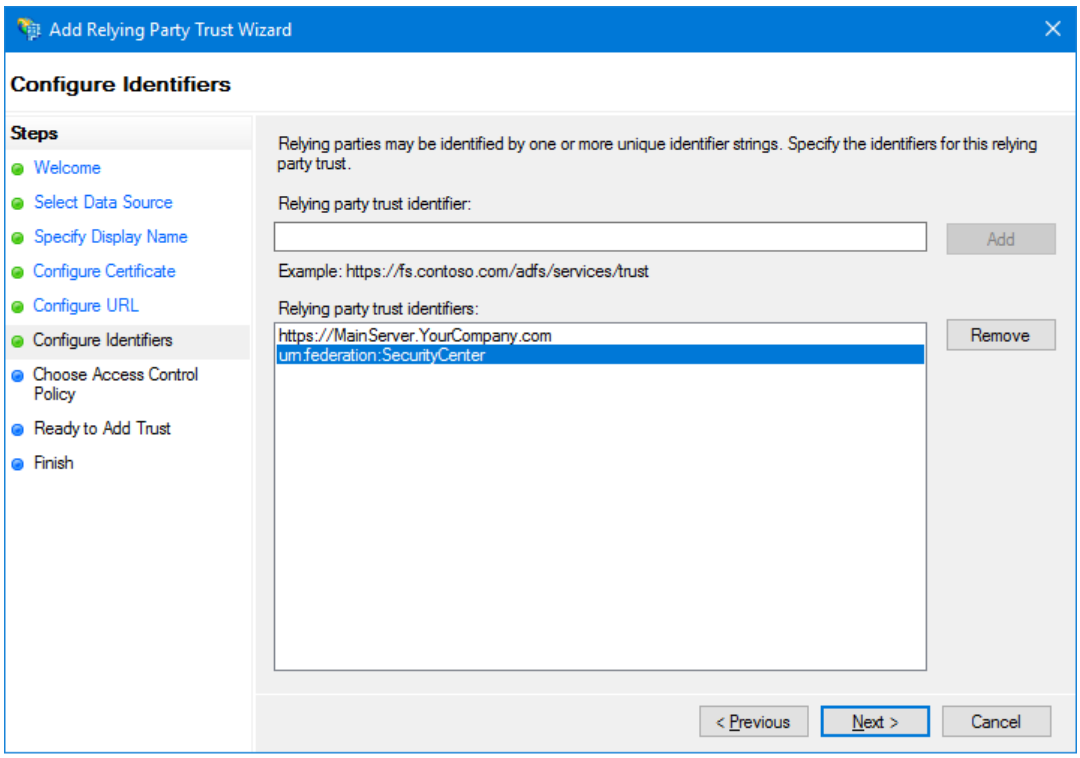
Por exemplo: `https://MainServer.YourCompany.com`



6 (Somente PA) Na página *Configurar identificadores*, no campo **Identificador de parte confiável**, digite uma cadeia de caracteres que identifique o servidor principal do Security Center e clique em **Adicionar**.

IMPORTANTE: Um exemplo seria usar a URL do seu servidor principal: `https://MainServer.YourCompany.com`. Anote este valor. Você precisará inserir este identificador em uma etapa posterior, quando configurar sua função ADFS no servidor Security Center.

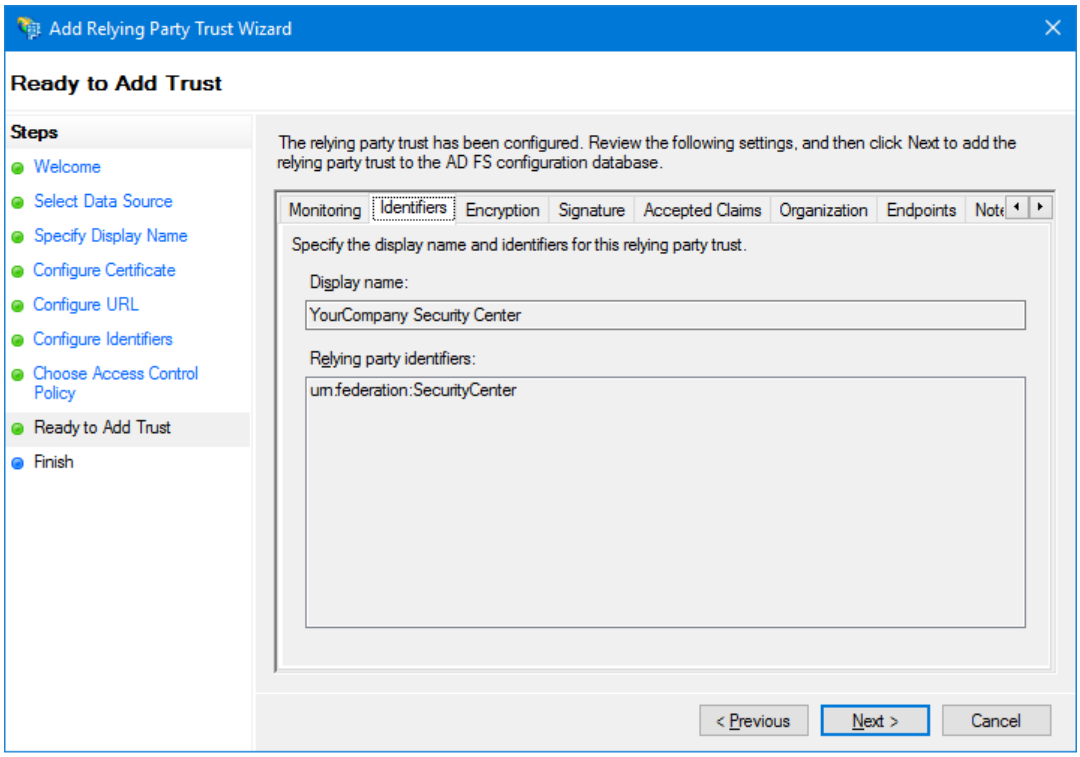
MELHOR PRÁTICA: Recomendamos usar o valor padrão configurado para a função ADFS, `urn:federation:SecurityCenter`, para que tenha menos uma coisa para se lembrar.



7 (Somente PA) Na lista **Identificadores de parte confiável**, selecione a linha que corresponde à URL do seu servidor principal e clique em **Remover** > **Próximo**.

8 Na página *Escolher política de controle de acesso*, selecione **Autorizar todos** e clique em **Próximo**.

9 Na página *Pronto para adicionar confiança*, clique em **Identificadores** e verifique os identificadores inseridos.



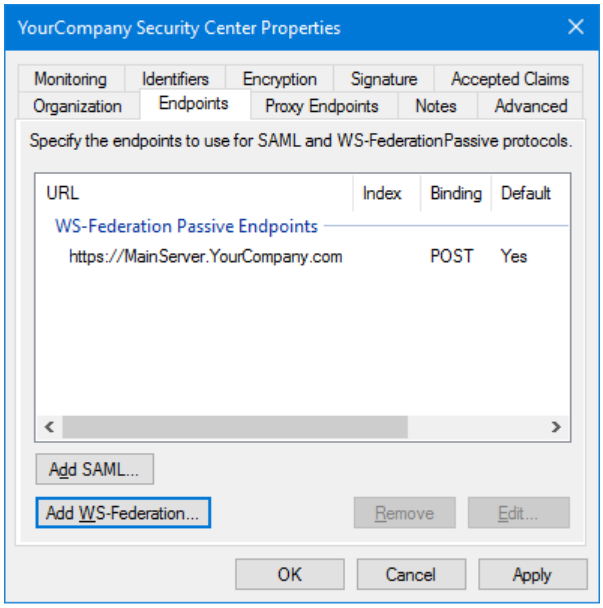
10 Clique em **Próximo**, deixe **Configurar política de emissão de declarações para este aplicativo** selecionado e clique em **Fechar**.

O servidor principal do Security Center é adicionado às partes confiáveis do seu servidor ADFS.

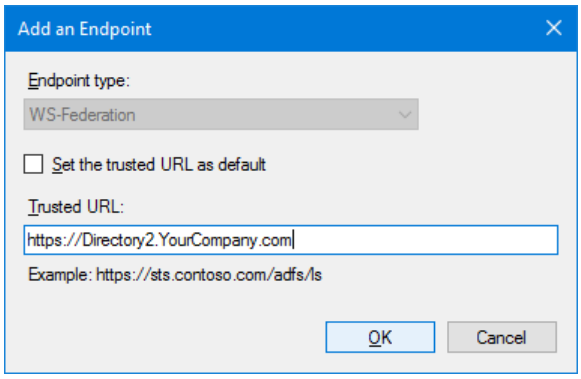
11 Se o failover do Directory estiver configurado no seu sistema, você deve adicionar a URL de cada servidor do Directory como pontos de extremidade à parte confiável Security Center do seu servidor ADFS.

NOTA: A função ADFS é executada no mesmo servidor da função Directory. Quando a função Directory falhada é transferida para o servidor seguinte em linha, a função ADFS falhada também é transferida para o mesmo servidor. Por este motivo, o servidor ADFS deve conhecer a URL de todos os servidores do Directory existentes no seu sistema. Para a URL do servidor, digite `https://` seguido do nome de host totalmente qualificado.

a) Na janela *ADFS*, selecione a parte confiável Security Center e clique em **Propriedades** > **Pontos de extremidade**.

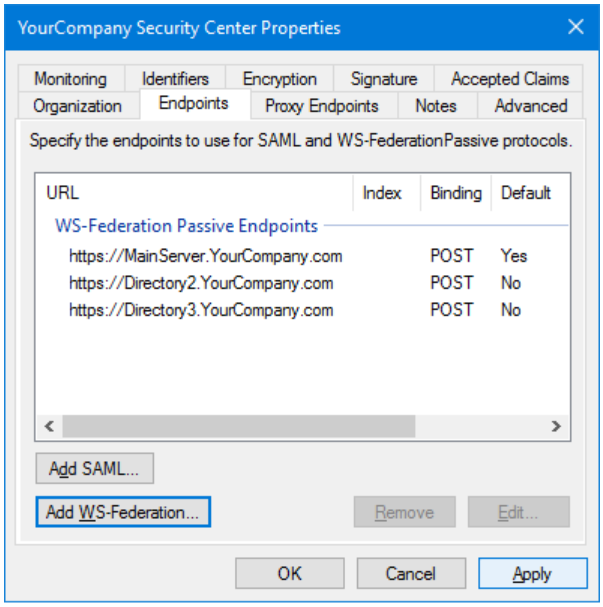


b) Clique em **Adicionar WS-Federation**, digite a URL de um servidor do Directory e clique em **OK**.



c) Repita a etapa anterior para todos os servidores do Directory existentes no seu sistema.

d) Clique em **Aplicar** > **OK**.



Após terminar

Configurar regras de declaração para o Security Center.

Configurar regras de declaração para o Security Center

Depois de criar a confiança da parte confiável em seu servidor ADFS para o Security Center, você deve configurar quais declarações o Security Center requer.

Antes de iniciar

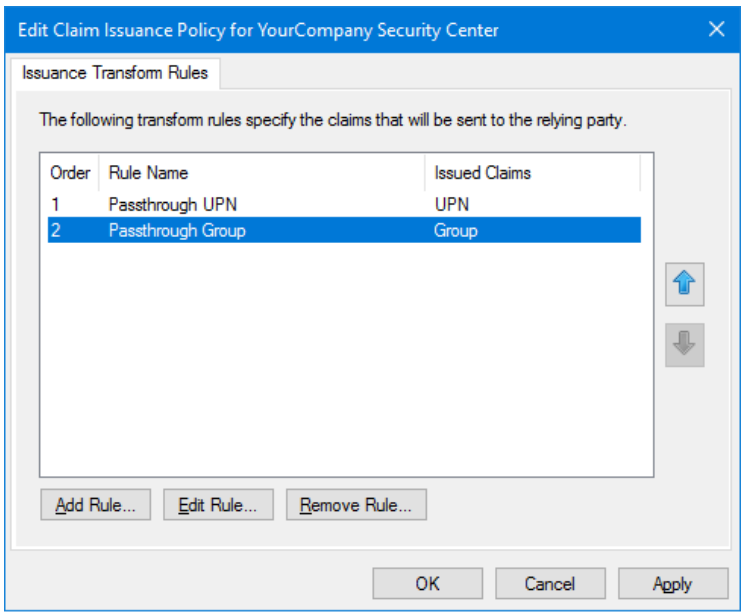
A janela *Gerenciamento de ADFS* deve estar aberta em seu servidor ADFS, e a confiança da parte confiável deve ser criada para o seu servidor principal Security Center.

O que você deve saber

Esta tarefa é parte do processo de implementação para autenticação baseada em reivindicações usando ADFS com base em um exemplo de cenário. As capturas de tela de exemplo foram tiradas a partir do Windows Server 2016. Caso esteja usando uma versão diferente, as suas capturas de tela podem parecer diferentes.

Para configurar as regras de declaração para o Security Center:

1. Na janela *ADFS*, clique em **Confianças de partes confiáveis**, selecione a parte confiável que corresponde ao seu sistema Security Center e clique em **Editar política de emissão de declarações** no painel *Ações*.
   Aparece a janela *Editar política de emissão de declarações*.
2. Adicione uma primeira regra de declaração para **UPN**.
   a) Clique em **Adicionar regra**.
   b) Na lista suspensa **Modelo de regra de declaração**, selecione **Passar ou filtrar uma declaração recebida** e clique em **Próximo**.
   c) Configure a regra e clique em **Concluir**.
   - **Nome da regra de declaração:** Digite um nome que ajude a lembrar da regra.
   - **Tipo de declaração de entrada:** Selecione **UPN**.
   - **Passar todos os valores de declaração:** Selecione essa opção.
3. Adicione uma segunda regra de declaração para **Grupo**.
   Siga as instruções para regras de declaração UPN. Somente dessa vez, altere **UPN** para **Group**.



4. Clique em **Aplicar** > **OK**.

Mapear grupos ADFS remotos para o Security Center

Para aceitar grupos ADFS remotos como grupos de usuários válidos no Security Center, você deve criar um grupo de usuários do Security Center para cada um deles.

Antes de iniciar

Todos os servidores ADFS envolvidos na cadeia de confiança devem ser completamente configurados.

Para mapear grupos ADFS remotos para o Security Center:

1 Crie um grupo de usuários para cada grupo ADFS que você aceitar como grupo de usuários do Security Center.

Os grupos de usuários devem ter exatamente o mesmo nome definido nos Active Directories remotos, seguido pelo nome de domínio ADFS remoto.

Por exemplo, se o domínio da empresa XYZ tiver um grupo de usuários chamado *Operadores*, o grupo de usuários no Security Center deverá ser chamado *Operators@CompanyXYZ.com*.

2 Aplique os direitos e privilégios de acesso desejados a esses grupos de usuários.

Após terminar

Adicione os grupos de usuários mapeados para grupos ADFS remotos à lista de grupos de usuários aceitos na sua função ADFS.

Criar Active Directory Federation Services

Para que o Security Center receba declarações de um servidor ADFS, você precisará criar e configurar uma função ADFS no Security Center.

Antes de iniciar

- Todos os servidores ADFS envolvidos na cadeia de confiança devem ser completamente configurados.
- Mapeie os grupos ADFS remotos aceitos para grupos de usuários do Security Center.

O que você deve saber

Serviços de Federação do Active directory (ADFS) é um componente do sistema operacional Microsoft® Windows® que emite e transforma reclamações, e implementa entidades federadas. É também um tipo de função que permite que o Security Center receba reclamações de um servidor externo do ADFS.

Você precisa criar uma função ADFS no Security Center para cada ADFS raiz que você possuir. Em nosso cenário de exemplo, seu servidor ADFS local é o seu ADFS raiz, portanto, você só precisa criar uma função ADFS.

Em uma situação em que você não tem um servidor ADFS local, mas vários servidores ADFS independentes que atuam como *serviços de token de segurança* para o Security Center, você precisará criar uma função ADFS para cada um deles e adicionar uma confiança de parte confiável para o Security Center a cada uma dessas configurações de servidor ADFS.

Para criar uma função ADFS:

1 Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.

2 Clique em **Adicionar uma entidade** ( ) > **Active Directory Federation Services**.

3 Na página **Informações básicas**, insira um nome e uma descrição para a função.

4 Selecione uma **Partição** da qual esta função seja membro e clique em **Próximo**.

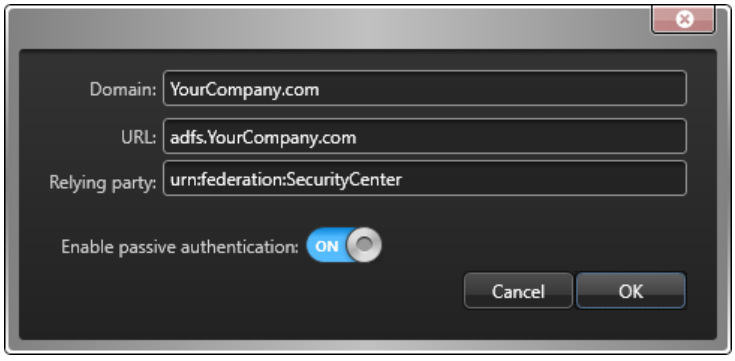
As partições determinam quais usuários do Security Center têm acesso a essa entidade. Somente usuários que receberam acesso à partição podem ver a função ADFS.

5 Clique em **Próximo > Criar > Fechar**.

Uma nova função ADFS ( ) é criada.

6 Clique na aba **Propriedades** e configure a **Cadeia de confiança (domínios)**.

a) Clique em **Adicionar um item** ( ), configure o servidor ADFS e clique em **OK**.



- **Domínio:** Este é o domínio do servidor ADFS local. Exemplo: `YourDomain.com`.
- **URL:** Este é o endereço do documento de metadados do servidor ADFS. É sempre no seguinte formato: `adfs.YourCompany.com`

  Substitua `YourCompany.com` pelo nome do seu servidor ADFS.

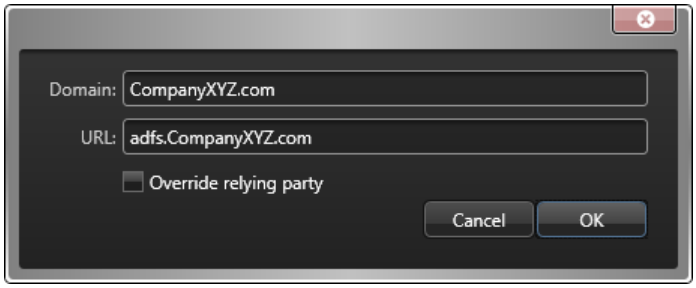
- **Parte confiável:** Esse é o identificador que foi inserido como **Identificador da parte confiável** quando você adicionou a confiança da parte confiável para o Security Center.

  É assim que o Security Center se identifica como a parte de confiança ao servidor ADFS, mesmo quando a função falha para outro servidor.

- **Ativar autenticação passiva:** Selecione esta opção para habilitar o *autenticação passiva* (padrão=OFF).

  IMPORTANTE: O logon de usuário supervisionado não funcionaria se você habilitar a autenticação passiva. Isto acontece porque a autenticação do usuário é processada fora do Security Center.

b) Clique em **Adicionar um item** (), configure o servidor ADFS remoto e clique em **OK**.



- **Domínio:** Este é o domínio do servidor ADFS remoto. Exemplo: `CompanyXYZ.com`. Os usuários desse domínio devem anexar o domínio aos seus nomes de usuário quando fazem logon no Security Center. Exemplo: `johnny@CompanyXYZ.com`.
- **URL:** Este é o endereço do documento de metadados do servidor ADFS remoto. É sempre no seguinte formato: `adfs.CompanyXYZ.com`

  Substitua `CompanyXYZ.com` pelo nome do seu servidor ADFS remoto.

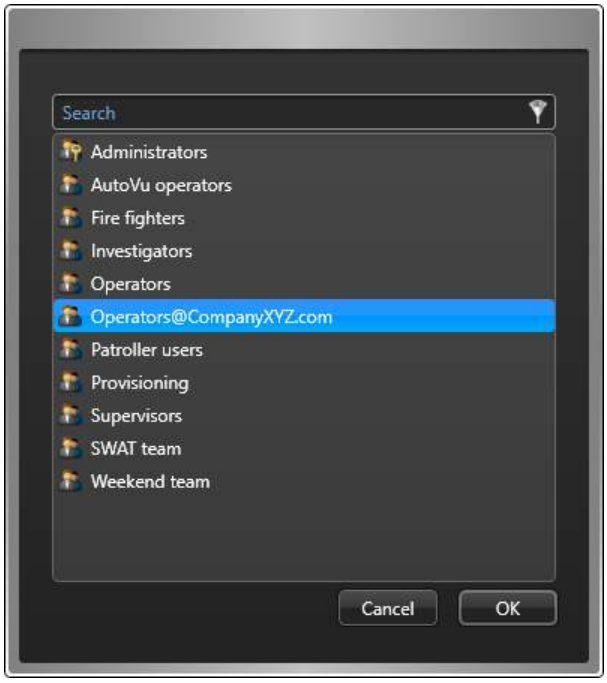
- **Sobrescrever parte confiável:** (Configurações avançadas) Selecione esta opção se o provedor de declarações neste domínio esperar uma audiência diferente na solicitação de token feita pela parte confiável e digite o valor que ele espera.

c) Se você configurou mais de um servidor ADFS remoto como provedores de reivindicações para seu servidor ADFS local, adicione-os agora.

7 Configure os grupos de usuários externos que o Security Center irá aceitar.

a) Na seção *Grupos de usuários aceitos*, clique em **Adicionar um item** ().

b) Na caixa de diálogo exibida, selecione os grupos de usuários mapeados para os grupos do ADFS remoto e clique em **OK**.



Todos os usuários que são membros dos grupos de usuários aceitos devem ser capazes de fazer logon no seu sistema. Todos devem anexar seu nome de domínio após seu nome de usuário para fazer logon. O Security Center não mantém nem valida as suas senhas. O servidor ADFS sim. O Security Center confia neles como usuários autênticos se o ADFS os aceitar.

8 Clique em **Aplicar**.

22

Criptografia de transmissão de fusão

Esta seção inclui os seguintes tópicos:

- "O que é a criptografia de transmissão de fusão?" na página 417
- "Como a criptografia de transmissão de fusão funciona?" na página 419
- "Impacto no desempenho da criptografia de transmissão de fusão" na página 422
- "Boas práticas para gerenciamento de chaves privadas" na página 423
- "Configurar criptografia de transmissão de fusão" na página 425
- "Desabilitar a criptografia de transmissão de fusão" na página 428
- "Impedir que usuários visualizem dados criptografados em uma máquina específica" na página 429
- "Impedir o uso de certificados comprometidos no seu sistema" na página 430
- "Autorizar um cliente a visualizar novos dados de uma câmera criptografada" na página 431
- "Autorizar um novo cliente a visualizar todos os dados de uma câmera criptografada" na página 432
- "Removendo a criptografia de arquivos de vídeo" na página 433

O que é a criptografia de transmissão de fusão?

A criptografia de fluxo de fusão é uma tecnologia proprietária da Genetec Inc. usada para proteger a privacidade de seus arquivos de vídeo. O Archiver usa uma estratégia de criptografia de dois níveis para garantir que somente as máquinas cliente autorizadas possam acessar seus dados privados.

O que é um fluxo de fusão?

Um fluxo de fusão é uma estrutura de dados de propriedade de Genetec Inc. para transmissão de fluxo de multimídia. Cada fluxo de fusão é um conjunto de fluxos de dados (vídeo, áudio e metadados) e fluxos chave relacionados com uma única câmera. As transmissões de fusão são criadas em resposta a solicitações específicas de cliente. As transmissões de chaves estão inclusas somente se as transmissões de dados estiverem criptografadas.

Benefícios da criptografia de fluxo de fusão

Os benefícios da criptografia de fluxo de fusão são os seguintes:

- Nenhum dado capturado pelo Security Center é armazenado ou transmitido como *texto simples*. Isso significa que a privacidade de seus dados está protegida, mesmo se você terceirizar o gerenciamento de seu data center.
- As transmissões de dados são criptografadas usando o padrão de criptografia AES 128-bit aprovado pelo governo dos EUA.
- As chaves usadas para criptografar os fluxos de dados mudam a cada minuto, desencorajando qualquer tipo de ataque de força bruta.
- Cada fluxo de dados é criptografado com um fluxo de chave diferente, reduzindo a superfície de ataque.
- Os fluxos de chaves são criptografados usando *criptografia por chave pública*, garantindo que somente máquinas cliente autorizadas (com uma *chave privada* válida instalada) podem visualizar os dados criptografados.
- Se uma chave privada for comprometida (vazada), você pode evitar que ela seja usada novamente em seu sistema.
- A sobrecarga da criptografia é mantida ao mínimo, criptografando o fluxo de dados apenas uma vez. Archivers auxiliares não precisam criptografar os dados novamente.

Limitações

As limitações da criptografia de fluxo de fusão são os seguintes:

- O multicast da câmera é desativado quando os fluxos de dados devem ser criptografados.
- As gravações na unidade não podem ser criptografadas. Desative a gravação na unidade se desejar criptografia.
- O vídeo criptografado não pode ser visualizado com o Security Center 5.3 e anteriores.
- O vídeo criptografado não pode ser visualizado em dispositivos Security Center Mobile.
- A detecção de movimento por software não está disponível quando a criptografia está ativada.
- As miniaturas não podem ser geradas para vídeo criptografado.
- A criptografia não pode ser adicionada depois que o vídeo foi arquivado.

  No entanto, você ainda pode criptografar seus arquivos de vídeo exportados. Para obter mais informações, consulte o *Guia do Usuário do Security Desk*.

- Novas chaves de criptografia não podem ser adicionadas a dados arquivados, o que significa que a autorização para visualizar dados arquivados não pode ser concedida a novas máquinas.
- Os certificados de criptografia são validados apenas para datas de validade. Isso significa que qualquer certificado que você inscrever entra em vigor imediatamente, independentemente da data de ativação.
- A criptografia não pode ser removida dos arquivos de vídeo.

  A solução é exportar vídeo no formato ASF.
- O vídeo criptografado não pode ser exportado no formato legado G64.

  Quando você exporta vídeo criptografado no formato G64x, o vídeo é exportado com criptografia. Todas as informações necessárias para máquinas de cliente autorizadas para descriptografar o vídeo são encontradas no arquivo G64x.
- O vídeo criptografado não pode ser recuperado se você perder suas chaves particulares.

  Veja Boas práticas para gerenciamento de chaves privadas na página 423.

Tópicos relacionados

Acessar vídeos confidenciais usando cartões inteligentes na página 499

Como a criptografia de transmissão de fusão funciona?

A aplicação da criptografia de transmissão de fusão requer que todas as máquinas clientes autorizadas a ver dados criptografados tenham uma chave privada instalada. A chave privada deve corresponder a um dos certificados de criptografia configurados no Archiver.

Criptografia em dois níveis

O Archiver usa uma estratégia de criptografia de dois níveis para proteger a privacidade de seus dados.

- Criptografia de primeiro nível: O Archiver recebe a transmissão de dados como *texto simples* da câmera. Em seguida, o Archiver criptografa a transmissão de dados usando *chaves simétricas* geradas aleatoriamente que mudam a cada minuto. O fluxo de chaves simétricas é chamado de *transmissão de chave principal*. A transmissão de chave principal é a *primeira chave* necessária para desbloquear os dados privados. Ele é compartilhado por todas as máquinas clientes.
- Criptografia de segundo nível: Para garantir que somente clientes autorizados possam acessar a transmissão de chave principal, o Archiver a protege usando *criptografia por chave pública* (consulte RSA). O Archiver criptografa o fluxo de chaves principal individualmente para cada cliente autorizado, usando uma *chave pública*. Somente o cliente que tem a *chave privada* (correspondente à chave pública) instalada pode desbloquear a transmissão de chave principal (a *primeira chave*). A chave privada é a *segunda chave* necessária para desbloquear os dados privados. Essa chave privada deve ser mantida na máquina cliente.

As chaves públicas e privadas fazem parte de um *certificado de criptografia* que é criado para um cliente específico. O certificado também identifica o cliente. Para ativar a criptografia, o certificado deve ser removido de sua chave privada e entregue ao Archiver. O Archiver então pega a chave pública do certificado para criptografar o fluxo de chaves principal para aquele cliente. Por esse motivo, o fluxo de chave mestre criptografada é chamado de *transmissão de chave específica do cliente*.

Quando o cliente solicita dados criptografados, ele se identifica ao Archiver enviando seu certificado junto com a solicitação de dados. Com base no certificado, o Archiver sabe qual cliente está solicitando os dados e envia o fluxo de chave específico do cliente correspondente ao fluxo de dados criptografados para o cliente. Uma vez que apenas o cliente pretendido tem a chave privada correspondente, apenas o cliente pretendido pode descriptografar as informações.

Resumo

Todos os vídeos que devem ser protegidos devem passar pelo Archiver antes de serem enviados para o cliente solicitante. O Archiver criptografa o vídeo e envia as informações solicitadas agrupadas em um fluxo composto chamado de *transmissão de fusão*. O fluxo de fusão contém os fluxos de dados criptografados e seus fluxos de chave específica do cliente correspondentes.

Se o fluxo de fusão é interceptado por uma parte não autorizada em seu caminho para o cliente pretendido, ele permanece protegido porque a parte não autorizada não tem a chave privada e, portanto, não pode descriptografar os dados contidos dentro.

MELHOR PRÁTICA: É recomendável criar o certificado de criptografia na máquina cliente que solicitará a exibição do vídeo. Isso limita a exposição da chave privada.

Tópicos relacionados

Impedir que usuários visualizem dados criptografados em uma máquina específica na página 429
Autorizar um novo cliente a visualizar todos os dados de uma câmera criptografada na página 432

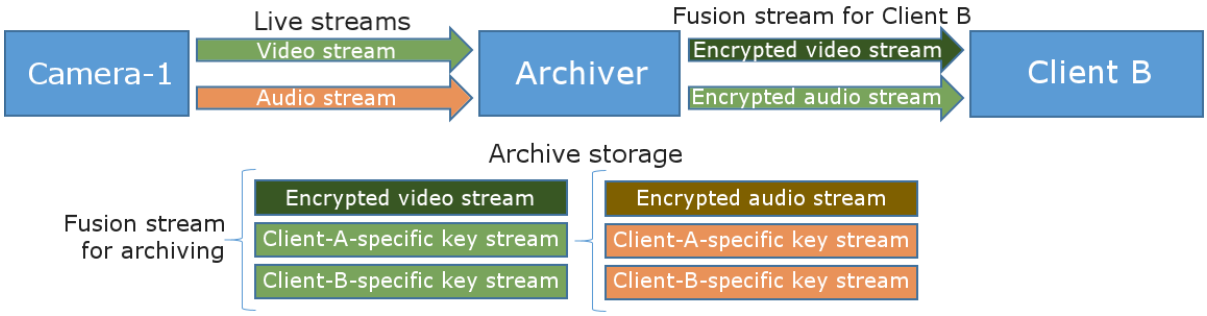
Cenários de criptografia de transmissão de fusão

Quando uma máquina cliente solicita uma transmissão de dados (vídeo, áudio, metadados) de uma câmera criptografada, o Archiver envia uma transmissão de fusão contendo todas as informações que o cliente precisa, e apenas o que ele precisa.

Configuração do cenário

Você quer que todos os vídeos e áudios da Câmera 1 sejam criptografados. Você deseja que o Cliente A e o Cliente B (estações de trabalho) tenham acesso. Primeiro, você solicita e instala um *certificado de criptografia* em cada um deles. Em seguida, ativar a criptografia no Archiver responsável pela Câmera 1, usando os certificados obtidos para o Cliente A e o Cliente B.

O diagrama a seguir ilustra sua configuração com o Cliente B solicitando vídeo da Câmera 1.



O que acontece quando a criptografia está ativada

- A detecção de movimento pelo Archiver na Câmera 1 é desativada.
- O Multicast da Câmera 1 é desativado.
- O Archiver gera um fluxo de fusão para arquivamento, que inclui (ver ilustração):
  - Um fluxo de vídeo criptografado.
  - Um *transmissão de chave específica do cliente* para que o Cliente A possa descriptografar o fluxo de vídeo.
  - Um fluxo de chave específico do cliente para que o Cliente B possa descriptografar o fluxo de vídeo.
  - Um fluxo de áudio criptografado.
  - Um fluxo de chave específico do cliente para que o Cliente A possa descriptografar o fluxo de áudio.
  - Um fluxo de chave específico do cliente para que o Cliente B possa descriptografar o fluxo de áudio.

Cenário: O cliente B solicita apenas vídeo da Câmera 1

- O Cliente B envia uma solicitação de vídeo da Câmera 1 para o Archiver, com seu certificado de criptografia.
- O Archiver responde enviando um fluxo de fusão para o Cliente B, que inclui (ver ilustração):
  - Stream de vídeo criptografado.
  - Chave de stream específica por cliente para o Cliente B descriptografar o vídeo.

Cenário: O cliente B solicita vídeo e áudio da Câmera 1

- O Cliente B envia uma solicitação de vídeo e áudio da Câmera 1 para o Archiver, com seu certificado de criptografia.
- O Archiver responde enviando um fluxo de fusão para o Cliente B, que inclui:
  - Stream de vídeo criptografado.
  - Chave de stream específica por cliente para o Cliente B descriptografar o vídeo.
  - Fluxo de áudio criptografado.
  - Chave de transmissão específica por cliente para o Cliente B descriptografar o áudio.

Impacto no desempenho da criptografia de transmissão de fusão

A criptografia de transmissão de fusão tem impacto no desempenho do Archiver e das estações de trabalho do Security Desk. Talvez seja necessário reavaliar o tipo e o número de máquinas que você precisa se planeja ativar esse recurso.

Impacto da criptografia no desempenho do Archiver

O primeiro certificado de criptografia ativado no Archiver reduzirá a capacidade do Archiver em 30%. Cada certificado de criptografia adicional aplicado a todas as câmeras reduz ainda mais a capacidade de arquivamento em 4%.

Exemplo: Em um Archiver que suporta 300 câmeras sem criptografia:

Número de certificados ativados	Número de câmeras suportadas
0 certificados de criptografia (sem criptografia)	300 câmeras
1 certificados de criptografia	210 câmeras
5 certificados de criptografia	178 câmeras
10 certificados de criptografia	145 câmeras
20 certificados de criptografia	96 câmeras

BEST PRACTICE: Não coloque mais de 20 certificados de criptografia por Archiver.

Impacto da criptografia no desempenho da estação de trabalho

A criptografia de vídeo pode aumentar o uso da CPU em até 40% ao exibir vídeos em baixa resolução (CIF). O impacto torna-se menos perceptível na medida em que a resolução do vídeo aumenta, porque muito mais poder de processamento é gasto na decodificação do vídeo do que na decifração do vídeo. O impacto sobre o desempenho torna-se imperceptível ao visualizar vídeos em HD e Ultra-HD.

Boas práticas para gerenciamento de chaves privadas

A eficácia da criptografia de transmissão de fusão depende de uma infraestrutura de chave pública externa para gerenciar as chaves privadas. Toda a segurança do sistema é baseada no fato de que as chaves privadas permanecem secretas. Assim, a transferência e a manipulação das chaves privadas devem ser feitas de forma segura.

Protegendo as chaves privadas

A maneira mais segura de lidar com um par de chaves pública-privada é gerar os *certificados de criptografia* diretamente na máquina do cliente e, em seguida, atribuir esse certificado (somente a parte da chave pública) para o Archiver responsável por realizar a criptografia. Desta forma, você reduz a superfície de ataque, garantindo que a chave privada nunca deixe a máquina cliente onde ela é usada.

Se você quiser usar a mesma chave privada em várias máquinas cliente, certifique-se de distribuí-la de forma segura. Use uma senha forte para criptografar a chave privada enquanto estiver em trânsito. Para aprender como fazer isso, consulte Importar ou exportar certificados e chaves privadas.

Depois que todas as cópias da chave privada forem instaladas nas máquinas cliente, você pode excluir com segurança os arquivos temporários que foram usados para distribuir a chave privada.

MELHOR PRÁTICA: Se a sua empresa utilizar os Serviços de Domínio do Active Directory (ADDS), recomenda-se usar o mecanismo de Roaming de Credencial, quando as chaves privadas forem associadas a perfis de grupos de usuários em vez de máquinas específicas.

Impedindo a divulgação de chave privada

Você pode se preocupar com os usuários exportarem as chaves privadas de seus computadores clientes. Para reduzir esse risco, você pode seguir qualquer uma dessas práticas recomendadas de *defesa aprofundada*.

- **Marcar as chaves privadas como não exportáveis:** Para impedir que os clientes do Windows extraiam chaves privadas, você pode marcar as chaves privadas como não exportáveis.

  Você define o sinalizador não exportável ao importar um certificado.

  Isso é feito desta forma:

  1. Crie um certificado e exporte as chaves públicas e privadas no formato PFX. Use uma senha forte para criptografar a chave privada.
  2. Importe somente a chave pública para os servidores Archiver.
  3. Importe a chave privada para cada máquina individual e defina a chave privada como não exportável.
     ```
     certutil -importPFX [PFXfile] NoExport
     ```
  4. Quando a chave privada tiver sido importada para todas as máquinas, destrua o arquivo PFX original.

  IMPORTANTE: Há aplicativos de terceiros que não aplicam o sinalizador não-exportável. Como é possível exportar chaves privadas usando esses aplicativos de terceiros, marcar chaves privadas como não exportáveis não é totalmente infalível.
- **Executar a conta de operador em modo não privilegiado:** Você pode impedir que os usuários do Security Desk exportem as chaves privadas instalando os certificados no armazenamento do computador local em vez dos armazenamentos pessoais dos usuários e negando-lhes privilégios de administrador. No entanto, o Security Desk ainda precisa ter acesso às chaves privadas. Isso significa que você precisa executar o Security Desk como administrador e digitar a senha para os usuários do Security Desk.
- **Restringir o uso de aplicativos por meio da Política de Grupo do Windows:** Você pode impedir que os usuários do Security Desk acessem as chaves privadas bloqueando as ferramentas usadas para manipular os certificados, como *certmgr.msi*, através da Política de Grupo do Windows.

Criando um backup de chave particular

Se você perder suas chaves privadas, não poderá recuperar seus dados criptografados. Recomenda-se que você use uma máquina cliente de backup protegida para criar um certificado de criptografia adicional para todos os dados que você criptografa. A chave privada correspondente a este certificado não deve ser usada em qualquer outra máquina cliente. A única finalidade desta máquina de backup é que você tenha uma solução de backup caso todas as chaves privadas usadas em suas máquinas clientes sejam perdidas.

Configurar criptografia de transmissão de fusão

Para configurar criptografia de transmissão de fusão, você precisa solicitar e instalar certificados de criptografia em máquinas autorizadas a visualizar câmeras criptografadas e, em seguida, usar esses certificados para ativar esse recurso no Archiver.

O que você deve saber

A criptografia de fluxo de fusão é para a proteção de sua privacidade de dados. Para proteger seus dados contra violação, consulte Proteção de arquivos de vídeo contra adulteração na página 539.

Para configurar a criptografia de fluxo de fusão:

1. Solicite e instale os certificados de criptografia nas máquinas clientes que têm autorização para acessar os dados privados da sua empresa.
2. Ative criptografia no seu Archiver ou em câmeras individuais.

Solicitando e instalando certificados de criptografia

Para autorizar uma máquina cliente para visualizar dados criptografados, você deve solicitar um certificado de criptografia da máquina cliente, instale o certificado com uma chave privada localmente e dê o certificado somente com a chave pública para o Archiver encarregado da criptografia.

Antes de iniciar

Há muitas maneiras de solicitar e gerenciar *certificados digitais*. Antes de prosseguir, consulte o departamento de TI sobre as políticas e procedimentos padrão seguidos na sua empresa.

O que você deve saber

O certificado de criptografia contém um par de chave pública e particular. A chave pública é usada pelo Archiver para criptografar os dados privados para uma máquina cliente específica. A chave privada é usada pela máquina cliente para descriptografar os dados privados.

MELHOR PRÁTICA: A chave privada nunca deve deixar a máquina onde ela é necessária.

Para solicitar e instalar um certificado de criptografia em uma máquina cliente:

1. Faça logon como um administrador local da máquina cliente.
2. Adicione os snap-in de Certificados à conta de seu computador local.

   Instalar os certificados no armazenamento de computador local dá mais controle sobre o gerenciamento de chaves privadas.
3. Siga o procedimento da sua empresa para solicitar e instalar o certificado.
4. Se o cliente só deve ter acesso a dados criptografados por um tempo limitado, defina a data de expiração do certificado de acordo.
5. Se você não planeja executar o Config Tool a partir deste computador, exporte o certificado apenas com a chave pública para um arquivo de certificado (.cer).

   Salve o arquivo de certificado em um local que possa ser acessado de onde você planeja executar o Config Tool.

Após terminar

Ative criptografia no seu Archiver ou em câmeras individuais.

Tópicos relacionados

Boas práticas para gerenciamento de chaves privadas na página 423

Habilitar a criptografia de transmissão de fusão

Para proteger a privacidade de seus dados, você pode habilitar a criptografia de transmissão de fusão na função Archiver ou em cada câmera.

Antes de iniciar

Solicite e instale os certificados de criptografia nas máquinas clientes que têm autorização para acessar os dados privados da sua empresa.

O que você deve saber

Não é necessário instalar os certificados no servidores do Archiver. Os certificados de criptografia são aplicados ao Archiver pelo Config Tool. Por este motivo, o Config Tool tem de ter acesso aos certificados, a partir do armazenamento de certificados da máquina local ou a partir de arquivos de certificados exportados (.cer).

IMPORTANTE: Para ativar a criptografia, você deve adicionar pelo menos um certificado ao Archiver.

Para ativar a criptografia da fluxo de fusão:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Fazer um dos seguintes:
- Para ativar a criptografia no Archiver, selecione a função Archiver a ser configurada e clique na aba **Configurações padrão da câmera** tab.
- Para ativar a criptografia em uma câmera, selecione a câmera a ser configurada, clique na aba **Gravação** e, em seguida, clique em **Configurações personalizadas**.

3 Clique em **Exibir configurações avançadas** e ative **Criptografia**.
4 Em **Certificados**, clique em **Adicionar um item** ( ).
A caixa de diálogo **Selecionar certificado** aparecerá.
5 Fazer um dos seguintes:
- Se os certificados de criptografia estiverem instalados no computador local, selecione-os na lista **Certificados instalados** e clique em **OK**.
- Se eles não estiverem instalados em seu computador local, faça o seguinte:
  1 Clique em **Pesquisar arquivo de certificado**.
  2 Clique em para abrir a janela do navegador e navegue até a pasta onde os arquivos de certificados estão salvos.
  Como padrão, o navegador procura arquivos **Certificados X.509**. Se você não encontrar os arquivos desejados, procure por arquivos de **Intercâmbio de Informações Pessoais** em vez disso.
  3 Selecione os certificados que deseja e clique em **Abrir**.
  4 Se o arquivo de certificado estiver protegido por senha, clique em e digite a **Senha**.
  5 (Opcional) Clique em **Validar arquivo** para se certificar de que o arquivo selecionado contém uma chave pública.
  6 Clique em **OK**.

6 Clique em **Aplicar**.

O Archiver inicia a criptografia de todos os dados transmitidos das câmeras selecionadas. Somente as estações de trabalho clientes com um ou mais dos certificados configurados instalados localmente podem visualizar os dados gravados a partir deste ponto.

Tópicos relacionados

Desabilitar a criptografia de transmissão de fusão na página 428
Impedir que usuários visualizem dados criptografados em uma máquina específica na página 429
Impedir o uso de certificados comprometidos no seu sistema na página 430

Autorizar um cliente a visualizar novos dados de uma câmera criptografada na página 431
Autorizar um novo cliente a visualizar todos os dados de uma câmera criptografada na página 432
Acessar vídeos confidenciais usando cartões inteligentes na página 499

Desabilitar a criptografia de transmissão de fusão

Você pode desabilitar a criptografia de transmissão de fusão na função Archiver ou nas câmeras individuais.

O que você deve saber

Você pode desabilitar a criptografia de transmissão de fusão desligando a opção **Criptografia** no Archiver ou em uma câmera.

MELHOR PRÁTICA: Não remova os *certificados de criptografia* do Archiver para o caso de querer voltar a ativar a criptografia.

Desabilitar a criptografia da fluxo de fusão

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Fazer um dos seguintes:
   - Para desabilitar a criptografia no Archiver, selecione a função Archiver a ser configurada e clique na aba **Configurações padrão da câmera**.
   - Para desabilitar a criptografia em uma câmera, selecione a câmera a ser configurada, clique na aba **Gravação** e, em seguida, clique em **Configurações personalizadas**.
3 Clique em **Exibir configurações avançadas** e desative **Criptografia**.
4 Clique em **Aplicar**.

O Archiver interrompe a criptografia de todos os dados transmitidos das câmeras selecionadas. Os arquivos de vídeo que foram criptografados no passado permanecem criptografados.

Tópicos relacionados

Removendo a criptografia de arquivos de vídeo na página 433

Impedir que usuários visualizem dados criptografados em uma máquina específica

Se você não quiser mais que as pessoas usem uma máquina cliente específica para acessar os dados de uma câmera criptografada, você pode remover o certificado de criptografia usado para ativar a criptografia de transmissão de fusão naquela câmera a partir daquela máquina.

O que você deve saber

O acesso aos dados das câmeras criptografadas é controlado através dos certificados de criptografia instalados na máquina usada para acessar os dados, ao contrário dos privilégios do usuário. Siga este procedimento somente se você estiver alterando a configuração de uma máquina, e não porque um certificado de criptografia esteja comprometido. Se você acha que a distribuição de um certificado de criptografia foi comprometida, você pode impedir que ele seja usado novamente no seu sistema.

IMPORTANTE: Se esse cliente for a única máquina que pode acessar a câmera criptografada, certifique-se de que ele não perca seu certificado de criptografia (contendo a *chave privada*). Se você perder o certificado, não poderá recuperar os arquivos criptografados dessa câmera. Se você tiver apenas uma máquina que pode exibir a câmera criptografada, siga as práticas recomendadas para gerenciar chaves privadas.

Para impedir um cliente de visualizar dados de uma câmera criptografada:

1. Faça logon na máquina cliente como um administrador local.
2. Adicione os snap-in de Certificados à conta de seu computador local.
3. Exclua os certificados correspondentes às câmeras criptografadas que você não deseja mais ver nesta máquina.
4. Se este cliente é o único que utiliza este certificado, remova também o certificado do Archiver.

   Isso evita que o Archiver execute criptografia desnecessária. Para informações sobre como remover um certificado do Archiver, consulte Impedir o uso de certificados comprometidos no seu sistema na página 430.

O cliente não poderá mais ver os dados novos ou arquivados da câmera enquanto a câmera permanecer criptografada.

Tópicos relacionados

Como a criptografia de transmissão de fusão funciona? na página 419
Impedir o uso de certificados comprometidos no seu sistema na página 430
Autorizar um cliente a visualizar novos dados de uma câmera criptografada na página 431

Impedir o uso de certificados comprometidos no seu sistema

Se suspeitar que um certificado de criptografia foi comprometido, você pode garantir que o certificado nunca seja usado novamente em seu sistema removendo-o do Archiver e excluindo todas as transmissões de chaves que foram geradas com esse certificado.

O que você deve saber

O certificado de criptografia (contendo a *chave privada*) é o que permite a uma máquina cliente consultar o Archiver em busca de dados criptografados e descriptografar a transmissão de chaves e os dados quando são recebidos do Archiver. Para mais informações, consulte Como a criptografia de transmissão de fusão funciona? na página 419

CUIDADO: No Archiver, se você remover o último certificado usado para criptografar uma câmera, a câmera deixa de ser criptografada e todos os dados futuros dessa câmera se tornam acessíveis a todas as máquinas do seu sistema. No entanto, os dados que foram previamente criptografados permanecem criptografados.

Para impedir o uso de um certificado comprometido no seu sistema:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Tome uma das seguintes ações:
   - Se a criptografia estiver configurada no nível do Archiver, selecione o Archiver e clique na aba **Configurações padrão da câmera**.
   - Se a criptografia estiver configurada no nível da câmera, selecione a câmera e clique na aba **Gravação**.
3 Na lista **Certificados**, selecione o certificado comprometido e clique em **Remover o item** ( ).

   NOTA: Você não pode deixar a **Criptografia** ativada se não houver certificados configurados.

4 Clique em **Aplicar**.
5 Na caixa de mensagem que aparece, tome uma das seguintes ações:
   - Clique em **Sim** para excluir o certificado selecionado com as transmissões de chaves associadas (*transmissões de chaves específicas de cliente*).

     MELHOR PRÁTICA: Esta é a escolha recomendada se você souber que seu certificado foi comprometido.

     CUIDADO: Se esse certificado for o único certificado a partir do qual você pode acessar seus dados criptografados, excluí-lo significa que você nunca poderá recuperar seus dados.
   - Clique em **Não** para excluir somente o certificado selecionado do Archiver, sem excluir as transmissões de chaves associadas.

     Esta opção impede o Archiver de gerar novas transmissões de chaves a partir do certificado selecionado. Isso impede que as máquinas clientes afetadas acessem novos dados da câmera criptografada. Isso não impede que os dados que foram arquivados antes desta operação sejam acessados de máquinas nas quais o certificado selecionado está instalado.
6 Clique em **Aplicar**.

Tópicos relacionados

Impedir que usuários visualizem dados criptografados em uma máquina específica na página 429
Autorizar um novo cliente a visualizar todos os dados de uma câmera criptografada na página 432

Autorizar um cliente a visualizar novos dados de uma câmera criptografada

Você pode conceder a uma nova máquina cliente os direitos de acessar os dados futuros de uma câmera criptografada adicionando um novo certificado de criptografia (chave pública) para esse cliente no Archiver responsável por essa câmera.

Antes de iniciar

Adicionar mais certificados de criptografia a um Archiver afeta seu desempenho. Veja Impacto no desempenho da criptografia de transmissão de fusão na página 422.

O que você deve saber

Uma máquina cliente tem acesso a dados criptografados porque o Archiver transmite tanto o fluxo de dados criptografados quanto o fluxo de chaves para o cliente. O fluxo de chaves fornece ao cliente sua primeira chave para desbloquear os dados criptografados. O cliente precisa de uma *segunda chave* para descriptografar a *primeira chave*, que é a sua *chave privada*. Quando você adiciona o certificado do cliente ao Archiver, está pedindo ao Archiver para criar uma nova *primeira chave* que o cliente é capaz de desbloquear.

IMPORTANTE: Se esse cliente for a última máquina que tiver acesso aos dados da câmera criptografada, certifique-se de não perder sua chave particular. Se isso acontecer, você não será capaz de recuperar os arquivos criptografados para essa câmera. Se você estiver nessa situação, siga as práticas recomendadas para gerenciar chaves privadas.

Para autorizar um novo cliente a visualizar os novos dados de uma câmera criptografada:

1 Solicite e instale um certificado de criptografia para a nova máquina cliente.
2 Adicione o novo certificado (chave pública) ao Archiver responsável pela câmera.
Para instruções de como fazer isso, leia Habilitar a criptografia de transmissão de fusão na página 426.

A nova máquina cliente pode acessar quaisquer novos dados da câmera criptografada a partir deste ponto, mas não pode acessar os dados arquivados antes desta operação.

Tópicos relacionados

Impedir que usuários visualizem dados criptografados em uma máquina específica na página 429
Autorizar um novo cliente a visualizar todos os dados de uma câmera criptografada na página 432

Autorizar um novo cliente a visualizar todos os dados de uma câmera criptografada

Você pode conceder a um novo cliente acesso a todos os dados de uma câmera criptografada importando o certificado de criptografia (chave privada) de outro cliente que tenha acesso.

Antes de iniciar

IMPORTANTE: Chaves privadas devem ser tratadas com cuidado. Veja Boas práticas para gerenciamento de chaves privadas na página 423.

Para autorizar um novo cliente a visualizar todos os dados de uma câmera criptografada:

1 Exporte o certificado de uma máquina cliente autorizada com a chave privada.
2 Importe o certificado com a chave privada para a nova máquina cliente.

O novo cliente agora tem todos os direitos de acesso concedidos ao cliente original através do certificado de criptografia importado. Se o cliente original tiver acesso a mais de uma câmera criptografada através deste certificado, o novo cliente também terá acesso.

Tópicos relacionados

Como a criptografia de transmissão de fusão funciona? na página 419
Impedir o uso de certificados comprometidos no seu sistema na página 430
Autorizar um cliente a visualizar novos dados de uma câmera criptografada na página 431

Removendo a criptografia de arquivos de vídeo

Não é possível remover a criptografia dos arquivos de vídeo. No entanto, você pode exportar seus arquivos de vídeo sem criptografia, usando o formato ASF.

Antes de iniciar

Você precisa de um computador cliente autorizado a acessar a câmera criptografada e uma conta de usuário do Security Center que tenha os privilégios *Usar formato ASF* e *Remover criptografia*.

Para exportar vídeo de uma câmera criptografada sem a criptografia:

1 Abra o Security Desk a partir da estação de trabalho cliente autorizada.
2 Exportar o vídeo desejado em formato ASF.
Para obter mais informações sobre a exportação de vídeo, consulte o *Guia do Usuário do Security Desk*.

Vídeo

Esta parte inclui as seguintes chapters:

- "Vídeo em um relance" na página 435
- "Implantação de vídeo" na página 438
- "Câmeras" na página 473
- "Arquivos de vídeos" na página 519
- "Solução de problemas de vídeo" na página 546

23

Vídeo em um relance

Esta seção inclui os seguintes tópicos:

- "Sobre Security Center Omnicast" na página 436
- "Entidades relacionadas à vigilância por vídeo" na página 437

Sobre Security Center Omnicast™

Security Center Omnicast™ é o sistema de gerenciamento de vídeo (VMS) IP que oferece a organizações de todos os tamanhos a habilidade de implementar um sistema de vigilância adaptado às suas necessidades. Com uma ampla gama de câmeras IP, atende à crescente demanda por vídeos HD e análises, o tempo todo protegendo a privacidade individual.

Os principais recursos do Omnicast™ incluem:

- Visualizar vídeo ao vivo e de reprodução de todas as *câmeras*
- Visualizar até 64 fluxos de vídeo lado a lado em uma única estação de trabalho
- Visualizar todas as câmeras em linhas do tempo independentes ou sincronizadas
- Controle PTZ completo usando o teclado do PC ou de CCTV, ou na tela, usando o mouse
- Zoom digital
- Detecção de movimento
- Rastreamento visual: seguir indivíduos ou objetos em movimento por diferentes câmeras
- Pesquisar vídeo por *marcador*, movimentação ou data e hora
- Exportar vídeo
- Proteger vídeo contra exclusão acidental
- Proteger vídeo contra adulteração com o uso de marcas d'água
- Proteger a privacidade de indivíduos no vídeo

O Omnicast™ também oferece suporte a vídeo para *eventos* rastreados por outros sistemas unificados no Security Center.

- Melhorar todos os relatórios de eventos com vídeo ao vivo e de reprodução
- Melhorar o monitoramento de alarmes com vídeo ao vivo e de reprodução
- Melhorar a detecção de intrusão com vídeo ao vivo e de reprodução
- Melhorar o sistema de controle de acesso Synergis™ com vídeo ao vivo e de reprodução
  - Verificação de vídeo: compara *titular de cartão* foto com vídeos ao vivo e de reprodução
  - Consolidar todos os eventos de acesso com vídeo ao vivo e de reprodução
- Melhorar sistema de reconhecimento automático de placas de veículos AutoVu™ com vídeo ao vivo e de reprodução

Entidades relacionadas à vigilância por vídeo

O sistema de vigilância por vídeo suporta muitas das entidades que estão disponíveis no Security Center.

Ícone	Entidade	Descrição
	**Archiver (função)**	Controla as unidades de vídeo e gerencia o arquivo de vídeos.
	**Archiver auxiliar (função)**	Complementa o arquivo de vídeos gerado pelo Archiver. Pode arquivar de qualquer câmera no sistema.
	**Media Router (função)**	Gerencia o roteamento de todas as transmissões de áudio e vídeo na rede.
	**Rede**	Rede (com recursos de transmissão específicos) que o Media Router leva em consideração ao fazer decisões de roteamento.
	**Servidor**	O servidor na sua rede. Usado para hospedar as funções necessárias em seu sistema.
	**Área**	Agrupamento lógico de câmeras e sequências de câmeras.
	**Monitor analógico**	Representa um monitor analógico físico conectado a um decodificador de vídeo.
	**Câmera**	Fonte única de vídeo no sistema. Pode suportar áudio.
	**Câmera (compatível com PTZ)**	Câmera PTZ (câmera de domo).
	**Sequência de câmera**	Ordem predefinida de exibição de sequências de vídeo de forma rotativa dentro de um único ladrilho no Security Desk.
	**Grupo de monitores**	Grupo de monitores analógicos com características comuns.
	**Agenda**	Intervalo de datas e horas, pode suportar períodos diurnos e noturnos.
	**Unidade de vídeo**	Unidade IP incorporando um ou mais codificadores de vídeo.
	**Partição**	Grupo de entidades do sistema visíveis apenas para um grupo de usuários.
	**Usuário**	Indivíduo que utiliza os aplicativos do Security Center.
	**Grupo de usuários**	Grupo de usuários que compartilham características em comum.

24

Implantação de vídeo

Esta seção inclui os seguintes tópicos:

- "Preparar a implementação de seu sistema de vigilância por vídeo" na página 439
- "Implementar seu sistema de vigilância por vídeo" na página 441
- "Sobre Archivers" na página 442
- "Configurar funções Archiver" na página 443
- "Mover a função Archiver para outro servidor" na página 444
- "Sobre unidades de vídeo" na página 446
- "Adicionar unidades de vídeo manualmente" na página 447
- "Definição das configurações padrão de câmeras" na página 449
- "Definir configurações de gravação de câmeras" na página 451
- "Configurar codecs de áudio" na página 453
- "Visualizar estados de gravação de câmeras" na página 454
- "Investigar eventos do Archiver" na página 455
- "Sobre Archivers auxiliares" na página 456
- "Criar Archivers auxiliares" na página 458
- "Adicionando câmeras a Archivers auxiliares" na página 459
- "Definindo configurações de gravação de câmera para um Archiver auxiliar" na página 460
- "Sobre o Media Router" na página 462
- "Configurar a função Media Router" na página 463
- "Adicionar redirecionadores ao Media Router" na página 464
- "Sobre o Media Gateway" na página 469
- "Criar a função Media Gateway" na página 470
- "Configurar a função Media Gateway para receber solicitações de vídeo" na página 471
- "Limitar conexões ao Media Gateway" na página 472

Preparar a implementação de seu sistema de vigilância por vídeo

Para garantir uma implementação sem problemas da vigilância por vídeo, você precisa realizar uma série de passos de pré-configuração.

Antes de implementar seu sistema de vídeo:

1 Tenha um diagrama de rede mostrando todas as redes públicas e privadas usadas na sua organização, seu intervalo de endereços IP, suas capacidades de transmissão de vídeo (Multicast, Unicast UDP e Unicast TCP).

Para redes públicas, você também precisa do nome e do endereço IP público de seus servidores proxy. Consulte seu departamento de TI para obter essas informações.

2 Abra as portas usadas pelo Security Center para comunicar e transmitir vídeo e certifique-se de que elas sejam redirecionadas para fins de firewall e NAT.

3 Instale os seguintes componentes de software do Security Center:

a) Software do servidor Security Center em seu servidor principal.

O servidor principal é o computador que hospeda a função Directory.

b) (Opcional) Software do servidor Security Center em servidores de expansão.

Um servidor de expansão é qualquer outro servidor no sistema que não hospede a função Directory. Você pode adicionar servidores de expansão a qualquer momento.

c) Software de cliente Security Center em pelo menos uma estação de trabalho.

Para obter mais informações sobre a instalação do Security Center, consulte o *Guia de Instalação e Atualização do Security Center*.

4 Tenha uma lista de *partições* (se existirem).

As partições são usadas para organizar seu sistema em sistemas secundários gerenciáveis. Isso é especialmente importante em um ambiente de múltiplos locatários. Se, por exemplo, você estiver instalando um sistema de grande dimensão em um shopping center ou em uma torre de escritórios, você pode querer dar privilégios de administração local aos locatários. Usando partições, você pode agrupar os locatários de modo que eles somente possam ver e gerenciar o conteúdo de suas lojas ou escritórios, mas não os de outros.

5 Tenha uma lista de todos os usuários conhecidos com seus nomes e suas responsabilidades.

Para poupar tempo, identifique os usuários que têm as mesmas funções e responsabilidades e organize-os em grupos de usuários.

NOTA: Para instalações de grande dimensão, os usuários e grupos de usuários podem ser importados de um Active Directory do Windows.

6 Instale e conecte todos os equipamentos de vídeo (unidades de vídeo, câmeras fixas e PTZ) na rede IP da sua empresa, com as seguintes informações:

- Fabricante, modelo e endereço IP de cada unidade de vídeo.
- Credenciais de login (nome de usuário e senha), se aplicável.
- Protocolo de comunicação utilizado (HTTP ou HTTPS).

DICA: Um mapa do local (plantas) mostrando onde as câmeras estão localizadas seria útil.

7 Se você tiver câmeras conectadas a uma matriz de CCTV convencional (*matriz de hardware* no Omnicast), você precisa do seguinte:

- Um sistema Omnicast™ 4.x para gerenciar os codificadores de vídeo conectados às saídas da matriz de CCTV.
- Um sistema Omnicast™ 4.x federado no Security Center.

Após terminar

Implemente seu sistema de vigilância por vídeo.

Tópicos relacionados

Importar grupos de segurança de um Active Directory na página 389
Configurar uma Omnicast Federation na página 229

Implementar seu sistema de vigilância por vídeo

Para integrar uma variedade de recursos de vídeo, você pode implantar seu sistema de vigilância por vídeo assim que as etapas prévias de configuração forem concluídas.

Antes de iniciar

Execute as etapas de pré-configuração.

O que você deve saber

As informações sobre como configurar uma instalação de vídeo típica são descritas aqui. Seu processo pode ser diferente dependendo das exigências específicas de sua instalação.

Para implementar seu sistema de vídeo:

1. Use a conta *Admin* no Config Tool para se conectar ao seu sistema.
2. Crie uma partição para cada grupo de entidades independente.
   Definindo primeiro as partições, você não terá que mover entidades depois de criá-las.
3. Para organizar as entidades no seu sistema (áreas, portas e assim por diante, configure a exibição de área.
4. Configure a função Archiver.
5. Configure seu ambiente de rede.
6. Se necessário, configure funções Archiver adicionais.
7. Configure as funções Archiver auxiliar.
8. Configure a função Media Router.
9. Defina campos personalizados para as entidades do seu sistema.
10. Crie grupos de usuários e crie usuários.
11. Se necessário, proceda à federação de sistemas Omnicast™ remotos.
12. Crie alarmes.

Sobre Archivers

A função Archiver é responsável pelo descobrimento, escolha de status e controle das unidades de vídeo. O Archiver também gerencia o arquivo de vídeo e realiza detecção de movimento quando não for feito na própria unidade.

Todas as comunicações entre o sistema e as unidades de vídeo são estabelecidas através da função Archiver. Todos os eventos gerados pelas unidades (movimento, *análise de vídeo* e assim por diante) são encaminhados pelo Archiver às partes interessadas no sistema. Múltiplas instâncias da função Archiver podem ser criadas no sistema.

Configurar funções Archiver

Para que o seu sistema Security Center gerencie suas câmeras, arquivos de vídeos e detecção de movimentos, você deve configurar a função Archiver.

O que você deve saber

Quando o Omnicast™ está ativado em sua licença, uma função Archiver é criada por padrão e atribuída ao *servidor principal*.

Para configurar a função Archiver:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Selecione a função Archiver a ser configurada e clique na aba **Recursos**.
3 Configure o banco de dados de arquivos.
4 Defina as configurações de armazenamento de arquivos.
5 (Opcional) Altere o servidor host da função.
6 Para continuar a ver vídeo, mesmo que o servidor que hospeda a função Archiver fique offline, configure o failover do Archiver.
7 Adicione as unidades de vídeo que você deseja que esta função Archiver controle.
8 Clique na aba **Extensões** e conclua a configuração das extensões que foram criadas quando você adicionou as unidades de vídeo.

   Para obter uma lista das configurações na aba **Extensões**, consulte Archiver - Aba Extensões na página 1050.
9 Clique na aba **Configurações padrão da câmera** e defina as configurações padrão da câmera para todas as câmeras gravadas por esta função Archiver.

   Para obter uma lista das configurações na aba **Configurações padrão da câmera**, consulte Definição das configurações padrão de câmeras na página 449.
10 Configure as câmeras associadas às unidades de vídeo que você adicionou.
11 Se a gravação for realizada em unidades fixas, configure a transferência de arquivos de vídeo.

Após terminar

Se você tiver um sistema de grande dimensão, você pode distribuir a carga criando mais funções Archiver e hospedando-as em *servidores* separados.

Tópicos relacionados

Sobre Archivers na página 442

Mover a função Archiver para outro servidor

No Security Center, se o servidor que hospeda a função Archiver falhar, for muito lento ou tiver espaço em disco limitado, você pode mover a função para outro servidor sem instalar qualquer software adicional.

Antes de iniciar

Certifique-se de que você tenha outro servidor configurado e pronto para aceitar uma nova função.

O que você deve saber

Cada Archiver é responsável pelos *arquivos de vídeos* das *câmeras* que controla. Os arquivos de vídeos incluem o banco de dados de arquivos e o armazenamento de arquivos, que podem ser hospedados no servidor que hospeda o Archiver ou em um servidor diferente. Ao mover o Archiver para outro servidor, garanta que o novo servidor também tenha acesso a esses arquivos de vídeos.

Para mover a função Archiver para outro servidor:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Selecione a função Archiver a ser configurada e clique na aba **Recursos**.
3 Se o seu servidor atual ainda estiver em execução e o banco de dados de arquivos e o armazenamento de arquivos forem locais para o servidor atual, faça o backup de todo o conteúdo de seus arquivos de vídeo.
   a) Na seção *Transferência de arquivos*, configure temporariamente a pasta de backup em um local acessível pelo novo servidor. Verifique se o local escolhido tem espaço em disco suficiente para armazenar os arquivos de vídeos do seu *Archiver*.
   b) Com as opções a seguir, realize um backup manual:
      - Para o tipo de backup, selecione **Backup**.
      - Para a origem, selecione a função Archiver atual.
      - Para o intervalo de tempo, selecione um intervalo grande o suficiente para incluir todos os arquivos de vídeo.
      - Para os dados, selecione **Tudo desde a última transferência**.
   c) Retorne à tarefa *Vídeo*.
4 Na lista suspensa **Servidor**, selecione o novo servidor.
5 Com base nas características do novo servidor, faça os ajustes necessários aos seguintes:
   - O banco de dados do arquivo
   - As configurações de armazenamento de arquivo.

   IMPORTANTE: Se o novo servidor for o mesmo servidor físico que o antigo (por exemplo, o mesmo servidor mas com GUID diferente no Security Center), não será necessário fazer estes ajustes.
6 Clique em **Aplicar**.
7 Para restaurar os arquivos de vídeos pertencentes a esta função Archiver, considere o seguinte:
   - Se você executou um backup completo, restaure-o com as seguintes opções:
      - Para o tipo de restauração, selecione **Archiver**.
      - Para o Archiver, selecione o Archiver atual.
      - Para o intervalo de tempo, selecione os mesmos horários de início e de término usados para o backup.
      - Para as câmeras que deseja restaurar, selecione tudo.
      - Desligue a opção **Proteger vídeo contra exclusão**.
   - Se seu servidor anterior tiver avariado e todos os seus backups forem anteriores à falha do servidor, restaure todos os arquivos de vídeos até o período de retenção de arquivos do Archiver.

- Se o banco de dados de arquivos e o armazenamento de arquivos permaneceram no mesmo local, como em um terceiro servidor, não será necessário restaurar os arquivos de vídeos.

8 Se você alterou temporariamente a localização da pasta Backup, defina a pasta de volta para seu local original.

9 Clique em **Aplicar**.

Sobre unidades de vídeo

Uma unidade de vídeo é um tipo de dispositivo de codificação e decodificação de vídeo capaz de comunicar-se por uma rede IP e pode incorporar um ou mais decodificadores de vídeo. Os modelos de codificação de ponta também incluem suas próprias capacidades analíticas de vídeo e gravação. Câmeras (com IP ou analógicas), codificadores e decodificadores de vídeo são exemplos de unidades de vídeo. No Security Center, uma unidade de vídeo se refere a um tipo de entidade que representa um dispositivo de codificação ou decodificação de vídeo.

As unidades de vídeo são criadas manualmente, ou então automaticamente pelo Archiver se a unidade suportar *descoberta automática*.

Adicionar unidades de vídeo manualmente

Para monitorar vídeo no Security Center, você deve adicionar unidades de vídeo a um Archiver.

Antes de iniciar

Você deve conhecer o fabricante, o tipo de produto (modelo ou série), o endereço IP e as credenciais de login (nome de usuário e senha) para as unidades que pretende adicionar.

DICA: Se não souber o endereço IP da unidade, você pode usar a *Ferramenta de registro de unidades* para descobri-lo.

O que você deve saber

Se você estiver registrando uma câmera Sharp executando o SharpOS 11.3 ou superior no Archiver, para acessar as transmissões de vídeo da câmera ou se for exigido controle de entrada/saída da unidade de processamento de LPR, você deve configurar a extensão AutoVu™ para permitir autenticação básica. No Config Tool, na aba **Extensões** do Archiver, selecione a extensão do Genetec™ AutoVu™ e desligue **Recusar Autenticação Básica**.

Para adicionar uma unidade de vídeo:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.

2 Clique em **Adicionar uma entidade ( )** > **Unidade de vídeo** .

A caixa de dialogo *Adição manual* se abrirá.

3 Se você tiver várias funções Archiver, selecione a que deseja para gerenciar a unidade na lista suspensa **Archiver**.

4 Selecione o fabricante e o tipo de produto da unidade.

5 Digite o endereço IP e a porta HTTP da unidade.

Para adicionar várias unidades em uma única operação, use um intervalo de endereços IP.

6 Selecione quais credenciais o Archiver usa para se conectar à unidade.

- **Login inicial:** Use as credenciais de login padrão definidas na extensão do fabricante para este Archiver. Se a extensão ainda não tiver sido definida, credenciais em branco serão usadas.
- **Específico:** Digite as credenciais de login específicas usadas por esta unidade. Essa opção pode ser alterada para **Usar login padrão** posteriormente durante a configuração da unidade de vídeo.

7 Se a unidade de vídeo estiver configurada para usar HTTPS, ative **HTTPS** e digite a porta HTTPS da unidade.

8 Conclua todas as outras configurações conforme necessário e clique em **Adicionar**.

Se a extensão do fabricante não existir, ela será criada para você.

Se a câmera adicionada for um codificador com várias transmissões disponíveis, cada transmissão será adicionado com a cadeia de caracteres *Câmera - n* anexa ao nome da câmera, onde *n* representa o número da transmissão. Para uma câmera IP com apenas um fluxo disponível, o nome da câmera não é modificado.

NOTA: Se o fabricante suportar *descoberta automática*, todas as outras unidades presentes no seu sistema que compartilhem a mesma *porta de detecção* são adicionadas automaticamente ao mesmo Archiver, além das adicionadas manualmente.

9 Para atualizar a **exibição da Função**, pressione **F5**.

As novas unidades de vídeo são adicionadas sob a entidade Archiver selecionada.

Após terminar

Se necessário, altere as configurações padrão das unidades de vídeo em suas abas de configuração.

Se estiver a ter problemas ao adicionar uma unidade de vídeo, você poderá solucionar o problemas.

Tópicos relacionados

Unidade de vídeo - Aba Identidade na página 1036
Unidade de vídeo - Aba Propriedades na página 1037
Unidade de vídeo - Aba Periféricos na página 1039

Definição das configurações padrão de câmeras

Você pode usar a aba **Configurações padrão de câmera** para definir as configurações padrão de qualidade de vídeo e de gravação para todas as câmeras controladas por um Archiver.

O que você deve saber

- Quaisquer definições de gravação configuradas no assistente de instalação do Security Center são transferidas para a aba **Configurações padrão de câmera**.
- As configurações de gravação das afetam seu espaço em disco.
- Configurações de gravação definidas na aba **Gravação** de uma câmera individual sobrescrevem as definições da aba **Configurações padrão da câmera**.

Para definir as configurações padrão de gravação de câmeras:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Selecione o Archiver a ser configurado e clique na aba **Configurações padrão da câmera**.
3 Em **Qualidade do vídeo** selecione uma **Resolução**.
   - **Alta:** 1270x720 e superior.
   - **Padrão:** Entre 320x240 e 1280x720.
   - **Baixa:** 320x240 e inferior.
   - **Padrão:** Configurações padrão do fabricante.
   - **Taxa de quadros:** Você pode selecionar um valor entre 1 e 30 fps. Não se aplica às configurações padrão.
4 Na lista suspensa **Modos de gravação**, selecione um dos seguintes:
   - **Contínuo:** Grava continuamente. A gravação não pode ser interrompida pelo usuário ( ).
   - **Em movimento/Manual:** A gravação é desencadeada por uma ação (como *Iniciar gravação*, *Adicionar favorito* ou *Disparar alarme*) por meio de detecção de movimento ou manualmente por um usuário. Neste modo, o botão **Gravar** no Security Desk aparece de uma das seguintes maneiras:
     - Cinza ( ) quando o Archiver não está gravando
     - Vermelho ( ) quando está gravando mas pode ser interrompido pelo usuário
     - Vermelho com um cadeado ( ) quando está gravando mas não pode ser interrompida pelo usuário (gravação com movimento ou alarme).
   - **Manual:** Grava quando disparado manualmente por um usuário. Neste modo, o botão **Gravar** no Security Desk aparece de uma das seguintes maneiras:
     - Cinza ( ) quando o Archiver não está gravando
     - Vermelho ( ) quando está gravando mas pode ser interrompido pelo usuário
     - Vermelho com um cadeado ( ) quando está gravando mas não pode ser interrompida pelo usuário (gravação com movimento ou alarme).
   - **Personalizar:** A gravação é especificada por um agendamento personalizado. Para obter mais informações sobre como criar agendas usando a tarefa *Sistema*, consulte Criando agendamentos na página 199.

     CUIDADO: Agendamentos de gravação do mesmo tipo (por exemplo, dois agendamentos diários) não podem ser sobrepostos, independentemente do modo de gravação configurado para cada um. Quando ocorre um conflito de agendamento o Archiver e as unidades de vídeo são exibidas em amarelo no navegador de entidades e emitem mensagens de alerta de entidades.
   - **Desligado:** A gravação fica desligada ( ), mesmo quando um alarme é disparado.

5 Ajuste as seguintes configurações avançadas de gravação.

- **Gravar áudio:** Ajuste em **Ligado** para gravar áudio com o seu vídeo. Uma entidade de microfone deve estar conectada às suas câmeras. Para mais informações, consulte Definição das configurações de câmera na página 475.
- **Gravar metadados:** Ajuste em **Ligado** para gravar metadados com o seu vídeo.
- **Arquivamento redundante:** Ajuste em **Ligado** para permitir que servidores primários, secundários e terciários arquivem vídeo ao mesmo tempo. Esta configuração só é efetiva se o failover estiver configurado. Para mais informações, consulte Configurar failover do Archiver na página 188.
- **Limpeza automática:** Especifique um período de retenção para o vídeo gravado (em dias). Arquivos de vídeo mais antigos do que esse período são excluídos.
- **Tempo de gravação anterior a um evento:** Use o controle deslizante para definir a duração (em segundos) da gravação antes de um evento. Esse buffer é salvo sempre que começa a gravação, garantindo que o que quer que tenha iniciado a gravação também seja capturado no vídeo.
- **Tempo para gravar após um movimento:** Use o controle deslizante para definir a duração (em segundos) da gravação após um evento de movimento. Durante esse período, o usuário não pode interromper a gravação.
- **Duração inicial de gravação manual:** Use o controle deslizante para selecionar a duração (em minutos) da gravação quando for iniciada manualmente por um usuário ou quando a ação *Iniciar gravação* for desencadeada.
- **Codificação:** Defina como **Ligado** para ativar *criptografia de fluxo de fusão* para todas as câmeras gerenciadas pelo Archiver selecionado. Somente usuários que tenham um ou mais dos **Certificados** listados instalados em suas estações de trabalho podem visualizar vídeo.

  NOTA: Para ativar a **Criptografia**, você deve adicionar pelo menos um *certificado de criptografia* à função Archiver. Para mais informações, consulte O que é a criptografia de transmissão de fusão? na página 417.

6 Clique em **Aplicar**.

Definir configurações de gravação de câmeras

A definição do modo de gravação (contínuo, havendo movimento etc.) ou a ativação de criptografia para as suas câmaras pode ser feita pela aba **Gravação** de cada câmera individual.

Antes de iniciar

Se você estiver usando vários grupos de discos para armazenamento de arquivos, defina temporariamente o *modo de gravação* como Desligado e reative-o no fim do processo. Isso evita que você crie arquivos de vídeo no grupo de discos errado.

O que você deve saber

- As configurações de gravação das câmeras afetam seu espaço em disco.
- Configurações de gravação definidas na aba **Gravação** de uma câmera individual sobrescrevem as definições da aba **Configurações padrão da câmera** do Archiver.

Para definir as configurações de gravação de câmeras:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Selecione a câmera a ser configurada e clique na aba **Gravação**.
3 Na página **Configurações de gravação**, selecione uma das seguintes opções:
   - **Herdar do Archiver:** A câmera herda as configurações de gravação definidas para a função Archiver na aba **Configurações padrão da câmera**.
   - **Definições personalizadas:** A câmera usa suas próprias configurações.
4 Na lista suspensa **Modos de gravação**, selecione um dos seguintes modos de gravação:
   - **Contínuo:** Grava continuamente. A gravação não pode ser interrompida pelo usuário ( ).
   - **Em movimento/Manual:** A gravação é desencadeada por uma ação (como *Iniciar gravação*, *Adicionar favorito* ou *Disparar alarme*) por meio de detecção de movimento ou manualmente por um usuário. Neste modo, o botão **Gravar** no Security Desk aparece de uma das seguintes maneiras:
      - Cinza ( ) quando o Archiver não está gravando
      - Vermelho ( ) quando está gravando mas pode ser interrompido pelo usuário
      - Vermelho com um cadeado ( ) quando está gravando mas não pode ser interrompida pelo usuário (gravação com movimento ou alarme).
   - **Manual:** Grava quando disparado manualmente por um usuário. Neste modo, o botão **Gravar** no Security Desk aparece de uma das seguintes maneiras:
      - Cinza ( ) quando o Archiver não está gravando
      - Vermelho ( ) quando está gravando mas pode ser interrompido pelo usuário
      - Vermelho com um cadeado ( ) quando está gravando mas não pode ser interrompida pelo usuário (gravação com movimento ou alarme).
   - **Personalizar:** A gravação é especificada por um agendamento personalizado. Para obter mais informações sobre como criar agendas usando a tarefa *Sistema*, consulte Criando agendamentos na página 199.

     CUIDADO: Agendamentos de gravação do mesmo tipo (por exemplo, dois agendamentos diários) não podem ser sobrepostos, independentemente do modo de gravação configurado para cada um. Quando ocorre um conflito de agendamento o Archiver e as unidades de vídeo são exibidas em amarelo no navegador de entidades e emitem mensagens de alerta de entidades.
   - **Desligado:** A gravação fica desligada ( ), mesmo quando um alarme é disparado.

5 Ajuste as seguintes configurações avançadas de gravação.

- **Gravar áudio:** Ajuste em **Ligado** para gravar áudio com o seu vídeo. Uma entidade de microfone deve estar conectada às suas câmeras. Para mais informações, consulte Definição das configurações de câmera na página 475.
- **Gravar metadados:** Ajuste em **Ligado** para gravar metadados com o seu vídeo.
- **Arquivamento redundante:** Ajuste em **Ligado** para permitir que servidores primários, secundários e terciários arquivem vídeo ao mesmo tempo. Esta configuração só é efetiva se o failover estiver configurado. Para mais informações, consulte Configurar failover do Archiver na página 188.
- **Limpeza automática:** Especifique um período de retenção para o vídeo gravado (em dias). Arquivos de vídeo mais antigos do que esse período são excluídos.
- **Tempo de gravação anterior a um evento:** Use o controle deslizante para definir a duração (em segundos) da gravação antes de um evento. Esse buffer é salvo sempre que começa a gravação, garantindo que o que quer que tenha iniciado a gravação também seja capturado no vídeo.
- **Tempo para gravar após um movimento:** Use o controle deslizante para definir a duração (em segundos) da gravação após um evento de movimento. Durante esse período, o usuário não pode interromper a gravação.
- **Duração inicial de gravação manual:** Use o controle deslizante para selecionar a duração (em minutos) da gravação quando for iniciada manualmente por um usuário ou quando a ação *Iniciar gravação* for desencadeada.
- **Codificação:** Defina como **Ligado** para ativar *criptografia de fluxo de fusão* para todas as câmeras gerenciadas pelo Archiver selecionado. Somente usuários que tenham um ou mais dos **Certificados** listados instalados em suas estações de trabalho podem visualizar vídeo.

  NOTA: Para ativar a **Criptografia**, você deve adicionar pelo menos um *certificado de criptografia* à função Archiver. Para mais informações, consulte O que é a criptografia de transmissão de fusão? na página 417.

6 Clique em **Aplicar**.

Configurar codecs de áudio

Para assegurar que o áudio é devidamente capturado no Security Center, as unidades de vídeo devem usar um codec de áudio compatível.

O que você deve saber

- O Security Center suporta os seguintes codecs de áudio: G.711, G.721, G.723, AAC (8 kHz ou 16 kHz).
- O Security Center suporta sinais de áudio mono e estéreo. Estes sinais devem ter uma única origem e ser codificados com um dos codecs suportados.
- O Security Center não suporta dois sinais mono independentes e não os mistura para criar um sinal estéreo. A mistura de sinais de dois microfones para obter os canais esquerdo e direito para estéreo deve ser realizada em um mixer de áudio. O áudio misturado forma uma única origem que emite um sinal estéreo. O sinal deve ser codificado com um codec compatível antes de ser importado para o Security Center.
- É possível associar uma pista de áudio a múltiplas câmeras, mas não é possível associar múltiplas pistas de áudio a uma única câmera.

Para configurar o codec de áudio de uma unidade de vídeo:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Selecione a unidade de vídeo a ser configurada e clique na aba **Periféricos**.
3 Clique duas vezes no **Microfone** da unidade de vídeo e selecione um codec de áudio na lista suspensa **Formato de dados**.

NOTA: A lista suspensa **Formato de dados** somente exibe os codecs compatíveis com a unidade de vídeo selecionada.

4 Clique em **Aplicar**.

Visualizar estados de gravação de câmeras

Você pode visualizar o estado de gravação e estatísticas de cada câmera individual controlada por um Archiver ou um Archiver auxiliar para verificar se cada codificador está transmitindo vídeo e áudio atualmente e se a função atualmente está gravando os dados.

Para visualizar o estado de gravação de uma câmera:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.

2 Clique na aba **Recursos**, em seguida clique em **Estatísticas** ( ).

Os campos Câmeras ativas e Câmeras de arquivamento mostram quantas câmeras estão ativas e quantas têm o arquivamento ativado.

3 Clique em **Ver detalhes**.

Na caixa de diálogo *Câmeras de arquivamento*, os estados de gravação das câmeras são listados. Os possíveis estados de gravação são:

- **Gravação inativa:** A gravação está ativada, mas o Archiver não está gravando. Se suspeitar de algum problema, clique na coluna **Descrição**. As possíveis causas são:
  - Perda do banco de dados.
  - Discos cheios.
  - Não é possível gravar em nenhum disco.
- **Gravação ativa:** A gravação foi iniciada por um usuário.
- **Gravação ativa (travada pelo sistema):** A gravação é atualmente controlada pelo Archiver, segundo uma agenda de Havendo movimento ou Contínua.
- **Gravação inativa (travada pelo sistema):** A gravação está atualmente desativada nesta câmera por um agendamento.
- **Gravação prestes a parar:** A gravação foi iniciada por um usuário e está dentro dos últimos 30 segundos de gravação.

Investigar eventos do Archiver

Você pode procurar eventos relacionados a funções Archiver usando o relatório *Eventos do Archiver*.

O que você deve saber

Você pode verificar o status de um Archiver selecionando-o, definindo o intervalo de tempo para uma semana e certificando-se de que não há eventos críticos no relatório. Você também pode solucionar problemas de um Archiver procurando eventos importantes, como *Limiar de carga de disco excedido* ou *Não é possível gravar em nenhum disco*, e ver quando esses eventos ocorreram.

Para investigar eventos do Archiver:

1 Na página inicial, abra a tarefa **Eventos do arquivador** .

2 Definir os filtros de consulta para o relatório. Escolha de um ou mais dos filtros abaixo:

- **Archiver:** Seleciona os Archivers que deseja investigar.
- **Campos personalizados:** Restringir a busca a campo personalizado predefinido para a entidade. Este filtro aparece somente se os campos personalizados estiverem definidos para a entidade e estavam visíveis para você, quando foi criado ou configurado pela última vez.
- **Eventos:** Selecionar os eventos de interesse. Os tipos de evento disponíveis dependem da tarefa que está usando.
- **Carimbo de tempo do evento:** Definir o intervalo de tempo para consulta O intervalo pode ser definido para um período específico ou para unidades de tempo globais, como a semana ou mês anteriores.
- **Descrição:** Restringir a busca a entidades que contêm este string de texto.

3 Clique em **Gerar relatório**.

Os eventos do Archiver são listados no painel de relatório.

Colunas de relatório para a tarefa Eventos do Archiver

Após gerar um relatório, os resultados da sua pesquisa são listados em um painel de relatório. Esta seção lista as colunas disponíveis para a tarefa de relatório relevante.

- **Campos personalizados:** Os campos personalizados predefinidos para a entidade. As colunas aparecem somente se os campos personalizados estiverem definidos para a entidade e se estiver visível para você, quando forem criados ou configurados pela última vez.
- **Descrição:** Descrição do evento, atividade, entidade ou incidente.

  IMPORTANTE: Para cumprir com as leis estaduais, se a opção **Relatório gerado** é usada para um relatório de Trilha de atividade que contém dados LPR, o motivo da pesquisa LPR é incluído no campo **Descrição** .
- **Evento:** Nome do evento
- **Carimbo de tempo do evento:** Data e hora em que o evento ocorreu.
- **Origem (entidade):** O nome do sistema a que a câmera pertence

Sobre Archivers auxiliares

A função Archiver auxiliar complementa o arquivo de vídeo produzido pela função Archiver. Ao contrário da função Archiver, a função Archiver auxiliar não está vinculada a nenhuma *porta de descoberta* particular, portanto, ela pode arquivar qualquer câmera no sistema, incluindo câmeras federadas de outros sistemas do Security Center. A função Archiver auxiliar não pode operar de forma independente; ela necessita da função Archiver para comunicar com unidades de vídeo.

É possível criar múltiplas instâncias desta função no sistema.

Cenários de Archivers auxiliares

Seguem alguns exemplos de cenários onde você precisaria de Archivers auxiliares:

- Você precisa criar uma cópia de alta resolução fora do local (fora de sua LAN corporativa) de seu arquivo de vídeos para câmeras selecionadas. Nesse cenário, você executa o Archiver auxiliar de um local seguro, provavelmente em um servidor localizado em um prédio separado com grande capacidade de armazenamento. O Archiver auxiliar grava transmissões de vídeo de alta qualidade de câmeras específicas usando configurações de gravação (modo, agendas etc.) diferentes das do Archiver.
- Você precisa criar uma cópia de menor qualidade de seu arquivo de vídeos para manter por um período de tempo mais longo. Nesse cenário, você grava a transmissão de vídeo de baixa qualidade com o Archiver auxiliar e define um período de retenção mais longo.
- Você precisa gravar mais câmeras durante as horas em que não há guardas de plantão. Neste cenário, você configura um Archiver auxiliar para arquivar continuamente câmeras durante as horas fora do expediente que também são arquivadas pelo Archiver normal.

Limitações de Archivers auxiliares

Os Archivers auxiliares não podem gravar câmeras que sejam federadas de um sistema Omnicast™ 4.x (através de *Omnicast™ Federation™* ou através de um sistema Security Center remoto que federa um sistema Omnicast™ 4.x).

Diferenças entre Archivers e Archivers auxiliares

A função Archiver e a função Archiver auxiliar possuem várias características diferentes.

A tabela a seguir destaca as diferenças entre o Archiver e o Auxiliary Archiver.

Características	Função Archiver	Função do arquivador auxiliar
Descoberta automática de unidade	Sim, em unidades que a suportam.	Não.
Comando e controle de	Sim.	Não, depende da função Archiver.
Criptografia de comandos através de protocolos seguros (como HTTPS e *SSL*)	Sim, em unidades que a suportam.	Não se aplica.
Câmeras gravadas	Uma câmera só pode ser associada a uma função Archiver.	Uma câmera pode ser associada a vários Auxiliary Archivers.

Características	Função Archiver	Função do arquivador auxiliar
	Só pode gravar câmaras com as quais tem uma conexão direta, normalmente na mesma LAN.	Pode gravar qualquer câmera no sistema, incluindo câmeras federadas, mas somente de sistemas Security Center.
Configurações de gravação	Cada câmera tem a opção de seguir as configurações padrão da função ou suas próprias configurações personalizadas.	Cada câmera tem a opção de seguir as configurações padrão da função ou suas próprias configurações personalizadas.
Fluxo de vídeo gravado	Somente pode gravar a transmissão designada para *Gravação*.	Pode gravar qualquer transmissão de vídeo.
Gravação manual	Sim, quando os agendamentos de gravação Manual estão em vigor.	Não, embora possam ser configuradas agendas de gravação Manual.
Registro de eventos no banco de dados	Sim. Os eventos podem ser pesquisados e visualizados com a tarefa de manutenção de vídeo *Eventos do Archiver*.	Sim. Os eventos podem ser pesquisados e visualizados com a tarefa de manutenção de vídeo *Eventos do Archiver*.
Registro dos eventos em um arquivo simples	Sim. Encontrado na pasta *ArchiverLogs*.	Não.
Backup e restauração do banco de dados	Sim. *Arquivos de vídeo* não são incluídos.	Sim. Arquivos de vídeo não são incluídos.
Compatível com *failover*.	Sim. Um *servidor secundário* pode ser adicionado à função Archiver.	Não se aplica.
Múltiplas cópias do arquivo de vídeo	Sim, por meio de *arquivamento redundante*, mas as cópias mestre e redundante são idênticas porque utilizam as mesmas configurações de gravação.	Sim. Cada Archiver auxiliar um conjunto diferente de arquivos de vídeo que obedecem a configurações de gravação.
Proteção de arquivo de vídeo	Sim.	Sim.
Marca d'água de vídeo	Sim.	Sim.

Criar Archivers auxiliares

Para criar um conjunto de arquivos de vídeo além daqueles gerenciados pela função Archiver, você deve criar um Auxiliary Archiver.

O que você deve saber

A função Auxiliary Archiver não é criada por padrão; ela deve ser criada manualmente.

NOTA: Depois de criar o Auxiliary Archiver, você não deve mover a função para um servidor diferente, a menos que tanto o banco de dados quanto o armazenamento de vídeo estejam configurados em uma máquina separada.

Para criar uma função Auxiliary Archiver:

1 Abra a tarefa **Sistema** e clique na visualização **Funções**.

2 Clique em **Adicionar uma entidade** () > **Archiver auxiliar**.

3 Na página **Informações específicas**, faça o seguinte:

a) (Se você tiver vários servidores no seu sistema) Na lista suspensa **Servidor**, selecione o *servidor* onde esta função será hospedada.

b) Insira o nome do **Servidor de dados** para o banco de dados de arquivos de vídeo.

Um servidor de dados padrão, chamado **(local)\SQLEXPRESS**, é instalado em todos os computadores onde o serviço Genetec™ Server está instalado. Você pode usá-lo ou usar outro servidor de dados em sua rede.

c) Digite o nome de **Banco de dados** do banco de dados de arquivos de vídeo.

CUIDADO: O nome padrão é *AuxiliaryArchiver*. Se o servidor selecionado já estiver hospedando outra instância do Auxiliary Archiver, você deve escolher um nome diferente. Caso contrário, a nova função corromperá o banco de dados existente.

DICA: Você deve usar um nome de banco de dados diferente para cada instância do Auxiliary Archiver, independentemente de haver ou não um conflito, para evitar confusão.

d) Clique em **Próximo**.

4 Na página **Informações básicas**, insira um nome e uma descrição para a função.

5 Selecione uma **Partição** da qual esta função seja membro e clique em **Próximo**.

As partições determinam quais usuários do Security Center têm acesso a essa entidade. Somente usuários que receberam acesso à partição podem ver a função Archiver auxiliar.

6 Clique em **Próximo** > **Criar** > **Fechar**.

A nova função Auxiliary Archiver () é criada. Aguarde alguns segundos para que a função se conecte ao bancos de dados no servidor de dados selecionado.

7 Selecione a aba **Recursos** e configure o servidor e o banco de dados para este Archiver auxiliar.

NOTA: Para cada novo Auxiliary Archiver é atribuído o valor padrão de 558 para sua porta RTSP. Esse valor de porta deve ser exclusivo para todas as funções de arquivamento hospedadas na mesma máquina.

8 Defina as configurações de armazenamento de arquivo.

9 Clique na aba **Gravação de câmera** e defina as configurações padrão da câmera para todas as câmeras gravadas por este Archiver auxiliar. Veja Definindo configurações de gravação de câmera para um Archiver auxiliar na página 460.

10 Clique na aba **Câmeras** e selecione as câmeras que você deseja arquivar.

Tópicos relacionados

Archiver auxiliar - Aba Recursos na página 1058

Adicionando câmeras a Archivers auxiliares

Para que o Archiver auxiliar crie arquivos de vídeo, você deve adicionar câmeras a serem controladas pela função.

O que você deve saber

- Você não pode adicionar câmeras federadas de sistemas Omnicast™ 4.x ao Archiver auxiliar.
- Se você estiver usando o Windows Server 2008 ou anterior, poderá melhorar consideravelmente o desempenho do sistema atribuindo uma porta multicast diferente para cada câmera.

Para adicionar uma câmera ao Archiver auxiliar:

1. Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2. Selecione o Archiver auxiliar, clique na aba **Câmeras** e clique em **Adicionar um item** ( ).
3. Na caixa de diálogo que aparecer, selecione as câmeras que deseja e clique em **OK**.

   NOTA: Leva alguns segundos para que as câmeras selecionadas sejam adicionadas. Se a função não puder adicionar uma câmera no tempo determinado, um status com falha será indicado e a câmera será removida.

4. Clique em **Aplicar**.
5. Para substituir as configurações de gravação padrão em uma câmera:
   a) Selecione a câmera na lista e clique em **Pular para** ( ).
      A página de configuração da câmera é selecionada.
   b) Na aba **Gravação** da câmera, selecione a aba que corresponde ao Archiver auxiliar atual.
   c) Em **Configurações da gravação**, clique em **Configurações personalizadas** e faça as alterações necessárias.
   d) Clique em **Aplicar**.

Removendo câmeras de Auxiliary Archivers

Você pode remover uma câmera do Auxiliary Archiver para que ela não seja mais gravada pelo Auxiliary Archiver.

O que você deve saber

CUIDADO: A remoção de uma câmera do Archiver auxiliar elimina instantaneamente o *arquivo de vídeo* associado do banco de dados do Archiver auxiliar.

Para remover uma câmera de um Auxiliary Archiver:

1. Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2. Selecione o Archiver auxiliar, clique na aba **Câmeras** e clique em **Excluir o item** ( ).
3. Na caixa de diálogo de confirmação que aparece, clique em **Excluir**.

   Todos os registros de arquivo de vídeo desta câmera são excluídos do banco de dados da função.

4. Na seguinte caixa de diálogo de confirmação, faça uma das seguintes opções:
   - Clique em **Não** se quiser manter os *arquivos de vídeo* no disco.

     Isto permite reproduzir os arquivos de vídeo com o *Player de arquivo de vídeo* no Security Desk, mas você não poderá mais consultar o arquivo de vídeo com a tarefa *Arquivos*.
   - Clique em **Sim** se não quiser manter os arquivos de vídeo.

Definindo configurações de gravação de câmera para um Archiver auxiliar

Você pode usar a aba **Gravação da câmera** para definir as configurações de gravação para todas as câmeras controladas por um Archiver auxiliar.

Antes de iniciar

Se você estiver usando vários grupos de discos para armazenamento de arquivos, defina temporariamente o *modo de gravação* como Desligado e reative-o ao fim do processo para evitar criar os arquivos de vídeo no grupo de discos errado.

O que você deve saber

- As configurações de gravação das câmeras afetam seu espaço em disco.
- Configurações de gravação definidas na aba **Gravação** de uma câmera individual sobrescrevem as definições da aba **Configurações padrão da câmera** do Archiver auxiliar.

Para configurar as definições de gravação para câmaras gerenciadas por um Archiver auxiliar:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Selecione o Archiver auxiliar a ser configurado e clique na aba **Gravação da câmara**.
3 Na lista suspensa **Transmissão de vídeo**, selecione a transmissão de vídeo padrão que o Archiver auxiliar deve gravar para cada câmera. As transmissões de vídeo são configuradas para cada câmera.
4 Na lista suspensa **Modos de gravação**, selecione um dos seguintes modos de gravação:
   - **Contínuo:** Grava continuamente. A gravação não pode ser interrompida pelo usuário ( ).
   - **Manual:** Grava quando disparado manualmente por um usuário. Neste modo, o botão *Gravar* do Archiver auxiliar no menu de contexto de ladrilho do Security Desk aparece de uma das seguintes maneiras:
     - Cinza ( ) quando o Auxiliary Archiver não está gravando
     - Vermelho ( ) quando o Auxiliary Archiver está gravando
   - **Personalizar:** A gravação é especificada por um agendamento personalizado. Você pode usar a agenda personalizado que você criou com o assistente de instalação ou clicar em para adicionar uma nova agenda de gravação personalizada que você criou usando a tarefa *Sistema*. Para obter mais informações sobre como criar agendas usando a tarefa *Sistema*, consulte Criando agendamentos na página 199.

     CUIDADO: Agendamentos de gravação do mesmo tipo (por exemplo, dois agendamentos diários) não podem ser sobrepostos, independentemente do modo de gravação configurado para cada um. Quando há um conflito de agendamento o Archiver e as unidades de vídeo são exibidas em amarelo no navegador de entidades e emitem mensagens de alerta de entidades.
   - **Desligado:** A gravação fica desligada ( ), mesmo quando um alarme é disparado.
5 (Opcional) Clique em **Exibir configurações avançadas** para definir configurações avançadas de gravação. Você pode configurar o seguinte:
   - **Gravar áudio:** Ajuste em **Ligado** para gravar áudio com o seu vídeo. Uma entidade de microfone deve estar conectada às suas câmeras para que esta opção funcione. Para mais informações, consulte Definição das configurações de câmera na página 475.

     NOTA: Não é necessário que os dispositivos anexos pertençam à mesma unidade do codificador de vídeo. No entanto, para que a gravação de áudio funcione, garanta que o microfone pertence a uma unidade gerenciada pelo mesmo Archiver, com a mesma extensão Archiver, que o codificador de vídeo.

- **Gravar metadados:** Ajuste em **Ligado** para gravar metadados (como sobreposições) com o seu vídeo.
- **Limpeza automática:** Especifique um período de retenção para o vídeo gravado (em dias). Arquivos de vídeo mais antigos do que esse período são excluídos.

6 Clique em **Aplicar**.

Sobre o Media Router

O Media Router é a função central que comanda todas as solicitações de transmissão (áudio e vídeo) no Security Center. Estabelece sessões de transmissão entre a fonte de fluxo (câmera ou Archiver) e seus solicitantes (aplicativos cliente). As decisões de roteamento são baseadas no local (endereço de IP) e nas capacidades de transmissão de todas as partes envolvidas (origem, destinos, redes e servidores).

O Media Router garante que todos os fluxos de vídeo usem a melhor rota para chegar aos seus destinos, enquanto realizam qualquer transformação necessária (por exemplo, de unicast para multicast ou de IPv4 para IPv6).

A função Media Router tem porta RTSP padrão 554 e seus redirecionadores têm porta RTSP padrão 560 e porta RTP padrão 5004. As funções Archiver têm duas portas RTSP padrão: 555 e 605. Se o Media Router, o redirecionador e o Archiver estiverem hospedados no mesmo servidor, cada uma dessas portas deverá ser exclusiva.

Se várias funções Archiver forem criadas no mesmo servidor, elas deverão ter portas RTSP diferentes. Caso contrário, a entidade da função fica em amarelo e um evento de *Aviso de entidade* é gerado.

Somente uma única instância da função Media Router é permitida por sistema.

Configurar a função Media Router

Você pode definir as configurações da função Media Router para otimizar a taxa de transferência e aumentar a segurança de sua rede privada.

O que você deve saber

Quando o Omnicast™ está ativado em sua licença, uma função Media Router é criada por padrão e hospedada no *servidor principal*. A configuração padrão geralmente é suficiente, a menos que você tenha um sistema complexo envolvendo várias redes privadas.

Para configurar a função Media Router:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.

2 Selecione a função do **Media Router**.

3 (Opcional) Clique na aba **Recursos** e configure o seguinte:

a) Altere o servidor principal da função.

b) Para configurar o failover para o Media Router, adicione um servidor em espera.

4 Clique na guia **Propriedades.**

5 Se o endereço inicial de multicast e as configurações de porta padrão entrarem em conflito com outros aplicativos em seu sistema, selecione um endereço IP ou uma porta diferente nos campos **Endereço inicial de multicast**.

No multicast, todas as fontes de áudio e vídeo são transmitidas para diferentes endereços multicast enquanto usam o mesmo número de porta, porque os switches e roteadores multicast usam o endereço IP de destino para fazer suas decisões de roteamento. Da mesma forma, o Media Router atribui o mesmo número de porta a todos os dispositivos de streaming (microfones e câmeras), começando com o endereço IP especificado e adicionando 1 para cada novo dispositivo encontrado.

6 Para proteger e autenticar pedidos de vídeo RTSP no Security Center, ative a opção **Usar comunicação segura**.

Quando a comunicação segura está ativada, todas as comunicações de vídeo usam RTSP sobre TLS. Se sua rede estiver configurada para Multicast ou Unicast UDP, somente o canal de controle RTSP será criptografado. Se sua rede estiver configurada para Unicast TCP, somente o canal de controle RTSP será criptografado para redirecionamento de vídeo ao vivo. A reprodução de vídeo e exportação de vídeo sempre usa RTSP sobre TCP, portanto, o canal de controle RTSP e o canal de dados de vídeo são ambos criptografados.

IMPORTANTE: A comunicação segura é ativada como padrão em novas instalações, mas desativada se você atualizar de uma versão anterior à 5.5. Quando a comunicação segura está ativada, os sistemas Security Center mais antigos que o 5.5 não podem federar o seu sistema Security Center.

7 Adicione ou altere as configurações do redirecionador.

8 Clique em **Aplicar**.

Tópicos relacionados

Adicionar redes na página 157

Adicionar redirecionadores ao Media Router

Para alcançar clientes em redes remotas ou equilibrar a carga de trabalho de redirecionamento entre vários servidores, você pode criar agentes redirecionadores em servidores adicionais.

O que você deve saber

Redirecionadores são servidores atribuídos para hospedar *agentes redirecionadores*. Um agente redirecionador é um módulo de software lançado pelo Media Router para redirecionar fluxos de dados de uma extremidade IP para outra. O Media Router cria automaticamente um agente redirecionador em cada servidor atribuído a uma função Archiver auxiliar.

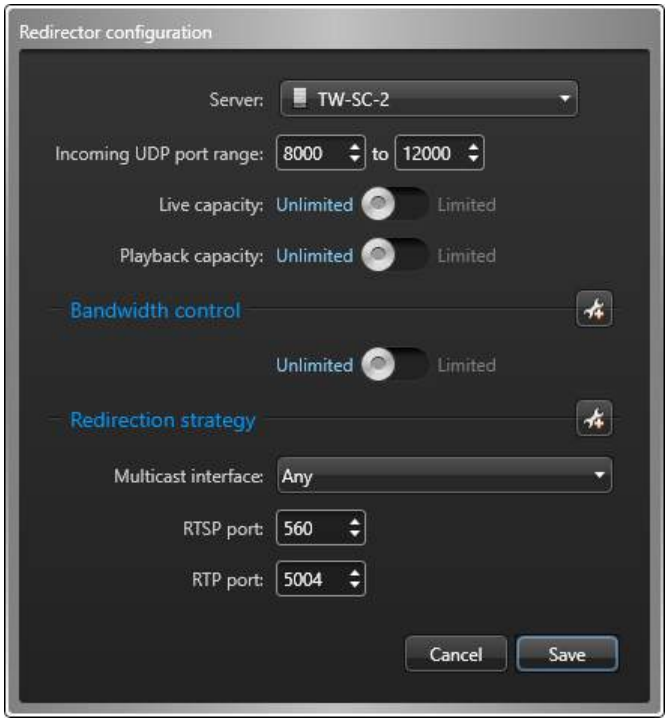
Para adicionar um redirecionador para a Função Media Router:

1 Abra a tarefa *Sistema* e clique na visualização **Funções**.

2 Selecione o Media Router e clique na aba **Propriedades**.

3 Clique em **Adicionar um item** ( ).

4 Na caixa de diálogo *Configuração do redirecionador*, defina as configurações do redirecionador como segue:



- **Servidor:** Servidor selecionado para hospedar o agente redirecionador.
- **Intervalo de portas UDP de entrada:** Intervalo de portas usadas pelo agente redirecionador para enviar vídeo usando *UDP*. Se o agente redirecionador estiver executando por trás de um firewall, certifique-se de que essas portas estejam desbloqueadas para pacotes de entrada para conexões UDP.
- **Capacidade de vídeo ao vivo:** Limita o número máximo de streams ao vivo que podem ser redirecionadas por este servidor (redirecionador). Este recurso impede a sobrecarga do servidor com excesso de usuários que tentam visualizar simultaneamente o vídeo que precisa de redirecionamento. Quando o limite é alcançado, uma mensagem de erro é exibida no aplicativo cliente quando os usuários solicitam o vídeo ao vivo, afirmando que a capacidade de stream foi ultrapassada.
- **Capacidade de reprodução:** Limita o número máximo de reproduções de streams que podem ser redirecionadas por este servidor (redirecionador). Este recurso impede a sobrecarga do servidor com excesso de usuários que tentam visualizar simultaneamente o vídeo que precisa de

redirecionamento. Quando o limite é alcançado, uma mensagem de erro é exibida no aplicativo cliente quando os usuários tentam solicitar reprodução do vídeo, afirmando que a capacidade de stream foi ultrapassada.

- **Controle de largura de banda:** Limita a largura de banda máxima para streams de vídeo que podem ser redirecionados por este servidor (redirecionador). Você também pode configurar um novo limite de largura de banda para vídeo ao vivo e de reprodução. Este recurso impede a sobrecarga da rede com excesso de streams de vídeo vindos de um local remoto que tenha largura de banda limitada.

  Quando o limite é alcançado e os usuários solicitam uma nova transmissão de vídeo, uma mensagem é exibida afirmando que o limite de largura de banda foi ultrapassado. Se o limite de largura de banda for alcançado e um usuário com um alto *nível de usuário* solicitar um stream, o usuário com o nível de usuário mais baixo que estiver visualizando o vídeo que está sendo redirecionado desse redirecionador perde sua conexão de stream de vídeo. Se vários usuários com o mesmo nível de usuário estiverem exibindo streams de vídeo redirecionados, o usuário que solicitou o stream de vídeo por último perde a conexão do stream.
- **Estratégia de redirecionamento:** Se você tiver múltiplas placas de rede, você poderá especificar as ações realizadas em cada placa de rede. Por exemplo, você pode querer especificar que a exportação de vídeo e a transferência de vídeo somente possam ser realizadas por sua placa de rede sem fio. Para mais informações, consulte Configurar o uso de placas de rede para um redirecionador on page 465.

  NOTE: Por padrão, todas as ações são realizadas em todas as placas de rede disponíveis.
- **Interface de multicast:** Adaptador de rede a usar para streaming de dados no modo multicast.
- **Porta RTSP:** Porta usada pelo agente redirecionador para receber comandos TCP.

  NOTE: Se você configurar o agente redirecionador no servidor que hospeda o Media Router, a porta RTSP não pode ser a mesma usada pelo Media Router.
- **Porta RTP:** Porta usada pelo agente redirecionador para stream de dados de vídeo ao vivo usando TCP.

5 Clique em **Salvar** > **Aplicar**.

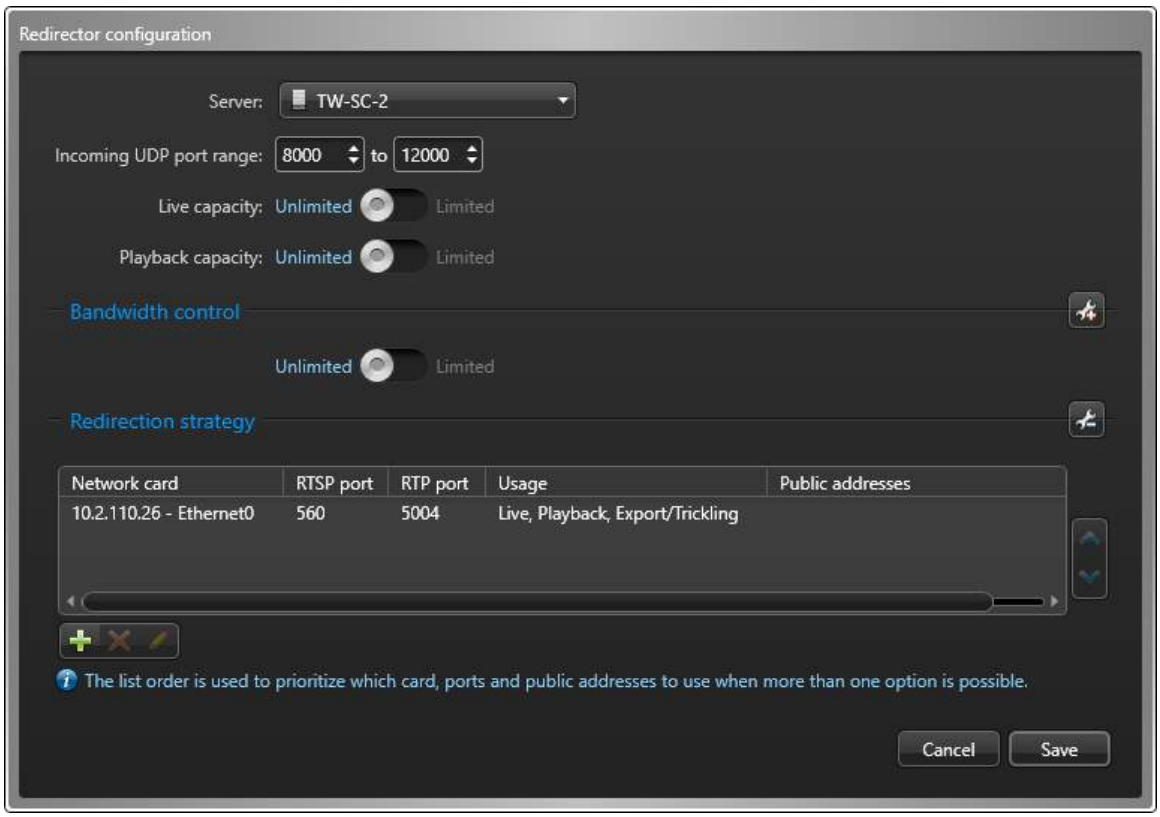
Configurar o uso de placas de rede para um redirecionador

Você pode configurar um redirecionador para usar placas de rede diferentes para ações específicas. Por exemplo, você pode especificar que a exportação e a transferência de vídeo somente possam ser realizadas por sua placa de rede sem fio. Você também pode atribuir vários endereços públicos à mesma placa de rede para tirar partido de várias opções de rede.

Para configurar o uso da placa de rede para um redirecionador:

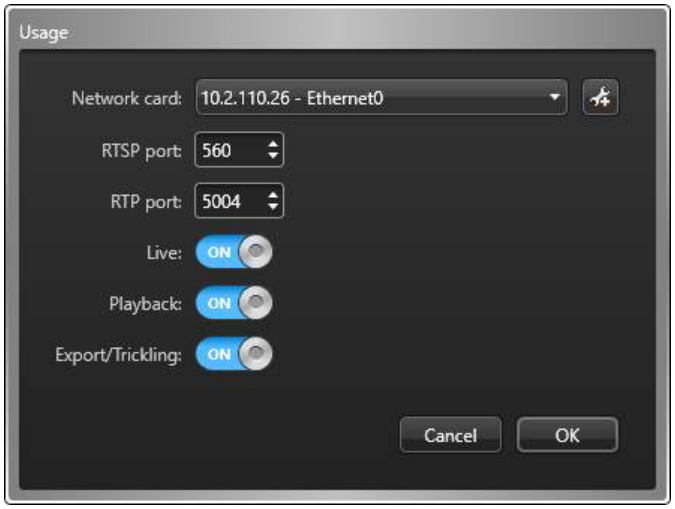
1 Abra a tarefa *Sistema* e clique na visualização **Funções**.
2 Selecione o Media Router e clique na aba **Propriedades**.
3 Na lista **Redirecionadores**, selecione o redirecionador que deseja configurar e clique em **Editar o item** ( ).

  A janela *Configuração do redirecionador* se abre.
4 Ao lado de *Estratégia de redirecionamento*, clique em **Avançado** ( ).



5 Clique em **Adicionar** ( ).

6 Na caixa de diálogo *Uso*, selecione a placa de rede que deseja configurar.



7 Digite a **porta RTSP** (canal de controle) e a **porta RTP** (canal de dados).

8 Ative as ações que você deseja atribuir à placa de rede selecionada. Pode escolher entre as seguintes opções:

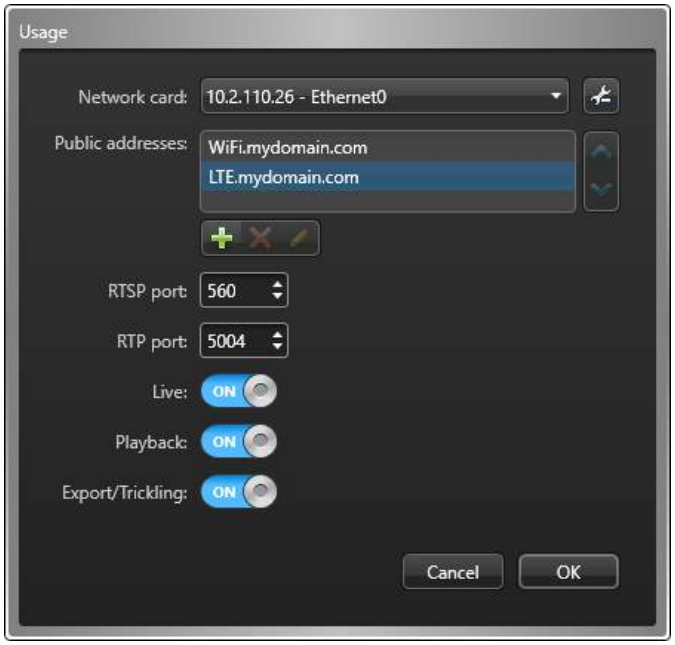
- **Ao vivo**
- **Reprodução**
- **Exportação/Trickling**

IMPORTANTE: Não é possível adicionar a mesma combinação de placa de rede e porta duas vezes; a combinação de placa de rede e número de porta deve ser exclusiva. Para a mesma placa de rede, ambos os números de porta devem ser diferentes.

9 Para configurar vários endereços públicos para a mesma placa de rede, clique em **Adicionar sobrescrita de endereço público** ( ).

Esta configuração poderá ser necessária se um sistema Security Center autônomo estiver instalado em um veículo em movimento, como um trem ou um ônibus. O sistema no veículo é federado por um sistema central no terminal principal. Quando o veículo está longe do terminal principal, o sistema central comunica com o sistema remoto através da rede celular. Quando o veículo está perto do terminal principal, o sistema central muda para a rede Wi-Fi porque é mais barato e tem maior largura de banda.

10 Clique em **Adicionar** ( ) para adicionar endereços públicos.



IMPORTANTE: Se você decidir sobrescrever o endereço público do redirecionador configurado no Server Admin, garanta o seguinte:

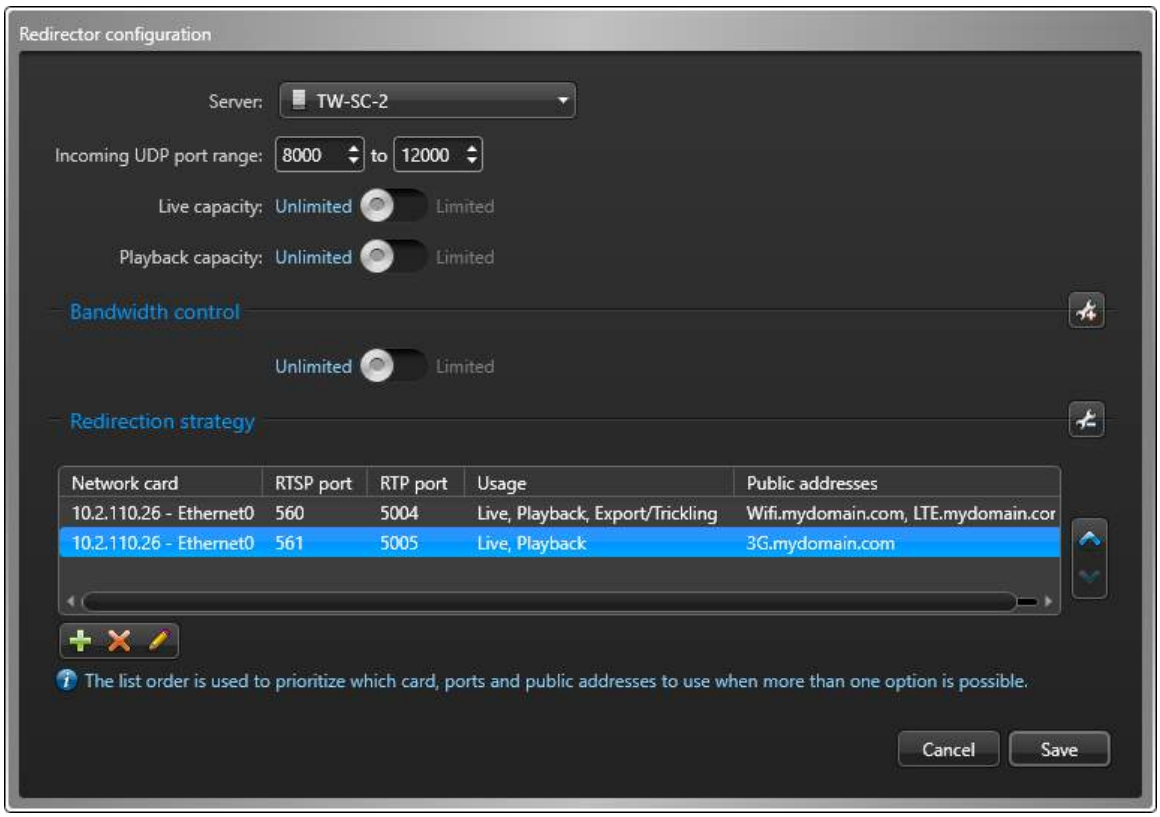
- A rota de rede sendo usada está definida para pública (**O uso de endereço privado** está desligado). Veja Criar conexões diretas entre redes na página 157.
- O endereço público no seu redirecionador está configurado. Veja Server Admin - Página Servidor de expansão na página 107.

11 Clique em **OK**.

12 (Opcional) Altere a prioridade da placa de rede.

a) Na janela *Configuração do redirecionador*, selecione uma placa na lista **Placas de rede**.

b) Clique nos botões ou para movê-lo para a parte superior ou inferior da lista.



No exemplo mostrado na captura de tela, o redirecionador está equipado com apenas uma placa de rede. Se for solicitado vídeo ao vivo ou de reprodução desse sistema, o Media Router sempre tenta a rede Wi-Fi primeiro, seguida da rede LTE e, depois, da rede 3G. Para exportação e trickling de vídeo, somente as redes Wi-Fi e LTE podem ser usadas.

13 Clique em **Salvar** > **Aplicar**.

- Para editar as configurações de uma placa de rede, selecione-a na lista de placas de rede e clique em **Editar o item** ( ).
- Para excluir uma placa de rede, selecione-a na lista de placas de rede e clique em **Excluir** ( ).

Sobre o Media Gateway

O Media Gateway é uma função usada pelo Web Client do Security Center e aplicações externas para solicitar vídeo ao vivo e reprodução usando o Real Time Streaming Protocol (RTSP), e receber transmissões de vídeo puras a partir de câmeras gerenciadas por sistemas do Security Center.

Existem muitos usos para fluxos de vídeo não processados (não decodificados). Por exemplo, um sistema externo pode usar os fluxos de vídeo não processados para executar análises de vídeo e eventos de disparo. Outro aplicativo pode exibir vídeo em uma página da Web usando um visualizador disponível comercialmente que suporte a codificação específica da câmera.

NOTA: A função Media Gateway não suporta transmissões federadas do Omnicast™.

O Media Gateway inclui os seguintes recursos:

- Suporta o padrão RFC 2326.
- Requer uma licença válida que forneça uma ou mais transmissões RTSP, conforme indicado pela opção de licença *Número de transmissões RTSP*.
- Uma única instância dessa função é permitida por sistema.
- A função pode ser atribuída a vários servidores para distribuição de carga.
- O vídeo ao vivo e de reprodução pode ser solicitado, mas fluxos que não sejam de vídeo, como áudio, comandos PTZ, sobreposições e metadados não são suportados.
- A porta RTSP padrão é 654.

Criar a função Media Gateway

Para solicitar vídeo ao vivo e de reprodução e receber transmissões de vídeo não processado usando o protocolo RTSP, você deve primeiro criar o Media Gateway em Config Tool.

Antes de iniciar

Certifique-se de que:

- A função *Gateway de mídia* não exista anteriormente no seu sistema.
- A opção **Número de transmissões RTSP** em sua licença do Security Center suporte ao menos uma transmissão.
- A função *Media Router* esteja ativa em seu sistema.

Para criar a função Media Gateway:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Clique na seta próximo a **Unidade de vídeo** e, em seguida, clique em Media Gateway.
3 Na página *Informações básicas*, digite um **Nome de entidade** e (opcional) uma **Descrição da entidade**.
4 Selecione uma **Partição** existente ou crie uma nova.
A função Media Gateway é criada na partição selecionada.
5 Clique em **Criar** para adicionar a função Media Gateway em seu sistema.
6 Clique em **Fechar**.

Após terminar

Configure a função Media Gateway.

Configurar a função Media Gateway para receber solicitações de vídeo

Para solicitar vídeo ao vivo e de reprodução e receber transmissões de vídeo não processado usando o protocolo RTSP, você deve primeiro configurar o Media Gateway no Config Tool.

Antes de iniciar

Crie a função *Gateway de mídia* em seu sistema.

Para configurar a função Media Gateway:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Na árvore de entidades, selecione a função Media Gateway e clique na aba **Recursos**.
3 (Opcional) Altere o servidor primário da função.
4 Para configurar a distribuição de carga para o Media Gateway, adicione servidores à função.
   a) Na lista **Servidores**, clique em **Adicionar um item** ( ).
      Aparece uma caixa de diálogo listando todos os servidores restantes em seu sistema ainda não atribuídos à função.
   b) Selecione o servidor que deseja adicionar e clique em **Adicionar**.
   As solicitações RTSP têm agora a carga balanceada entre os servidores listados.
5 Clique na guia **Propriedades.**
6 Certifique-se que o **Endereço multicast inicial** padrão e as configurações de porta não entrem em conflito com outras funções, como Archivers, redirecionadores etc. e aplicativos no seu sistema.
   No multicast, todas as fontes de vídeo são transmitidas para diferentes endereços multicast enquanto usam o mesmo número de porta, porque os switches e roteadores multicast usam o endereço IP de destino para fazer suas decisões de roteamento. De igual forma, o Media Gateway atribui o mesmo número de porta a todas as câmeras de transmissão, começando com o endereço IP especificado e adicionando 1 para cada nova câmera encontrada.
7 Se a **porta RTSP** padrão entrar em conflito com outras funções ou outros aplicativos em seu servidor, selecione um número de porta diferente.
   NOTA: A porta RTSP padrão é 654.
8 Se a **Autenticação de usuários** estiver ativada, configure os usuários que podem autenticar solicitações de vídeo feitas por aplicativos cliente RTSP. Recomenda-se ativar esta opção para fins de segurança; no entanto, você pode desativá-lo se souber que sua rede é segura.
   NOTA: As câmeras que um aplicativo cliente RTSP pode exibir no sistema dependem da conta de usuário que o cliente usa para fazer logon no Security Center. Atribua uma senha a cada conta de usuário adicionada à lista, de preferência uma senha diferente da usada no Security Center.
9 Clique em **Aplicar**.

Após terminar

Consulte a *Documentação do Kit de Desenvolvimento de Software do Security Center* para obter detalhes sobre o envio de solicitações de vídeo RTSP.

Limitar conexões ao Media Gateway

Você pode limitar o número de conexões ao vivo e de reprodução simultâneas que a função Media Gateway aceita gerando um arquivo de configuração (gconfig).

O que você deve saber

- Se você salvar o arquivo gconfig na máquina que hospeda a função Media Gateway, a configuração é encaminhada para todas as máquinas de Agente. Se necessitar de uma configuração exclusiva em uma máquina de Agente específica, você pode salvar um arquivo gconfig modificado na máquina de Agente.
- Ambas as conexões RTSP e interface Web são incluídas no número total de conexões.

Para limitar as conexões ao Media Gateway

1 Crie o seguinte arquivo *mediagateway.gconfig* , onde *n1* é o número máximo de conexões ao vivo simultâneas e *n2* é o número máximo de conexões de reprodução simultâneas que o Media Gateway aceita.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <MediaGateway MaximumLiveSessionCount="n1" MaximumPlaybackSessionCount="n2"></
MediaGateway>
</configuration>
```

NOTA:

- O valor padrão é *0* e permite um número ilimitado de conexões.
- Um valor negativo evita qualquer conexão.

2 Salve o arquivo *mediagateway.gconfig* na pasta de instalação do Security Center.

Em uma máquina de 64 bits, a localização padrão é *C:\Program Files (x86)\Genetec Security Center 5.7\ConfigurationFiles*.

NOTA:

- Salvar o arquivo na máquina que hospeda a função Media Gateway configura essa máquina e todas as máquinas de Agente.
- Salvar o arquivo em uma máquina de Agente somente configura essa máquina.

3 Reinicie a função.

NOTA:

- Se você tiver salvo o arquivo gconfig na máquina que hospeda a função Media Gateway, reinicie a função.
- Se você tiver salvo o arquivo gconfig em uma máquina de Agente, reinicie a máquina.

25

Câmeras

Esta seção inclui os seguintes tópicos:

- "Sobre as câmeras (codificadores de vídeo)" na página 474
- "Definição das configurações de câmera" na página 475
- "Configurar transmissões de vídeo de câmeras" na página 477
- "Aumentar a qualidade de gravação de vídeo em eventos importantes" na página 479
- "Alterar endereços multicast de câmeras" na página 481
- "Alterar portas multicast de câmeras" na página 482
- "Testar configurações de transmissão de vídeo de câmeras" na página 483
- "Sobre a detecção de movimento" na página 485
- "Configuração da detecção de movimento" na página 487
- "Teste de configurações de detecção de movimento" na página 490
- "Ajustar configurações de cor da câmera" na página 492
- "Sobre a proteção de privacidade" na página 493
- "Configurar proteção de privacidade" na página 495
- "Sobre rastreamento visual" na página 500
- "Configurar o rastreamento visual" na página 501
- "Visualizar configurações de câmeras" na página 502
- "Configurar motores PTZ" na página 504
- "Definir níveis de usuário para controlar motores PTZ" na página 508
- "Sobre sequências de câmeras" na página 509
- "Criar sequências de câmeras" na página 510
- "Sobre monitores analógicos" na página 511
- "Configurar monitores analógicos" na página 512
- "Câmeras usadas junto ao corpo" na página 514
- "Configurar câmeras usadas junto ao corpo " na página 515

Sobre as câmeras (codificadores de vídeo)

Uma entidade de câmera representa uma única fonte de vídeo no sistema. Essa fonte pode ser uma câmera IP ou uma câmera analógica que esteja conectada ao decodificador de vídeo de uma unidade de vídeo. Vários streams de vídeo podem ser gerados a partir da mesma fonte de vídeo.

Um codificador de vídeo é um dispositivo que converte uma fonte de vídeo analógico para um formato digital, usando um algoritmo de compressão padrão (H.264, MPEG-4 ou M-JPEG). O codificador de vídeo é um dos muitos dispositivos encontrados em uma unidade de vídeo.

Cada codificador de vídeo pode gerar um ou vários fluxos de vídeo usando diferentes esquemas e formatos de compressão para diferentes usos. Em uma câmera IP, a câmera e o codificador de vídeo são uma unidade inseparável, e os dois termos são geralmente usados de forma intercambiável.

As câmeras (ou os codificadores de vídeo) são criadas automaticamente quando você adiciona as unidades de vídeo de que fazem parte ao Security Center.

Sobre transmissões de vídeo

A maioria dos codificadores de vídeo e câmeras IP suportados pelo Security Center podem gerar várias transmissões de vídeo a partir da mesma origem de vídeo.

Quando uma câmera possui várias transmissões de vídeo, você pode definir diferentes configurações de qualidade de vídeo para a transmissão de monitoramento ao vivo e a transmissão de gravação. Transmissões adicionais também podem ser configuradas para outras necessidades, como baixa largura de banda para acesso remoto ou transmissões de baixa resolução vs alta resolução.

Cada fluxo de vídeo é definido pelas seguintes configurações:

- **Qualidade do vídeo:** A qualidade da transmissão de vídeo, composta por parâmetros como resolução de imagem, *taxa de bits*, taxa de quadros e assim por diante, que variam dependendo do fabricante. A qualidade de vídeo pode ter várias configurações para diferentes *agendas*. A qualidade do vídeo afeta diretamente a largura de banda e o espaço em disco para arquivamento.
- **Uso do stream:** A finalidade da transmissão de vídeo, e quando ela é usada: para vídeo ao vivo, gravações e assim por diante.
- **Configurações de rede:** O tipo de conexão específico e endereço *multicast* que são configurados para a transmissão, com base no uso da transmissão e na sua configuração de rede.

Seleção automática de fluxo

A exibição de vídeo em alta resolução exige muitos recursos da CPU. Para exibir o número máximo de transmissões simultâneas de vídeo ao vivo no Security Desk, o uso da CPU deve ser otimizado.

Você pode configurar o Security Desk para usar o modo de transmissão de vídeo *Automático*. Quando este modo é selecionado, o Security Desk exibe a transmissão em *Baixa resolução* ou *Alta resolução*, dependendo do tamanho do ladrilho selecionado. O fluxo de vídeo que tem uma resolução de imagem igual ou inferior à área de exibição do ladrilho é selecionado.

A transmissão de vídeo também se altera dinamicamente quando o usuário redimensiona a janela do Security Desk ou altera o *padrão do ladrilho*.

NOTA: Quando o modo *Automático* é selecionado como a transmissão de visualização padrão no Security Desk, a transmissão em *Alta resolução* sempre é usada quando um ladrilho é maximizado ou quando o zoom digital está em uso.

Para obter mais informações sobre como alterar a transmissão ao vivo padrão no Security Desk, consulte o *Guia do Usuário do Security Desk*.

Definição das configurações de câmera

Para um desempenho ideal, defina as configurações da câmera após as unidades de vídeo terem sido adicionadas ao Security Center.

O que você deve saber

O Security Center oferece configurações padrão; porém, é recomendado que você reveja cuidadosamente a configuração de cada entidade para obter os melhores resultados.

NOTA: Para câmeras federadas, somente as configurações nas abas **Identidade** e **Rastreamento visual** são editáveis.

Para configurar uma câmera:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Selecione a câmera para configurar.
3 Configure as transmissões de vídeo que o codificador deve gerar.
4 Defina configurações de gravação específicas para a câmera.

   Se você não definir configurações específicas para a câmera, ela seguirá as configurações de gravação das funções de arquivamento (Archiver e Archivers auxiliares) que a controlam.

   NOTA: Se uma câmera tiver sido configurada para transferência de arquivos, a gravação somente pode ser configurada usando a respectiva página Web.

5 Defina as configurações de detecção de movimento da câmera.
6 (Opcional) Defina as configurações de proteção de privacidade da câmera.

   NOTA: A aba **Proteção de privacidade** somente é apresentada se você tiver uma licença de proteção de privacidade.

7 Ajuste os atributos de vídeo da câmera (brilho, contraste, matiz, saturação) para levar em consideração diferentes horas do dia.
8 Configure o Rastreamento visual para que os usuários possam alternar para câmeras adjacentes clicando em uma câmera em um ladrilho do Security Desk.
9 Clique na aba **Hardware** e associe dispositivos de hardware à câmera se eles não estiverem integrados.
   - **Motores PTZ:** Configure o motor PTZ.
   - **Microfones:** Selecione um microfone na lista suspensa **Microfone**.
   - **Alto-falantes:** Selecione um alto-falante na lista suspensa **Alto-falante**.
   - **Rotação da imagem:** Use esta configuração para corrigir a orientação da imagem quando a câmera estiver montada de cabeça para baixo ou com um ângulo de 90 graus. Este método utiliza a capacidade da câmera para rodar a imagem.
     - Este recurso somente está disponível se ele for compatível com o hardware da câmera.
     - As opções de rotação variam de acordo com o modelo da câmera.
     - É preferível utilizar o recurso *Rotação da imagem* em vez de *Rotação do vídeo* se isso não interferir na taxa de quadros de vídeo.
   - **Rotação do vídeo:** Use esta configuração para corrigir a orientação da imagem quando a câmera estiver montada de cabeça para baixo ou com um ângulo de 90 graus. Este método utiliza Security Center para rodar o vídeo.
     - Usar a *Rotação do vídeo* coloca carga extra sobre as estações de trabalho clientes, por isso é preferível usar a *Rotação da imagem* se ela estiver disponível para a câmera.
     - Este recurso não está disponível para câmeras PTZ ou câmeras que usem lentes panomórficas (olho de peixe).

10 Se a câmera incluir lentes intercambiáveis, selecione o **Tipo de lente** correto.
11 Clique em **Aplicar**.
12 Teste as definições de vídeo que você configurou.

Após terminar

Você pode copiar as configurações que você definiu para esta câmera para outras câmeras do mesmo modelo.

Configurar transmissões de vídeo de câmeras

Antes de começar a monitorar o vídeo no Security Desk, você deve decidir como deseja usar cada transmissão de vídeo e definir as configurações apropriadas para ela.

O que você deve saber

Cada definição de fluxo de vídeo afeta sua largura de banda e armazenamento de arquivo. Você deve encontrar um equilíbrio entre qualidade, uso de CPU e espaço em disco.

O Security Desk só muda para uma resolução mais alta quando isso faz diferença na visualização dos usuários. Portanto, certifique-se que a transmissão *Ao vivo* tenha uma resolução melhor do que a transmissão de *Baixa resolução* e que a transmissão de *Alta resolução* tenha melhor resolução do que a transmissão *Ao vivo*.

Para configurar os fluxos de vídeo de uma câmera:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Selecione a câmera a ser configurada e clique na aba **Vídeo**.
3 Se a câmera suportar vários fluxos de vídeo, selecione uma guia de fluxo de vídeo na parte inferior da aba **Vídeo**.
4 Na seção **Qualidade de vídeo**, defina as configurações de qualidade de vídeo (resolução, taxa de quadros e assim por diante) para a transmissão de vídeo selecionada.
5 Na seção **Uso da transmissão**, especifique a finalidade da transmissão de vídeo selecionada.

   NOTA: Um fluxo pode ser atribuído a todas, algumas, ou nenhuma das opções de uso. Um fluxo que não tem uso atribuído não é gerado pelo codificador de vídeo, que conserva CPU na unidade.

   - **Ao vivo:** Transmissão padrão para ver vídeos ao vivo no Security Desk.
   - **Gravando:** Stream gravado pelo Archiver para futura investigação.

     DICA: A qualidade do fluxo de gravação pode ser aumentada temporariamente quando a gravação é acionada por certos tipos de eventos.
   - **Remoto:** Stream utilizado para ver vídeos quando a largura de banda de internet é limitada.
   - **Baixa resolução:** Transmissão utilizada em vez da transmissão *Ao vivo* quando o ladrilho utilizado para visualizar a transmissão no Security Desk é pequeno.
   - **Alta resolução:** Transmissão utilizada em vez da transmissão *Ao vivo* quando o ladrilho utilizado para visualizar a transmissão no Security Desk é grande.

6 Na lista suspensa **Tipo de conexão**, na seção **Rede**, selecione como a comunicação entre o Archiver e a câmera é estabelecida para enviar ou receber transmissões de vídeo:
   - **Melhor disponível:** Permite que o Archiver selecione o melhor tipo de conexão disponível para o stream. Os melhores tipos disponíveis são classificados nesta ordem, de acordo com a disponibilidade:
     - Multicast (não disponível para o fluxo de gravação).
     - UDP
     - TCP
     - RTSP sobre HTTP
     - RTSP sobre TCP
   - **UDP Unicast:** Força o stream a ser enviado em UDP para o Archiver. O stream deve ser formatado usando o protocolo RTP.
   - **TCP Unicast:** Força o envio da transmissão em *TCP* para o Archiver. Aqui, TCP é considerado no sentido amplo. Para alguns tipos de câmeras, o Archiver estabelece uma conexão TCP com a unidade e recebe a transmissão em um protocolo exclusivo. Para outros, o stream é enviado sobre HTTP.

Tipicamente, a transmissão não é formatada de acordo com o protocolo RTP pela unidade. O Archiver precisa converter o stream para o protocolo RTP para ser arquivada ou retransmitida ao sistema.

- **Fluxo RTSP sobre HTTP:** Este é um caso especial de conexão TCP. O Archiver usa o protocolo RTSP para solicitar o stream por um túnel HTTP. O stream é enviado de volta por esse túnel usando o protocolo RTP. Este tipo de conexão é usado para minimizar o número de portas necessárias para se comunicar com uma unidade. Normalmente, esse é o melhor modo de solicitar o stream quando a unidade está por trás de um NAT ou firewall, pois as solicitações enviadas a portas HTTP são facilmente redirecionadas por eles.
- **Fluxo RTSP sobre TCP:** Este é outro caso especial de conexão TCP. O Archiver usa o protocolo RTSP para solicitar o stream em TCP. A solicitação é enviada à porta RTSP da unidade.

7 Clique em **Aplicar**.
8 Configure os outros fluxos de vídeo disponíveis na câmera.

Tópicos relacionados

Câmera - Aba vídeo na página 989
Aumentar a qualidade de gravação de vídeo em eventos importantes na página 479

Aumentar a qualidade de gravação de vídeo em eventos importantes

Para fornecer suporte adequado para investigações futuras de filmagens de vídeo, você pode aumentar a qualidade de vídeo da transmissão de gravação quando ocorrerem eventos importantes.

O que você deve saber

Para economizar espaço de armazenamento, a transmissão de vídeo usada para gravação é geralmente de menor qualidade (menor taxa de quadros ou menor resolução de imagem) do que a transmissão usada para exibição ao vivo.

As configurações de *Aumentar qualidade na gravação de eventos* têm prioridade sobre as configurações de *Aumentar qualidade na gravação manual*. A duração do aumento da qualidade do vídeo depende do tipo de evento e das configurações de gravação das câmeras.

Para aumentar a qualidade de gravação de vídeo em eventos importantes:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Selecione a câmera a ser configurada e clique na aba **Vídeo**.
3 Coloque em **Ligado** uma ou ambas as configurações de aumento da qualidade:
   - **Melhorar a qualidade na gravação manual:** Aumenta temporariamente a qualidade de vídeo quando um usuário do Security Desk inicia manualmente a gravação clicando no botão *Gravar* (⚫) ou o botão *Adicionar marcador* ().
   - **Melhorar a qualidade na gravação de evento:** Aumenta temporariamente a qualidade de vídeo quando a gravação é acionada por um evento do sistema: a ação *Iniciar gravação* foi executada, um *alarme* foi acionado ou ocorreu um evento de movimento.
4 Na seção *Qualidade de vídeo*, defina as configurações de aumento de qualidade.
5 Clique em **Aplicar**.

Aumentar a qualidade de gravação de vídeo manualmente

Você pode aumentar a qualidade de vídeo do fluxo de gravação usando uma ação manual.

Antes de iniciar

As configurações de qualidade de vídeo para a transmissão de gravação durante o *Aumento de qualidade na gravação manual* e *Aumento da qualidade na gravação de eventos* devem ser definidas na aba **Vídeo** da câmera.

O que você deve saber

Quando a qualidade do vídeo é aumentada através de uma ação, as configurações personalizadas de aumento de qualidade substituem as configurações gerais para gravação de eventos até que você desencadeie outra ação ou até que o Archiver seja reiniciado.

Para aumentar a qualidade de gravação de vídeo manualmente:

1 Na bandeja de notificação do Security Desk, clique em **Ações instantâneas** ().
2 Na caixa de diálogo *Ações instantâneas*, clique em **Ação manual**.
3 Na janela *Configurar uma ação*, selecione um dos seguintes tipos de ação e selecione uma câmera:
   - **Substituir com qualidade de gravação manual:** Defina a opção **Aumentar qualidade de gravação manual** como **Ligado**.

- **Sobrepor com a qualidade de gravação do evento:** Defina a opção **Aumentar qualidade de gravação de eventos** como **Ligado**.

4 Clique em **OK**.

As configurações personalizadas de aumento de qualidade de gravação de vídeo são aplicadas à câmera selecionada.

5 Para retornar às configurações normais de qualidade de gravação de vídeo:

a) Na bandeja de notificação, clique em **Ações instantâneas** ().
b) Na caixa de diálogo *Ações instantâneas*, clique em **Ação manual**.
c) Selecione a ação **Qualidade da gravação como configuração padrão** e selecione uma câmera.
d) Clique em **OK**.

Alterar endereços multicast de câmeras

Se você tiver falta de endereços de multicast, você pode usar o mesmo endereço de multicast para várias câmeras e atribuir um número de porta diferente a cada uma.

O que você deve saber

Uma vez que um endereço multicast e número de porta são automaticamente atribuídos a uma unidade de vídeo quando ela é descoberta, você só precisa editar os endereços multicast quando você não tem suficiente deles (certos switches são limitados a 128).

NOTA: Usar o mesmo endereço multicast em vários codificadores é menos eficiente do que usar um endereço diferente para cada codificador, porque causa mais tráfego de rede.

Para alterar o endereço multicast de um codificador de vídeo:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Selecione a câmera a ser configurada e clique na aba **Vídeo**.
3 Na seção **Configurações de rede**, digite o **Endereço multicast** e o número da porta que deseja usar.

   NOTA: Todos os endereços multicast devem ser dentro do intervalo entre 224.0.1.0 e 239.255.255.255.

4 Clique em **Aplicar**.
5 Para reiniciar a unidade de vídeo, selecione a unidade na visualização de funções e unidades e clique em **Reinicializar** () na barra de ferramenta, na parte inferior do espaço de trabalho.

Tópicos relacionados

Alterar portas multicast de câmeras na página 482

Alterar portas multicast de câmeras

Se você estiver usando o Windows Server 2008 ou anterior, e tiver um grande número de câmeras transmitindo em multicast, poderá melhorar o desempenho do sistema atribuindo um número da porta multicast diferente para cada câmera em seu sistema.

O que você deve saber

O Windows Server 2008 e versões anteriores usam muitos recursos de CPU para processar pacotes multicast quando eles estão na mesma porta. Por padrão, o sistema apenas incrementa o endereço de multicast atribuído a cada codificador de vídeo que descobrir e não os números de porta. Você deve também alterar o número da porta se usar frequentemente o multicast. Por exemplo, se você usar Archivers auxiliares ou se tudo for gravado em multicast.

Para alterar a porta multicast de um codificador de vídeo:

1. Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2. Selecione a câmera a ser configurada e clique na aba **Vídeo**.
3. Na seção *Configurações de rede*, ao lado de **Endereço multicast**, configure o número da porta que deseja usar.
4. Clique em **Aplicar**.
5. Para reiniciar a unidade de vídeo, selecione a unidade na visualização de funções e unidades e clique em **Reinicializar** ( ) na barra de ferramenta

Tópicos relacionados

Alterar endereços multicast de câmeras na página 481

Testar configurações de transmissão de vídeo de câmeras

Depois de configurar as câmeras, verifique se as configurações de vídeo estão corretas e se você pode ver a câmera.

Para testar as configurações de vídeo de uma câmera:

1 Abra a tarefa **Vídeo** e clique duas vezes na câmera que deseja testar.

A caixa de diálogo *Vídeo ao vivo* é aberta e mostra estatísticas ao vivo sobre a transmissão de vídeo vindo do codificador de vídeo.

2 Se você configurou várias transmissões de vídeo, clique na lista suspensa **Stream**para selecionar uma transmissão diferente para exibição: ao vivo, gravação e assim por diante.

3 Se você tiver configurado transmissões separadas de **Alta resolução** e **Baixa resolução**, selecione **Automático** na lista suspensa **Stream** e redimensione a caixa de diálogo *Vídeo ao vivo* para testar se a seleção de transmissão muda automaticamente.

4 Se você estiver tendo problemas de transmissão, clique em **Exibir informações de diagnóstico** para exibir informações de diagnóstico como uma sobreposição transparente no vídeo.

5 Para capturar essas informações para enviá-las para o Suporte Técnico, clique em **Copiar para a área de transferência**.

6 Para ocultar as informações de diagnóstico, clique em **Fechar**.

Sobre a detecção de movimento

A detecção de movimento é o recurso que busca mudanças em uma série de imagens de vídeo. A definição do que constitui um movimento em um vídeo pode ser baseada em critérios altamente sofisticados.

Existem dois tipos de detecção de movimento:

- **Detecção de movimentos por software:** A detecção de movimento é executada pelo *Archiver* na transmissão de vídeo definida para gravação e os eventos de movimento são gerados pelo Security Center.
- **Detecção de movimento por hardware:** A detecção de movimento é executada pela *unidade de vídeo* e os eventos de movimento são gerados pela unidade e enviados ao Security Center.

As capacidades suportadas diferem entre os dois tipos, conforme mostrado na tabela abaixo.

Capacidade	Software	Hardware
Definir configurações de detecção de movimento	Config Tool	Ferramenta de configuração proprietária da unidade[1]
Tarefa de pesquisa de movimento em Security Desk	Sim	Consulte a nossa Lista de dispositivos suportados[2]
Mostra indicadores de movimento (barras verdes) na linha do tempo durante a reprodução de vídeo	Sim	Consulte a nossa Lista de dispositivos suportados[2]
Múltiplas zonas de detecção de movimento	Sim	Específico da câmera[3]
Exige recursos adicionais de servidor	Sim	Não
Calibração automática da sensibilidade[4]	Sim	Não

IMPORTANTE:

1 Para facilitar a configuração da detecção de movimento por hardware, os blocos de movimento derivados da detecção de movimento por software são mostrados em Config Tool.
2 Algumas câmeras suportam a detecção de movimento como parte de suas capacidades analíticas de vídeo.
3 Nem todas as unidades suportam múltiplas zonas de detecção de movimento. Se você alterar a detecção de movimento de **Archiver** para **Unidade**, as configurações de zona existentes não suportadas pela unidade são perdidas.
4 A unidade e o Archiver poderão interpretar a sensibilidade de forma diferente, portanto, testar as suas zonas de movimento no Config Tool pode não refletir com precisão o comportamento da unidade.

Para configurar a detecção de movimento, você deve especificar áreas da imagem de vídeo, sensibilidade de movimento e uma agenda que estabeleça quando aplicar configurações de detecção de movimento. Cada câmera possui uma configuração de detecção de movimento padrão baseada na agenda **Sempre**. A configuração de detecção de movimento padrão pode ser modificada, mas não excluída.

Quando uma transmissão *H.264* é selecionada como a transmissão de gravação, o botão **Configurações avançadas** fica disponível. Clicar neste botão abre a caixa de diálogo *Configurações avançadas de detecção de movimento para H.264*, que pode ser usada para refinar as configurações de detecção de movimento.

Bloco de movimento

Um *bloco de movimento* ocorre quando é detectado movimento dentro de um dos blocos que você configurar na imagem de vídeo. Há movimento positivo em uma imagem de vídeo quando a área coberta pelo bloco detecta movimento em dois quadros de vídeo consecutivos. O número de blocos de movimento detectados representa a quantidade de movimento. Um bloco de movimento é representado por uma sobreposição quadrada verde semitransparente na imagem de vídeo.

Detecção de movimento positiva

Ver blocos de movimento no vídeo não significa necessariamente que o sistema gerará um evento relacionado ao movimento. Pode ser apenas ruído. Para determinar quando o movimento começou (evento *Movimento ativo*) e parou (evento *Movimento inativo*), ajuste os parâmetros *Sensibilidade*, *Ocorrências de quadros consecutivos*, *Limiar de movimento ativo* e *Limiar de movimento inativo* para conseguir os melhores resultados no ambiente específico.

Práticas recomendadas para configurar a detecção de movimento

O objetivo principal em usar a detecção de movimento é minimizar requisitos de armazenamento, tempos de pesquisa e tempos de obtenção, reduzindo a quantidade de gravações de vídeo que deve ser salva. No entanto, a configuração da detecção de movimento deve ser feita com cuidado e para cada câmera. Ao configurar a detecção de movimento, considere o seguinte:

- É preferível ter configurações sensíveis que possam acionar falsos eventos de movimento do que perder gravações esperadas quando as configurações não são suficientemente sensíveis.
- Todas as configurações de movimento são armazenadas no banco de dados do Directory, portanto, certifique-se de fazer backup do banco de dados quando forem feitas alterações.
- A detecção de movimento é a capacidade de análise de vídeo mais básica. Devido a possíveis falsos eventos de movimento, ela não deve ser usada para acionar alarmes em situações críticas, por exemplo em substituição a um sistema especializado de detecção de intrusão.
- Se você definir o parâmetro **Tempo de gravação antes de um evento** para um valor alto, isto aumenta os recursos de memória (RAM) exigidos pelo Archiver. Isso reduz a contagem de câmeras permitida no Archiver. As câmeras com uma resolução mais alta têm o mesmo efeito sobre os recursos de memória.

Ao configurar a detecção de movimento por software:

- É sempre possível usar transmissões MJPEG.
- É possível usar transmissões MPEG-4.
- Também é possível usar transmissões H.264, mas por causa da noção de *perfis*, algumas câmeras devem ser configuradas pela caixa de diálogo adicional *Configurações avançadas de detecção de movimento H.264*.

Para obter instruções de pré-configuração ou quaisquer etapas de configuração adicionais necessárias para habilitar a detecção de movimento no Security Center para unidades de vídeo específicas, consulte o *Guia de Configuração de Unidades de Vídeo do Security Center*.

Configuração da detecção de movimento

Para monitorar e relatar o movimento detectado em uma imagem de câmera, você deve configurar a detecção de movimento para a unidade de vídeo.

Antes de iniciar

Certifique-se de que a unidade suporta a detecção de movimento.

O que você deve saber

A detecção de movimento pode ser realizada pelo Archiver ou pela unidade, em toda a imagem de vídeo (padrão) ou apenas em determinadas áreas (zonas de movimento).

MELHOR PRÁTICA: Para fluxos H.264 e MPEG-4, a detecção de movimento por software é realizada pela análise de quadros P-. Certifique-se de que a sua transmissão de vídeo não é composta apenas de quadros-chave ao definir as configurações de *Intervalo de quadros chave* e *Taxa de quadros* da câmera.

Para saber mais sobre como configurar a detecção avançada de movimento, assista nosso Webinar de GTAP.

Para configurar a detecção de movimento:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Selecione a câmera a ser configurada e clique na aba **Detecção de movimento**.
3 Coloque a opção **Detecção de movimento** em **Ligado**.
4 Na opção **Detecção feita em**, selecione se a detecção de movimento é realizada pelo Archiver ou pela unidade de vídeo.
5 Na opção **Sensibilidade**, selecione a quantidade de diferença que deve ser detectada em um *bloco* entre dois quadros consecutivos antes de ser destacado como um *bloco de movimento*.

   Uma imagem simples, como a visualização de uma parede vazia, é mais propensa a gerar ruído do que uma imagem contendo muitos detalhes.

   DICA: Primeiro, defina um valor alto e, em seguida, baixe-o lentamente até que você esteja recebendo somente algumas falsas leituras de movimento na imagem.

   Você também pode calibrar a sensibilidade automaticamente.

6 Na opção **Ocorrências consecutivas do quadro**, selecione quantos quadros em sequência o *Limiar de movimento* ativo deve ser alcançado para gerar uma ocorrência positiva de movimento.
7 Defina as zonas de detecção de movimento.
8 Defina os critérios de detecção de movimento para cada zona de movimento da seguinte forma:

   Se esses valores forem muito baixos, o movimento será detectado com muita frequência. Se esses valores estiverem muito próximos, você pode receber muitos eventos de *Movimento ativo* e *Movimento inativo* consecutivos.

   - **Limiar de movimento ativo:** Indica o número mínimo de *blocos de movimento* que devem ser detectados antes que o movimento seja significativo o suficiente para ser relatado. Juntamente com as *Ocorrências de quadros consecutivos*, uma detecção de movimento positiva é feita.
   - **Limiar de desativação por movimento:** O fim do movimento é detectado quando o número de blocos de movimento cai abaixo do *Limiar de movimento inativo* por, pelo menos, 5 segundos.

9 Selecione os tipos de eventos que você deseja gerar quando o movimento for detectado para cada zona de movimento.

Tópicos relacionados

Câmera - Aba Detecção de movimento na página 994
Solução de problemas: problema de sensibilidade da câmera Axis P1428-E na página 574

A detecção de movimento não está funcionando no Security Center na página 575
Câmeras Axis não têm uma aba de Detecção de movimento na página 576

Calibrar automaticamente a sensibilidade da detecção de movimento

Você pode determinar o que constitui detecção de movimento positiva, calibrando automaticamente o valor de sensibilidade.

Antes de iniciar

Verifique se não há movimento no campo de visão da câmera (0 blocos de movimento).

O que você deve saber

Se a câmera estiver localizada no exterior, a precisão deste teste pode ser afetada devido ao vento, movimentação de árvores e assim por diante.

Para definir automaticamente a sensibilidade de detecção de movimento:

1 Abrir a tarefa **Vídeo**.
2 Selecione a câmera a ser configurada e clique na aba **Detecção de movimento**.
3 Selecione uma das seguintes opções na lista suspensa **Calibração automática**:

- **Zona atual:** Calibra a sensibilidade para o movimento detectado na zona de movimento selecionada na imagem de vídeo.
- **Todas as zonas:** Calibra a sensibilidade para o movimento detectado em todas as zonas de movimento selecionadas na imagem de vídeo.
- **Qualquer movimento:** Calibra a sensibilidade para o movimento detectado em toda a imagem de vídeo.

Diferentes valores de sensibilidade são testados para encontrar o valor mais alto sem detectar movimento na imagem. Este teste é responsável por qualquer ruído de fundo indesejado que sua câmera possa captar e considerar como movimento.

Definir zonas de detecção de movimento

Para definir as áreas da imagem de vídeo onde o movimento é significativo, você pode desenhar zonas de detecção de movimento ou *blocos* na imagem.

Para definir uma zona de detecção de movimento:

1 Abrir a tarefa *Vídeo*.
2 Selecione a câmera a ser configurada e clique na aba **Detecção de movimento**.
3 Em **Zona de movimento 1**, use as seguintes ferramentas para definir a zona de detecção de movimento:

DICA: Para câmeras posicionadas perto de uma janela ou porta, certifique-se de que a zona de detecção de movimento cobre essa área importante.

- Para preencher toda a imagem com blocos de detecção de movimento, use a ferramenta **Preencher** ( ).
- Para desenhar um grupo de blocos de detecção de movimento, use a ferramenta **Retângulo** ( ).
- Para desenhar blocos de detecção de movimento individuais, use a ferramenta **Caneta** ( ).
- Para trocar a área com blocos de detecção de movimento pela área sem quaisquer blocos selecionados, use a ferramenta **Inverter** ( ).

- Para apagar todos os blocos de detecção de movimento na imagem, use a ferramenta **Limpar todos** ( ).
- Para apagar os blocos de detecção de movimento que não são necessários, use a ferramenta **Borracha** ( ).

4 Para remover os blocos onde ocorre normalmente movimento para que eles não gerem falsas leituras de movimento, clique em **Modo de aprendizado** ( ).

Você só deve usar esta opção se a imagem de vídeo estiver exibindo o que exibe normalmente. Se normalmente houver muito movimento na imagem, mas você usar o *Modo de aprendizado* a meio da noite, isso não será útil.

As áreas afetadas onde o movimento normalmente ocorre são desativadas.

5 Se necessário, inclua zonas adicionais de detecção de movimento na imagem.
6 Clique em **Aplicar**.

Selecionar quais eventos são acionados por movimento

Quando o movimento é detectado em uma zona de movimento, você pode selecionar qual evento é disparado quando o período de movimento começa e qual é disparado quando ele para.

O que você deve saber

Os eventos padrão que são disparados quando a detecção de movimento é gerada são os seguintes:

- **Movimento ativo:** Evento padrão disparado no início do período de movimento.
- **Movimento inativo:** Evento padrão disparado no fim do período de movimento.

Usar eventos personalizados é útil quando você tem várias zonas de movimento. Cada zona pode ser configurada para detectar movimento em uma área diferente do campo de visão da câmera e gerar eventos diferentes. Ter diferentes eventos permite programar ações diferentes para responder a diferentes situações.

Para selecionar quais eventos são disparados com o movimento:

1 Abrir a tarefa **Vídeo**.
2 Selecione a câmera a ser configurada e clique na aba **Detecção de movimento**.
3 Em **Zona de movimento 1**, clique em **Eventos**.
4 Na caixa de diálogo **Eventos de movimento**, selecione quais eventos serão acionados para o **Evento de movimento ativo** e o **Evento de movimento inativo**.
5 Clique em **OK** e, em seguida, clique em **Aplicar**.
6 Se você tiver mais de uma zona de movimento configurada, repita os passos para cada zona.

Teste de configurações de detecção de movimento

Depois de modificar as configurações de detecção de movimento de uma câmera, teste suas novas configurações para se certificar de que você obtém os resultados esperados.

O que você deve saber

Há limitações com a detecção de movimento por hardware. Se a detecção de movimento é executada na unidade, o teste pode não ser completamente preciso.

CUIDADO: Reflexos de luz nas janelas, luzes acesas ou apagadas e alterações de nível de luz causadas pelo movimento de nuvens podem causar respostas indesejáveis de detecção de movimento e gerar falsos alarmes. Portanto, você deve realizar vários testes para diferentes condições de dia e à noite. Para a vigilância de áreas interiores, certifique-se de que há iluminação consistente das áreas durante o dia e à noite. Superfícies uniformes sem contraste podem desencadear falsos alarmes mesmo com iluminação uniforme.

Para testar suas configurações de detecção de movimento:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.

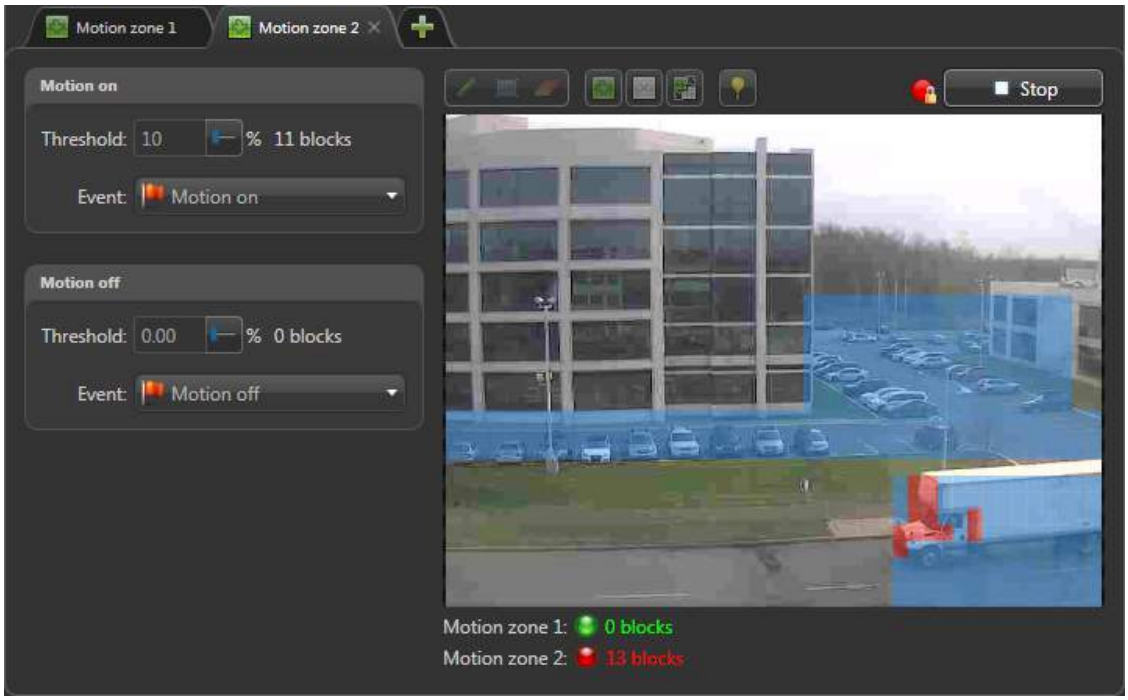
2 Selecione a câmera a ser configurada e clique na aba **Detecção de movimento**.

3 Em **Zona de movimento**, selecione um dos seguintes modos de teste da lista suspensa **Testar zona**:

- **Testar zona:** A zona de movimentação é exibida como sobreposições em azul. Os *blocos de movimentação* aparecem como sobreposições em verde. O número de blocos de movimentação é atualizado em tempo real. Quando o número de blocos de movimento alcança o *Limiar de movimento*, eles são exibidos em vermelho.

  NOTA: Se a câmera estiver configurada para gravar em movimento, o estado de gravação ( ) ficará vermelho quando o ***Limite de movimento*** for alcançado.

- **Testar todas as zonas:** Neste modo, todas as *zonas de movimento* são exibidas ao mesmo tempo, com o número de blocos de movimento em cada uma exibido separadamente.



- **Visualizar todos os movimentos:** Neste modo, toda a imagem de vídeo é testada quanto a movimentação. Todos os movimentos na imagem são exibidos como blocos de movimento

(sobreposições verdes). O número total de blocos de movimentação é atualizado em tempo real. Utilize este modo para testar a definição de sensibilidade para esta câmara.

Tópicos relacionados

Sobre a detecção de movimento na página 485

Ajustar configurações de cor da câmera

Você pode ajustar os atributos de vídeo, como brilho, contraste, matiz e saturação de uma câmera com base em horários, para levar em consideração diferentes horários do dia.

Antes de iniciar

Devem ser criadas agendas antes de você definir os atributos de vídeo para essa agenda.

O que você deve saber

Essas configurações são úteis para horários noturnos, uma vez que a iluminação ambiente é diferente ao amanhecer e ao anoitecer.

Para ajustar as configurações de cor de uma câmera:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Selecione uma câmera e clique na aba **Cor**.
3 Ajuste os valores de **Brilho**, **Contraste**, **Matiz** e **Saturação** para a imagem de vídeo.
4 Para adicionar uma nova configuração de cor, clique em **Adicionar agenda**.
5 Selecione uma agenda criada anteriormente e clique em **Adicionar**.
6 Ajuste os valores de **Brilho**, **Contraste**, **Matiz** e **Saturação** para a imagem de vídeo durante aquela agenda.
7 Para redefinir todos os parâmetros para seus valores padrão, clique em **Carregar padrão**.
8 Clique em **Aplicar**.

Tópicos relacionados

Sobre agendas vespertinas na página 197

Sobre a proteção de privacidade

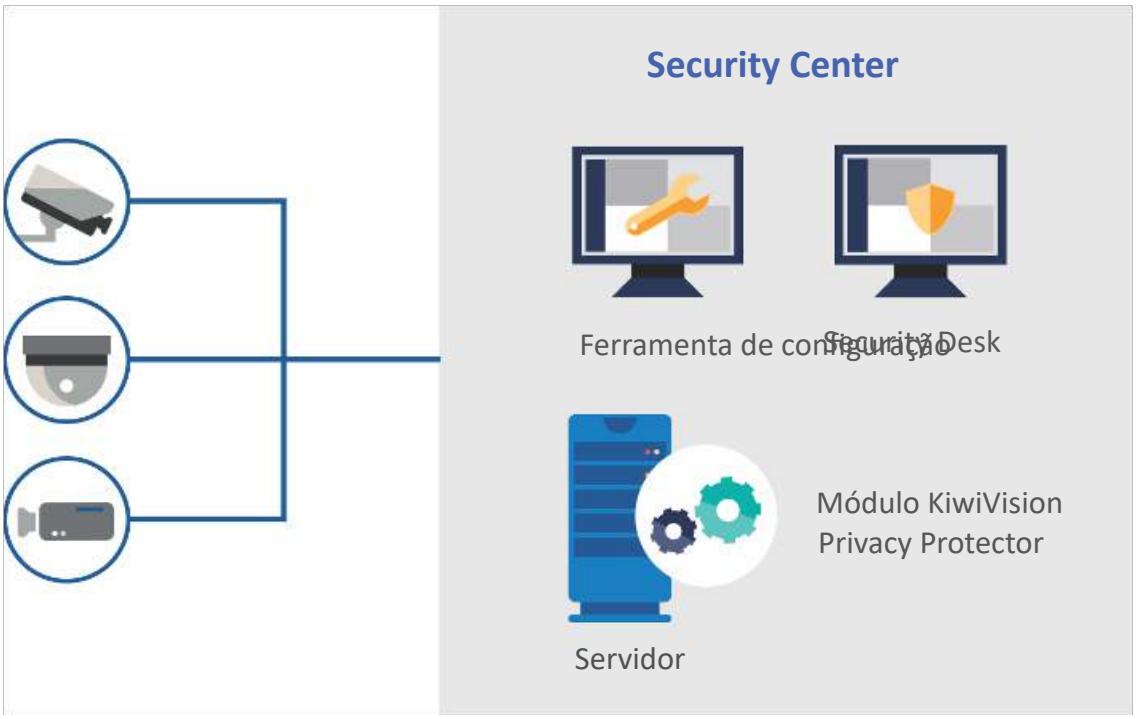
No Security Center, proteção de privacidade é a tecnologia de software usada para desfocar ou mascarar partes de uma transmissão de vídeo. Tudo o que esteja se movendo e seja analisado como não fazendo parte do plano de fundo na cena é desfocado e mascarado para proteger a identidade de pessoas ou objetos em movimento sem obscurecer movimentos ou ações, para que possa continuar havendo monitoramento.

Função Privacy Protector

A função Privacy Protector™ é responsável pela realização de operações de análise em transmissões. É uma função de processamento de mídia que solicita os vídeos originais do Archiver e modifica a transmissão para aplicar anonimização de vídeo confidencial. A transmissão de vídeo protegida por privacidade (anonimizada) é então enviada de volta para o Archiver para gravação.

- Você deve ter uma licença do Privacy Protector e pelo menos uma função do Privacy Protector deve existir para usar o recurso de proteção de privacidade.
- Não há balanceamento de carga. A função funciona como o Archiver, se um agente estiver indisponível o próximo que esteja disponível é usado. Se um servidor falhar, todo o trabalho é transferido para um servidor de failover.
- A função Privacy Protector oferece também a transmissão pública de vídeo desfocada ou mascarada para clientes.

NOTA: Usando a compatibilidade com versões anteriores, as versões mais antigas de Security Center podem visualizar as transmissões protegidas (através do Federation™), mas não as originais. Isso se aplica também a versões anteriores do Media Gateway (transmissões RTSP) e o Web Client.



Transmissões da proteção de privacidade

Quando a proteção de privacidade está habilitada na configuração da câmera, duas transmissões de vídeo são arquivadas:

- Transmissão de vídeo (Público) - contém conteúdo desfocado para proteção de privacidade para deixar o vídeo anônimo. Isso garante que todo acesso regular ao vídeo irá sempre acessar o vídeo desfocado.
- Transmissão de vídeo confidencial (Privado) - contém a transmissão de vídeo original da unidade de vídeo e o conteúdo do vídeo não está desfocado ou mascarado.

  NOTA: A transmissão confidencial só pode ser visualizada se o usuário solicitar explicitamente e tiver o privilégio *Remover a proteção de privacidade*.

NOTA: Quando exportar vídeo for usado, a transmissão exibida no ladrilho é usada. Se uma proteção de privacidade for removida, o vídeo original será exportado.

Exemplo

Assista a este vídeo para saber mais. Clique no ícone **Legendas** (**CC**) para ligar a legenda do vídeo em um dos idiomas disponíveis. O vídeo pode não ser exibido no Internet Explorer. Para resolver isso, abra as **Configurações de compatibilidade de exibição** e limpe **Exibir sites da intranet em Visualizar compatibilidade**.

Tópicos relacionados

Static vs. dynamic privacy masking

Configurar proteção de privacidade na página 495
Acessar vídeos confidenciais usando cartões inteligentes na página 499

Configurar proteção de privacidade

Para desfocar ou anonimizar uma transmissão de vídeo, você deve configurar a proteção de privacidade para a câmera.

Antes de iniciar

- A proteção de privacidade somente é suportada em câmeras nativas. A proteção de privacidade não pode ser habilitada em câmeras federadas ou DVRs.
- Certifique-se de que o OpenCL esteja disponível instalando os mais recentes controladores de adaptador de placa gráfica na estação de trabalho do Config Tool usada para configurar a proteção de privacidade. Para garantir o melhor desempenho, você deve também atualizar os controladores de adaptador de placa gráfica na estação de trabalho do Security Desk.

O que você deve saber

- Não é possível configurar a proteção de privacidade em câmeras federadas.
- A proteção de privacidade não é compatível com lentes olho de peixe.
- A proteção de privacidade somente suporta câmeras PTZ que sejam usadas como câmeras fixas. Após mover o PTZ, a transmissão fica desfocada durante o período de aprendizado na inicialização.
- A proteção de privacidade consome muitos recursos.
  - O número de transmissões duplica quando a proteção de privacidade está habilitada.
  - O desfoque é computado e aplicado na imagem decodificada.
- Usando a compatibilidade com versões anteriores, as versões mais antigas de Security Center podem visualizar as transmissões protegidas (através do Federation™), mas não as originais. Isso se aplica também a versões anteriores do Media Gateway (transmissões RTSP) e o Web Client.

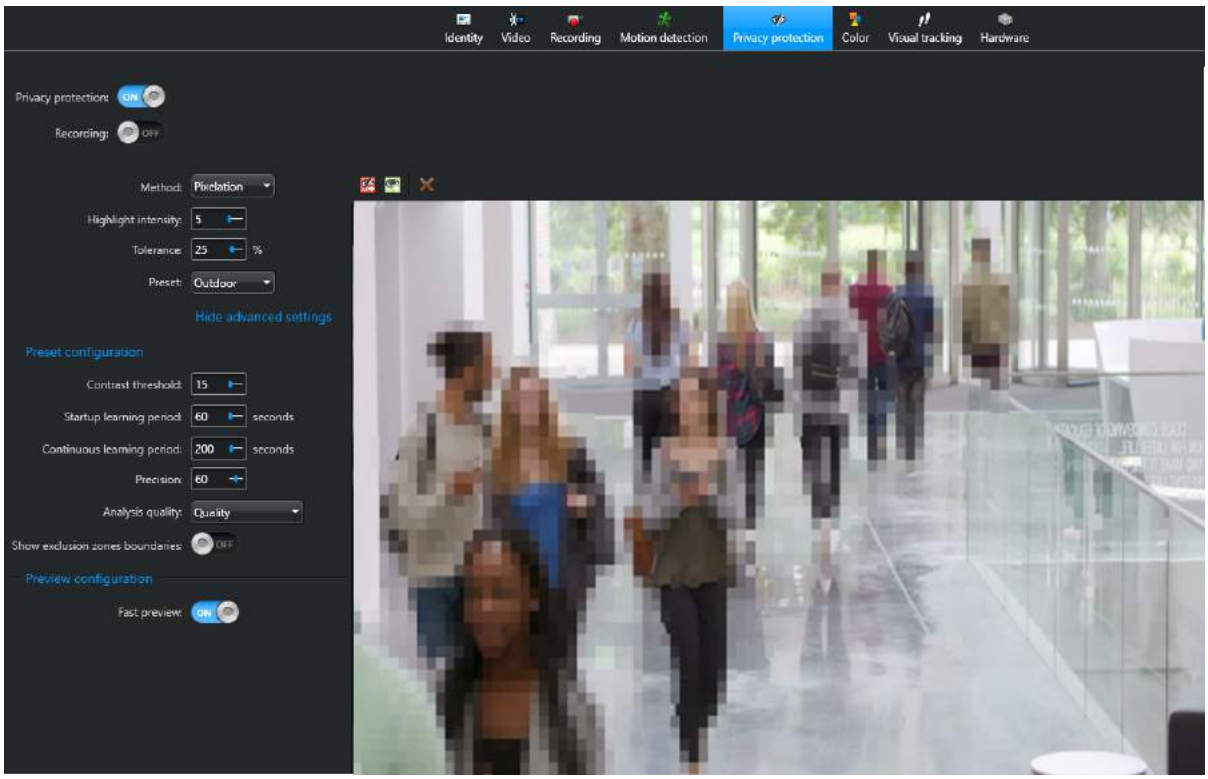
Para configurar a proteção de privacidade:

1 Crie uma função Privacy Protector; não é necessária configuração. Na tarefa *Sistema*, clique em **Tarefas** > **Adicionar uma entidade** > **Privacy Protector** e preencha os campos conforme necessário.

CUIDADO: Certifique-se de a tarefa Privacy Protector não esteja no mesmo servidor do Archiver porque isso pode afetar o desempenho da CPU e os arquivos. Quando o uso da CPU é intensivo no servidor do Archiver, podem ocorrer situações de *Fila de arquivamento cheia* e perda de dados.

2 Na página inicial do Config Tool, abra a tarefa *Vídeo*.

3 Selecione a câmera a ser configurada e clique na aba **Proteção de privacidade**.



4 Selecione a opção de **Proteção de privacidade** desejada. Escolha entre **Ligado** ou **Desligado**.

- **ATIVO:** Especifica que a análise de proteção de privacidade de vídeo e função anônima estão habilitadas. Tanto a transmissão ao vivo da tarefa (*Monitoramento* no Security Desk) e Prévia rápida (*Pré-visualização* seção da aba **Proteção de Privacidade** no Config Tool) ficam anônimas.
- **INATIVO:** Especifica que a análise de proteção de privacidade de vídeo e função anônima estão desabilitadas.

NOTA: Caso exista mais de uma função Privacy Protector, é exibida uma caixa de combinação para selecionar aquela que você deseja usar.

5 Selecione a opção de **Gravação** desejada. Escolha entre **Ligado** ou **Desligado**.

- **ATIVO:** Especifica a gravação contínua da transmissão com proteção de privacidade. Quando a **Gravação** está **Ligada**, a transmissão ao vivo é usada para a transmissão de arquivos anônima.

  IMPORTANTE: As configurações de gravação da câmera (vídeo confidencial) e as configurações de gravação da transmissão com privacidade protegida trabalham independente uma da outra. Agendamentos de arquivo não são suportados para a transmissão com privacidade protegida. A transmissão original (não anônima) é arquivada usando as configurações na aba **Gravação**.
- **INATIVO:** Especifica que a transmissão com proteção de privacidade não é gravada.

6 Selecione um método de proteção de privacidade entre os seguintes:

- **Método:** Especifica o método de proteção de privacidade. A opção selecionada varia dependendo de como você precisa aplicar proteção de privacidade no vídeo. Escolha um dos seguintes:
  - **Desfoque:** Remove o foco dos blocos ativos. O parâmetro adicional **Nível de intensidade** controla a intensidade do desfoque.
  - **Colorir:** Preenche os blocos com uma cor sólida. O parâmetro adicional **Intensidade de destaque** controla a intensidade da coloração. Colorir é útil quando você quer garantir que nenhuma pessoa seja reconhecida em nenhuma cena.
  - **Pixel:** Define a aparência dos blocos que obscurece objetos em movimento. O parâmetro adicional **Intensidade de destaque** controla a intensidade do pixel.

7 Selecione ou especifique o seguinte:

- **Cor:** (Somente para o método colorir) especifica a cor a ser usada para colorir. Especifique uma cor do seletor de cor **Básico** ou clique em **Personalizado** para mais opções.

- **Destacar intensidade:** (Somente para os métodos colorir e pixel) Especifica a intensidade de cor ou pixel. O valor padrão é 5. É possível especificar valores no intervalo de 0 - 255.
- **Nível de intensidade:** (Somente método de desfoque) Especifica a intensidade do desfoque. O valor padrão é 5. É possível especificar valores no intervalo de 1 - 5.
- **Tolerância:** Especifica a tolerância de mudança de iluminação como porcentagem. O valor padrão é 25%. É possível especificar valores de 1 - 100%.

8 Selecione uma Predefinição.

- **Predefinição:** Especifica um conjunto padrão otimizado de configurações para o uso selecionado. Escolha entre **Interno** ou **Externo**.
  - **Interno:** Especifica um conjunto de configurações padrão otimizadas para situações em ambientes internos.
  - **Externo:** Especifica um conjunto de configurações padrão otimizadas para situações em ambientes externos.

Use **Predefinição** quando pretender usar as configurações padrão para **Interior** ou **Exterior** em vez de Configurações avançadas.

9 Determine uma ou mais zonas de exclusão.

a) Selecione um dos seguintes:

- **Adicionar zona sempre desfocada ( ):** O método de proteção de privacidade é sempre aplicado a essas zonas. Tudo o que estiver dentro de uma zona sempre desfocada, incluindo o plano de fundo, fica protegido.
- **Adicionar zona nunca desfocada ( ):** O método de proteção de privacidade nunca é aplicado a essas zonas. Tudo o que esteja dentro de uma zona nunca desfocada, incluído movimento, nunca fica protegido.

b) Clique e arraste sobre uma área da prévia de vídeo para definir a zona.

No caso de zonas sobrepostas, as zonas sempre desfocadas têm prioridade sobre zonas nunca desfocadas.

NOTA: Os blocos de vídeo não podem ser parcialmente desfocados. Quando a borda de uma zona sempre desfocada divide um bloco de vídeo, o bloco inteiro, incluindo a área fora da zona, ficará sempre desfocado. Quando a borda de uma zona nunca desfocada divide um bloco de vídeo, o bloco inteiro, incluindo a área dentro da zona, ficará desfocado quando for detectado movimento. O tamanho dos blocos de vídeo protegidos é definido pelo parâmetro **Precisão**.

10 (Opcional) Mostre ou oculte as configurações avançadas conforme necessário.

A primeira parte das configurações avançadas é específica ao método de proteção de privacidade. A segunda parte, períodos de aprendizado na Inicialização e Contínuo, define as durações usadas para adquirir o plano de fundo e atualizá-lo.

- Clique em **Mostrar configurações avançadas** quando desejar ajustar as configurações avançadas individualmente.
- Clique em **Ocultar configurações avançadas** quando pretender usar as configurações padrão para Interior ou Exterior.

11 Na seção *Configuração da predefinição*, digite ou selecione o seguinte conforme necessário:

- **Limite de contraste:** (Somente para predefinição externa) Especifica que bordas na imagem são consideradas apenas para borrar ou usar a função anônima se o seu valor excede o limite especificado. O valor padrão é 15. É possível especificar valores no intervalo de 0 - 255.

  NOTA: O ruído de câmera e mudanças de iluminação faz com que as bordas fiquem com contraste baixo (na maioria dos casos não é visível para o observador humano). Essas bordas podem se transformar rapidamente, por isso é que não devem ser consideradas para o modelo de plano de fundo ou pixelização. Se este valor for muito baixo, alterações menores na imagem poderão ser pixelizadas. Se o valor for muito alto enquanto o contraste na imagem é muito baixo, como roupas pretas em um fundo preto, partes de objetos da frente podem ser visíveis, habilitando o reconhecimento de pessoas.
- **Número de estados de iluminação:** (Somente para predefinição interna) Especifica o modelo de estados de iluminação a usar. Especificar um número maior de estados de iluminação ajuda ao Privacy Protector a lidar com condições de modificação de iluminação rápidas. Isso funciona somente quando mudanças rápidas e globais em iluminação ocorrem e m estado intermediário deve ser adicionado. Por exemplo, se existirem dois estados de iluminação (*luzes ligadas* e *luzes desligadas*), três estados devem ser especificados: ligado, desligado e intermédio. O valor padrão é 1, o qual desabilita a verificação de iluminação global, e o modelo de estado de iluminação padrão é usado. É possível especificar valores no intervalo de 1 - 10.

  DICA: Use a configuração padrão quando esperar mudanças de iluminação pequenas ou graduais que o modelo pode adaptar para durante o período de aprendizado constante.
- **Tolerância de mudança de iluminação:** (Somente para predefinição interna) Especifica o quão grande as mudanças na imagem do vídeo devem ser (em porcentagem) para alterar o modelo de fundo. Valores menores resultam em mudanças rápidas, enquanto valores maiores resultam em mudanças lentas. O valor padrão é 80%. É possível especificar valores de 1 - 100%.
- **Período de aprendizagem inicial:** Especifica o tempo gasto analisando o vídeo para reconhecer o fundo. A configuração padrão é de 60 segundos. É possível especificar valores no intervalo de 1 - 1000 segundos.
- **Período de aprendizado contínuo:** Especifica o tempo que passa antes de analisar o vídeo novamente para identificar e disfarçar qualquer pessoa se movendo ou objetos. A configuração padrão é de 200 segundos. É possível especificar valores no intervalo de 1 - 1000 segundos.

  DICA: Especifique um período de aprendizagem 50% maior do que o tempo que as pessoas são esperadas a ficarem paradas. Isso garante que as pessoas que não se movem (por um período de tempo) não fiquem visíveis.
- **Precisão:** Especifica o tamanho do bloco na imagem de vídeo protegida. Especifica um número de resultados em blocos menores. A configuração padrão é 60. É possível especificar valores no intervalo de 0 - 100.
- **Qualidade de análise:** Especifica a redução de análise que é usada para executar a análise do vídeo. Selecione um dos seguintes:
  - **Equilibrado:** Especifica uma altura de resolução de vídeo reduzida de 240 pixels.
  - **Desempenho:** Especifica uma altura de resolução de vídeo reduzida de 80 pixels.
  - **Qualidade:** Especifica uma altura de resolução de vídeo reduzida de 480 pixels.
- **Exibir limites de zonas de exclusão:** Quando estiver habilitado, uma caixa com entorno azul, delimitando as zonas de exclusão é exibida quando a câmera associada é monitorada no Security Desk.

12 Na seção *Configuração da prévia*, habilite ou desabilite **Prévia rápida** conforme necessário. A opção Prévia rápida é somente para Config Tool.

- **Prévia rápida: ATIVO:** Especifica um valor de *período de aprendizagem* (um segundo) em vez dos valores especificados nas configurações avançadas. Essa configuração é para a **Pré-visualização**

somente no lado direito da página de *Proteção de privacidade*, essa configuração não impacta no servidor da transmissão atual.

MELHOR PRÁTICA: Use **a Prévia rápida: ATIVO** quando desejar testar muitos parâmetros diferentes sem esperar pelo modelo de plano de fundo para atualizar a cada vez. Ao usar a prévia rápida, o modelo de fundo será menos preciso.

- **Prévia rápida: INATIVO:** Use **a Prévia rápida: INATIVO** quando desejar que o algoritmo de proteção de privacidade seja exatamente o que será após as mudanças serem aplicadas.

13 Clique em **Aplicar**.

Tópicos relacionados

Sobre a proteção de privacidade na página 493

Acessar vídeos confidenciais usando cartões inteligentes

Para assegurar que os vídeos confidenciais são mantidos protegidos, você pode definir criptografia e controlar o acesso mediante cartões inteligentes.

Antes de iniciar

Familiarize-se com a documentação do fabricante do cartão inteligente.

O que você deve saber

Um aplicativo de proteção de privacidade típico exige autorização especial para acessar os vídeos confidenciais originais desprotegidos. Para melhor segurança, é geralmente necessária criptografia. As etapas seguintes explicam como definir criptografia usando cartões inteligentes.

- O servidor Privacy Protector correspondente deve ter o certificado necessário para descriptografar a transmissão e o certificado com a chave privada deve ser instalado.

Para proteger vídeos confidenciais originais com criptografia:

1 Gere e instale um certificado nos servidores executando a função Privacy Protector.
2 Exporte e instale a chave pública nos servidores do Archiver.
3 Na aba **Gravação**, habilite criptografia para a câmera.
4 Adicione o certificado da etapa 1.
5 Adicione o certificado do seu cartão inteligente.

NOTA: O modo de instalação do certificado varia em função do fabricante do cartão inteligente.

6 Habilite a proteção de privacidade.

Sempre que seja necessário desproteger um vídeo, as seguintes condições devem ser satisfeitas:

- O usuário deve ter o privilégio *Remover proteção de privacidade* no Security Desk.
- O cartão inteligente deve estar no leitor de cartões conectado à estação de trabalho.

Tópicos relacionados

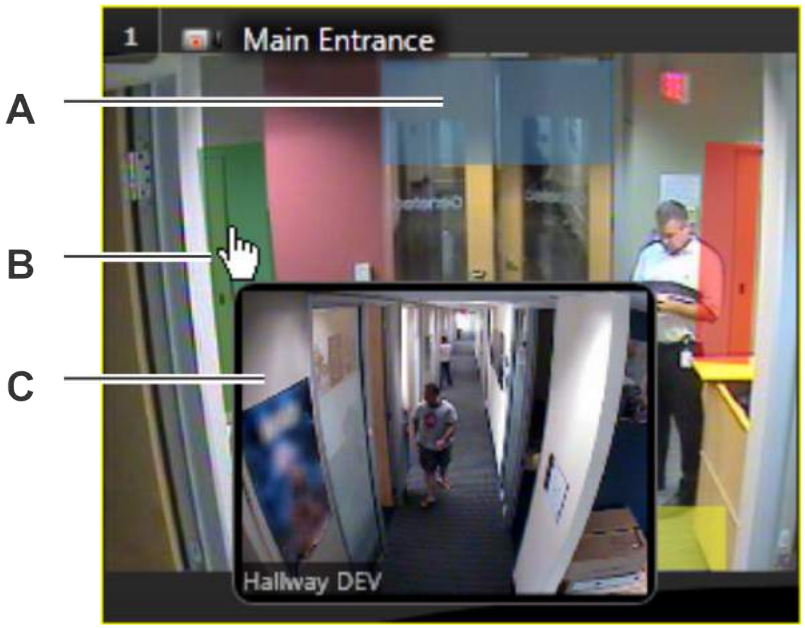
Sobre a proteção de privacidade na página 493
O que é a criptografia de transmissão de fusão? na página 417
Habilitar a criptografia de transmissão de fusão na página 426

Sobre rastreamento visual

Rastreamento visual é um recurso do Security Desk que permite seguir um indivíduo por diferentes áreas da empresa sem perdê-lo de vista, desde que os lugares por onde esta pessoa passar estejam monitorados por câmeras.

O rastreamento visual funciona com o vídeo ao vivo e em reprodução. Quando o rastreamento visual está ligado, sobreposições transparentes (formas coloridas desenhadas sobre o vídeo) aparecem no ladrilho onde a câmera é exibida. Cada sobreposição corresponde a uma ou mais câmeras adjacentes às quais é possível pular.

Além disso, quando mais de uma câmera é associada a uma dada sobreposição, uma lista de nomes de câmeras é mostrada em vez da pré-visualização do vídeo. É necessário escolher um nome de câmera para mudar para aquela câmera. O fluxo do vídeo exibido no ladrilho muda para a próxima câmera, como é determinado pela configuração de rastreamento visual.



A	Sobreposições semitransparentes na imagem do vídeo significam uma ligação de um rastreamento visual a outra câmera.
B	Clique na sobreposição colorida para mudar para a próxima câmera.
C	Passar o ponteiro do mouse na sobreposição produz uma pré-visualização da próxima câmera.

Configurar o rastreamento visual

Para saltar para câmeras adjacentes a partir de uma câmera exibida no Security Desk, você deve configurar o rastreamento visual criando sobreposições de vídeo para uma câmera.

O que você deve saber

O rastreamento visual somente é suportado para câmeras PTZ se elas forem usadas como câmeras fixas.

Para configurar o rastreamento visual:

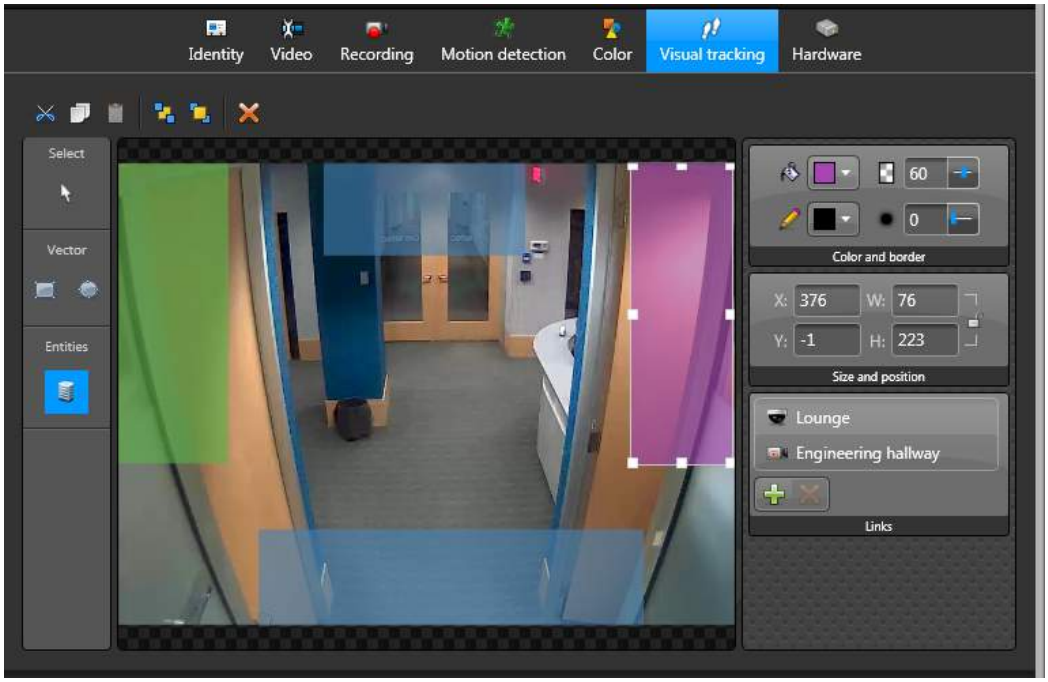
1 Abra a tarefa *Exibição de área*.

2 Selecione uma câmera e clique na aba **Rastreamento visual**.

3 Selecione a ferramenta de desenho **Retângulo** ou **Elipse** e desenhe uma forma sobre o vídeo ao vivo.

DICA: Se configurar várias câmeras para usarem as mesmas sobreposições de polígono, você pode copiar e colar os polígonos de uma câmera para outra usando os atalhos habituais.

4 Redimensione, reposicione e gire a forma usando o mouse ou usando os parâmetros **Tamanho** e **Posição**.



5 Selecione a cor de preenchimento e a opacidade para a sobreposição.

DICA: Uma opacidade de 60% estabelece um bom equilíbrio entre transparência e visibilidade.

6 Defina uma cor e uma espessura de borda.

7 Na exibição de área dentro da aba **Rastreamento visual**, arraste as câmeras para as quais deseja saltar até a forma colorida.

NOTA: Clique em **Entidades** ( ) na barra de ferramentas para apresentar a exibição de área.

Os nomes das câmeras aparecem na visualização **Entidades**. Se várias câmeras estiverem associadas à mesma sobreposição, o usuário do Security Desk deve selecionar uma câmera antes de saltar para aquela câmera, em vez de clicar na sobreposição colorida.

8 Adicione tantas sobreposições quanto necessário.

9 Clique em **Aplicar**.

Visualizar configurações de câmeras

Você pode exibir uma lista de todas as câmeras locais e federadas do Security Center que fazem parte do sistema e suas configurações usando o relatório *Configuração da câmera*.

O que você deve saber

O relatório de configuração da câmera é útil para comparar as configurações da câmera e certificar-se de que suas câmeras estão configuradas adequadamente de acordo com suas necessidades. Se a câmera tiver vários fluxos de vídeo ou vários agendamentos de streaming definidos, cada fluxo e agendamento será exibido como um item de resultado separado.

Este relatório não é suportado com câmeras federadas do Security Center 5.0–5.2 ou câmeras federadas Omnicast™.

NOTA: Esse relatório pode levar alguns minutos para gerar, dependendo de quantas câmeras você está consultando.

Para visualizar as configurações de câmeras no seu sistema:

1 Abra a tarefa **Configuração da câmera**.
2 Definir os filtros de consulta para o relatório. Escolha um ou mais dos filtros abaixo:
   - **Câmeras:** Selecionar as câmeras para investigar.
   - **Campos personalizados:** Restringir a busca a campo personalizado predefinido para a entidade. Este filtro aparece somente se os campos personalizados estiverem definidos para a entidade e estavam visíveis para você, quando foi criado ou configurado pela última vez.
3 Clique em **Gerar relatório**.

   As seguintes configurações da câmera são listadas no painel do relatório:
   - **Taxa de transferência de bits:** Configuração de taxa de bits para a câmera.
   - **Câmera:** Nome de câmera.
   - **Descrição:** Descrição da entidade.
   - **Transferência na unidade:** Se a câmera está configurada para transferência de borda ou não (sim ou não).
   - **Caminho de entidade:** Lista de todas as áreas relacionadas, começando pela entidade do sistema. Se uma câmera tiver várias áreas pai, "*\" é mostrado como o caminho
   - **Taxa de quadros:** Configuração de velocidade de quadro para a câmera.
   - **Qualidade da imagem:** Configuração de qualidade de imagem para a câmera.
   - **Intervalo do quadro-chave:** Configuração de intervalo chave para a câmera.
   - **ID lógico:** ID lógica da câmera.
   - **Fabricante:** Fabricante da unidade.
   - **Endereço multicast:** Endereço multicast da câmera.
   - **Configuração da rede:** Tipo de conexão usada pela câmera.
   - **Proprietário:** Archiver que gerencia a câmera.
   - **Porta:** Porta de conexão da unidade de vídeo.
   - **Tipo de produto:** Modelo ou série da unidade de vídeo.
   - **Modo de gravação:** Configurações de gravação para a câmera.
   - **Resolução:** Resolução do fluxo de vídeo da câmera.

- **Fluxo:** O fluxo de vídeo da câmera.
- **Uso do stream:** A finalidade do fluxo de vídeo (para vídeo ao vivo, gravações, e assim por diante).
- **Agendamento de fluxo:** Agendamento de quando a câmera transmite vídeo.
- **Tipo:** Tipo da câmera (câmera fixa ou câmera PTZ).

4 Para modificar as configurações de uma câmera, clique com o botão direito em um item no painel de relatório e, em seguida, clique em **Configurar entidade** ( ) para ir à página de configuração dessa entidade no Config Tool.

NOTA: É preciso ter o privilégio do usuário para modificar as entidades para usar este comando.

Configurar motores PTZ

Se o motor PTZ não estiver integrado na câmera na unidade de vídeo, você precisará configurar o motor PTZ separadamente antes de poder controlá-lo no Security Desk.

O que você deve saber

Alguns motores PTZ suportam os seguintes comandos adicionais:

- **Caixa de zoom:** Amplie uma área desenhando uma caixa na imagem de vídeo com o mouse. Funciona como o zoom digital para câmeras fixas.
- **Centralizar no clique:** Centraliza a câmera em um ponto da imagem de vídeo com um único clique.
- **Zoom avançado:** Ampliar ou reduzir um fator de zoom específico (valor absoluto) com o controle deslizante do ladrilho. Por exemplo, você pode mover o controle deslizante para 10x e ele manterá sua posição quando for solto. Quando **PTZ avançado** está desativado, o fator de zoom não fica disponível e o controle deslizante volta para sua posição central quando é liberado, como um joystick usado para panorâmica e inclinação de uma câmera.

Quando esses comandos estão ativados, eles substituem os comandos normais de panorâmica, inclinação e zoom ao controlar o PTZ no Security Desk.

Para configurar motores PTZ:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Selecione a câmera a ser configurada e clique na aba **Hardware**.
3 Alterne a opção **PTZ** para **Ligado**.
4 Na lista suspensa **Protocolo**, selecione o protocolo usado pelo motor PTZ.
5 Ao lado do campo **Protocolo**, clique em para configurar as opções de **Retardo ocioso**, **Comando ocioso** e **Retardo de bloqueio**.
6 Na lista suspensa **Porta serial**, selecione a porta serial usada para controlar o motor PTZ.
7 Na caixa **Endereço PTZ**, selecione o número que identifica o motor PTZ na porta serial.
Esse número é importante porque é possível conectar mais de um motor PTZ na mesma porta serial. Este número deve corresponder às configurações de chaves dip no hardware PTZ.
8 Para ativar os comandos de PTZ avançado (caixa de zoom, centralizar no clique e zoom avançado), coloque a opção **PTZ avançado** em **Ligado** e calibre as coordenadas de PTZ.
9 Clique em **Aplicar.**

Após terminar

- Teste o motor PTZ.
- Defina quais usuários têm prioridade para controlar o motor PTZ.

Tópicos relacionados

Câmera - Aba hardware na página 998

Calibrar coordenadas PTZ

Na maioria das câmeras, é necessário calibrar os limites do movimento PTZ para usar os comandos de caixa de zoom, centralizar no clique e zoom avançado corretamente no Security Desk.

O que você deve saber

Nem todas as câmeras exigem calibração PTZ. Por exemplo, as câmeras Axis não necessitam de calibração.

Para calibrar as coordenadas PTZ:

1 Abrir a tarefa **Vídeo**.
2 Selecione a câmera e clique na aba **Hardware**.
3 Próximo à opção **PTZ avançado**, clique em **Calibrar**.
4 Para definir automaticamente as coordenadas PTZ, clique em **Assistente de calibração** e siga as instruções na tela.
5 Para configurar manualmente as coordenadas PTZ, mova o motor PTZ na imagem de vídeo ao vivo e insira os valores correspondentes à direita:
   - **Fator de zoom máximo:** Dê zoom até o nível máximo que deseja que os usuários do Security Desk alcancem e insira o valor de **Zoom**da seção **Coordenadas**.
   - **Campo de visão horizontal:** Insira o campo de visão horizontal especificado pelo fabricante da câmera. Se não tiver esta informação, diminua o zoom até o valor de **Zoom** indicar 1x e estime o ângulo do campo de visão horizontal a partir da imagem que você vê na tela.
   - **Campo de visão vertical:** Insira o campo de visão vertical especificado pelo fabricante da câmera. Se não tiver esta informação, diminua o zoom até o valor de **Zoom** indicar 1x e estime o ângulo do campo de visão vertical a partir da imagem que você vê na tela.
   - **Ângulo mínimo de pan:** Gire a câmera para a posição mais à esquerda da área sob vigilância e insira o valor de **Panorâmica** da seção **Coordenadas**.
   - **Ângulo máximo de pan:** Gire a câmera para a posição mais à direita da área sob vigilância e insira o valor de **Panorâmica** da seção **Coordenadas**.
   - **Ângulo mínimo de inclinação:** Gire a câmera para a posição mais inferior da área sob vigilância e insira o valor de **Inclinação** da seção **Coordenadas**.
   - **Ângulo máximo de inclinação:** Gire a câmera para a posição mais superior da área sob vigilância e insira o valor de **Inclinação** da seção **Coordenadas**.
6 Se quiser inverter a imagem da câmera em algum ponto, selecione uma das seguintes opções na lista suspensa **Inverter câmera**:
   - **Inclinação mínima:** Inverte a imagem da câmera quando o motor PTZ alcança a coordenada mínima de inclinação.
   - **Inclinação máxima:** Inverte a imagem da câmera quando o motor PTZ alcança a coordenada máxima de inclinação.
7 Se você perceber que o valor de **Ângulo mínimo de panorâmica** é maior do que o **Ângulo máximo de panorâmica**, selecione a opção **Inverter eixo de panorâmica**.
8 Se você perceber que o valor de **Ângulo mínimo de inclinação** é maior do que o **Ângulo máximo de inclinação**, selecione a opção **Inverter eixo de inclinação**.

Após terminar

Teste os comandos de caixa de zoom, centralizar no clique e zoom avançado com um ladrilho do Security Desk. Se necessário, ajuste a calibração e teste a câmera PTZ novamente.

Teste de controles PTZ

Depois de configurar o seu motor PTZ, você deve testar se os controles estão funcionando corretamente.

O que você deve saber

Toda vez que você alterar um parâmetro PTZ, você deve remover a câmera do ladrilho e arrastá-la de volta para ele para que as alterações entrem em vigor.

Para testar controles PTZ:

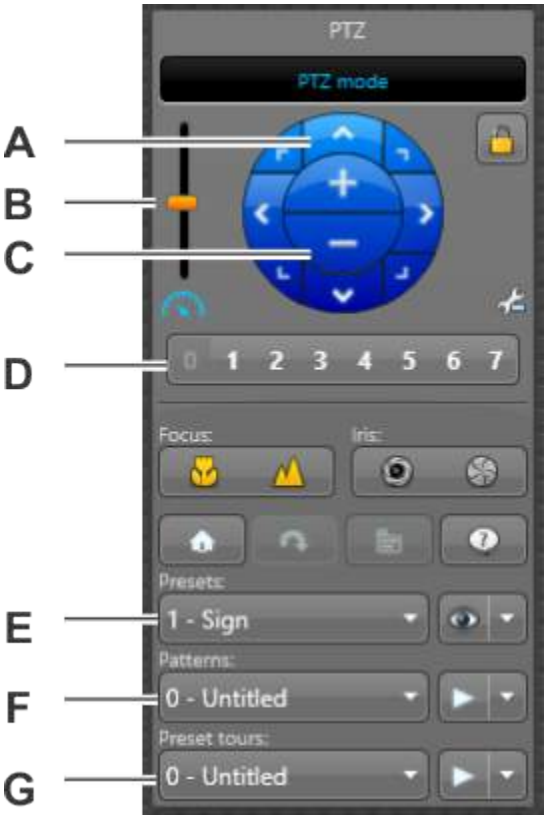
1 Abra a tarefa **Vídeo** e clique duas vezes na câmera que deseja testar.

2 Na caixa de diálogo **Vídeo ao vivo**, teste os controles PTZ na imagem de vídeo usando o widget PTZ.

Widget PTZ

O widget *PTZ* é usado para realizar operações panorâmicas, inclinadas e operações de zoom na câmera exibida. Ele aparece no painel quando o ladrilho selecionado exibe uma câmera habilitada para PTZ ( ).

IMPORTANTE: Nem todas as câmeras PTZ oferecem suporte a todos os recursos PTZ. Se um ou mais botões PTZ estiverem em cinza, isso significa que a câmera PTZ com que você está trabalhando não suporta tal comando.



Botão/Letra	Comando	Descrição
A	**Setas de direção**	Panorâmica do motor PTZ usando as oito setas de direção.
B	**Barra de velocidade**	Ajuste a velocidade do motor PTZ.
C	**Aproximar/afastar zoom**	Aproxime e afaste o zoom usando os comandos mais (+) e menos (-).
D	**Botões de acesso rápido**	Mova o motor PTZ para um dos oito acessos rápidos da predefinição PTZ.
E	**Predefinições**	Selecione a predefinição da lista suspensa para mover o motor PTZ para essa predefinição, salve uma nova posição de predefinição ou renomeie a predefinição.

Botão/Letra	Comando	Descrição
F	**Padrões**	Selecionar um padrão PTZ da lista suspensa para iniciar um padrão PTZ (séries de predefinições ou movimentos PTZ gravados), gravar um novo padrão ou renomeá-lo.
G	**Auxiliares**	Selecione um auxiliar da lista suspensa para iniciar ou parar um comando auxiliar ou renomear o comando auxiliar.
	**Bloquear PTZ**	Bloqueio o motor PTZ, assim somente você tem o controle do PTZ.
	**Alternar para modo avançado**	Abrir o menu do modo avançado de PTZ.
	**Aproximar foco**	Focar o PTZ perto
	**Afastar foco**	Focar o PTZ longe
	**Abrir diafragma**	Controlar manualmente a íris (abrir íris)
	**Fechar o diafragma**	Controlar manualmente a íris (fechar íris)
	**Início do PTZ**	Vá para a posição (padrão) da página inicial de PTZ
	**Inverter**	Girar o motor PTZ em 180 graus
	**Menu ativo/inativo**	Abrir o menu PTZ Esta opção é apenas para as câmeras PTZ analógicas.
	**Comandos específicos**	Use os comandos que são específicos para esse modelo de câmera.
	**Vai para predefinição**	Pular para a posição pré-definida selecionada na lista suspensa. • **Salvar:** Salva a predefinição na lista suspensa, usando a posição atual de PTZ. • **Limpar predefinição:** Apaga a posição PTZ da predefinição.
	**Iniciar padrão**	Inicie o padrão PTZ selecionado na lista suspensa. É possível clicar qualquer em predefinição de botão de PTZ para interromper o padrão. • **Renomear:** Renomear a pré-definição, o padrão ou auxiliar selecionados. • **Gravar padrão:** Gravar um novo padrão PTZ • **Limpar padrão:** Apaga o padrão.
	**Iniciar um comando auxiliar**	Inicia um comando auxiliar de PTZ (por exemplo, um limpador de para-brisa).
	**Parar comando auxiliar**	Interrompe o comando auxiliar de PTZ
	**Renomear**	Renomear a pré-definição, o padrão ou auxiliar selecionados.

Definir níveis de usuário para controlar motores PTZ

Você pode selecionar quais usuários ou grupos de usuários têm prioridade para controlar câmeras PTZ diferentes, substituindo seu nível geral de usuário para áreas específicas ou câmeras.

O que você deve saber

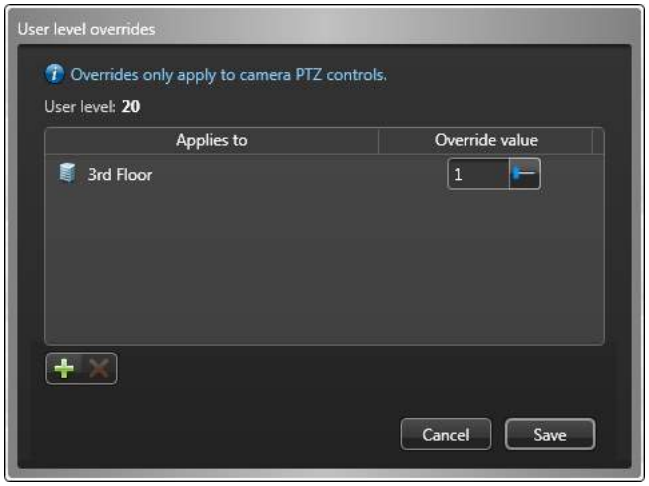
Por padrão, a prioridade para controlar as câmeras PTZ é determinada pelo *nível de usuário* geral, que é definido individualmente ou herdado de seu grupo de usuários pai. No entanto, as substituições de nível de usuário têm precedência sobre o nível geral de usuário. Você pode criar uma sobreposição para controles PTZ por área ou câmera. Se você substituir um nível de usuário para uma área, ele se aplicará a todas as câmeras PTZ nessa área.

A definição de substituições de nível de usuário para controles PTZ é útil se você tiver vários grupos de usuários que têm acesso às mesmas câmeras.

Para definir níveis de usuário para controlar um motor PTZ:

1 Na página inicial Config Tool, abra a tarefa *Gerenciamento de usuários*.
2 Selecione o usuário ou grupo de usuários a configurar e clique na aba **Propriedades**.
3 Coloque a opção **Nível de usuário** em **Substituir** e clique em **Configurar sobreposições de PTZ**.
4 Na caixa de diálogo **Sobreposições de nível de usuário**, clique em **Adicionar um item** ( ).
5 Selecione a câmera ou área para a qual criar uma sobreposição e clique em **OK**.
6 Na coluna **Valor da sobreposição**, selecione um nível de usuário que se aplique às câmeras ou à área.
7 Clique em **Salvar** > **Aplicar**.

Exemplo: Paul é membro do grupo de usuários Operador em sua empresa e está encarregado de monitorar o terceiro andar de seu prédio. Como parte do grupo de usuários Operador, ele tem, por padrão, nível de usuário de 20. Como ele está encarregado de monitorar o terceiro andar, ele precisa ter a mais alta prioridade para controlar todas as câmeras PTZ nesse andar. Portanto, uma sobreposição de nível de usuário com o valor de 1 é criada para ele para o terceiro andar.



Sobre sequências de câmeras

É um tipo de entidade que define uma lista de câmeras que são exibidas, uma depois da outra, de modo giratório, em um único ladrilho no Security Desk.

Quando exibida em um Security Desk, a sequência de câmeras pode ser pausada (interromper o ciclo) e descompactada (mostrar todas as câmeras).

As câmeras que compõem a sequência podem ser fixas, habilitadas para PTZ ou federadas. Cada câmera recebe uma quantidade predefinida de tempo de exibição. As câmaras PTZ podem ser configuradas para apontar para uma posição predefinida, para executar um padrão ou para ligar/desligar um interruptor auxiliar.

Criar sequências de câmeras

Você pode agrupar câmeras fixas, habilitadas para PTZ e federadas em uma sequência de câmeras, para que elas sejam exibidas uma após a outra em ladrilhos do Security Desk.

O que você deve saber

As câmeras da lista de sequência de câmeras são exibidas na mesma ordem no Security Desk.

Para criar uma sequência de câmera:

1 Abra a tarefa **Exibição de área**.

2 Clique em **Adicionar uma entidade** ( ) > **Sequência de câmeras**.

Uma nova entidade de sequência de câmeras ( ) aparecerá na visualização de área.

3 Digite um nome para a sequência de câmeras e pressione **ENTER**.

4 Clique na aba **Câmeras** e clique em **Adicionar um item** ( ).

5 Na lista suspensa **Câmera**, selecione uma câmera para fazer parte da sequência.

6 Na caixa **Tempo de permanência**, defina a quantidade de tempo que a câmera será exibida quando estiver circulando pela sequência.

7 Na lista suspensa **Comando PTZ**, selecione qual ação a câmera PTZ realizará quando for exibida na sequência.

Esta opção é apenas para as câmeras habilitadas para PTZ.

- **Predefinição:** Move a câmera PTZ para uma posição predefinida.
- **Posição:** Inicia um padrão PTZ.

8 Na lista suspensa **Auxiliar de PTZ**, configure o número do interruptor e o estado para o qual defini-lo.

Esta opção é apenas para câmeras habilitadas para PTZ que suportam interruptores auxiliares.

9 Clique em **Salvar** > **Aplicar**.

10 Se necessário, inclua câmeras adicionais na sequência.

11 Para alterar a ordem das câmeras na sequência, use os botões e .

12 Para remover uma câmera da sequência, selecione a câmera e clique em **Remover o item** ( ).

13 Clique em **Aplicar**.

Tópicos relacionados

Sobre sequências de câmeras na página 509

Sobre monitores analógicos

É um tipo de entidade que representa um monitor que exibe vídeos a partir de uma fonte analógica, como um decodificador ou câmera analógica. Este termo é usado no Security Center para se referir aos monitores que não são controlados por um computador.

É um dispositivo que converte um stream de vídeo digital em sinais analógicos (NTCS ou PAL) para exibir em um monitor analógico. É um dos muitos dispositivos encontrados em uma unidade de decodificação de vídeo. Uma unidade de decodificação de vídeo pode ter vários decodificadores de vídeo, cada um ligado a um monitor analógico. Cada decodificador de vídeo encontrado numa unidade de decodificação de vídeo é representado por uma entidade de monitor analógico no Security Center.

A entidade *grupo de monitores* é usada para configurar as propriedades de um grupo de monitores analógicos.

Configurar monitores analógicos

Para obter um desempenho ideal com seu monitor analógico, defina suas configurações.

O que você deve saber

As entidades de monitor analógico são criadas automaticamente quando as unidades de decodificação de vídeo às quais elas estão conectadas são adicionadas ao seu sistema. Embora o Security Center forneça configurações padrão operacionais quando entidades de monitor analógico são adicionadas, recomendamos configurar cada monitor analógico.

Para configurar monitores analógicos:

1 Adicione uma unidade de decodificação de vídeo ao seu sistema.
2 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
3 Selecione um monitor analógico para configurar e clique na aba **Propriedades**.
4 Defina as configurações de vídeo, as configurações de rede e o hardware conectado ao monitor analógico.
5 Clique em **Aplicar**.
6 Configure cada monitor analógico conectado ao decodificador.

Tópicos relacionados

Monitor analógico - Aba Propriedades na página 982

Adicionar monitores analógicos como destinatários de alarmes

Para receber alarmes em seus monitores analógicos físicos, você deve criar um grupo de monitores e, em seguida, adicionar esse grupo como destinatário do alarme.

O que você deve saber

Quando você recebe alarmes em um monitor analógico, os alarmes de alta prioridade não substituem os alarmes de prioridade inferior que são exibidos no monitor. Para obter mais informações sobre como visualizar vídeo ou receber alarmes em monitores analógicos no Security Desk, consulte o *Guia do Usuário do Security Desk*.

IMPORTANTE: Se você adicionar mais de um monitor analógico a um grupo de monitores, o primeiro monitor analógico na lista receberá o alarme de prioridade mais alta, o segundo monitor analógico receberá o segundo alarme de maior prioridade e assim por diante. O último monitor analógico na lista do grupo de monitores receberá todos os outros alarmes.

Para adicionar monitores analógicos como destinatários de alarmes:

1 Abra a tarefa **Alarmes** e clique na visualização **Grupos de monitores**.
2 Clique em **Grupo de monitores** ( ) e digite um nome para o seu grupo de monitores.
3 Selecione o grupo de monitores e clique na aba **Monitores**.
4 Na parte inferior da página, clique em , selecione os monitores analógicos a serem incluídos no grupo de monitores e clique em **OK**.

   Você pode selecionar vários monitores analógicos segurando as teclas Shift ou Ctrl.

5 Clique em **Aplicar**.
6 Na tarefa **Alarmes**, clique na visualização **Alarmes** , selecione um alarme e, em seguida, clique na aba **Propriedades**.
7 Na seção **Destinatários**, clique em , selecione os grupos de monitores que serão destinatários do alarme e clique em **OK**.

8 Clique em **Aplicar**.

Quando o alarme é acionado, o vídeo associado ao alarme é mostrado no monitor analógico físico.

Testar configurações de monitores analógicos

Depois de configurar seus monitores analógicos, você deve sempre testar para se certificar de que você pode ver vídeo nos monitores analógicos.

Antes de iniciar

Certifique-se de que as câmeras com as quais deseja testar a exibição de vídeo são suportadas (do mesmo fabricante que o decodificador e usam o mesmo formato de vídeo).

O que você deve saber

Para obter mais informações sobre como visualizar vídeo em um monitor analógico no Security Desk, consulte o *Guia do Usuário do Security Desk*.

Para testar as configurações de monitores analógicos:

1 Abra o Security Desk.
2 Na tarefa Monitoramento, exiba um monitor analógico em um ladrilho na tela e, em seguida, adicione uma câmera suportada ao ladrilho.

Câmeras usadas junto ao corpo

Uma câmera usada junto ao corpo (BWC), também conhecida como câmera corporal, é um sistema de gravação de vídeo tipicamente usado por agentes da lei para gravar suas interações com o público ou coletar evidências em vídeo de cenários de crime.

Função Body-Worn Camera Manager

A Body-Worn Camera Manager é a função usada para configurar e gerenciar câmeras usadas junto ao corpo no Security Center. Isto inclui configurar câmeras ou estações de câmeras, adicionar usuários, carregar conteúdo para um Archiver e definir o período de retenção de evidências carregadas.

Esta função do Security Center é usada quando os usuários não carregam ou não podem carregar seus dados de evidência na nuvem (Genetec Clearance™) ou quando os usuários desejam acessar as funções Archiver do Security Center, como o período de retenção.

Os arquivos da câmera usada junto ao corpo podem ser pesquisados usando a tarefa *Arquivos* no Security Desk.

Genetec Clearance™ Uploader

A Genetec Clearance™ Uploader é um aplicativo usado para carregar automaticamente uma mídia de uma câmera usada junto ao corpo ou pasta de sincronização, ou outro dispositivo para o Genetec Clearance™ ou um arquivo de vídeo Security Center dependendo do arquivo de configuração *.json* que seja usado.

Tópicos relacionados

Configurar câmeras usadas junto ao corpo na página 515
Adicionar câmeras ou usuários à função Body-Worn Camera Manager na página 517

Configurar câmeras usadas junto ao corpo

Para usar o Security Center para carregar evidências de uma câmera usada junto ao corpo (BWC) ou pasta de sincronização para um arquivo do Security Center, você deve configurar a função Body-Worn Camera Manager.

Antes de iniciar

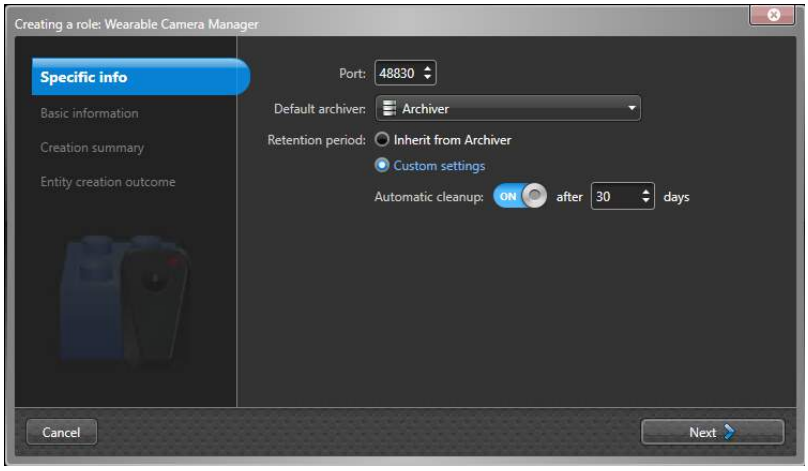
- Certifique-se de ter uma licença válida de *câmera usada junto ao corpo* (Número do componente: GSC-Om-X-1BWC).
- Familiarize-se com o Genetec Clearance™ Uploader no *Guia do Usuário do Genetec Clearance™*.
- Instale o Genetec Clearance™ Uploader. Para mais informações, consulte Instalar o Genetec Clearance™ Uploader no *Guia do Usuário do Genetec Clearance™*.

O que você deve saber

- O arquivamento redundante ou failover não é suportado ao usar câmeras usadas junto ao corpo.
- Para obter uma lista de *câmeras usadas junto ao corpo* que são suportadas no Security Center, consulte a nossa Lista de Dispositivos Suportados.
- O arquivo de configuração *.json* é usado para definir para o Genetec Clearance™ Uploader onde contactar a função e para proteger a comunicação.

Para configurar câmeras usadas junto ao corpo

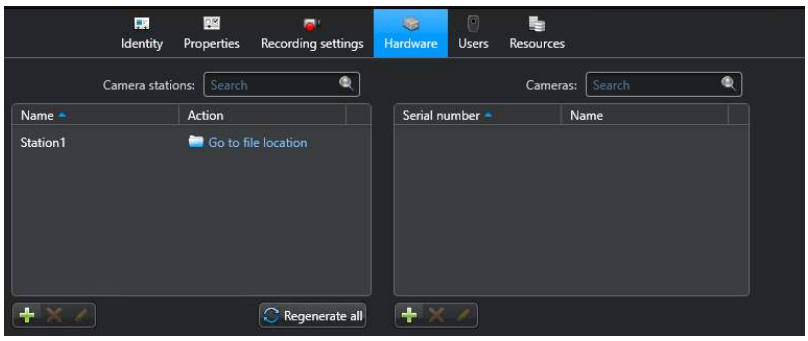
1 Crie uma função Body-Worn Camera Manager.
   a) Na tarefa Sistema, clique em **Funções** > **Adicionar uma entidade** > **Body-Worn Camera Manager**.
   b) (Opcional) Na seção *Informações específicas*, clique em **Configurações personalizadas**, selecione um período de retenção e clique em **Próximo**.



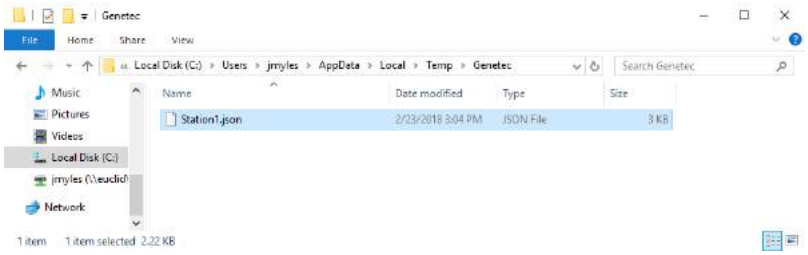
   Selecionar um período de retenção automaticamente assegura que os vídeos mais antigos são excluídos após o período especificado.

   IMPORTANTE: Os arquivos importados não devem ser mais antigos do que período de retenção atual.

   c) Na seção *Informações básicas*, digite o nome de uma Entidade e clique em **Próximo**.
   d) Na seção *Resumo de criação*, clique em **Criar**.
2 Configure a estação de câmeras.
   a) Na seção **Estações de câmeras** da aba *Hardware*, clique em .
   b) Digite um nome para a estação e clique em **Aplicar**.



c) Na seção *Estações de câmeras*, clique em **Ir para localização do arquivo** e copie ou transfira o arquivo *.json* para a estação de câmeras ou para uma localização que possa ser acessada pelo Genetec Clearance™ Uploader.



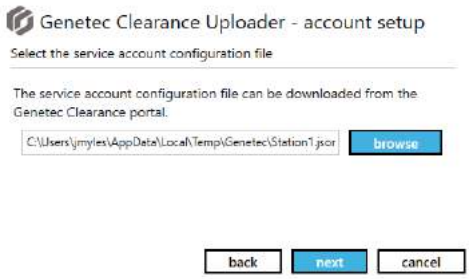
NOTA: Neste exemplo, usamos Genetec Clearance™ Uploader.

d) (Opcional) Exclua as estações de câmeras que já não são necessárias. Selecione uma **Estação de câmeras** e clique em .

3 (Opcional) Adicione uma câmera ou um usuário.

4 Configure o Genetec Clearance™ Uploader.

a) No Genetec Clearance™ Uploader (assistente Configuração de Contas), navegue para e selecione o arquivo de configuração *.json* da estação de câmeras e conclua as etapas necessárias.



IMPORTANTE: Certifique-se de excluir o arquivo de configuração original da respectiva localização de download ou cópia após tê-lo transferido com sucesso. Por exemplo, *C:\Users\username\AppData\Local\Temp\Genetec*.

5 (Opcional) Defina uma pasta de sincronização.

a) Na seção *Configurações* de do Genetec Clearance™ Uploader, defina a **Pasta de sincronização** para **Ligado** se desejar carregar automaticamente arquivos na pasta para Security Center.

IMPORTANTE: Alterar a configuração da **Pasta de sincronização** implica que o serviço Genetec Clearance™ Uploader seja manualmente reiniciado. A **Pasta de sincronização** que você definiu é automaticamente criada para você depois que o serviço seja reiniciado.

Após terminar

Agora já é possível acoplar ou conectar a sua câmera usada junto ao corpo ou arrastar arquivos de evidência para a pasta de sincronização.

- O carregamento começa quando uma câmera é conectada ao Genetec Clearance™ Uploader ou quando a pasta de sincronização contém novos arquivos. As evidências são carregadas automaticamente, não é necessária qualquer intervenção.
- Após conclusão do carregamento, poderá localizar e visualizar as evidências carregadas em Security Desk usando o relatório Arquivos na tarefa **Arquivos**.

  NOTA: Dependendo do tamanho e do número de arquivos de evidência carregados, os vídeos podem não aparecer nos arquivos do Security Desk imediatamente.

Tópicos relacionados

Câmeras usadas junto ao corpo na página 514
O relatório Arquivos de câmera usada junto ao corpo está vazio na página 587

Adicionar câmeras ou usuários à função Body-Worn Camera Manager

Você pode adicionar câmeras ou usuários à função Body-Worn Camera Manager automática ou manualmente A criação automática apenas ocorre quando há um vídeo na câmera usada junto ao corpo a ser carregado. Se deseja atribuir uma nova câmera a um usuário existente, use o processo manual para evitar a criação de um novo usuário.

Antes de iniciar

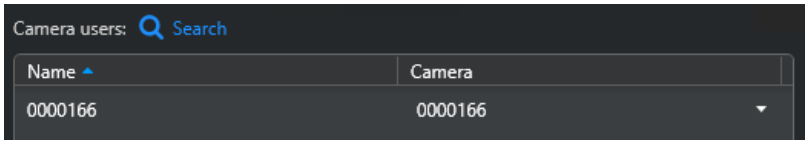
Certifique-se de ter uma licença válida de *câmera usada junto ao corpo* (Número do componente: GSC-Om-X-1BWC).

O que você deve saber

- O arquivamento redundante ou failover não é suportado ao usar câmeras usadas junto ao corpo.
- Para obter uma lista de *câmeras usadas junto ao corpo* que são suportadas no Security Center, consulte a nossa Lista de Dispositivos Suportados.

O carregamento começa quando uma câmera é conectada ao Genetec Clearance™ Uploader ou quando a pasta de sincronização contém novos arquivos.

- Se o dispositivo de câmera usada junto ao corpo foi configurado previamente, a câmera é criada automaticamente com o número de série do dispositivo de câmera. Nesta situação, o usuário de câmera é criado ao mesmo tempo.
- Se o usuário é automaticamente criado, o **Nome** do usuário de câmera é igual ao número de série da **Câmera**.

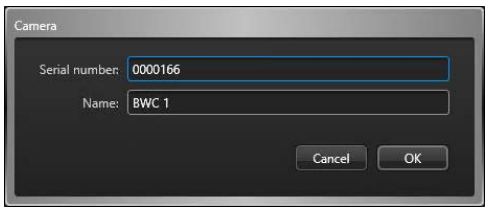


NOTA: O dispositivo e usuário de câmera podem ser modificados após serem criados. Escolha nomes que possam ser usados para ajudá-lo a rastrear e encontrar o seu vídeo importado.

Adicionar câmeras manualmente:

1 Adicionar uma câmera. Na seção **Câmeras** da aba *Hardware*, clique em .

a) Na caixa de diálogo *Câmera*, insira um **Número de série** e **Nome** e, em seguida, clique em **OK**.



IMPORTANTE: Certifique-se de inserir o número de série correto. Este número de série é usado para corresponder um dispositivo do número de série na solicitação de carregamento e o número de série na aba **Hardware** da função Body-Worn Camera Manager.

2 (Opcional) Clique em para modificar uma câmera salva anteriormente.

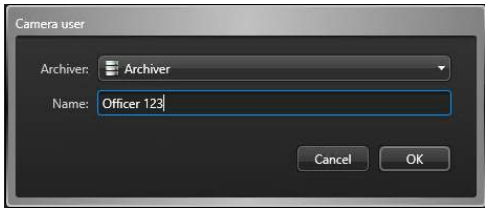
3 (Opcional) Clique em para excluir câmeras que já não são necessárias.

4 Clique em **Aplicar**.

Adicionar usuários de câmera manualmente:

1 Adicionar um usuário de câmera. Na seção **Câmeras** da aba *Usuários*, clique em .

a) Na caixa de diálogo *Usuário de câmera*, selecione um **Archiver** da lista **Archiver**.



b) Insira um **Nome** e clique em **OK**.

2 (Opcional) Modifique um usuário salvo anteriormente. Selecione um **Uusário de câmera**e clique em para ir para a página de configuração da entidade selecionada e fazer as alterações necessárias.

3 (Opcional) Exclua um usuário que já não é necessário. Selecione um **Usuário de câmera** e clique em para ir para a página de configuração da entidade selecionada. Selecione o **Usuário de câmera** na Exibição de área e clique em .

4 Clique em **Aplicar**.

Tópicos relacionados

Câmeras usadas junto ao corpo na página 514

26

Arquivos de vídeos

Esta seção inclui os seguintes tópicos:

- "Sobre arquivos de vídeos" na página 520
- "Gerenciar arquivos de vídeos" na página 522
- "Distribuir o armazenamento de arquivos por múltiplos discos" na página 523
- "Monitorar o espaço em disco disponível para arquivos de vídeo" na página 524
- "Transferir arquivos de vídeo" na página 527
- "Proteger arquivos de vídeo contra exclusão" na página 537
- "Proteção de arquivos de vídeo contra adulteração" na página 539
- "Exibir propriedades de arquivos de vídeo" na página 540
- "Gerenciar os efeitos do Horário de Verão em arquivos de vídeo" na página 542
- "Importar arquivos de vídeo externos para o Security Center" na página 544

Sobre arquivos de vídeos

Um arquivo de vídeo é uma coleção de transmissões de vídeo, áudio e metadados gerida por uma tarefa de Archiver ou Archiver auxiliar. Estas coleções são catalogadas no banco de dados de arquivos, que inclui eventos de câmera vinculados às gravações.

Cada Archiver e Archiver auxiliar é responsável pelos arquivo de vídeos das *câmeras* que controla. Os arquivos de vídeo são divididos no banco de dados do arquivo e o armazenamento de arquivos.

Banco de dados de arquivos

O banco de dados de arquivos em seu sistema Security Center armazena um catálogo de vídeos e eventos. Cada função Archiver e função Archiver auxiliar em seu sistema mantém um banco de dados de arquivos.

O banco de dados de arquivos armazena os seguintes tipos de informações:

- Um catálogo de filmagens gravadas.
- Eventos que descrevem as atividades de gravação, como quando a gravação foi iniciada e interrompida e o que desencadeou o evento.
- Eventos associados às filmagens gravadas, como movimento detectado, *marcadores* e metadados ocasionais.
- Eventos relacionados ao processo de arquivamento, como *A carga do disco está acima de 80%* e *Não é possível gravar em nenhuma unidade*.

Para funções Archiver, o nome padrão do banco de dados é *Archiver*. Para funções Archiver auxiliar, o nome padrão do banco de dados é *AuxiliaryArchiver* .

IMPORTANTE: Um banco de dados de arquivos separado deve ser configurado para cada servidor atribuído à função Archiver ou Archiver auxiliar. Devido a este requisito, é recomendado hospedar o banco de dados de arquivos localmente em cada servidor. Quando duas ou mais funções de arquivamento estão hospedadas no mesmo servidor, você deve atribuir um banco de dados diferente a cada função em vez de usar o padrão.

Tópicos relacionados

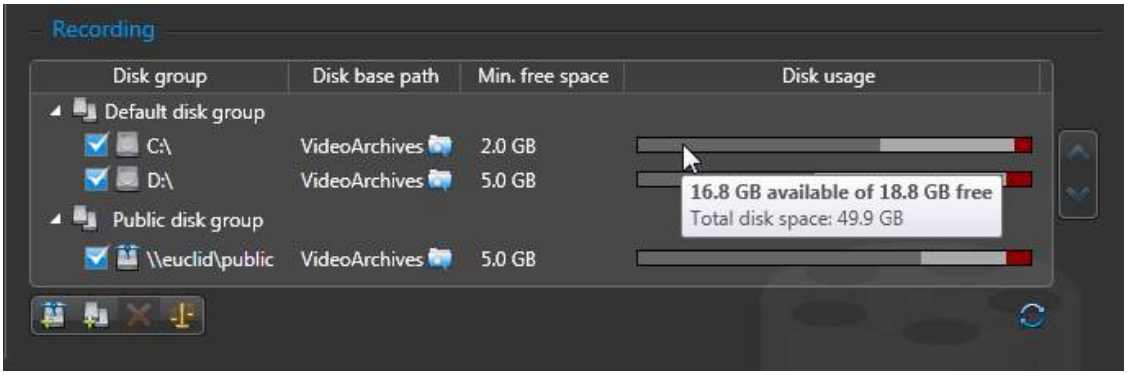
Bancos de dados na página 138

Armazenamento de arquivos

No Security Center, as gravações de vídeo são armazenadas em disco, em pequenos arquivos G64 que contêm uma ou mais pequenas sequências de vídeos.

Semelhante ao banco de dados de arquivos, o armazenamento de arquivos é específico para cada servidor. A localização dos arquivos de vídeo e a descrição das *sequências de vídeos* que eles contêm (câmera de origem, início e fim da sequência) são armazenados no catálogo do banco de dados gerenciado pelo *Archiver* ou *Archiver auxiliar*.

As unidades locais e unidades de rede podem ser usadas para armazenar vídeo. Na aba **Recursos** da função de arquivamento, todas as unidades locais encontradas no servidor host são listadas por padrão e agrupadas no *Grupo de discos padrão*, como mostrado na imagem a seguir:



O espaço em disco não pode ser alocado antecipadamente para arquivos de vídeos. Em vez disso, as funções de arquivamento somente podem utilizar uma quantidade limitada do espaço disponível em disco. Este limite é definido pelo atributo **Espaço livre mín.** para cada disco. O espaço livre mínimo recomendado é, pelo menos, 1% do espaço total em disco.

IMPORTANTE: Você deve garantir que o usuário do serviço executando a função Archiver ou Archiver auxiliar tenha acesso de gravação a todas as pastas raiz de arquivos atribuídas à função.

Requisitos de armazenamento de arquivos

Como a função Archiver e as funções Archiver auxiliar podem controlar um número diferente de câmeras, você deve avaliar separadamente os requisitos de armazenamento para cada uma dessas funções.

Os requisitos de armazenamento são afetados pelos seguintes fatores:

- Número de câmeras das quais arquivar.
- Período de retenção de arquivos: quantidade de tempo durante o qual os arquivos são mantidos online.
- Porcentagem de arquivos de vídeos protegidos contra exclusão automática.
- Porcentagem de tempo de gravação, que depende do modo de arquivamento selecionado: contínuo, em movimento, manual, agendado ou desativado. A gravação contínua consome espaço em disco mais rápido que cada um dos outros modos de arquivamento.
- Taxa de quadros: gravações com taxas de quadros mais elevadas requerem mais espaço de armazenamento.
- Resolução de imagem, que depende do formato de dados do vídeo: gravações com resolução mais elevada requerem mais espaço de armazenamento.
- Porcentagem de movimento: a maioria dos esquemas de codificação de vídeo comprime os dados armazenando apenas as mudanças entre quadros consecutivos. Cenas com muito movimento requerem mais espaço de armazenamento do que cenas com pouco movimento.
- Áudio: incluir áudio aumenta o espaço de armazenamento necessário.
- Metadados de recursos como *análise de vídeo*, *proteção de privacidade* e *criptografia de fluxo de fusão*. Incluir metadados pode aumentar o espaço de armazenamento necessário.

DICA: Verificar regularmente as estatísticas de uso de discos é a melhor maneira de estimar requisitos de armazenamento futuros e fazer ajustes rapidamente.

Tópicos relacionados

Câmera - Aba vídeo na página 989
Liberando espaço de armazenamento para arquivos de vídeo na página 525
Definir configurações de gravação de câmeras na página 451
Monitorar o espaço em disco disponível para arquivos de vídeo na página 524

Gerenciar arquivos de vídeos

Você deve trabalhar com seus arquivo de vídeos para garantir que as gravações estão sempre disponíveis para auxiliar em investigações.

O Security Center armazena vídeos de vigilância como *arquivos de vídeos*. Você controla onde os arquivos são armazenados e por quanto tempo eles são retidos. Para garantir que seus vídeos são corretamente arquivados e estão disponíveis quando necessário, você deve executar as seguintes tarefas:

- Verificar os requisitos de armazenamento de arquivos para garantir que tem espaço suficiente para as gravações de vídeo.
- Se o desempenho do armazenamento for um problema, considere distribuir o armazenamento de arquivos por vários discos.
- Monitore regularmente quanto espaço livre em disco existe para assegurar que sempre existe espaço suficiente para novas gravações.
- Quando necessário, libere espaço em disco excluindo arquivos de vídeo mais antigos, diminuindo períodos de retenção para câmeras e assim por diante.
- Garanta que as gravações são corretamente arquivadas, facilmente acessíveis e estão protegidas. Você pode:
  - Transferir gravações de vídeo de câmeras ou outros dispositivos avançados para seus arquivos de vídeos.
  - Copiar arquivos de vídeo de uma função Archiver para outra.
  - Fazer backup de arquivos de vídeos para protegê-los contra perda.
  - Restaurar arquivos de vídeos de um backup para um Archiver.
- Proteger arquivos de vídeo importantes contra exclusão automática.
- Proteger arquivos de vídeo importantes contra a adulteração adicionando marcas d'água.
- Auditar o armazenamento de arquivos revisando as propriedades dos arquivos de vídeo.
- Se necessário, gerir os efeitos do Horário de Verão nos seus arquivos de vídeos.
- Importar arquivos de vídeo externos para o Security Center.

Distribuir o armazenamento de arquivos por múltiplos discos

Para evitar um gargalo no Archiver ou Auxiliary Archiver devido à taxa de transferência do disco, você pode habilitar a função para gravar simultaneamente em vários discos.

O que você deve saber

As funções Archiver e Archiver auxiliar podem gravar em vários discos, espalhando o arquivo de vídeos por vários *grupos de discos*. Cada grupo de discos deve corresponder a um controlador de disco separado. Ao dividir o arquivo de vídeos de câmeras diferentes por diferentes grupos de disco, você pode maximizar a taxa de transferência em termos de acesso a discos.

CUIDADO: Nada impede que outros aplicativos usem o espaço em disco reservado para o Archiver ou Archiver auxiliar, por isso é recomendável atribuir um disco a estas funções que não seja compartilhado com outros aplicativos. Nos casos em que vários Archivers compartilhem o mesmo servidor, use um disco separado para cada um.

Para distribuir as câmeras de arquivamento em vários grupos de discos:

1. Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2. Selecione a função Archiver e clique na aba **Recursos**.
3. Para criar um grupo de discos, clique em **Adicionar grupo** ( ).
4. Na coluna **Grupo de discos**, clique em **Novo grupo de discos** e digite um nome para o grupo.
5. Clique em **Distribuição de câmeras** ( ).
6. Na caixa de diálogo **Distribuição de câmeras**, divida as câmeras entre os grupos de discos, selecionando-as uma de cada vez e movendo-as com os botões de seta.
7. Clique em **Fechar** > **Aplicar**.

Monitorar o espaço em disco disponível para arquivos de vídeo

Para evitar uma paragem repentina do arquivamento de vídeo, você deve monitorar regularmente o espaço em disco que ainda resta.

O que você deve saber

Demasiados arquivos de vídeos protegidos em um disco podem esgotar o espaço de armazenamento disponível para novos arquivos de vídeo. Ao verificar regularmente o espaço em disco, também deverá verificar a porcentagem de arquivos de vídeo em cada disco.

DICA: Você também pode criar um *evento causa-efeito* para alertá-lo quando um Archiver ou um Archiver auxiliar está ficando sem espaço em disco ou deixou de arquivar.

Para monitorar o espaço em disco disponível para arquivos de vídeo:

1 Abra a tarefa *Vídeo* e selecione a função do Archiver ou Archiver auxiliar.

2 Clique na aba **Recursos** , em seguida clique em **Estatísticas** ( ).

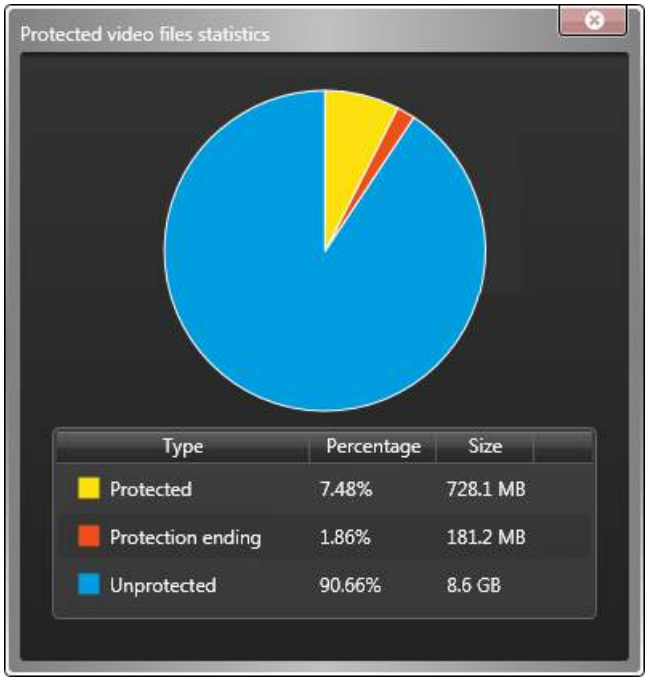
3 Na caixa de diálogo *Estatísticas*, clique em **Atualizar** ( ) para visualizar as últimas informações.

NOTA: As informações na caixa de diálogo *Estatísticas* não são atualizadas automaticamente. Se forem exibidas informações, o carimbo de data e hora da **Última atualização** mostra quando essas informações foram atualizadas pela última vez.

4 Na caixa de diálogo *Estatísticas* , confira as seguintes estatísticas:

- **Espaço disponível:** Espaço em disco disponível para arquivos em vídeo.
- **Uso médio de disco:** O espaço médio usado por dia (primeira linha) e espaço médio usado por câmera por dia (segunda linha).
- **Tempo de gravação restante estimado:** Número de dias, horas e minutos de tempo de gravação restantes com base na média de utilização de disco e a carga atual.
- **Câmeras ativas:** Número de câmeras ativas no momento.
- **Arquivando câmeras:** Número de câmeras que têm o arquivamento habilitado.

5 Selecione um grupo de discos e clique no ícone ( ) para abrir *Estatísticas de arquivos de vídeo protegidos*.



O gráfico pizza indica o status dos arquivos de vídeo no disco, conforme é mostrado:

- **Protegido:** Porcentagem de arquivos de vídeo no disco que estão protegidos atualmente.
- **Proteção finalizada:** Porcentagem de arquivos de vídeo no disco que um usuário decidiu desproteger. Quando um usuário escolhe remover a proteção de um arquivo de vídeo, o Archiver aguarda 24 horas antes de remover a proteção do arquivo. Durante esse tempo, o status indica *Proteção finalizada*.
- **Desprotegido:** Porcentagem de arquivos de vídeo no disco que não estão protegidos.

Após terminar

Se o disco estiver ficando cheio, considere verificar os arquivos de vídeos para ver se há vídeos que possam ser excluídos. Você também pode definir as configurações do Archiver para liberar o máximo possível de espaço em disco.

Liberando espaço de armazenamento para arquivos de vídeo

Dentro de cada grupo de discos, você pode liberar espaço de armazenamento para novos arquivos de vídeo.

Antes de iniciar

O que você deve saber

Há diferentes maneiras de liberar espaço de armazenamento para arquivos de vídeo. Usar uma combinação das seguintes estratégias pode ajudar a maximizar o armazenamento disponível:

- Excluir os arquivos de vídeo mais antigos quando o espaço disponível em disco ficar baixo. Essa estratégia é recomendada se a maioria de suas filmagens forem igualmente importantes e você quiser manter o máximo possível de filmagens. Isso maximiza o uso do disco.
- Configurar períodos de retenção de arquivos para câmeras para especificar o tempo que as filmagens gravadas devem ser mantidas online. O vídeo é excluído automaticamente no fim do período de retenção. Essa estratégia mantém as filmagens mais importantes por um período mais longo.

- Limita o tamanho e a duração dos arquivos de vídeo. Se você protege diversas sequências curtas de vídeos para que não sejam excluídas, limitar o tamanho dos seus arquivos de vídeo pode ajudar a optimizar o seu uso do armazenamento.
- Limite o espaço de disco alocado para arquivo de vídeo protegidos; eles não são excluídos automaticamente durante os procedimentos de limpeza normais.

IMPORTANTE: O arquivamento é interrompido quando o espaço acaba. É altamente recomendado que você alinhe as estratégias de retenção de arquivo com o espaço de armazenamento disponível. Somente a exclusão de arquivos pode afetar o desempenho do arquivamento quando o armazenamento estiver cheio.

Para liberar espaço de armazenamento para arquivos de vídeo:

1 Abra a tarefa *Vídeo* e selecione a função do Archiver ou Auxiliary Archiver a configurar.
2 Clique na aba **Recursos**, em seguida clique em **Configurações avançadas**.
3 Na janela *Configurações avançadas*, defina as seguintes opções, como necessário:
   - Defina a opção **Excluir arquivos de vídeo mais antigos quando os discos estiverem cheios** para **Ligado**.
   - Defina a opção **Limiar de proteção de vídeo** na porcentagem máxima de espaço de armazenamento que os arquivos de vídeo podem ocupar em disco.

     Quando esse limiar é ultrapassado, o Archiver gera um evento *Limiar de proteção de vídeo excedido*a cada 15 minutos, para que você possa rever os arquivos de vídeo e excluir os que não são mais necessários. O Archiver não exclui os arquivos protegidos.
   - Na seção *Arquivos de vídeo*, defina:
     - A **Duração máxima** para sequências de vídeo, em minutos.
     - O **Tamanho máximo** de arquivos de vídeo. Selecione **Específico** e defina um tamanho máximo, em megabytes.
4 Depois de definir as configurações avançadas, clique em **OK** > **Aplicar**.

Para definir um período de retenção para um vídeo armazenado pelo Archiver ou Auxiliary Archiver:

1 Na tarefa *Vídeo*, selecione um Archiver ou Auxiliary Archiver na árvore de entidades de função e realize uma das ações a seguir:
   - Para uma função Archiver, clique na aba **Configurações padrão da câmera**.
   - Para uma função Auxiliary Archiver, clique na aba **Gravação da câmera**.
2 Defina **Limpeza automática**, para o número de dias exigido e clique em **Aplicar**.

Definir um período de retenção para uma câmera específica:

1 Na tarefa *Vídeo*, expanda a árvore de entidades de função e selecione a câmera.
   Isso é útil para câmeras que têm filmagens mais importantes.

   DICA: Você pode querer definir um período de retenção mais curto para câmeras PTZ, porque elas muitas vezes usam mais armazenamento devido ao aumento do movimento.
2 Clique na aba **Gravação**.
3 Se as **Configurações de gravação** estiverem definidas para **Herdar de Archiver**, altere para **Configurações personalizadas**.
4 Defina **Limpeza automática**, para o número de dias exigido e clique em **Aplicar**.

Transferir arquivos de vídeo

Utilize Security Center para mover arquivos de vídeo entre localizações. Mover vídeos garante que eles ficam devidamente arquivados, facilmente acessíveis e protegidos.

O Security Center permite gerir dinamicamente onde seus arquivos de vídeo são armazenados com transferência de arquivo. Com a transferência de arquivo, você pode:

- Transferir gravações de vídeo de câmeras ou outros dispositivos avançados para seus arquivos de vídeos.
- Copiar arquivos de vídeo de uma função Archiver para outra.
- Fazer backup de arquivos de vídeos para protegê-los contra perda.
- Restaurar arquivos de vídeos de um backup para um Archiver.

Com a transferência de arquivo, você obtém controle total dos locais onde suas gravações de vídeo são armazenadas. Esta flexibilidade reduz os custos com armazenamento de arquivos de longo prazo e ajuda a otimizar a pesquisa de vídeos e o desempenho investigativo.

Para melhor gerir transferências repetitivas, você pode definir *grupos de transferência*. Um grupo de transferência é um cenário de transferência de arquivos persistente que permite executar uma transferência de vídeo sem redefinir as configurações de transferência. Estas transferências podem ser agendadas ou executadas sob demanda. Os grupos de transferência definem quais câmeras ou funções de arquivamento estão inclusas na transferência, quando os arquivos são transferidos, quais dados são transferidos e assim por diante.

NOTA: Somente os administradores de sistema podem definir as configurações de transferência de arquivo.

Os grupos de transferência somente movem novos vídeos. Por exemplo, se o último quadro de vídeo recuperado de uma unidade for "7/30/2014 3:44:40" e você tentar recuperar vídeo entre 3:40:00 e 3:50:00, apenas vídeo entre 3:44:40 e 3:50:00 é recuperado e armazenado no Archiver.

Antes de uma grande operação, como uma atualização de software ou a substituição de um servidor, a transferência de arquivo permite agir rapidamente para mover arquivos de vídeos importantes sem criar um grupo de transferência.

Além das gravações de vídeo, as seguintes informações são enviadas junto com uma transferência de arquivo, se disponíveis:

- Áudio e metadados
- Marcas d'água de vídeo
- Configurações de bloqueio de câmera
- Configurações de proteção

Quando o vídeo é transferido para um Archiver, ele é conservado de acordo com o período de retenção desse Archiver.

Limitações da transferência de arquivo

Somente é possível transferir arquivos originais entre Archivers. Por exemplo, os arquivos só podem ser duplicados do Archiver onde o vídeo foi gravado originalmente.

Solução de problemas de transferência de arquivo

Se o Archiver ficar offline durante uma transferência de arquivo e o processo for interrompido, a transferência deve ser reiniciada depois que o Archiver for reconectado.

- Se você estava executando uma transferência de arquivo manual, então você deve reiniciar o processo manualmente.

- Se a transferência de arquivo estava definida para ser executada segundo uma agenda, a transferência será reiniciada na próxima hora agendada.

NOTA: A transferência de arquivo reinicia no último quadro transferido com êxito.

Tópicos relacionados

Consolidar arquivos de vídeo após failover do Archiver na página 193

Recuperar gravações de vídeo das unidades

Para armazenar vídeo em suas unidades de vídeo, e periodicamente transferir essas gravações para o Security Center, é necessário ativar a gravação avançada nas unidades e configurar as câmeras para transferir vídeo para seu Archiver principal.

Antes de iniciar

Você deve determinar se a unidade de vídeo suporta gravação avançada e transferência de arquivos. Para saber quais dispositivos avançados são suportados atualmente, entre em contato com a Assistência Técnica da Genetec™.

O que você deve saber

Você pode configurar os arquivos para serem recuperados automaticamente quando a unidade se conectar ao Archiver.

Você pode continuar a gravar vídeo no Archiver, mesmo que a câmera esteja configurada para transferência de arquivo. As câmeras só podem ser adicionadas a um grupo de transferência para recuperar gravações de vídeo de unidades.

A transferência de arquivos de unidades para Archivers é útil nos seguintes cenários:

- Para locais remotos conectados a um local central com largura de banda limitada: Geralmente, um servidor é implantado no local remoto para hospedar a gravação. No entanto, com a transferência de arquivos, você pode recuperar o vídeo diretamente das câmeras sob demanda sem precisar de um servidor.
- Para vigilância na cidade inteira usando câmeras de gravação avançada: As câmeras estão sempre gravando. As gravações só são recuperadas sob demanda para fins de investigação ou fora dos horários de pico.
- Se houver uma falha de rede, as partes de vídeo que estão faltando nas gravações do Archiver podem ser recuperadas da unidade de vídeo.

Para recuperar arquivos de vídeo das unidades:

1 Habilite a gravação avançada na unidade de vídeo.
2 Selecione quais câmeras transferirão arquivos de vídeo para o Archiver e defina as configurações de transferência. Você pode definir que as transferências ocorram no momento da conexão, segundo uma agenda ou manualmente.

Tópicos relacionados

Transferir arquivos de vídeo na página 527
Duplicar arquivo de vídeos na página 530

Ativar a gravação avançada

Para armazenar gravações em uma unidade de vídeo, você deve ativar a gravação avançada nas configurações da unidade. O Security Center pode recuperar essas gravações e transferi-las para um Archiver.

O que você deve saber

Você pode definir a gravação de vídeo como sendo contínua ou acionada por eventos específicos, como entradas, movimento, análise e assim por diante. A gravação em unidade só pode ser ativada a partir da página Web da unidade.

NOTA: As unidades Bosch suportam gravação em um dispositivo separado das unidades de vídeo. Para obter informações sobre como habilitar a gravação avançada em unidades Bosch, consulte o *Guia de Configuração de Unidades de Vídeo do Security Center*.

Para ativar a gravação avançada:

1 Abrir a tarefa *Vídeo*.

2 Selecione a unidade de vídeo e clique em **Unidade** > **Página Web da unidade** ( ) na barra de ferramentas localizada na parte inferior do espaço de trabalho.

3 Após abrir a página Web da unidade, siga as instruções do fabricante da unidade para habilitar a gravação.

4 Feche a janela do navegador da Web quando terminar.

Definir configurações de transferência de vídeo para câmeras

Para transferir gravações de vídeo de unidades de vídeo para o Security Center, você deve definir as configurações de transferência de vídeo para essas câmeras, como o tipo de dados de vídeo que deseja baixar e quando.

Antes de iniciar

Habilite a gravação avançada em todas as câmeras necessárias.

Para definir configurações de transferência de vídeo para câmeras:

1 Na página inicial do Config Tool, abra a tarefa *Transferência de arquivos*.

2 Clique em **Adicionar um item ( )** > **Recuperar da unidade** .

3 Na caixa de diálogo *Propriedades do grupo de transferência*, digite um nome para este cenário de transferência de arquivos.

4 Na seção *Origens*, clique em **Adicionar um item ( )** , selecione as câmeras que deseja e clique em **Adicionar**.

DICA: Mantenha pressionado Ctrl ou Shift para selecionar várias câmeras.

5 Para **Recorrência**, selecione uma agenda para a transferência de arquivos:

- **Manual:** Transfere arquivos manualmente.
- **Minutos:** Transfere arquivos a cada 1–59 minutos.
- **A cada hora:** Transfere arquivos a cada 1–23 horas.
- **Diariamente:** Transfere arquivos todos os dias a uma hora especificada. Opcionalmente, defina uma duração máxima para a conclusão da transferência.
- **Semanalmente:** Transfere arquivos todas as semanas, em dias específicos a uma hora especificada. Opcionalmente, defina uma duração máxima para a conclusão da transferência.

NOTA: Se você definir uma duração máxima de transferência de arquivos para uma agenda *Diariamente* ou *Semanalmente*, as transferências em curso são interrompidas na hora especificada e serão retomadas a partir do último quadro de vídeo transferido com êxito na próxima transferência agendada. Caso você não defina uma duração máxima e a transferência ainda esteja em curso no início da próxima transferência agendada, a nova transferência começará assim que a transferência atual for concluída.

A transferência de arquivos com agendamento é recomendada para câmeras fixas com largura de banda da rede limitada. A transferência pode ser agendada para um horário em que a demanda de rede seja baixa.

6 Para recuperar arquivos após conexão à rede, defina a opção **Ao reconectar** para **Ligado** e especifique quantos segundos o Archiver deve aguardar antes de consultar o dispositivo avançado sobre arquivos a transferir. O dispositivo avançado deve ter tempo suficiente para concluir a escrita do vídeo que está gravando no armazenamento local antes de iniciar a transferência.

   Esta opção é recomendada para câmaras ligadas a unidades móveis que entram e saem regularmente de áreas com cobertura Wi-Fi. Também é útil se você tem uma rede instável onde suas câmeras frequentemente ficam online e offline.

7 Em *Dados*, selecione **Tudo** para transferir tudo desde a última transferência bem-sucedida ou **Específico** para transferir sequências específicas com base em filtragem de eventos.

8 Se você selecionar **Específico**, selecione os tipos de dados a transferir:

   - **Todos os repositórios quando a câmera estava off-line:** Transfira segmentos de vídeo gravados entre um evento *Unidade perdida* e um evento *Unidade descoberta*.
   - **Alarmes:** Transfere segmentos de vídeo relacionados a eventos de alarme. A própria gravação do alarme não é transferida.
   - **marcadores:** Transfere segmentos de vídeo que contenham marcadores.
   - **Disparos de entradas:** Transfere segmentos de vídeo que contenham eventos de entrada.
   - **Eventos de movimento:** Transfira segmentos de vídeo gravados entre um evento *Movimento ativo* e um evento *Movimento inativo*. Esta opção se aplica apenas a unidades com detecção de movimento.
   - **Eventos de análise de vídeo:** Transfere segmentos de vídeo que contenham eventos de análise de vídeo.
   - **Intervalo de tempo:** Transfira segmentos de vídeo gravados durante um período específico. Você pode especificar um intervalo de tempo ou um intervalo de tempo relativo, como últimos *n* dias, horas ou minutos).

9 Somente em transferências baseadas em eventos: Se você tiver selecionado dados específicos, especifique quantos segundos de vídeo devem ser transferidos antes e depois da ocorrência do evento.

   Exemplo: Se você selecionar o filtro **Eventos de movimento**, esta definição indica quantos segundos de vídeo anteriores ao evento *Movimento ativo*, e quantos segundos de vídeo posteriores ao evento *Movimento inativo*, são incluídos na transferência.

10 Clique em **Salvar**.

Duplicar arquivo de vídeos

Para copiar arquivos de vídeos de um Archiver para outro, você pode duplicar arquivos específicos segundo uma agenda usando a transferência de arquivos. Os arquivos duplicados podem ser consultados no Security Desk.

O que você deve saber

Ao duplicar vídeo de uma função Archiver para outra, os arquivos originais são mantidos pelo Archiver de origem até que o período de retenção termine.

A transferência de vídeos entre Archivers é útil nos seguintes cenários:

- Para soluções de armazenamento multicamada: O vídeo de alta qualidade é gravado em tempo real no primeiro Archiver, que usa um dispositivo de armazenamento dispendioso e de alto desempenho. Arquivos de vídeo importantes são periodicamente duplicados no segundo Archiver, que usa um dispositivo mais lento que é melhor para armazenamento de longo prazo.
- Se você movesse unidades de vídeo para um novo Archiver usando a ferramenta Mover unidade e também deseja transferir os arquivos de vídeo dessas câmeras para o novo Archiver.
- Transferir gravações de vídeo de um local federado para um sistema central para armazenamento de longo prazo, investigações locais e para gerenciar largura de banda.

Para duplicar arquivos:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo* e selecione um Archiver de origem para duplicar.

2 Clique na aba **Recursos** e, em seguida, clique em **Configurações avançadas**.

3 Defina **Taxa de transferência de arquivos máxima** para a máxima largura de banda disponível para o Archiver para transferência de arquivos.

Essa configuração garante que haja suficiente largura de banda da rede disponível para solicitações de reprodução e vídeo ao vivo.

4 Na página inicial do Config Tool, abra a tarefa *Transferência de arquivos*.

5 Clique em **Adicionar um item ( )** > **Duplicar arquivos** .

6 Na caixa de diálogo *Propriedades do grupo de transferência*, digite um nome para este cenário de transferência de arquivos.

7 Na seção *Origens*, clique em **Adicionar um item ( )** , selecione as câmeras ou Archivers que deseja e clique em **Adicionar**.

Quando uma câmera é selecionada como uma origem, a transferência irá incluir vídeos associados de todos os Archivers.

DICA: Mantenha pressionado Ctrl ou Shift para selecionar várias câmeras ou Archivers.

8 Na lista suspensa **Destino**, selecione um Archiver para receber o vídeo.

9 Para **Recorrência**, selecione uma agenda para a transferência de arquivos:

- **Manual:** Transfere arquivos manualmente.
- **Minutos:** Transfere arquivos a cada 1–59 minutos.
- **A cada hora:** Transfere arquivos a cada 1–23 horas.
- **Diariamente:** Transfere arquivos todos os dias a uma hora especificada. Opcionalmente, defina uma duração máxima para a conclusão da transferência.
- **Semanalmente:** Transfere arquivos todas as semanas, em dias específicos a uma hora especificada. Opcionalmente, defina uma duração máxima para a conclusão da transferência.

NOTA: Se você definir uma duração máxima de transferência de arquivos para uma agenda *Diariamente* ou *Semanalmente*, as transferências em curso são interrompidas na hora especificada e serão retomadas a partir do último quadro de vídeo transferido com êxito na próxima transferência agendada. Caso você não defina uma duração máxima e a transferência ainda esteja em curso no início da próxima transferência agendada, a nova transferência começará assim que a transferência atual for concluída.

A transferência de arquivos com agendamento é recomendada para câmeras fixas com largura de banda da rede limitada. A transferência pode ser agendada para um horário em que a demanda de rede seja baixa.

10 Na opção **Cobertura**, selecione entre transferir todos os dados que foram acumulados desde a última transferência ou apenas por um intervalo de dias definido.

11 Em *Dados*, selecione **Tudo** para transferir tudo desde a última transferência bem-sucedida ou **Específico** para transferir sequências específicas com base em filtragem de eventos.

12 Se você selecionar **Específico**, selecione o tipo de dados a transferir:

- **Alarmes:** Transfere segmentos de vídeo relacionados a eventos de alarme. A própria gravação do alarme não é transferida.
- **marcadores:** Transfere segmentos de vídeo que contenham marcadores.
- **Disparos de entradas:** Transfere segmentos de vídeo que contenham eventos de entrada.
- **Eventos de movimento:** Transfira segmentos de vídeo gravados entre um evento *Movimento ativo* e um evento *Movimento inativo*. Esta opção se aplica apenas a unidades com detecção de movimento.
- **Vídeo protegido:** Transfere segmentos de vídeo que estejam protegidos.
- **Eventos de análise de vídeo:** Transfere segmentos de vídeo que contenham eventos de análise de vídeo.
- **Intervalo de tempo:** Transfira segmentos de vídeo gravados durante um período específico. Você pode especificar um intervalo de tempo ou um intervalo de tempo relativo, como últimos *n* dias, horas ou minutos).

13 Somente em transferências baseadas em eventos: Se você tiver selecionado dados específicos, especifique quantos segundos de vídeo devem ser transferidos antes e depois da ocorrência do evento.

Exemplo: Se você selecionar o filtro **Eventos de movimento**, esta definição indica quantos segundos de vídeo anteriores ao evento *Movimento ativo*, e quantos segundos de vídeo posteriores ao evento *Movimento inativo*, são incluídos na transferência.

14 Clique em **Salvar**.

Tópicos relacionados

Transferir arquivos de vídeo na página 527
Recuperar gravações de vídeo das unidades na página 528

Fazer backup de arquivos de vídeos segundo uma agenda

Para salvar vídeos importantes regularmente, é possível fazer backup de arquivos específicos em um servidor de arquivos ou em uma unidade de rede com agendamento usando a transferência de arquivos.

O que você deve saber

O vídeo é salvo em arquivos de vídeo G64x, que podem ser restaurados posteriormente. Não é possível pesquisar arquivos de vídeo em backup no Security Desk, a menos que sejam restaurados; no entanto, continua a ser possível pesquisar os arquivos originais.

Você também pode fazer backup de arquivos de vídeo manualmente se for necessário ignorar a agenda de backup.

Fazer backup de seus arquivos de vídeo é útil nos seguintes cenários:

- Se você estiver executando manutenção no servidor e precisar armazenar temporariamente os arquivos em um local seguro.
- Se o Archiver falhar e você precisar restaurar o vídeo para outro Archiver.

Backup de arquivos de vídeo em um cronograma

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Selecione um Archiver na árvore de entidades de função e clique na aba **Recursos**.
3 Na seção *Transferência de arquivos*, configure as seguintes opções:
   - **Pasta de backup:** Localização onde os arquivos de backup são salvos como arquivos G64x.
   - **Apagar arquivos mais antigos quando os discos estiverem cheios:** Ative esta opção para eliminar os arquivos de vídeo mais antigos quando o disco estiver cheio.
   - **Limpeza automática:** Ligue esta opção para especificar um período de retenção para os arquivos de vídeo em backup (em dias). Se você não ativar essa opção, os arquivos de vídeo em backup não são automaticamente excluídos pelo sistema e devem ser removidos manualmente.
4 Clique em **Configurações avançadas**.
5 Defina **Taxa de transferência de arquivos máxima** para a máxima largura de banda disponível para o Archiver para transferência de arquivos.
6 Clique em **OK** > **Aplicar**.
7 Na página inicial do Config Tool, abra a tarefa *Transferência de arquivos*.
8 Clique em **Adicionar um item ( )** > **Backup** .
9 Na caixa de diálogo *Propriedades do grupo de transferência*, digite um nome para este cenário de transferência de arquivos.
10 Na seção *Origens*, clique em **Adicionar um item ( )** , selecione as câmeras ou Archivers que deseja e clique em **Adicionar**.
   Quando uma câmera é selecionada como uma origem, a transferência irá incluir vídeos associados de todos os Archivers.
   DICA: Mantenha pressionado Ctrl ou Shift para selecionar várias câmeras ou Archivers.
11 Para **Recorrência**, selecione uma agenda para a transferência de arquivos:

- **Manual:** Transfere arquivos manualmente.
- **Minutos:** Transfere arquivos a cada 1–59 minutos.
- **A cada hora:** Transfere arquivos a cada 1–23 horas.
- **Diariamente:** Transfere arquivos todos os dias a uma hora especificada. Opcionalmente, defina uma duração máxima para a conclusão da transferência.
- **Semanalmente:** Transfere arquivos todas as semanas, em dias específicos a uma hora especificada. Opcionalmente, defina uma duração máxima para a conclusão da transferência.

NOTA: Se você definir uma duração máxima de transferência de arquivos para uma agenda *Diariamente* ou *Semanalmente*, as transferências em curso são interrompidas na hora especificada e serão retomadas a partir do último quadro de vídeo transferido com êxito na próxima transferência agendada. Caso você não defina uma duração máxima e a transferência ainda esteja em curso no início da próxima transferência agendada, a nova transferência começará assim que a transferência atual for concluída.

A transferência de arquivos com agendamento é recomendada para câmeras fixas com largura de banda da rede limitada. A transferência pode ser agendada para um horário em que a demanda de rede seja baixa.

12 Na opção **Cobertura**, selecione entre transferir todos os dados que foram acumulados desde a última transferência ou apenas por um intervalo de dias definido.

13 Em *Dados*, selecione **Tudo** para transferir tudo desde a última transferência bem-sucedida ou **Específico** para transferir sequências específicas com base em filtragem de eventos.

14 Se você selecionar **Específico**, selecione o tipo de dados a transferir:

- **Alarmes:** Transfere segmentos de vídeo relacionados a eventos de alarme. A própria gravação do alarme não é transferida.
- **marcadores:** Transfere segmentos de vídeo que contenham marcadores.
- **Disparos de entradas:** Transfere segmentos de vídeo que contenham eventos de entrada.
- **Eventos de movimento:** Transfira segmentos de vídeo gravados entre um evento *Movimento ativo* e um evento *Movimento inativo*. Esta opção se aplica apenas a unidades com detecção de movimento.
- **Vídeo protegido:** Transfere segmentos de vídeo que estejam protegidos.
- **Eventos de análise de vídeo:** Transfere segmentos de vídeo que contenham eventos de análise de vídeo.
- **Intervalo de tempo:** Transfira segmentos de vídeo gravados durante um período específico. Você pode especificar um intervalo de tempo ou um intervalo de tempo relativo, como últimos *n* dias, horas ou minutos).

15 Somente em transferências baseadas em eventos: Se você tiver selecionado dados específicos, especifique quantos segundos de vídeo devem ser transferidos antes e depois da ocorrência do evento.

Exemplo: Se você selecionar o filtro **Eventos de movimento**, esta definição indica quantos segundos de vídeo anteriores ao evento *Movimento ativo*, e quantos segundos de vídeo posteriores ao evento *Movimento inativo*, são incluídos na transferência.

16 Clique em **Salvar**.

O backup dos arquivos de vídeo é feito na hora agendada.

Tópicos relacionados

Transferir arquivos de vídeo na página 527
Restaurar arquivos de vídeo na página 535
Transferir arquivos de vídeos sob demanda na página 534

Ignorar agendas de transferência de arquivos

Se você precisar recuperar gravações de vídeo de uma unidade de vídeo, copiar arquivos para outro Archiver ou fazer backup de seus arquivos de vídeo antes da próxima transferência agendada, é possível executar uma transferência agendada a pedido.

Antes de iniciar

As configurações de transferência de arquivo para o grupo de transferência devem ser configuradas.

Para ignorar um agendamento de transferência de arquivo:

1 Na página inicial do Config Tool, abra a tarefa *Transferência de arquivos*.
2 Selecione um ou mais grupos de transferência na lista.

DICA: Mantenha pressionado Ctrl ou Shift para selecionar várias câmeras ou Archivers.

3 Clique em **Iniciar transferência para grupos de transferência selecionados** ( ).

Transferir arquivos de vídeos sob demanda

Para salvaguardar rapidamente seus arquivos de vídeos antes de uma grande operação, como uma atualização de software ou a substituição de um servidor, você pode mover arquivos de vídeos sob demanda sem criar um grupo de transferência.

Para transferir arquivos de vídeos sob demanda:

1 Na página inicial do Config Tool, abra a tarefa *Transferência de arquivos*.
2 Na parte inferior da janela, clique em **Transferir agora**.
3 Na caixa de diálogo *Propriedades do grupo de transferência*, selecione o tipo de transferência que deseja realizar:

- **Backup:** Faz o backup de arquivos de vídeo de um Archiver para um arquivo G64x.
- **Repositórios duplicados:** Copie arquivos de vídeos de um Archiver para outro.

4 Na seção *Origens*, clique em **Adicionar um item ( )** , selecione as câmeras ou Archivers que deseja e clique em **Adicionar**.

Quando uma câmera é selecionada como uma origem, a transferência irá incluir vídeos associados de todos os Archivers.

DICA: Mantenha pressionado Ctrl ou Shift para selecionar várias câmeras ou Archivers.

5 Para **Duplicar arquivos**, selecione um Archiver para receber os vídeos na lista suspensa **Destino**.
6 Para **Intervalo de tempo**, defina a hora de início e de término dos arquivos de vídeos a serem transferidos.
7 Em *Dados*, selecione **Tudo** para transferir tudo desde a última transferência bem-sucedida ou **Específico** para transferir sequências específicas com base em filtragem de eventos.
8 Se você selecionar **Específico**, selecione o tipo de dados a transferir:

- **Alarmes:** Transfere segmentos de vídeo relacionados a eventos de alarme. A própria gravação do alarme não é transferida.
- **marcadores:** Transfere segmentos de vídeo que contenham marcadores.
- **Disparos de entradas:** Transfere segmentos de vídeo que contenham eventos de entrada.
- **Eventos de movimento:** Transfira segmentos de vídeo gravados entre um evento *Movimento ativo* e um evento *Movimento inativo*. Esta opção se aplica apenas a unidades com detecção de movimento.
- **Vídeo protegido:** Transfere segmentos de vídeo que estejam protegidos.
- **Eventos de análise de vídeo:** Transfere segmentos de vídeo que contenham eventos de análise de vídeo.
- **Intervalo de tempo:** Transfira segmentos de vídeo gravados durante um período específico. Você pode especificar um intervalo de tempo ou um intervalo de tempo relativo, como últimos *n* dias, horas ou minutos).

9 Somente em transferências baseadas em eventos: Se você tiver selecionado dados específicos, especifique quantos segundos de vídeo devem ser transferidos antes e depois da ocorrência do evento.

Exemplo: Se você selecionar o filtro **Eventos de movimento**, esta definição indica quantos segundos de vídeo anteriores ao evento *Movimento ativo*, e quantos segundos de vídeo posteriores ao evento *Movimento inativo*, são incluídos na transferência.

10 Clique em **Iniciar**.

A transferência de arquivos começa imediatamente.

Tópicos relacionados

Transferir arquivos de vídeo na página 527
Fazer backup de arquivos de vídeos segundo uma agenda na página 532

Restaurar arquivos de vídeo

Depois de fazer backup dos seus arquivos de vídeo, você pode restaurar o backup para um Archiver ou Archiver auxiliar.

O que você deve saber

Por padrão, os arquivos de backup são recuperados da **pasta Backup**, que é especificada na seção *Transferência de arquivos* da aba **Recursos** quando você faz backup de arquivos de vídeo segundo uma agenda. Se necessário, os arquivos de backup G64x podem também ser selecionados de uma pasta diferente.

Os arquivos de backup somente podem ser restaurados para um Archiver no seu sistema Security Center.

Somente os tipos de dados de vídeo que foram copiados são restaurados. Depois de restaurar os arquivos, o vídeo pode ser pesquisado usando relatórios do Security Desk.

Para restaurar arquivos de vídeo:

1 Na página inicial do Config Tool, abra a tarefa *Transferência de arquivos*.
2 Na parte inferior da janela, clique em **Restaurar arquivos**.
3 Na caixa de diálogo *Restaurar arquivos*, selecione um **Tipo de restauração**. Estão disponíveis as seguintes opções:

- **Câmera:** Restaura vídeos de câmeras registradas que foram copiados para a pasta de backup padrão. Se selecionar **Câmera**, você deve especificar uma ou mais câmeras registradas para restaurar.

  NOTA: Os arquivos de vídeo de uma câmera excluída só podem ser restaurados desta forma se os vídeos dessa câmera ainda forem gerenciados pelo Archiver. Se uma câmera e todos os arquivos associados forem excluídos, você deve usar **Personalizar** para restaurar os arquivos.
- **Archiver:** Restaura o vídeo de Archivers específicos que foram copiados para a pasta de backup padrão. Se selecionar **Archiver**, você deve selecionar um ou mais Archivers para restaurar.
- **Personalizar:** Restaura vídeos de um arquivo ou localização de backup específico, como uma pasta ou um dispositivo de armazenamento USB. Se selecionar **Personalizar**, você deve selecionar um Archiver para receber os vídeos e um arquivo ou localização de backup de onde carregar.

4 Na seção *Quando*, selecione **De**, **Até** ou ambos para filtrar arquivos dentro do período especificado.
5 Clique em **Localizar arquivos**.
6 Selecione os arquivos que deseja restaurar.

DICA: Mantenha pressionado Ctrl ou Shift para selecionar várias câmeras ou Archivers.

7 Se necessário, proteja os arquivos restaurados contra exclusão automática com as seguintes opções:

- **Proteger vídeo contra exclusão:** Ativa ou desativa a proteção dos arquivos de vídeo restaurados.
- **Indefinidamente:** Sem data de término. Você deve remover a proteção manualmente.
- **Por x dias:** Os vídeos são protegidos pelo número de dias selecionado.
- **Até:** Os vídeos são protegidos até a data selecionada.

Por padrão, **Proteger vídeos contra exclusão** está habilitado e definido para 5 dias.

MELHOR PRÁTICA: Se estiver restaurando sequências de vídeo antigas, é recomendável proteger seus arquivos de vídeo contra a exclusão porque o período de retenção pode já ter passado.

8 Clique em **Restaurar**.

Tópicos relacionados

Fazer backup de arquivos de vídeos segundo uma agenda na página 532

Status e detalhes de transferência de arquivos

Você pode monitorar e analisar o status de suas transferências de arquivos na tarefa *Transferência de arquivos*.

As seguintes informações são fornecidas para cada grupo de transferência:

- **Grupo de transferência:** Grupo de câmeras ou Archivers com as mesmas configurações de transferência de vídeo.
- **Tipo:** Tipo de transferência de vídeo Entre *Recuperar da unidade*, *Duplicar arquivos* ou *Backup*.
- **Recorrência:** Com que frequência a transferência de vídeo volta a ocorrer, com base no agendamento definido.
- **Status:** Estado da transferência atual. O status pode ser um dos seguintes:
  - **Inativo:** A transferência está esperando para começar.
  - **Pendente:** A transferência começará assim que aparecer uma vaga na fila de download.
  - **Ativo:** O transferência foi iniciada. O progresso e a taxa de transferência de bits são mostrados.
  - **Erro:** Algumas câmeras não puderam ser processadas com sucesso, mas outras ainda estão ativas.
  - **Sucesso:** A transferência foi concluída com êxito.
- **Tamanho dos dados transferidos:** Tamanho dos dados de vídeo que foram transferidos.
- **Último início de transferência:** Data e hora em que a última transferência foi iniciada.
- **Último término de transferência:** Data e horário em que a última transferência foi finalizada.
- **Último status de transferência:** O status da última transferência.
- **Próxima transferência:** Data e hora em que a próxima transferência está definida para iniciar.
- **Mostrar detalhes da transferência ( ):** Informações de transferência sobre cada câmera no grupo de transferência.
  - **Origem:** Nome da câmera.
  - **Para:** Destino da transferência (um Archiver ou a pasta de backup do Archiver).
  - **Status:** Estado da transferência.
  - **Tamanho dos dados transferidos:** Tamanho dos dados de vídeo que foram transferidos.
  - **Último início de transferência:** Data e hora em que a última transferência foi iniciada.
  - **Último término de transferência:** Data e horário em que a última transferência foi finalizada.
  - **Último status de transferência:** O status da última transferência.
  - **Resultado:** Resultado da última transferência. Pode exibir erros sobre a transferência, se algum ocorrer.

Proteger arquivos de vídeo contra exclusão

É possível proteger imagens de vídeo importantes de serem excluídas pelo sistema quando o espaço em disco do Archiver ficar cheio ou quando seu período normal de retenção terminar.

O que você deve saber

É possível proteger os vídeos contra exclusão. A proteção é aplicada em todos os arquivos de vídeo necessários para armazenar a sequência de vídeos protegida. Como nenhum arquivo de vídeo pode ser parcialmente protegido, o tamanho real da sequência de vídeos protegida depende da granularidade dos arquivos de vídeo.

O Archiver não pode proteger arquivos parciais, para que seja possível proteger um segmento maior do que o selecionado.

CUIDADO: Demasiados arquivos de vídeo protegidos em um disco podem reduzir o espaço de armazenamento disponível para novos arquivos. Para evitar desperdiçar espaço de armazenamento, verifique regularmente a porcentagem de arquivos de vídeo protegidos em cada disco.

Para liberar espaço de armazenamento, é possível fazer o backup de arquivos de vídeo protegidos ou duplicar os arquivos protegidos em outro Archiver usando o *transferência de arquivo*, e então desproteger o arquivo de vídeo original.

Para proteger um arquivo de vídeo:

1 Abra a tarefa **Detalhes de armazenamento de arquivo**.

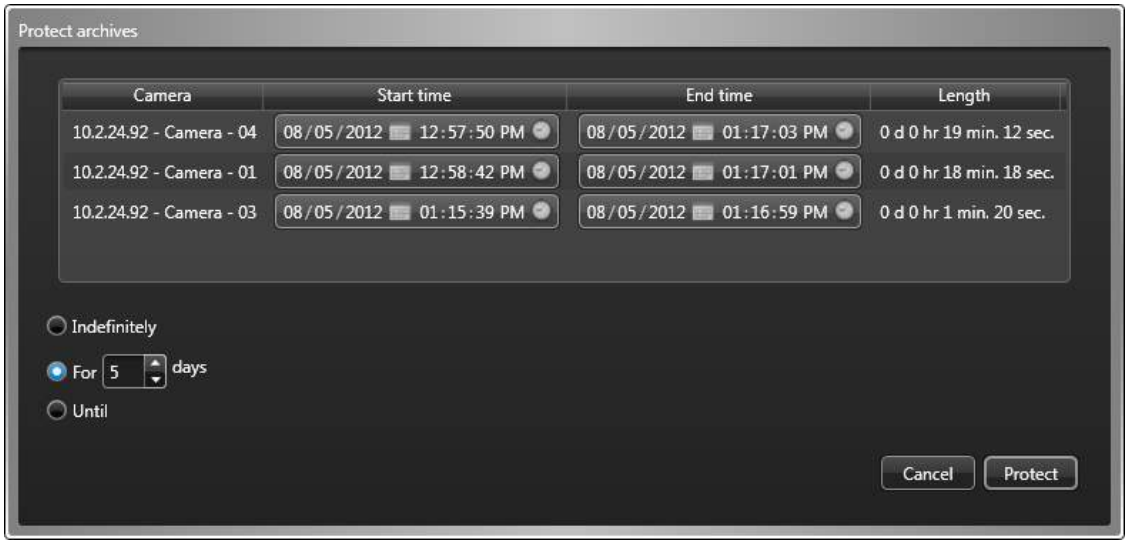
2 Crie o seu relatório.

Os arquivos de vídeo associados às câmeras selecionadas são listados no painel de relatório.

3 No painel de relatório, selecione o arquivo de vídeo a ser protegido e clique em **Proteger** ( ).

Para selecionar vários arquivos de vídeo, segure a tecla Ctrl ou Shift.

4 Na caixa de diálogo *Proteger arquivos*, defina a **Hora de início** e a **Hora de término** do vídeo a ser protegido.



5 Selecione quanto tempo o arquivo de vídeo deve ser protegido, entre uma das seguintes opções:

- **Indefinidamente:** Sem data de término. É necessário remover manualmente a proteção selecionando o arquivo de vídeo no painel de relatório e clicando em **Desproteger** ( ).

  NOTA: Se o período de retenção terminar, os arquivos de vídeo desprotegidos não são imediatamente excluídos. Se necessário, você tem 24 horas para restaurar a proteção de vídeo.

- **Por x dias:** O arquivo de vídeo é protegido pelo número de dias selecionado.

- **Até:** O arquivo de vídeo é protegido até a data selecionada.

6 Clique em **Proteger**.

O arquivo de vídeo está protegido.

Tópicos relacionados

Armazenamento de arquivos na página 520
Duplicar arquivo de vídeos na página 530
Transferir arquivos de vídeos sob demanda na página 534

Proteção de arquivos de vídeo contra adulteração

Se você quiser usar sua evidência de vídeo no tribunal, você pode habilitar a marca d'água de vídeo no Archiver, para proteger o vídeo contra adulteração e provar que ele não foi alterado.

O que você deve saber

A marca d'água de vídeo adiciona uma assinatura digital (marca d'água) a cada quadro do vídeo gravado para garantir sua autenticidade. Se o vídeo for posteriormente alterado através da adição, exclusão ou modificação de um quadro, as assinaturas do conteúdo modificado não corresponderão mais, mostrando que o vídeo foi adulterado.

Para proteger seus arquivos de vídeo contra adulteração:

1 Abra a tarefa *Sistema* e clique na visualização **Funções**.
2 Selecione a função Archiver e clique na aba **Recursos** e clique em **Configurações avançadas**.
3 Defina a opção **Marca d'água de vídeo** como **Ligada** e clique em **OK** > **Aplicar**.
4 Configure uma chave de criptografia para a impressão digital da marca d'água.

Configurar uma chave de criptografia para marcas d'água de vídeo

Você pode gerar sua própria chave de criptografia para a marca d'água de vídeo e configurar o Archiver para usá-la.

Para configurar uma chave de criptografia para a marca d'água de vídeo:

1 Execute *EncryptionKeyGenerator.exe* na pasta de instalação do Security Center.

   O programa gera dois arquivos de 1 KB chamados *fingerprint.bin* e *private.bin* e guarda-os na pasta de instalação. O primeiro arquivo contém uma impressão digital de 20 bytes aleatória usada para a criptografia. O segundo arquivo contém uma chave de criptografia RSA de 248 bits. Esses dois arquivos serão diferentes cada vez que o programa for executado.
2 Faça uma cópia de *fingerprint.bin* e *private.bin* e guarde em um local seguro.
3 No Config Tool, abra a tarefa *Sistema* e clique na visualização **Funções**.
4 Selecione o Archiver e reinicie a função.
5 Se você tiver um servidor secundário atribuído à função Archiver, copie os mesmos arquivos de criptografia personalizados para a pasta de instalação do Security Center nesse servidor.

Na próxima vez que o Archiver gravar vídeo em disco, os arquivos de vídeo receberão a marca d'água e a impressão digital será criptografada usando a nova chave de criptografia.

Exibir propriedades de arquivos de vídeo

Você pode exibir propriedades de arquivos de vídeo, como nome do arquivo, hora de início e de término, tamanho do arquivo e assim por diante, no relatório *Detalhes de armazenamento de arquivos*. Você também pode alterar o status de proteção dos arquivos de vídeo.

Para visualizar as propriedades de um arquivo de vídeo:

1 Na página inicial, abra a tarefa *Detalhes de armazenamento de arquivos*.

2 Definir os filtros de consulta para o relatório. Selecione um ou mais dos seguintes filtros:

- **Câmeras:** Selecionar as câmeras para investigar.
- **Campos personalizados:** Restringir a busca a campo personalizado predefinido para a entidade. Este filtro aparece somente se os campos personalizados estiverem definidos para a entidade e estavam visíveis para você, quando foi criado ou configurado pela última vez.
- **Carimbo de tempo do evento:** Definir o intervalo de tempo para consulta O intervalo pode ser definido para um período específico ou para unidades de tempo globais, como a semana ou mês anteriores.
- **Tipo de mídia:**

  Selecione o tipo de mídia que está procurando:

  - **Vídeo:** Arquivos que contém gravação de vídeo.
  - **Áudio:** Arquivos que contém gravações de áudio.
  - **Metadados:** Arquivos que contém metadados como sobreposição.
- **Tipo de origem:**

  Refine a pesquisa ao selecionar a origem dos arquivos:

  - **Baixado do armazenamento interno da unidade:** Arquivos criados pela câmera, baixado por um Archiver e no momento armazenado no disco do Archiver.
  - **Duplicado de outro Archiver.:** Arquivos criados por um Archiver e transferido a outro.
  - **No armazenamento interno da unidade:** Arquivos criados pela câmera e no momento armazenados nela.
  - **Gravado pelo Archiver:** Arquivos criados e no momento armazenados por um Archiver.
  - **Restaurado de backup:** Arquivos restaurados de um conjunto de backup offline; ou seja, um arquivo de backup contendo arquivos que não foram acessados pelo Security Center antes de restaurá-los.
- **Fonte:** O nome do sistema a que a câmera pertence
- **Status:**

  Selecione os status de arquivo de vídeo que deseja investigar:

  - **Desprotegido:** Os arquivos de vídeo não estão protegidos contra a limpeza de rotina do Archiver. Esses arquivos podem ser excluídos assim que o período de retenção vencer ou quando o Archiver ficar sem espaço em disco, dependendo das opções de função do Archiver.
  - **Proteção finalizada:** Arquivos de vídeo que você desprotegeu há menos de 24 horas.
  - **Protegido:** Arquivos de vídeo que são protegidos. Eles não são excluídos, mesmo quando o disco está cheio. Para esses arquivos, também é possível especificar uma data de término de proteção.

3 Clique em **Gerar relatório**.

Os arquivos de vídeo associados às câmeras selecionadas são listados no painel de relatório, juntamente com suas propriedades de arquivo.

4 Para visualizar a sequência de vídeo em um ladrilho, clique duas vezes ou arraste um arquivo de vídeo do painel de relatório para a tela.

A sequência selecionada começa a rodar imediatamente.

Após terminar

- Para exportar um arquivo de vídeo no Security Desk, selecione o item no painel de relatório e clique em **Exportar vídeo** ( ).
- Para remover um arquivo de vídeo, selecione o item no painel de relatório e clique em **Excluir** ( ).
- Para proteger um arquivo de vídeo contra exclusão automática, selecione o item no painel de relatório e clique em **Proteger** ( ).
- Para desproteger um arquivo de vídeo, selecione o item no painel de relatório e clique em **Desproteger** ( ).

Tópicos relacionados

Proteger arquivos de vídeo contra exclusão na página 537

Colunas de relatório para a tarefa Detalhes de armazenamento do arquivo

Após gerar um relatório, os resultados da sua pesquisa são listados em um painel de relatório. Esta seção lista as colunas disponíveis para a tarefa de relatório relevante.

- **Câmera:** Nome de câmera.
- **Campos personalizados:** Os campos personalizados predefinidos para a entidade. As colunas aparecem somente se os campos personalizados estiverem definidos para a entidade e se estiver visível para você, quando forem criados ou configurados pela última vez.
- **Disco:** Unidade no servidor onde a função do Archiver está em execução.
- **Horário final:** Final do intervalo de tempo, sequência de reprodução ou de vídeo.
- **Nome do arquivo:** Nome do arquivo de vídeo.
- **Tamanho do arquivo:** Tamanho do arquivo de vídeo.
- **Comprimento:** Duração da sequência de vídeo no arquivo, em horas, minutos e segundos.
- **Tipo de mídia:** Tipo de mídia (vídeo, vídeo confidencial, áudio, metadados) contida no arquivo.
- **Tipo de origem:** Origem do arquivo:
  - **Baixado do armazenamento interno da unidade:** Arquivos criados pela câmera, baixado por um Archiver e no momento armazenado no disco do Archiver.
  - **Duplicado de outro Archiver.:** Arquivos criados por um Archiver e transferido a outro.
  - **No armazenamento interno da unidade:** Arquivos criados pela câmera e no momento armazenados nela.
  - **Gravado pelo Archiver:** Arquivos criados e no momento armazenados por um Archiver.
  - **Restaurado de backup:** Arquivos restaurados de um conjunto de backup offline; ou seja, um arquivo de backup contendo arquivos que não foram acessados pelo Security Center antes de restaurá-los.
- **Status de proteção:** Status de proteção do arquivo de vídeo.
- **Servidor:** Nome do servidor onde a função Archiver está em execução.
- **Origem (entidade):** O nome do sistema a que a câmera pertence
- **Horário de início:** Começo do intervalo de tempo, sequência de reprodução ou de vídeo.

Gerenciar os efeitos do Horário de Verão em arquivos de vídeo

As alterações de hora anuais de ou para o horário de verão (DST) podem afetar a maneira como os arquivos de vídeo são visualizados e consultados no Security Center.

As alterações de horário não impedem que suas câmeras gravem dados de vídeo. O *Archiver* sempre grava usando o Tempo Universal Coordenado (UTC), que não muda de horário para DST, e as consultas de arquivo sempre são enviadas para o servidor com carimbos de data/hora em UTC.

Usar UTC isola os arquivos de vídeo contra efeitos das mudanças de horário. No entanto, como o Security Desk e o Config Tool podem ser configurados para usar (e exibir) um fuso horário diferente de UTC, efeitos colaterais podem ser observados quando a hora é adiantada ou atrasada.

NOTA: O fuso horário de Horário da Costa Leste (EST) é usado como um exemplo, no entanto isso se aplica a todos os fusos horários que estão sujeitos ao DST.

Efeitos da hora atrasada

Quando a hora é atrasada, ela muda do Horário de Verão (DST) para a Hora Padrão do Leste dos EUA (EST).

A mudança de horário de DST para EST ocorre às 2:00. Antes das 2:00, o Security Center usa DST (UTC-4). Depois das 2:00, ele usa EST (UTC-5), conforme mostrado na seguinte tabela:

	DST		Mudança de horário	EST	
Horário local	0:00	1:00	02:00 = 01:00	2:00	3:00
Offset (horas)	-4	-4	-5	-5	-5
UTC	4:00	5:00	6:00	7:00	8:00

Devido à hora ter sido atrasada, os seguintes comportamentos podem ser observados ao reproduzir vídeo ou exportar arquivos:

- O tempo retrocede uma hora na linha do tempo. Após 1:59:59, a hora exibida retrocede para 1:00:00.
- A hora de fim de uma sequência de vídeo pode ser anterior à hora de início.
- A exportação de arquivos entre a 1:00 e as 2:00 sempre inclui uma hora adicional de vídeo. Por exemplo, ao exportar arquivos entre a 1:50 e as 2:00 na noite de mudança da hora, a sequência exportada inclui 1 hora e 10 minutos de vídeo porque a consulta inclui vídeo das 5:50 às 7:00 UTC.

Para evitar que o tempo seja atrasado uma hora durante a reprodução de vídeo, você deve configurar o Security Desk para usar UTC. Após exportar a sequência, você pode reverter para o fuso horário configurado anteriormente para exibir a sequência relativa à sua referência de hora local.

Efeitos da hora adiantada

Quando a hora é adiantada, ela muda da Hora Padrão do Leste dos EUA (EST) para o Horário de Verão (DST).

A mudança de horário de EST para DST ocorre às 2:00. Antes das 2:00, o Security Center usa EST (UTC-5). Depois das 2:00, ele usa DST (UTC-4), conforme mostrado na seguinte tabela:

	EST		Mudança de horário	DST	
Horário local	0:00	1:00	2:00 = 3:00	4:00	5:00
Offset (horas)	-5	-5	-4	-4	-4
UTC	5:00	6:00	7:00	8:00	9:00

Devido à hora ter sido adiantada, os seguintes comportamentos podem ser observados ao reproduzir vídeo ou exportar arquivos:

- O tempo é adiantado em uma hora na linha do tempo. Às 1:59:59, a hora exibida avança para as 3:00.
- Não há arquivos para exportação entre as 2:00 e as 3:00, porque este período foi ignorado.

Para evitar que o tempo seja adiantado em uma hora durante a reprodução de vídeo, você deve configurar o Security Desk para usar UTC.

Mudar o fuso horário para UTC

Se você estiver trabalhando com arquivos gravados durante uma mudança de horário e desejar remover os impactos associados da linha de tempo, você pode definir o fuso horário para UTC (Tempo Universal Coordenado) no Security Desk antes de realizar sua tarefa.

O que você deve saber

O Security Desk e o Config Tool exibem a hora em função do fuso horário selecionado. No entanto, o servidor usa UTC e o aplicativo cliente converte os carimbos de data/hora UTC do servidor para o fuso horário selecionado. Você pode definir os aplicativos clientes para usarem UTC para ignorar a conversão da hora e evitar os impactos causados pela mudança da hora.

NOTA: As definições de hora e data aplicam-se apenas ao aplicativo cliente que configurar. Cada aplicativo deve ser configurado separadamente.

Para mudar o fuso horário para UTC:

1 Na página inicial, clicar em **Opções** > **Data e hora**.
2 Se necessário, selecione **Exibir abreviaturas dos fusos horários** para exibir o fuso horário selecionado ao lado da hora na bandeja de notificação.
3 Selecione **Exibir o horário baseado em fuso horário seguinte** e, em seguida, selecione **(UTC) Tempo Universal Coordenado**.
4 Clique em **Salvar**.

O aplicativo cliente agora exibe a hora atual e carimbos de data/hora de arquivos em função do fuso horário UTC.

Importar arquivos de vídeo externos para o Security Center

Para visualizar arquivos de vídeo MOV, AVI e MP4 no Security Center, é necessário importá-los usando um dispositivo offline.

Antes de iniciar

Você deve definir a data e a hora no dispositivo usado para gravar arquivos de vídeo. Não definir a data pode impedir a importação dos arquivos.

O que você deve saber

Os nomes de arquivos importados devem ter o seguinte formato: *XXXX_YYYY.MM.DD_HH.MM.SS*, em que *XXXX* é um nome descritivo e os outros valores representam a data e a hora.

Os seguintes codecs são compatíveis:

- Transmissões de vídeo: H.263, H.264, H.265, MJPEG e MPEG-4
- Transmissões de áudio: G.711, G.721, G.723, AAC (8 kHz ou 16 kHz)

Para importar um arquivo de vídeo:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Selecione um Archiver na árvore de entidades de função para gerenciar o dispositivo offline.
3 Clique em **Unidade de vídeo** ( ).
A caixa de dialogo *Adição manual* se abrirá.
4 Na lista suspensa **Fabricante**, selecione **Dispositivo offline**.
5 Na lista suspensa **Tipo de produto**, selecione **Compartilhamento de rede**.
6 Digite um **Nome de unidade**.
Esse é o nome padrão da câmera e será usado para gerar um identificador exclusivo (GUID) para ela.
7 Digite o **Caminho** da localização onde serão colocados os arquivos de vídeo importados.
O caminho pode ser local ou um caminho de rede compartilhada. A conta de usuário que está executando o serviço Genetec™ Server deve ter acesso de leitura e gravação à pasta de rede compartilhada.
8 Selecione uma **Localização** para o dispositivo online no Security Center e clique em **Adicionar**.
9 Na tarefa *Vídeo*, selecione o Archiver que gerencia o novo dispositivo offline e clique na aba **Configurações padrão da câmera**.
10 Garanta que **Limpeza automática** esteja definido para um momento mais longínquo do que o arquivo mais antigo que deseja importar.
Por exemplo, se o arquivo de vídeo mais antigo tiver 30 dias, defina **Limpeza automática** para, no mínimo, 32 dias para que o arquivo não seja imediatamente excluído após a importação.
IMPORTANTE: A opção **Limpeza automática** também especifica o período de retenção para vídeos de todas as câmeras que são gerenciadas pelo Archiver selecionado. Certifique-se de que nenhuma alteração não afete suas configurações de gravação da câmera.
11 Se necessário, copie arquivos de vídeo para o **Caminho** definido para o dispositivo offline.
Conforme os arquivos são processados, eles desaparecem da pasta. Isso pode levar até 30 segundos ou mais dependendo do número de arquivos e seu tamanho.
NOTA:
- Se um arquivo não desaparecer da pasta, a importação falhou.
- Se você vir uma pasta *FailedAudioImports*, os arquivos de vídeo foram importados, mas o áudio não. Você pode encontrar o arquivo original nesta pasta.

Após terminar

Visualize seus arquivos de vídeo importados usando o relatório *Arquivos*. Para obter mais informações, consulte o *Guia do Usuário do Security Desk*.

27

Solução de problemas de vídeo

Esta seção inclui os seguintes tópicos:

- "Mover unidades de vídeo para um Archiver diferente" na página 548
- "Troca de unidades de vídeo" na página 549
- "Atualizar o firmware da unidade de vídeo" na página 551
- "Localizar arquivos órfãos em seu sistema" na página 552
- "Localizar arquivos ausentes em seu sistema" na página 554
- "Solução de problemas: problemas com a transmissão de vídeo" na página 556
- "Optimizar o desempenho do decodificador de vídeo no seu computador" na página 557
- "Não está sendo gravado vídeo" na página 558
- "Solução de problemas de unidades de vídeo offline no Security Center" na página 559
- "Executar rastreamentos de rede" na página 560
- "Solução de problemas: erros "Impossível estabelecer sessão de vídeo com o servidor"" na página 562
- "Impossível assistir vídeo ao vivo no Security Desk" na página 563
- "Impossível assistir a reprodução de vídeo no Security Desk " na página 565
- "Solução de problemas: As câmeras não estão gravando" na página 566
- "Solução de problemas: Não é possível adicionar unidades de vídeo" na página 569
- "Solução de problemas: Não é possível excluir unidades de vídeo" na página 572
- "Solução de problemas: problemas com a transmissão de vídeo H.264:" na página 573
- "Solução de problemas: problema de sensibilidade da câmera Axis P1428-E" na página 574
- "A detecção de movimento não está funcionando no Security Center" na página 575
- "Câmeras Axis não têm uma aba de Detecção de movimento" na página 576
- "Configurar o Security Center para abrir vídeo ao vivo rapidamente" na página 577
- "A proteção de privacidade não está a funcionar no Security Center" na página 578
- "Erros de arquivos de configuração de câmeras usadas junto ao corpo" na página 579
- "Avisos de conversão para câmeras usadas junto ao corpo" na página 582
- "Failover está configurado no Archiver para câmeras usadas junto ao corpo" na página 584

- "A porta de câmera usada junto ao corpo já está em uso" na página 586
- " O relatório Arquivos de câmera usada junto ao corpo está vazio" na página 587

Mover unidades de vídeo para um Archiver diferente

Se você quiser que uma função Archiver diferente gerencie e controle uma unidade de vídeo, para balanceamento de carga ou outra finalidade, você pode mover a unidade para outro Archiver usando a ferramenta *Mover unidade*.

Antes de iniciar

- A função Archiver deve estar na mesma LAN que a unidade de vídeo que controla.
- Se estiver utilizando definições personalizadas para a extensão da unidade, tais como credenciais de logon personalizadas, é necessário configurar as mesmas definições de extensão na nova função Archiver.

O que você deve saber

Os arquivos existentes não são movidos com a unidade de vídeo para a nova função Archiver. Eles permanecem associados ao Archiver antigo até que seu período de retenção termine.

Para mover unidades de vídeo para um Archiver diferente:

1 Na página inicial do Config Tool, clique em **Ferramentas** > **Mover unidade**.
2 Na lista suspensa **Tipo de unidade**, selecione **Unidade de vídeo**.
3 Selecione os dados que deseja mover.
4 Em **Archiver**, selecione a nova função Archiver que controla a unidade.
5 Clique em **Mover** > **Fechar**.

Após terminar

Mova quaisquer arquivos de vídeo importantes para o novo Archiver quando for conveniente.

Tópicos relacionados
Archiver - Aba Extensões na página 1050

Troca de unidades de vídeo

Se uma unidade de vídeo falhar e estiver offline no Security Center, exibida em vermelho na visualização de área, você pode substituir a unidade por uma compatível usando as mesmas configurações.

Antes de iniciar

Antes de substituir a unidade usando a ferramenta de Substituição de unidade, copie as configurações da unidade de vídeo antiga e as câmeras que ela controla para a nova unidade de vídeo.

O que você deve saber

Para garantir que os *arquivos de vídeos* associados à unidade antiga não sejam perdidos, a ferramenta de Substituição de unidade reassocia esses arquivos à nova unidade.

IMPORTANTE: Câmeras controladas pela nova unidade de vídeo são tratadas como câmeras novas pelo sistema. Se existirem associações entre câmeras antigas e outras entidades no sistema, essas associações devem ser recriadas manualmente para as câmeras novas.

Para substituir uma unidade de vídeo:

1 Adicione uma nova unidade de vídeo para o Archiver que controla a unidade antiga.

A nova unidade deve ser compatível com a antiga em termos de configurações e câmeras que elas controlam.

2 Copie as configurações da unidade de vídeo antiga para a nova unidade de vídeo, usando a Ferramenta de cópia de configuração.

3 Copie as configurações das câmeras controladas pela unidade de vídeo antiga para as novas câmeras, usando a Ferramenta de cópia de configuração.

4 Na página inicial, clique em **Ferramentas** > **Substituição de unidade**.

5 Na opção **Tipo de unidade**, selecione **Câmeras**.

6 Para cada uma das câmeras antigas, faça o seguinte:

a) Selecione a câmera **Antiga** e a **Nova**.
b) Clique em **Trocar**.

Os arquivos de vídeo e registros de eventos associados às câmeras antigas estão agora associadas às câmeras novas.

7 Se as câmeras antigas estavam associadas com entidades como portas e alarmes, representadas em mapas ou usadas para *rastreamento visual*, você deve substituir essas associações manualmente.

Para cada uma das câmeras antigas, faça o seguinte:

a) Selecione a câmera na exibição de área.
b) Clique em **Identidade** > **Parte de...**
c) Clique em uma entidade relacionada e clique em **Pular para** ( ).
d) Na página de configuração da entidade, remova a associação à câmera antiga e adicione a associação à câmera nova.
e) Se a câmera está representada em um mapa ou usada para rastreamento visual, substitua a câmera antiga com a câmera nova.

8 Verifique se os arquivos de vídeo estão associados à nova unidade de vídeo:

a) No Security Desk, abra a tarefa *Arquivos*.
b) Selecione uma câmera que seja controlada pela nova unidade de vídeo.

Todos os dias que incluem arquivos de vídeo para a câmera selecionada são listados na aba **Todos disponíveis**.

c) Selecione um dia e clique em **Gerar relatório**.

9 Depois que tudo estiver verificado, volte para a tarefa *Vídeo* do Config Tool.

10 Clique com o botão direito do mouse na unidade antiga e clique em **Excluir** ( ).

11 Clique em **Continuar** para confirmar exclusão.

Tópicos relacionados

Adicionar câmeras aos seus mapas na página 269
Configurar o rastreamento visual na página 501

Atualizar o firmware da unidade de vídeo

Você pode atualizar o firmware em sua unidade de vídeo diretamente do Config Tool.

Antes de iniciar

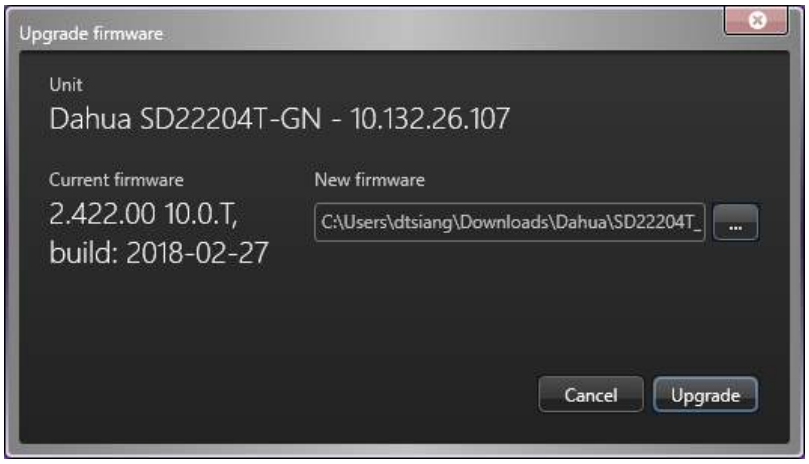
- Se o *Serviço Genetec™ Update (GUS)* estiver em execução, o status da atualização de firmware é indicado na página *Identidade* da unidade e na coluna **Descrição do firmware proposto** do relatório *Inventário de hardware*:
  - **Atualizado:** Nenhuma atualização de firmware é necessária.
  - **Opcional:** A atualização de firmware é sugerida.
  - **Recomendado:** A atualização de firmware é recomendada.
  - **Crítico:** A atualização de firmware conserta um problema de vulnerabilidade de segurança e é altamente recomendada.
- Baixe o firmware recomendado do site do fabricante. Se o GUS não estiver em execução, você pode encontrar o firmware recomendado para a unidade na nossa Lista de Dispositivos Compatíveis.
- Tome nota das definições de configuração da unidade. Para alguns fabricantes, a unidade é redefinida para suas configurações padrão após a atualização do firmware.

O que você deve saber

Para alguns fabricantes, não é possível atualizar o firmware da unidade a partir do Config Tool. Para obter informações específicas do fabricante, consulte a documentação do fabricante.

Para atualizar o firmware de uma unidade de vídeo:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Selecione a unidade de vídeo a atualizar e clique na aba **Identidade**.
3 Clique em **Atualizar** ().
4 Na caixa de diálogo *Atualizar firmware*, navegue até ao arquivo de firmware baixado e clique em **Atualizar**.



A unidade é reiniciada.

Após terminar

Reconfigure a unidade se as configurações tiverem sido redefinidas para o padrão durante a atualização.

Localizar arquivos órfãos em seu sistema

Para localizar arquivos de vídeo que já não são referenciados pelo banco de dados do Archiver, você pode usar a ferramenta *VideoFileAnalyzer.exe* encontrada na pasta de instalação do Security Center.

O que você deve saber

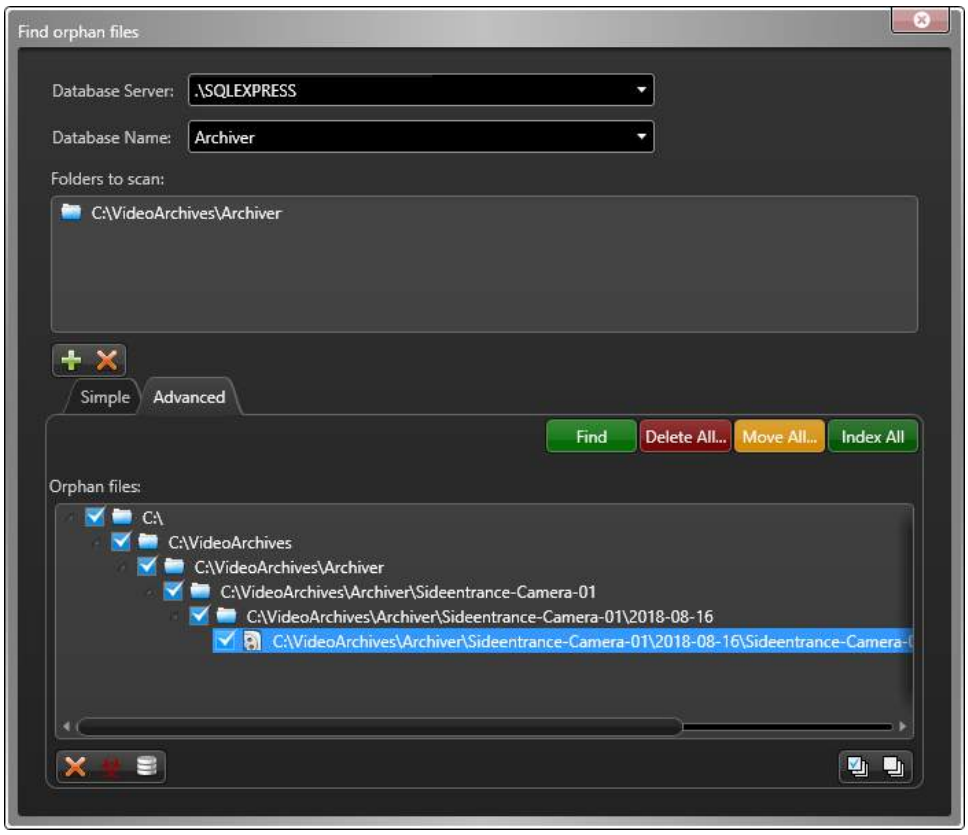
Um arquivo órfão é um arquivo de vídeo que não é mais referenciado por qualquer banco de dados de arquivos. Os arquivos órfãos permanecem no disco até serem manualmente excluídos. Essa situação ocorre quando o banco de dados de arquivos é alterado inadvertidamente, criando uma incompatibilidade entre o número de arquivos de vídeo referenciado no banco de dados e o número real de arquivos de vídeo armazenados no disco.

Para evitar esse problema faça um backup completo dos arquivos antes de alterar o banco de dados e restaure o backup após alterar o banco de dados.

Para localizar arquivos órfãos em seu sistema:

1 Abra a ferramenta *VideoFileAnalyzer.exe*.
   - *C:\Program files (x86)\Genetec Security Center 5.7* (computador de 64 bits)
   - *C:\Program files\Genetec Security Center 5.7* (computador de 32 bits)
2 Na parte inferior da caixa de diálogo *Analisador de arquivos de vídeo*, clique em **Localizar arquivos órfãos**.
3 Na caixa de diálogo *Localizar arquivos órfãos*, especifique o banco de dados de arquivos em que deseja localizar arquivos de vídeo.

   Você pode encontrar o nome do servidor de banco de dados e o nome do banco de dados na página *Recursos* da função Archiver ou Archiver auxiliar em Config Tool.
4 Na seção *Pastas a analisar*, clique em **Adicionar** () para adicionar as pastas que deseja analisar e, em seguida, clique em **OK**.
5 Clique em **Avançado** > **Localizar**.



6 Selecione arquivos na seção *Arquivos órfãos* e execute uma das seguintes ações:

- Para remover permanentemente os arquivos selecionados do seu sistema, clique em **Excluir arquivos** ().
- Para mover os arquivos selecionados para outro local e liberar espaço de armazenamento de arquivos, clique em **Mover arquivos para outra pasta** ().

  Movendo os arquivos, você pode examiná-los e decidir o que fazer com eles mais tarde sem afetar a operação da função de arquivamento.
- Para indexar os arquivos selecionados novamente no banco de dados de arquivos, clique em **Adicionar arquivos ao banco de dados** (). Isto garante que possam ser localizados utilizando o relatório *Arquivos* em Security Center.

  NOTA: Somente são recuperadas informações básicas, como a hora de início e de fim da gravação. Esta operação só deve ser utilizada como medida de emergência; portanto, é recomendável fazer backup de seu banco de dados antes de reindexar os arquivos.

Para excluir, mover ou indexar todos os arquivos localizados nas pastas adicionadas, clique no botão colorido correspondente.

Tópicos relacionados

Fazer backup de bancos de dados na página 151

Localizar arquivos ausentes em seu sistema

Para localizar arquivos de vídeo que ainda são referenciados pelo seu banco de dados de arquivo, mas que não são mais acessíveis a partir do dispositivo de armazenamento, você pode usar a ferramenta *VideoFileAnalyzer.exe*.

O que você deve saber

Um arquivo ausente é um arquivo de vídeo que ainda é referenciado por um banco de dados designado do Archiver, mas que não pode mais ser acessado. Esta situação ocorre se os ficheiros de vídeo forem apagados manualmente sem usar a tarefa *Detalhes de armazenamento de arquivos*, criando uma incompatibilidade entre o número de arquivo de vídeo referenciados no banco de dados e o número real de arquivos de vídeo no disco.

Para localizar arquivos ausentes em seu sistema:

1 Abra a ferramenta *VideoFileAnalyzer.exe*.

- *C:\Program files (x86)\Genetec Security Center 5.7* (computador de 64 bits)
- *C:\Program files\Genetec Security Center 5.7* (computador de 32 bits)

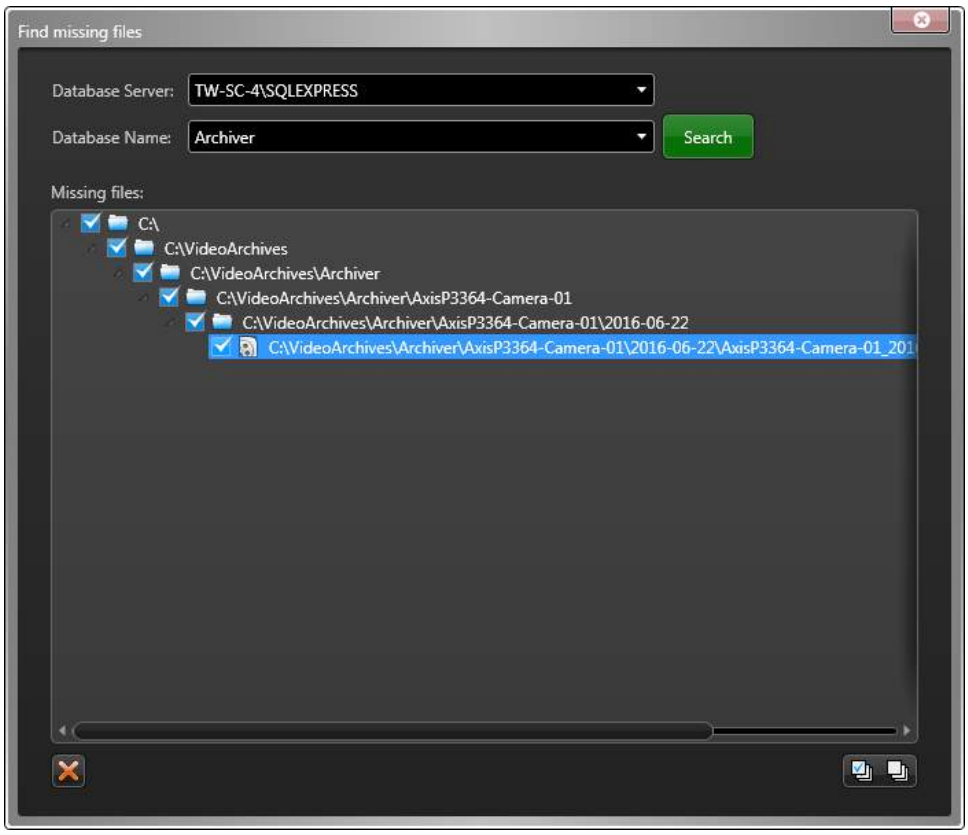
2 Na parte inferior da caixa de diálogo *Analisador de arquivos de vídeo*, clique em **Localizar arquivos ausentes**.

3 Na caixa de diálogo *Localizar arquivos ausentes*, especifique o **servidor do banco de dados** e o **nome do banco de dados** que você deseja verificar em busca de arquivos de vídeo ausentes.

Você pode encontrar o nome do servidor de banco de dados e o nome do banco de dados na página *Recursos* da função Archiver ou Archiver auxiliar em Config Tool.

4 Clique em **Pesquisar**.

5 Quando a pesquisa estiver concluída, selecione arquivos na seção *Arquivos ausentes* e clique em **Excluir arquivos** ( ).



Os índices de arquivos selecionados são removidos permanentemente do banco de dados de arquivo.

Solução de problemas: problemas com a transmissão de vídeo

No Security Desk, você pode diagnosticar o status das transmissões de vídeo exibidas na tela.

O que você deve saber

O diagnóstico da transmissão de vídeo ajuda a determinar em que ponto no caminho da rede onde o fluxo de informações é interrompido. Cada componente é exibido com informações de entrada e saída de tráfego. As informações podem ser usadas para identificar potenciais problemas com a unidade de vídeo, a função de arquivamento ou com redireção para Security Desk e assim por diante.

Para solucionar as possíveis causas de problemas de transmissão de vídeos:

1 No Security Desk, exiba uma câmera em uma janela.

2 Pressione `Ctrl+Shift+R`.

As informações de diagnóstico sobre o fluxo de vídeo são sobrepostas à janela.

3 Clique em **OK** para exibir informações sobre cada uma das seguintes conexões de transmissão de vídeo:

- **Archiver ou Archiver auxiliar ou redirecionador de Federation™:** O status de transmissão da câmera de origem para a função Archiver, Archiver auxiliar ou redirecionador de Federation™ que inicialmente fornece a transmissão.
- **Redirecionador:** O status de transmissão da função Archiver, Archiver auxiliar ou redirecionador de Federation™ para o redirecionador encaminhar a transmissão para o próximo salto.

  NOTA: Todos os redirecionadores envolvidos no roteamento são listados.
- **Media player:** O status do fluxo do último redirecionador envolvido no roteamento para sua estação de trabalho do Security Desk.

4 Clique em **Fechar**.

Optimizar o desempenho do decodificador de vídeo no seu computador

O Security Desk pode detectar e usar hardware compatível para acelerar a decodificação de vídeo. A aceleração de hardware melhora o desempenho, especialmente ao exibir vários fluxos H.264 de alta definição.

O que você deve saber

Para obter informações sobre placas de vídeo recomendadas e benchmarks de desempenho, consulte o*Security Center Guia Requisitos do Sistema*.

NOTA: O Security Desk não suporta a aceleração de hardware no Windows XP.

Para optimizar o desempenho do decodificador de vídeo no seu computador:

1 Para otimizar a operação com placas de vídeo NVIDIA, verifique o seguinte:
- A placa de vídeo é um modelo compatível.
- O monitor ou projetor usado para exibir vídeo está conectado a esta placa de vídeo.
- O driver instalado é o mais recente disponível no site oficial da NVIDIA.

2 Para otimizar a operação com o Intel Quick Sync, verifique o seguinte:
- Sua CPU suporta Quick Sync; consulte http://ark.intel.com para confirmar.
- A placa de vídeo integrada na CPU é de um modelo compatível.
- Um monitor está conectado à saída integrada da placa-mãe.
- Os gráficos integrados Intel estão habilitados na BIOS.
- O driver instalado é o mais recente disponível no site oficial da Intel.

NOTA: Em computadores de alto desempenho, a decodificação GPU da NVIDIA funciona melhor quando o Quick Sync está desativado.

3 Para solucionar problemas com várias telas e várias GPUs, verifique o seguinte:
- Se o modo "SLI" (Scalable Link Interface) estiver disponível, desative-o.
- Se você tiver várias placas de vídeo NVIDIA, conecte cada monitor a uma placa diferente para usá-los em paralelo.
- Se você tiver placas de vídeo usando drivers diferentes (AMD, NVIDIA, Intel), defina um monitor conectado a uma placa NVIDIA como o monitor principal.
- Se placas de vídeo integradas e discretas estiverem disponíveis e se a placa de vídeo NVIDIA atender aos requisitos recomendados, desative a placa de vídeo integrada no BIOS. Ter a placa integrada disponível dificulta o desempenho discreto da placa de vídeo.
- Após a instalação de Security Center em laptops usando a tecnologia NVIDIA OPTIMUS (combinada com GPUs da Intel e NVIDIA), todos os aplicativos de uso intensivo do vídeo devem ser executados (Security Desk, Genetec™ Video Player, e assim por diante) para registrá-los como aplicativos que exigem NVIDIA GPU. Após a configuração inicial, o aplicativo usará sempre NVIDIA GPU.

Tópicos relacionados

Caixa de diálogo Informações de hardware na página 306

Não está sendo gravado vídeo

Se o botão **Gravar** estiver amarelo () no widget de câmera ou nos controles de vídeo da tarefa *Monitoramento*, o Archiver não está gravando vídeo da câmera.

O problema de gravação poder ser causado por vídeo e áudio da câmera ou por chaves de criptografia geradas pelo Archiver.

As seguintes etapas de solução de problemas são recomendadas para resolver esta questão:

Problema de gravação	Causa possível	Solução de problemas
Não é possível gravar dados no disco rígido	O Archiver não consegue gravar na unidade de disco.	1 Verifique se o Archiver consegue acessar o disco. 2 Verifique se o disco não está cheio.
Não é possível gravar dados no banco de dados	O Archiver não consegue atualizar o banco de dados.	1 Verifique se o Archiver tem acesso ao banco de dados. 2 Verifique se o disco do banco de dados não está cheio. 3 Verifique se o servidor de banco de dados não está sobrecarregado.
Transmissão de vídeo não recebida.	A câmera deveria estar transmitindo mas nenhuma transmissão é recebida.	1 Verifique se a câmera está transmitindo vídeo ao vivo. 2 Verifique se as portas do firewall estão corretamente configuradas. 3 Execute uma análise Wireshark para determinar o motivo de o Archiver não receber a transmissão.

Solução de problemas de unidades de vídeo offline no Security Center

Quando uma câmera está vermelha na exibição de área, significa que a unidade de vídeo está offline ou que perdeu a comunicação com o Archiver.

Antes de iniciar

Verifique se tem acesso ao Security Desk e Config Tool para realizar as seguintes etapas.

O que você deve saber

Quando uma unidade fica offline no Security Center, isso normalmente coincide com um evento *Perda de unidade* no Security Desk. Isso pode ser causado por uma conexão de rede instável ou problemas com a unidade.

Para solucionar problemas de uma unidade offline:

1 Verifique se pode fazer o ping na unidade:
   a) Na tarefa *Vídeo* do Config Tool, selecione a unidade de vídeo em vermelho.
   b) Na parte inferior da tarefa *Vídeo* clique em **Unidade** > **Ping** ( ).

   Se não houver resposta, a unidade estará offline (quebrada, desligada e assim por diante), ou há um problema com a sua rede.
2 Certifique-se de que consegue conectar à unidade e clique em **Unidade** > **Página da unidade na internet**.

   DICA: Você também pode determinar se tem as credenciais corretas para a unidade.
3 Reinicie a unidade:
   a) Na tarefa *Vídeo* do Config Tool, selecione a unidade de vídeo em vermelho.
   b) Na parte inferior da tarefa *Vídeo* clique em **Unidade** > **Reiniciar** ( ).
4 Verifique se a unidade seja suportada pelo Security Centere que esteja executando o firmware certificado.

   Para uma lista de unidades de vídeo suportadas no Security Center, consulte nossa Lista de Dispositivos Suportados.
5 Reinicie a função Archiver que controla a unidade:

   IMPORTANTE: Realize esta etapa em um momento não crucial, uma vez que todas as unidades conectadas ao Archiver ficarão offline temporariamente.

   a) Na tarefa *Vídeo* de Config Tool, selecione o Archiver.
   b) Na parte inferior da tarefa *Vídeo*, clique em **Manutenção** > **Desativar função** ( ).
   c) Na caixa de diálogo de confirmação que abrir, clique em **Continuar**.

      O Archiver e todas as unidades de vídeo controladas pela função ficarão em vermelho.
   d) Na parte inferior da tarefa *Vídeo*, clique em **Manutenção** > **Ativar função** ( ).

Após terminar

Se a unidade de vídeo ainda estiver offline, entre em contato com a Assistência Técnica da Genetec™.

Executar rastreamentos de rede

Você pode executar um rastreamento de rede diretamente do Config Tool mesmo que você não tenha um analisador de pacotes de rede instalado no seu computador.

O que você deve saber

- O Security Center usa a biblioteca WinPcap para capturar o rastreamento de rede.
- Para ler esses arquivos de dados de pacotes de rede (*.pcap*), você precisa ter um analisador de pacotes de rede compatível, como o Wireshark, instalado.

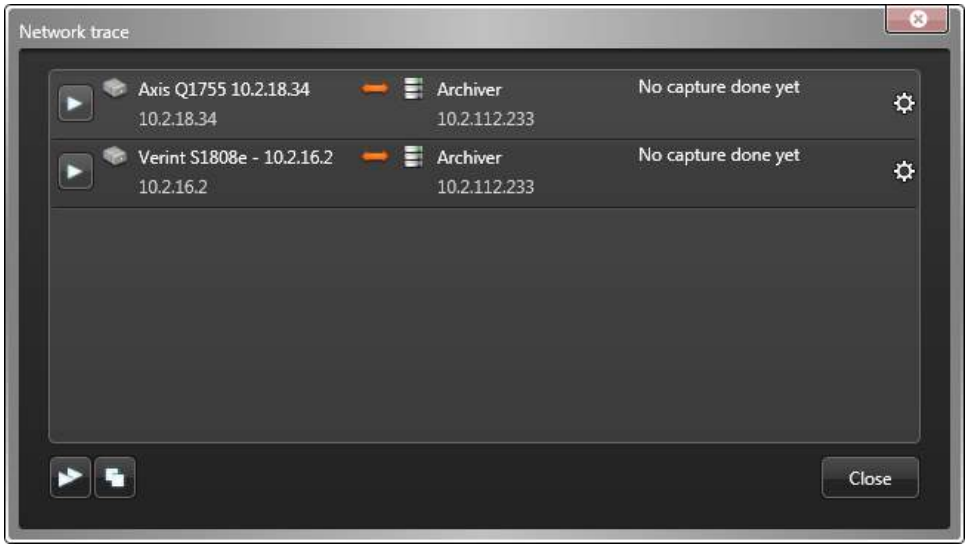
Para executar um rastreamento de rede:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.

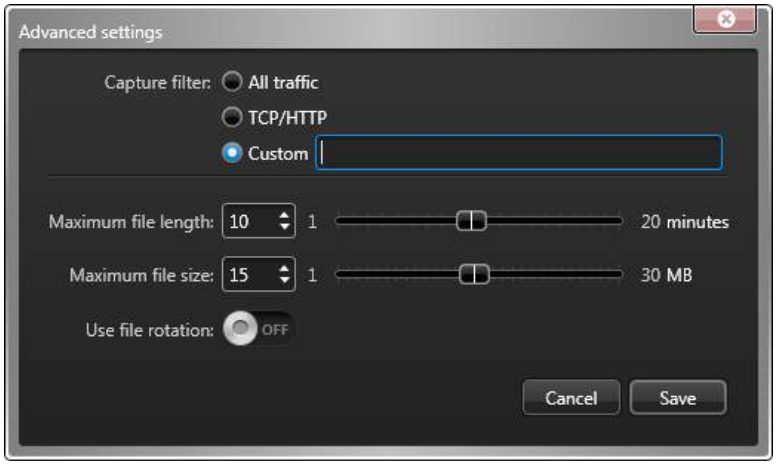
2 Na árvore de entidades, selecione unidades de vídeo para analisar.

DICA: Pressione a tecla Ctrl para realizar uma seleção múltipla.

3 Clique com o botão direito em sua seleção e clique em **Unidade** > **Rastreamento de rede**.



4 (Opcional) Clique em **Configurações avançadas** (⚙) para alterar as configurações padrão de uma determinada captura.



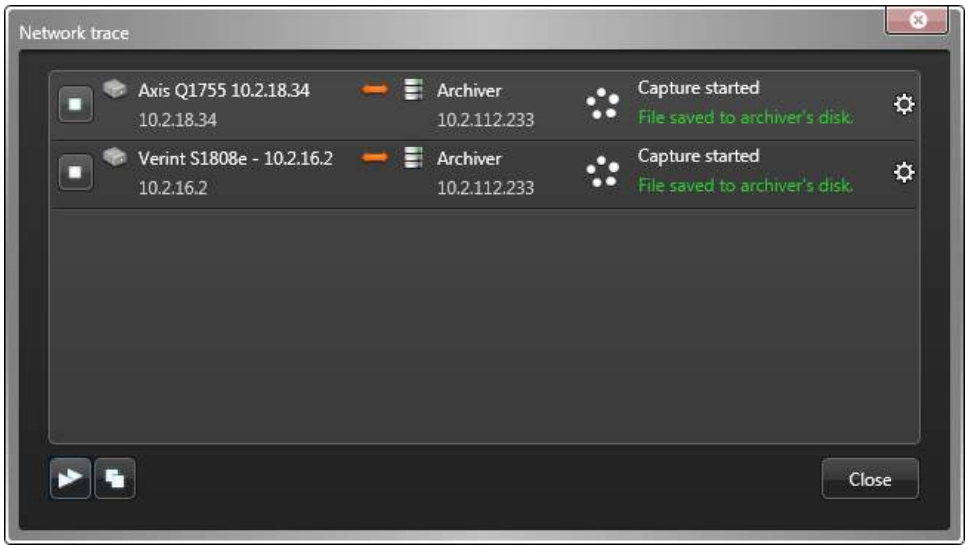
- **Filtro de captura:** Selecione o tipo tráfego que deseja capturar.
  - **Todo o tráfego:** Captura tudo o que existe entre a unidade de vídeo e o Archiver.

- **TCP e HTTP:** Captura somente o tráfego TCP e HTTP entre a unidade de vídeo e o Archiver. Isto elimina outro tráfego como UDP.
- **Personalizar:** Filtro personalizado. Use a mesma sintaxe que para o Wireshark. Exemplo: `host 10.1.1.1 and not udp`.

- **Extensão máxima de arquivo:** Duração máxima da captura (padrão = 10 minutos).
- **Tamanho máximo de arquivo:** Tamanho máximo do arquivo de dados capturados (padrão = 15 MB).
- **Usar rotação de arquivos:**
  - Desligado (padrão): A captura para quando o comprimento máximo do arquivo ou o tamanho máximo do arquivo é atingido, o que ocorrer primeiro.
  - Ligado: A captura é mantida até o comprimento máximo do arquivo. Um novo arquivo é criado sempre que o tamanho máximo do arquivo é atingido, mas apenas os dois últimos são mantidos.

5 Fazer um dos seguintes:

- Clique em **Iniciar captura** ( ) para iniciar uma captura específica.
- Clique em **Iniciar todas as capturas** ( ) para iniciar todas as capturas configuradas.



6 Clique em **Fechar** quando terminar.

Os pacotes de rede capturados são salvos em arquivos de dados no servidor que hospeda a função Archiver, na pasta *C:\Windows\Temp*.

Os nomes dos arquivos seguem o formato *genetec_capture_<address>_<date>_<time>_<sequence>.pcap*, onde:

- <*address*> é o endereço IP da unidade de vídeo.
- <*date*> é a data do início da captura no formato "aa-mm-dd".
- <*time*> é a hora de início da captura em horas, minutos e segundos.
- <*sequence*> é o número sequencial do arquivo.

  NOTA: Quando a rotação de arquivos está ativada, ela indica quantos arquivos foram criados durante o evento de captura. Apenas os dois últimos são mantidos. Caso contrário, ela permanece em '0001'.

Solução de problemas: erros "Impossível estabelecer sessão de vídeo com o servidor"

Se surgir uma mensagem *Erro: Impossível estabelecer sessão de vídeo com o servidor*, você pode tentar determinar a causa.

Antes de iniciar

Verifique se tem acesso ao Security Desk e Config Tool para realizar as seguintes etapas.

O que você deve saber

A mensagem *Erro: Impossível estabelecer sessão de vídeo com o servidor* pode aparecer por vários motivos. Pode haver um problema com o servidor, a função Media Router, a função *Federation™*, a função Archiver ou a própria unidade de vídeo.

Para diagnosticar um erro *Impossível estabelecer sessão de vídeo com o servidor***:**

1. Certifique-se de que o servidor esteja em execução.
2. Certifique-se de que a função Archiver esteja online:
   a) Na tarefa *Vídeo* de Config Tool, selecione o Archiver.
   b) Na parte inferior da tarefa *Vídeo*, clique em **Manutenção** > **Diagnosticar** ( ).
   c) Solucione os problemas que possam existir.
3. Se você estiver tentando exibir uma câmera federada, verifique se a função *Security Center Federation™* ou a função *Omnicast™ Federation™* está online:
   a) Na tarefa Config Tool *Sistema*, clique na visualização **Funções**.
   b) Selecione a função Federation™ e clique em **Manutenção** > **Diagnosticar** ( ).
   c) Solucione os problemas que possam existir.
4. Se você estiver tentando exibir uma câmera federada, verifique se o servidor do sistema Security Center federado está online.
5. Pode ser um problema de conexão com o Media Router. Certifique-se de que a função Media Router esteja online:
   a) Na tarefa Config Tool *Sistema*, clique na visualização **Funções**.
   b) Selecione a função Media Router e clique em **Manutenção** > **Diagnosticar** ( ).
   c) Solucione os problemas que possam existir.
6. Reinicie a função Media Router:
   a) Na tarefa Config Tool *Sistema*, clique na visualização **Funções**.
   b) Selecione a função Media Router e clique em **Manutenção** > **Desativar função** ( ).
   c) Na caixa de diálogo de confirmação que abrir, clique em **Continuar**.
   O Media Router fica vermelho.
   d) Na parte inferior da tarefa *Sistema*, clique em **Manutenção** > **Ativar função** ( ).
7. Certifique-se de que a unidade está online.
   Se a unidade estiver em vermelho na visualização *Funções e unidades*, solucione problemas relacionados com o motivo de a unidades de vídeo estar offline.

Impossível assistir vídeo ao vivo no Security Desk

Se você não puder exibir vídeo ao vivo no Security Desk, você pode tentar solucionar o problema.

Antes de iniciar

Verifique se tem acesso ao Security Desk e Config Tool para realizar as seguintes etapas.

O que você deve saber

Há várias causas possíveis para um erro de sinal ausente:

- A rede está lenta.
- A conexão da porta está com problemas.
- A transmissão de vídeo caiu enquanto era redirecionada para o Security Desk.

Para solucionar problemas de exibição de vídeo ao vivo:

1 Aguarde para ver se a câmera se conecta.

2 Se o problema persistir por mais de 10 segundos, clique em **Exibir diagnóstico** no ladrilho, ou pressione `Ctrl+Shift+D`.

Informações sobre o fluxo de vídeo são exibidas. A etapa atual é destacada:

- **Iniciando:** O reprodutor de mídia está preparando os recursos exigidos para exibir a transmissão de vídeo.
- **Conectando ao Media Router:** O reprodutor de mídia está estabelecendo conexão com o Media Router para obter a localização de rede da transmissão.
- **Conectando ao Archiver e redirecionador:** O reprodutor de mídia está estabelecendo uma conexão com o Archiver e o redirecionador para solicitar vídeo.
- **Solicitando fluxo ao vivo:** A conexão é estabelecida entre o Archiver e o Media Player. O Media Player está agora solicitando o stream ao vivo.
- **Analisando o fluxo:** A transmissão foi solicitada e recebida pela estação de trabalho do cliente. O reprodutor de mídia está analisando a transmissão para detectar o formato de vídeo e a presença de quadros-chave. Uma vez que a transmissão seja validada, o vídeo é decodificado.

DICA: Clique no link **Ajuda** para obter uma lista de coisas que você pode tentar para solucionar o problema.

3 Confirme se a unidade está online.

Se a unidade estiver em vermelho na tarefa *Vídeo* no Config Tool, solucione problemas relacionados com o motivo das unidades de vídeo estarem offline.

4 Verifique se pode fazer o ping na unidade:
   a) Na tarefa *Vídeo* do Config Tool, selecione a unidade de vídeo em vermelho.
   b) Na parte inferior da tarefa *Vídeo* clique em **Unidade** > **Ping** ( ).

   Se não houver resposta, a unidade estará offline (quebrada, desligada e assim por diante), ou há um problema com a sua rede.
5 Certifique-se de que consegue conectar à unidade e clique em **Unidade** > **Página da unidade na internet**.

   DICA: Você também pode determinar se tem as credenciais corretas para a unidade.
6 Verifique se a unidade seja suportada pelo Security Centere que esteja executando o firmware certificado.

   Para uma lista de unidades de vídeo suportadas no Security Center, consulte nossa Lista de Dispositivos Suportados.
7 Altere o tipo de conexão da unidade de vídeo para o Archiver:
   a) Na tarefa *Vídeo* do Config Tool, selecione a câmera em vermelho.
   b) Clique na aba **Vídeo**.
   c) Na lista suspensa **Tipo de conexão** na seção *Configurações de rede*, selecione um tipo de conexão diferente.
   d) Clique em **Aplicar**.
8 Tente visualizar o vídeo de reprodução da câmera:
   a) Na tarefa *Arquivos* de Security Desk, selecione a câmera.
   b) Selecione o arquivo de vídeo mais recente disponível e clique em **Gerar relatório**.
   c) Depois que o relatório for gerado, tente ver o vídeo a partir do arquivo.
      - Se você puder ver o vídeo, continue com a próxima etapa de solução de problemas.
      - Se você não puder visualizar nenhum vídeo, entre em contato com o Centro de Assistência Técnica Genetec™.
9 Se você tiver um servidor de expansão em seu sistema executando a função Archiver, tente exibir vídeo do servidor de expansão:
   a) Abra o Security Desk no servidor de expansão.
   b) Na tarefa *Monitoramento*, arraste a câmera da visualização de área para um ladrilho na tela.
      - Se você puder visualizar vídeo, pode ser um problema com o redirecionamento do Media Router para o seu Security Desk. Continue com a próxima etapa de solução de problemas.
      - Se você não puder visualizar nenhum vídeo, entre em contato com o Centro de Assistência Técnica Genetec™.
10 Certifique-se de que as portas corretas estão abertas na sua rede para que o firewall não bloqueie a transmissão de vídeo.
11 Verifique se cada rede no seu sistema está configurada corretamente, da seguinte maneira:
   a) Na tarefa *Visualização de rede* do Config Tool, selecione uma rede.
   b) Clique na aba **Propriedades** e certifique-se de que todas as configurações estão corretas: prefixo IP, máscara de sub-rede, rotas, capacidades de rede e assim por diante.
   c) Altere as configurações de rede, se necessário, e clique em **Aplicar**.

   Para mais informações, consulte Sobre redes na página 154.
12 Force o Security Desk a utilizar um tipo de conexão diferente:
   a) Na página inicial do Security Desk, clique em **Opções** > **Geral**.
   b) Na seção *Opções de rede*, próximo à opção **Rede**, selecione **Específica**.
   c) Na lista suspensa, selecione uma rede diferente e clique em **Salvar**.
   d) Reinicie o Security Desk.
   e) Se a alteração da conexão de rede não funcionar, repita as etapas para testar usando outras redes.
13 Se ainda não conseguir ver o vídeo, clique em **Exibir status da transmissão de vídeo** no ladrilho, em seguida solucione problemas da transmissão de vídeo.
14 Se o problema persistir, entre em contato com o Centro de Assistência Técnica Genetec™.

Impossível assistir a reprodução de vídeo no Security Desk

Se não conseguir visualizar arquivos de vídeo ou reprodução de vídeo no Security Desk, pode tentar resolver o problema.

O que você deve saber

Verifique se tem acesso ao Security Desk e Config Tool para realizar as seguintes etapas.

Para solucionar problemas de visualização de vídeo de reprodução:

1 Tente exibir vídeo ao vivo da câmera arrastando a câmera da visualização de área para um ladrilho na tarefa *Monitoramento* do Security Desk.

- Se você puder exibir vídeo ao vivo, continue com a próxima etapa de solução de problemas.
- Se você não conseguir visualizar nenhum vídeo, provavelmente é um problema de rede. Veja Solução de problemas de unidades de vídeo offline no Security Center na página 559.

2 Tente visualizar o vídeo de reprodução na tarefa *Arquivos*:

a) Na tarefa *Arquivos* de Security Desk, selecione a sua câmera.
b) Pesquise por arquivos de vídeos em diferentes datas e horas e clique em **Gerar relatório**.
c) Depois que o relatório for gerado, tente ver o vídeo a partir dos arquivos.
d) Repita as etapas com outras câmaras que estão ligadas ao mesmo Archiver.

- Se você puder visualizar o vídeo de alguns dos arquivos de vídeo, continue com a próxima etapa de solução de problemas.
- Se você não conseguir visualizar nenhum vídeo, ignore a próxima etapa de solução de problemas.

3 Verifique se a unidade seja suportada pelo Security Centere que esteja executando o firmware certificado.

Para uma lista de unidades de vídeo suportadas no Security Center, consulte nossa Lista de Dispositivos Suportados.

4 Tente visualizar o vídeo de reprodução da tarefa *Arquivos* em outro Security Desk e no servidor em que a função Archiver está em execução.

- Se você puder visualizar vídeo, pode ser um problema com o redirecionamento do Media Router para o seu Security Desk. Continue com a próxima etapa de solução de problemas.
- Se você não puder visualizar nenhum vídeo, entre em contato com a Assistência Técnica Genetec™.

5 Certifique-se de que as portas corretas estão abertas na sua rede para que o firewall não bloqueie a transmissão de vídeo.

6 Se você ainda não puder visualizar vídeo de reprodução, entre em contato com o Centro de Assistência Técnica Genetec™.

Solução de problemas: As câmeras não estão gravando

Se não conseguir gravar vídeo ou se houver arquivos de vídeo em falta ou lacunas nos arquivos, você poderá tentar determinar a causa do problema.

Antes de iniciar

Verifique se tem acesso ao Security Desk e Config Tool para realizar as seguintes etapas.

O que você deve saber

Se você pode ver o vídeo ao vivo de uma câmera, mas não pode gravar o vídeo, pode ser devido ao modo de gravação da câmera, à agenda de arquivamento, ao banco de dados de função Archiver ou até mesmo ao uso da CPU.

Seguem alguns modos de identificar se a câmera não está gravando:

- Ao visualizar vídeo ao vivo, o estado de gravação da câmara é indicado no canto inferior direito do ladrilho. Se o status indicar 

, a câmera não está gravando.
- Você está tentando visualizar vídeo de reprodução, mas não há nenhum vídeo disponível para a data e hora que você selecionou, e você sabe que deve haver.

Para solucionar problemas de uma câmera que não grava:

1 Verifique se a unidade seja suportada pelo Security Centere que esteja executando o firmware certificado.
Para uma lista de unidades de vídeo suportadas no Security Center, consulte nossa Lista de Dispositivos Suportados.

2 Verifique o tipo de gravação da câmera para garantir que a câmera está configurada para gravar vídeo segundo a agenda:
a) Na tarefa *Vídeo* de Config Tool, selecione a sua câmera.
b) Clique na guia **Gravando**.
- Se a opção **Configurações de gravação** estiver definida para **Configurações personalizadas**, verifique se todas as configurações de gravação estão corretas e clique em **Aplicar**.
- Se a opção **Configurações de gravação** estiver definida para **Herdar do Archiver**, continue para a próxima subetapa.

c) Na tarefa *Vídeo*, selecione o Archiver.
d) Clique na aba **Configurações padrão da câmera**.
e) Na seção *Modos de gravação*, garanta que o Archiver esteja definido para gravar segundo a **Agenda** e que o **Modo** de gravação esteja definido para **Desligado**.

3 Se o modo de gravação da câmara estiver definido como **Ativado por movimento/Manual**, verifique se as configurações de detecção de movimento estão configuradas corretamente:
a) Na tarefa *Vídeo* de Config Tool, selecione a sua câmera.
b) Clique na guia **Detecção de movimento**.
c) Verifique as configurações de detecção de movimento.

4 Verifique o status do banco de dados da função Archiver:
a) Na tarefa *Vídeo* de Config Tool, selecione o Archiver.
b) Clique na guia **Recursos**.
- Se o status do banco de dados do Archiver for **Conectado**, siga para a próxima etapa da solução de problemas.
- Se o status do banco de dados do Archiver for **Desconectado** ou **Indisponível**, continue para a próxima subetapa.

c) Alterne para um banco de dados de arquivos diferente ou crie um novo.

CUIDADO: Realize esta etapa em um momento não crucial, uma vez que todas as unidades conectadas ao Archiver ficarão temporariamente offline. Não exclua nem sobrescreva o banco de dados existente, ou seus arquivos de vídeo serão excluídos.

1. No campo **Banco de dados**, digite um nome diferente e clique em **Aplicar**.
2. Aguarde até que a função estabeleça conexão com o novo banco de dados. Se o banco de dados não existir, ele será criado.
3. Se a câmera puder gravar usando o novo banco de dados, você pode continuar a usar o novo banco de dados.

   CUIDADO: Ao alternar para um banco de dados diferente, os arquivos de vídeos referenciados na banco de dados antigo não são mais incluídos nas pesquisas do Security Center e não serão excluídos pela limpeza automática do Archiver.
4. Se a câmera ainda não estiver gravando, volte ao banco de dados original e continue para a próxima etapa de solução de problemas.

5 Verifique quanto espaço em disco está disponível para arquivamento:
   a) Na tarefa *Vídeo* de Config Tool, selecione o Archiver.
   b) Clique na aba **Recursos**.
   c) Na tabela de informações do disco, certifique-se de que o valor de **Espaço livre mín.** seja de pelo menos 0,2% do espaço total em disco.

      O **Espaço livre mín.** é a quantidade mínima de espaço livre que o Archiver deve deixar intocado no disco.
   d) Se o valor de **Espaço livre mín.** for inferior a 0,2% do espaço total em disco, clique no valor e, em seguida, aumente-o.

      Para ver o espaço total em disco, coloque o cursor do mouse sobre o medidor de **Uso do disco**.

6 Verifique se há eventos de *Arquivamento interrompido* e *Gravação interrompida* que ocorreram no seu sistema.

   No Windows, no servidor onde a função Archiver está em execução, abra os arquivos *.log* localizados em *C:\ArchiverLogs*.

   Se houver eventos de *Arquivamento interrompido* ou *Gravação interrompida* na coluna **Tipo de entrada**, reinicie o serviço Genetec™ Server:

   a) Abra o painel de controle do Windows.
   b) Clique em **Ferramentas administrativas** > **Serviços**.
   c) Clique com o botão direito do mouse no serviço **Genetec™ Server** e clique em **Reiniciar**.

7 Verifique se ocorreram eventos de *Transmissão perdida* e *Pacotes RTP perdidos* no sistema.

   No Windows, no servidor onde a função Archiver está em execução, abra os arquivos *.log* localizados em *C:\ArchiverLogs*.

   - Se houver muitos eventos de *Transmissão perdida* e *Pacotes RTP perdidos* na coluna **Tipo de entrada**, pode ser um problema de rede ou de uso de CPU. Continue para a próxima etapa de solução de problemas.
   - Se não houver muitos eventos de *Transmissão perdida* e *Pacotes RTP perdidos*, ignore a próxima etapa da solução de problemas.

8 Verifique seu uso da CPU:
   a) Clique com o botão direito do mouse na barra de tarefas do Windows e abra o *Gerenciador de Tarefas do Windows*.
   b) Clique na aba **Desempenho** e verifique se **Uso da CPU** não ultrapassa 60%.

      Se **Uso da CPU** estiver acima de 60%, reinicie o servidor e considere adicionar mais CPU ao servidor.
   c) Clique na aba **Rede** e certifique-se de que a **Velocidade do link** da rede não esteja acima de 300 Mbps.

9 Se você estiver tendo problemas de gravação apenas com uma unidade de vídeo, tente o seguinte:
   a) Na tarefa *Vídeo* do Config Tool, clique com o botão direito na unidade de vídeo em vermelho e clique em **Excluir**.
   b) Na caixa de diálogo de confirmação, escolha se pretende manter os arquivos de vídeos da unidade.

      A unidade de vídeo é removida do Archiver.
   c) Adicione a unidade de vídeo.

Após terminar

Se ainda não conseguir gravar vídeo na câmera, entre em contato com o Centro de Assistência Técnica da Genetec™.

Solução de problemas: Não é possível adicionar unidades de vídeo

Se não estiver conseguindo adicionar uma unidade de vídeo a um Archiver, você pode tentar determinar a causa do problema.

Antes de iniciar

Faça logon no Config Tool como um administrador.

O que você deve saber

Problemas em adicionar unidades de vídeo podem ser devidos a problemas de rede, problemas de credenciais do usuário e assim por diante.

Para solucionar problemas de uma unidade de vídeo que não pode ser adicionada:

1 Verifique se pode fazer o ping na unidade:
   a) Na tarefa *Vídeo* do Config Tool, selecione a unidade de vídeo em vermelho.
   b) Na parte inferior da tarefa *Vídeo* clique em **Unidade** > **Ping** ( ).

   Se não houver resposta, a unidade estará offline (quebrada, desligada e assim por diante), ou há um problema com a sua rede.
2 Certifique-se de que consegue conectar à unidade e clique em **Unidade** > **Página da unidade na internet**.

   DICA: Você também pode determinar se tem as credenciais corretas para a unidade.
3 Reinicie a unidade:
   a) Na tarefa *Vídeo* do Config Tool, selecione a unidade de vídeo em vermelho.
   b) Na parte inferior da tarefa *Vídeo* clique em **Unidade** > **Reiniciar** ( ).
4 Tente adicionar novamente a unidade. Se não tiver sucesso, avance para a próxima etapa.
5 Verifique se a unidade seja suportada pelo Security Centere que esteja executando o firmware certificado.

   Para uma lista de unidades de vídeo suportadas no Security Center, consulte nossa Lista de Dispositivos Suportados.
6 Confirme que está disponível uma conexão de câmera em sua licença do Security Center:
   a) Na página inicial de Config Tool, clique na página *Sobre* e, em seguida, clique na aba **Omnicast™**.
   b) Na opção de licença **Número de câmeras**, verifique se há uma conexão de câmera disponível.

   NOTA: Algumas câmeras também exigem uma licença restrita.

   - Se a unidade de vídeo que você está tentando adicionar for de um fabricante restrito, verifique se há uma conexão de câmera disponível na opção de licença **Número de câmeras restritas**.
   - Para exibir uma lista de fabricantes que exigem uma licença restrita, use o filtro **Tipo de licença** *Restrito* na página da Web Lista de Dispositivos Suportados.
7 Certifique-se de que está utilizando as credenciais corretas para adicionar a unidade:

   Para alguns fabricantes, é necessário definir as credenciais padrão na aba **Extensões** do Archiver.
   a) Na tarefa *Vídeo* do Config Tool, selecione o Archiver ao qual você deseja adicionar a unidade de vídeo.
   b) Clique na aba **Extensões**.
   c) Para adicionar a extensão da unidade de vídeo, clique em **Adicionar um item** ( ), selecione o tipo de extensão e clique em **Adicionar**.
   d) Selecione a extensão.
   e) Na seção *Logon padrão*, digite o nome de usuário e a senha para a unidade.
8 Verifique se o Archiver está conectado ao banco de dados correto:
   a) Na tarefa *Vídeo* de Config Tool, selecione o Archiver.

b) Clique na guia **Recursos**.

- Se o status do banco de dados do Archiver for **Conectado**, siga para a próxima etapa da solução de problemas.
- Se o status do banco de dados do Archiver for **Desconectado** ou **Indisponível**, continue para a próxima subetapa.

c) Alterne para um banco de dados de arquivos diferente ou crie um novo.

CUIDADO: Realize esta etapa em um momento não crucial, uma vez que todas as unidades conectadas ao Archiver ficarão temporariamente offline. Não exclua nem sobrescreva o banco de dados existente, ou seus arquivos de vídeo serão excluídos.

1 No campo **Banco de dados**, digite um nome diferente e clique em **Aplicar**.
2 Aguarde até que a função estabeleça conexão com o novo banco de dados. Se o banco de dados não existir, ele será criado.
3 Se a câmera puder gravar usando o novo banco de dados, você pode continuar a usar o novo banco de dados.

CUIDADO: Ao alternar para um banco de dados diferente, os arquivos de vídeos referenciados na banco de dados antigo não são mais incluídos nas pesquisas do Security Center e não serão excluídos pela limpeza automática do Archiver.

4 Se a câmera ainda não estiver gravando, volte ao banco de dados original e continue para a próxima etapa de solução de problemas.

9 Certifique-se de que a função Media Router esteja conectada ao banco de dados correto:

NOTA: Se a câmera tiver sido adicionada anteriormente no Security Center e o endereço IP ou nome foi alterado, você também pode recriar o banco de dados do Media Router.

a) Na tarefa *Vídeo* do Config Tool, selecione o Media Router.
b) Clique na aba **Recursos**.

- Se o status do banco de dados do Media Router for **Conectado**, siga para a próxima etapa da solução de problemas.
- Se o status do banco de dados do Media Router for **Desconectado** ou **Indisponível**, continue para a próxima subetapa.

c) Clique em **Criar um banco de dados** ( ).

10 Tente adicionar a unidade com o firewall desligado.

Para obter instruções sobre como desabilitar o firewall do Windows, consulte KBA00596: "Configurações recomendadas do firewall do Windows" no hub TechDoc da Genetec™.

IMPORTANTE: Reative-o após a conclusão dos testes.

11 Verifique se cada rede no seu sistema está configurada corretamente, da seguinte maneira:
a) Na tarefa *Visualização de rede* do Config Tool, selecione uma rede.
b) Clique na aba **Propriedades** e certifique-se de que todas as configurações estão corretas: prefixo IP, máscara de sub-rede, rotas, capacidades de rede e assim por diante.
c) Altere as configurações de rede, se necessário, e clique em **Aplicar**.

Para mais informações, consulte Sobre redes na página 154.

12 Verifique se o Archiver, o Media Router e todos os redirecionadores estão usando a NIC (placas de interface de rede) correta:
a) Na tarefa *Sistema* do Config Tool, clique na visualização **Funções**.
b) Selecione a função **Archiver** e clique na aba **Recursos**.
c) Na lista suspensa **Placa de rede**, selecione a NIC adequada.
d) Na árvore de entidades, selecione a função **Media Router** e clique na aba **Recursos**.
e) Na seção *Servidores*, clique em **Avançado** ( ).
f) Selecione a **Placa de rede** adequada para cada servidor e clique em **Aplicar**.
g) Clique na guia **Propriedades.**
h) Selecione um **Redirecionador** e clique em **Editar o item** ( ).
i) Na lista suspensa **Interface multicast**, selecione a NIC adequada.
j) Repita as duas últimas subetapas para cada redirecionador.

13 Tente adicionar novamente a unidade. Se não tiver sucesso, avance para a próxima etapa.
14 Verifique a prioridade das NICs no Windows:
   a) No Windows, clique em **Iniciar** > **Executar** e digite `ncpa.cpl`.
      A janela *Conexões de rede* será aberta.
   b) Clique no menu **Avançado** e selecione **Configurações avançadas**.
   c) Observe qual NIC no servidor está configurada como prioridade de rede um (parte superior da lista de conexões) e qual está configurada como a prioridade dois.
   d) Se necessário, use os botões de seta no lado direito para reposicionar as conexões na lista.
15 Tente adicionar novamente a unidade. Se não tiver sucesso, avance para a próxima etapa.
16 Pode ser um problema de conexão com o Media Router. Certifique-se de que a função Media Router esteja online:
   a) Na tarefa Config Tool *Sistema*, clique na visualização **Funções**.
   b) Selecione a função Media Router e clique em **Manutenção** > **Diagnosticar** ().
   c) Solucione os problemas que possam existir.
17 Certifique-se de que a função Archiver esteja online:
   a) Na tarefa *Vídeo* de Config Tool, selecione o Archiver.
   b) Na parte inferior da tarefa *Vídeo*, clique em **Manutenção** > **Diagnosticar** ().
   c) Solucione os problemas que possam existir.

Após terminar

Se ainda não puder adicionar a unidade de vídeo, entre em contato com a Assistência Técnica da Genetec™.

Solução de problemas: Não é possível excluir unidades de vídeo

Se não conseguir excluir uma unidade de vídeo, pode desativar temporariamente o Archiver.

Para excluir uma unidade de vídeo:

1. Na tarefa *Vídeo* de Config Tool, selecione o Archiver.
2. Na parte inferior da tarefa *Vídeo*, clique em **Manutenção** > **Desativar função** ( ).
3. Na caixa de diálogo de confirmação que abrir, clique em **Continuar**.
   O Archiver e todas as unidades de vídeo controladas pela função ficarão em vermelho.
4. Selecione a unidade de vídeo e, na parte inferior da tarefa *Vídeo*, clique em **Excluir** ( ).
5. Selecione o Archiver e, na parte inferior da tarefa *Vídeo*, clique em **Manutenção** > **Ativar função** ( ).

Solução de problemas: problemas com a transmissão de vídeo H.264:

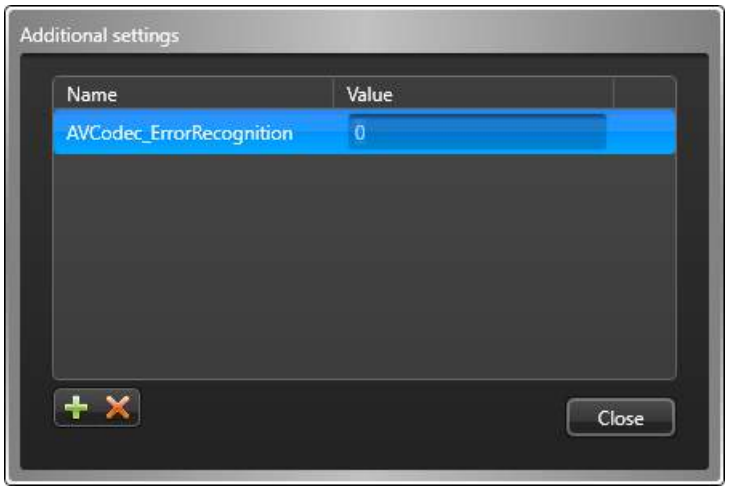
Se você estiver tendo problemas ao visualizar transmissões de vídeo H.264, você pode desativar a configuração avançada da função Archiver *AVCodec_ErrorRecognition*.

O que você deve saber

Verifique se tem acesso ao Security Desk e Config Tool para realizar as seguintes etapas.

Para solucionar problemas com o stream de vídeo H.264:

1 Na tarefa Config Tool *Vídeo*, selecione o Archiver para configurar.
2 Clique na aba **Recursos**.
3 Na parte inferior da aba **Recursos**, clique em **Configurações avançadas**.
4 Clique em **Configurações adicionais**.
5 Na caixa de diálogo *Configurações adicionais*, clique em **Adicionar um item** ( ).
6 Na coluna **Nome**, digite `AVCodec_ErrorRecognition`.



7 Na coluna **Valor**, digite 0.
8 Clicar**Fechar** > **OK** > **Aplicar**.
9 Quando for solicitado a reiniciar o Archiver, clique em **Sim**.

Você deve ver melhora no fluxo de vídeo. Se não houver nenhuma alteração, você pode tentar outros valores (1-4).

Solução de problemas: problema de sensibilidade da câmera Axis P1428-E

Se você não conseguir diminuir a sensibilidade da câmera Axis P1428-E para obter uma detecção de movimento confiável executada pelo Archiver em sua transmissão de vídeo H.264, você pode diminuir o valor de **Peso dos vectores** em *Configurações avançadas*.

O que você deve saber

A câmera Axis P1428-E codifica os vetores de movimento de forma diferente da maioria das câmeras, fazendo com que o algoritmo de detecção de movimento do Archiver seja extremamente sensível.

Para diminuir a sensibilidade de detecção de movimento na câmera Axis P1428-E:

1. Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2. Selecione a câmera a ser configurada e clique na aba **Detecção de movimento**.
3. Clique em **Configurações avançadas**.

   NOTA: As **Configurações avançadas** somente estão visíveis quando a opção **A detecção é feita em: Archiver** é selecionada.

4. Na caixa de diálogo *Configurações avançadas de detecção de movimento H.264*, diminua o **Peso dos vectores** para 1 ou 0 e clique em **OK**.

   Isto permite que o algoritmo de detecção de movimento do Archiver responda de modo diferente a configurações de *Sensibilidade*.
5. Teste a detecção de movimento com diferentes configurações de sensibilidade até obter resultados satisfatórios.
6. Clique em **Aplicar**.

A detecção de movimento não está funcionando no Security Center

Se a detecção de movimento não estiver funcionando para algumas câmeras no Security Center, você poderá solucionar o problema.

O que você deve saber

Estas informações estavam no artigo obsoleto KBA-00965 da base de dados de conhecimento.

Para solucionar problemas de detecção de movimento no Security Center:

1. Verifique se a unidade seja suportada pelo Security Centere que esteja executando o firmware certificado.

   Para uma lista de unidades de vídeo suportadas no Security Center, consulte nossa Lista de Dispositivos Suportados.
2. Certifique-se de que não haja problemas conhecidos ou limitações relacionadas à detecção de movimento para sua câmera nas *Notas de Versão do Security Center*.
3. Certifique-se de que as configurações de detecção de movimento estejam definidas adequadamente para a câmera.
4. Verifique se está recebendo eventos de movimento no Security Desk:
   a) Na página inicial do Security Desk, clique em **Opções** > **Eventos**.
   b) Verifique se os eventos *Movimento ativo* e *Movimento inativo* estão selecionados em clique em **Salvar**.
   c) Abra a tarefa de *Monitoramento* .
   d) Na parte inferior da tarefa *Monitoramento*, clique em **Monitoramento** ( ) e, em seguida, clique em **Adicionar** ( ).
   e) Na caixa de diálogo *Selecionar uma entidade para monitorar*, selecione uma câmera e clique em **Adicionar**.

      As entidades selecionadas são adicionadas à lista **Monitoramento de evento** .
   f) Crie algum movimento perto da câmera para confirmar que os eventos de movimento aparecem na lista de eventos da tarefa *Monitoramento*.
5. Se você não receber nenhum evento de movimento, abaixe o valor de **Limiar de movimento ativo** na aba **Detecção de movimento** da câmera e tente criar movimento perto da câmera novamente.
6. Tome uma das seguintes ações:
   - Se você receber os eventos de movimento, verifique se a detecção de movimento está funcionando configurando a câmera para gravar quando ocorre movimento:
     1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
     2 Selecione a câmera a ser configurada e clique na aba **Gravação**.
     3 Na lista suspensa **Modos de gravação**, selecione **Havendo movimento/Manual**.
     4 Clique em **Aplicar**.
   - Se você ainda não receber nenhum evento de movimento, poderá ser um problema com sua câmera. Entre em contato com a Assistência Técnica da Genetec™.

Tópicos relacionados

Câmeras Axis não têm uma aba de Detecção de movimento na página 576

Câmeras Axis não têm uma aba de Detecção de movimento

Se a câmera Axis não apresentar a aba **Detecção de movimento** no Config Tool, você deve desinstalar o aplicativo *Axis Video Motion Detection* pela página Web da unidade.

O que você deve saber

A aba **Detecção de movimento** fica oculta quando o Security Center detecta que o aplicativo *Axis Video Motion Detection* está instalado na unidade.

NOTA: Estas informações estavam no artigo obsoleto KBA-01211 da base de dados de conhecimento.

Para mostrar a guia de detecção de movimento para câmeras Axis:

1 Clique em **Unidade** > **Página Web da unidade** e faça logon.
2 Clique em **Configuração** > **Aplicativos**.
3 Em **Aplicativos Instalados**, selecione **Axis Video Motion Detection** e clique em **Remover**.
4 No menu **Opções do Sistema**, redefina a câmera para suas configurações de fábrica.

A aba **Detecção de movimento** é agora visível no Security Center.

Tópicos relacionados

A detecção de movimento não está funcionando no Security Center na página 575

Configurar o Security Center para abrir vídeo ao vivo rapidamente

Você pode minimizar o tempo necessário para que uma câmera abra e exiba vídeo ao vivo na tarefa *Monitoramento* do Security Desk, ajustando várias configurações no Config Tool e no Security Desk.

O que você deve saber

Vários fatores afetam o tempo necessário para exibir vídeo ao vivo de uma câmera no Security Desk:

- Formato de compressão de vídeo: as transmissão de vídeo MJPEG são normalmente exibidas mais rapidamente do que as transmissão de vídeo H.264.
- Qualidade da imagem: uma câmera normalmente exibe vídeo ao vivo mais rapidamente com uma qualidade de imagem de vídeo de 70% do que com uma qualidade de imagem de vídeo de 100% ou inferior a 60%.
- Intervalo de quadros-chave: definir um **Intervalo de quadros-chave** baixo para a câmera no Config Tool pode produzir melhores resultados.

Para configurar uma câmera para exibir vídeos ao vivo mais rapidamente:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.
2 Selecione a câmera a ser configurada e clique na aba **Vídeo**.
3 Na seção *Uso de transmissão*, ative **Ao vivo** e **Gravação** para a transmissão selecionada.
4 Na seção *Configurações de rede*, selecione **Multicast** como o **Tipo de conexão**.
5 Clique em **Aplicar**.
6 Clique na aba **Gravação** e selecione **Contínuo** na lista suspensa **Modos de gravação**.
7 Clique em **Aplicar**.
8 Na página inicial do Security Desk, clique em **Opções** > **Vídeo**.
9 Desça até a seção *Cache de vídeo* e desative **Cache de vídeo ao vivo**.
10 Em *Configurações avançadas*, defina o **Atraso do buffer de tremulação** para 0 ms.
11 Reinicie o Security Desk.

A proteção de privacidade não está a funcionar no Security Center

Se a proteção de privacidade não estiver funcionando para algumas câmeras no Security Center, você poderá solucionar o problema.

O que você deve saber

- Devido aos exigentes requisitos de CPU da proteção de privacidade, um único servidor Privacy Protector™ poderá ter problemas para lidar com apenas algumas transmissões em alta definição.
- A proteção de privacidade somente é suportada quando usada com câmeras nativas. A proteção de privacidade não pode ser habilitada em câmeras federadas ou DVRs. As câmeras usadas junto ao corpo não são suportadas.

Para solucionar problemas com a proteção de privacidade no Security Center:

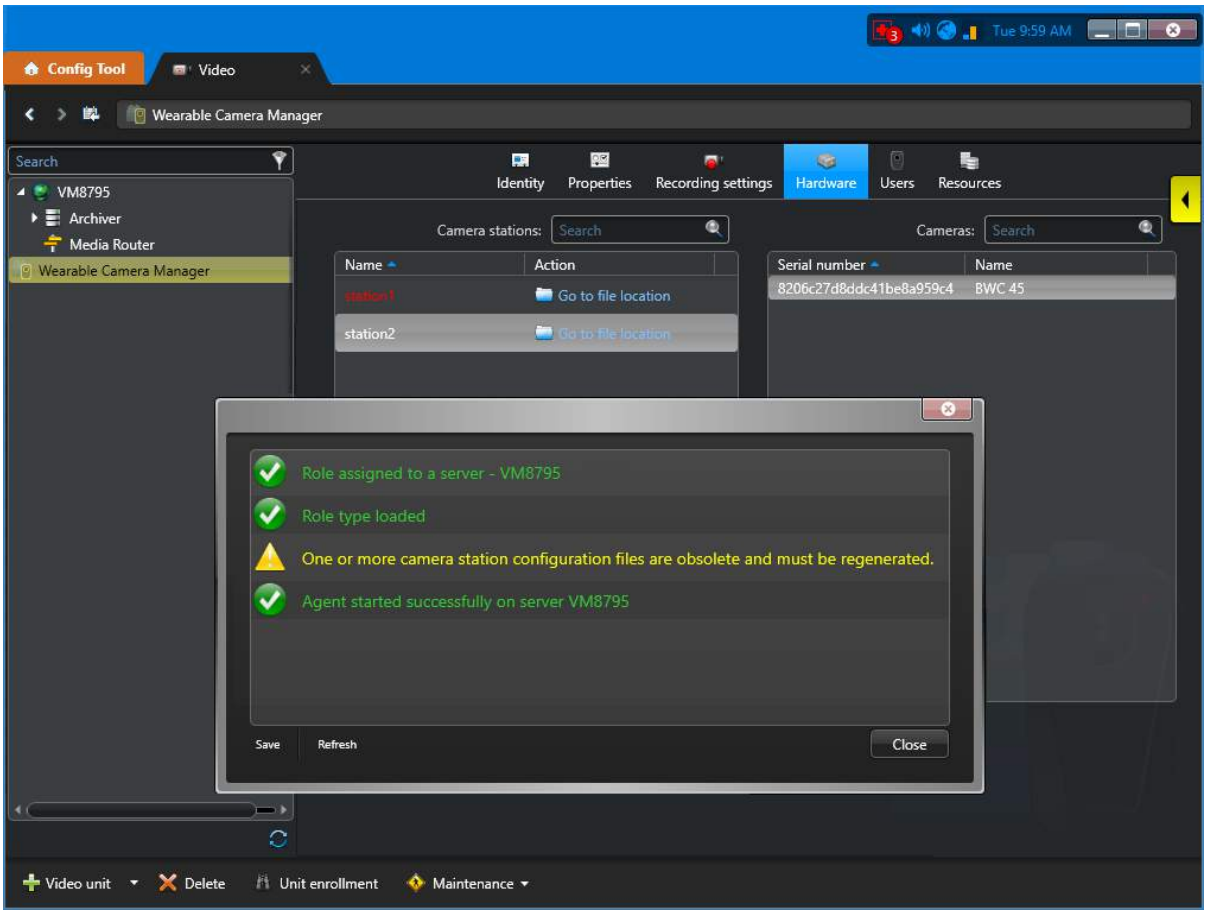
1. Verifique se a unidade seja suportada pelo Security Centere que esteja executando o firmware certificado.
   Para uma lista de unidades de vídeo suportadas no Security Center, consulte nossa Lista de Dispositivos Suportados.
2. Certifique-se de que não haja problemas conhecidos ou limitações relacionadas à proteção de privacidade para sua câmera nas *Notas de Versão do Security Center*.
3. Certifique-se de que as configurações de proteção de privacidade estejam definidas adequadamente para a câmera.
4. Para maximizar o número de transmissões que um único servidor pode processar, verifique o seguinte:
   - Use um núcleo de CPU Intel compatível com Quicksync Technology para uma codificação mais eficiente.
   - Tente limitar a taxa de quadros e a resolução das transmissões de vídeo originais (configuração da câmera).
   - Use uma estação de trabalho de alto desempenho.

Erros de arquivos de configuração de câmeras usadas junto ao corpo

Um ou mais arquivos de configuração de estações de câmeras usadas junto ao corpo contêm erros. Você pode corrigir este erro regenerando um ou todos os arquivos de configuração.

Causa

Error: Um ou mais arquivos de configuração de estação de câmera estão obsoletos e devem ser regenerados.



O arquivo de configuração de estação de câmera obsoleto é realçado em vermelho.

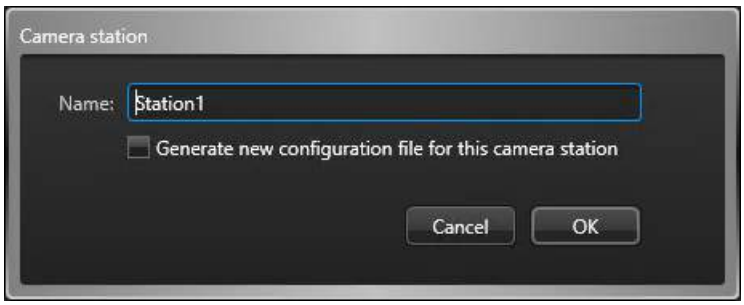
Solução 1

Regenerar um arquivo de configuração de estação de câmera.

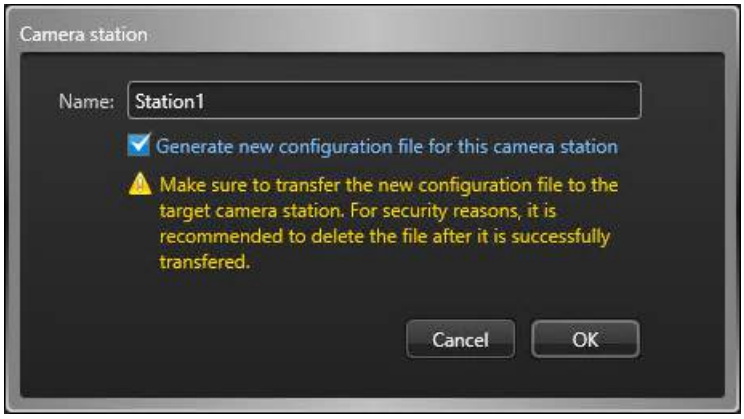
NOTA: Regenerar um arquivo é tipicamente usado quando o arquivo está obsoleto ou quando há suspeita que o arquivo esteja comprometido. Regenerar o arquivo de configuração torna todas as instâncias anteriores do arquivo inutilizáveis.

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*, selecione a função Body-Worn Camera Manager e clique na aba **Hardware**.

2 Na seção *Estações de câmera*, selecione a estação de câmera e clique em **Editar o item** ( ).



3 Selecione **Gerar novo arquivo de configuração para esta estação de câmera** e clique em **OK**.



4 Transfira o novo arquivo de configuração *.json* para a estação de câmera ou o Genetec Clearance™ Uploader.

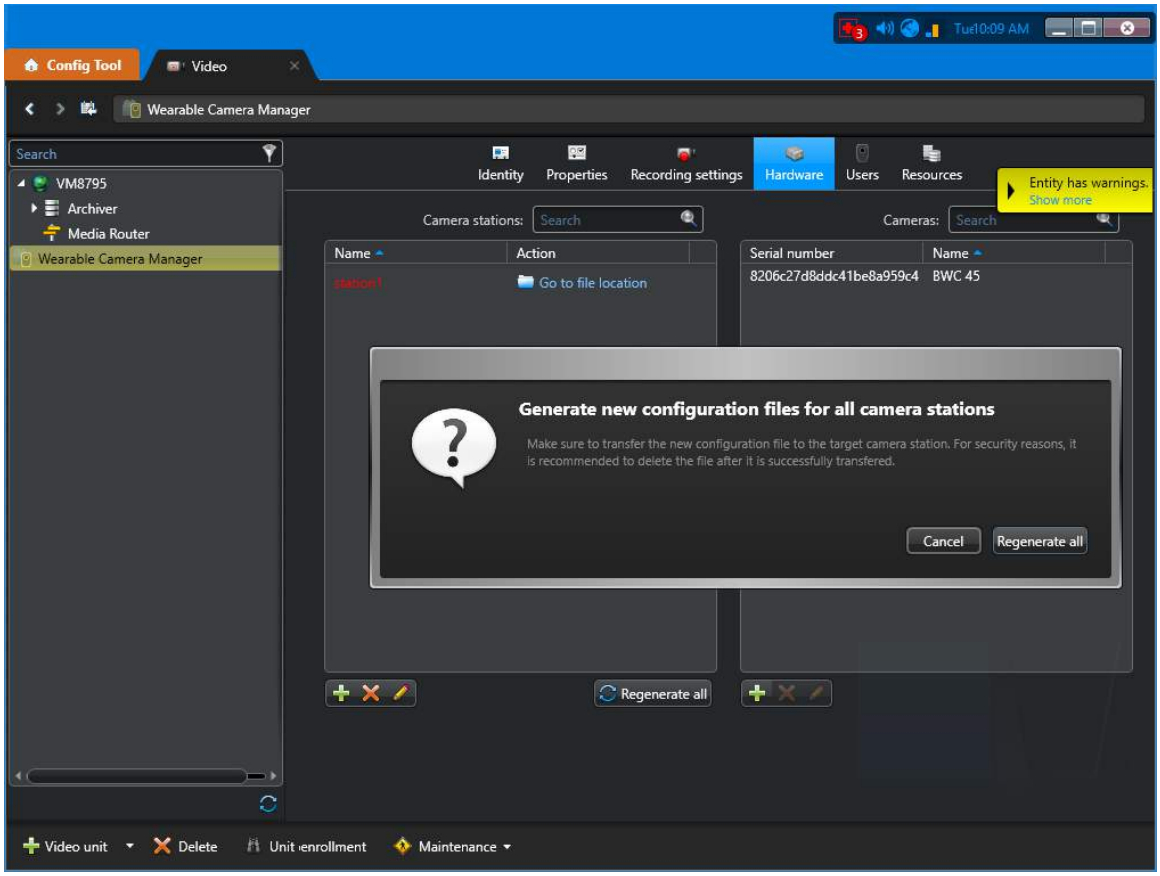
IMPORTANTE: Por motivos de segurança, certifique-se de excluir o arquivo de configuração original da respectiva localização original após tê-lo transferido com sucesso. Por exemplo, *C:\Users\username\AppData\Local\Temp\Genetec*.

Solução 2

Regenerar todos os arquivos de configuração de estação de câmera.

NOTA: Regenerar tudo é tipicamente usado quando o endereço IP, porta ou certificado da função Body-Worn Camera Manager é alterado. Isto assegura que todas as estações de câmera conseguem comunicar com a função.

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*, selecione a função Body-Worn Camera Manager e clique na aba **Hardware**.
2 Na seção *Estações de câmera*, clique em **Regenerar tudo** ( ).
3 Na caixa de diálogo de confirmação que abrir, clique em **Regenerar tudo**.



4 Transfira todos os novos arquivos de configuração *.json* para as estações de câmera relevantes ou o Genetec Clearance™ Uploader.

IMPORTANTE: Por motivos de segurança, certifique-se de excluir o arquivo de configuração original da respectiva localização original após tê-lo transferido com sucesso. Por exemplo, *C:\Users\username\AppData\Local\Temp\Genetec*.

Tópicos relacionados

Configurar câmeras usadas junto ao corpo na página 515
Adicionar câmeras ou usuários à função Body-Worn Camera Manager na página 517

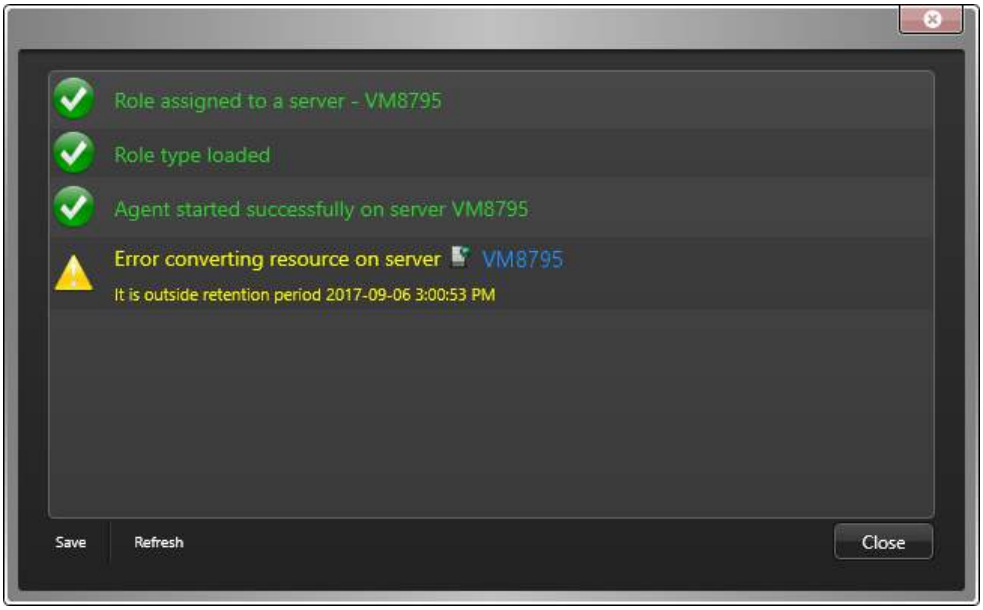
Avisos de conversão para câmeras usadas junto ao corpo

Os avisos de conversão são exibidos quando arquivos de evidência não podem ser importados ou baixados.

NOTA: Todos esses avisos de conversão desaparecem após 2 minutos.

Fora do período de retenção

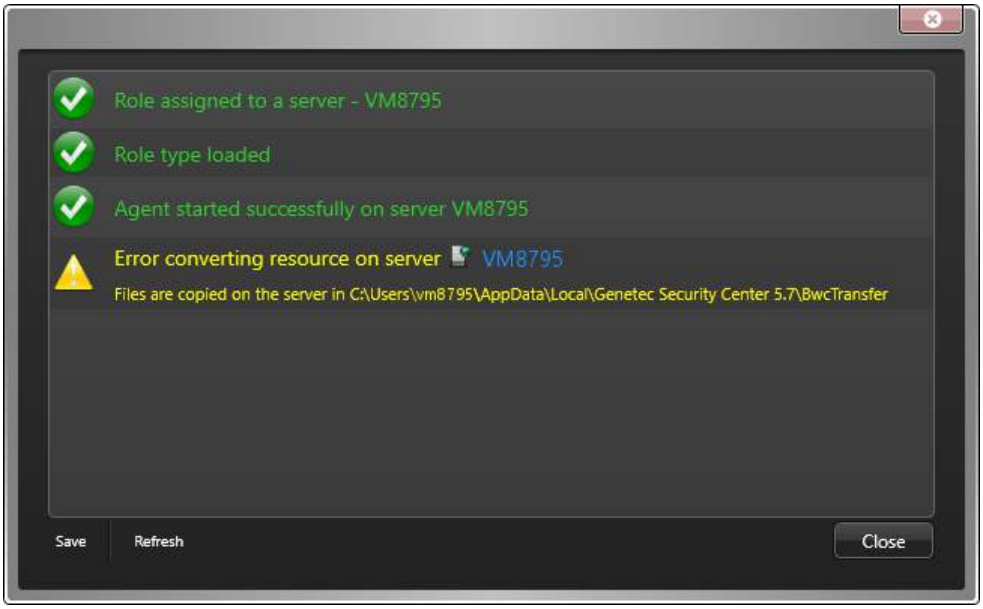
Causa: O usuário da câmera usada junto ao corpo, a função Archiver ou a função Body-Worn Camera Manager estão definidos para apenas conservar arquivos durante um período de retenção específico, mas o Genetec Clearance™ Uploader tentou importar um arquivo fora desse período.



Solução: Para importar arquivos mais antigos, o período de retenção deve ser prolongado ou a opção **Limpeza automática** deve ser desativada. Isto pode ser feito no Config Tool, na página *Configurações padrão da câmera* do Archiver, na página *Configurações de gravação* do Body-Worn Camera Manager ou da página *Gravação* do usuário da câmera usada junto ao corpo.

Erro ao converter recursos

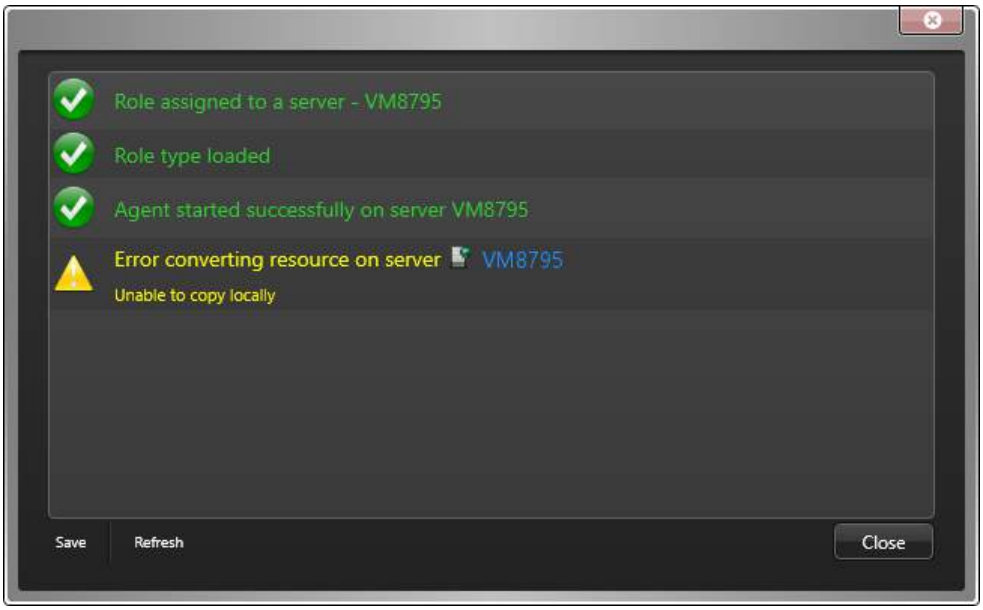
Causa: O arquivo baixado não pode ser convertido porque o seu formato não é suportado. O arquivo baixado foi copiado para a localização de servidor especificada na mensagem de aviso.



Solução: Acesso os arquivos manualmente na localização especificada na mensagem de aviso.

Não é possível copiar localmente

Causa: Ocorreu um erro de conversão e o arquivo baixado não pode ser copiado para a localização de servidor especificada na mensagem de aviso.



Solução: Verifique o disco local para garantir que tem espaço de armazenamento suficiente.

NOTA: É necessária intervenção manual para recuperar o arquivo e você deve entrar em contato com a Central de Assistência Técnica da Genetec™.

Failover está configurado no Archiver para câmeras usadas junto ao corpo

O failover não pode ser configurado na função Archiver quanto é usado por uma função Body-Worn Camera Manager.

Causa

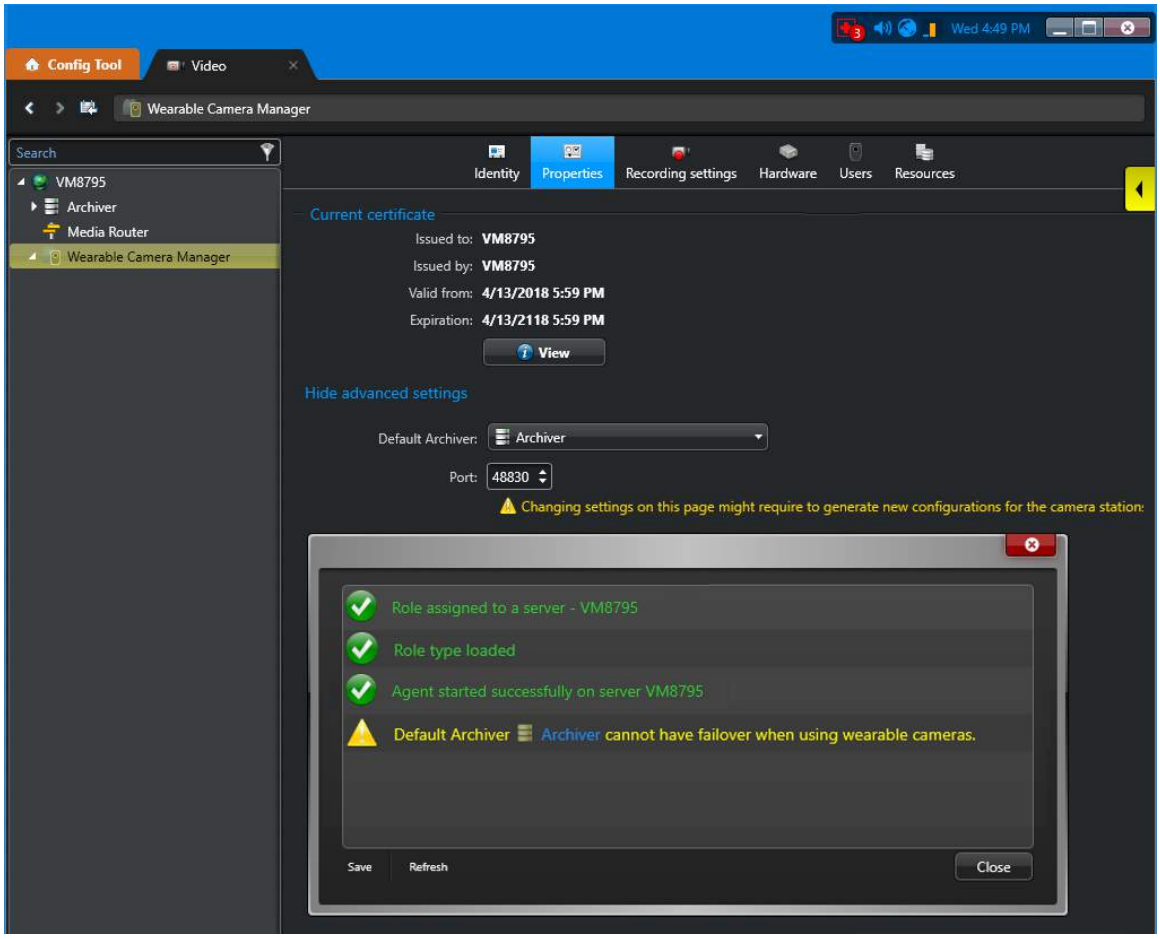
O failover e o arquivamento redundante não são suportados em funções Archiver usadas para câmaras usadas no corpo (ou usadas junto ao corpo).

Solução 1

Altere o Archiver padrão atribuído ao Body-Worn Camera Manager para um que não tenha failover configurado.

MELHOR PRÁTICA: Recomendamos usar um Archiver dedicado para câmeras usadas no corpo.

1 Na página inicial do Config Tool, abra a tarefa *Vídeo* e selecione a função Body-Worn Camera Manager.
2 Clique na aba **Propriedades** e, em seguida, clique na aba **Mostrar configurações avançadas**.



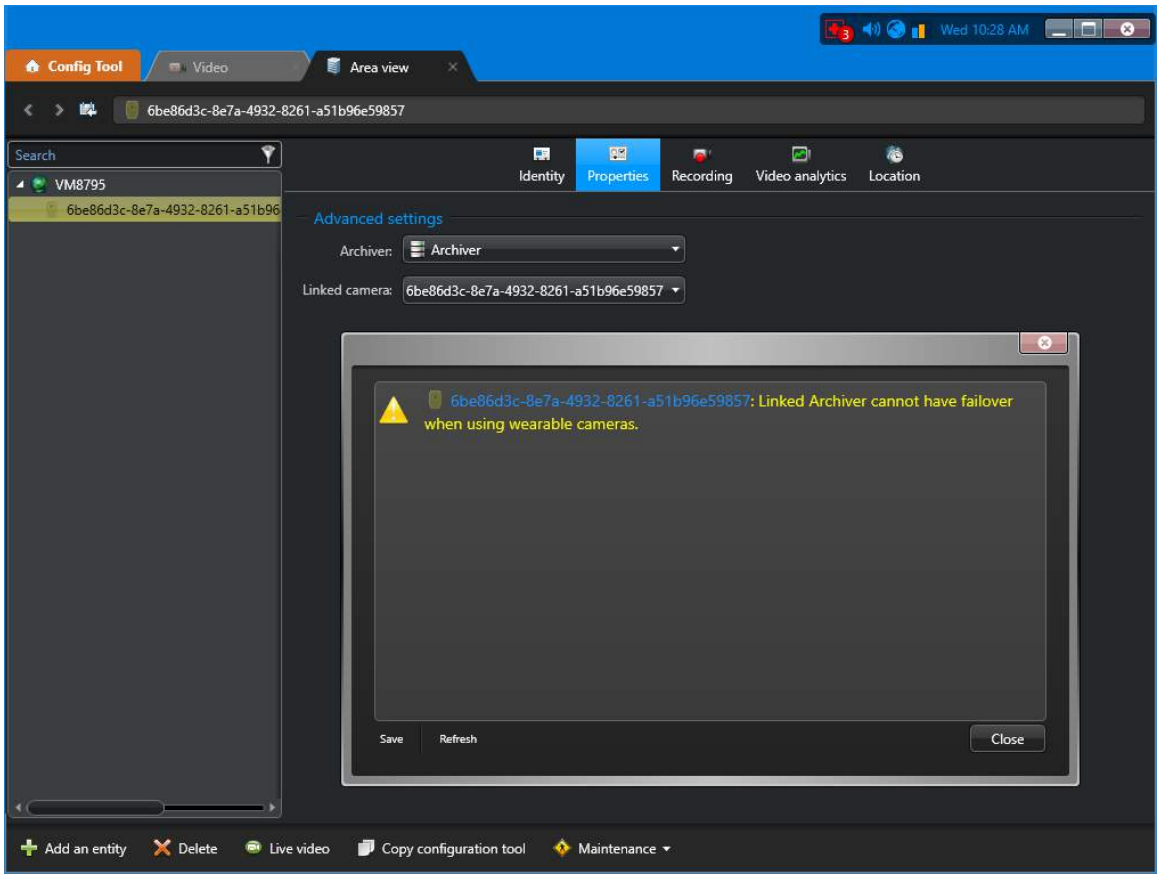
3 Na lista suspensa **Archiver padrão**, selecione um Archiver que não tenha failover configurado.
4 Selecione ou digite a porta necessária.
5 Clique em **Aplicar**.

IMPORTANTE: Você deve gerar novos arquivos de configuração para suas estações de câmera após alterar estas configurações. Consulte Erros de arquivos de configuração de câmeras usadas junto ao corpo na página 579.

Solução 2

Atribua um Archiver diferente ao usuário da câmera usada no corpo na tarefa *Exibição de área*.

1 No Config Tool, abra a tarefa *Exibição de área*.



2 Selecione um usuário de câmera usada no corpo ( ) e clique na aba **Propriedades**.

3 Em *Configurações avançadas*, selecione o **Archiver** e a **Câmera vinculada** nas respectivas listas suspensas.

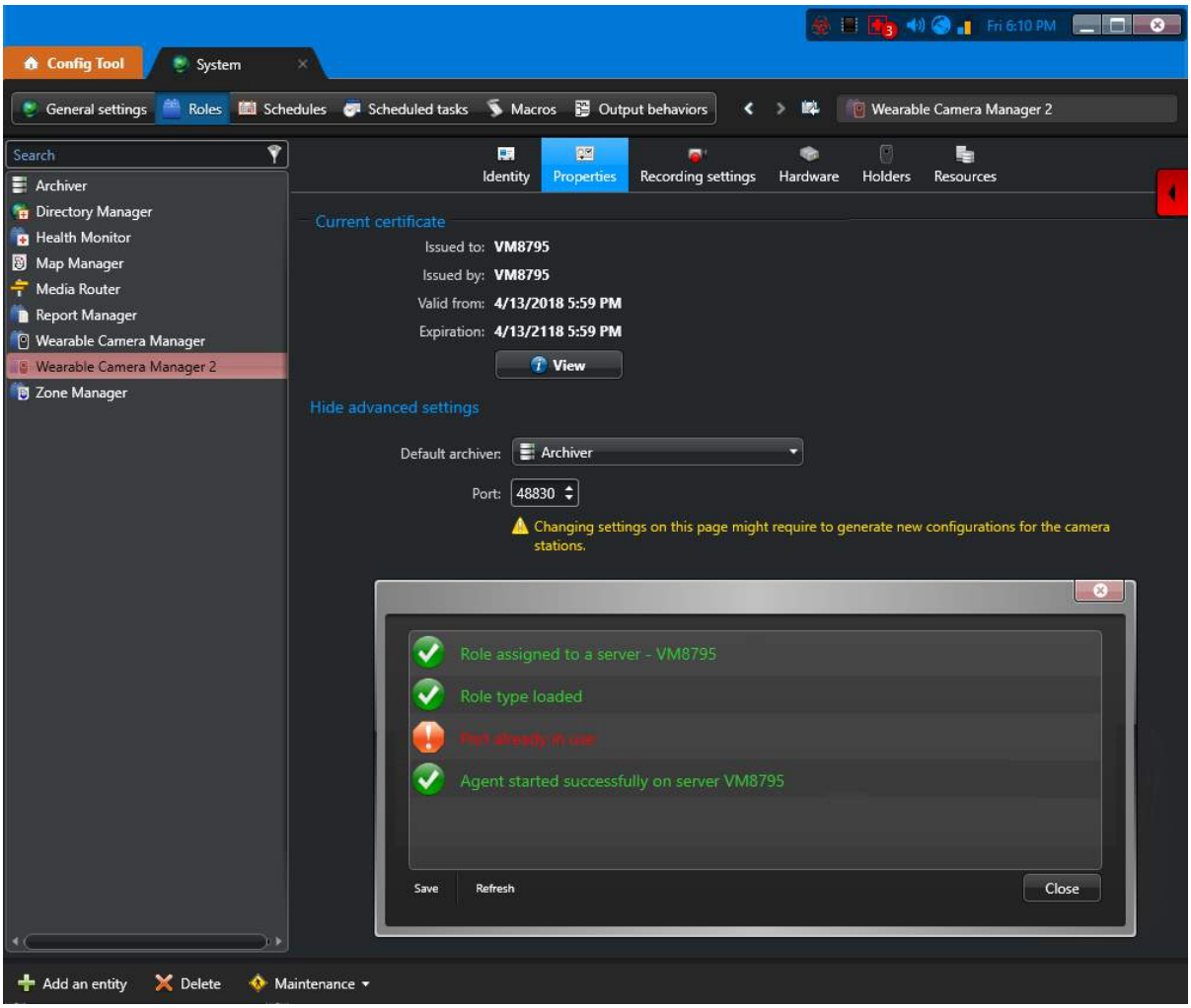
4 Clique em **Aplicar**.

A porta de câmera usada junto ao corpo já está em uso

A função Body-Worn Camera Manager está de momento offline porque a porta já está em uso Para resolver este problema, altere a porta especificada na função Body-Worn Camera Manager.

Causa

A função Body-Worn Camera Manager não consegue abrir uma conexão na porta especificada porque a porta já está em uso.



Solução

1 No Config Tool, abra a tarefa *Sistema* e selecione a tarefa Body-Worn Camera Manager.
2 Altere a porta especificada na aba **Propriedades** da tarefa Body-Worn Camera Manager.

IMPORTANTE: Você deve gerar novos arquivos de configuração para suas estações de câmera após alterar estas configurações. Consulte Erros de arquivos de configuração de câmeras usadas junto ao corpo na página 579.

O relatório Arquivos de câmera usada junto ao corpo está vazio

O relatório *Arquivos* no Security Desk está vazio. Isto acontece quando o tempo do processo de download ou carregamento expira.

Causa

Este problema pode ser provocado por um ou mais dos seguintes:

- Problemas de processamento de download ao copiar de câmera para localização de pasta de downloads.
- Problemas de processamento na conversão de arquivos G64.
- Conversões de arquivos G64 em andamento.
- O tempo de processamento do carregamento para o arquivo Security Center expira.

Solução

1 Nos registos de eventos do Genetec Clearance™ Uploader, verifique se os arquivos foram baixados.
2 No Security Desk, verifique se os arquivos baixados estão na pasta de arquivos.

   Por exemplo, *C:\VideoArchives\Archiver\0000166\2018-02-26*.
3 Se *.G64* for mencionado no caminho de arquivo da pasta de arquivos, aguarde alguns minutos.

   A função precisa de tempo para converter os arquivos para que o Archiver possa lê-los.
4 Se o Archiver continuar vazio ou não responder, faça o seguinte:

   a No Config Tool, desative e ative a função Body-Worn Camera Manager.
   b No Config Tool, desative e ative a função Archiver.
5 No Security Desk, gere novamente o relatório de Arquivos.

Controle de acesso

Esta parte inclui as seguintes chapters:

- "Controle de acesso em um relance" na página 589
- "Implantação do controle de acesso" na página 593
- "Unidades de controle de acesso" na página 602
- "Áreas, portas e elevadores" na página 613
- "Titulares de cartão" na página 645
- "Credenciais" na página 673
- "Gerenciamento global de titulares de cartão" na página 699
- "Ferramenta de importação" na página 713
- "Teste do sistema de controle de acesso" na página 727
- "Solução de problemas de controle de acesso" na página 740

28

Controle de acesso em um relance

Esta seção inclui os seguintes tópicos:

- "Sobre o Security Center Synergis" na página 590
- "Entidades relacionadas ao controle de acesso" na página 592

Sobre o Security Center Synergis™

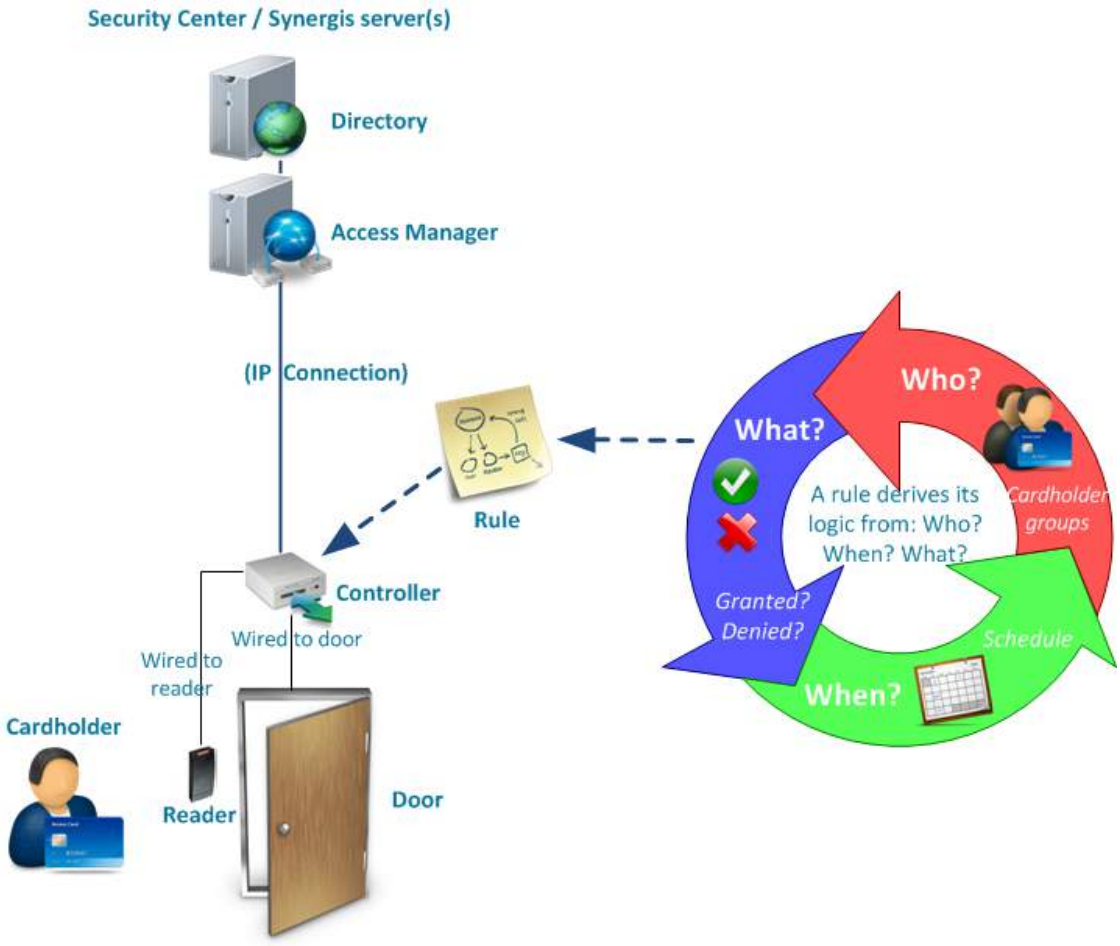
Security Center Synergis™ é o sistema de controle de acesso IP (ACS) que aumenta a segurança física da sua organização e a prontidão para responder a ameaças. Com um crescente portfólio de hardware de controle de portas e travas eletrônicas de terceiros, permite que você aproveite o seu investimento existente em rede e equipamentos de segurança.

O Synergis™ foi projetado com uma arquitetura aberta e distribuída. Você pode construir seu sistema com novos leitores de IP ou usar os que já tem. Integre seu sistema de controle de acesso com outros sistemas de terceiros, como gerenciamento de intrusão ou de edifícios e distribua componentes de servidor Synergis™ em muitas máquinas de rede diferentes para otimizar a largura de banda e a carga de trabalho.

O Synergis™ *Enterprise* suporta um número ilimitado de portas, controladores e estações de trabalho clientes. Você pode expandir seu sistema uma porta por vez ou dimensionar seu sistema em vários edifícios usando o recurso Federation™.

Como funciona o Synergis™

A arquitetura do Synergis™ é baseada na função de servidor conhecida como *Access Manager*, que controla os controladores de portas físicas.



Segue uma descrição geral de como a arquitetura do Synergis™ funciona:

- As configurações do sistema são salvas pela função Directory.
- O Directory envia a configuração ao Access Manager.

- O Access Manager se comunica diretamente com os controladores de portas físicas, chamados unidades de controle de acesso, por TCP/IP.
- O Access Manager encaminha horários, informações do titular do cartão e regras de acesso aos controladores das portas.
- Quando um titular de cartão apresenta sua credencial a um leitor, o controlador se refere à regra de acesso para determinar se o acesso deve ser concedido ou negado ao usuário.
- Uma vez que os controladores tenham sincronizado com o Access Manager, eles podem operar de forma autônoma, mesmo se perderem a conexão de rede com o Access Manager.

Com a configuração adicional, um titular de cartão pode pertencer a um grupo de titular de cartão, uma porta pode ser parte de uma área, e pode haver vários horários e regras enviadas para uma unidade.

Vantagens do Synergis™

Ao contrário de outros produtos ou soluções, o Synergis™ não usa "Códigos de autorização" ou "Níveis de acesso" para conceder ou negar acesso. Em vez disso, a lógica básica usada pelo Synergis™ para conceder ou negar acesso é definida pela *regra de acesso*.

A maior diferença entre uma abordagem de *regra de acesso* e uma abordagem de *nível de acesso* é que as regras de acesso são aplicadas aos pontos de acesso dos locais físicos que queremos proteger, enquanto os níveis de acesso são aplicados às pessoas. As regras de acesso especificam *quem* pode passar por uma porta e *quando* pode passar. Um nível de acesso define *onde* e *quando* uma pessoa pode obter acesso.

Uma regra de acesso contém os três Qs:

- Quem? (Quem pode passar — *titulares de cartão* ou *grupos de titulares de cartão*)
- Quê? (Se o acesso é concedido ou negado)
- Quando? (A *agenda* para quando a regra de acesso é aplicada)

Observe que o Synergis™ não concede acesso a um cartão ou a uma credencial. Em vez disso, o acesso é concedido ou negado com base nos próprios titulares. Esta mudança sutil, mas fundamental na lógica aplicada tem um benefício significativo na gestão de cartões perdidos e roubados. As regras de acesso que foram transmitidas para os *controladores de portas* não precisam ser modificadas. Se você associar uma nova credencial a um titular de cartão, a regra antiga ainda é válida.

Entidades relacionadas ao controle de acesso

O sistema de controle de acesso Synergis™ suporta muitas das entidades que estão disponíveis no Security Center.

Ícone	Entidade	Descrição
	**Access Manager (função)**	Função que gerencia os controladores de porta no sistema.
	**Unidade de controle de acesso**	Controlador de porta ao qual um leitor está ligado.
	**Porta**	Barreira física controlada por uma unidade de controle de acesso.
	**Elevador**	Uma única cabine de elevador.
	**Regra de acesso**	Lógica utilizada para determinar se deve ou não conceder acesso.
	**Área protegida**	Local físico cujo acesso é controlado por *regras de acesso* e outros comportamentos de controle de acesso, como anti-passback, intertravamento, regra de primeira pessoa, regra de duas pessoas e assim por diante.
	**Titular do cartão**	Pessoa que possui uma credencial.
	**Grupo de titulares de cartão**	Grupo de titulares de cartão que compartilham características em comum.
	**Credencial**	Reivindicação de identidade, como cartão, PIN, varredura biométrica, e assim por diante.
	**Modelo do crachá**	Modelo de impressão personalizado para as credenciais do usuário.
	**Agendamento**	Intervalo de data e hora.
	**Partição**	Grupo de entidades do sistema visíveis apenas para um grupo de usuários.
	**Usuário**	Indivíduo que usa aplicativos do Security Center.
	**Grupo de usuários**	Grupo de usuários que compartilham características em comum.

29

Implantação do controle de acesso

Esta seção inclui os seguintes tópicos:

- "Preparar a instalação do seu sistema de controle de acesso" na página 594
- "Implantar seu sistema de controle de acesso" na página 596
- "Implementar seu sistema de controle de acesso com vídeo" na página 597
- "Sobre o Access Manager" na página 598
- "Configurar funções do Access Manager" na página 599
- "Adicionar extensões de unidades de controle de acesso" na página 601

Preparar a instalação do seu sistema de controle de acesso

Para garantir que a instalação do seu controle de acesso aconteça sem problemas, você deve realizar uma série de passos de pré-configuração.

Antes de implementar seu sistema de controle de acesso:

1 Tenha um diagrama de rede mostrando todas as redes públicas e privadas usadas em sua organização e seus intervalos de endereço IP.

Para redes públicas, você também precisa do nome e do endereço IP público de seus servidores proxy. Consulte seu departamento de TI para obter essas informações.

2 Instale os seguintes componentes de software do Security Center:

a) Software do servidor Security Center em seu servidor principal.

O servidor principal é o computador que hospeda a função Directory.

b) (Opcional) Software do servidor Security Center em servidores de expansão.

Um servidor de expansão é qualquer outro servidor no sistema que não hospede a função Directory. Você pode adicionar servidores de expansão a qualquer momento.

c) Software de cliente Security Center em pelo menos uma estação de trabalho.

Para obter mais informações sobre a instalação do Security Center, consulte o *Guia de Instalação e Atualização do Security Center*.

3 Tenha uma lista de *partições* (se existirem).

As partições são usadas para organizar seu sistema em sistemas secundários gerenciáveis. Isso é especialmente importante em um ambiente de múltiplos locatários. Se, por exemplo, você estiver instalando um sistema de grande dimensão em um shopping center ou em uma torre de escritórios, você pode querer dar privilégios de administração local aos locatários. Usando partições, você pode agrupar os locatários de modo que eles somente possam ver e gerenciar o conteúdo de suas lojas ou escritórios, mas não os de outros.

4 Tenha uma lista de todos os usuários conhecidos com seus nomes e suas responsabilidades.

Para poupar tempo, identifique os usuários que têm as mesmas funções e responsabilidades e organize-os em grupos de usuários.

NOTA: Para instalações de grande dimensão, os usuários e grupos de usuários podem ser importados de um Active Directory do Windows.

5 Instale todas as *unidades de controle de acesso* (controladores de portas e leitores de borda) na rede IP da sua empresa e ligue-as a suas portas, coletando as seguintes informações:

- Fabricante, modelo e endereço IP de cada unidade.
- Fabricante e modelo dos *módulos de interface* conectados a cada unidade.
- Credenciais de login (nome de usuário e senha) para cada unidade.
- A quais *pontos de acesso* cada unidade/módulo de interface está conectado.
- As portas são *Card-in/Card-out* ou *Card-in/REX-out*?
- Quais entradas estão conectadas aos sensores de porta, REX e estações manuais?
- Que saídas estão conectadas a fechaduras de portas, sinais sonoros ou botões?

DICA: Um mapa ou uma planta do local, mostrando localizações de portas, elevadores, controladores e leitores seria útil.

6 Tenha uma lista de áreas protegidas com as respectivas portas de perímetro onde o acesso é controlado.

7 Tenha uma lista de todos os titulares de cartão conhecidos (e grupos de titulares de cartão, quando aplicável).

Titulares de cartão são pessoas que têm acesso físico ao local monitorado.

NOTA: Para instalações de grande dimensão, os titulares de cartão podem ser importados de um arquivo de texto ou de um Active Directory do Windows.

8 Tenha uma lista das credenciais disponíveis com seus códigos de instalação e números de cartão.

9 Tenha uma lista (e detalhes) de todas as agendas necessárias (horário de expediente, feriados e assim por diante).

10 Tenha uma lista (e detalhes) de todas as *regras de acesso* (*quem* é permitido *onde* e *quando*).

11 Se estiver integrando o Omnicast™, tenha uma lista indicando quais câmeras serão associadas a quais pontos de acesso (lados de portas e andares de elevadores).

NOTA: Uma câmera pode ser associada a mais de uma porta e vice-versa.

Implantar seu sistema de controle de acesso

Para integrar uma variedade de capacidades de controle de acesso e fornecer conectividade IP de ponta a ponta, você pode implantar seu sistema de controle de acesso assim que as etapas de pré-configuração forem concluídas.

Antes de iniciar

Execute as etapas de pré-configuração.

O que você deve saber

Um sistema Security Center pode ser implantado com apenas controle de acesso (Synergis™ sozinho) ou controle de acesso com integração de vídeo (Synergis™ com *Omnicast*™). Não importa se o vídeo ou o sistema de controle de acesso é configurado primeiro.

NOTA: Salvo especificação em contrário, você pode executar as seguintes etapas em qualquer ordem.

Para implantar seu sistema de controle de acesso:

1 Use a conta *Admin* no Config Tool para se conectar ao seu sistema.
2 Crie uma partição para cada grupo de entidades independente.
Definindo primeiro as partições, você não terá que mover entidades depois de criá-las.
3 Para organizar as entidades no seu sistema (áreas, portas e assim por diante, configure a exibição de área.
4 Configure as configurações transversais ao sistema para controle de acesso.
5 Configure as funções Access Manager.
6 Defina campos personalizados para as entidades do seu sistema.
7 Descubra e registre unidades de controle de acesso.
A função Access Manager precisa detectar os controladores de porta através da rede IP.
8 Configure as unidades de controle de acesso recém-registradas e os módulos de interface que estão ligados a elas.
9 Crie portas e configure a ligação de leitores, sensores, bloqueios e assim por diante às unidades de controle de acesso.
10 Crie elevadores e configure a ligação do leitor de cabine e botões de andares às unidades de controle de acesso.
11 Crie agendas, tais como horas abertas e fechadas, feriados e assim por diante.
12 Crie regras de acesso e vincule as regras a portas e agendas.
13 Transforme as áreas na exibição de área em áreas protegidas com regras de acesso, portas de perímetro e comportamentos avançados de controle de acesso.
14 Crie grupos de titulares de cartão e crie titulares de cartão e, em seguida, vincule-os às regras de acesso.
15 Crie modelos de crachás.
16 Crie credenciais.
17 Crie grupos de usuários e crie usuários.
18 Crie alarmes.
19 Crie níveis de ameaça.

Após terminar

Teste sua configuração.

Implementar seu sistema de controle de acesso com vídeo

Uma vez que seus sistemas Omnicast™ e Synergis™ estejam disponíveis, você poderá integrar os dois sistemas.

Antes de iniciar

Faça o seguinte:

- Configure seu sistema de controle de acesso.
- Configure seu sistema Omnicast™.

Para implementar seu sistema de controle de acesso com vídeo:

1 Se o *Archiver* do Omnicast™ e o *Access Manager* do Synergis™ se encontrarem no mesmo sistema Security Center, faça o seguinte:
   a) Conecte suas portas às câmeras Omnicast™.
   b) Conecte seus elevadores às câmeras Omnicast™.
2 Se o Archiver do Omnicast™ e o Access Manager do Synergis™ se encontrarem em sistemas independentes, faça o seguinte:
   a) Federe as câmeras Omnicast™ com seu sistema de controle de acesso.
   b) Conecte suas portas às câmeras Omnicast™.
   c) Conecte seus elevadores às câmeras Omnicast™.

Sobre o Access Manager

A função Gestor de Aceso gerencia e monitora as unidades de controle de acesso no sistema.

O Access Manager mantém as unidades atualizadas com as configurações de controle de acesso configuradas no Security Center, em tempo real ou em uma programação, para que possam tomar decisões independentes de controle de acesso, independentemente de estarem ou não conectadas ao Access Manager.

O Access Manager também registra os *eventos* de controle de acesso no banco de dados para investigação de controle de acesso e relatórios de manutenção. Todos os eventos gerados pelas unidades (acesso concedido, acesso negado, porta aberta etc.) são encaminhados pelo Access Manager, através do Directory, às partes envolvidas no sistema.

Múltiplas instâncias desta função podem ser criadas no sistema.

Configurar funções do Access Manager

Para monitorar as unidades, mantê-las sincronizadas com as configurações de controle de acesso no Security Center e permitir que elas tomem decisões de controle de acesso independentemente, você pode configurar um Access Manager para controlar as unidades.

O que você deve saber

Quando o Synergis™ está ativado em sua licença, uma função Access Manager é criada por padrão e hospedada no servidor principal.

Para configurar uma função do Access Manager:

1 Na página inicial do Config Tool, abra a tarefa *Controle de acesso* e clique na visualização **Funções e unidades**.

2 Selecione a função do Access Manager a ser configurada e clique na aba **Recursos**.

3 Se necessário, configure o banco de dados necessário para executar este Access Manager.

Caso você planeje configurar o failover do Access Manager, consulte Configurar failover de função na página 165.

4 Clique em **Propriedades** e defina as configurações gerais do Access Manager.

- **Manutenção de eventos:** Especifique quanto tempo você deseja manter os eventos no banco de dados do Access Manager antes de serem excluídos. O evento de controle de acesso é usado para relatórios e fins de manutenção (inclui eventos relacionados a portas, elevadores, áreas e outras entidades do controle de acesso).
  - **Indefinidamente:** Manter os eventos até que sejam excluídos manualmente.
  - **Por:** Selecione o número de dias para o período de retenção.

  CUIDADO: Se estiver usando o mecanismo de banco de dados *SQL Server 2014 Express* (incluído com os arquivos de instalação do Security Center), o tamanho do banco de dados será limitado a 10 GB. Um evento de porta usa (em média) 200 bytes na base de dados. Se você configurar o Access Manager para manter eventos de porta indefinidamente, o banco de dados uma hora atingirá o limite de 10 GB e o mecanismo parará.
- **Ativar ponto a ponto:** Selecione esta opção para ativar a comunicação entre as unidades Synergis™ gerenciadas por este Access Manager.

  MELHOR PRÁTICA: Somente ative a comunicação ponto a ponto se você planejar criar zonas de E/S que envolvam várias unidades Synergis™ ou aplicar antirretorno a áreas controladas por múltiplas unidades Synergis™. Deixe essa opção desmarcada para melhor segurança e desempenho do sistema.
- **Ativar antirretorno global:** Selecione esta opção se precisar aplicar o antirretorno a áreas controladas por várias unidades Synergis™. Para ativar esta opção, primeiro você deve ativar o ponto a ponto.

  MELHOR PRÁTICA: Se todas as áreas antirretorno são controladas por uma única unidade, não habilite o antirretorno global. Habilitar o antirretorno global aumenta a comunicação entre as unidades Synergis™.

5 Se necessário, adicione as extensões dos tipos de unidade de controle de acesso que você deseja que este Access Manager gerencie.

6 Adicione as unidades de controle de acesso que você deseja que este Access Manager controle.

Após terminar

Se você precisar de mais de uma função do Access Manager em seu sistema, você pode criar funções adicionais e hospedá-las em servidores separados.

Tópicos relacionados

Sobre o Access Manager na página 598

Criar zonas de E/S na página 950
Aplicar anti-passback a áreas na página 633

Adicionar extensões de unidades de controle de acesso

Para que o Access Manager se comunique com unidades de controle de acesso, você deve adicionar as extensões específicas do fabricante.

O que você deve saber

A partir do Security Center 5.3, as extensões são adicionadas por padrão quando o Access Manager é criado. Portanto, você só precisa adicionar as extensões manualmente se o Access Manager tiver sido criado antes da versão 5.3. Porém, a extensão Genetec™ Synergis™ exigida pelas unidades Synergis™ é criada com a porta de descoberta padrão, 2000. Se você configurou suas unidades Synergis™ com um número de porta diferente, você deve também alterá-la ou adicioná-la no Access Manager.

MELHOR PRÁTICA: Se você tiver duas ou mais funções Access Manager controlando unidades Synergis™ na mesma sub-rede, certifique-se de elas usarem portas de descoberta diferentes. Caso contrário, podem ocorrer problemas de desempenho com suas unidades Synergis™.

Para adicionar uma extensão ao Access Manager:

1 Abra a tarefa *Controle de acesso* e clique na visualização **Funções e unidades**.

2 Selecione a função Access Manager e clique na aba **Extensões**.

3 No fim da lista de extensões, clique em **Adicionar um item** ( ).

4 Na caixa de diálogo *Adicionar extensões*, selecione os tipos de extensão de que precisa e clique em **Adicionar.**

NOTA: Se você tiver selecionado apenas **HID VertX**, o procedimento termina aqui.

5 Selecione a extensão Genetec™ Synergis™ adicionada.

6 Para adicionar uma porta de descoberta, clique em **Adicionar um item** ( ) na parte inferior da seção *Portas de descoberta*.

7 Na caixa de diálogo *Porta de descoberta*, digite o número da porta configurada para suas unidades Synergis™ e clique em **Criar**.

O número da porta deve corresponder à porta de descoberta configurada em suas unidades Synergis™. O valor padrão é 2000.

8 Clique em **Aplicar.**

Tópicos relacionados

Abas de configuração do Access Manager na página 1043

30

Unidades de controle de acesso

Esta seção inclui os seguintes tópicos:

- "Sobre unidades de controle de acesso" na página 603
- "Sobre a sincronização de unidades" na página 604
- "Como as unidades de controle de acesso funcionam" na página 605
- "Preparar a adição de unidades de controle de acesso HID" na página 606
- "Adicionar unidades de controle de acesso" na página 608
- "Definir configurações da unidade de controle de acesso" na página 609
- "Habilitar a supervisão de leitores no HID VertX" na página 611
- "Ativar dispositivos de controle de acesso externos" na página 612

Sobre unidades de controle de acesso

É um tipo de entidade que representa um dispositivo de controle de acesso inteligente, como um aparelho Synergis™ ou um controlador de rede HID, que se comunica diretamente com o Access Manager por uma rede IP. Uma unidade de controle de acesso opera de modo autônomo quando está desconectada do Access Manager.

Tipos suportados de unidades de controle de acesso

O Security Center suporta os seguintes tipos de unidades de controle de acesso:

- **Aparelhos Synergis™:** Um aparelho Synergis ™ é um aparelho de segurança preparado para IP fabricado pela Genetec Inc., que é dedicado a funções de controle de acesso. Todos os aparelhos Synergis™ são fornecidos pré-instalados com Synergis™ Softwire e podem ser inscritos como unidades de controle de acesso no Security Center.

  Existem duas gerações de aparelhos Synergis™:

  - Synergis™ Cloud Link (segunda geração)
  - Synergis™ Master Controller (primeira geração)

  Todos os aparelhos Synergis™ suportam uma variedade de módulos de interface de terceiros por IP e RS-485. Para obter uma lista completa de módulos de interface suportados e limitações, consulte *Notes de Versão do Synergis™ Softwire* e *Guias de Integração do Synergis™ Softwire*.
- **Controladores de rede HID:** Os controladores de rede HID incluem os controladores VertX EVO (V1000, V2000), Edge EVO e os controladores VertX e Edge legados. Controladores HID são dispositivos IP inteligentes que podem adquirir seu endereço de rede automaticamente quando sua rede tem um servidor DHCP (o padrão). Eles também podem ser configurados com endereços estáticos (recomendado).

Em outras palavras, os aparelhos Synergis™ também são chamados de *unidades Synergis™* e os controladores de rede HID são chamados de *unidades HID*.

Sobre módulos de interface

Uma unidade de controle de acesso normalmente controla sub-painéis, como sub-painéis da série VertX HID e sub-painéis da série Mercury MR, que por sua vez se conectam a sensores de porta e leitores. No caso dos aparelhos Synergis™, a unidade também é capaz de gerenciar outros dispositivos inteligentes, como fechaduras inteligentes e outros controladores.

No Security Center, todos os dispositivos diretamente conectados à unidade de controle de acesso são chamados de módulos de interface, daí a seguinte definição:

Um módulo da interface é um dispositivo de segurança que se comunica com uma unidade de controle de acesso por IP ou RS-485 e oferece conexões de entrada, saída e leitor à unidade.

Tópicos relacionados

Recursos e modelos de HID suportados pelo Security Center na página 1163
Sobre a sincronização de unidades na página 604
Como as unidades de controle de acesso funcionam na página 605
Aplicar anti-passback a áreas na página 633

Sobre a sincronização de unidades

A sincronização de unidades é o processo de baixar as configurações mais recentes do Security Center para uma unidade de controle de acesso. Essas configurações, como regras de acesso, titulares de cartão, credenciais, agendamentos de desbloqueio, etc. são necessárias para que a unidade possa tomar decisões autônomas e precisas na ausência do Access Manager.

Uma unidade é sincronizada pela primeira vez quando você a inscreve no seu sistema. O Gestor de Acesso através do qual a unidade é registrada automaticamente cuida desse processo. Somente as configurações necessárias para que a unidade tome decisões autônomas são baixadas. Ao sincronizar uma unidade, o Gestor de Acesso sabe quanta memória a unidade tem e a preenche com tanta informação como ela pode manipular.

As funções do Gestor de Acesso sincronizam automaticamente as unidades atribuídas a ele quando uma alteração é feita no Security Center. Para unidades HID, você pode configurar a sincronização para ocorrer periodicamente, ou somente a pedido.

Você pode solicitar uma sincronização manual a qualquer momento se você suspeitar que uma unidade não está perfeitamente em sincronia com o sistema, acessando a aba **Sincronização** no Config Tool e clicando em **Sincronizar agora**.

Enquanto a unidade está a sincronizar, o ícone de sincronização ( ) aparece sobre a unidade e as entidades que controla, como portas, elevadores e zonas.

IMPORTANTE: Todos os erros de sincronização são exibidos em amarelo. Preste atenção a esses erros para evitar qualquer interrupção na operação. Por exemplo, as unidades HID VertX estão limitadas a 65.000 credenciais. Exceder esse limite faz com que a sincronização falhe e a unidade seja reinicializada.

Tópicos relacionados

Sobre unidades de controle de acesso na página 603
Como as unidades de controle de acesso funcionam na página 605
Unidade de controle de acesso - HID - Aba Sincronização na página 969
Unidade de controle de acesso - Synergis – Aba Sincronização na página 976

Como as unidades de controle de acesso funcionam

Todas as unidades de controle de acesso tomam decisões autônomas por padrão, dependendo das configurações de controle de acesso baixadas do Security Center durante a sincronização da unidade. A unidade só retorna ao Access Manager quando ela se defronta com uma credencial desconhecida.

Operação online

A unidade de controle de acesso está operando online quando ela está conectada ao seu Access Manager. A unidade toma decisões por conta própria, com base nas configurações de controle de acesso (regras de acesso, titulares de cartão, credenciais, horários de desbloqueio e assim por diante) baixadas do Security Center quando foi sincronizada pela última vez.

Quando as configurações de controle de acesso são alteradas no sistema, o Access Manager atualiza automaticamente as unidades que são afetadas pela alteração, a cada 15 segundos. Para unidades HID, você também tem a opção de configurar a sincronização para ser realizada diariamente, semanalmente ou sob demanda. Quando uma credencial desconhecida é apresentada, a unidade consulta imediatamente seu Access Manager para realizar a decisão correta e, portanto, atualiza sua memória ao mesmo tempo.

Enquanto a unidade permanecer conectada ao seu Access Manager, ela relata todas as decisões que tomar (*Acesso concedido* e *Acesso negado*) e todas as atividades (*Porta aberta*, *Porta fechada*, *Entrada detectada* e assim por diante) em tempo real para o Access Manager. O Access Manager pode substituir uma decisão de negar acesso se contradizer as configurações atuais no Security Center.

Modo de servidor

O modo de servidor é um modo de operação especial restrito a unidades Synergis™, onde a unidade permite o acesso ao Access Manager (o servidor) para tomar todas as decisões de controle de acesso. A unidade deve permanecer conectada ao Access Manager a todo momento para operar nesse modo.

NOTA: Não habilite este modo a menos que seja instruído por um de nossos representantes. Quando a unidade opera no modo servidor, certos recursos de controle de acesso não são mais suportados.

Operação offline

Diz-se que a unidade de controle de acesso opera offline quando a conexão com seu Access Manager é perdida. Quando estiver operando offline, a unidade aparece em vermelho no Config Tool e no Security Desk.

Embora esteja offline, a unidade continua a tomar decisões de controle de acesso com base nas informações baixadas anteriormente pelo Access Manager durante a sincronização. A diferença é que o Access Manager não é mais capaz de anular quaisquer decisões de negação nem atualizar a unidade quando as configurações são alteradas no Security Center. Todas as atividades são registradas localmente na unidade e são enviadas para o Security Desk quando a conexão com o Access Manager é restabelecida.

Tópicos relacionados

Sobre unidades de controle de acesso na página 603
Sobre a sincronização de unidades na página 604

Preparar a adição de unidades de controle de acesso HID

Antes de poder adicionar uma unidade HID no Security Center, você deve saber seu endereço IP e credenciais de login. Para encontrar estas informações, você pode usar a ferramenta *Registro de unidades*.

O que você deve saber

Os dispositivos HID VertX (V1000, V2000) e Edge são dispositivos IP que podem adquirir seu endereço de rede automaticamente quando sua rede possui um *servidor DHCP*. Se nenhum servidor DHCP estiver presente na rede, você deve atribuir uma configuração de IP estático à unidade (recomendado).

Para alterar a configuração de IP inicial da unidade, se necessário, você pode usar a *GUI de Descoberta HID*. Para obter mais informações sobre a *GUI de Descoberta HID*, consulte sua documentação de HID.

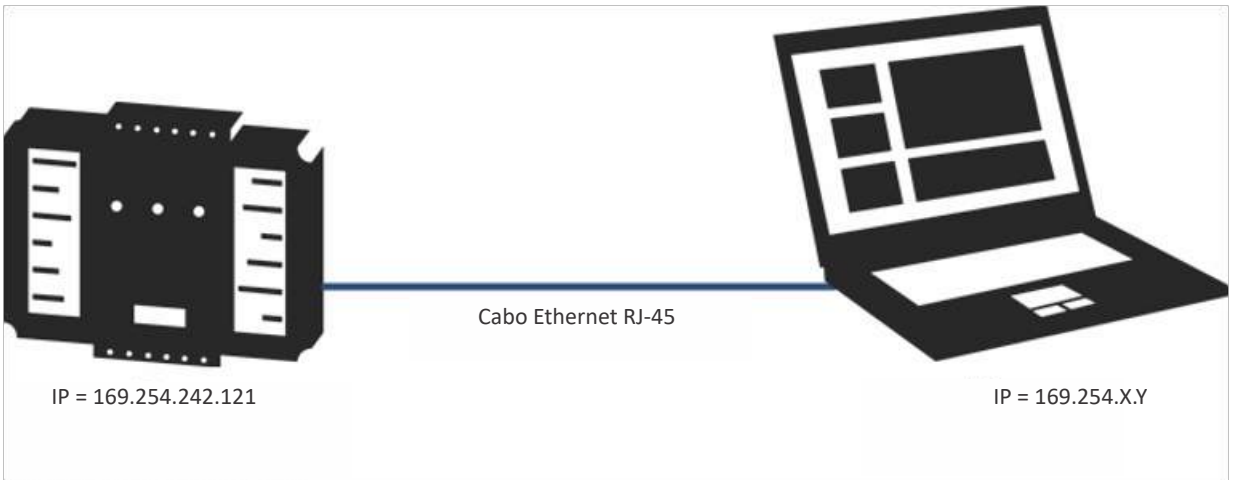
Para obter mais informações sobre a configuração inicial de hardware HID, consulte a documentação do dispositivo HID na pasta *Documentation\Controllers* do pacote de instalação do Security Center ou baixe a documentação de http://www.HIDglobal.com.

Para preparar a adição de uma unidade HID no Security Center:

1 Descubra as unidades de controle de acesso em sua rede.

2 Se a unidade HID que você deseja não for encontrada, desconecte o cabo de rede da estação de trabalho e conecte-o diretamente à unidade HID. Para unidades PoE, como Edge ou Edge EVO, conecte o laptop e a unidade a um comutador autônomo.

O endereço 169.254.242.121 é o endereço predefinido de fábrica para todos os dispositivos HID. Mesmo que a unidade tenha sido definida com uma configuração de IP, ela ainda escuta neste endereço para possíveis necessidades de solução de problemas.



3 Digite *http://169.254.242.121* em seu navegador.

4 Para fazer logon, insira o nome de usuário padrão (root) e a senha (pass).

NOTA: A interface Web para unidades EVO só pode ser acessada com a conta *admin*. Por padrão, a senha fica está em branco. Altere-a depois de alterar as configurações de IP. Para registrar a unidade no Security Center, você deve usar root/pass.

5 Na página **Configuração básica**, atribua a configuração de IP do dispositivo.

CUIDADO: Se nenhum servidor DNS estiver presente na sua rede, você deve usar o *endereço IP* da própria unidade como valor de **Servidor DNS primário**, e o endereço IP da **Estação Central Básica** deve ser definido para o endereço IP do servidor do Security Center que está executando a função *Access Manager*.

6 (Opcional) Clique em **Alterar senha de login** e altere a senha.

A alteração da senha se aplica ao usuário *admin*, não ao usuário *root*.

7 Clique em **Enviar**.

A nova configuração de IP é aplicada à unidade e ela é reiniciada. Agora você pode adicionar a unidade no Security Center.

Adicionar unidades de controle de acesso

Para controlar o acesso no seu sistema e monitorar eventos relacionados ao controle de acesso no Security Center, você deve adicionar unidades de controle de acesso a um Access Manager.

Antes de iniciar

Adicione as extensões de unidades de controle de acesso.

As unidades HID que você pretende adicionar devem estar online, e você deve saber seus endereços IP e credenciais de login (nome de usuário e senha).

O que você deve saber

Esta seção cobre apenas a inclusão de unidades HID. Para obter informações sobre como adicionar unidades Synergis™, consulte o *Guia de Configuração de Aparelhos Synergis™*.

Para adicionar uma unidade HID:

1 Abra a tarefa *Controle de acesso* e clique na visualização **Funções e unidades**.

2 Clique em **Adicionar uma entidade** () e selecione **Unidade de controle de acesso**.

3 Na lista suspensa **Endpoint de rede**, na aba **Informações da unidade**, selecione o Access Manager que gerenciará a unidade.

4 Clique em **Tipo da unidade** e selecione **HID VertX**.

Se o tipo de unidade estiver acinzentado, a extensão não foi adicionada no Access Manager.

5 Digite o endereço IP da unidade HID.

6 Ative a opção **Modo seguro** (padrão=ativado).

Ativar o modo seguro desativa os protocolos não seguros de FTP e Telnet. Ele também deixa a conexão entre o Access Manager e unidades HID menos suscetível a problemas de rede. Certifique-se de que a unidade HID atenda ao firmware mínimo suportado nessa página. Caso contrário, a inscrição falhará.

7 Digite seu **Nome do usuário** e **Senha**.

NOTA: Se o modo seguro estiver ativado, você deve fornecer a senha de *admin*. Se o modo seguro não estiver ativado, você deve fornecer a senha de *root* (padrão=pass).

8 Se houver um roteador NAT entre a unidade e o Access Manager, selecione **Usar endereço de host traduzido** e especifique o endereço IP do roteador NAT que é visível a partir da unidade.

9 Clique em **Próximo**.

10 Revise o *Resumo de criação* e clique em **Criar**.

O Access Manager tenta se conectar à unidade e inscrevê-la em seu sistema. Quando o processo for concluído com êxito, uma mensagem de confirmação será exibida.

11 Clique em **Fechar**.

A unidade de controle de acesso recém-adicionada aparece sob o Access Manager ao qual ela foi atribuída na visualização **Funções e unidades**.

NOTA: Poderá demorar alguns minutos até que a unidade possa ser utilizada, enquanto é submetida à sincronização automática. Esse processo envolve o Access Manager enviar agendamentos, regras de acesso e informações do titular do cartão para a unidade. A unidade salva as informações localmente para que possa funcionar mesmo se o Access Manager não estiver disponível.

12 Confirme que a unidade foi sincronizada com êxito com o Access Manager:

a) Na visualização **Funções e unidades**, selecione a unidade de controle de acesso que acabou de ser adicionada.

b) Clique na aba **Sincronização** e verifique a data e hora da **Última atualização**.

Definir configurações da unidade de controle de acesso

Para um desempenho ideal, configure as unidades de controle de acesso após terem sido adicionadas ao Security Center.

O que você deve saber

O Security Center oferece configurações padrão; porém, é recomendado que você passe cuidadosamente pela configuração de cada entidade para obter os melhores resultados.

Unidades HID e Synergis™ têm capacidades diferentes, portanto, diferentes requisitos de configuração. Para obter informações sobre os requisitos de configuração das unidades Synergis™, consulte o *Guia de Configuração do Aparelho Synergis™*.

DICA: Para ganhar tempo configurando suas unidades de controle de acesso, você pode configurar uma delas e então copiar as configurações que elas têm em comum para o resto das unidades.

Para definir configurações de uma unidade de controle de acesso:

1 Abra a tarefa **Controle de acesso** e clique na visualização **Funções e unidades**.
2 Selecione a unidade de controle de acesso (HID ou Synergis™) para configurar e clique na aba **Propriedades**.
3 Na aba **Propriedades**, faça um dos seguintes:
- Configurar as propriedades da unidade HID.
- Configurar as propriedades da unidade Synergis™.

4 Configure a fiação das entidades controladas por esta unidade:
- Configure a fiação de portas.
- Configure a fiação de andares de elevadores.
- Configure a fiação de zonas de hardware.

5 Clique na aba **Periféricos** da unidade de controle de acesso.
Aqui é onde você configura as propriedades dos periféricos conectados à unidade, como o tipo de leitor e o tipo de contato de entrada. Valide a configuração da fiação e dê nomes significativos aos dispositivos, se necessário.
- Configure os periféricos acoplados à unidade HID.
- Configure os periféricos acoplados à unidade HID Synergis™.

6 (somente unidades HID) Selecione a aba **Sincronização** e escolha com que frequência deseja sincronizar a unidade:
- **Automaticamente:** Essa é a configuração recomendada.
  Qualquer alteração de configuração é enviada para a unidade de controle de acesso 15 segundos depois que a alteração é salva pelo Config Tool, Web Client ou Security Desk. Somente configurações que afetam aquela unidade específica são enviadas.
- **Diariamente:** A unidade é sincronizada diariamente, nas horas especificadas.
- **A cada:** A unidade é sincronizada semanalmente, no dia e horas especificadas.
- **Manual:** A unidade é sincronizada apenas quando você clica em **Sincronizar agora**.
  Certifique-se de sincronizar a unidade antes que a configuração expire.

7 Clique em **Aplicar**.

Tópicos relacionados

Habilitar a supervisão de leitores no HID VertX na página 611

Inscrição automática de unidades de controle de acesso

O registro automático acontece quando novas unidades IP em uma rede são descobertas automaticamente e adicionadas ao Security Center. A função que é responsável pelas unidades *transmite* uma solicitação de descoberta em uma porta específica e as unidades que escutam nessa porta respondem com uma mensagem que contém suas próprias informações de conexão. Em seguida, a função usa a informação para configurar a conexão à unidade e habilitar a comunicação.

A função Access Manager é capaz de descobrir automaticamente os aparelhos Synergis™ como unidades de controle de acesso quando as seguintes condições forem atendidas:

- O aparelho Synergis™ nunca foi conectado a nenhum Access Manager antes.
- O aparelho Synergis™ e o Access Manager usam a mesma porta de detecção.
- O aparelho Synergis™ e o Access Manager estão no mesmo segmento de rede.
- O aparelho Synergis™ está usando o nome de usuário e a senha padrão de logon (`admin`/`softwire`).

As unidades HID não suportam a detecção automática.

Quando a detecção automática não é suportada ou não funciona, use a *Ferramenta de registro de unidades* para localizar as unidades em sua rede e adicioná-las manualmente.

Redefinir o certificado confiável

Se o Access Manager não conseguir se conectar a uma unidade Synergis™ previamente registrada porque o certificado em que o Access Manager confia foi alterado, você pode redefini-lo no Config Tool para que o novo certificado possa ser aceito.

O que você deve saber

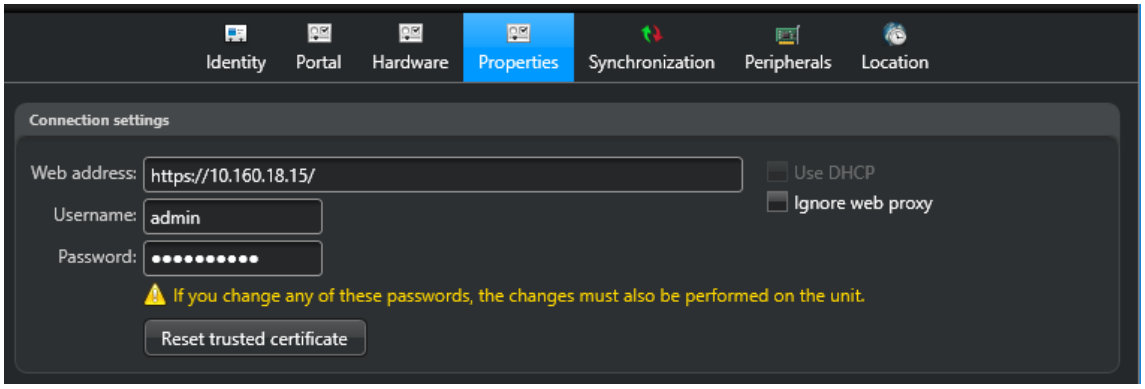
Existem dois casos legítimos em que a unidade poderá alterar seu certificado após ser registrada para o Access Manager:

- Quando você instala um certificado assinado por CA na unidade após ela ter sido registrada.
- Quando a unidade é um equipamento SV e você atualiza o software Security Center no equipamento. Um novo certificado poderá ser instalado porque o equipamento SV também atua com um servidor do Security Center.

Para redefinir um certificado de unidade confiado por um Access Manager:

1 Na página inicial do Config Tool, abra a tarefa *Controle de acesso* e clique na visualização **Funções e unidades**.

2 Selecione a unidade à qual o Access Manager não consegue se conectar (exibida em vermelho) e clique em **Propriedades**.



3 Clique em **Redefinir certificado confiável**.

Habilitar a supervisão de leitores no HID VertX

Para ser possível monitorar leitores entrando no estado offline ou portas controladas por unidades HID no Security Desk e no Config Tool, você deve habilitar a supervisão de leitores na unidade HID Config Tool e apresentar o cartão de configuração HID a cada leitor.

Antes de iniciar

Certifique-se de ter à sua disposição os cartões de configuração HID para leitores Wiegand. Por exemplo, para leitores iCLASS SE, os cartões de configuração seriam:

- SEC9X-CRD-0-043J para habilitar supervisão
- SEC9X-CRD-0-0000 para desabilitar supervisão

O que você deve saber

No Security Desk, você obtém o evento *Porta offline: O dispositivo está offline* em uma porta quando um dos leitores associados a essa porta entra em estado offline.

DICA: O evento *Porta offline: O dispositivo está offline* é acionado por desconexões de unidades e desconexões de leitores. Por isso, não é possível saber qual é qual a menos que você também monitore as unidades de controle de acesso. Se você tiver dois leitores em uma porta, você deve acessar Config Tool e verificar a página *Periféricos* para descobrir qual leitor está offline.

Limitation: Não existe um evento que indique quando o leitor passa a estar online novamente.

Para habilitar a supervisão de leitores em uma unidade HID VertX:

1 Na página inicial do Config Tool, abra a tarefa *Controle de acesso* e clique na visualização **Funções e unidades**.
2 Selecione a unidade HID a modificar e clique na aba **Propriedades**.
3 Na seção *Configurações gerais*, selecione **Supervisão de leitores**.
Todos os leitores conectados a essa unidade HID devem ser configurados para supervisão.
4 Defina o **Tempo limite** usado para detectar que um leitor está offline.
É recomendado que seja definido um valor de tempo limite pelo menos três vezes o tempo de rotação do sinal *Estou aqui* (padrão=10 segundos) configurado no leitor.
5 Clique em **Aplicar**.
6 Configure cada leitor físico para supervisão.
a) Reinicie o leitor.
b) No arranque, quando o LED do leitor estiver roxo, segure e apresente o cartão de configuração HID ao leitor até que o leitor pare de soar.
c) Repita o processo para cada leitor conectado à unidade HID.

Para desabilitar a supervisão de leitores em uma unidade HID VertX:

1 Na página *Propriedades* da unidade, desmarque **Supervisão de leitores** e clique em **Aplicar**.
2 Desabilite a supervisão em cada leitor físico apresentando o segundo cartão.

Ativar dispositivos de controle de acesso externos

Você pode ativar e desativar dispositivos de controle de acesso externos, como leitores USB, blocos de assinatura, scanners de cartão e assim por diante, na caixa de diálogo *Opções*.

O que você deve saber

Essas configurações são salvas localmente para o seu perfil de usuário do Windows. Para obter informações sobre os dispositivos de controle de acesso disponíveis, consulte a documentação do fabricante.

Para ativar ou desativar dispositivos de controle de acesso externos:

1 Na página inicial, clique em **Opções** > **Dispositivos externos**.
2 Ao lado de cada dispositivo externo, defina a opção como **ATIVO** ou **INATIVO**.
3 Clique em **Salvar**.
4 Reinicie o aplicativo.

Tópicos relacionados

Configurar estações de codificação de smart cards na página 663
Utilizar coletores de assinatura na página 670

31

Áreas, portas e elevadores

Esta seção inclui os seguintes tópicos:

- "Sobre portas" na página 614
- "Criar portas" na página 616
- "Mapear entidades de porta a ligações físicas de porta" na página 617
- "Selecionar quem tem acesso a portas" na página 619
- "Sobre elevadores" na página 620
- "Diferenças entre unidades HID e Synergis em controle de elevadores" na página 622
- "Criar elevadores" na página 624
- "Selecionar o comportamento do relé de saída para andares de elevadores" na página 625
- "Mapear a fiação de andares físicos de elevadores para entidades de elevador" na página 626
- "Selecionar quem tem acesso a elevadores" na página 628
- "Sobre áreas protegidas" na página 629
- "Configurar áreas protegidas" na página 631
- "Adicionar portas a áreas" na página 632
- "Aplicar anti-passback a áreas" na página 633
- "Definir limites de ocupação de área" na página 635
- "Intertravar portas dentro de áreas" na página 636
- "Fiscalizar uma presença de supervisão em áreas protegidas" na página 637
- "Exigir que os visitantes sejam escoltados para acessar áreas protegidas não ANSSI" na página 638
- "Configurar acompanhamento de visitantes para catracas conforme a ANSSI" na página 639
- "Habilitar PIN de dureza" na página 642
- "Sobre regras de acesso" na página 643
- "Criar regras de acesso" na página 644

Sobre portas

Uma entidade de porta representa uma barreira física. Frequentemente, é uma porta, mas também pode ser um portão, uma catraca ou qualquer outra barreira controlável. Toda porta tem dois lados, chamados de *Entrada* e *Saída* por padrão. Cada lado é um ponto de acesso (entrada ou saída) de uma área protegida.

Existem três configurações básicas de porta:

- Entrada de cartão/Saída de cartão - são necessários 2 *leitores*
- Entrada de cartão/Saída REX - é necessário 1 leitor
- Portas sem leitor - Não são necessários leitores

Portas sem leitores

Se um leitor não for necessário para uma configuração de porta, as E/S encontradas nos módulos de interface (como HID VertX V200 e V300) podem ser usadas para controlar o REX, sensor de porta e bloqueio. Não é necessário vincular quaisquer regras de acesso a uma porta sem leitor. No entanto, você ainda pode atribuir horários de desbloqueio para portas sem leitor.

Alguns exemplos de onde as portas sem leitor podem ser usadas podem incluir os seguintes:

- Saídas de incêndio - Bloqueadas de fora, com uma barra anti-pânico para abrir a porta do interior usando um REX.
- Estádios/Teatros/Arenas - Todo mundo deve entrar através da bilheteria, mas uma vez que o evento é concluído, muitas saídas são disponibilizadas para diminuir o congestionamento na entrada principal.

Fiação de portas

É recomendado ter um eletricista para verificar a funcionalidade entre todos os sensores de porta e atuadores.

Sinais sonoros de portas

Você pode atribuir uma saída da unidade de controle de acesso para soar um sinal sonoro na aba *Hardware*. O *Sinal sonoro* não se refere ao sinal do leitor, mas sim a um sinal sonoro externo que está conectado a um relé de saída na unidade de controle de acesso. A saída do sinal sonoro é acionada pelas *ações Alarme de som* e *Silenciar alarme*.

Sensores de entrada

Você pode configurar um sensor de entrada em cada lado de uma porta para aumentar a precisão de contagem de pessoas e a aplicação de regras de restrição de acesso avançadas em áreas, como anti-passback e regra de primeira pessoa. O sistema só pode gerar o evento *Entrada detectada* quando um sensor de entrada é acionado. Na ausência de um sensor de entrada, o sensor de porta é usado, e a entrada é assumida quando o sensor de porta é acionado. Se ambos os tipos de sensores estiverem ausentes, a entrada é assumida quando um acesso é concedido.

Regra de duas pessoas

Você pode proteger uma área com alto nível de proteção com a *regra de duas pessoas*. A regra de duas pessoas é a restrição de acesso aplicada a uma porta que exige que dois titulares de cartão (inclusive visitantes) apresentem as credenciais com um certo intervalo entre si para ganhar acesso.

NOTA: Um visitante que necessite de um host não pode ser contado como uma das duas pessoas na regra de duas pessoas.

DICA: Uma porta pode ser configurada no Security Center para proteger uma área física (uma divisão) sem necessariamente configurar uma área protegida se não houver outros tipos de restrições de acesso que precisam ser aplicadas.

Tópicos relacionados

Sobre áreas protegidas na página 629

Criar portas

Uma vez que a fiação física entre a unidade de controle de acesso e a porta está completa, você pode criar e configurar a porta no Config Tool.

Antes de iniciar

Conecte suas portas a unidades de controle de acesso.

Para criar uma porta:

1 Na página inicial do Config Tool, abra a tarefa *Exibição de área*.
2 Selecione a área onde você deseja adicionar a porta.
3 Clique em **Adicionar uma entidade** () > **Porta**.
4 No assistente **Criando uma porta**, digite o nome e descrição da porta.
5 Na lista suspensa **Localização**, selecione a área na qual a porta será criada e clique em **Próximo**.
6 Na página **Informações da porta**, atribua nomes aos lados da porta.
Exemplo: Dentro/Fora, Protegido/Não protegido, Entrada/Saída, Leste/Oeste.
7 Para associar a porta com a unidade de controle de acesso à qual ela está conectada:
a) Na lista suspensa **Unidade de controle de acesso**, selecione uma unidade.
b) Na lista suspensa **Módulo de interface**, selecione um módulo de interface.
c) Na lista suspensa **Tipo de porta**, selecione um tipo de porta.
8 Clique em **Próximo**.
9 Revise o *Resumo de criação* e clique em **Criar** > **Fechar.**
A nova porta aparece na *árvore de entidades* da visualização de área.
10 Selecione a porta e clique na aba **Propriedades**.
11 Configure o comportamento de controle de acesso geral da porta.
12 Clique em **Aplicar**.
13 Descreva a ligação física entre a unidade de controle de acesso e a porta no Security Center.
14 Selecione quem tem acesso à porta.

Após terminar

Conecte a porta às áreas que ela protege.

Tópicos relacionados
Sobre portas na página 614

Mapear entidades de porta a ligações físicas de porta

Para que sua entidade de porta seja funcional, você deve combinar as ligações de hardware que você fez com a porta (conexões de leitor, fechaduras de porta, sensores de porta, REX, sinais sonoros etc.) no Security Center, para que o Access Manager saiba como controlar a porta.

O que você deve saber

A maneira como você conecta a porta e atribui as interfaces de hardware afeta como a porta pode ser protegida e monitorada. Por exemplo, se a porta tiver um sensor de entrada, você pode monitorar eventos de *A porta forçada para abrir* e eventos de *Entrada detectada*. Se um lado da porta for configurado com um REX, a regra de acesso não pode ser aplicada a esse lado da porta.

IMPORTANTE: A configuração de hardware da porta deve corresponder às configurações de E/S definidas para a unidade de controle de acesso que controla a porta.

Para mapear a fiação física de uma porta para uma entidade de porta:

1 Na página inicial do Config Tool, abra a tarefa *Exibição de área*.
2 Selecione a entidade de porta a ser configurada e clique na aba **Hardware**.
3 Na lista suspensa **Unidade preferida**, selecione a unidade de controle de acesso que está conectada à porta.
4 Na seção Lado da porta (A), selecione o **Leitor**, **REX** e **Sensor de entrada** nas listas suspensas com base na ligação da porta.
5 Para alterar as definições do leitor da porta, clique em **Configurações do leitor** ( ).

   A caixa de diálogo *Configurações do leitor* permite configurar o seguinte:

   - **Tempo limite para digitação de PIN:** Isso configura apenas o tempo limite de digitação do PIN após o cartão ter sido lido. Por exemplo, por padrão (5 segundos), você tem 5 segundos para digitar todos os dígitos do PIN.
   - **Usar cartão e PIN:** Ajuste em **ATIVO** para alterar o modo do leitor para Cartão e PIN e selecione o **agendamento**ao qual esse modo se aplica. Quando não está em um período de tempo agendado, o leitor se comporta somente em modo de Cartão.

   NOTA: Certifique-se de que suas configurações correspondem às capacidades do seu leitor. O sistema não pode validar as capacidades do seu hardware. Você pode configurar esse tipo de leitor na aba **Periféricos** da unidade.

6 Repita as etapas para o lado (B) da porta.
7 Na seção *Conexões adicionais*, atribua as entradas e saídas para o sinal sonoro, fechadura e assim por diante.
8 Clique em **Aplicar**.
9 Conecte câmeras que exibem cada lado da porta à entidade de porta.

Exemplo

Se uma porta física tem o seguinte instalado, então a entidade de porta deve ter uma configuração Entrada de cartão/Saída REX no Config Tool:

- Um leitor ligado ao *lado da porta* A
- Um REX ligado ao lado da porta A
- Um relé de curso na fechadura
- Um sensor de porta
- Um relé auxiliar ligado a um sinal sonoro

Tópicos relacionados

Unidade de controle de acesso - HID - Aba Periféricos na página 970
Unidade de controle de acesso - Synergis - Aba Periféricos na página 977

Ligar câmeras a portas

Você pode ligar câmeras a entidades de porta, de modo que quando um evento de controle de acesso é acionado na porta (*porta forçada*, *acesso negado*), ele faz com que o vídeo da câmera seja exibido em um ladrilho de monitoramento do Security Desk e seja gravado.

Antes de iniciar

Para monitorar portas com câmeras, você deve ter uma das seguintes configurações do Security Center:

- Uma função Archiver com câmeras disponíveis.
- Uma função Omnicast™ Federation™ para conexão a um sistema Omnicast™ externo.
- Uma função Security Center Federation™ para conexão a um sistema Security Center externo com câmeras.

O que você deve saber

Se houver várias câmeras associadas a uma porta, por padrão, as câmeras ligadas ao lado (A) dessa porta são exibidas em um ladrilho do Security Desk. Várias câmeras associadas a uma única porta (entidades compostas) podem ser percorridas ou descompactadas no Security Desk.

Para ligar câmeras a uma porta:

1 Na página inicial do Config Tool, abra a tarefa *Exibição de área*.
2 Selecione a entidade de porta a ser configurada e clique na aba **Hardware**.
3 Na seção *Lado da porta (Dentro)*, clique em **Associar uma câmera** ( ).
4 Na lista suspensa **Câmera**, selecione uma câmera.

   Se a câmera tiver um motor PTZ, você também pode incluir o número PTZ predefinido para garantir que a câmera aponta para a porta.

5 Para adicionar outra câmera ao lado da porta, clique em **Associar uma câmera** ( ) novamente.
6 Repita as etapas para o *Lado da porta (Fora)*.
7 Clique em **Aplicar**.

Selecionar quem tem acesso a portas

Uma porta conectada a uma unidade de controle de acesso é bloqueada por padrão. Você pode definir agendas para quando o *acesso livre* (desbloqueado) através da porta é permitido e para quando o *acesso controlado* (credenciais devem ser apresentadas para desbloquear a porta) está em vigor, aplicando regras de acesso.

Antes de iniciar

- Descreva a ligação física entre a unidade de controle de acesso e a porta no Security Center.
- Crie as regras de acesso.

O que você deve saber

Se a porta estiver configurada como um ponto de acesso a uma área protegida, todas as regras de acesso atribuídas à área são aplicadas à porta. Se restrições de acesso adicionais forem aplicadas na área, elas também serão aplicadas à porta.

Para selecionar quem tem acesso a uma porta:

1 Na página inicial do Config Tool, abra a tarefa *Exibição de área*.

2 Selecione a entidade de porta e clique na aba **Agendas de desbloqueio**.

3 Na seção *Agendas de desbloqueio*, clique em **Adicionar um item** ( ).

4 Selecione as agendas às quais você deseja aplicar períodos de acesso livre e clique em **Selecionar**.

Exemplo: Um uso típico de uma agenda de desbloqueio poderá ser o seguinte: A porta principal do escritório deve estar desbloqueada das 9:00 às 12:00, bloqueada das 12:00 às 13:00 e desbloqueada novamente das 13:00 às 18:00.

5 Na seção *Exceções a agendas de desbloqueio*, clique em **Adicionar um item** ( ).

6 Selecione as agendas às quais você deseja aplicar períodos de acesso controlado e regras de acesso e clique em **Selecionar**.

7 Clique em **Aplicar** e, em seguida, clique na aba **Regras de acesso**.

MELHOR PRÁTICA: Se todas as portas perimétricas ao redor da área compartilham as mesmas regras de acesso, associe essas regras de acesso à área em vez de às portas.

8 Na opção **O acesso à porta se aplica a**, selecione se as regras de acesso para os períodos de acesso controlado se aplicam a **Ambos os lados** ou a **Lados individuais** da porta.

NOTA: Se a porta é configurada apenas com um leitor, você só pode configurar regras de acesso para o lado onde o leitor está configurado.

9 Na seção *Regras de acesso*, clique em **Adicionar um item** ( ), selecione regras de acesso (e titulares de cartão) e clique em **OK**.

Se você atribuir titulares de cartão ou grupos de titulares de cartão diretamente para a porta, os titulares de cartão têm acesso concedido o tempo todo.

10 Se as regras de acesso forem específicas para cada lado da porta, defina regras de acesso para o outro lado da porta.

11 Clique em **Aplicar**.

Tópicos relacionados

Considerações sobre conexão de E/S do HID na página 1161

Sobre elevadores

É um tipo de entidade que oferece propriedades de controle de acesso aos elevadores. Para um elevador, cada andar é considerado um ponto de acesso.

Quando um titular de cartão usa uma credencial, os botões de andar para acessar os pisos para os quais o titular do cartão é autorizado, são ativados. Isto é conseguido controlando um relé de saída para habilitar o botão de andar.

O acompanhamento do andar é conseguido através do monitoramento das entradas, que registra os botões de andares que são pressionados. Isso permite relatórios de rastreamento do uso de elevadores no Security Desk.

Hardware necessário para controle de elevador e controle de andar

Para controlar o acesso a um elevador, você precisa do seguinte:

- Uma *unidade de controle de acesso*.

  NOTA: Apenas unidades Synergis™ são suportadas para novas instalações.
- Um leitor na cabine do elevador.
- Saídas que fecham contatos de relé para ativar os botões de andar.
- Entradas que registram os botões de andar que foram selecionados (somente necessário quando o rastreamento de andar for necessário).
- *Módulos de interface* alimentando ou conectando o hardware acima à unidade de controle de acesso.

Modos do leitor

As seguintes configurações do leitor podem ser aplicadas ao leitor da cabine do elevador:

- Apenas cartão
- Cartão ou PIN
- Cartão e PIN
- Cartão e PIN em um horário

Configurações gerais do elevador

É possível definir as seguintes configurações gerais para o elevador:

- **Horário da concessão:** Este valor indica por quanto tempo os botões da andar do elevador permanecem ativados depois que o acesso foi concedido.
- **Relé de saída para acesso livre:** Existem duas escolhas possíveis: (1) *Normal*, significa que o acesso ao andar fica ativado quando o relé de saída da unidade de controle de acesso é desenergizado; (2) *Ativo*, significa que o acesso ao andar fica ativado quando o relé de saída da unidade de controle de acesso é energizado.

Limitações

- Um elevador (tanto o leitor da cabine quanto as E/S) deve ser controlado por uma única unidade de controle de acesso.
- *Anti-passback*, *intertravamento* e *Contagem de pessoas* não funcionam com elevadores.
- Um *certificado de segurança* mínima não pode ser fiscalizado em elevadores.

Tópicos relacionados

Diferenças entre unidades HID e Synergis em controle de elevadores na página 622

Diferenças entre unidades HID e Synergis™ em controle de elevadores

Ambas as unidades HID e Synergis™ podem ser usadas para controle de elevadores. No entanto, devido às muitas limitações da HID em relação ao controle de elevadores, recomendamos apenas unidades Synergis™ para novas instalações.

NOTA: Se você precisar substituir uma unidade HID VertX V1000 defeituosa que controla um elevador, recomendamos enfaticamente mudar para unidades Synergis™, especialmente se você tiver agendas de desbloqueio em seus andares.

Recursos com suporte	Unidades HID	Synergis™ unidades

Modelos de controlador / número de entradas / número de saídas	• HID VertX V2000 / 4 /6
	• HID iClass Edge / 2 / 2
	• HID VertX V1000 com
	  • V100 / 4 / 4
	  • V200 / 2 / 18
	  • V300 / 12 / 4
		A unidade Synergis™ requer *módulos de interface* para E/S:
		• HID VertX
		  • V100 / 4 / 4
		  • V200 / 2 / 18
		  • V300 / 12 / 4
		• Mercury
		  • MR50 / 2 / 2
		  • MR52 / 8 / 6
		  • MR16IN / 16 / 2
		  • MR16OUT / 0 / 16
		• Leitores STid
		Módulos de interface de diferentes fabricantes podem ser misturados na mesma unidade.

Número de elevadores por unidade	Um.	Até 32 Uma unidade Synergis™ pode suportar até 32 módulos de interface. Assim, uma unidade Synergis™ poderia suportar 32 elevadores com 6 andares cada (usando 32 MR52) ou 6 elevadores com 60 andares cada. Este número será menor se você usar rastreamento de andares, uma vez que você precisa substituir módulos de saída com módulos de entrada. Com os módulos V100 e V300, você recebe um pouco menos, já que eles têm menos saídas por módulo.
Uso misto	Uma unidade HID usada para controlar um elevador não pode ser usada para controlar qualquer outra coisa.	Uma unidade Synergis™ pode ser usada para controlar elevadores, portas e zonas, tudo ao mesmo tempo.

Recursos com suporte	Unidades HID	Synergis™ unidades
Tipos de leitor	• Wiegand • Clock & Data • Wiegand (Dorado) • Clock & Data (Dorado)	• Wiegand • Clock & Data • Wiegand (Dorado) • Clock & Data (Dorado) • Leitores de cartão inteligente STid.
Exceção a regras de acesso	Não suportado.	Pode ser configurado para o leitor de cabine e para cada andar individual.
Rastreamento de andar	Suportado apenas quando a unidade está online (conectada ao Access Manager).	Suportado mesmo quando a unidade está offline (desconectada do Access Manager).
Seleção de andar única por concessão de acesso	Não suportado.	Assim que o titular de cartão seleciona um andar e a unidade Synergis™ recebe o sinal da entrada de rastreamento de andar, todas as saídas de andar retornam ao estado controlado.
Tempo de concessão do elevador sem sobreposição	Não suportado. Todos os andares liberados pelo primeiro cartão lido permanecem liberados quando um segundo cartão é lido antes do tempo de concessão expirar.	Suportado. Uma leitura de cartão subsequente encerra o tempo de concessão atual em todos os andares liberados pelo cartão lido anteriormente, independentemente se o titular de cartão anterior tiver selecionado um andar ou não.
Diferentes horários de acesso para diferentes andares. Cenário: Bob recebe acesso ao andar 1 das 9:00 às 10:00 através da regra de acesso 1 e ao andar 2 das 10:00 às 11:00 através da regra de acesso 2.	Não suportado. Os horários de diferentes regras de acesso aplicadas a diferentes andares são mesclados quando as regras são concedidas ao mesmo titular. No nosso cenário de exemplo, Bob tem acesso aos andares 1 e 2 das 9:00 às 11:00.	Suportado. Os horários de diferentes regras de acesso aplicadas a diferentes andares são mantidos separados. No nosso cenário de exemplo, Bob somente tem acesso ao andar 1 das 9:00 às 11:00 e ao andar 2 das 10:00 às 11:00.

Criar elevadores

Para controlar o acesso e monitorar eventos de controle de acesso relacionados a elevadores, você deve criar entidades de elevador no Security Center.

Antes de iniciar

Certifique-se de que tenha todo o hardware necessário para controlar o elevador, instalado o leitor na cabine do elevador e ligado o leitor ao módulo de interface conectado à unidade de controle de acesso.

Para criar um elevador:

1 Na página inicial do Config Tool, abra a tarefa *Exibição de área*.

2 Clique em **Adicionar uma entidade** ( ) > **Elevador**.

3 No assistente de criação do elevador, digite o nome e a descrição do elevador.

4 Na lista suspensa **Localização**, selecione a área na qual o elevador será criado e clique em **Próximo**.

NOTA: Ao contrário das portas, os elevadores não são tratados como *pontos de acesso* a áreas. No entanto, cada andar de elevador é um ponto de acesso por conta própria.

5 Digite o número de andares do elevador e clique em **Criar**.

As entidades de andar padrão são criadas.

6 Para alterar o nome de um andar, selecione-o e digite um novo nome.

7 Faça ajustes, se necessário, e clique em **Próximo**.

8 Revise o *Resumo de criação* e clique em **Criar** > **Fechar.**

O novo elevador aparece na visualização de área com seus andares. Ele aparece inicialmente em vermelho até que esteja totalmente configurado.

9 Selecione as configurações de relé de saída para o andar do elevador.

As configurações do relé de saída afetam a forma como você ligará a unidade.

10 Descreva a ligação física entre a unidade de controle de acesso e o elevador ao Security Center.

11 Selecione quem tem acesso aos andares do elevador.

Selecionar o comportamento do relé de saída para andares de elevadores

Antes de terminar a fiação do elevador, é necessário configurar as configurações do relé de saída da unidade.

Antes de iniciar

Crie a entidade do elevador no Security Center.

O que você deve saber

As configurações do relé de saída afetam a forma como você ligará a unidade. Você deve usar os contatos de relé NO ou NC apropriados nas unidades, com base nas configurações selecionadas no Security Center.

Para selecionar o comportamento do relé de saída para um andar de elevador:

1 Na página inicial do Config Tool, abra a tarefa *Exibição de área*.
2 Selecione o elevador a configurar e clique na aba **Avançado**.
3 Na opção **Tempo de concessão**, selecione por quanto tempo os botões de andares dos elevadores permanecem ativados depois que o acesso foi concedido.
4 Na opção **Acesso livre quando o relé de saída está**, selecione em que estado o relé deve estar para que o acesso livre seja concedido:
   - **Normal:** O acesso ao andar é ativado quando o relé de saída da unidade de controle de acesso é desenergizado. Significa que uma perda de energia resulta em acesso livre ao andar.
   - **Ativo:** O acesso ao andar é ativado quando o relé de saída da unidade de controle de acesso é energizado. Significa que uma perda de energia resulta no acesso ao andar ser negado.
5 Clique em **Aplicar**.

Após terminar

Conclua a fiação dos andares de elevadores de acordo com as configurações de relé especificadas e mapeie sua fiação para a entidade de elevador.

Mapear a fiação de andares físicos de elevadores para entidades de elevador

Para que sua entidade de elevador seja funcional, você deve combinar a fiação de hardware que você fez para o elevador no Security Center, para que o Access Manager saiba como controlar o elevador.

Para mapear a fiação física de um elevador para uma entidade de elevador:

1 Na página inicial do Config Tool, abra a tarefa *Exibição de área*.

2 Selecione a entidade de elevador a configurar e clique na aba **Andares**.

3 Na lista suspensa **Unidade preferida**, selecione uma unidade de controle de acesso que esteja conectada ao leitor de cabine do elevador.

4 Na lista suspensa **Leitor de cabine do elevador**, atribua a entrada do leitor.

5 Para alterar as definições do leitor de cabine do elevador, clique em **Configurações do leitor** ( ).

A caixa de diálogo *Configurações do leitor* permite configurar o seguinte:

- **Tempo limite para digitação de PIN:** Isso configura apenas o tempo limite de digitação do PIN após o cartão ter sido lido. Por exemplo, por padrão (5 segundos), você tem 5 segundos para digitar todos os dígitos do PIN.
- **Usar cartão e PIN:** Ajuste em **ATIVO** para alterar o modo do leitor para Cartão e PIN e selecione o **agendamento**ao qual esse modo se aplica. Quando não está em um período de tempo agendado, o leitor se comporta somente em modo de Cartão.

NOTA: Certifique-se de que suas configurações correspondem às capacidades do seu leitor. O sistema não pode validar as capacidades do seu hardware. Você pode configurar esse tipo de leitor na aba **Periféricos** da unidade.

6 Na seção **Andares**, use os botões a seguir para adicionar andares de elevador ou alterar sua configuração:

- Para adicionar um andar de elevador, clique em .
- Para excluir o andar de elevador selecionado, clique em .
- Para mover o andar de elevador selecionado para cima, clique em .
- Para mover o andar de elevador selecionado para baixo, clique em .
- Para modificar o andar de elevador selecionado, clique em .

A caixa de diálogo *Propriedades do andar* permite configurar o seguinte:

- Alterar o nome do andar.
- Atribuir um relé de saída ao botão correspondente a esse andar.

  Utilize os contatos de relé NO ou NC apropriados na unidade, de acordo com as definições do relé de saída configuradas na aba **Avançado**.

  NOTA: O estado do relé de saída pode ser invertido de acordo com suas exigências regulatórias.
- (Opcional) Atribua uma entrada para rastreamento de andar.

NOTA: Em uma unidade de controle de acesso dedicada ao controle do elevador, todas as entradas podem ser usadas para rastreamento do andar, exceto para as entradas do monitor de porta.

7 Associe câmeras à cabine do elevador e a cada andar de elevador.

8 Clique em **Aplicar**.

Tópicos relacionados

Unidade de controle de acesso - HID - Aba Periféricos na página 970
Unidade de controle de acesso - Synergis - Aba Periféricos na página 977

Vincular câmeras a elevadores

Você pode vincular câmeras a entidades de elevador, de modo que quando um evento de controle de acesso é acionado no elevador (elevador acessado ou acesso negado), ele faz com que o feed de vídeo da câmera seja exibido em um ladrilho de monitoramento do Security Desk. A gravação de vídeo é iniciada automaticamente com o evento de acesso ao andar.

Antes de iniciar

Para monitorar elevadores com câmeras, você deve ter uma das seguintes configurações do Security Center:

- Uma função Archiver com câmeras disponíveis.
- Uma função Omnicast™ Federation™ para conexão a um sistema Omnicast™ externo.
- Uma função Federation™ do Security Center para conexão a um sistema Security Center externo com câmeras.

Para ligar câmeras a um elevador:

1 Na página inicial do Config Tool, abra a tarefa *Exibição de área*.
2 Selecione a entidade de elevador a configurar e clique na aba **Andares**.
3 Na seção *Cabine*, clique em **Associar uma câmera** ( ).
4 Na lista suspensa **Câmera**, selecione uma câmera.

   Se a câmera tiver um motor PTZ, você também pode incluir o número PTZ predefinido para garantir que a câmera aponta para o elevador.

5 Para adicionar outra câmera ao elevador, clique em **Associar uma câmera** ( ) novamente.
6 Para ligar uma câmera a cada andar do elevador:
   a) Na seção **Andares**, selecione um andar e clique em **Editar o item** ( ).
   b) Na caixa de diálogo **Propriedades do andar**, clique em **Associar uma câmera** ( ).
   c) Na lista suspensa **Câmera**, selecione uma câmera.
   d) Clique em **OK**.
   e) Repita as etapas para todos os andares do elevador.
7 Clique em **Aplicar**.

Selecionar quem tem acesso a elevadores

Você pode definir horários para quando o acesso a um elevador é controlado, e quem pode acessar o elevador com suas credenciais quando o acesso é controlado aplicando regras de acesso.

Antes de iniciar

Crie as regras de acesso.

O que você deve saber

Assim como uma porta, o controle de elevador requer regras de acesso para determinar *quem* receberá acesso, *onde* e *quando*. Você também pode atribuir agendas de desbloqueio para permitir *acesso livre* (sem necessidade de credenciais) durante certos períodos.

Para selecionar quem tem acesso a um elevador:

1. Na página inicial do Config Tool, abra a tarefa *Exibição de área*.
2. Selecione a entidade de elevador e clique na aba **Acesso**.
3. Na seção *Regras de acesso*, clique em **Adicionar um item** ( ).
4. Selecione as regras de acesso a serem aplicadas ao elevador e clique em **Selecionar**.

   As regras de acesso determinam quais titulares de cartão podem acessar o elevador e quando.
5. Para cada regra de acesso, clique na lista suspensa **Andar** e selecione a qual piso a regra de acesso se aplica.
6. Na seção *Exceções*, clique em **Adicionar um item** ( ).
7. Selecione as agendas às quais você deseja aplicar exceções e clique em **Selecionar**.
8. Na lista suspensa da coluna **Andar**, selecione a quais andares a exceção se aplica.
9. Na lista suspensa da coluna **Modo**, selecione se o elevador tem acesso livre ou acesso controlado durante a agenda de exceções.
   - **Acesso livre:** Titulares de cartão não precisam de uma credencial para acessar o elevador e nenhuma regra de acesso se aplica.
   - **Acesso controlado:** Titulares de cartão precisam de uma credencial para acessar o elevador e as regras de acesso se aplicam.
10. Clique em **Aplicar**.

Tópicos relacionados

Considerações sobre conexão de E/S do HID na página 1161

Boas práticas para configurar exceções de acesso controlado

Os elevadores estão em modo de acesso controlado por padrão. Portanto, a melhor prática é começar com uma agenda de desbloqueio que informa quando o elevador deve estar em modo de acesso livre (desbloqueado). Consequentemente, qualquer horário não selecionado na agenda define o elevador para modo de acesso controlado.

Quando as agendas se sobrepõem, as agendas de acesso controlado têm prioridade sobre as agendas de desbloqueio (acesso livre). Uma agenda de exceções controladas só é útil se houver pelo menos uma agenda de exceções de desbloqueio.

Sobre áreas protegidas

Uma área protegida é uma entidade de área que representa um local físico onde o acesso é controlado. Uma área protegida consiste em portas de perímetro (portas usadas para entrar ou sair da área) e restrições de acesso (regras que regem o acesso à área).

Na presença de uma ameaça, o acesso a áreas protegidas pode ser restrito (para manter o perigo fora) ou relaxado (para permitir que as pessoas se afastem do perigo), ativando *níveis de ameaça*.

Você pode configurar as seguintes restrições de acesso em uma área protegida:

- Regras de acesso
- Anti-passback
- Intertravamento
- Regra de primeira pessoa a entrar
- Regra de acompanhante de visitante

Permissões de acesso

As restrições de acesso básicas a uma área são definidas através da concessão de acesso a titulares de cartões específicos (quem podem acessar esta área e quando). Quando nada está configurado, ninguém tem permissão para entrar ou sair da área. Os direitos de acesso podem ser concedidos através de regras de acesso (abordagem recomendada) se for restringido por uma programação, ou diretamente aos portadores de cartão, se não houver restrição de horário. Os direitos de acesso podem ser concedidos em toda a área, ou individualmente para cada ponto de acesso da área.

Anti-passback

O antirretorno é uma restrição de acesso colocada em uma área protegida que evita que um titular de cartão entre em uma área de onde ainda não saiu e vice-versa. Quando o acesso é negado devido a uma violação de anti-passback, a violação deve ser "*perdoada*" no Security Desk para que o titular de cartão destrave a porta. O evento de anti-passback pode ser perdoado automaticamente após um período de tempo se ele estiver configurado com um valor de tempo limite.

NOTA: As unidades HID suportam anti-passback *ou* intertravamento, mas não ambos simultaneamente.

Intertravamento

Um intertravamento (também conhecido como portão duplo ou câmara de vácuo) é uma restrição de acesso colocada em uma área protegida que permite que somente uma porta seja aberta em determinado momento. Isto é tipicamente usado em uma passagem com pelo menos duas portas. O titular de cartão destrava a primeira porta, entra na passagem, mas não pode destravar a segunda porta até que a primeira porta esteja fechada.

Para a lógica de intertravamento funcionar, os sensores de portas devem ser capazes de detectar quando a porta é aberta.

NOTA: As unidades HID suportam anti-passback *ou* intertravamento, mas não ambos simultaneamente.

Regra de primeira pessoa a entrar

A regra de primeira pessoa a entrar é a restrição de acesso adicional feita a uma área protegida que impede alguém de entrar na área até que um supervisor esteja no local. A restrição pode ser aplicada quando existe acesso livre (mediante agendas de desbloqueio de portas) e quando existe acesso controlado (mediante regras de acesso).

- Quando aplicada nos horários de desbloqueio da porta, as portas permanecem bloqueadas até que um supervisor entre na área. Os portadores de cartão que têm acesso ainda podem entrar na área. Uma vez que uma programação de desbloqueio seja ativada, ela permanece em vigor até o final do intervalo de tempo atual definido na programação.
- Quando aplicada a regras de acesso, ninguém pode entrar na área mesmo que tenha credenciais válidas, até que um supervisor entre na área. Um cronograma define quando se aplica a regra de primeira pessoa a entrar. Você pode configurar titulares de cartão para serem isentos dessa restrição. Um titular de cartão isento pode acessar a área sem qualquer supervisor estar no local, mas não pode limpar a restrição para outros titulares.

  NOTA: O cronograma da regra de primeira pessoa a entrar deve definir intervalos de tempo distintos para permitir que a restrição seja redefinida. A agenda *Sempre* não pode ser usada.
- Para limpar a restrição de regra de primeira pessoa a entrar, o supervisor deve chegar dentro do intervalo de tempo definido pela agenda de desbloqueio ou pela agenda de regras de primeira pessoa a entrar, até alguns minutos antes, definido pelo valor **Diferença de tempo no local**. Uma vez que a restrição é limpa, o acesso normal (acesso livre ou controlado) é retomado até o final do intervalo de tempo atual definido na programação.

  Se o cronograma de desbloqueio ou o cronograma de regras de primeira pessoa incluir vários intervalos de tempo, o supervisor deve entrar novamente na área no início de cada intervalo de tempo para limpar a restrição.

NOTA: A *regra de primeira pessoa a entrar* funciona apenas em áreas controladas por uma única unidade Synergis™. As unidades HID não suportam este recurso. A *regra de primeira pessoa a entrar* funciona melhor quando as portas estão equipadas com sensores de entrada ou sensores de porta. Uma unidade Synergis™ é capaz de diferenciar entre *Sem entrada*, *Entrada suposta* e *Entrada detectada*. Quando nenhum sensor está configurado para uma porta, a entrada é suposta quando o acesso é concedido.

Regra de acompanhante de visitante

A regra de acompanhante de visitante é a restrição de acesso adicional aplicada a uma área protegida que exige que os visitantes sejam acompanhados por um titular de cartão durante a estadia. Os visitantes que tenham um host não podem passar por pontos de acesso até que eles e seu host (titular de cartão) apresentem as credenciais com um intervalo de tempo entre uma apresentação e outra. O host deve apresentar sua credencial após os visitantes antes que o acesso seja concedido a ambos. Se vários visitantes são acompanhados pelo mesmo acompanhante, ele só precisará apresentar sua credencial, uma vez que todos os visitantes tenham apresentado suas credenciais.

Para catracas compatíveis com ANSSI, o host deve apresentar o crachá e entrar antes do(s) visitante(s). Para delegações de visitantes com dois hosts, o host final deve apresentar credenciais e entrar na área depois dos visitantes.

NOTA: As unidades HID não suportam a regra de acompanhante do visitante.

Configurar áreas protegidas

Para configurar um sistema de controle de acesso com regras de acesso e comportamento de controle de acesso, você deve configurar suas áreas como áreas protegidas.

Antes de iniciar

Crie as áreas que representarão suas áreas protegidas.

Para configurar uma área protegida:

1 Na página inicial do Config Tool, abra a tarefa *Exibição de área*.

2 Selecione a entidade de área ( ) que deseja configurar e clique na aba **Identidade**.

3 Clique em **Controle de acesso** para deixar a opção **Ligada** e, em seguida, clique em **Aplicar**.

Duas novas abas, **Propriedades** e **Avançado**, aparecem e o ícone associado é atualizado para mostrar que agora essa é uma área protegida ( ).

4 Clique na aba **Propriedades** e defina o seguinte:

- **Regras de acesso:** Defina quais titulares de cartão podem acessar (entrar ou sair) a área e quando, atribuindo regras de acesso à área. Você também pode atribuir titulares de cartão ou grupos de titulares de cartão diretamente para a área, caso no qual os titulares de cartão terão acesso concedido o tempo todo.
- **Portas:** Conecte as portas que são utilizados para entrar e sair da área (portas de perímetro), bem como as que são cativas. As portas cativas são necessárias para o devido rastreamento da *contagem de pessoas* e *anti-passback*.

NOTA: As regras de acesso atribuídas à área se aplicam a todas as portas de perímetro da área. Se for necessário que cada porta de perímetro seja governada por seu próprio conjunto de regras, configure as regras de acesso de cada porta.

5 Clique na aba **Avançado** e defina o seguinte:

- **Antirretorno:** Restrição de acesso feita a uma área protegida que impede que um titular de cartão entre em uma área da qual ainda não saiu e vice-versa.
- **Intertravamento:** Lógica que só permite abrir uma porta de perímetro de cada vez.
- **Regra de primeira pessoa a entrar:** A programação de desbloqueio não é acionada ou o acesso regular é desativado até que um supervisor esteja presente na área.
- **Regra de acompanhante de visitante:** Os visitantes devem ser acompanhados pelo seu host designado (titular de cartão) para entrar na área.
- **PIN de dureza:** Um titular de cartão que esteja sendo coagido a abrir uma porta pode digitar seu PIN com o último dígito aumentado em 1 para acionar um evento do Security Desk. Somente funciona em portas com leitores definidos para Cartão e PIN.

6 Clique em **Aplicar**.

Tópicos relacionados

Sobre áreas protegidas na página 629

Adicionar portas a áreas

Para certificar-se de que uma área está segura, adicione as portas à área no Config Tool.

Antes de iniciar

Crie as áreas às quais deseja associar portas.

O que você deve saber

Portas que são membros de uma área podem ser configuradas como portas *Cativas* ou de *Perímetro*. As portas de perímetro são usadas para entrar e sair de uma área e ajudar a controlar o acesso. As portas cativas são portas que são usadas dentro da área. Configure os *lados da porta* corretamente para garantir que *Contagem de pessoas* e *anti-retorno* sejam devidamente rastreados. Os lados de *Entrada* e *Saída* de uma porta são relativos à área sendo configurada.

NOTA: As regras de acesso configuradas para uma área só se aplicam às portas do perímetro. Todas as regras que negam acesso têm precedência sobre as regras que concedem acesso.

Para adicionar uma porta a uma área:

1 Na página inicial do Config Tool, abra a tarefa *Exibição de área*.
2 Selecione uma área e clique na aba **Propriedades**.
3 Na seção *Portas*, clique em **Adicionar um item** () e selecione as portas que deseja associar à sua área.
4 Para todas as portas na seção **Portas**, faça o seguinte:
   - Se a porta for utilizada para entrar ou sair da área, coloque o controle deslizante em **Perímetro**.
   - Se a porta estiver localizada dentro da área, coloque o controle deslizante em **Cativa**.

     NOTA: Se uma área menor for aninhada dentro de uma área maior, você não precisa adicionar as portas do perímetro da área menor como portas cativas da área maior. O sistema cuida automaticamente da lógica das áreas aninhadas ao calcular as contagens de pessoas e aplicar as regras de anti-passback.
   - Para alternar os lados da porta, clique em **Alternar lado da porta** enquanto a porta estiver selecionada.
5 Clique em **Aplicar**.

Após terminar

Para controlar o acesso à sua área protegida, aplique regras de acesso à área.

Aplicar anti-passback a áreas

Uma vez que sua área tenha sido criada e contenha pelo menos uma porta de perímetro, você pode aplicar o antirretorno para impedir que os titulares de cartão entrem em áreas de que ainda não tenham saído, e vice-versa.

Antes de iniciar

Crie e configure uma área protegida à qual aplicar a restrição de anti-passback.

O que você deve saber

Uma área com antirretorno deve ser controlada por uma única unidade. Se a área não for controlada por uma única unidade, os seguintes critérios devem ser atendidos para aplicar antirretorno.

- Todas as unidades que controlam as portas dentro da área são unidades Synergis™.
- Todas as unidades que controlam a área são gerenciadas pela mesma função Access Manager.
- O anti-passback global is enabled na função Access Manager.

Limitações: Para áreas controladas por unidades HID, a lógica de anti-passback só é aplicada a portas de perímetro, não a portas cativas.

Para configurar o antirretorno para uma área:

1 Na página inicial do Config Tool, abra a tarefa *Exibição de área*.
2 Selecione a área protegida e clique na aba **Avançado**.
3 Defina **Anti-passback** como **Ligado**.
4 Se as portas forem controladas por uma unidade HID, defina **Intertravamento** como **Desligado**.
5 Defina:
   - **Cronograma:** Selecione *Sempre* se quiser que o anti-passback seja aplicado sempre.
   - **Tipo:** Tipo de antirretorno para aplicar.
     - **Virtual:** O antirretorno lógico apenas registra os eventos de antirretorno no banco de dados. Ele não impede a porta de ser desbloqueada devido a um evento de antirretorno.
     - **Física:** O antirretorno físico registra uma entrada no banco de dados e impede a porta de ser desbloqueada devido a um evento de antirretorno.
   - **Tempo limite de presença:** Configura por quantos minutos a presença de um titular de cartão na área é lembrada para fins de detecção de retorno (não é usado para contar pessoas). Depois desse período, um titular de cartão que nunca tenha deixado a área pode entrar novamente sem disparar um evento de retorno. O valor padrão de zero (0) minutos significa que a presença de um titular de cartão nunca tem o limite de tempo esgotado.

     NOTA: Quando o antirretorno global está ativado, a presença de um titular de cartão em uma área é esquecida após sete dias se nenhuma entrada ou saída dessa área é registrada para esse titular do cartão durante esse período. Isso significa que titulares de cartão podem entrar novamente em uma área da qual nunca saíram ou deixar uma área em que nunca entraram sem disparar um evento de retorno se nenhum movimento tiver sido registrado para esses titulares naquela área por sete dias. Isso se aplica mesmo que o **Tempo limite de presença** esteja definido como infinito (=0).
   - **Estrita:** Ative esta opção para gerar eventos de passback para ambos os tipos de violação de acesso: quando titulares de cartão tentarem entrar novamente em uma área da qual saíram e quando tentarem sai de uma área em que nunca entraram. Caso contrário, o padrão é definido como **Desligado** e a lógica de anti-passback é somente verificada em entradas de áreas, e os eventos de passback são somente gerados quando os titulares de cartão tentam entrar novamente em uma área da qual nunca saíram.

     MELHOR PRÁTICA: Se você optar por ativar o anti-passback *estrito* e *físico* em uma área que não seja controlada com catracas ou dispositivos similares que apenas permitam entrar uma pessoa por vez,

conceda o privilégio *Perdoar violação de anti-passback* a operadores responsáveis por monitorar essa área.

NOTA: Com o anti-passback estrito desligado, você pode ter portas de perímetro Card-In/REX-out, mas o parâmetro **Tempo limite de presença** precisa ser configurado (> 0). Com o anti-passbacl estrito ligado, todas as portas de perímetro precisam ser configuradas como Card-In/Card-Out, o **Tempo limite de presença** deve ser configurado como infinito (= 0) e nenhum REX pode ser configurado.

6 Clique em **Aplicar**.

Tópicos relacionados

Sobre áreas protegidas na página 629
Sobre unidades de controle de acesso na página 603

Habilitar anti-passback global em funções do Access Manager

Se as áreas nas quais você deseja aplicar as restrições de anti-passback forem controladas por várias unidades Synergis™, você deve ativar o anti-passback global nas funções do Access Manager.

O que você deve saber

Quando anti-passback *estrito* e *rígido* é aplicado a uma área sem anti-passback global, um titular de cartão que tenha entrado na área através de uma porta não pode abandonar a área através de outra porta se as duas portas não forem controladas pela mesma unidade. Além disso, o mesmo titular de cartão que tenha entrado na área através de uma porta pode reentrar na área através de uma porta diferente se as duas portas não forem controladas pela mesma unidade. Com anti-passback global habilitado, essas duas violações podem ser evitadas.

IMPORTANTE: O anti-passback global só funciona em áreas que sejam totalmente controladas por unidades Synergis™. Todas as unidades que controlam a mesma área devem ser gerenciadas pelo mesmo Access Manager.

DICA: Se você precisar alternar suas unidades entre as funções do Access Manager para atender às exigências de anti-passback global, use a ferramenta Mover unidade.

Para ativar o antirretorno global em uma função do Access Manager:

1 Na página inicial do Config Tool, abra a tarefa *Controle de acesso* e clique na visualização **Funções e unidades**.
2 Selecione a função do Access Manager a ser configurada e clique na aba **Propriedades**.
3 Na página *Propriedades*, selecione as seguintes opções: **Habilitar ponto a ponto** e **Habilitar anti-passback global**.
4 Clique em **Aplicar**.

Definir limites de ocupação de área

Definir um limite de ocupação máxima é útil para controlar quantas pessoas estão em uma determinada área por questões legais ou de segurança. Ultrapassar o limite definido aciona eventos que, por sua vez, podem ser usados para desencadear alarmes e ações.

Antes de iniciar

Faça o seguinte:

- Crie e configure uma área protegida.
- Ative o anti-passback e defina-o como *Rígido* e *Estrito*, defina a agenda para *Sempre* e o **Tempo limite de presença** para **0**.
- Certifique-se de não haver agendas de desbloqueio definidas para as portas perimetrais da área.

O que você deve saber

A ocupação máxima requer o Security Center 5.7 SR2 ou posterior e o Synergis™ Softwire 10.7 ou posterior.

Para definir um limite de ocupação:

1 Na tarefa **Exibição de área**, selecione uma área e clique em **Avançado**.

2 Em *Ocupação máxima*, defina o seguinte:

- **Status:** Definir para **ATIVO** para habilitar o recurso de ocupação máxima. Habilitar um limite de *Ocupação máxima* em uma área gera os seguintes eventos:
  - *Ocupação máxima alcançada* quando a área alcança o limite configurado. Esse evento coloca a área em estado de alerta.
  - *Ocupação máxima excedida* quando titulares de cartão adicionais entram na área
  - *Abaixo da capacidade máxima* quando o número de ocupantes fica abaixo do limite configurado.
- **Tipo:** Selecione entre as seguintes opções:
  - *Pesado*: Quando a o limite de ocupação máxima é alcançado, irá negar solicitação de acesso na área porta do perímetro.
  - *Leve*: Não irá negar solicitações de acesso subsequentes.
- **Limite de ocupação máxima:** Digite o número de pessoas que a área pode suportar antes de disparar o limite.

3 Clique em **Aplicar**.

A exibição de área na tarefa *Contagem de pessoas* do Security Desk controla quantos titulares de cartão estão na área e exibe o número ao lado da área na *árvore de entidades* (por exemplo, uma área com um limite de seis pessoas, mas com apenas três ocupantes seria exibido como "3/6"). Quando a área atinge o limite de capacidade, a sua entidade fica amarela. Se entrarem mais titulares de cartão na área, o número fica vermelho.

Você pode monitorar eventos de ocupação máxima nas tarefas *Monitoramento* ou *Mapas* do Security Desk.

Intertravar portas dentro de áreas

Uma vez que sua área seja criada e contenha pelo menos duas portas de perímetro, você pode aplicar uma lógica de bloqueio para que uma única porta possa ser aberta de cada vez.

Antes de iniciar

Faça o seguinte:

- Crie e configure uma área protegida à qual aplicar a lógica de intertravamento.
- Conecte pelo menos duas portas de perímetro à sua área.

O que você deve saber

Para a lógica de intertravamento funcionar, os sensores de portas devem ser capazes de detectar quando a porta é aberta.

Para interligar portas de perímetro de uma área:

1 Na página inicial do Config Tool, abra a tarefa *Exibição de área*.
2 Selecione a área protegida e clique na aba **Avançado**.
3 Defina **Intertravamento** como **Ligado**.

   Quando ajustado para Ligado, somente uma porta de perímetro da área pode estar aberta a qualquer momento. Para abrir uma porta, todas as outras devem estar fechadas.
4 Se a porta for controlada por uma unidade HID, defina **Anti-passback** como **Desligado**.
5 Defina:
   - **Substituir:** Selecione a entrada que está ligada à tecla ou chave de acionamento de *sobrescrita*. Quando a chave está ligada, o recurso de intertravamento fica desativado.
   - **Trancamento:** Selecione a entrada que está ligada à tecla ou chave de acionamento de *travamento*. Quando a chave está ativada, todas as portas do perímetro permanecem trancadas até a chave voltar à sua posição normal.
   - **Prioridade:** Quando ambas as entradas de *sobrescrita* e *travamento* estiverem configuradas, selecione qual tem a prioridade quando ambas as entradas estiverem ativas.
6 Clique em **Aplicar**.

Tópicos relacionados

Sobre áreas protegidas na página 629

Fiscalizar uma presença de supervisão em áreas protegidas

Você pode manter uma área segura bloqueada até que um supervisor apareça, impondo a regra *primeira pessoa a entrar* na área.

Antes de iniciar

Crie e configure uma área protegida à qual aplicar a regra de primeira pessoa a entrar.

O que você deve saber

A *regra de primeira pessoa a entrar* funciona apenas em áreas controladas por uma única unidade Synergis™. As unidades HID não suportam este recurso.

Para garantir que um supervisor esteja no local antes de conceder acesso a uma área:

1 Na página inicial do Config Tool, abra a tarefa *Exibição de área*.

2 Selecione a área protegida e clique na aba **Avançado**.

3 Na seção *Regra de primeira pessoa a entrar*, faça o seguinte:

- Para ignorar os horários de desbloqueio da porta quando nenhum supervisor está presente, defina a opção **Impor agendamentos de desbloqueio de portas** como **Ligado**.
- Para ignorar as regras de acesso quando nenhum supervisor está presente, defina a opção **Impor regras de acesso** como **Ligado** e selecione o cronograma para determinar quando aplicar a regra de primeira pessoa a entrar.

4 Clique em **Diferença de tempo no local** para dar mais liberdade ao tempo que o supervisor tem para aparecer e liberar a restrição da regra de primeira pessoa a entrar.

Se o diferençal de tempo for zero, o supervisor não poderá aparecer antes do início do cronograma de acesso, ou sua chegada será ignorada.

5 Na lista **Supervisores**, clique em **Adicionar um item** (+) e selecione os grupos de titulares de cartão e titulares de cartão a designar como supervisores da área.

Você deve configurar ao menos um supervisor. Somente um supervisor precisa estar presente na área para satisfazer a restrição de regra de primeira pessoa a entrar.

6 (Opcional) Na **Lista de isenções**, clique em **Adicionar um item**(+) e selecione os grupos de titulares de cartão e titulares de cartão aos quais a regra de primeira pessoa a entrar não se aplica.

O acesso é concedido a esses titulares apenas com base nas regras de acesso. Um supervisor não precisa estar presente para conceder-lhes acesso à área.

7 Clique em **Aplicar**.

Tópicos relacionados

Sobre áreas protegidas na página 629

Exigir que os visitantes sejam escoltados para acessar áreas protegidas não ANSSI

Você pode aumentar a segurança de certas áreas exigindo que os visitantes sejam acompanhados por um ou dois hosts designados. Todos os hosts devem apresentar suas credenciais (em qualquer ordem) após o visitante, dentro de determinado prazo antes que o acesso seja concedido a todo o grupo.

Antes de iniciar

Faça o seguinte:

- Crie e configure uma área protegida à qual aplicar a regra de acompanhamento de visitante.
- Conecte pelo menos uma porta de perímetro à sua área.

Para exigir que um visitante seja escoltado para acessar uma área protegida:

1 Na página inicial do Config Tool, abra a tarefa *Exibição de área*.
2 Selecione a área protegida e clique na aba **Avançado**.
3 Na seção **Regra de acompanhamento de visitante**, faça o seguinte:
   - Coloque a opção **Impor regra de acompanhamento de visitante** em **Ligado**.
   - Clique em **Reverter para valor herdado** ( ) se a área pai tiver a regra de acompanhamento de visitante imposta.
4 Clique em **Aplicar**.
5 Selecione a aba **Propriedades**.
6 (Opcional) Para todas as portas de perímetro configuradas para esta área:
   a) Selecione a porta e clique em **Saltar para** ( ).
   b) Selecione a aba **Propriedades** da porta.
   c) Defina o **Retardo máximo entre apresentações de cartão** em segundos.

      O acesso será negado se a escolta não apresentar sua credencial dentro do retardo especificado depois do visitante.

   d) Clique em **Aplicar**.

Após terminar

Ao fazer o cadastro de visitantes que precisam de acesso supervisionado a esta área, atribua um ou dois hosts (titulares de cartão que tenham acesso a essa área) ao visitante e selecione **Acompanhamento necessário**.

Tópicos relacionados

Sobre áreas protegidas na página 629

Configurar acompanhamento de visitantes para catracas conforme a ANSSI

A conformidade com a ANSSI (*Agence Nationale de la Sécurité des Systèmes d'Information*) aumenta a segurança para áreas acessíveis por catracas. Os requisitos de conformidade impõem restrições à configuração de hosts de visitantes e adicionam limites de tamanho à delegação de visitantes.

Antes de iniciar

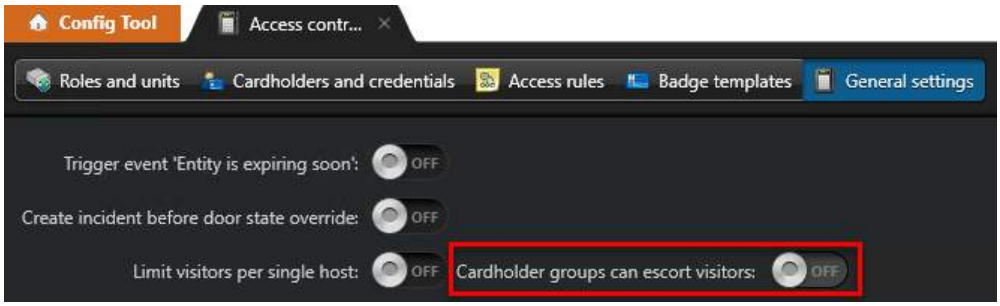
Crie uma área protegida com, pelo menos, uma porta.

O que você deve saber

As catracas conformes a ANSSI requerem o Security Center 5.7 SR2 ou posterior e o Synergis™ Softwire 10.7 ou posterior com interfaces limitadas.

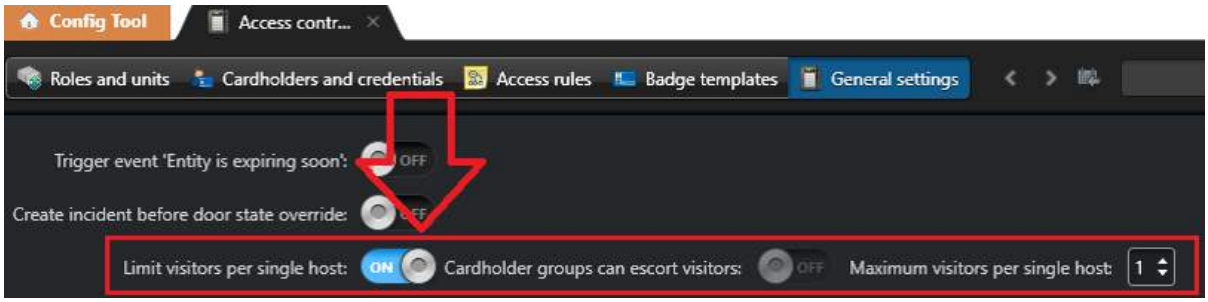
Configurar acompanhamento de visitantes conforme a ANSSI:

1 Clique em **Controle de acesso** > **Configurações gerais** e defina **Grupos de titulares de cartão podem acompanhar os visitantes** para **Desligado**.



Se a opção for deixada em **Ligado**, então os eventos *Visitante perdido* e *Host de cauda ausente* não serão acionados.

2 (Opcional) Defina **Limite de visitantes para um único host** para **Ligado** e defina um limite.



NOTA: O número definido não é um limite por host, é o limiar acima do qual deve ser adicionado um segundo host. Não há limite para o número de visitantes em delegações com dois hosts.

3 Clique em **Aplicar**.

4 Clique em **Sistema** > **Configurações gerais** > **Campos personalizados** e clique em **Adicionar um item** ( ).

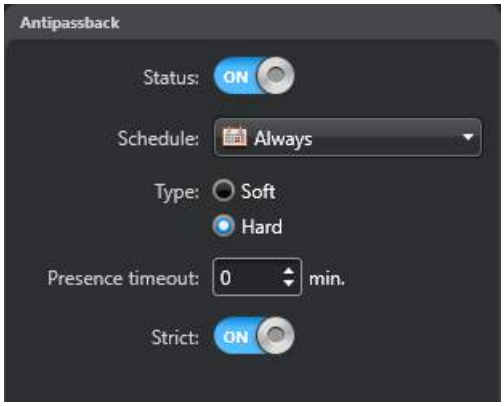
5 Na lista **Tipo de entidade**, selecione **Porta** ( ).

6 Na lista **Tipo de dados**, selecione **Boolianos**.

7 No campo **Nome**, digite `TurnstileANSSI`.

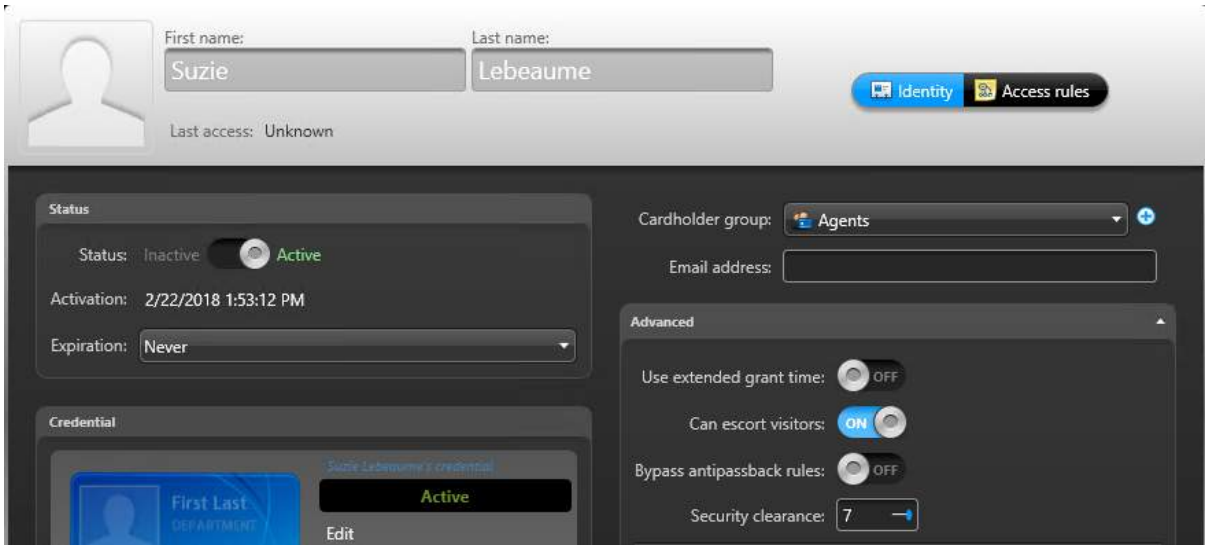
8 Clique em **Salvar e fechar** > **Aplicar**.

9 Na tarefa *Exibição de área*, clique a área na *árvore de entidades*.
10 Na aba **Avançado**, defina **Impor regra de acompanhamento de visitante** para **Ligado**.
11 (Opcional) Defina Anti-passback para **Ligado**.



12 Selecione a porta da área na *árvore de entidades*.
13 Clique em **Campos personalizados**, selecione **TurnstileANSSI** e clique em **Aplicar**.
14 (Opcional) Clique em **Identidade** e defina o ícone para uma catraca ( ).
15 Clique em **Propriedades**.
16 Em **Acompanhante de visitantes e regra de duas pessoas**, defina **Atraso máximo entre apresentações de cartão** para um valor superior aos 5 segundos padrão, para dar tempo aos visitantes de apresentar o crachá e passar pela catraca.

    Um visitante deve apresentar a sua credencial e entrar dentro do atraso definido, caso contrário, é acionado um evento de *Visitante perdido*.
17 Clique em **Aplicar**.
18 Na tarefa *Gerenciamento de titulares de cartões*, certifique-se de que os Titulares do cartão que são hosts designados tenham a opção **Pode acompanhar visitantes** definida para **Ligado** e que todos os outros titulares do cartão tenham **Pode acompanhar visitantes** definido para **Desligado**.



19 Clique em **Salvar e fechar**.

    Todos os titulares do cartão criados em versões do Security Center anteriores a 5.7 SR2 têm a opção **Pode acompanhar visitantes** ativada por padrão. Você pode usar a caixa de verificação **Opções** na ferramenta **Copiar configuração** para desativar a opção **Pode acompanhar visitantes** para vários titulares do cartão ao mesmo tempo. A caixa de verificação **Opções** copiará os valores do seguinte:

    - Usar tempo de concessão estendido
    - Pode acompanhar visitantes
    - Desconsiderar regras anti-passback

- Certificado de segurança

Certifique-se de somente usar este recurso em titulares do cartão com valores de opção correspondentes.

Habilitar PIN de dureza

Nos casos em que um titular de cartão estiver sendo forçado a desbloquear uma porta, a capacidade de acionar um alarme de uma forma não óbvia pode ajudar a garantir a segurança desse funcionário. O *PIN de dureza*concederá a entrada ao gerar um evento *PIN de dureza inserido*, que pode ser usado para acionar ações do sistema.

O que você deve saber

O *PIN de dureza* requer Security Center 5.7 SR2, Synergis™ Softwire 10.7 e leitores definidos como Cartão e PIN.

Para indicar uma dureza, os titulares de cartão devem apresentar crachá e inserir seu PIN regular + 1 ao último dígito. Por exemplo, se o PIN regular for 1234, o PIN de dureza será 1235. Se o último dígito for um 9, ele se tornará um 0; por exemplo, 9999 se tornaria 9990.

Para habilitar o PIN de dureza:

1 Na Página inicial do Config Tool, abra a tarefa **Visualização da área**.
2 Selecione a área que deseja modificar e clique em **Avançado**.
3 Em *PIN de dureza*, defina a barra de **Status**como **Ligado**.
4 Clique em **Aplicar**.
Quaisquer alterações feitas às configurações do *PIN de dureza* são identificadas no relatório *Trilhas de auditoria*.

Sobre regras de acesso

É um tipo de entidade que define uma lista de titulares de cartão a quem o acesso é dado ou negado com base em um cronograma. Uma regra de acesso pode ser aplicada a uma área protegida ou a um ponto de acesso.

Uma regra de acesso contém os três Qs:

- Quem? (Quem pode passar — *titulares de cartão* ou *grupos de titulares de cartão*)
- Quê? (Se o acesso é concedido ou negado)
- Quando? (O *agenda* quando a regra de acesso é aplicada)

Essa lógica é diferente de outras soluções de controle de acesso, onde um nível de acesso define *onde* e *quando* alguém pode ter acesso.

As regras de acesso que foram transmitidas para os controladores de portas (chamadas *unidades de controle de acesso* em Security Center) não precisam ser modificadas. Se você associar uma nova credencial a um titular de cartão, a regra antiga ainda é válida.

Regras de acesso permanente x temporário

As regras de acesso são ou permanentes ou temporárias. É uma regra de acesso que tem uma hora de ativação e término. Regras de acesso temporário são adequadas para situações em que titulares de cartão permanentes precisam de acesso temporário ou sazonal a áreas restritas. Essas regras de acesso são automaticamente excluídas sete dias após o término para evitar que o sistema fique sobrecarregado.

Exemplos de casos de uso típico de regras de acesso temporário incluem titulares de cartão sazonais, como alunos que precisam acessar um laboratório durante o semestre e titulares de cartão permanentes que precisam de acesso de curto prazo a uma área restrita, como técnicos de manutenção que precisam trabalhar em servidores de armazenamento em um data center altamente seguro.

A partir da tarefa de *Gerenciamento de titulares de cartão* , é possível designar uma regra de acesso temporário a um titular de cartão por vez. Para designar uma regra de acesso temporário a múltiplos titulares de cartão ou grupos de titulares de cartão, é necessário atualizar as propriedades de regras de acesso em Config Tool.

Limitações

Regras de acesso temporário funcionam com unidades HID e Synergis™ . No entanto, somente unidades Synergis™ podem aplicar regras de acesso temporário enquanto opera offline (desconectado do Access Manager). Para unidades HID funcionarem com regras de acesso temporário, o controlador deve estar sempre conectado ao Access Manager e a sincronização deve estar sempre definida em *Automaticamente*. A ativação de regras de acesso temporário é imediata devido à pesquisa de host. Entretanto, o término de uma regra de acesso temporário somente entra em vigor após a sincronização com o Access Manager.

Tópicos relacionados

Sobre o Security Center Synergis na página 590

Criar regras de acesso

Para controlar o acesso em qualquer local da sua localização, você deve criar regras de acesso que serão aplicadas às áreas, portas e elevadores.

Antes de iniciar

Crie as agendas que se aplicarão a esta regra de acesso.

O que você deve saber

Como prática recomendada, use um nome descritivo ao criar novas regras de acesso para que você possa determinar facilmente o que cada regra faz (por exemplo "*Somente Técnicos de Laboratório*", "Todos os Funcionários em Horário Normal").

Para criar uma regra de acesso:

1 Na página inicial do Config Tool, abra a tarefa *Controle de acesso* e clique na visualização **Regras de acesso**.

2 Clique em **Regra de acesso** ( ).

3 Atribua um nome e uma descrição à regra de acesso.

4 Na lista suspensa **Partição**, selecione a partição na qual a regra de acesso será criada e clique em **Próximo**.

5 Selecione a agenda para quando você deseja que sua regra esteja ativa. O padrão é *Sempre*.

6 Selecione o tipo de regra que deseja (*Permanente* ou *Temporária*).

A regra de acesso Permanente é o padrão. É uma regra de acesso que tem uma hora de ativação e término. Regras de acesso temporário são adequadas para situações em que titulares de cartão permanentes precisam de acesso temporário ou sazonal a áreas restritas. Essas regras de acesso são automaticamente excluídas sete dias após o término para evitar que o sistema fique sobrecarregado.

7 Se você selecionar Temporário, especifique o seguinte:

- **Ativação:** Data e hora de ativação ou quando a regra de agendamento de regra se aplicar.
- **Validade:** Data e hora de vencimento ou quando a regra de agendamento deixar de se aplicar.

8 Clique em **Próximo**.

9 Revise o *Resumo de criação* e clique em **Criar** > **Fechar.**

10 Selecione a regra de acesso criada e clique em **Propriedades**.

11 Selecione se pretende **conceder acesso** ou **negar acesso** quando a regra estiver ativa.

MELHOR PRÁTICA: Geralmente, os agendamentos são usados para conceder acesso. O acesso é negado quando os agendamentos estão inativos. Use agendas explícitas de **negação** apenas para exceções.

12 Na seção *Titulares de cartão afetados por esta regra*, clique em **Adicionar um item** ( ), selecione os titulares de cartão ou grupos de titulares de cartão aos quais a regra de acesso se aplica e clique em **Adicionar**.

MELHOR PRÁTICA:

Crie grupos de titulares de cartões em vez de titulares de cartões individuais, pois isso se torna muito mais gerenciável em grandes sistemas à medida que mais pessoas vão e vêm.

13 Clique em **Aplicar**.

Após terminar

Atribua a regra de acesso a áreas protegidas, portas e elevadores para que a regra de acesso fique operacional.

32

Titulares de cartão

Esta seção inclui os seguintes tópicos:

- "Sobre os titulares de cartão" na página 646
- "Criar grupos de titulares de cartão" na página 647
- "Criando titulares de cartão" na página 648
- "Cortar imagens" na página 653
- "Aplicar fundos transparentes a imagens" na página 654
- "Definir o tamanho máximo de arquivos de imagem" na página 656
- "Atribuição de credenciais" na página 657
- "Configurar estações de codificação de smart cards" na página 663
- "Configurar perfis de credencial móvel" na página 665
- "Modificar titulares de cartão importados de um Active Directory" na página 667
- "Selecionar quais campos do titular de cartão sincronizar com o Active Directory" na página 669
- "Utilizar coletores de assinatura" na página 670
- "Receber notificações quando os portadores de cartão estiverem para expirar" na página 671

Sobre os titulares de cartão

É um tipo de entidade que representa uma pessoa que pode entrar e sair das áreas protegidas por ter suas credenciais (normalmente cartões de acesso) e cujas atividades podem ser rastreadas. Eles são o *Quem* em uma regra de acesso.

Grupos de titulares

A entidade *grupo de titulares de cartão* é usada para configurar os *direitos de acesso* e as propriedades comuns de um grupo de titulares de cartão.

Se você tiver um grande sistema de controle de acesso, os titulares de cartão e as regras de acesso serão muito mais fáceis de gerenciar quando os titular de cartão são membros de grupos de titulares de cartão.

Criar grupos de titulares de cartão

Para configurar os direitos de acesso e as propriedades comuns a um grupo de titulares de cartões, é possível criar grupos de titulares de cartões.

O que você deve saber

Se você tiver um grande sistema de controle de acesso, os titulares de cartão e as regras de acesso serão muito mais fáceis de gerenciar quando os titular de cartão são membros de grupos de titulares de cartão.

Para criar um grupo de titulares de cartão:

1. Abra a tarefa **Controle de acesso** e clique na visualização **Grupos de titulares de cartão**.
2. Clique em **Grupo de titulares de cartão** ( ).

   Um novo grupo de portadores de cartões aparece na árvore de entidades.
3. Digite um nome para o grupo e pressione **ENTER**.
4. Selecione o grupo de titulares de cartão e clique na aba **Propriedades**.
5. Na parte inferior da página, clique em para adicionar portadores de cartão individuais ou grupos de portadores de cartão ao seu novo grupo.
6. Clique em **Aplicar**.

Criando titulares de cartão

Para adicionar novos funcionários que devem entrar e sair de áreas protegidas usando cartões de acesso e rastrear suas atividades, é possível criar titulares de cartão, usando a tarefa *Gerenciamento de titulares de cartão* .

Antes de iniciar

- Definir o tamanho de arquivo máximo de imagens de titulares de cartão.
- Para adicionar informações personalizadas a titulares de cartão, crie campos personalizados.
- Se precisar de diferentes grupos de titulares de cartão com diferentes direitos de acesso, crie grupos de titulares de cartão.

O que você deve saber

Em vez de criar titulares de cartão manualmente, é possível importá-los de um arquivo CSVou do Active Directory da sua empresa.

Para criar um titular de cartão:

1 Abra a tarefa *Gerenciamento de titulares de cartões* e clique em **Criar novo titular de cartão** ( ).

2 Na parte superior da caixa de diálogo, digite o nome e sobrenome do titular de cartão.

3 Para atribuir uma foto ao titular de cartão, clique na silhueta e selecione uma das seguintes opções:

- **Carregar do arquivo:** Selecionar uma imagem do disco: Todos os formatos de imagem padrão são compatíveis.
- **Carregar a partir da câmera Web:** Tire uma foto instantânea com sua câmera Web. Esta opção aparece somente se você tiver uma câmera web vinculada a sua estação de trabalho.
- **Carregar da câmera:** Tire uma foto instantânea de uma câmera gerenciada pelo Security Center. Se selecionar **Carregar da câmera**, aparecerá uma caixa de diálogo de captura separada. Selecione a fonte de vídeo e clique em **Tirar uma foto instantânea** ( ).
- **Carregar da área de transferênci:a:** Carregar a imagem copiada para a área de transferência. Esta opção aparece somente se tiver usado o comando de copiar do Windows para salvar uma imagem na área de transferência.

4 Para editar a imagem, clique para abrir o *Editor de imagem* e use as opções de edição na parte superior da caixa de diálogo do editor.

5 Na seção *Status*, defina:

- **Status:** Define o status para *Ativo* ou *Inativo*. Para as credenciais funcionarem, e para ter acesso a qualquer área, o status deve estar *Ativo*.
- **Ativação:** Se, no momento, o status estiver definido como *Inativo*, defina data e hora para ativar seu perfil.
- **Validade:** Defina uma data de vencimento para o perfil:
  - **Nunca:** Nunca vence.
  - **Data específica:** Vence em uma data e horário específicos.
  - **Definir vencimento no primeiro uso:** Vence após um número específico de dias depois do primeiro uso.
  - **Quando não é usado:** Vence quando não foi utilizado durante um número específico de dias.

6 Atribuir uma credencial ao titular de cartão para que possam acessar áreas protegidas.

NOTA: É possível atribuir uma credencial agora ou depois que todas as credenciais tiverem sido inseridas no sistema.

7 Atribua o titular de cartão a um *grupo de titulares de cartão*.

NOTA: Um titular de cartão pode pertencer a mais de um grupo de titular de cartão.

a) Para atribuir o primeiro grupo de titular de cartão, clique na lista suspensa **Grupo de titulares de cartão** e selecione o grupo.

b) Para atribuir grupos de titulares adicionais, clique em **Avançado** ( ), depois clique em **Adicionar um item** ( ). Na caixa de diálogo que aparecer, selecione os grupos de titulares de cartão e clique em **OK**.

8 Digite o endereço de e-mail do titular de cartão.

É necessário um endereço de e-mail válido se quiser atribuir *credenciais móveis* ao titular de cartão.

9 (Opcional) Se campos personalizados são definidos para titulares de cartão, como departamento, números de telefone, etc., digite as informações adicionais.

10 (Opcional) Na seção *Avançado* , configure as seguintes propriedades do titular de cartão:

NOTA: Algumas dessas propriedades podem ser herdadas dos grupos de titulares de cartão principais. Quando um valor especificado é configurado para o titular de cartão, clique em **Reverter para o valor herdado** ( ) para herdar a propriedade do grupo de titulares principal. Se existirem vários grupos principais, é herdado o valor privilegiado mais alto.

a) Se o titular de cartão recebeu uma credencial, conceda privilégios de acesso ao titular de cartão:

- **Usar tempo de concessão estendido:** Concede mais tempo para passar pelas portas onde o parâmetro do *tempo de concessão estendido* estiver configurado para uma porta. Use esta opção para quem tiver mobilidade reduzida.
- **Desconsiderar as regras antirretorno:** Isenta de todas as restrições antirretorno.

b) No campo **Autorização de segurança** , digite o nível de autorização de segurança do titular de cartão. O nível de autorização de segurança determina o acesso a áreas onde há um nível de ameaça definido no Security Center. O nível 0 é o nível de autorização mais alto, com mais privilégios.

c) No campo **Nome da entidade** , digite um nome para a entidade do titular de cartão, caso não queira usar o nome do titular.

Por padrão, o **Nome da entidade** usa os campos **Nome** e **Sobrenome** .

d) No campo **Descrição** , digite uma descrição para o titular do cartão.

e) Atribuir o titular do cartão a uma *partição*.

As partições determinam quais usuários do Security Center têm acesso a essa entidade. Somente usuários que receberam acesso à partição podem visualizar o titular de cartão.

11 Clique em **Salvar**.

Exemplo

Assista a este vídeo para saber mais. Clique no ícone **Legendas** (**CC**) para ligar a legenda do vídeo em um dos idiomas disponíveis. O vídeo pode não ser exibido no Internet Explorer. Para resolver isso, abra as **Configurações de compatibilidade de exibição** e limpe **Exibir sites da intranet em Visualizar compatibilidade**.

Após terminar

Atribuir regras de acesso ao titular de cartão.

Tópicos relacionados

Cortar imagens na página 653
Aplicar fundos transparentes a imagens na página 654

Criar portas na página 616
Configurar áreas protegidas na página 631

Atribuir regras de acesso a titulares de cartão

Para conceder ou negar acesso a um titular de cartão para acessar áreas, portas e elevadores, é preciso atribuir regras de acesso a eles.

Antes de iniciar

Criar regras de acesso.

O que você deve saber

É possível atribuir regras de acesso enquanto se cria titulares de cartão ou depois que forem criados. Neste procedimento, supõe-se que um titular de cartão já foi criado.

MELHOR PRÁTICA: Atribua regras de acesso a grupos de titulares de cartão, em vez de titulares individuais. Atribua regras de acesso a titulares de cartão individuais somente como medida temporária. Quando usado com muita frequência, o sistema de controle de acesso pode se tornar difícil de ser gerenciado rapidamente. Se precisar conceder acesso temporário ou de curto prazo a um titular do cartão, crie um *regra de acesso temporário*.

Para atribuir regras de acesso a um titular de cartão:

1 Na tarefa *Gerenciamento de titulares de cartão* , selecione um titular de cartão e depois clique em **Modificar** ( ).

2 Clique na aba **Regras de acesso** ( ) > **Adicionar** ( ).

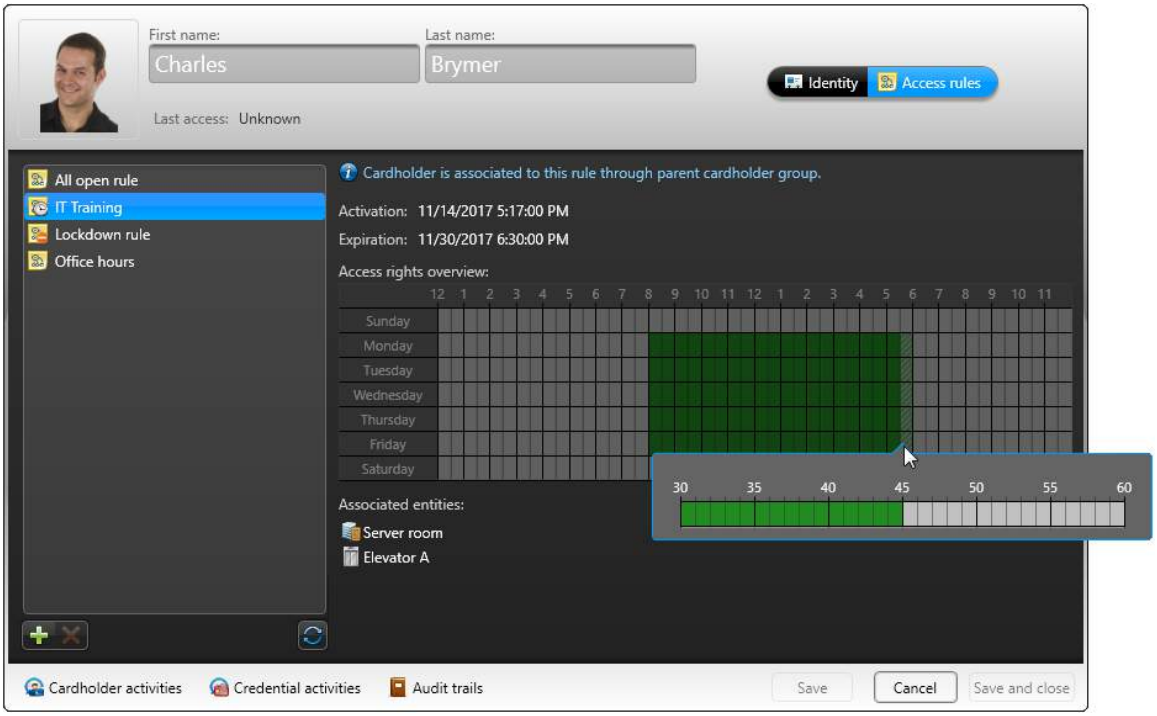
Uma caixa de diálogo listando as regras de acesso que ainda não foram atribuídas a esse titular de cartão abre.

3 Fazer um dos seguintes:

- Selecione a regra que deseja adicionar e clique em **Adicionar**.
- Crie e atribua uma regra de acesso temporário.

4 Selecione a regra de acesso da lista.

O agendamento que se aplica à regra de acesso é mostrado em uma grade à direita. Cada bloco de tempo representa 30 minutos. Áreas verdes indicam períodos quando o acesso é concedido pela regra. Áreas vermelhas indicam períodos quando o acesso é negado pela regra. Áreas cinzas são os horários não especificados pelo agendamento, por isso, o acesso é negado. Se for uma regra de acesso temporário ( ), os horários de ativação e término estão indicados. Áreas, portas e elevadores com os quais as regras estão associadas estão listados na parte de baixo.



5 Para visualizar um bloco de tempo parcial (hachurado) em minutos, clique e segure o botão esquerdo do mouse.

6 Para atribuir outra regra de acesso ao titular de cartão, clique em .

7 Para remover uma regra de acesso diretamente atribuída ao titular de cartão, clique em .
Não é possível remover *Toda regra aberta*ou a *Regra para travar*.

8 Clique em **Salvar**.

Exemplo

Assista a este vídeo para saber mais. Clique no ícone **Legendas** (**CC**) para ligar a legenda do vídeo em um dos idiomas disponíveis. O vídeo pode não ser exibido no Internet Explorer. Para resolver isso, abra as **Configurações de compatibilidade de exibição** e limpe **Exibir sites da intranet em Visualizar compatibilidade**.

Após terminar

Atribuir uma credencial ao titular de cartão.

Atribuindo regras de acesso temporárias a titulares de cartão

Para se adaptar a titulares de cartão sazonais, como alunos que estão matriculados durante um semestre ou titulares de cartão permanentes que precisam de acesso de curto prazo a uma área restrita, é possível criar e atribuir regras de acesso temporário.

O que você deve saber

É uma regra de acesso que tem uma hora de ativação e término. Regras de acesso temporário são adequadas para situações em que titulares de cartão permanentes precisam de acesso temporário ou sazonal a áreas restritas. Essas regras de acesso são automaticamente excluídas sete dias após o término para evitar que o sistema fique sobrecarregado.

NOTA: A partir da tarefa de *Gerenciamento de titulares de cartão* , é possível designar uma regra de acesso temporário a um titular de cartão por vez. Para designar uma regra de acesso temporário a múltiplos titulares de cartão ou grupos de titulares de cartão, é necessário atualizar as propriedades de regras de acesso em Config Tool. Para usuários Security Desk conseguirem criar regras de acesso temporário, é necessário conceder o privilégio *Adicionar regras de acesso* .

Para atribuir regras de acesso temporário a um titular de cartão:

1 Na tarefa *Gerenciamento de titulares de cartão* , selecione um titular de cartão e depois clique em **Modificar** ( ).

2 Clique na aba **Regras de acesso** ( ) > **Adicionar** ( ).

Uma caixa de diálogo listando as regras de acesso que ainda não foram atribuídas a esse titular de cartão abre.

3 Fazer um dos seguintes:

- Selecionar uma regra de acesso temporário existente ( ) e clicar em **Adicionar**.
- Clique em **Regra de acesso temporário** ( ).

  O assistente de criação de regra de acesso temporário abre.

4 Na página *Informações básicas* , insira um nome de regra e uma descrição, e depois clique em **Próximo**.

5 Na página de *Informações de regras de acesso* , faça uma das seguintes ações:

- Clique em **Use uma regra de acesso existente como modelo**, depois selecione da lista suspensa de **Regras de acesso** , a regra de acesso que deseja usar como modelo.

  O agendamento e as entidades associadas serão copiadas para a sua regra de acesso temporário.
- Clique em **Especifique parâmetros de acesso personalizado**e especifique os itens que seguem:
  - **Acesso a:** Expandir a visualização da área e selecionar as entidades às quais deseja acesso.
  - **Ativação:** Data e hora de ativação ou quando a regra de agendamento de regra se aplicar.
  - **Validade:** Data e hora de vencimento ou quando a regra de agendamento deixar de se aplicar.
  - **Cronograma:** Escolha quando essa regra de acesso estiver ativada.

6 Clique em **Próximo** > **Criar**.

Uma regra de acesso temporário ( ) é criada e atribuída ao seu titular de cartão.

7 Clique em **Salvar**.

Após terminar

(Opcional) Atribua a regra de acesso temporário criada aos outros titulares de cartão.

Cortar imagens

Para cortar uma área de uma imagem do titular ou visitante e se concentrar na parte da imagem que você gostaria de manter, você pode recortar a imagem usando o *Editor de imagens*.

Para cortar uma imagem:

1 Clique na imagem.

2 No *Editor de imagens*, clique na aba **Cortar** ( ).

3 Na imagem, clique e arraste o ícone para cortar a imagem.

4 Para ajustar a área de corte, faça um dos seguintes:

- Use os ícones azuis na imagem para ajustar a área de corte.
- Na parte inferior da caixa de diálogo *Editor de imagem*, use os valores de **Largura** e **Altura** para redimensionar a área de corte. Os valores de largura e altura podem ser em pixels, polegadas ou milímetros.

5 Para reverter a imagem para o seu estado original, clique em **Redefinir**.

6 Clique em **Aplicar**.

Exemplo

Assista a este vídeo para saber mais. Clique no ícone **Legendas** (**CC**) para ligar a legenda do vídeo em um dos idiomas disponíveis. O vídeo pode não ser exibido no Internet Explorer. Para resolver isso, abra as **Configurações de compatibilidade de exibição** e limpe **Exibir sites da intranet em Visualizar compatibilidade**.

Aplicar fundos transparentes a imagens

Se a imagem de um titular de cartão ou de um visitante foi tirada na frente de uma tela de chroma key, você pode tornar o plano de fundo transparente. Isso é útil se você criar um modelo de crachá que tenha uma imagem em segundo plano.

O que você deve saber

Você também pode definir a transparência e a cor dos fundos de imagens de titulares de cartão na ferramenta Importar, para que possa utilizar as mesmas configurações ao importar várias imagens de titulares de cartão.

Para aplicar um fundo transparente em uma foto:

1 Clique na imagem.

2 No *Editor de imagem*, clique na aba ***Transparência***.

O cursor muda para a ferramenta conta-gotas quando você aponta para a imagem.

3 Clique no fundo onde está a cor do croma (geralmente verde ou azul).

4 Usando o controle deslizante de **Tolerância**, ajuste a porcentagem de transparência.

5 Para reverter a imagem para o seu estado original, clique em **Redefinir**.

6 Clique em **Salvar**.

Exemplo

Assista a este vídeo para saber mais. Clique no ícone **Legendas** (**CC**) para ligar a legenda do vídeo em um dos idiomas disponíveis. O vídeo pode não ser exibido no Internet Explorer. Para resolver isso, abra as **Configurações de compatibilidade de exibição** e limpe **Exibir sites da intranet em Visualizar compatibilidade**.

Definir o tamanho máximo de arquivos de imagem

Para melhorar a nitidez das imagens do titular de cartão e do visitante, você pode aumentar o tamanho máximo de arquivo das imagens que são armazenadas no banco de dados do Directory.

O que você deve saber

O tamanho máximo de arquivo é aplicável a imagens de titulares de cartão e visitantes e a todos os campos de dados de imagem no Security Center. Esta configuração também se aplica ao *Ferramenta de importação* e pode ser modificada ao executar esta ferramenta. Ao carregar arquivos de imagem, o Security Center reduz automaticamente o tamanho da imagem para que o tamanho do arquivo fique abaixo do limite definido.

O valor padrão é 20 KB. Você pode definir o limite em qualquer ponto entre 20 e 5000 KB.

Para definir o tamanho de arquivo máximo de imagens:

1 Abra a tarefa *Controle de acesso* e clique na visualização **Configurações gerais**.
2 Na opção **Tamanho máximo de arquivo de imagem**, defina o número máximo de kilobytes.
3 Clique em **Aplicar**.

O novo limite será aplicado a todas as futuras atualizações de campos de imagem.

Tópicos relacionados

Importar titulares de cartão e credenciais na página 718

Atribuição de credenciais

Para conceder a titulares de cartão ou visitantes acesso a áreas protegidas, é necessário atribuir credenciais a eles.

O que você deve saber

Os titulares de cartão e visitantes podem ser atribuídos a múltiplas *credenciais*. É possível atribuir credenciais enquanto se cria um novo titular de cartão ou visitante (exceto para *credenciais móveis*), ou após terem sido criados. Neste procedimento, supõe-se que os titulares de cartão já foram criados.

Para atribuir credenciais:

1 Fazer um dos seguintes:

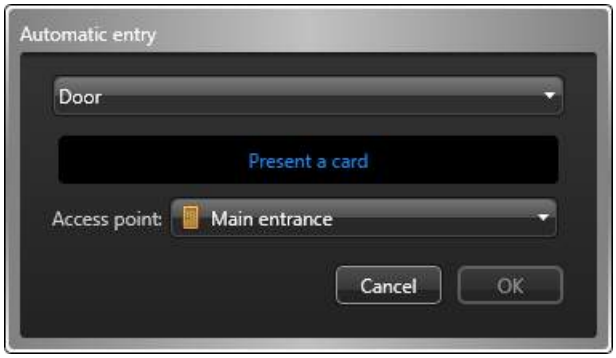
- Para titulares de cartão, abra a tarefa *Gerenciamento de titulares de cartão* , selecione um titular de cartão e depois clique em **Modificar** ( ).
- Para visitantes, abra a tarefa *Gerenciamento de visitantes* , selecione um visitante e depois clique em **Modificar** ( ).

2 Na seção *Credencial* , clique em **Adicionar uma credencial** ( ).

3 Selecione uma das seguintes opções:

- **Entrada automática:** Apresentar o cartão a um leitor.
- **Entrada manual:** Digite manualmente os dados do cartão. Use este método quando não tiver um leitor de cartão por perto.
- **Credencial existente:** Selecione uma credencial não atribuída, pré-registrada
- **PIN:** Crie uma credencial com PIN.
- **Placa de licença:** Digite um número de placa de licença do titular do cartão. Utilize esse método se uma câmera Sharp for utilizada para acionar uma barreira de acesso de veículos. Nesse caso, a placa de veículo do titular do cartão pode ser usada como credencial.
- **Solicitar cartão:** Solicitar um cartão de credencial para o titular ou visitante. Use este método quando não tiver uma impressora no local.
- **Credencial móvel:** Solicitar uma credencial móvel para titular de cartão ou visitante. É necessário ter um provedor de credenciais móveis configurado e leitores de credenciais móveis instalados. O titular de cartão deve ter um endereço de e-mail válido configurado.
- **Credencial em papel (impressa):** Imprimir um crachá(etiqueta com nome ou identidade com foto) sem atribuir uma credencial. A credencial de papel não pode ser usada para abrir portas. É usado somente para identificar visualmente o titular do cartão ou o visitante.

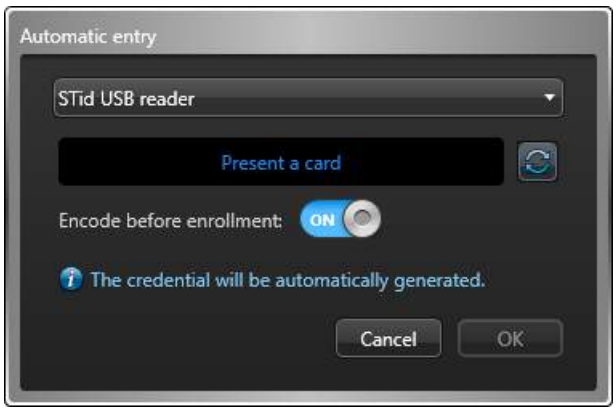
4 Se selecionar **Entrada automática**, depois é necessário selecionar um leitor (USB ou uma porta) e apresentar o cartão no leitor.



Se você tem um leitor decodificador de smart card instalado, defina a opção **Codificar antes da inscrição** para **INATIVO** para ler um cartão pré-codificado.

Quando o LED do leitor fica verde (pronto para ler), coloque o smart card no leitor. O LED do leitor fica amarelo e depois verde com um som curto antes de desligar.

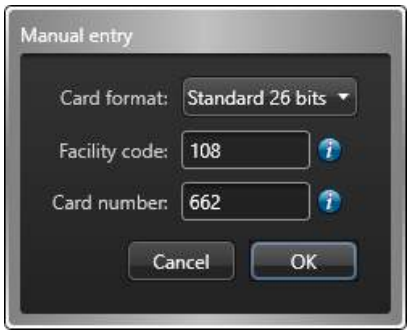
Se deseja gerar e codificar em seu cartão uma credencial aleatória de 128 bits MIFARE DESFire antes da inscrição, configure a opção **Codificar antes da inscrição** como **ATIVO**.



Quando o LED do leitor fica vermelho (pronto para codificar), coloque o smart card no leitor por aproximadamente 2 segundos. O LED do leitor fica amarelo e depois verde com um som curto antes de desligar. Se você ouvir um bip longo e o LED permanecer vermelho, tente novamente.

A caixa de diálogo fecha automaticamente após um cartão elegível ser apresentado. Se o cartão não tiver sido instalado, ele é instalado automaticamente. Se já estiver atribuído a alguém, ele será rejeitado.

5 Se selecionar **Entrada manual**, é necessário selecionar um formato de cartão, inserir os campos de dados necessários e clicar em **OK**.

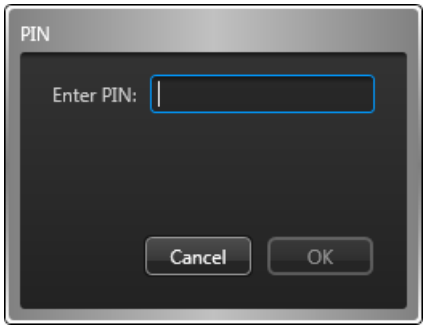


CUIDADO: Cuidado ao digitar os dados do cartão, porque o sistema não pode validar caso os dados inseridos correspondam a um cartão físico ou não.

Se o cartão não tiver sido instalado, ele é instalado automaticamente. Se já estiver atribuído a alguém, ele será rejeitado.

6 Se selecionar **Credencial existente**, aparece uma caixa de diálogo listando todas as credenciais existentes, mas não atribuídas no sistema. Selecione uma credencial não atribuída da lista e clique em **OK**.

7 Se selecionar **PIN**, é necessário fazer o seguinte:

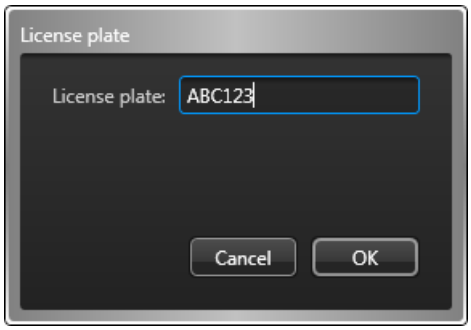


a) Entre o PIN como um valor numérico.

NOTA: Não ultrapasse o número de dígitos aceitos por seus leitores. Um comprimento comum de PIN é de cinco dígitos. Mas alguns modelos aceitam até 15 dígitos.

b) Clique em **OK**.

8 Se selecionar **Placa de licença**, é necessário fazer o seguinte:

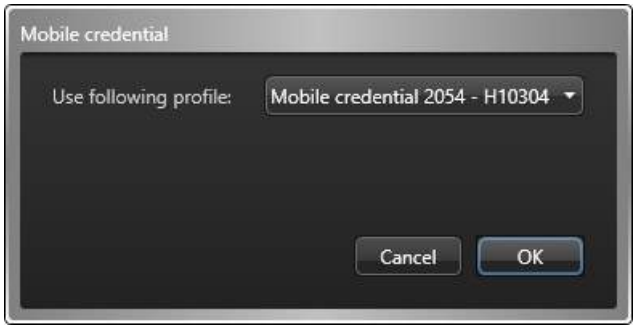


a) Entre o número da placa de licença.

NOTA: Não é necessário entrar espaços que aparecem no número da placa. O sistema trata “ABC123” e “ABC 123” como a mesma placa.

b) Clique em **OK**.

9 Se selecionar **Credencial móvel**, é necessário fazer o seguinte:



a) Selecionar o perfil de credencial (se existir mais de um).

É possível atribuir uma credencial móvel de cada perfil a cada titular de cartão.

b) Clique em **OK**.

NOTA: Um convite por e-mail é enviado ao titular de cartão com um link para baixar o aplicativo de credencial móvel. O titular de cartão deve aceitar o convite para a credencial ser *ativada* no seu telefone. Se o titular de cartão recusar o convite ou o convite expirar, a credencial continua *inutilizada*, e o provedor de credencial móvel pode atribui-la ao próximo titular de cartão que precisar de uma. Security Center não sabe que a credencial móvel solicitada não foi aceita pelo titular de cartão até que a mesma credencial

móvel tenha sido atribuída a outra pessoa, momento em que, Security Center remove automaticamente do titular de cartão atual.

IMPORTANTE: Uma credencial móvel que foi ativada (emparelhada com um telefone) nunca poderá ser reutilizada em outro telefone. Se um titular de cartão perder seu telefone ou precisar mudar de telefone, precisa informar o operador Security Center , que deve excluir a credencial ou marcar como *perdida*. Depois disso, o operador deve entrar no portal do provedor de credenciais e *revogar* a credencial móvel.

10 Depois que a credencial for atribuída, ela aparece na seção *Credencial* .

O nome e status da credencial são exibidos. *Ativo* indica que a credencial está atribuída.

NOTA: Se a credencial é um PIN, o ícone de teclado é exibido. Se a credencial é uma placa de licença, um ícone de placa é exibido. Se a credencial for um cartão, um *modelo de crachá* padrão é atribuído e é exibida uma visualização da impressão do crachá em vez do ícone da credencial.

11 (Opcional) Se a credencial é um cartão, selecione um modelo de crachá diferente conforme as seguintes instruções.

a) Na seção *Credencial* , clicar na imagem do crachá.
b) Selecione um modelo de crachá e clique em **OK**.

Aparece uma visualização de impressão do crachá, com os dados correspondentes ao titular de cartão atual ou visitante e sua credencial.

12 Clique em **Salvar**.

É necessário salvar todas as suas mudanças antes de poder imprimir o crachá.

13 Para imprimir o crachá, clique em **Imprimir crachá** ao lado da visualização do crachá.

Tópicos relacionados

Projetar modelos de crachá na página 695
Configurar perfis de credencial móvel na página 665

Solicitar cartões de credencial

Quando não tiver cartões de credencial em posse, é possível solicitar que os cartões de credencial a serem atribuídos, por outra pessoa, aos titulares de cartão e visitantes que você está gerenciando.

O que você deve saber

É possível solicitar um cartão enquanto se cria um novo titular de cartão ou visitante ou depois que forem criados. Neste procedimento, supõe-se que um titular de cartão ou visitante já foi criado.

NOTA: É possível gerenciar somente os visitantes no Security Desk.

Para solicitar um cartão de credencial:

1 Fazer um dos seguintes:

- Para titulares de cartão, abra a tarefa **Gerenciamento de titulares de cartão** , selecione um titular de cartão e depois clique em **Modificar** ( ).
- Para visitantes, abra a tarefa **Gerenciamento de visitantes** , selecione um visitante e clique em **Modificar** ( ).

2 Na seção *Credencial* , clique em **Adicionar uma credencial** ( ).

3 No menu suspenso, clique em **Solicitar cartão**.

4 Na caixa de diálogo **Solicitar cartão** , selecione o motivo pelo qual está solicitando um cartão.

NOTA: As razões para solicitação de um cartão aparecem somente se o seu administrador tiver criado razões possíveis no Config Tool.

5 Na lista suspensa **Modelo do crachá** , selecione um modelo de crachá.

É preciso selecionar um modelo de crachá somente se quiser que um crachá seja impresso.

Uma visualização de impressão do crachá aparece.

6 Na opção **Ativar** , selecione quando ativar a credencial.
   - **Nunca:** A credencial nunca será ativada.
   - **Após inscrição:** Depois que outro usuário respondeu ao pedido do cartão.
   - **Ligado:** Selecione uma data específica para ativar a credencial
7 Se desejar receber um e-mail quando a credencial tiver sido impressa, selecione a opção **Envie um e-mail quando o cartão estiver pronto** .

   NOTA: Para que essa opção funcione, o seu usuário deve ter um endereço de e-mail válido.
8 Clique em **OK**.

   A credencial é exibida como **Solicitada** na seção *Credencial* da janela de detalhes do titular do cartão ou visitante.
9 Clique em **Salvar**.

O ícone **Solicitações de cartão** ( ) aparece na bandeja de notificação.

Tópicos relacionados

Projetar modelos de crachá na página 695
Adicionar motivos para solicitações de cartão de credencial na página 686
Responder a solicitações de cartão de credencial na página 687

Impressão de credenciais em papel

Quando não tiver credenciais atribuídas a titulares de cartão ou visitantes, é possível imprimir credenciais em papel (crachás sem dados de credencial) como etiquetas com nome ou identificação com foto para identificação visual.

Antes de iniciar

Adicione um modelo de crachá.

O que você deve saber

Para imprimir um crachá, é necessário um modelo de crachá. Um modelo de crachá é geralmente associado a uma credencial em cartão para que possa ser usado para destravar portas, mas também é possível imprimir um crachá sem qualquer dado de credencial (chamado de credencial em papel) que pode ser usado como uma etiqueta de nome ou uma identificação com foto para identificação visual.

É possível imprimir um crachá enquanto se cria um novo titular de cartão ou visitante ou depois que forem criados. Presume-se que o titular de cartão ou visitante já foi criado.

NOTA: É possível gerenciar somente os visitantes no Security Desk.

Para imprimir um crachá:

1 Fazer um dos seguintes:
   - Para titulares de cartão, abra a tarefa **Gerenciamento de titulares de cartão** , selecione um titular de cartão e depois clique em **Modificar** ( ).
   - Para visitantes, abra a tarefa **Gerenciamento de visitantes** , selecione um visitante e clique em **Modificar** ( ).
2 Na seção *Credencial* , clique em **Adicionar uma credencial** ( ).
3 No menu que aparecer, clique em **Credencial em papel (imprimir)**.

   Aparece a caixa de diálogo **Impressão do crachá** .
4 Na lista suspensa, selecione um modelo de crachá.

Uma visualização da impressão do crachá é mostrada. As informações do titular de cartão ou visitante podem ser mostradas no crachá, dependendo de como o modelo do crachá é criado. Nenhum dado de credencial é mostrado no crachá.

5 Para imprimir a credencial em papel, clique em **Imprimir crachá**.

Tópicos relacionados

Projetar modelos de crachá na página 695

Configurar estações de codificação de smart cards

Se você tiver um leitor de codificação USB STid, você pode configurar uma estação de codificação de smart card para gerar, codificar e registrar credenciais MIFARE DESFire, tudo a partir de um único local.

Antes de iniciar

- Certifique-se de que sua licença de software suporta as opções *Leitor de registros USB* e *Codificação de smart cards*.
- Selecione uma estação de trabalho do Security Desk como sua estação de codificação.
- Conecte o leitor de codificação USB à sua estação de codificação (consulte o *Guia de Integração do Synergis™ Softwire* para saber os modelos suportados).
- Tenha à sua disposição um cartão MIFARE DESFire e uma estação de trabalho equipada com o software *SECard* da STid para configurar o cartão MIFARE DESFire como o cartão Secure Key Bundle (SKB).

O que você deve saber

O cartão SKB contém um conjunto de chaves indexadas como um segredo compartilhado entre o leitor de codificação e os leitores nas portas. São necessárias três chaves para que a solução de codificação de smart cards funcione: a *Chave mestre de cartão*, a *Chave mestre de aplicativo* e a *Chave de leitura de aplicativo*. Os aplicativos do Security Center e as unidades Synergis™ só precisam saber onde estas três chaves estão armazenadas (índice de localização) nos smart cards, e não os valores das chaves. Essas informações são salvas em um arquivo de configuração chamado *SmartCardSites.xml*, que se encontra na pasta de instalação do Security Center.

Este arquivo de configuração vem com as seguintes configurações padrão prontas para uso:

- ID do aplicativo = 1
- Comunicação de arquivo = AES
- ID do arquivo = 1
- Deslocamento do arquivo = 0
- Comprimento do arquivo de credencial = 16 bytes (128 bits)
- Modo de comunicação de chave = Criptografado (encriptado)
- Índice de localização da chave mestre do cartão = 1 (no smart card)
- Índice de localização da chave mestre do aplicativo = 2 (no smart card)
- Índice de localização da chave de leitura do aplicativo = 3 (no smart card)
- Número da fechadura mestre do aplicativo = 0
- Número da fechadura de leitura do aplicativo = 1

Para configurar uma estação de codificação de smart cards:

1 Configure seu cartão SKB usando o software *SECard* da STid.

Fazer um dos seguintes:

- Se for uma nova instalação, configure o cartão MIFARE DESFire em branco como um cartão SKB. Use SECard para gerar chaves aleatórias e as configurações de chave padrão encontradas no arquivo *SmartCardSites.xml*.
- Se você tiver um cartão SKB existente que deseja usar, entre em contato com o seu representante da Genetec Inc. para ajudá-lo a configurar o arquivo *SmartCardSites.xml* para corresponder ao seu cartão SKB existente.

2 Abra o Security Desk e ative o leitor USB STid.

3 Transfira as chaves do cartão SKB para o leitor USB na sua estação de codificação.
   a) Abra a tarefa *Gerenciamento de credenciais* e clique em **Criar nova credencial** > **Inserção automática**.
   b) Selecione **Leitor USB STid** e defina **Codificar antes do registro** como **Desligado**.

   O LED do leitor fica verde (pronto para ler).
   c) Apresente o cartão SKB ao leitor por aproximadamente 3 segundos.
   O LED do leitor LED fica amarelo e depois verde quando as chaves são transferidas. Se ouvir um som longo, tente novamente.
   d) Clique em **Cancelar**.
4 Se não for uma nova instalação, e se você não estiver usando leitores STid em suas portas, termine aqui.
5 Faça o upload do arquivo *SmartCardsSites.xml* que se encontra na sua estação de codificação para as unidades Synergis™ que controlam os leitores de smart cards STid.
   Para obter mais detalhes sobre este procedimento, consulte o *Guia de Integração do Synergis™ Softwire*.
6 Transfira as chaves do cartão SKB para os leitores de smart cards nas portas.
   Vá para cada porta em sua instalação e apresente o cartão SKB em cada leitor de porta por aproximadamente 3 segundos para permitir que o leitor leia as credenciais MIFARE DESFire geradas pelo seu leitor de codificação.

Exemplo

Assista a este vídeo para saber mais. Clique no ícone **Legendas** (**CC**) para ligar a legenda do vídeo em um dos idiomas disponíveis. O vídeo pode não ser exibido no Internet Explorer. Para resolver isso, abra as **Configurações de compatibilidade de exibição** e limpe **Exibir sites da intranet em Visualizar compatibilidade**.

Após terminar

Gere, registre e atribua credenciais MIFARE DESFire aos seus titulares de cartão.

Configurar perfis de credencial móvel

Para atribuir credenciais móveis a titulares de cartão e visitantes, você deve primeiro adquirir o serviço de um provedor de credenciais móveis e configurar os perfis de credencial móvel no seu sistema.

Antes de iniciar

Certifique-se de ter adquirido um ou mais serviços de um provedor de credenciais móveis.

O que você deve saber

É uma credencial em um smartphone que utiliza tecnologia Bluetooth ou de Leitor de Comunicação de Campo Próximo (NFC) para acessar áreas protegidas. As credenciais móveis são como credenciais de cartão. Elas obedecem a formatos de credenciais padrão como *Padrão 26 bits* e *HID H10304 37 Bits*.

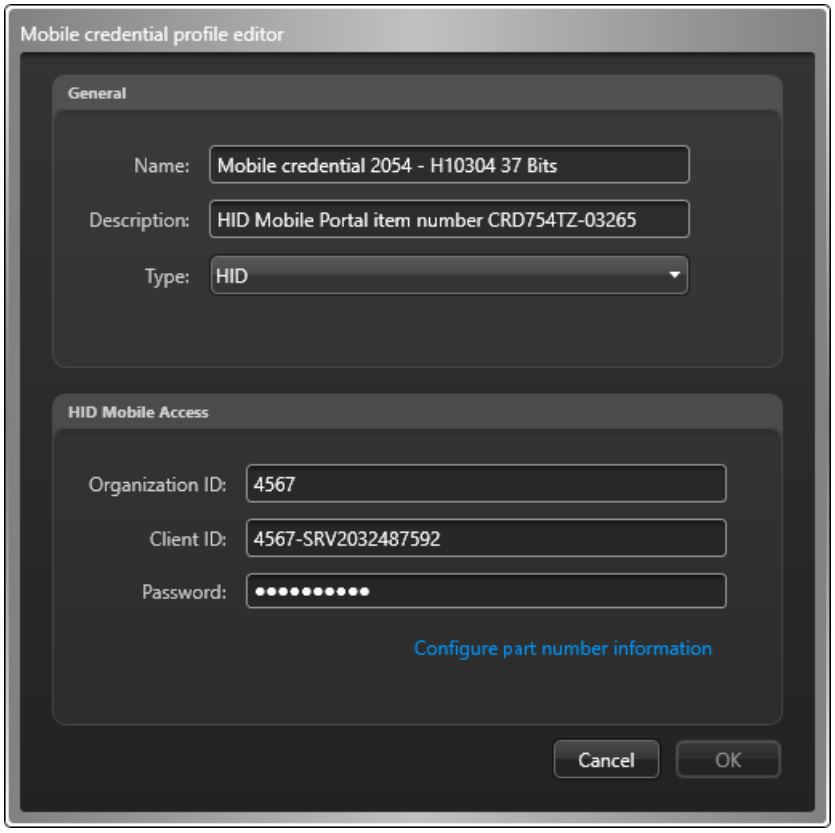
NOTA: Se a HID Global for o seu provedor de credenciais móveis, você deve adquirir um serviço (identificado por um *número de referência*) para cada formato de credencial que pretende suportar e especificar quantas credenciais pretende criar e o código de instalação que pretende usar. Para cada serviço que adquirir, você deve configurar um *perfil de credencial móvel* no Security Center. O HID Mobile Access Portal permite até 10 credencias móveis por celular e até 5 celulares por titular de cartão.

Para configurar um perfile de credencial móvel:

1 Abra a tarefa *Controle de acesso* e clique na visualização **Configurações gerais**.

2 Na seção *Provedor de credenciais móveis*, clique em **Adicionar um item** ( ).

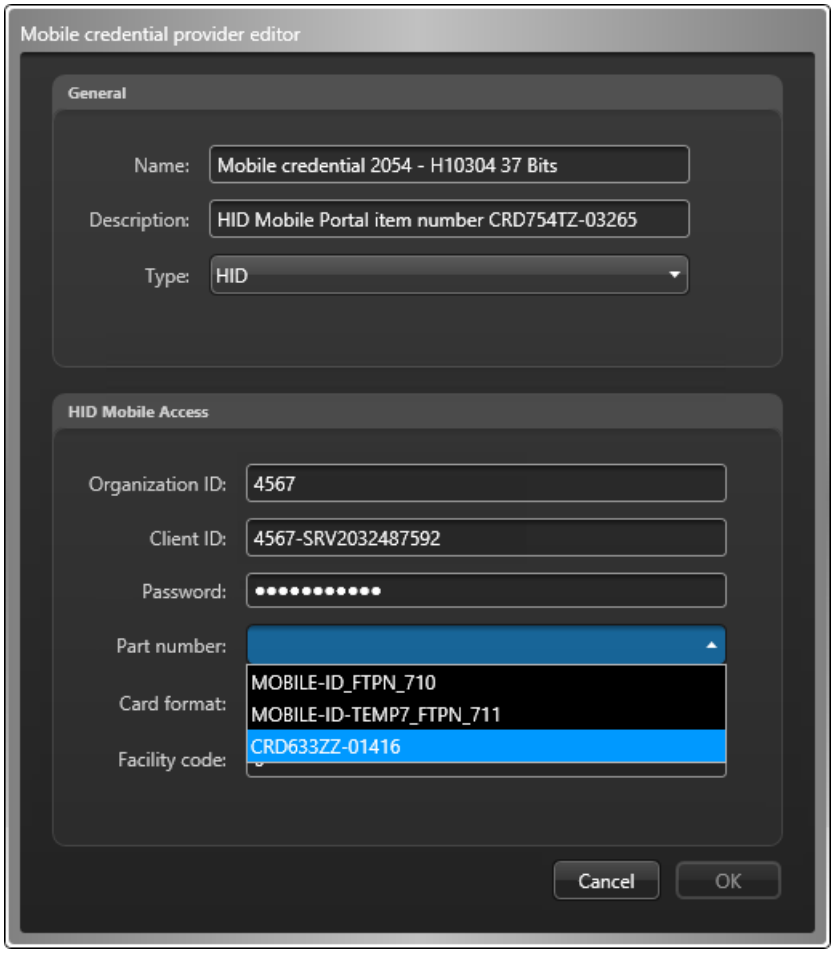
3 Na caixa de diálogo *Editor de provedor de credenciais móveis*, digite as seguintes informações:
A seguinte captura de tela ilustra os campos a preencher se o seu provedor for a HID Global.



- **Nome:** Nome usado para identificar esse perfil de credencial no Security Center. Sugerimos incluir o código da instalação e o formato do cartão no nome para ajudar o operador a escolher o perfil correto, se houver mais de um definido no sistema.
- **Descrição:** Descrição desse perfil.
- **Tipo:** Identifica o seu provedor de credencial móvel.
- **ID da organização:** ID numérica emitida para a sua empresa pela HID Global.
- **ID do Cliente:** ID do cliente associada à conta do sistema criada no portal de acesso da HID Mobile.
- **Senha:** Senha criada para a conta do sistema no portal de acesso da HID Mobile. Deve ter pelo menos 8 caracteres e conter letras maiúsculas e minúsculas e pelo menos um número e um símbolo.

4 Clique em **Configurar informações de número de referência** para obter os números de referência adquiridos no portal de credenciais móveis.

5 Selecione o **Número de referência** correspondente ao seu perfil de credencial e preencha o resto.



- **Número do componente:** Número do componente identificando o serviço comprado.
- **Formato do cartão:** Formato do cartão correspondente ao número do componente selecionado.
- **Código da instalação:** Código da instalação correspondente ao número do componente selecionado.

6 Clique em **OK** e, em seguida, clique em **Aplicar**.

Tópicos relacionados

Atribuição de credenciais na página 657

Modificar titulares de cartão importados de um Active Directory

Se você tiver titulares de cartão que são importados de um Active Directory, existem algumas propriedades do titular de cartão que você pode modificar no Security Center.

Você pode fazer as seguintes modificações:

- Atribuir imagens a titulares de cartão importados.
- Atribuir cartões temporários a titulares de cartão importados.
- Modificar o status de titulares de cartão importados.

Cartões temporários a titulares de cartão importados

Se um titular de cartão importado esquecer ou perder seu cartão, você pode atribuir um cartão temporário na tarefa *Gerenciamento de titulares* de cartão. Quando você atribui um cartão temporário, as credenciais ficam acinzentadas no Config Tool até que o cartão seja devolvido. Para mais informações sobre atribuir ou devolver cartões temporários, consulte o *Guia do Usuário do Security Desk*.

Atribuir imagens a titulares de cartão importados.

Você pode atribuir imagens a titulares de cartão importados do Security Center e sincronizar as imagens com o Active Directory.

Antes de iniciar

O campo *Imagem* do titular de cartão deve ser mapeado para o atributo *thumbnailPhoto* do AD.

Para atribuir uma imagem a um titular de cartão importado:

1 Na tarefa **Gerenciamento de titulares de cartão**, atribua uma imagem ao titular de cartão.
2 Abra a tarefa **Sistema** e clique na visualização **Funções**.
3 Selecione a função Active Directory e clique na aba **Links**.
4 Selecione a opção **Upload de imagens para o Active Directory** e defina o **Tamanho máximo do arquivo de imagem** (padrão=20 KB).
5 Clique em **Aplicar**.
6 Clique na aba **Propriedades** e, em seguida, clique em **Sincronizar agora**.

NOTA: Se o Security Center sincronizar com o AD com base em uma tarefa agendada, na próxima vez que a sincronização ocorrer a nova imagem do titular de cartão será sincronizada com o AD.

Modificar o status de titulares de cartão importados

Você pode modificar o status e a data de validade de um titular de cartão importado no Security Center. O titular do cartão torna-se dessincronizado com o AD.

Para modificar o status de titulares de cartão importados:

1 Abra a tarefa **Controle de acesso**.
2 Selecione um titular de cartão importado ( ) e clique na aba **Propriedades**.
3 Na seção **Status**, mova o controle deslizante de **Manter sincronizado** para **Substituir**.
4 Defina o status e a data de validade do titular do cartão:

- **Status:** Define o status para *Ativo* ou *Inativo*. Para as credenciais funcionarem, e para ter acesso a qualquer área, o status deve estar *Ativo*.
- **Ativação:** Exibe a data atual.
- **Validade:** Defina uma data de vencimento para o perfil:
  - **Nunca:** Nunca vence.
  - **Data específica:** Vence em uma data e horário específicos.
  - **Definir vencimento no primeiro uso:** Vence após um número específico de dias depois do primeiro uso.
  - **Quando não é usado:** Vence quando não foi utilizado durante um número específico de dias.

5 Clique em **Aplicar**.

O titular de cartão não está mais sincronizado com o AD. Ele só será sincronizado novamente depois de definir o status do titular de cartão como **Manter sincronizado**.

Selecionar quais campos do titular de cartão sincronizar com o Active Directory

Antes de sincronizar com o AD, é necessário selecionar quais atributos de titular de cartão deseja importar do AD, mapeando-os para os campos do Security Center na aba *Links* da função Active Directory. O mapeamento pode ser diferente para cada função Active Directory no seu sistema.

O que você deve saber

O campo de imagem do titular do cartão pode ser mapeado para qualquer atributo binário do AD se você quiser importá-los do AD. Porém, se você quiser fazer o upload de imagens do titular de cartão do Security Center para o AD, você deve mapeá-lo para o atributo *thumbnailPhoto* do AD.

Para mapear os atributos do AD para os campos de titular do cartão:

1 Na aba **Links** da função Active Directory, clique em **Adicionar um item** ( ).

2 Selecione um campo de titular de cartão do Security Center e um atributo do AD e clique em **OK**.

IMPORTANTE: O tipo de dado do campo Security Center deve corresponder ao do atributo do AD: texto com texto, decimal com decimal, data com data e assim por diante. O tipo de dado de imagem do Security Center deve ser mapeado para o tipo de dado binário do AD, e o atributo do AD mapeado deve conter uma imagem JPEG válida.

O novo mapeamento aparece na aba **Links**.

3 Repita os passos anteriores conforme necessário.

4 Se você estiver importando campos de credenciais de titular de cartão, faça o seguinte na aba **Links**:

- Na lista suspensa **Formato de cartão**, selecione o formato de cartão padrão a ser usado para as credenciais de titular de cartão importadas quando a propriedade de formato de cartão não estiver mapeada para um atributo do AD ou quando o atributo mapeado estiver vazio.
- Na lista suspensa **Modelo de crachá**, selecione um modelo de crachá padrão a ser usado para as credenciais de titular de cartão importadas.

5 Clique em **Aplicar**.

Os campos de titular de cartão mapeados são exibidos na aba **Links**. Quando você sincroniza com o AD, a maioria deles são somente leitura.

Tópicos relacionados

Integração com o Active Directory do Windows na página 384

Utilizar coletores de assinatura

Se você tiver um coletor de assinatura acoplado ao seu computador, você poderá usá-lo para capturar assinaturas de titulares de cartões e visitantes e salvá-las diretamente em um campo personalizado de assinatura criado anteriormente.

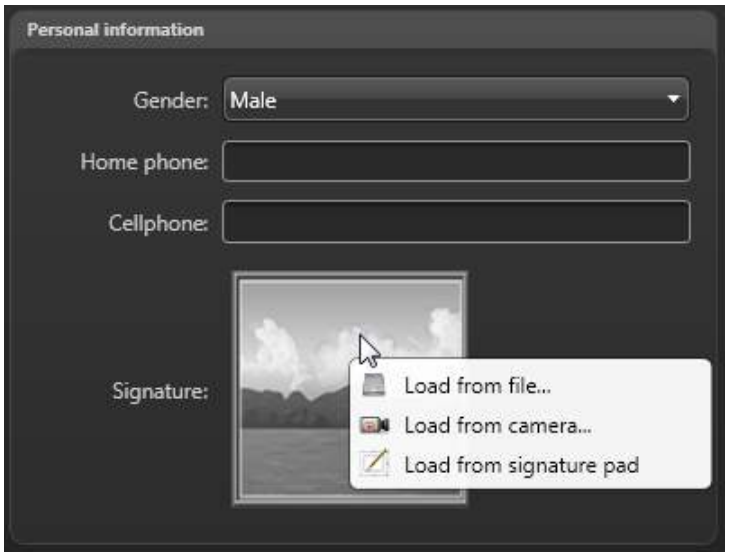
Antes de iniciar

- Certifique-se de que os campos personalizados de assinatura do titular de cartão e do visitante tenham sido criados com o tipo *Dados de imagem*.
- Instale um coletor de assinatura Topaz em seu computador e ative-o no Security Desk.

Para usar um coletor de assinaturas:

1 Abra a tarefa *Gerenciamento de titulares de cartão* ou *Gerenciamento de visitantes* para criar ou modificar o titular de cartão ou visitante.

2 Na caixa de diálogo de propriedades, clique no campo personalizado reservado para a assinatura e selecione **Carregar do coletor de assinatura**.



3 Entregue o coletor de assinatura ao titular de cartão ou visitante e peça para assinar.

A assinatura capturada aparece no campo de assinatura.

4 Clique em **Salvar**.

Receber notificações quando os portadores de cartão estiverem para expirar

Você pode configurar o Security Center para enviar a você ou a outro usuário um e-mail antes que os titulares de cartão ou suas credenciais expirem.

Antes de iniciar

Se você deseja que o usuário seja notificado por e-mail, verifique se ele tem um endereço de e-mail válido.

O que você deve saber

Os usuários podem ser notificados para cada titular de cartão ou credencial que esteja prestes a expirar, ou apenas para entidades específicas.

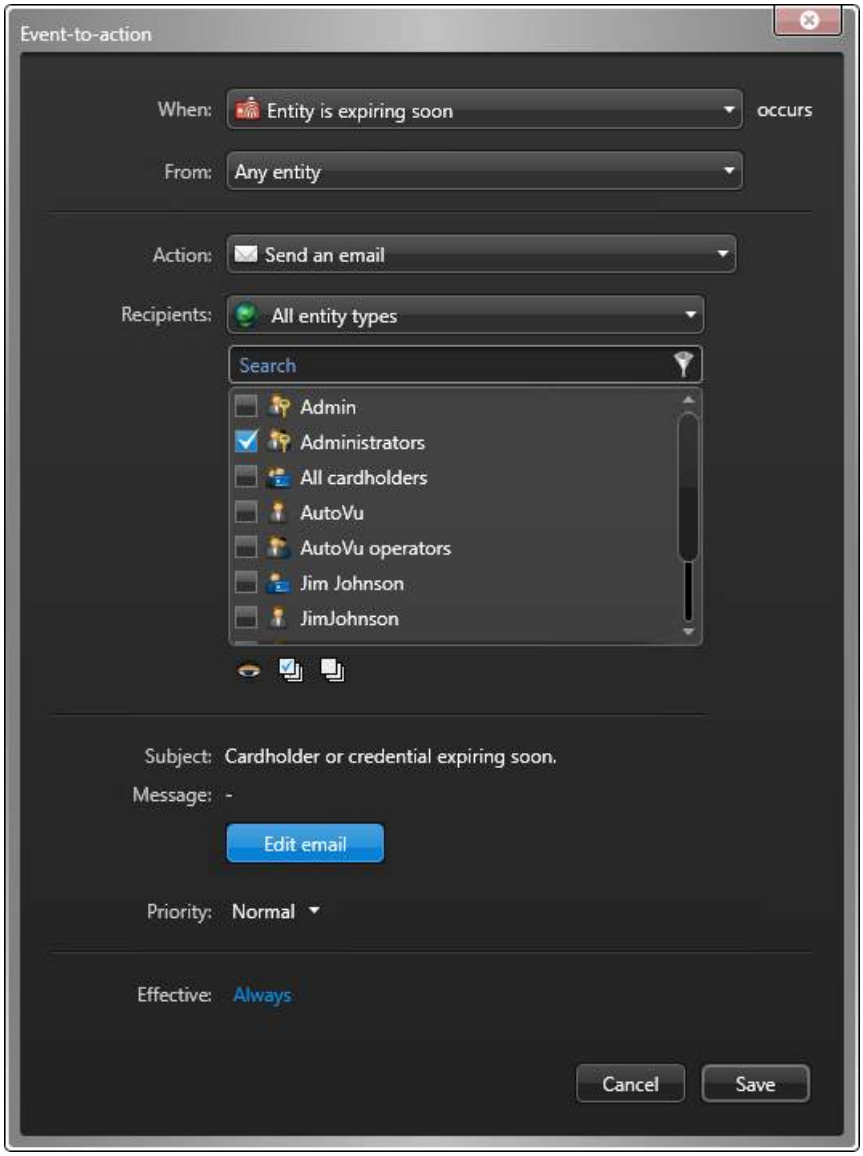
Se um titular de cartão expirar, sua credencial não será mais válida.

Para receber uma notificação quando o titular de cartão ou sua credencial estiver expirando:

1 Abra a tarefa *Controle de acesso* e clique na visualização **Configurações gerais**.
2 Coloque a opção **Disparar o evento 'Entidade expirará em breve'** como **Ligado** e selecione quantos dias antes da expiração o evento será disparado.
3 Clique em **Aplicar**.
4 Abra a tarefa *Sistema* e clique na visualização **Configurações gerais**.
5 Clique em *Ações* e clique em **Adicionar um item** ( ).
6 Na página *evento para ação*, role até a lista **Quando** e clique em **Entidade expirará em breve**.
7 (opcional) Selecione uma entidade na lista **De**.

CUIDADO: Certifique-se de que a entidade que você está selecionando é a que você deseja monitorar. Caso selecione um titular do cartão, e é a credencial que expirará em breve, o evento para ação não será executado.

8 No menu **Ação**, selecione **Enviar um e-mail**, depois selecione os **Destinatários**, edite o e-mail e defina a **Prioridade**.



9 Clique em **Salvar**.

10 Se necessário, altere o intervalo de tempo quando este evento para ação estiver em efeito.

O destinatário recebe um e-mail, em um número de dias especificado antes que a entidade expire.

33

Credenciais

Esta seção inclui os seguintes tópicos:

- "Sobre credenciais" na página 674
- "Métodos de inscrição de credenciais" na página 677
- "Registrar várias credenciais automaticamente" na página 678
- "Inscrição de várias credenciais manualmente" na página 680
- "Criar credenciais" na página 682
- "Adicionar motivos para solicitações de cartão de credencial" na página 686
- "Responder a solicitações de cartão de credencial" na página 687
- "Como os formatos de cartão de credenciais funcionam com o Active Directory no Security Center" na página 688
- "Formatos de cartão personalizados" na página 689
- "Ferramenta de edição de formato de cartão personalizado" na página 690
- "Criar formatos de cartão personalizados" na página 691
- "Projetar modelos de crachá" na página 695

Sobre credenciais

É um tipo de entidade que representa um cartão de proximidade, um modelo biométrico ou um PIN necessário para obter acesso a uma área protegida. Uma credencial pode ser atribuída a apenas um titular de cartão de cada vez.

A entidade credencial representa um cartão de proximidade, um modelo biométrico ou um PIN. As credenciais são usadas pelo Security Center para identificar quem está solicitando acesso por meio de um *ponto de acesso* protegido. As credenciais são, na verdade, *reivindicações de identidade*. Uma credencial distingue um titular de cartão de outro. Para que o controle de acesso seja operacional, cada titular de cartão deve possuir pelo menos uma credencial. Elas são tipicamente (mas não exclusivamente) cartões de controle de acesso.

A credencial necessária depende do tipo de leitor instalado na porta.

Formatos de cartão suportados

O Security Center suporta alguns formatos de cartão padrão.

Para formatos de cartão, um número de cartão é sempre necessário. Dependendo do formato do cartão, o código da instalação pode não ser necessário. A tabela a seguir descreve os formatos de cartão padrão suportados pelo Security Center, seus valores numéricos e os intervalos válidos para o código de instalação (também conhecidos como *Código de ID da Empresa*) e número do cartão (também conhecido como *Número de ID de Cartão*).

Formato do cartão	Intervalo do código da instalação	Intervalo do número do cartão
Padrão 26 bits	0 a 255	0 a 65 535
HID H10306 34 Bits	0 a 65 535	0 a 65 535
HID H10302 37 Bits	Não é exigido[1]	0 a 34 359 738 367
HID H10304 37 Bits	0 a 65 535	0 a 524 287
HID Corporate 1000 (35 Bits)	0 a 4095	0 a 1 048 575
HID Corporate 1000 (48 bits)	0 a 4 194 303	0 a 8 388 607

[1] Se HID H10302 de 37 Bits for o único formato de cartão referenciado em seu arquivo CSV, é preferível ligar o número do cartão ao campo de dados do cartão do Security Center em vez do campo de número de cartão, uma vez que o código da instalação não é exigido. Como um único valor é armazenado na campo de dados de cartão da credencial, não é necessário nenhum caractere separador.

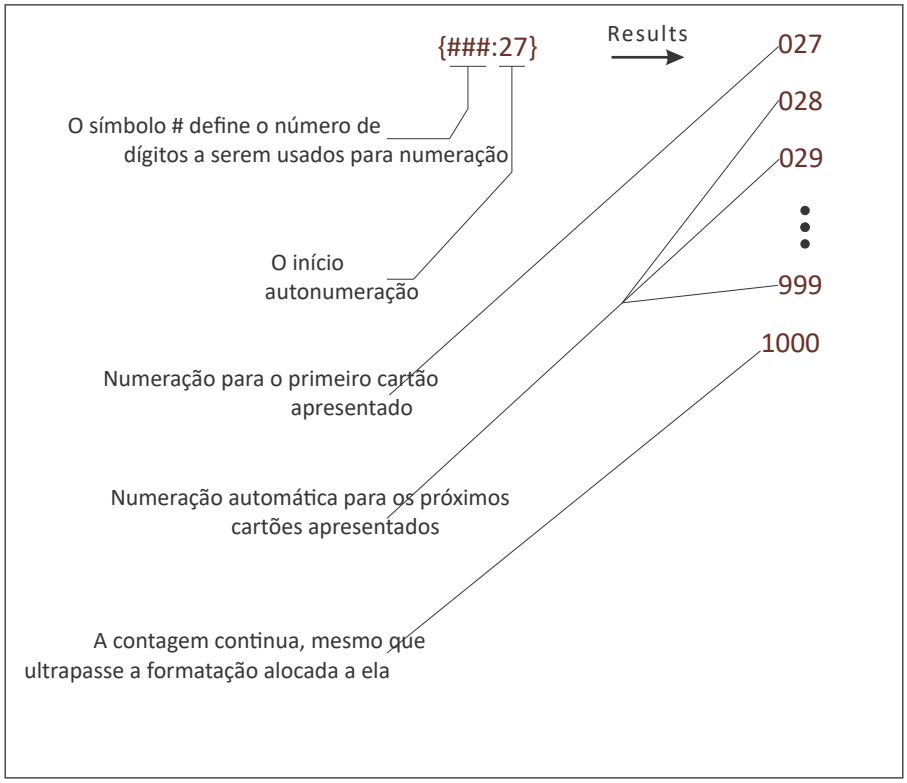
Os formatos personalizados de cartão também podem ser definidos com a *Ferramenta de edição de formato personalizado*.

O prefixo de credencial e o contador

O **Prefixo de credencial** define o nome das credenciais registradas. A tarefa de Gerenciamento de credenciais garante que todas as credenciais registradas tenham um nome exclusivo adicionando automaticamente um número ao nome definido no **Prefixo de credencial**. Você também pode controlar o contador adicionando um formato de numeração automática (entre colchetes) ao prefixo da credencial.

O formato de numeração automática da credencial define o estilo do contador. O formato de numeração automática pode ser colocado em qualquer lugar no prefixo de credencial. Apenas um formato de numeração automática pode ser usado no prefixo de credencial de cada vez.

O formato de numeração automática é explicado abaixo.



Seguem exemplos do formato de numeração automática.

Prefixo de credencial	Sequência de credenciais gerada	Comentários
Credencial_	Credencial_0 Credencial_1 Credencial_2	Quando o formato de numeração automática é omitido, a numeração automática é anexada ao final do prefixo e começa em 0.
Credencial #{##:1}	Credencial #01 Credencial #02 Credencial #03	Uma numeração automática para o prefixo da credencial.
1{####:46} 11203162-2	10046 11203162-2 10047 11203162-2 10048 11203162-2	As credenciais registradas podem ter numeração automática no Security Center para que seus nomes correspondam ao número de série impresso no verso de uma série de cartões.

Recomendação de nomenclatura de cartões

Ao registrar as credenciais do cartão, é recomendável usar o número do cartão impresso no cartão como o nome da credencial no Security Center. Se um cartão perdido for encontrado, você poderá encontrá-lo facilmente no sistema.

Se pretender imprimir o nome de credencial num crachá como um código de barras, certifique-se de que apenas os caracteres suportados pelo tipo de código de barras sejam utilizados.

Recomendação de PIN

Ao usar PIN como credencial, você pode usá-lo com um cartão (Cartão e PIN) ou isoladamente (Cartão ou PIN). As capacidades e a configuração do seu leitor determinam como o PIN é necessário.

Se você planeja usar seus leitores em modo de cartão ou PIN, verifique se os PINs são exclusivos para todos os titulares de cartões e se não há duplicatas no sistema. Duplicar PINs pode causar confusão, pois não há nenhuma maneira de determinar a que titular pertence quando um usuário o digita na porta.

Métodos de inscrição de credenciais

Se você precisar de muitas credenciais de cartão no seu sistema de controle de acesso, poderá inscrever várias credenciais de uma vez.

Os dois métodos de inscrição a seguir estão disponíveis na tarefa *Gerenciamento de credenciais*:

- **Entrada automática:** Esse é o método recomendado quando os cartões que você deseja registrar estão à sua disposição e quando os dados do cartão não forem encontrados em qualquer intervalo de valores conhecido. Também é apropriado usar este método de inscrição quando os cartões vêm em muitos tipos de formatos.
- **Entrada manual:** Este é o método recomendado quando todos os cartões que você deseja registrar são do mesmo formato e um dos campos de dados (tipicamente o *Número do cartão*) contém um intervalo de valores consecutivos. Você não precisa dos cartões efetivos ou de um leitor de cartão para usar este método, e pode ser uma forma eficaz de pré-inscrição de grandes quantidades de cartões.

Você também pode inscrever credenciais usando a *Ferramenta de importação*.

Registrar várias credenciais automaticamente

Se você precisar de muitas credenciais de cartão no seu sistema de controle de acesso, poderá registrar várias credenciais de cartão automaticamente apresentando-as a um leitor.

Antes de iniciar

Você deve ter acesso a um leitor de cartões. Os cartões que você apresentar devem ser de um formato predefinido no seu sistema.

Assegure-se de que esse seja o método de registro correto necessário.

O que você deve saber

Todas as credenciais que registrar devem ser novas em seu sistema Security Center. Qualquer credencial registrada anteriormente é descartada, porque a mesma credencial não pode ser registrada duas vezes no Security Center.

Para registrar várias credenciais automaticamente:

1 Na tarefa **Gerenciamento de credenciais**, clique em **Inscrição em lote**.

2 Na aba *Entrada automática* , selecione um leitor de cartões que esteja próximo.

Verifique se o leitor selecionado suporta os formatos de cartão que você tem.

3 Na seção **Prefixo de credencial**, digite o padrão para os nomes de credenciais registrados.

4 Na seção *Status da credencial* , defina o status, a data de ativação e a data de validade das credenciais.

- **Status:** Todos os valores possíveis são aceitos.
- **Ativação:** Pode ser *Nunca* ou uma data específica.
- **Validade:** Defina uma data de vencimento para a credencial:
  - **Nunca:** A credencial nunca vence.
  - **Data específica:** A credencial vence em uma data e horário específicos.
  - **Definir vencimento no primeiro uso:** A credencial vence depois de um número específico de dias após o primeiro uso.
  - **Quando não é usado:** A credencial vence quando não foi utilizada durante um valor específico de dias.

5 Na seção *Segurança* , selecione a partição à qual as credenciais registradas pertencem.

Este campo determina quais usuários podem visualizar e modificar as credenciais.

- Para adicionar uma partição, clique em **Adicionar** ( ).
- Para remover uma partição, selecione a partição e clique em **Remover** ( ).

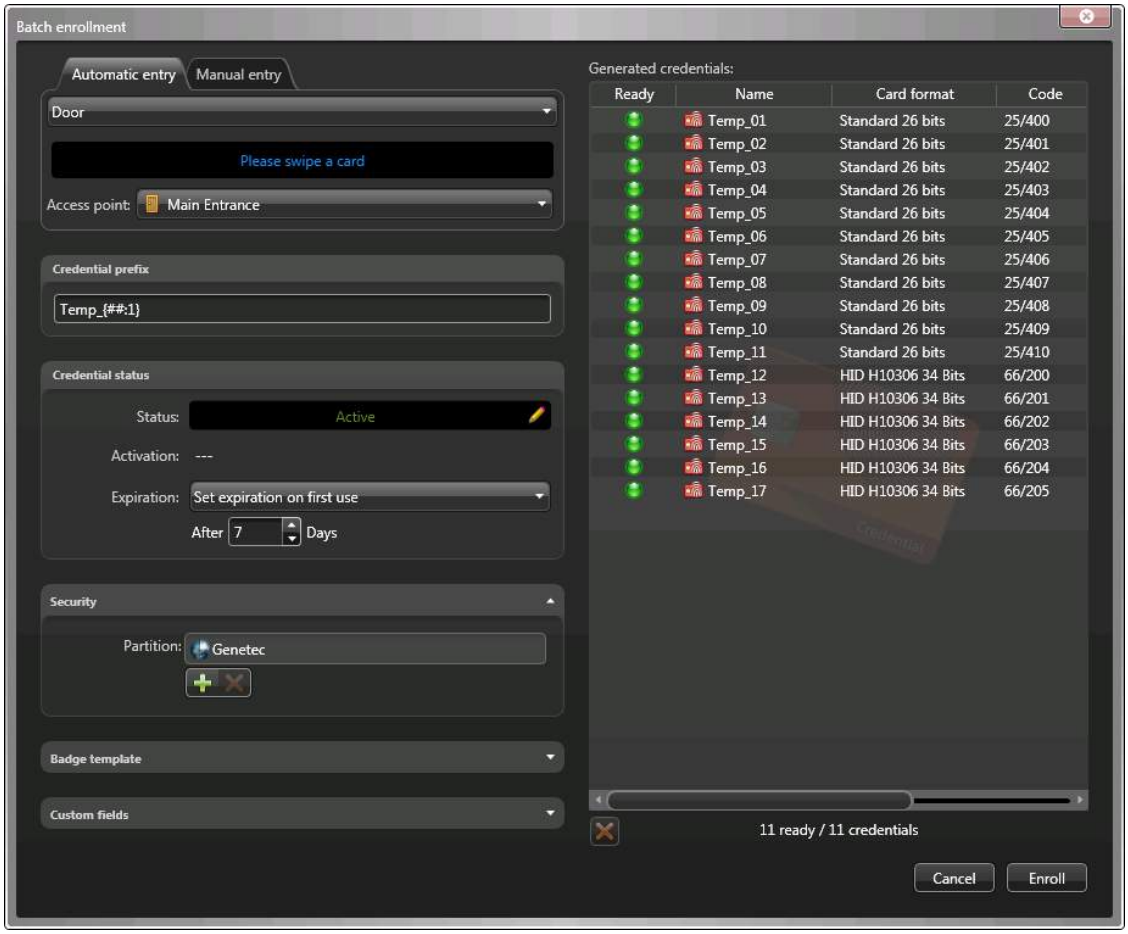
6 Na lista suspensa **Modelo do crachá**, selecione o modelo de crachá padrão usado para representar a credencial.

7 Na seção *Campos personalizados* , defina os valores padrão para os campos personalizados.

Os campos personalizados só estão disponíveis se tiverem sido criados para as credenciais.

8 Apresente o cartão no leitor selecionado.

Todos os cartões apresentados são listados na seção *Credenciais geradas*.



Se algumas das credenciais já estiver registrada, ela será descartada e marcada como rejeitada na lista com um botão vermelho. Se você apresentar o mesmo cartão duas vezes, ele será destacado momentaneamente na lista.

Para obter informações sobre como pode codificar uma credencial no seu cartão antes de registrá-lo, consulte Atribuição de credenciais na página 657.

9 Para excluir um cartão descartado da lista, selecione-o e clique em .

10 Clique em **Inscrever**.

Após terminar

Atribua as credenciais aos seus titulares de cartão.

Tópicos relacionados

Métodos de inscrição de credenciais na página 677
Como os formatos de cartão de credenciais funcionam com o Active Directory no Security Center na página 688
Sobre credenciais na página 674

Inscrição de várias credenciais manualmente

Se você precisar de muitas credenciais de cartão no seu sistema de controle de acesso, poderá inscrever várias credenciais simultaneamente digitando o formato de cartão e os dados manualmente.

Antes de iniciar

Você deve saber o intervalo exato de valores representados nos dados do cartão. Como esses cartões não são apresentados por um leitor, o aplicativo não pode validá-los.

Assegure-se de que esse seja o método de registro correto necessário.

O que você deve saber

Todas as credenciais que registrar devem ser novas em seu sistema Security Center. Qualquer credencial registrada anteriormente é descartada, porque a mesma credencial não pode ser registrada duas vezes no Security Center. Apenas um máximo de 5000 credenciais podem ser criadas de uma só vez.

Para inscrever várias credenciais manualmente:

1. Na tarefa **Gerenciamento de credenciais**, clique em **Inscrição em lote**.
2. Clique na aba *Entrada manual* .
3. Na lista suspensa **Formato do cartão**, defina o formato de cartão usado pelas credenciais que deseja inscrever.

   Esta opção determina os campos de dados que você deve inserir e o intervalo de valores que eles podem ter.
4. Nos campos **Código da instalação** e **Número do cartão**, digite os valores de início e fim para os números de cartões.

   O campo **Número do cartão** é usado como um gerador de sequência.

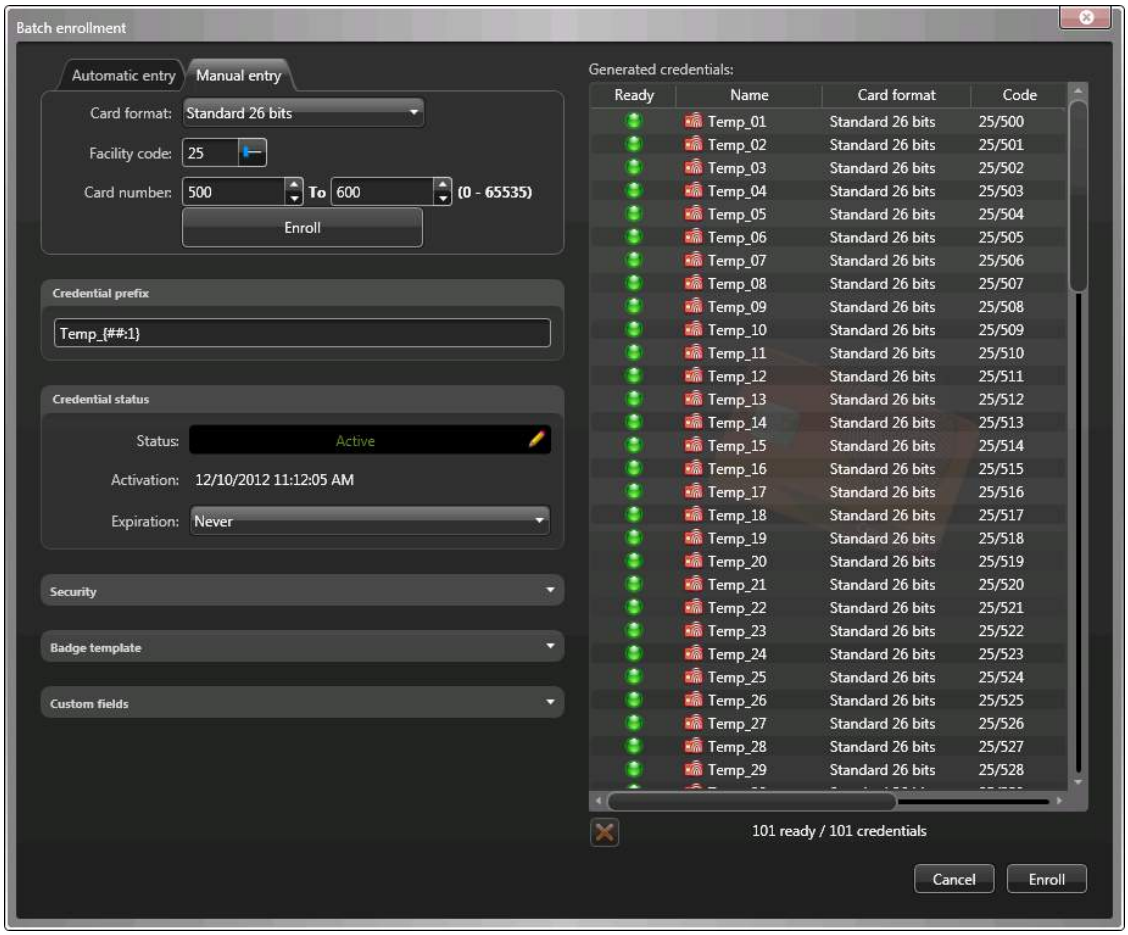
   NOTA: Se o intervalo especificado do **Número do cartão** tiver mais do que 5000 valores, o valor final será automaticamente ajustado para o valor inicial mais 5000.
5. Na seção **Prefixo de credencial**, digite o padrão para os nomes de credenciais registrados.
6. Na seção *Status da credencial* , defina o status, a data de ativação e a data de validade das credenciais.
   - **Status:** Todos os valores possíveis são aceitos.
   - **Ativação:** Pode ser *Nunca* ou uma data específica.
   - **Validade:** Defina uma data de vencimento para a credencial:
     - **Nunca:** A credencial nunca vence.
     - **Data específica:** A credencial vence em uma data e horário específicos.
     - **Definir vencimento no primeiro uso:** A credencial vence depois de um número específico de dias após o primeiro uso.
     - **Quando não é usado:** A credencial vence quando não foi utilizada durante um valor específico de dias.
7. Na seção *Segurança* , selecione a partição à qual as credenciais registradas pertencem.

   Este campo determina quais usuários podem visualizar e modificar as credenciais.
   - Para adicionar uma partição, clique em **Adicionar** ( ).
   - Para remover uma partição, selecione a partição e clique em **Remover** ( ).
8. Na lista suspensa **Modelo do crachá**, selecione o modelo de crachá padrão usado para representar a credencial.
9. Na seção *Campos personalizados* , defina os valores padrão para os campos personalizados.

   Os campos personalizados só estão disponíveis se tiverem sido criados para as credenciais.

10 Clique em **Inscrever**.

As credenciais que você vai criar são listadas na seção *Credenciais geradas*.



Se algumas das credenciais já estão registradas, elas serão descartadas e marcadas como rejeitadas na lista com um botão vermelho.

11 Para remover uma credencial cartão descartada da lista, selecione-a e clique em .

12 Clique em **Inscrever**.

Após terminar

Atribua as credenciais aos seus titulares de cartão.

Tópicos relacionados

Métodos de inscrição de credenciais na página 677
Como os formatos de cartão de credenciais funcionam com o Active Directory no Security Center na página 688
Sobre credenciais na página 674

Criar credenciais

Você pode criar uma nova credencial, configurar suas propriedades e atribuí-la a um titular de cartão ou visitante usando a tarefa *Gerenciamento de credenciais* .

O que você deve saber

Em vez de criar titulares de cartão manualmente, é possível importá-los de um arquivo CSV ou do Active Directory da sua empresa.

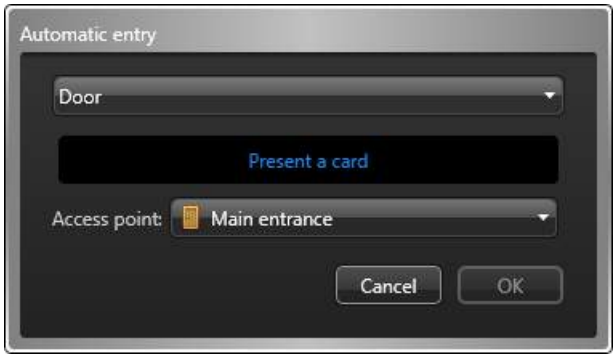
Para criar uma credencial:

1 Na tarefa **Gerenciamento de credenciais**, clique em **Criar nova credencial** ( ).

2 Selecione uma das seguintes opções:

- **Entrada automática:** Apresentar o cartão a um leitor.
- **Entrada manual:** Digite manualmente os dados do cartão. Use este método quando não tiver um leitor de cartão por perto.
- **PIN:** Crie uma credencial com PIN.
- **Placa de licença:** Digite um número de placa de licença do titular do cartão. Utilize esse método se uma câmera Sharp for utilizada para acionar uma barreira de acesso de veículos. Nesse caso, a placa de veículo do titular do cartão pode ser usada como credencial.

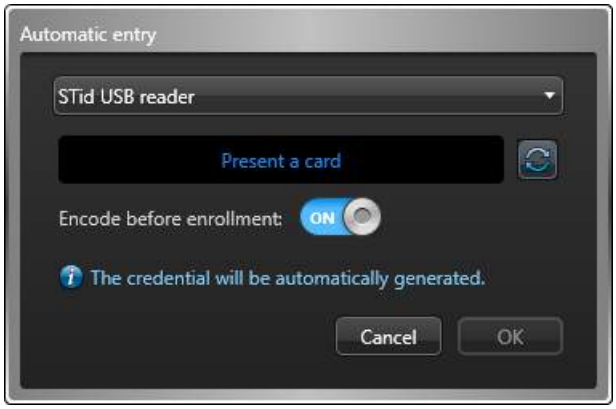
3 Se selecionar **Entrada automática**, depois é necessário selecionar um leitor (USB ou uma porta) e apresentar o cartão no leitor.



Se você tem um leitor decodificador de smart card instalado, defina a opção **Codificar antes da inscrição** para **INATIVO** para ler um cartão pré-codificado.

Quando o LED do leitor fica verde (pronto para ler), coloque o smart card no leitor. O LED do leitor fica amarelo e depois verde com um som curto antes de desligar.

Se deseja gerar e codificar em seu cartão uma credencial aleatória de 128 bits MIFARE DESFire antes da inscrição, configure a opção **Codificar antes da inscrição** como **ATIVO**.

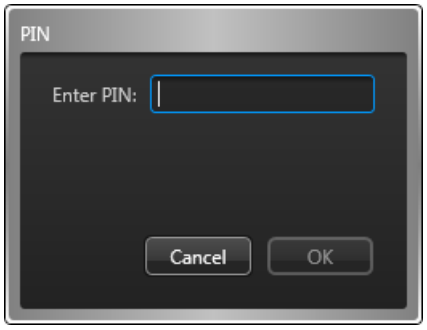


Quando o LED do leitor fica vermelho (pronto para codificar), coloque o smart card no leitor por aproximadamente 2 segundos. O LED do leitor fica amarelo e depois verde com um som curto antes de desligar. Se você ouvir um bip longo e o LED permanecer vermelho, tente novamente.

4 Se selecionar **Entrada manual**, é necessário selecionar um formato de cartão, inserir os campos de dados necessários e clicar em **OK**.

CUIDADO: Cuidado ao digitar os dados do cartão, porque o sistema não pode validar caso os dados inseridos correspondam a um cartão físico ou não.

5 Se selecionar **PIN**, é necessário fazer o seguinte:

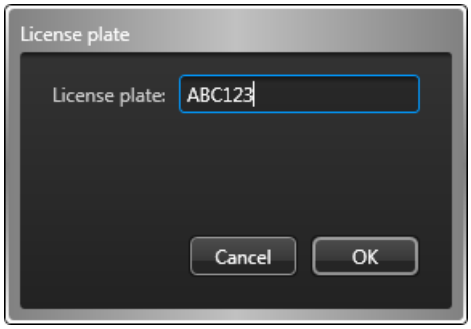


a) Entre o PIN como um valor numérico.

NOTA: Cuidado para não ultrapassar o número de dígitos aceitos pelos seus leitores. Um comprimento comum de PIN é de cinco dígitos. Mas alguns modelos aceitam até 15 dígitos.

b) Clique em **OK**.

6 Se selecionar **Placa de licença**, é necessário fazer o seguinte:



a) Entre o número da placa de licença.

NOTA: Não é necessário entrar espaços que aparecem no número da placa. O sistema trata “ABC123” e “ABC 123” como a mesma placa.

b) Clique em **OK**.

7 No campo **Nome da entidade**, digite um nome para a entidade de credencial.

A captura de tela a seguir é para as credenciais do cartão. A caixa de diálogo é diferente se você tiver selecionado credenciais de **PIN** ou **Placa de veículo**.

8 Clique no campo **Pertencem a**, selecione um titular de cartão ou visitante para atribuir a credencial e clique em **OK**.

Sem atribuir uma credencial, você não pode monitorar as atividades ou gerar relatórios de atividades para esse titular ou visitante.

9 Na seção *Status* , defina o status e o período de ativação da credencial.

Se a credencial estiver inativa, o titular do cartão ou visitante não terá acesso a nenhuma área.

- **Status:** Defina o status da credencial como **Ativo**.
- **Ativação:** Exibe a data atual.

- **Validade:** Defina uma data de vencimento para a credencial:
  - **Nunca:** A credencial nunca vence.
  - **Data específica:** A credencial vence em uma data e horário específicos.
  - **Definir vencimento no primeiro uso:** A credencial vence depois de um número específico de dias após o primeiro uso.
  - **Quando não é usado:** A credencial vence quando não foi utilizada durante um valor específico de dias.

10 Se campos personalizados forem definidos para credenciais, como o fabricante, o modelo de cartão e assim por diante, insira as informações personalizadas da credencial na seção designada.

11 (Opcional) Clique na seção *Avançado* e configure as seguintes propriedades da credencial:

a) No campo **Descrição**, digite uma descrição para a credencial.

b) Atribua a credencial a uma *partição*.

As partições determinam quais usuários do Security Center têm acesso a essa entidade. Somente usuários que receberam acesso à partição podem visualizar a credencial.

12 (Opcional) Se a credencial for uma credencial de cartão (não um PIN), selecione um modelo de crachá.

a) No canto inferior direito da caixa de diálogo de detalhes de credenciais, clique na imagem do crachá.

b) Selecione um modelo de crachá e clique em **OK**.

Os modelos de crachá são criados no Config Tool.

Aparece uma visualização do crachá, com os dados correspondentes à credencial.

NOTA: O modelo de crachá permanece associado à credencial mesmo se você cancelar a atribuição da credencial de um titular de cartão ou visitante.

13 Para imprimir o crachá, no canto inferior esquerdo da caixa de diálogo de detalhes de credenciais, clique em **Imprimir crachá**.

14 Quando tiver terminado de editar a credencial, clique em **Salvar**.

A nova credencial é adicionada à lista na tarefa **Gerenciamento de credenciais**.

Após terminar

Para modificar uma credencial, selecione a credencial na lista e clique em **Modificar** ( ).

Tópicos relacionados

Importar titulares de cartão e credenciais na página 718
Atribuição de credenciais na página 657
Projetar modelos de crachá na página 695
Responder a solicitações de cartão de credencial na página 687

Adicionar motivos para solicitações de cartão de credencial

Para permitir que os usuários especifiquem por que eles estão solicitando um cartão de credencial, você pode adicionar um conjunto de razões pelas quais eles podem escolher.

O que você deve saber

Um motivo comum pelo qual um usuário pode solicitar um cartão de credencial é: “não há impressora no local”.

Para adicionar um novo motivo para solicitação de cartão:

1. Abra a tarefa **Controle de acesso** e clique na visualização **Configurações gerais**.
2. Na seção *Motivos para solicitação do cartão*, clique em **Adicionar um item** ( ).
3. Na caixa de diálogo **Adicionar um novo motivo para solicitação de cartão**, digite um motivo e clique em **Adicionar** > **Aplicar**.
4. Para modificar um motivo para solicitação de cartão, selecione-o na lista e clique em **Editar o item** ( ).
5. Para excluir um motivo para solicitação de cartão, selecione-o na lista e clique em **Remover o item** ( ).

O novo motivo pode agora ser selecionado quando os usuários solicitarem cartões de credencial.

Responder a solicitações de cartão de credencial

Após uma solicitação de cartão de credencial ter sido feita, você pode responder atribuindo uma credencial para o solicitante para o qual foi feita a solicitação, ou negando a solicitação.

O que você deve saber

O número de solicitações de cartão pendentes é mostrado no ícone **Solicitações de cartão** ( ) na bandeja de notificação e na parte superior da tarefa *Gerenciamento de credenciais*.

As solicitações de credenciais são enviadas quando um usuário cria um novo titular de cartão, mas não pode atribuir uma credencial ou imprimir um cartão para o titular do cartão (por exemplo, porque nenhuma impressora está disponível). Depois de atribuir e imprimir um cartão de credencial, ele pode ser enviado para outro local, se necessário.

Para responder a uma solicitação de cartão de credencial:

1 Fazer um dos seguintes:

- Na bandeja de notificação, clique em **Solicitações de cartão** ( ).
- Na parte superior da tarefa **Gerenciamento de credenciais**, clique em **Solicitações de cartão**.

2 Na caixa de diálogo *Solicitações de cartão*, selecione a solicitação que deseja responder.
Mantenha pressionado `Shift` para selecionar várias solicitações.

3 Para modificar a solicitação, clique em **Modificar** ( ), edite a solicitação e clique em **OK**.

4 Para rejeitar a solicitação, clique em **Negar solicitação** ( ).

5 Para atribuir uma credencial de cartão, clique em **Cartão associado** ( ).
Na caixa de diálogo *Associar cartões*que será aberta, tome uma das seguintes opções:

- Para atribuir uma credencial automaticamente, clique em **Entrada automática**, depois selecione um leitor (USB ou uma porta) e apresente o cartão ao leitor.

  Se um cartão elegível for apresentado, ele será imediatamente atribuído. Se o cartão não tiver sido instalado, ele é instalado automaticamente. Se já estiver atribuído a alguém, ele será rejeitado.

  Para obter informações sobre como pode codificar uma credencial no seu cartão antes de registrá-lo, consulte Atribuição de credenciais na página 657.

- Para atribuir uma credencial manualmente, clique em **Entrada manual**, depois selecione um formato de cartão, digite os campos de dados necessários e clique em **Registrar**.

  Se um cartão elegível for inserido, ele será imediatamente atribuído. Se o cartão não tiver sido instalado, ele é instalado automaticamente. Se já estiver atribuído a alguém, ele será rejeitado.

  CUIDADO: Cuidado ao digitar os dados do cartão, porque o sistema não pode validar caso os dados inseridos correspondam a um cartão físico ou não.

- Para atribuir uma credencial existente, clique em **Credencial existente**, em seguida, clique duas vezes em uma credencial da lista de credenciais elegíveis.

6 Para imprimir o crachá no cartão, clique em **Imprimir cartões** ( ) e siga as instruções.

7 Clique em **Fechar** para concluir esta solicitação.

Após a solicitação do cartão ser concluída ou recusada, um e-mail é enviado ao solicitante somente se ele selecionou a opção **Envie um e-mail quando o cartão estiver pronto** ao solicitar o cartão.

Tópicos relacionados

Solicitar cartões de credencial na página 660
Criar credenciais na página 682

Como os formatos de cartão de credenciais funcionam com o Active Directory no Security Center

Se decidir mapear a propriedade *Formato de cartão* da credencial para um atributo do Active Directory, esse atributo deve conter um valor numérico (para formato de cartão padrão) ou o nome do formato de cartão exato (texto).

A tabela a seguir descreve os formatos de cartão padrão suportados pelo Security Center, seus valores numéricos e os intervalos válidos para o código de instalação (também conhecidos como *Código de ID da Empresa*) e número do cartão (também conhecido como *Número de ID de Cartão*).

Número	Nome do formato (Texto)	Intervalo do código da instalação	Intervalo do número do cartão
0	Padrão 26 bits	0 a 255	0 a 65 535
1	HID H10306 34 Bits	0 a 65 535	0 a 65 535
2	HID H10302 37 Bits	Não é exigido[1]	0 a 34 359 738 367
3	HID H10304 37 Bits	0 a 65 535	0 a 524 287
4	HID Corporate 1000 35 Bits	0 a 4095	0 a 1 048 575
5	HID Corporate 1000 (48 bits)	0 a 4 194 303	0 a 8 388 607

[1] Se HID H10302 de 37 Bits for o único formato de cartão referenciado em seu arquivo CSV, é preferível ligar o número do cartão ao campo de dados do cartão do Security Center em vez do campo de número de cartão, uma vez que o código da instalação não é exigido. Como um único valor é armazenado na campo de dados de cartão da credencial, não é necessário nenhum caractere separador.

IMPORTANTE: Para formatos de cartão personalizados, você deve usar a ortografia exata usada para criar o formato de cartão personalizado.

Tópicos relacionados

Integração com o Active Directory do Windows na página 384
Formatos de cartão personalizados na página 689
Ferramenta de edição de formato de cartão personalizado na página 690
Criar formatos de cartão personalizados na página 691

Formatos de cartão personalizados

Além dos formatos de cartão padrão suportados no Security Center, você pode definir formatos de cartão personalizados com campos de dados exclusivos.

Você pode definir formatos de cartão personalizados no Config Tool a partir da visualização *Configurações gerais* na tarefa Controle de acesso.

Benefícios dos formatos de cartão personalizados

Criar formatos de cartão personalizados tem os seguintes benefícios:

- Você pode inscrever manualmente um novo cartão usando um teclado de estação de trabalho padrão, enquanto um cartão com um formato desconhecido só pode ser registrado usando um leitor de cartão.
- Você pode ver o número do cartão no Config Tool e no Security Desk, enquanto que os dados para formatos de cartão desconhecidos não podem ser exibidos.
- Você pode importar cartões usando formatos personalizados com a *Ferramenta de importação*.
- Você pode inscrever cartões automaticamente com um leitor de cartões, ou manualmente em lote, sem um leitor de cartões, usando a tarefa Gerenciamento de credenciais.

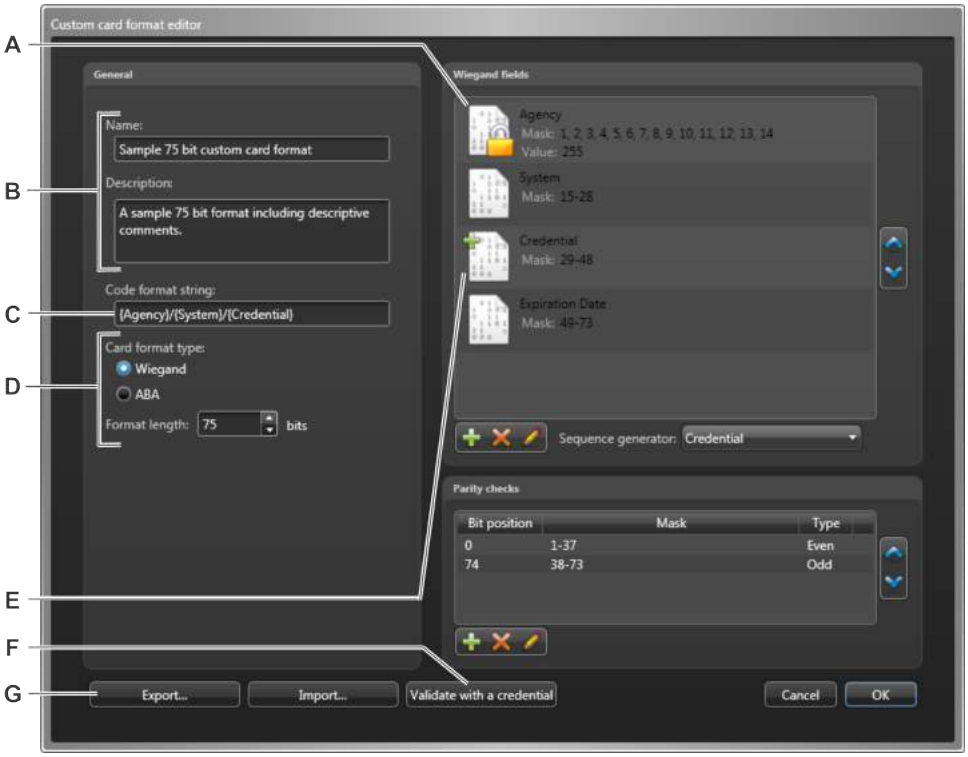
Tópicos relacionados

Importar grupos de segurança de um Active Directory na página 389
Sobre entidades federadas na página 225

Ferramenta de edição de formato de cartão personalizado

O *editor de formato de cartão personalizado* é uma ferramenta específica do Synergis™ que permite definir seus próprios formatos de cartão. Ele está acessível na visualização *Configurações gerais* na tarefa Controle de acesso.

Apenas usuários administrativos podem usar esta ferramenta.



A	Campo de valor fixo (indicado pelo ícone de cadeado).
B	Nome e descrição do formato de cartão listados na tarefa *Controle de acesso*, visualização.
C	Formato usado para exibir o *Código da credencial* em relatórios.
D	Selecione o tipo e o comprimento do formato do cartão antes de definir os campos.
E	Campo designado como o gerador de sequência (indicado pelo ícone de sinal de mais).
F	Valida o formato com credenciais pré-inscritas.
G	Importa/exporta formato de cartão de arquivo XML.

Tópicos relacionados

Como os formatos de cartão de credenciais funcionam com o Active Directory no Security Center na página 688

Criar formatos de cartão personalizados na página 691

Criar formatos de cartão personalizados

Para definir formatos de cartão personalizados que contenham campos de dados exclusivos, você pode criar formatos personalizados manualmente ou importá-los de arquivos XML, usando a ferramenta *Editor de formato de cartão personalizado*.

O que você deve saber

Se você excluir um formato de cartão personalizado depois que ele está sendo usado no Security Center, todas as credenciais que usam esse formato aparecem como *Desconhecido*, mas as credenciais ainda recebem acesso às portas.

Para criar um novo formato de cartão personalizado:

1 Abra a tarefa **Controle de acesso** e clique na visualização **Configurações gerais**.

2 Em **Formatos de cartão personalizados**, clique em **Adicionar um item** ( ).

3 No **Editor de formato de cartão personalizado**, digite o **Nome** e a **Descrição** do formato de cartão personalizado.

4 Especifique o **Tipo de formato do cartão** e o **Comprimento do formato**.

- **Wiegand** (8 a 128 bits)
- **ABA** (2 a 32 caracteres)

5 Defina os campos Wiegand ou defina os campos ABA que constituem o formato de cartão personalizado.

6 Se tiver selecionado o tipo de formato **Wiegand** , você pode precisar adicionar bits para verificação de paridade do formato.

7 (Somente para o tipo Wiegand) Se você deseja registrar um conjunto de credenciais em massa, você pode designar um campo como o **gerador da sequências**.

O campo designado como o gerador de sequências permite definir um intervalo de valores para registrar as credenciais em massa na tarefa *Gerenciamento de credenciais*.

8 Introduza a cadeia de formato para imprimir o **código da credencial**.

O código de credencial é a forma impressa dos dados de credencial. É uma coluna opcional que está disponível na maioria dos relatórios relacionados ao controle de acesso. A **Cadeia de formato do código** informa ao sistema como imprimir os dados da credencial. Para incluir um campo no código de credencial, o nome do campo deve ser especificado na sequência de formato de código, uma vez que está escrito na definição do campo de formato de cartão, entre colchetes “{ }”. Os nomes dos campos diferenciam entre maiúsculas e minúsculas. Quaisquer outros caracteres na cadeia de formato que não estejam entre colchetes são impressos como estão. Por exemplo, com a cadeia de formato “{Instalação}/{Número do cartão}”, uma credencial com os valores dos respectivos campos 230 e 7455 é impressa como “230/7455”.

9 Para validar o novo formato de cartão personalizado com uma credencial pré-registrada, clique em **Validar com uma credencial**, selecione uma credencial pré-registada e clique em **OK**.

10 (Opcional) Clique em **Exportar** para salvar o formato de cartão personalizado em um arquivo XML.

A exportação do formato de cartão personalizado para um arquivo XML permite importar a mesma definição de formato para outros sistemas Synergis™.

11 Clique em **OK** > **Aplicar**.

Tópicos relacionados

Formatos de cartão personalizados na página 689

Definir campos ABA

Se estiver adicionando um formato de cartão ABA personalizado, deverá definir os campos de dados ABA que constituem o formato do cartão.

O que você deve saber

O comprimento do campo ABA é medido em caracteres (4 bits cada). O comprimento máximo do campo ABA é de 18 caracteres, ou até o comprimento do formato do cartão, o que ocorrer primeiro. O comprimento máximo do formato de cartão ABA para unidades HID é 32 caracteres ou 128 bits, embora o máximo permitido pela unidade Synergis™ seja 128 caracteres ou 512 bits.

A ordem dos campos ABA no formato é importante por duas razões:

- Ela define o formato do cartão.
- Corresponde à ordem em que os valores do campo são lidos a partir dos dados do cartão Credencial quando se utiliza a ferramenta de Importação.

Para definir um campo ABA:

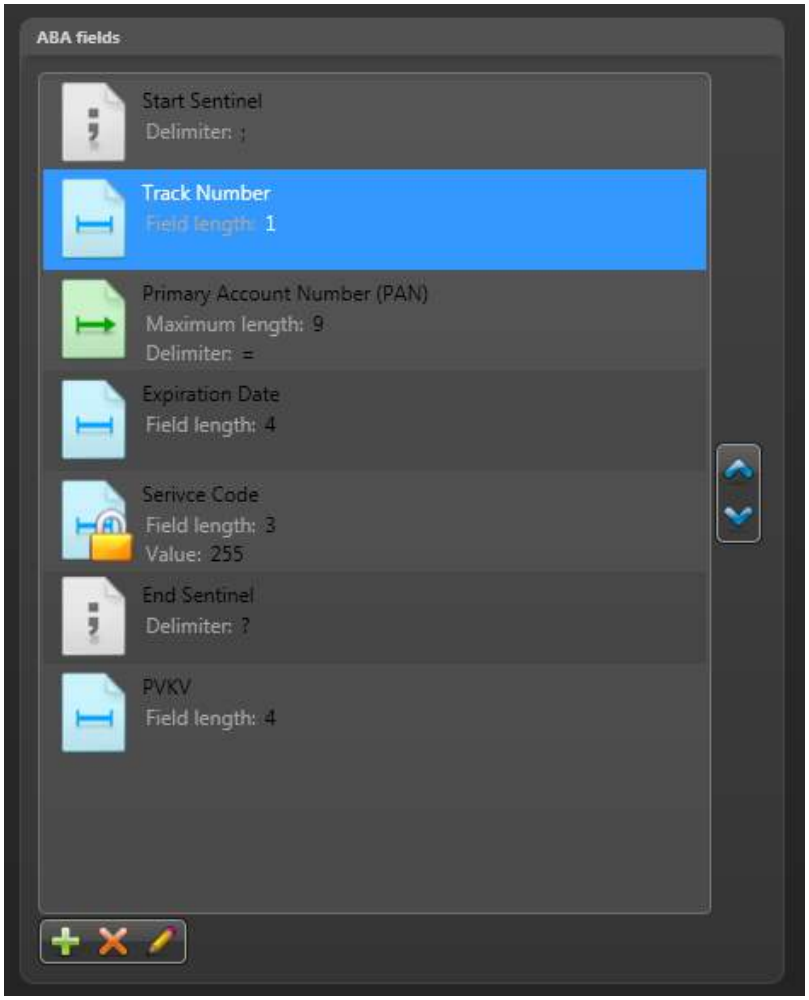
1 No *Editor de formato de cartão personalizado*, clique em **Adicionar um item** ( ) na seção **Campos ABA**.

2 Selecione um dos seguintes tipos de campo ABA:

- **Delimitador:** Especifica um caractere delimitador, normalmente usado no início ou no final do formato do cartão.
- **Tamanho fixo:** Um campo de comprimento fixo. O comprimento é especificado em caracteres (4 bits cada). O campo pode conter um valor fixo. O comprimento do campo deve ser longo o suficiente para manter o valor fixo.
- **Delimitado:** Um campo de comprimento variável. Você deve especificar um comprimento máximo (como caracteres de 4 bits) e um caractere delimitador.

3 Clique em **OK**.

O campo é adicionado na seção **Campos ABA**.



Definir campos Wiegand

Se estiver adicionando um formato de cartão Wiegand personalizado, deverá definir os campos de dados Wiegand que constituem o formato do cartão.

O que você deve saber

Um campo Wiegand é composto de uma série de bits. O comprimento máximo do campo é de 63 bits.

A ordem dos campos Wiegand é importante para o formato de cartão. Corresponde à ordem em que os valores dos campos são lidos a partir dos dados do cartão Credencial quando se utiliza a *Ferramenta de importação*.

Para definir um campo Wiegand:

1 No *Editor de formato de cartão personalizado*, clique em **Adicionar um item** (+) na seção **Campos Wiegand**.

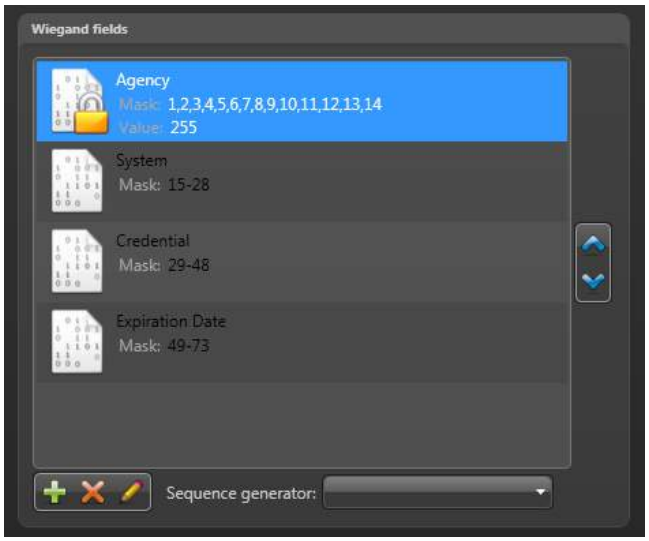
2 No campo **Nome**, digite um nome para o campo Wiegand.

3 No campo **Máscara**, digite o número de bits que fazem parte do campo Wiegand.

Os bits são nomeados de acordo com a sua posição no formato de cartão, começando do 0. Você pode digitar as máscaras como uma lista de posições de bit separadas por vírgula ou como um intervalo de posições de bit. Por exemplo, a máscara "**1,2,3,4,5,6,7,8**" também pode ser escrita como "**1-8**" ou "**1-4,5-8**". A ordem dos bits dentro do campo é importante ("**1,2,3,4**" não é a mesma coisa que "**4,3,2,1**").

4 Clique em **OK**.

O campo é adicionado na seção **Campos Wiegand**.



Adicionando verificações de paridade

Se estiver a definir um formato de cartão Wiegand personalizado, pode adicionar verificações de paridade para reforçar a validação das suas credenciais.

O que você deve saber

A ordem das verificações de paridade na lista **Verificações de paridade** é importante. Corresponde à ordem em que são avaliadas as verificações de paridade. A máscara de uma verificação de paridade subsequente pode incluir o bit de paridade de uma verificação de paridade anterior e suas máscaras podem se sobrepor.

Para adicionar uma verificação de paridade:

1 No *Editor de formato de cartão personalizado*, **clique em Adicionar um item** ( ) na seção **Verificações de paridade**.

2 Na caixa de diálogo **Verificações de paridade**, selecione o **Tipo** de verificação de paridade (**Par** ou **Ímpar**).

3 No campo **Bit de paridade**, digite a posição do bit de paridade no formato do cartão (começa em 0)

4 No campo **Máscara**, digite os bits que devem ser avaliados.

A sintaxe deve corresponder aos valores de máscara de campo de dados Wiegand, mas a ordem dos bits não é importante.

5 Clique em **OK**.

A verificação de paridade é adicionada na lista **Verificações de paridade**.

Projetar modelos de crachá

Para usar modelos de impressão personalizados para cartões de credencial, você pode criar novos modelos de crachá adaptados às suas necessidades.

O que você deve saber

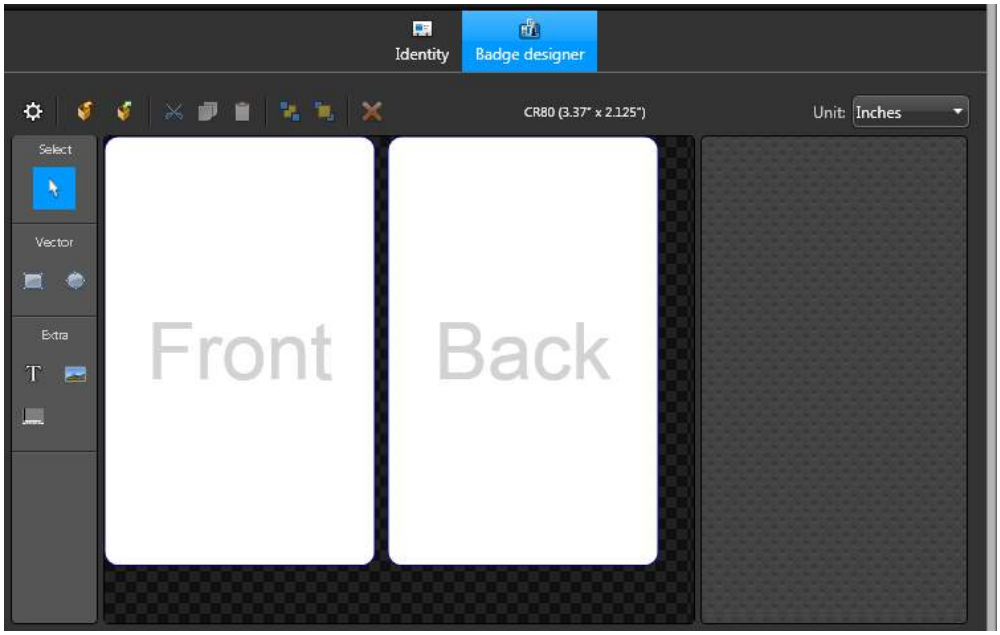
Um modelo de crachá é representado por uma entidade de *modelo de crachá* no Security Center e pode incluir campos do banco de dados de configuração para que o nome correto, a foto do titular de cartão e assim por diante, apareçam em cada cartão.

Por exemplo, você pode adicionar um logotipo da empresa, uma imagem de plano de fundo, foto do funcionário ou uma cor personalizada a ser impressa nos cartões de controle de acesso.

Para projetar um modelo de crachá:

1. Abra a tarefa **Controle de acesso** e clique na visualização **Modelo de crachá**.
2. Clique em **Modelo de crachá** ( ).
3. Digite um nome para o novo modelo de crachá que aparece na lista de entidades e pressione **ENTER**.
4. Na aba **Identidade**, digite uma descrição para o modelo de crachá.
5. Na seção **Relacionamentos**, selecione a partição onde deseja que o modelo de crachá seja colocado.

   As partições determinam quais usuários do Security Center têm acesso a essa entidade. Somente usuários que receberam acesso à partição podem visualizar o modelo de crachá.
6. Clique em **Aplicar**.
7. Clique na aba **Designer de crachás**.
8. Para selecionar o tamanho dos cartões de controle de acesso que deseja imprimir, clique em **Propriedades** ( ).
9. Na caixa de diálogo **Formato**, selecione um tamanho e uma orientação para o cartão.
   - Para criar um tamanho personalizado, clique em , digite o nome, largura e comprimento do cartão e clique em **OK**.
10. Clique em **OK**.



Uma vez que o tamanho/formato do cartão seja escolhido, você pode projetar o modelo de impressão real.

11 Na seção **Ferramentas**, selecione uma ferramenta e clique no modelo para usá-lo.

Existem seis ferramentas gráficas que você pode usar para editar o modelo:

- **Ferramenta de seleção:** Use para clicar e selecionar um objeto no modelo.
- **Ferramenta retângulo:** Use para desenhar um quadrado/retângulo no modelo.
- **Ferramenta elipse:** Use para desenhar círculos/ovais no modelo.
- **Ferramenta de texto:** Use para inserir texto no modelo. Você pode inserir um texto estático ou adicionar campos de texto dinâmicos de credencial e de titular de cartão, como *Nome*, *Sobrenome* e assim por diante.
- **Ferramenta de imagem:** Use para inserir uma figura no modelo. Você pode inserir imagens do titular do cartão, uma imagem de fundo para o cartão, e assim por diante.
- **Ferramenta de código de barras:** Use para inserir códigos de barras no modelo.

12 Se você adicionou uma imagem ao modelo, selecione a imagem para editá-la usando as opções nos widgets **Imagem** e **Cor e borda**.

No widget **Imagem**, selecione se a **Origem** da imagem é uma imagem do titular de cartão ou uma imagem de um arquivo e se a imagem deve ser esticada ou não.

- **Imagem do titular do cartão:** Imagem dinâmica do titular do cartão que muda, dependendo da credencial do cartão que você está imprimindo. Este campo de imagem está conectado ao valor de imagem *Titular de cartão* no banco de dados de configuração.

  DICA: Se a imagem de um titular de cartão foi tirada na frente de uma tela de chroma key, você pode tornar o plano de fundo transparente. Isso é útil se você estiver criando um modelo de crachá que tenha uma imagem em segundo plano.
- **Arquivo:** Imagem estática selecionada de um arquivo.

No widget **Cor e borda**, você pode usar as seguintes ferramentas:

- **Preencher:** Use para modificar a cor de preenchimento de um objeto inserido, como um quadrado ou um oval.
- **Borda:** Use para modificar a cor da borda de um objeto inserido, como um quadrado ou um oval.
- **Opacidade:** Use para modificar a opacidade de um objeto inserido, como um quadrado ou um oval.
- **Espessura da borda:** Use para modificar a espessura da borda do objeto inserido.

13 Se você adicionou texto ao modelo, selecione o texto para editá-lo usando as opções no widget **Texto**.

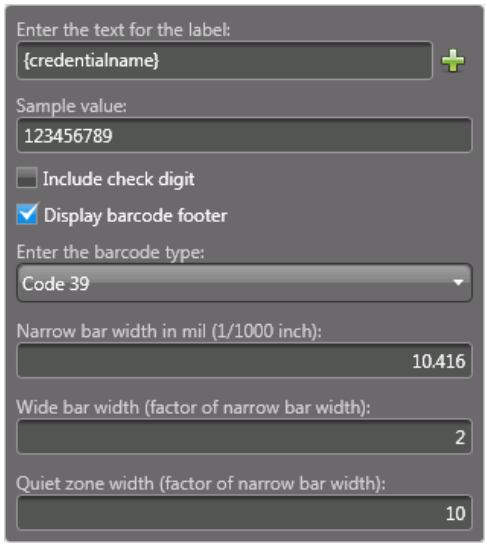
Clique com o botão direito do mouse no campo de texto para selecionar a **Ordem Z** e a **Borda**, **Fonte**, **Cor** e **Alinhamento** do texto.

No widget **Texto**, você pode usar as seguintes ferramentas:

- Clique em **Adicionar campo** () para adicionar um campo dinâmico de titular de cartão ou credencial. Você pode misturar texto estático com os campos dinâmicos.
- Clique em **Preenchimento** para definir a cor do texto.
- Clique em **Alinhar à esquerda**, ao **centro** ou à **direita** para definir o alinhamento do texto.
- Clique em **Quebrar texto se for muito longo** para ativar a quebra de texto.

  Se a quebra de texto estiver ativada, o sistema quebrará o texto se for muito longo para caber dentro da caixa de texto, sem alterar o tamanho da fonte. Se a quebra de texto estiver desativada, o sistema encaixará o texto dentro da caixa de texto alterando o tamanho da fonte.

14 Se você adicionou um código de barras ao modelo, clique com o botão direito do mouse no código de barras e clique em **Propriedades** para editá-lo. Os dados no código de barras podem ser estáticos ou usar propriedades de credenciais dinâmicas.

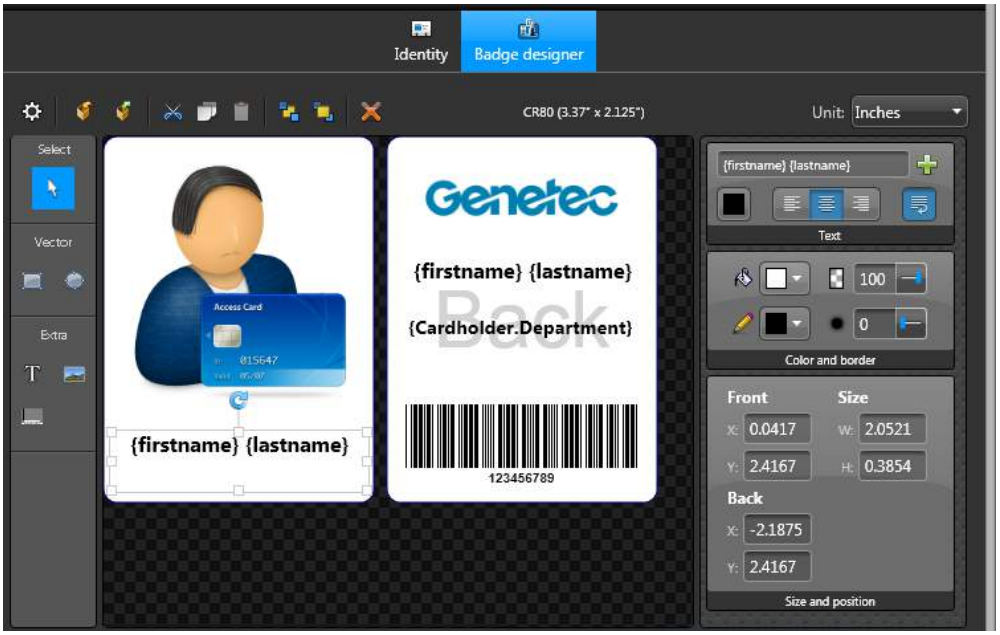


15 Na seção **Tamanho e posição**, selecione onde o texto, imagem ou código de barras está localizado no crachá e sua largura e altura.

16 Clique em **Aplicar**.

Exemplo

Aqui está um exemplo de modelo de crachá com objetos já inseridos:



- Foram inseridas duas imagens diferentes. Uma é dinâmica e a outra é estática:
  - A imagem dinâmica do titular do cartão aparece na parte frontal do cartão.
  - A imagem estática aparece na parte traseira do cartão. É o logotipo da empresa, que é exibido em cada cartão.
- Foram inseridos três campos de texto dinâmico:
  - **{Firstname} {lastname}** aparecem na frente do cartão. O texto impresso será obtido do banco de dados de configuração e veremos *primeiro nome, (espaço), sobrenome*. O texto é centralizado e a quebra de texto está ativada.

- **{Firstname} {lastname}** aparecem na traseira do cartão. É igual ao campo de nome na frente, mas com tamanho de fonte menor, e a quebra automática de texto está desativada.
- **{Cardholder.Department}** *Campo personalizado* criado para a entidade titular de cartão.

- Um código de barras foi inserido, contendo dados dinâmicos. Ele exibe o nome da credencial, usando o tipo de código de barras Código 39.

Pré-visualizar impressões de modelos de crachá

Depois de criar um novo modelo de crachá, você pode ver como vai parecer em um cartão de credencial.

Para pré-visualizar a impressão de um modelo de crachá:

1. Abra a tarefa **Controle de acesso** e clique na visualização **Credenciais**.
2. Selecione a credencial com a qual você deseja pré-visualizar o modelo de crachá e, em seguida, clique na aba **Modelos de crachá**.

34

Gerenciamento global de titulares de cartão

Esta seção inclui os seguintes tópicos:

- "Gerenciamento global de titulares de cartão" na página 700
- "Sobre Global Cardholder Synchronizers" na página 704
- "Regras e restrições do Gerenciamento global de titulares de cartões" na página 705
- "Preparar para sincronizar entidades entre locais" na página 708
- "Sincronizar entidades entre locais" na página 709
- "Compartilhar entidades com outros locais" na página 711
- "Ignorar status sincronizados de titulares de cartão" na página 712

Gerenciamento global de titulares de cartão

O Gerenciamento global de titulares de cartão (GCM) é utilizado para sincronizar titulares de cartão entre instalações independentes do Security Center.

O GCM permite que você tenha um repositório central de informações de titular de cartão para toda a organização, quer essa informação seja gerenciada por um escritório central ou por escritórios regionais individuais. Os diferentes locais podem compartilhar informações entre suas instalações independentes com um sistema centralizado de gerenciamento de recursos humanos.

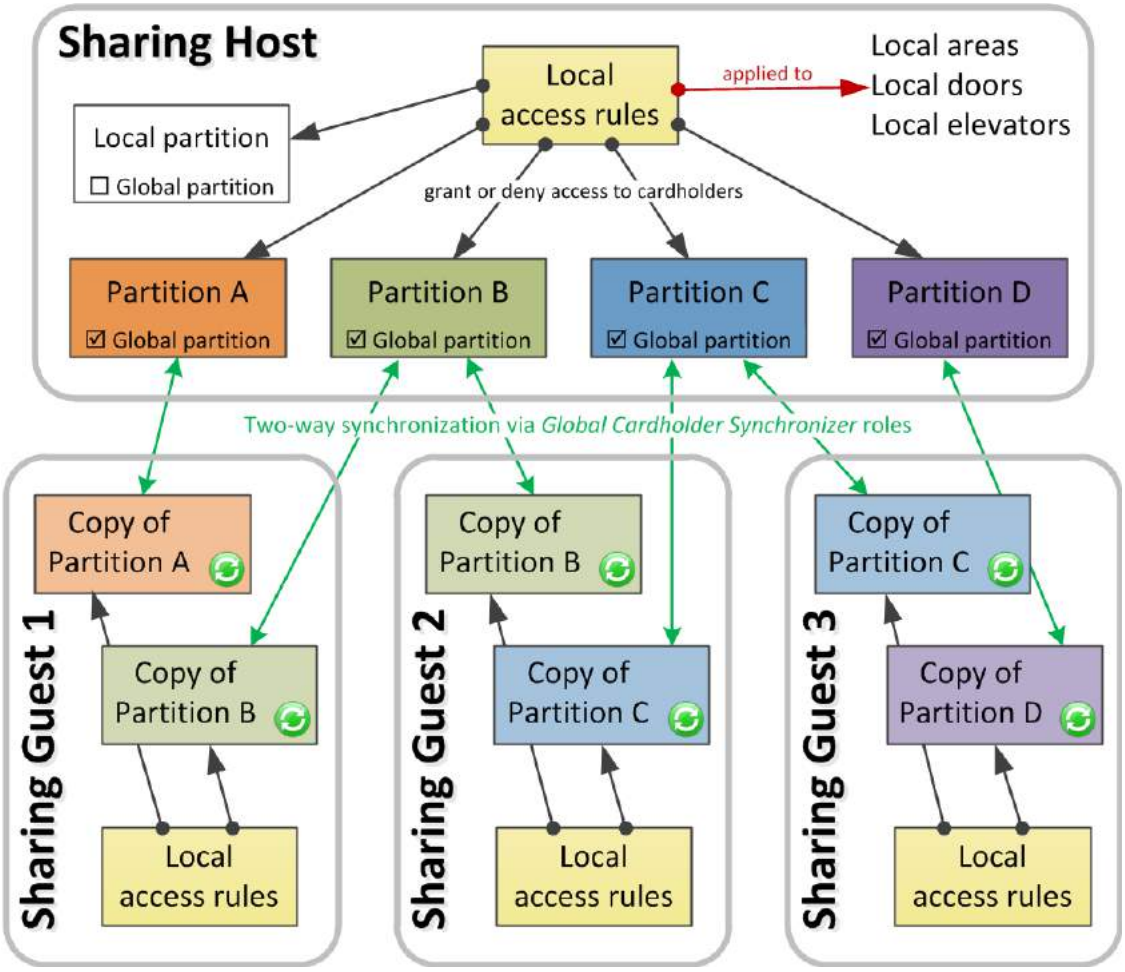
Cada escritório local continua a gerenciar os funcionários que trabalham em seu escritório local, como manter os perfis de funcionários, ID de foto, credenciais e assim por diante. Para os funcionários que precisam viajar de um local para outro, essa mesma informação pode ser compartilhada entre todos os locais da organização.

Com o gerenciamento global de titulares de cartão, é possível:

- Criar titulares de cartão globais a partir de um local central (por exemplo, sua sede) e sincronizá-los em sistemas remotos do Security Center que operam de forma independente do sistema central e uns dos outros.
- Permitir que administradores do sistema locais decidam quais áreas os titulares de cartão globais podem ou não acessar em suas instalações locais.
- Permitir que administradores de sistema locais efetuem alterações aos titulares de cartões globais e suas entidades relacionadas e sincronizem essas alterações com outros sistemas de compartilhamento.
- Permitir que administradores de sistema locais mantenham a posse exclusiva de seus titulares de cartão locais e entidades relacionadas, ao mesmo tempo em que compartilham titulares de cartão globais com outros sistemas.

Arquitetura de Gerenciamento global de titulares de cartão

Para compartilhar titulares de cartão em vários sistemas independentes do Security Center, um dos sistemas deve funcionar como o *host de compartilhamento*, enquanto os outros funcionam como *convidados de compartilhamento*.



Sistema host de compartilhamento

O host de compartilhamento é o sistema do Security Center que você escolher para *iniciar* o processo de compartilhamento, criando uma *partição global* naquele sistema. Todos os *titulares de cartão*, *grupos de titulares de cartão*, *credenciais* e *modelos de crachá* que são membros da partição global ficam automaticamente disponíveis para compartilhamento. Outros tipos de entidades podem ser parte da partição global, mas não serão visíveis para os convidados de compartilhamento.

O host de compartilhamento tem a *cópia mestre* da partição global e das entidades contidas nela. Todas as alterações feitas pelos convidados de compartilhamento para o conteúdo da partição global devem primeiro ser validadas pelo host de compartilhamento antes de serem propagadas para outras partes do compartilhamento.

A partição global é como um banco de dados central, o host de compartilhamento é como o servidor de banco de dados, enquanto os convidados do compartilhamento são como os clientes do banco de dados. Não há limite para o número de partições globais que um sistema host pode compartilhar.

Sistemas convidados do compartilhamento

O convidado de compartilhamento é um sistema do Security Center que *participa* no processo de compartilhamento. A participação é obtida criando uma função Sincronizador de Titular de Cartão Global (GCS) nesse sistema e usando-a para conectar o convidado do compartilhamento ao host do compartilhamento.

Como administrador do convidado de compartilhamento, você decide quais partições compartilhadas pelo host são de interesse para o seu sistema. Em seguida, a função GCS cria uma cópia das partições e

entidades globais selecionadas em seu sistema local. Somente *titulares de cartão*, *grupos de titulares de cartão*, *credenciais* e *modelos de crachá* são elegíveis para compartilhamento. As entidades compartilhadas são identificadas visualmente com um ícone verde ( ) sobreposto ao ícone de entidade regular.

Você pode atribuir regras de acesso local e credenciais aos titulares de cartões globais para conceder-lhes acesso às suas áreas locais, portas e elevadores. Você pode criar, modificar e excluir entidades da partição global. As ações que você pode realizar dependem dos direitos do *usuário* que representa a função GCS no host de compartilhamento. Todas as alterações feitas a entidades globais no sistema convidado devem ser validadas no sistema host. Todas as modificações rejeitadas no sistema host também são rejeitadas no seu sistema local.

Diferenças entre Federation™ e GCM

O gerenciamento global de titulares de cartão (GCM) e o Federation™ são ambos usados para compartilhamento de informações no Security Center, mas os titulares de cartão e outras informações são compartilhados de forma diferente.

A tabela a seguir destaca as diferenças entre o GCM e o Federation™.

MELHOR PRÁTICA: Use o GCM e o Federation™ em conjunto no mesmo sistema para um complementar o outro.

Federation™ (aplicado ao controle de acesso)	Gerenciamento Global de Titulares de Cartão (GCM)
Objetivo: Monitoramento central de atividades/ eventos	Objetivo: Compartilhamento de uma configuração central
Permite que uma organização *monitore*, a partir de uma localização central (host do Federation™) os eventos e as atividades de controle de acesso em locais remotos independentes (locais federados).	Permite que uma organização *compartilhe* a configuração comum de entidades de controle de acesso hospedadas em uma localização central (host de compartilhamento), com locais remotos independentes (convidados do compartilhamento).
O host do Federation™ usa a função Federation™ do Security Center para se conectar a locais remotos.	Os locais remotos usam a função Sincronizador de Titular de Cartão Global para se conectar ao host de compartilhamento.
Entidades criadas em locais remotos são federadas no sistema central.	Entidades criadas no sistema central são compartilhadas nos locais remotos.
O host do Federation™ pode observar, mas não pode alterar nada nos locais remotos.	O local remoto pode criar, modificar e excluir as entidades que são compartilhadas pelo host com todos os outros locais remotos (sincronização bidirecional).
Um local federado não tem visibilidade sobre o que está acontecendo no host do Federation™ ou em outros locais federados.	Todos os convidados do compartilhamento têm o mesmo acesso de leitura/gravação para todas as entidades compartilhadas (globais), mantendo a propriedade total das entidades locais.
Quase todas as entidades que geram eventos podem ser federadas (monitoradas).	Somente titulares de cartão, grupos de titulares de cartão, credenciais e modelos de crachá podem ser compartilhados.
Os campos personalizados não são federados.	Todos os campos personalizados e os tipos de dados são compartilhados.
Um titular de cartão federado pode obter acesso à instalação gerenciada pelo host do Federation™, mas não o inverso.	Um titular de cartão global pode ter acesso a todas as instalações que participam do compartilhamento.

Tópicos relacionados

Regras e restrições do Gerenciamento global de titulares de cartões na página 705
Sobre o recurso Federation na página 224

Diferenças entre integração do Active Directory e GCM

O gerenciamento global de titulares de cartão (GCM) e a integração do Active Directory são usados para centralizar o gerenciamento de informações de titulares de cartão no Security Center, mas as abordagens são diferentes.

A tabela a seguir destaca as diferenças entre o GCM e a integração do Active Directory.

MELHOR PRÁTICA: Use a integração do Active Directory e o GCM em conjunto. O host de compartilhamento deve ser o único sistema que se integra com o Active Directory. Essa solução mantém o Active Directory protegido na LAN corporativa, enquanto o host de compartilhamento apenas passa as informações dos funcionários que precisam ser compartilhadas com os sistemas satélites.

Integração do Active Directory	Gerenciamento Global de Titulares de Cartão (GCM)
Objetivo: Gerenciamento centralizado de segurança de funcionários (usuários e titulares de cartão)	Objetivo: Gerenciamento centralizado de segurança de funcionários (titulares de cartão)
Permite que uma organização *gerencie* as informações de funcionários a partir de um local central e as compartilhe com um único sistema Security Center (usuários e titulares de cartão).	Permite que uma organização *gerencie* as informações de titulares de cartão a partir de um local central e as compartilhe com todos os sistemas Security Center da organização.
O serviço de diretórios corporativo é a origem das informações. O Security Center obtém as informações de funcionários do serviço de diretórios corporativo.	Um sistema Security Center funciona como a origem das informações (host de compartilhamento) e a compartilha com todos os outros sistemas Security Center da organização (convidados de compartilhamento).
O sistema Security Center se conecta à origem das informações (serviço de diretórios) pela função Active Directory.	Os convidados de compartilhamento se conectam à fonte de informações (host de compartilhamento) por meio da função Sincronizador do Titular do Cartão Global.
Os campos personalizados definidos no Active Directory podem ser vinculados a campos personalizados do Security Center.	Todos os campos personalizados e os tipos de dados são compartilhados.
As informações compartilhadas do funcionário só podem ser modificadas no Active Directory. Somente a imagem do titular de cartão pode ser carregada no Security Center e atualizada no Active Directory.	As informações compartilhadas podem ser modificadas por todos os participantes do compartilhamento. O host de compartilhamento valida e propaga as alterações a todos os participantes do compartilhamento.
As informações de origem só podem ser compartilhadas com um sistema Security Center. Se vários sistemas Security Center precisarem compartilhar as mesmas informações, eles precisam se conectar individualmente ao serviço de diretórios corporativo.	O sistema Security Center central pode compartilhar as informações de titulares de cartão com quantos sistemas Security Center satélite forem necessários.

Sobre Global Cardholder Synchronizers

A função Global Cardholder Synchronizer garante a sincronização bilateral de titulares de cartão compartilhados e suas entidades relacionadas entre o sistema local (convidado de compartilhamento) onde ela reside e o sistema central (host de compartilhamento).

Cada sistema pode ter apenas uma instância dessa função.

O Sincronizador Global de Titulares de Cartão pode sincronizar o host e o convidado usando os três modos a seguir:

- **Sob demanda:** O sistema convidado só é sincronizado quando solicitado por um usuário.
- **Por agendamento:** O sistema convidado é sincronizado no horário usando uma tarefa agendada.
- **Automaticamente:** O sistema convidado é sincronizado automaticamente.

A sincronização de convidado para host é sempre executada imediatamente pela função GCS, porque todas as alterações nas partições globais devem ser validadas pelo sistema host antes que possam ser aceitas pelo sistema convidado. O sistema host processa as solicitações de alteração com base em primeiro a chegar, primeiro a ser atendido. A função Global Cardholder Synchronizer (GCS) deve permanecer conectada ao host do compartilhamento para manter as cópias locais das *entidades globais* sincronizadas com o host.

NOTA: O Global Cardholder Synchronizer pode sincronizar até um máximo de 250.000 credenciais.

Regras e restrições do Gerenciamento global de titulares de cartões

Existem algumas regras e restrições que se aplicam ao usar o Gerenciamento global de titulares de cartões.

Antes de começar a gerenciar globalmente os seus titulares de cartão, leia as seguintes regras e restrições.

Regras relativas a partições locais e globais

- Um convidado de compartilhamento não pode ter mais de um host. Apenas uma instância da função GCS é permitida por sistema.
- Uma partição global não pode ser modificada em um convidado de compartilhamento, mas seus membros podem. O que o convidado de compartilhamento está realmente autorizado a modificar está sujeito aos privilégios do usuário atribuídos à função GCS.
- Nenhum sistema tem permissão para compartilhar o que não possui. Não é permitido o compartilhamento em duas camadas. Um efeito desta regra é que uma partição local não pode ser convertida em uma partição global se ela contiver entidades globais, a menos que seja executada no sistema host.
- Adicionar uma entidade local a uma partição global transfere a propriedade dessa entidade do seu proprietário local (convidado do compartilhamento) para o proprietário da partição (host de compartilhamento).
- A exclusão de uma entidade global em um convidado de compartilhamento também a exclui no host de compartilhamento, a menos que essa entidade também pertença a outra partição global, nesse caso, somente sua associação será removida da primeira partição.

Regras relativas a entidades locais e globais

- Uma entidade é global em virtude de sua associação a uma partição global. Isso significa que um titular de cartão não se torna automaticamente global simplesmente porque seu grupo de titulares de cartão pai é global.
- As regras de acesso local também podem ser aplicadas a titulares de cartão locais e globais. As regras de acesso nunca são compartilhadas. Isso garante que os administradores locais sempre tenham total controle sobre a segurança de suas instalações locais.
- Os titulares/grupos de titulares de cartão globais podem se tornar membros de grupos de titulares de cartão locais.
- Os titulares/grupos locais não podem se tornar membros de grupos de titulares de cartão globais. Uma exceção a esta regra é quando ambas as entidades pertencem ao mesmo sistema. Neste caso, o titular de cartão local não pode ser compartilhado, embora o grupo de titulares de cartão possa.
- As credenciais globais e locais podem ser atribuídas a titulares de cartão globais.
- As credenciais globais não podem ser atribuídas a titulares de cartão locais.
- As credenciais globais usando formatos de cartão personalizados podem ser usadas e editadas no convidado do compartilhamento. No entanto, os dados de credenciais só seriam visíveis se o formato de cartão personalizado correspondente (arquivo XML) também estiver definido no convidado de compartilhamento usando a ferramenta *Editor de formato de cartão personalizado*.

MELHOR PRÁTICA: É sempre recomendável aplicar regras de acesso a grupos do titulares de cartão, em vez de titulares individuais. Por este motivo, recomenda-se o compartilhamento de titulares de cartão juntamente com os seus grupos de titulares de cartão pais. Se isso não for possível por qualquer motivo, recomendamos que você crie um grupo de titulares de cartão local para os titulares de cartão globais.

Regras relativas a campos personalizados e tipos de dados globais

- Campos personalizados e tipos de dados definidos para entidades globais são automaticamente compartilhados quando as entidades globais são compartilhadas.
- As definições de campos personalizados e tipos de dados globais não podem ser modificadas no convidado do compartilhamento.
- Os campos personalizados globais e locais permanecem separados, mesmo quando eles usam o mesmo nome. Eles são diferenciados pelo seu proprietário, que é o sistema que os define.
- Os tipos de dados globais não podem ser usados para definir campos personalizados locais.
- Os valores de campos personalizados de entidades globais podem ser modificados em convidados de compartilhamento.
- Os campos personalizados globais também se aplicam a entidades locais, mas seus valores permanecem locais.
- Os campos personalizados locais também se aplicam a entidades globais, mas seus valores permanecem locais.
- Quando um sistema convidado deixa de compartilhar uma partição global, todas as cópias locais das entidades globais compartilhadas e os valores de campos personalizados das entidades locais são excluídos.

MELHOR PRÁTICA: Se você quiser implementar o GCM em sua organização, recomendamos que defina todos os campos personalizados e tipos de dados para entidades globais no host de compartilhamento.

Regras relativas a Federation™ e entidades globais

- Se um *host de compartilhamento* também federar seu *convidado de compartilhamento*, somente as entidades locais pertencentes ao convidado de compartilhamento são federadas. As entidades que são compartilhadas não serão federadas no host de compartilhamento.
- O host de compartilhamento que também é um host de *federação* não deve compartilhar as entidades que federa adicionando-as a uma *partição global*, porque não possui as *entidades federadas*. Uma entidade só pode ser compartilhada pelo seu proprietário legítimo. Para que as entidades federadas sejam compartilhadas, o sistema federado precisa ser um convidado de compartilhamento do host do Federation™. Isso dá ao host do Federation™ o direito de compartilhar qualquer uma das entidades federadas.
- Um convidado de compartilhamento que passa a federar um terceiro sistema não pode compartilhar suas entidades federadas com o host de compartilhamento, porque ele não é o proprietário das entidades federadas.
- Se um convidado de compartilhamento for federado por outro sistema, suas entidades locais e globais aparecerão como entidades federadas no host do Federation™.

Regras relativas ao Active Directory e a entidades globais

- Os titulares de cartão e os grupos de titulares de cartão importados de um Active Directory podem ser adicionados a uma partição global no host de compartilhamento.
- Os portadores de cartão e os grupos de portadores de cartão importados de um Active Directory local para o *convidado de compartilhamento* não podem ser adicionados a uma partição global porque o Active Directory e o *host de compartilhamento* não podem ambos ser proprietários dos titulares de cartão compartilhados.
- Os titulares de cartão e grupos de titulares de cartão globais importados de um Active Directory só devem ser modificados através do serviço de diretório que os possui.

CUIDADO: Embora seja possível modificar titulares de cartão e grupos de titulares de cartão globais importados de um Active Directory no convidado de compartilhamento, essas alterações são temporárias. Você perde as alterações feitas quando o host de compartilhamento é sincronizado com o Active Directory.

MELHOR PRÁTICA: Se toda a entrada de dados de titulares de cartão tiver de ser centralizada, o sistema que importa titulares de cartão do Active Directory corporativo deve atuar como host de compartilhamento e todas as modificações devem ser feitas usando o serviço de diretório.

Tópicos relacionados

Importar grupos de segurança de um Active Directory na página 389
Sobre entidades federadas na página 225
Formatos de cartão personalizados na página 689

Preparar para sincronizar entidades entre locais

Antes de poder compartilhar e sincronizar titulares de cartão, grupos de titulares de cartão, credenciais e modelos de crachás entre locais, há algumas etapas que você deve seguir.

Antes de iniciar

IMPORTANTE: Você não deve tentar implantar a solução de Gerenciamento global de titulares de cartões sozinho se você pretende reunir sistemas que têm dados para compartilhar em ambas as extremidades, o que significa que tanto o host de compartilhamento como o convidado de compartilhamento têm dados existentes para compartilhar. Se esta é a sua situação, recomendamos que marque uma consulta técnica com um especialista da GTAP.

Para preparar a sincronização de entidades entre locais:

1 Decida qual sistema do Security Center será o host de compartilhamento.

O host de compartilhamento normalmente é o sistema em execução em sua sede ou o sistema sincronizado com o Active Directory corporativo.

2 Se o host de compartilhamento estiver protegido por um firewall, abra uma porta para permitir que a função Global Cardholder Synchronizer se conecte ao host de compartilhamento.

3 Decida que tipos de atualizações os usuários nos sistemas convidados podem executar nas partições globais compartilhadas.

Você pode limitar sua gama de ações restringindo os privilégios do usuário que representa as funções GCS no sistema host.

4 Certifique-se de seguir as melhores práticas recomendadas:

- Evite atribuir titulares do cartão diretamente a regras de acesso. Em vez disso, atribua grupos de titulares de cartão.
- Evite atribuir titulares de cartão ou grupos de titulares de cartão diretamente a portas. Em vez disso, use regras de acesso.

5 Faça backup do banco de dados do Directory em todos os sistemas em que pretende sincronizar e ativar backups agendados.

Após terminar

Compartilhe entidades entre locais.

Tópicos relacionados

Portas usadas por aplicativos principais no Security Center na página 1137
Diferenças entre integração do Active Directory e GCM na página 703

Sincronizar entidades entre locais

Para compartilhar informações com outros locais no seu sistema, é possível sincronizar titulares de cartão, grupos de titulares de cartão, credenciais e modelos de crachá.

Antes de iniciar

Prepare a sincronização.

Para sincronizar entidades entre locais:

1 No host de compartilhamento, crie partições globais ou altere o status de partições locais para global.
2 Crie um usuário com o nível adequado de privilégios administrativos sobre as entidades compartilhadas a serem usadas para conectar as funções GCS ao host de compartilhamento.

   Talvez seja necessário criar mais de uma conta de usuário se os convidados de compartilhamento tiverem requisitos de atualização diferentes.

3 Em cada sistema de convidado do compartilhamento, crie uma função GSC e sincronize o convidado do compartilhamento com o host de compartilhamento.
4 Atribua usuários locais a partições globais ( ).
5 Aplique regras de acesso local a titulares de cartão ( ) e grupos de titulares de cartão globais ( ).

   NOTA: Formatos de cartão personalizados não são compartilhados. Se você tiver credenciais compartilhadas que usam formatos de cartão personalizados, as credenciais funcionarão no seu sistema local, mas não será possível exibir os campos de dados do cartão, a menos que o formato de cartão personalizado em uso também esteja definido no sistema local.

6 Crie uma tarefa agendada para sincronizar periodicamente o seu sistema local com o host.

Tópicos relacionados

Ferramenta de edição de formato de cartão personalizado na página 690

Configurar partições para sincronização

A sincronização de entidades é iniciada no host de compartilhamento definindo uma partição como partição *global*.

O que você deve saber

Não é possível compartilhar a *Partição pública*.

Para configurar uma partição para sincronização:

1 Abra a tarefa **Controle de acesso** e selecione a visualização **Titulares de cartão e credenciais**.
2 Se as partições estiverem ocultas, clique em **Mostrar partições** ( )
3 Selecione a partição que deseja compartilhar.
4 Clique na aba **Propriedades** e altere a opção **Partição global** para **Ativo**.

A partição fica visível para todas as funções GCS conectadas a este sistema. Somente titulares de cartão, grupos de titulares de cartão, credenciais e modelos de crachá são compartilhados.

Sincronização do seu sistema com a hospedagem de compartilhamento

Você deve criar e configurar a função Sincronizador do Titular do Cartão Global (GCS) para conectar seu sistema local ao host de compartilhamento.

Para sincronizar seu sistema com a hospedagem de compartilhamento:

1 Abra a tarefa **Sistema** e clique na visualização **Funções**.

2 Clique em **Adicionar uma entidade** ( ) > **Global Cardholder Synchronizer**.

3 Na página **Informações Específicas**, digite os seguintes parâmetros e clique em **Próximo**.

- **Servidor:** *Servidor* onde esta função será hospedada.
- **Diretório:** Nome do *servidor principal* do host de compartilhamento. Se qualquer coisa diferente da porta de conexão padrão (5500) for usada, você deve indicar explicitamente o número da porta após o nome do Directory, separado por dois pontos. Por exemplo: `HostServer:5888`.
- **Nome de usuário e senha:** Credenciais usadas para conectar à hospedagem compartilhada. O alcance do visitante compartilhado pode fazer na divisão global será limitada pelo que este usuário pode ver e fazer na hospedagem compartilhada.

  O usuário deve ter o privilégio *Global Cardholder Synchronizer* no host de compartilhamento para se conectar.

4 Na página de **Informação básica**, digite o nome, a descrição e a divisão onde a função de GCS deve ser criada.

As partições determinam quais usuários do Security Center têm acesso a essa entidade. Somente usuários que receberam acesso à partição podem ver a função GCS.

5 Clique em **Seguinte**, **Criar** e **Fechar**

Uma nova função Sincronizador do Titular do Cartão Global ( ) é criada. Aguarde alguns segundos para que a função se conecte ao host de compartilhamento.

6 Clique na aba **Propriedades**, em seguida clique em **Atualizar** ( ) .

As partições compartilhadas pelo host estão listadas em **Partições globais**.

7 Selecione as partições que deseja que seu sistema local compartilhe e clique em **Aplicar**.

8 Clique em **Sincronizar** ( ).

A função GCS cria uma cópia local de todas as entidades compartilhadas no seu sistema. Isso pode demorar um pouco, dependendo de quantas entidades você está compartilhando.

Após terminar

Configure as entidades globais que você compartilhou para que possam ser usadas em seu sistema local.

Compartilhar entidades com outros locais

Compartilha uma entidade adicionando-a a uma partição global. Isso pode ser feito tanto a partir do host de compartilhamento ou do convidado de compartilhamento. Você também pode criar uma nova entidade diretamente em uma partição global.

O que você deve saber

Uma *entidade global* é uma entidade compartilhada por vários sistemas independentes do Security Center em virtude de sua associação a uma *partição global*. Somente titulares de cartão, grupos de titulares de cartão, credenciais e modelos de crachá são elegíveis para compartilhamento

Para compartilhar uma entidade com outro local:

1 Abra a tarefa **Controle de acesso** e selecione a visualização **Titulares de cartão e credenciais**.
2 Se as partições estiverem ocultas, clique em **Exibir partições** ( )
3 Selecione a partição global a partir da qual deseja compartilhar e clique na aba **Propriedades**.
4 Na seção **Membros**, clique em **Adicionar** ( ).
5 Na caixa de diálogo **Pesquisa** que aparecerá, selecione a entidade que deseja compartilhar e clique em **Selecionar**.

   No convidado de compartilhamento, apenas os titulares de cartões, grupos de titulares de cartões, credenciais e modelos de crachá podem ser adicionados a uma partição global.

No host de compartilhamento, o efeito dessa ação é imediatamente visível. Em um convidado de compartilhamento, a entidade recém-compartilhada não aparece até que uma sincronização seja executada em sua função GSC.

Tópicos relacionados

Abas de configuração do Global Cardholder Synchronizer na página 1063

Interromper o compartilhamento de entidades com outros locais

Você para de compartilhar uma entidade removendo-a de sua partição global. Isso pode ser feito tanto a partir do host de compartilhamento ou do convidado de compartilhamento.

O que você deve saber

Se você remover uma entidade compartilhada do sistema de convidados de compartilhamento, a entidade será convertida de uma entidade global para uma entidade local.

CUIDADO: A remoção de uma entidade compartilhada de uma partição global a exclui de todos os outros sistemas que possam compartilhá-la, mesmo do host de compartilhamento.

Para parar o compartilhamento de uma entidade com outro local:

1 Abra a tarefa **Controle de acesso** e selecione a visualização **Titulares de cartão e credenciais**.
2 Se as partições estiverem ocultas, clique em **Mostrar partições** ( )
3 Na seção **Membros**, selecione a entidade que deseja parar de compartilhar e clique em **Remover** ( ).
4 Para confirmar a ação, clique em **Remover**.

Após terminar

Qualquer entidade removida de uma partição acaba na partição raiz. Se a partição raiz não estiver onde você quer que ela fique, mova-a para outra partição local.

Ignorar status sincronizados de titulares de cartão

Se a função GCS estiver desconectada do host de compartilhamento e você precisar alterar o status do titular do cartão, poderá substituir a sincronização de entidade.

O que você deve saber

Se a função GCS estiver desconectada do host de compartilhamento, todas as entidades globais no convidado de compartilhamento ficam inativas (em vermelho) e não é possível fazer mais alterações porque elas não podem ser validadas pelo host de compartilhamento. No entanto, se você precisa urgentemente desativar um titular de cartão (por exemplo, se um funcionário acabou de ser demitido) você pode *anular* temporariamente a sincronização.

Para substituir o status de um titular de cartão sincronizado:

1 Abra a tarefa **Controle de acesso** e clique na visualização **Titulares de cartão e credenciais**.
2 Selecione o titular de cartão global que você precisa ativar ou desativar.
3 Clique na aba **Propriedades** e altere a opção **Status** para **Anular**.

O ícone do titular de cartão muda para . Agora você pode alterar o status do titular de cartão.

4 Faça as alterações necessárias e clique em **Aplicar**.

Após terminar

Quando a conexão com o host de compartilhamento for restabelecida, ative a sincronização novamente.

35

Ferramenta de importação

Esta seção inclui os seguintes tópicos:

- "Sobre a Ferramenta de importação" na página 714
- "Arquivos CSV e a ferramenta de importação" na página 715
- "Notas sobre nomes de entidades importadas" na página 717
- "Importar titulares de cartão e credenciais" na página 718
- "Substituir credenciais" na página 721
- "Substituir grupos de titulares do cartão" na página 722
- "Campos do banco de dados suportados pela ferramenta de importação" na página 724

Sobre a Ferramenta de importação

É uma ferramenta que permite importar titulares de cartão, grupos de titulares e credenciais de um arquivo CSV (Comma Separated Values - Valores separados por vírgula).

O arquivo CSV deve ser em texto simples com delimitadores (vírgulas, espaços, pontos e assim por diante) para separar os campos. Os campos delimitados nos arquivos de texto representam valores como nome, sobrenome, grupo do titular do cartão, caminho e nome do arquivo da foto do funcionário e assim por diante.

A opção de licença do Security Center da *Ferramenta de importação* deve ser ativada em seu sistema para que esta ferramenta fique disponível. Apenas usuários administrativos podem usar esta ferramenta.

Você pode usar a ferramenta de importação segundo uma agenda, usando a ação *Importar do arquivo*.

Como usar a ferramenta de Importação

Você pode usar a ferramenta de Importação para fazer o seguinte:

- Importar credenciais isoladamente (nome de credencial, formato de cartão, código de instalação e número de cartão, status e a *partição* à qual a credencial pertence);
- Importar titulares de cartão isoladamente (nome do titular de cartão, descrição, imagem, e-mail, status, *campos personalizados* e o grupo e a partição aos quais o titular de cartão pertence);
- Importar titulares de cartão e credenciais em conjunto (neste caso, o titular do cartão e a credencial são especificados na mesma linha e ligados automaticamente entre si).
- Substituir credenciais antigas por novas.

Limitações da ferramenta de Importação

Se você estiver importando vários titulares que são membros de diferentes partições, e não houver nenhum grupo de titulares de cartões ou se houver apenas um grupo de titulares de cartões especificado no ficheiro CSV, os titulares de cartões importados são adicionados a todas as partições.

Tópicos relacionados

Substituir credenciais na página 721
Tarefas agendadas na página 218

Arquivos CSV e a ferramenta de importação

Para que você possa importar arquivos CSV usando a ferramenta de importação, o arquivo CSV precisa seguir um determinado formato e incluir informações específicas para cada tipo de entidade. Esses arquivos podem ser criados a partir de uma planilha do Excel.

Informações mínimas exigidas nos arquivos CSV

As informações encontradas no arquivo CSV devem ser coerentes ou não serão aceitas pela ferramenta de importação. Quando as informações necessárias estão ausentes, o botão *Próximo* na página Vínculos é desativado. Cada tipo de entidade importada requer um mínimo de informação.

A tabela a seguir descreve o que é necessário para cada tipo de entidade.

Tipo da entidade	Informações mínimas requeridas
Credencial - Cartão	Você tem a escolha de duas chaves de credenciais: • Preencha todos os campos requeridos com um determinado formato de cartão. • Forneça os *Dados do cartão da credencial*. Se você escolher um formato de cartão personalizado, todos os campos exigidos pelo formato do cartão devem estar vinculados a uma coluna no arquivo CSV. Caso contrário, o arquivo CSV será rejeitado. Quando a credencial está sendo importada, uma dessas duas chaves deve estar presente. Se ambas as chaves estiverem faltando valores, a linha será descartada. Se ambas as chaves estiverem presentes, somente os dados do cartão serão importados.
Credencial - Placa de veículo	Digite um número de placa de licença do titular do cartão. Utilize esse método se uma câmera Sharp for utilizada para acionar uma barreira de acesso de veículos. Nesse caso, a placa de veículo do titular do cartão pode ser usada como credencial.
Credencial - PIN	As credenciais do PIN podem ser usadas com cartões ou como credenciais autônomas. Certifique-se de que o PIN de cada titular do cartão seja único caso planeje usar os seus leitores em modo Cartão ou PIN.
Titular do cartão	A chave padrão do titular do cartão é a combinação do nome e sobrenome do titular do cartão. Um desses dois campos deve ser vinculado a uma coluna CSV se os portadores de cartão devem ser importados. Quando os portadores estão sendo importados, todas as linhas CSV devem ter um valor em pelo menos um desses dois campos. Se não, a linha será descartada.
Grupo de titulares de cartão	Só é necessário o nome do grupo do titular do cartão. A falta do grupo do titular de cartão não fará com que uma linha seja descartada.
Partição	Somente o nome da partição é necessário. A falta do nome da partição não fará com que uma linha seja descartada.

Formato do arquivo CSV

Segue um arquivo de exemplo chamado *EmployeeData.csv*, contendo 3 novos titulares de cartão a importar. Ele pode ser criado a partir de uma planilha do Excel usando o comando "salvar como" e selecionando o formato .csv.

O arquivo de exemplo contém as seguintes 4 linhas de texto:

```
#First name,Last name,Cardholder description,Cardholder email,Picture,
Cardholder group,Cardholder status,Credential name,Facility code,Card
 number,Credential status

Abdoulai,Koffi,Market Analyst,akoffi@genetec.com,C:\Data\Cardholder\Pictures\
Abdoulai Koffi.png,Marketing,Yes,82968378,102,8,active

Andrew,Smith,Sales Representative,asmith@genetec.com,C:\Data\Cardholder\Pictures\
Andrew Smith.png,Sales,Yes,82748590,101,12,active

Audrey,Williams,Technical Writer,awilliams@genetec.com,C:\Data\Cardholder\Pictures\
Audrey Williams.png,TechWriters,Yes,83748952,104,18,active
```

A primeira linha é uma linha de comentário, listando os campos do titular do cartão e da credencial que estão incluídos no arquivo CSV como referência. As três linhas seguintes contêm os campos que serão importados. Você também pode adicionar campos personalizados adicionais se eles tiverem sido criados para titular de cartão ou credenciais no Security Center.

Limitações de campos personalizados

Você pode importar valores de campo personalizado de titular de cartão e credencial de arquivos CSV com as seguintes limitações:

- Não é possível importar campos personalizados usando o tipo de dados *Entidade*.
- Campos personalizados que usem o tipo de dados *Data* devem ser importados com o formato 'AAAA-MM-DD'.
- O desempenho da ferramenta de importação diminui à medida que aumenta o número de campos personalizados por registro importado.
- Quando você tem um grande número de campos personalizados por registro, o número de registros que você pode importar de uma vez também pode ser limitado. Por exemplo, se seus registros contiverem 100 campos personalizados cada, incluindo um campo de dados de imagem de 25 KB, você só poderá importar 1000 registros por vez.

Tópicos relacionados

Campos do banco de dados suportados pela ferramenta de importação na página 724
Sobre campos personalizados na página 86

Notas sobre nomes de entidades importadas

O Security Center suporta várias entidades com o mesmo nome. Se um titular de cartão já existir no Security Center com a mesma combinação de nome e sobrenome de um que esteja sendo importado, somente o primeiro titular de cartão correspondente encontrado no Security Center será atualizado (por exemplo, com uma nova descrição do arquivo CSV importado).

Se houver dois grupos de titulares de cartão com o mesmo nome (por exemplo, criados em duas partições diferentes) e um titular de cartão importado for atribuído a um desses grupos de titulares de cartão, o titular de cartão será atribuído ao primeiro grupo de titulares encontrado. A mesma lógica também se aplica a partições.

Se o mesmo titular de cartão for importado duas vezes, cada vez para um grupo de titulares de cartão diferente, no final, o titular de cartão pertencerá a ambos os grupos de titulares de cartões. Novamente, a mesma lógica se aplica a partições.

No entanto, a associação entre titulares de cartão e credenciais pode ser tratada de forma diferente, consoante a credencial faça ou não parte da chave do titular de cartão.

Exemplo

Se a chave do titular de cartão for composta somente do nome e sobrenome do titular de cartão. O resultado de importar o seguinte arquivo CSV é a criação de um novo titular de cartão: Nome = Joe, Sobrenome = Dalton, E-mail = JDalton@genetec.com, com duas credenciais de cartão (12/555 e 12/556).

Nome	Sobrenome	Código da instalação	Número do cartão	E-mail
Joe	Dalton	12	555	jdalton@acme.com
Joe	Dalton	12	556	jdalton@acme.com

No entanto, se a credencial também fizer parte da chave do titular de cartão, o mesmo arquivo CSV gerará dois titulares de cartão separados com o mesmo nome, sobrenome e endereço de e-mail.

Importar titulares de cartão e credenciais

Para acelerar a configuração do seu sistema, você pode importar cartões e credenciais de um arquivo CSV em vez de criá-los manualmente no Security Center.

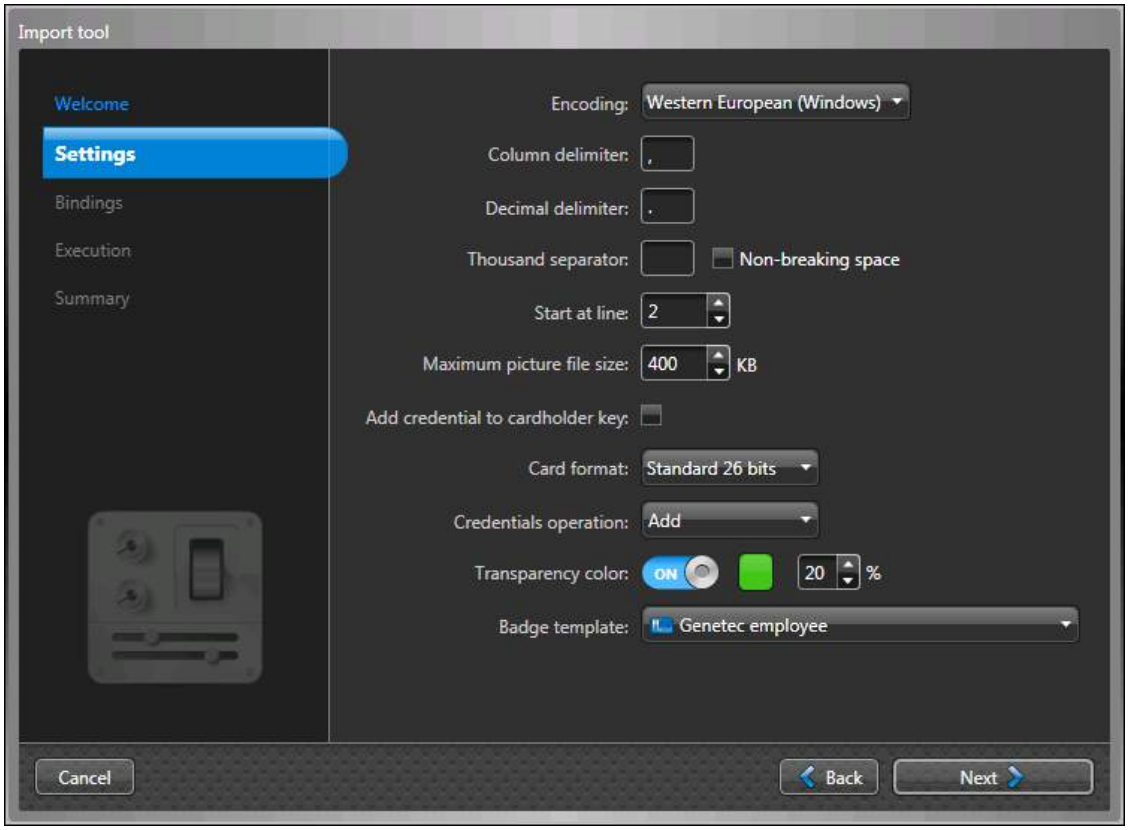
Para importar um titular de cartão ou uma credencial:

1 Na página inicial, clique em **Ferramentas** > **Ferramenta de importação**.

2 Digite o caminho para o arquivo CSV que deseja importar e clique em **Próximo**.

3 Na página **Configurações**, digite o tipo de **Codificação**.

Esta é a codificação de caracteres usada pelo arquivo CSV selecionado. A seleção padrão é a codificação padrão usada em seu PC. Se você abrir o arquivo CSV no seu PC e ver todos os caracteres exibidos corretamente, não é necessário alterar as configurações padrão.



4 Defina os delimitadores de campo CSV (Coluna, Decimal, Milhar).

Na primeira utilização, a ferramenta toma as definições de delimitador das Opções Regionais do Windows (**Painel de controle** > **Região e idioma** > **Configurações adicionais**). Após a primeira utilização, a ferramenta lembra as últimas configurações de delimitador que você usou. Por predefinição, o Microsoft Excel também utiliza os delimitadores de campo das Opções regionais do Windows ao salvar um arquivo CSV. Isso pode ser alterado no Excel. É recomendável que você abra o arquivo CSV no WordPad para confirmar os delimitadores de formatação obtidos. Quando usar um espaço como **Separador de milhares**, você pode especificar se o espaço pode ou não ser separável.

5 Defina onde a importação deve ser iniciada.

A primeira linha em um arquivo CSV é 1. Você pode optar por iniciar a importação em qualquer linha desejada. Por exemplo, você pode ignorar a primeira linha e usá-la como cabeçalho de coluna ou como linha de comentário. Uma linha de comentário é uma linha com o caractere de jogo da velha (#) na coluna 1.

6 (Opcional) Defina o tamanho máximo para arquivos de imagem.

Arquivos de imagem grandes (como os produzidos por câmeras digitais) podem rapidamente ocupar o banco de dados de configuração e ter impacto sobre o desempenho. Para minimizar o impacto de arquivos de imagem grandes, a ferramenta de importação automaticamente reduz seus tamanhos antes de carregá-los. Ela faz isso reduzindo a resolução da imagem até que o tamanho do arquivo fique abaixo do limite de **Tamanho máximo do arquivo de imagem**. O valor padrão é obtido das suas configurações do sistema de controle de acesso. Alterar o seu valor na ferramenta de importação também altera as definições do sistema.

7 Adicione a credencial como parte da chave do titular do cartão.

Por padrão, a ferramenta de importação usa a combinação de nome e sobrenome para identificar os titulares. Se um portador já existir no banco de dados, ele será atualizado com as informações lidas a partir do arquivo CSV. Se não, ele será adicionado. Usar apenas nome e sobrenome para diferenciar os titulares pode não ser suficiente. Uma solução é combinar as informações de credencial com a chave do titular do cartão. Isso é feito selecionando a opção **Adicionar credencial a chave de titular de cartão**. Com esta opção, duas linhas do arquivo CSV referem-se ao mesmo titular do cartão somente se elas contiverem o mesmo nome, sobrenome e dados de credencial do titular do cartão.

NOTA: Esta opção só é aplicável quando os titulares e as credenciais são importados do mesmo arquivo CSV. Quando esta solução não é aplicável, outras informações do titular do cartão podem ser usadas para fortalecer sua identificação.

8 (Opcional) Defina o **Formato do cartão** padrão.

O formato de cartão padrão é usado somente quando nenhum formato de cartão de credencial é especificado no arquivo CSV ou quando o campo identificado como **Formato do cartão** no arquivo CSV está em branco.

9 Selecione uma das seguintes opções de **Operação de credencial**:

- **Adicionar:** Esta é a opção padrão. Todas as credenciais lidas a partir do arquivo CSV são adicionadas como entidades ao seu sistema. Se uma credencial já existir em seu banco de dados, ela será atualizada.
- **Substituir:** Esta opção permite substituir credenciais antigas por novas. Na página **Vínculos** que aparece em seguida, você encontrará opções de campo adicionais para especificar os antigos (*anteriores*) e novos valores de credenciais.

10 (Opcional) Defina a transparência de fundo das imagens importadas do titular do cartão.

Se as imagens de titulares que você estiver importando tiverem sido tiradas na frente de uma tela de chroma key, você pode tornar o plano de fundo transparente. Isso é útil se você criar um modelo de crachá que tenha uma imagem em segundo plano.

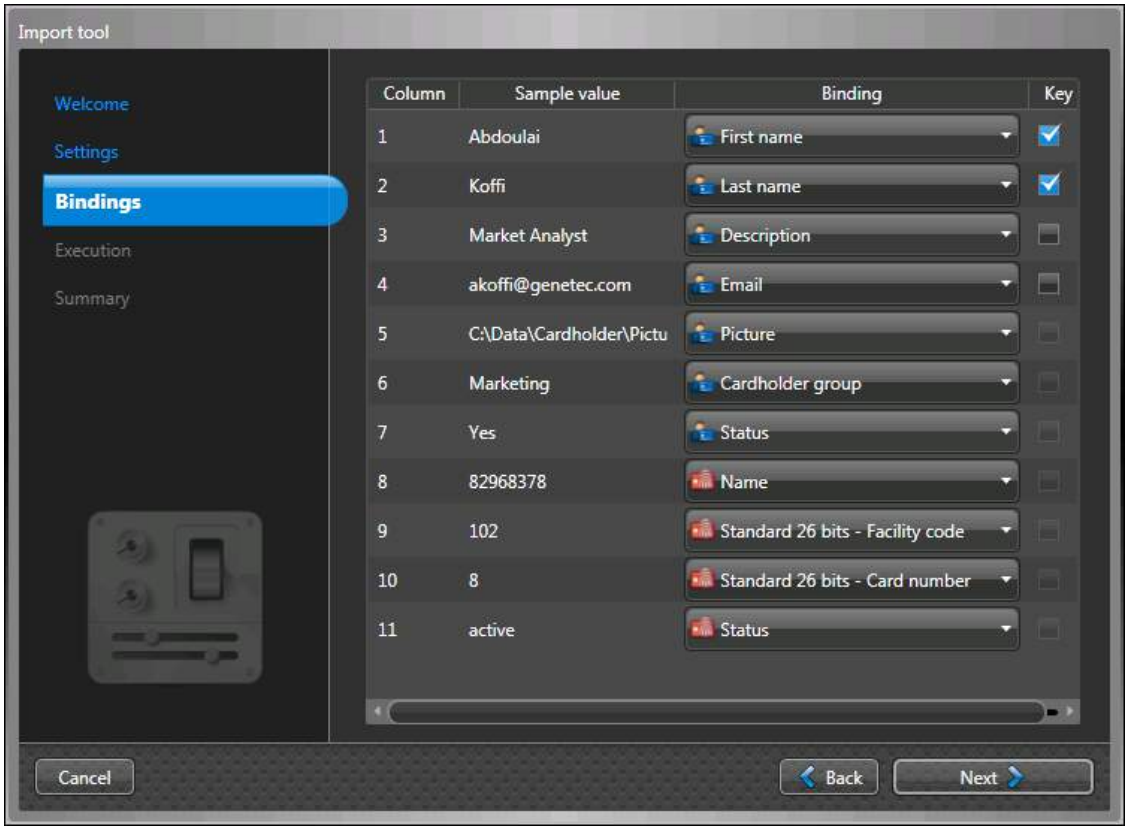
a) Coloque a opção **Cor de transparência** em **Ligado**.
b) Selecione a cor da tela de chroma key em que as fotos dos titulares foram tiradas (geralmente verde ou azul).
c) Defina a porcentagem de transparência.

11 (Opcional) Defina um **Modelo de crachá** padrão para os titulares de cartão importados.

Os modelos de crachá disponíveis são aqueles que você já criou no Config Tool.

12 Clique em **Próximo**.

A página de **Vínculos** aparecerá, exibindo dados de exemplos da primeira linha a ser importada do seu arquivo. A primeira linha a ser importada é a **Linha inicial**.



13 Vincule cada valor de amostra ao campo do banco de dados para o qual ele deve ser importado.

Se você precisar pular uma coluna no arquivo CSV, basta deixar a coluna **Vínculo** em branco.

NOTA: As informações lidas a partir do arquivo CSV são usadas para criar novas entidades em seu sistema. Para entidades como titulares de cartão e credenciais, é necessário um mínimo de informações. Se as informações estiverem incompletas, não será possível passar para a próxima etapa.

14 (Opcional) Adicione mais campos à chave do titular de cartão.

Quando você precisa mais do que o primeiro e o último nome para diferenciar os titulares, você pode complementar a chave do titular de cartão com informações adicionais. Isso é feito selecionando a caixa de seleção **Chave** ao lado de cada campo que deseja adicionar à chave do titular de cartão. Nem todos os campos podem ser parte da chave do titular de cartão. A caixa de verificação fica desativada se um campo não for elegível.

DICA: O outro método para fortalecer a identificação do titular de cartão é adicionar os dados de credencial à chave do titular de cartão.

15 Clique em **Próximo**.

A ferramenta de importação importa o conteúdo do arquivo CSV para o banco de dados. Uma janela de resumo aparecerá confirmando o número de entidades importadas e o número de erros encontrados.

16 Clique em para copiar e colar o conteúdo do relatório.

17 Clique em **Fechar**.

Tópicos relacionados

Campos do banco de dados suportados pela ferramenta de importação na página 724
Arquivos CSV e a ferramenta de importação na página 715
Definir o tamanho máximo de arquivos de imagem na página 656
Substituir credenciais na página 721
Projetar modelos de crachá na página 695

Substituir credenciais

Se você tiver várias credenciais que devem ser substituídas, você pode substituí-las todas ao mesmo tempo usando a ferramenta *Importar*.

Antes de iniciar

Crie um arquivo CSV com valores de credenciais antigos e novos. Cada linha deve conter a credencial antiga e a nova credencial para substituí-la.

O que você deve saber

A credencial antiga e nova devem usar o mesmo formato de cartão. Se as novas credenciais forem atribuídas aos mesmos titulares, elas também devem ser especificadas no arquivo CSV e não podem ser diferentes do titular atual das credenciais antigas.

Por exemplo, substituir credenciais é útil se você quiser dar a todos os funcionários em sua empresa novos cartões de identificação.

Para substituir uma credencial:

1. Na página inicial, clique em **Ferramentas** > **Ferramenta de importação**.
2. Digite o caminho para o arquivo CSV que deseja importar e clique em **Próximo**.
3. Na página **Configurações**, selecione **Substituir** como **Operação de credenciais** e clique em **Próximo**.
4. Na página **Vínculos**, vincule os valores de credenciais antigos com os campos identificados como **(valor anterior)** e os novos valores de credenciais com os campos não rotulados como **(valor anterior)**.
5. Clique em **Próximo**.

   A ferramenta de importação altera o status da credencial antiga para **Inativa**, enquanto cria a nova credencial como **Ativa**. Se os titulares também forem importados no mesmo arquivo, as novas credenciais serão associadas aos titulares do cartão.

   O resultado da operação é exibido em uma janela de resumo.
6. Clique em  para copiar e colar o conteúdo do relatório.
7. Clique em **Fechar**.

Tópicos relacionados

Importar titulares de cartão e credenciais na página 718

Substituir grupos de titulares do cartão

Caso precise reatribuir múltiplos grupos de titulares do cartão, você pode reatribuí-los de uma só vez usando a ferramenta de importação.

Antes de iniciar

Crie uma cópia do arquivo CSV existente do titular do cartão e atualize os dados dos grupos de titulares do cartão.

O que você deve saber

Substituir grupos de titulares do cartão em lotes é útil em contextos como o de um estudante que muda de grupos entre os semestres, pois diferentes cursos podem oferecer permissões de acesso diferentes.

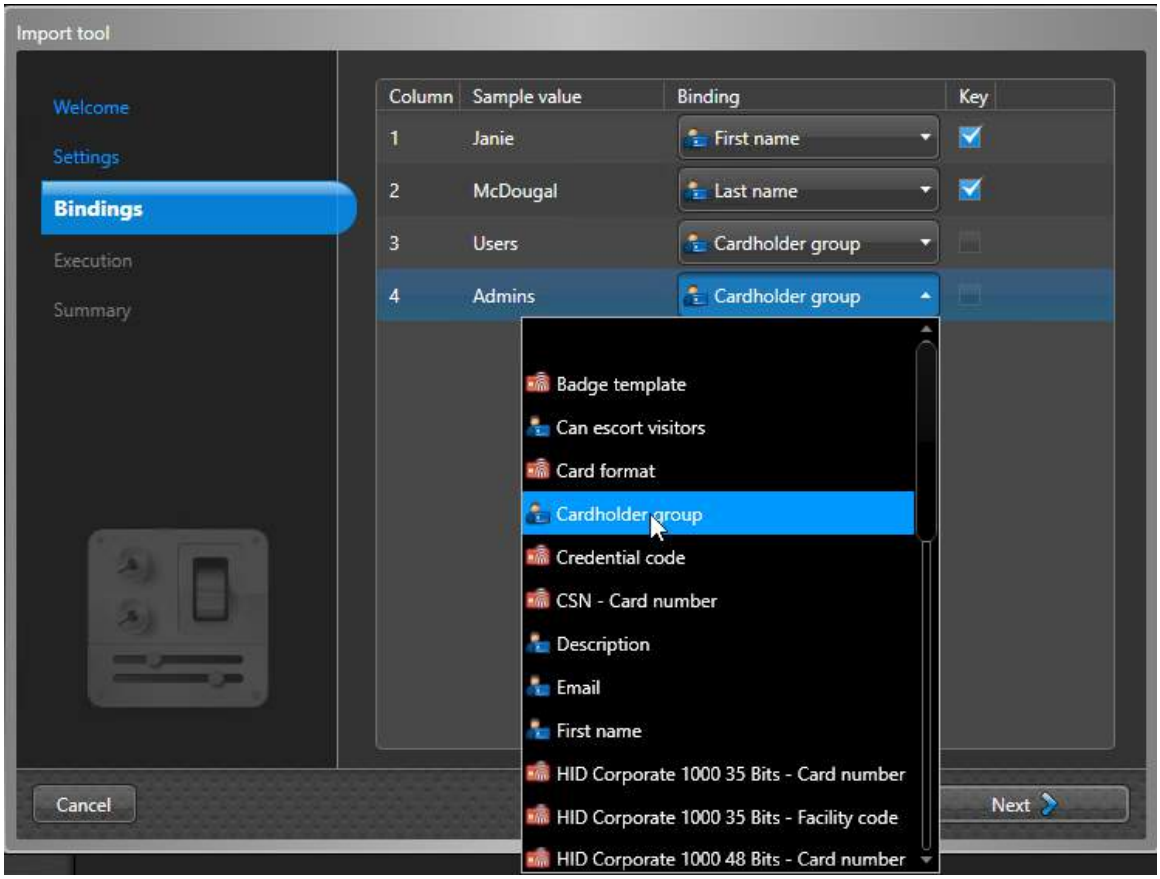
Para substituir um grupo de titulares do cartão:

1 Na página inicial do Config Tool, clique em **Ferramentas** > **Ferramenta de importação**.

2 Digite o caminho para o arquivo CSV que deseja importar e clique em **Próximo**.

3 Na página **Configurações**, da lista **Operação do grupo de titulares de cartão**, selecione **substituir** e clique em **Próximo**.

4 Na página **Vínculos**, defina as novas colunas do grupo do titular do cartão para **Grupo do titular do cartão**.



5 Clique em **Próximo**.

A ferramenta de importação atualiza a associação do grupo do titular do cartão para os novos grupos de titulares do cartão e exibe um resumo.

6 (Opcional) Clique em para copiar e colar o conteúdo do relatório.
7 Clique em **Fechar**.

Campos do banco de dados suportados pela ferramenta de importação

Usando a ferramenta de importação, você pode importar muitos campos de banco de dados de um arquivo CSV.

Nome do campo	Tipo de campo	Descrição
Data de ativação /	Cadeia	Cadeias em formato de data e hora.
Data de validade /	Cadeia	Cadeias em formato de data e hora.
Modelo do crachá	Cadeia	Credencial modelo de crachá
Formato do cartão	Número inteiro ou string sem assinatura	Formato de cartão de credencial. Você pode usar um dos seguintes valores: • 0 = Padrão 26 bits • 1 = HID H10306 34 Bits • 2 = HID H10302 37 Bits • 3 = HID H10304 37 Bits • 4 = HID Corporate 1000 35 Bits • 5 = HID Corporate 1000 48 Bits • CSN Para especificar um formato de cartão personalizado, você deve soletrá-lo exatamente da mesma maneira como o criou. Se nenhum formato de cartão for especificado em uma linha CSV, o formato padrão especificado na página de configurações de importação será usado.
{Formato} - Nome do campo	Formato de cartão padrão	Você pode especificar um campo em um formato de cartão específico, incluindo formatos de cartão personalizados.
{Formato} - Nome do campo (valor anterior)	Formato de cartão padrão	Campo de uma credencial antiga para substituir. Essas opções "(valor anterior)" aparecem somente se você selecionar *Substituir* como *Operação de credencial*
Titular do cartão <Nome de campo>	Como definido pelo campo personalizado	Campo personalizado do titular do cartão.
Grupo de titulares de cartão	Cadeia	Nome do grupo de titulares de cartão ao qual o titular deve pertencer. Se o grupo de titulares de cartão não existir, ele será criado na mesma partição que o titular do cartão.

Nome do campo	Tipo de campo	Descrição
CanEscort	Booleanos	Entradas válidas: • 0 • 1 • verdadeiro • falso • sim • não • ligado • desligado Para especificar um formato de cartão personalizado, você deve soletrá-lo exatamente da mesma maneira como o criou. Se nenhum formato de cartão for especificado em uma linha CSV, o formato padrão especificado na página de configurações de importação será usado.
Credencial <Nome de campo>	Como definido pelo campo personalizado	Campo personalizado de credencial.
Dados do cartão da credencial	Cadeia	O campo de dados do cartão permite que o usuário preencha os dados para formatos de cartão padrão e personalizados. Quando este campo é especificado, os campos de código de instalação e número de cartão são ignorados. Para todos os formatos de cartão padrão, a sequência deve conter o código de instalação seguido pelo número do cartão. Os separadores aceitos são os caracteres '/' e '|'. Por exemplo “35/20508” corresponde a Código de instalação = 35 e Número do cartão = 20508. Para um formato de cartão personalizado, os dados devem ser organizados de acordo com a definição de formato de cartão personalizado.
Descrição	Cadeia	Descrição da entidade do titular do cartão
E-mail	Cadeia	Endereço de e-mail do titular do cartão.
Nome	Cadeia	Primeiro nome do titular do cartão Este campo é parte da chave do titular de cartão padrão.
Sobrenome	Cadeia	Último nome do titular do cartão Este campo é parte da chave do titular de cartão padrão.
Placa de licença	Cadeia	Plate Reader de licença. Comprimento válido 1-32 dígitos.

Nome do campo	Tipo de campo	Descrição
Nome	Cadeia	Nome da entidade de credencial. Se nenhum nome for especificado, o valor padrão "Credencial importada" ou "Credencial importada não atribuída" será usado.
Partição	Cadeia	Nome da partição à qual o titular deve pertencer. Se a partição não existir, ela será criada. Se não for especificado, o titular de cartão é colocado na partição do sistema.
Partição	Cadeia	Nome da partição à qual a credencial deve pertencer. Se a partição não existir, ela será criada. Se não for especificado, a credencial de cartão é colocada na partição do sistema.
Foto	Cadeia	Caminho para um arquivo de imagem do titular de cartão (bmp, jpg, gif ou png). O caminho deve fazer referência a um arquivo localizado na máquina local ou na rede.
PIN	Número inteiro sem assinatura	Credencial correspondente a um PIN. O intervalo válido é entre 0 e 65535.
Status	Booleanos	Status do titular do cartão. Os seguintes valores são aceitos (sem diferenciar maiúsculas e minúsculas): • 1, Verdadeiro, Sim = Perfil ativado • 0, Falso, Não = Perfil desativado
Status	Cadeia	Status da credencial. Os seguintes valores são aceitos (sem diferenciar maiúsculas e minúsculas): • Ativo • Inativo • Perdida • Furtado • Expirado

Tópicos relacionados

Sobre partições na página 344
Arquivos CSV e a ferramenta de importação na página 715
Criar formatos de cartão personalizados na página 691
Substituir credenciais na página 721
Como os formatos de cartão de credenciais funcionam com o Active Directory no Security Center na página 688

36

Teste do sistema de controle de acesso

Esta seção inclui os seguintes tópicos:

- " Ferramenta Solução de problemas de acesso" na página 728
- "Testar regras de acesso em portas e elevadores" na página 729
- "Identificação de indivíduos que têm acesso a portas e elevadores" na página 730
- "Identificação de indivíduos que têm acesso concedido/negado nos pontos de acesso" na página 731
- "Testar direitos de acesso de titulares de cartão" na página 733
- "Exibir propriedades de credencial de titulares de cartão" na página 734
- "Visualizar propriedades de membros de grupos de titulares de cartão" na página 736
- "Identificação de quais entidades são afetadas pelas regras de acesso" na página 738
- "Visualizar a configuração de E/S de unidades de controle de acesso" na página 739

Ferramenta Solução de problemas de acesso

A ferramenta de solução de problemas de acesso permite testar e solucionar problemas do sistema de controle de acesso após a configuração, como regras de acesso e configurações de portas e elevadores.

Se você tem um sistema grande, você pode ter várias programações (Horário de funcionamento/Escritório fechado/Feriados/Fins de semana/Eventos especiais), várias áreas e subáreas, vários grupos de titulares de cartão e assim por diante. À medida que você constrói seu sistema e continua a criar entidades, a lógica básica de acesso aplicada a uma porta pode se tornar mais difícil de determinar.

Você pode usar a solução de problemas de acesso para fazer o seguinte:

- Quem tem permissão para passar por um ponto de acesso em uma determinada data e hora
- Quais pontos de acesso um titular de cartão tem permissão para usar em uma determinada data e hora
- Por que um determinado titular de cartão pode ou não usar um ponto de acesso em uma determinada data e hora

A solução de problemas de acesso é mais precisa ao examinar um evento que acabou de ocorrer. Ao usar a ferramenta de solução de problemas para investigar um evento passado (por exemplo, um evento de acesso negado), lembre-se de que suas configurações podem ter sido alteradas desde que esse evento ocorreu. A ferramenta de solução de problemas não leva em consideração configurações passadas. Ela só avalia uma situação com base nas configurações atuais.

Testar regras de acesso em portas e elevadores

Você pode descobrir quem tem o direito de passar por um lado de porta ou andar de elevador em determinada data e hora usando a ferramenta *Solução de problemas de acesso*.

O que você deve saber

A ferramenta de solução de problemas de porta não examina as credenciais de cada titular de cartão. Pode diagnosticar adicionalmente os direitos de acesso do titular de cartão clicando na aba Diagnóstico de acesso ().

Para testar as regras de acesso em uma porta ou elevador:

1 Na página inicial, clique em **Ferramentas** > **Solução de problemas de acesso** .
2 Na caixa de diálogo *Solução de problemas de acesso* , clique na aba *Solução de problemas da porta* .
3 Selecione a data e a hora nas quais você quer basear a avaliação da solução de problemas.
Somente são avaliadas *regras de acesso* com base em data e hora especificadas.
4 Selecione o ponto de acesso que você deseja que a solução de problemas examine:
   - Se você selecionar uma porta, especifique um lado da porta.
   - Se você selecionar um elevador, especifique um andar.
5 Clique em **Ir**.

Os titulares de cartões ativos que têm os direitos de usar o ponto de acesso selecionado na hora especificada, com base nas regras de acesso atuais, são listados.

Tópicos relacionados

Teste de direitos de acesso de titular de cartão com base em credenciais na página 733

Identificação de indivíduos que têm acesso a portas e elevadores

Você pode verificar quais titulares de cartão têm acesso a um lado de porta ou andar de elevador em particular em uma data e hora específicas, usando o relatório *Solução de problemas de porta*.

O que você deve saber

Este relatório é útil, pois permite que você veja qual é a configuração de uma porta ou elevador e determine se suas propriedades devem ser ajustadas.O solucionador de problemas de porta não examina as credenciais de cada titular do cartão. Pode ainda diagnosticar os direitos de acesso do titular do cartão usando a ferramenta *Solução de problemas de acesso*.

Para identificar indivíduos que têm acesso a uma porta ou um elevador:

1 Na página inicial, abra a tarefa **Solução de problemas de porta**.
2 Na aba *Filtros*, selecione uma data e hora para o relatório.
3 Selecione uma porta ou um elevador que deseja investigar.
4 Na lista suspensa **Ponto de acesso**, selecione o ponto de acesso (lado da porta ou andar do elevador) que deseja verificar.
5 Clique em **Gerar relatório**.

Todos os titulares de cartão que podem passar pelo ponto de acesso selecionado na hora especificada são listados no painel de relatório.

Após terminar

Se necessário, teste sua configuração de controle de acesso.

Tópicos relacionados

Testar regras de acesso em portas e elevadores na página 729
Criar portas na página 616
Criar elevadores na página 624
Pesquisar por entidades na página 75

Colunas do painel de relatórios para a tarefa Solução de problemas de porta

Após gerar um relatório, os resultados da sua pesquisa são listados em um painel de relatório. Esta seção lista as colunas disponíveis para a tarefa de relatório relevante.

- **Titular do cartão:** Nome da entidade do titular do cartão
- **Campos personalizados:** Os campos personalizados predefinidos para a entidade. As colunas aparecem somente se os campos personalizados estiverem definidos para a entidade e se estiver visível para você, quando forem criados ou configurados pela última vez.
- **Nome:** Nome do titular de cartão ou visitante.
- **Sobrenome:** Sobrenome do visitante ou titular do cartão.
- **Foto:** Foto do visitante ou titular do cartão.

Identificação de indivíduos que têm acesso concedido/negado nos pontos de acesso

Você pode descobrir quais os titulares de cartões tem ou não acesso atualmente a áreas selecionadas, portas e elevadores, usando o relatório *Direitos de acesso do titular do cartão*.

O que você deve saber

Este relatório é útil porque permite que você veja quando e onde um titular de cartão pode ir e determinar se suas propriedades de regra de acesso devem ser ajustadas.

DICA: Execute sua consulta em um ponto de acesso por vez, para que o relatório seja mais específico.

Para identificar indivíduos que têm acesso concedido/negado em um ponto de acesso:

1 Na página inicial, abra a tarefa **Direitos de acesso do titular do cartão**.

2 Defina os filtros de consulta para o seu relatório. Escolha um ou mais dos filtros abaixo:

- **Portas - Áreas - Elevadores:** Restringir a busca a atividades que acontecem em certas portas, áreas e elevadores.

3 Clique em **Gerar relatório**.

Os portadores associados ao ponto de acesso selecionado através de uma regra de acesso são listados no painel de relatório. Os resultados indicam se o titular de cartão tem acesso concedido concedido ou negado e por qual regra de acesso.

4 Para exibir um titular de cartão em um ladrilho, clique duas vezes ou arraste um titular de cartão do painel de relatório para a tela.

5 Para visualizar informações adicionais de titular do cartão no ladrilho, clique em  .

Após terminar

Se necessário, modifique os direitos de acesso do titular de cartão.

Tópicos relacionados

Atribuir regras de acesso a titulares de cartão na página 650

Colunas de relatório para a tarefa Direitos de acesso dos titulares de cartão

Após gerar um relatório, os resultados da sua pesquisa são listados em um painel de relatório. Esta seção lista as colunas disponíveis para a tarefa de relatório relevante.

- **Titular do cartão:** Nome da entidade do titular do cartão
- **Campos personalizados:** Os campos personalizados predefinidos para a entidade. As colunas aparecem somente se os campos personalizados estiverem definidos para a entidade e se estiver visível para você, quando forem criados ou configurados pela última vez.
- **Acesso negado por:** Regras de acesso negando para, pelo menos, uma das entidades selecionadas para o titular de cartão.
- **Nome:** Nome do titular de cartão ou visitante.
- **Acesso concedido por:** Regras de acesso de concessão para, pelo menos, uma das entidades selecionadas (área, porta, etc.)
- **Sobrenome:** Sobrenome do visitante ou titular do cartão.
- **Membro de:** Todos os grupos a que o titular do cartão pertence

- **Foto:** Foto do visitante ou titular do cartão.

Testar direitos de acesso de titulares de cartão

Você pode saber quais pontos de acesso um titular de cartão pode usar em determinada data e hora, usando a aba *Resolução de problemas de titular de cartão* na ferramenta Solução de problemas de acesso.

O que você deve saber

A solução de problemas de titular de cartão não examina as credenciais de cada titular de cartão. Pode diagnosticar com mais detalhe os direitos de acesso do titular de cartão clicando na aba Diagnóstico de acesso ( ).

Para solucionar problemas de direitos de acesso de um titular de cartão:

1. Na página inicial, clique em **Ferramentas** > **Solução de problemas de acesso** .
2. Na caixa de diálogo *Solução de problemas de acesso* , clique na aba *Resolução de problemas de titular de cartão* .
3. Selecione a data e a hora nas quais você quer basear a avaliação da solução de problemas. Somente são avaliadas *regras de acesso* com base em data e hora especificadas.
4. Selecione o titular de cartão que você deseja que a solução de problemas examine: Em vez de um titular de cartão, você também pode selecionar uma *credencial* ou um visitante.

   As entidades que estão atualmente inativas ficam acinzentadas.
5. Clique em **Ir**.

Os pontos de acesso que o titular de cartão (ou visitante) selecionado tem o direito de usar na hora especificada, com base nas regras de acesso atuais, são listados.

Teste de direitos de acesso de titular de cartão com base em credenciais

Você pode diagnosticar por que um titular de cartão com uma determinada credencial pode ou não pode acessar uma determinada porta ou elevador, em uma determinada data e hora, usando a aba *Diagnóstico de acesso do Diagnóstico de acesso* na ferramenta de solução de problemas de acesso.

Para testar os direitos de acesso de um titular de cartão com base em sua credencial:

1. Na página inicial, clicar em **Ferramentas** > **Solução de problemas de acesso** .
2. Na caixa de diálogo *Solução de problemas de acesso* , clique na aba **Diagnóstico de acesso** ( ).
3. Selecione a data e a hora nas quais você quer basear a avaliação da solução de problemas.
4. Selecione o titular que deseja examinar. Em vez de um titular, você também pode selecionar uma credencial ou um visitante.
5. Se o titular de cartão selecionado tiver mais de uma credencial, especifique a que deseja examinar.
6. Selecione um ponto de acesso para examinar.
   - Se você selecionar uma porta, especifique um lado da porta.
   - Se você selecionar um elevador, especifique um andar.
7. Clique em **Ir**.

A solução de problemas produz um diagnóstico com base na configuração atual do sistema, levando em consideração as regras de acesso e as datas de ativação e expiração do titular do cartão e da credencial.

Exibir propriedades de credencial de titulares de cartão

É possível exibir as propriedades da credencial (status, titular atribuído, formato do cartão, código da credencial, propriedades personalizadas etc.) do titular de cartão, usando o relatório *Configuração da credencial* .

O que você deve saber

Por exemplo, o relatório de Configurações de credencial é útil se foi solicitada uma credencial para um titular de cartão e deseja ver se foi ativada. Se fizer a busca por titular de cartão, a coluna *Status da credencial* indica se a credencial está no estado *Solicitado* ou *Ativo* . Também é possível pesquisar se há alguma credencial listada atualmente como perdida ou roubada.

Para exibir as propriedades de credencial de um titular de cartão:

1 Abra a tarefa **Gerenciamento de credenciais** .

2 Defina os filtros de consulta para o relatório. Escolha um ou mais dos filtros abaixo:

- **Credencial:** Especificar sem a credencial está atribuída ou não.
- **Titulares de cartão:** Restringir a busca a certos titulares.
- **Informações de credencial:** Restringir a busca aos formatos de cartão específicos, códigos da instalação, números de cartão ou placas de licença.
- **Campos personalizados:** Restringir a busca a campo personalizado predefinido para a entidade. Este filtro aparece somente se os campos personalizados estiverem definidos para a entidade e estavam visíveis para você, quando foi criado ou configurado pela última vez.
- **Status:** O status do perfil do titular do cartão ou do visitante Ativo; Vencido; Inativo; Perdido; Roubado. Nem todos os status estão disponíveis para todas as tarefas.
- **Credenciais não usadas:** Procure por credenciais que não produziram um evento de *acesso concedido* dentro de um determinado intervalo de tempo.

  NOTA: Para que o relatório gere resultados, todas as funções de Gerente de Acesso devem estar ativas e conectadas.

3 Clique em **Gerar relatório**.

As propriedades de credencial do titular de cartão selecionado são listadas no painel de relatório.

4 Para exibir um titular de cartão em um ladrilho, clique duas vezes ou arraste um titular de cartão do painel de relatório para a tela.

5 Para exibir informações adicionais de titular do cartão no ladrilho, clique em .

Colunas do painel de relatórios para a tarefa Configuração de credenciais

Após gerar um relatório, os resultados da sua pesquisa são listados em um painel de relatório. Esta seção lista as colunas disponíveis para a tarefa de relatório relevante.

- **Formato do cartão:** Formato do cartão de credencial
- **Titular do cartão:** Nome da entidade do titular do cartão
- **Data de ativação do titular do cartão:** Data em que o perfil do titular do cartão foi ativado.
- **Data de vencimento do titular do cartão:** Data em que o perfil do titular do cartão vence.
- **Status do titular do cartão:** O status do perfil do titular do cartão.
- **Credencial:** Nome da credencial usado pelo titular do cartão.
- **Data da ativação da credencial:** Horário em que a credencial do titular do cartão foi ativado.
- **Código da credencial:** Código da instalação e número do cartão.

- **Data de vencimento da credencial:** Data em que a credencial do titular do cartão vence.
- **Status da credencial:** O status do titular do cartão ou da credencial do visitante: Ativo; inativo
- **Campos personalizados:** Os campos personalizados predefinidos para a entidade. As colunas aparecem somente se os campos personalizados estiverem definidos para a entidade e se estiver visível para você, quando forem criados ou configurados pela última vez.
- **Descrição:** Descrição do evento, atividade, entidade ou incidente.

  IMPORTANTE: Para cumprir com as leis estaduais, se a opção **Relatório gerado** é usada para um relatório de Trilha de atividade que contém dados LPR, o motivo da pesquisa LPR é incluído no campo **Descrição** .
- **Endereço de e-mail:** Endereço de e-mail do visitante ou titular do cartão
- **Nome:** Nome do titular de cartão ou visitante.
- **Sobrenome:** Sobrenome do visitante ou titular do cartão.
- **Foto:** Foto do visitante ou titular do cartão.
- **PIN:** PIN da credencial
- **Função:** Tipo de função que gerencia a entidade importada Federada ou o Active Directory selecionado.

Visualizar propriedades de membros de grupos de titulares de cartão

É possível encontrar os membros de um grupo de titulares de cartão e visualizar todas as propriedades associadas (nome, sobrenome, foto, status, propriedades personalizadas, etc.) usando a tarefa *Configuração dos titulares de cartão* .

O que você deve saber

É possível pesquisar por um grupo específico de titulares de cartão para ver quais titulares de cartão são membros daquele grupo. Também é possível pesquisar por titulares de cartão expirados ou inativos para verificar se existe algum no seu sistema.

Para visualizar as propriedades de membros de grupo de titulares de cartão:

1 Na página inicial, abra a tarefa ***Configuração do titular do cartão*** .

2 Defina os filtros de consulta para o relatório. Escolha um ou mais dos filtros abaixo:

- **Data de ativação:** Data e hora em que o titular de cartão foi ativado.
- **Data de validade:** Especificar um intervalo de tempo para quando o perfil do visitante ou do titular do cartão expirar.
- **Titulares de cartão não usados:** Pesquise por titulares de cartão ou visitantes para quem nenhuma credencial atribuída produziu um evento de *acesso concedido* dentro de um determinado intervalo de tempo.

  NOTA: Para que o relatório gere resultados, todas as funções de Gerente de Acesso devem estar ativas e conectadas.
- **Status:** O status do perfil do titular do cartão ou do visitante Ativo; Vencido; Inativo; Perdido; Roubado. Nem todos os status estão disponíveis para todas as tarefas.
- **Nome:** Nome do titular de cartão ou visitante.
- **Sobrenome:** Sobrenome do visitante ou titular do cartão.
- **Endereço de e-mail:** Endereço de e-mail do visitante ou titular do cartão
- **Descrição:** Restringir a busca a entidades que contêm este string de texto.
- **Foto:** Foto do visitante ou titular do cartão.
- **Partição:** Divisão da entidade de que é membro
- **Grupos de titulares de cartão:** Restringir a busca a certos grupos de titulares.
- **Campos personalizados:** Restringir a busca a campo personalizado predefinido para a entidade. Este filtro aparece somente se os campos personalizados estiverem definidos para a entidade e estavam visíveis para você, quando foi criado ou configurado pela última vez.
- **Credencial:** Restringir a busca a certas credenciais.
- **Status da credencial:** O status do titular do cartão ou da credencial do visitante: Ativo; Vencido; Inativo; Perdido; Roubado. Nem todos os status estão disponíveis para todas as tarefas.
- **Informações de credencial:** Restringir a busca aos formatos de cartão específicos, códigos da instalação, números de cartão ou placas de licença.

3 Clique em **Gerar relatório**.

Os titulares de cartão membros dos grupos de titulares de cartão selecionados estão listados no painel de relatório.

4 Para exibir um titular de cartão em um ladrilho, clique duas vezes ou arraste um titular de cartão do painel de relatório para a tela.

5 Para visualizar informações adicionais de titular do cartão no ladrilho, clique em .

Colunas de relatório para a tarefa Configuração de titulares de cartão

Após gerar um relatório, os resultados da sua pesquisa são listados em um painel de relatório. Esta seção lista as colunas disponíveis para a tarefa de relatório relevante.

- **Titular do cartão:** Nome da entidade do titular do cartão
- **Data de ativação do titular do cartão:** Data em que o perfil do titular do cartão foi ativado.
- **Data de vencimento do titular do cartão:** Data em que o perfil do titular do cartão vence.
- **Status do titular do cartão:** O status do perfil do titular do cartão.
- **Campos personalizados:** Os campos personalizados predefinidos para a entidade. As colunas aparecem somente se os campos personalizados estiverem definidos para a entidade e se estiver visível para você, quando forem criados ou configurados pela última vez.
- **Endereço de e-mail:** Endereço de e-mail do visitante ou titular do cartão
- **Nome:** Nome do titular de cartão ou visitante.
- **Sobrenome:** Sobrenome do visitante ou titular do cartão.
- **Membro de:** Todos os grupos a que o titular do cartão pertence
- **Foto:** Foto do visitante ou titular do cartão.

Identificação de quais entidades são afetadas pelas regras de acesso

Você pode descobrir quais entidades e pontos de acesso são afetados por determinada regra de acesso, usando o relatório *Configuração de regra de acesso*.

O que você deve saber

Nos resultados do relatório, você pode ver os membros da regra de acesso, como os titulares de cartão, as portas e a programação associada. Isso ajuda a determinar se você deve adicionar ou remover entidades ou ajustar a programação.

Para identificar de quais entidades são afetadas por uma regra de acesso:

1 Abra a tarefa **Configuração de regra de acesso**.

2 Defina os filtros de consulta para o relatório. Escolha um ou mais dos filtros abaixo:

- **Regra de acesso:** Selecione a regra de acesso para investigar.
- **Status do titular do cartão:** Selecione o status do titular de cartão para investigar: Ativo; Vencido; Inativo.
- **Campos personalizados:** Restringir a busca a campo personalizado predefinido para a entidade. Este filtro aparece somente se os campos personalizados estiverem definidos para a entidade e estavam visíveis para você, quando foi criado ou configurado pela última vez.

3 Na opção **Expandir grupo do titular do cartão**, selecione **Ativar** para listar os membros dos grupos de titulares de cartão afetados no relatório em vez de dos próprios grupos de titulares de cartão.

4 Na opção **Incluir entidades de perímetro**, selecione **Ativar** para incluir as entidades do perímetro das áreas afetadas no relatório.

5 Clique em **Gerar relatório**.

As entidades e pontos de acesso afetados por esta regra de acesso são listados no painel de relatório.

Tópicos relacionados

Criar regras de acesso na página 644

Colunas de relatório para a tarefa Configuração da regra de acesso

Após gerar um relatório, os resultados da sua pesquisa são listados em um painel de relatório. Esta seção lista as colunas disponíveis para a tarefa de relatório relevante.

- **Regras de acesso:** Nome das regras de acesso.
- **Ativação:** (Somente regra de acesso temporário) Hora de ativação da regra de acesso temporário.
- **Validade:** (Somente regra de acesso temporário) Data e hora do término da regra de acesso.
- **Membro:** Nome da entidade afetada
- **Ponto de acesso:** Ponto de acesso envolvido (somente aplicável a áreas, portas e elevadores)
- **Tipo:** Tipo de entidade afetada
- **Status do titular do cartão:** O status do perfil do titular do cartão.
- **Campos personalizados:** Os campos personalizados predefinidos para a entidade. As colunas aparecem somente se os campos personalizados estiverem definidos para a entidade e se estiver visível para você, quando forem criados ou configurados pela última vez.

Visualizar a configuração de E/S de unidades de controle de acesso

Você pode visualizar as configurações de E/S (pontos de acesso controlados, portas e elevadores) de unidades de controle de acesso usando o relatório *Configuração de E/S*.

O que você deve saber

Por exemplo, você pode usar o relatório de *Configuração de I/O* para procurar uma porta específica e ver como o acesso através de cada lado da porta está configurado (REX, leitores, módulos de E/S e assim por diante).

Para visualizar a configuração de E/S de um unidade de controle de acesso:

1 Abra a tarefa Configuração de E/S.

2 Defina os filtros de consulta para o relatório. Escolha um ou mais dos filtros abaixo:

- **Unidades de controle de acesso:** Selecione as unidades de controle de acesso para investigar.
- **Campos personalizados:** Restringir a busca a campo personalizado predefinido para a entidade. Este filtro aparece somente se os campos personalizados estiverem definidos para a entidade e estavam visíveis para você, quando foi criado ou configurado pela última vez.
- **Dispositivos:** Selecione os dispositivos para investigar.
- **Localização:** Especifique as áreas onde os dispositivos estão localizados.

3 Clique em **Gerar relatório**.

As configurações de entrada e saída das unidades de controle de acesso selecionadas são listadas no painel de relatório.

Tópicos relacionados

Visualizar propriedades das unidades na página 93

Colunas de relatório para a tarefa Configuração de E/S

Após gerar um relatório, os resultados da sua pesquisa são listados em um painel de relatório. Esta seção lista as colunas disponíveis para a tarefa de relatório relevante.

- **Ponto de acesso:** Ponto de acesso envolvido (somente aplicável a áreas, portas e elevadores)
- **Gestor de Acesso:** Access Manager controlando a unidade.
- **Controlando:** Porta controlada pelo dispositivo
- **Campos personalizados:** Os campos personalizados predefinidos para a entidade. As colunas aparecem somente se os campos personalizados estiverem definidos para a entidade e se estiver visível para você, quando forem criados ou configurados pela última vez.
- **Dispositivo:** Dispositivo envolvido na unidade (leitor, entrada REX, módulo IO, relé de curso, etc.)
- **Endereço IP:** Endereço de IP da unidade ou computador que gerou o evento
- **Fabricante:** Fabricante da unidade.
- **Nome físico:** Nome do dispositivo
- **Unidade:** Controle de acesso, vídeo, detecção de invasão ou unidade LPR envolvida.
- **Tipo de unidade:** Tipo ou modelo de unidade envolvido

37

Solução de problemas de controle de acesso

Esta seção inclui os seguintes tópicos:

- "Visualizar eventos de saúde de controle de acesso" na página 741
- "Investigar eventos relacionados a unidades de controle de acesso" na página 742
- "Mover unidades de controle de acesso para um Access Manager diferente" na página 743
- "Preparar para substituir uma unidade de controle de acesso" na página 744
- "Substituir unidades de controle de acesso" na página 745
- "Atualizar firmware de unidade de controle de acesso" na página 747
- "Habilitar ou desabilitar registros de suporte para unidades de controle de acesso" na página 750
- "Solução de problemas: problemas de descoberta e inscrição de unidade HID" na página 751
- "Solução de problemas: muitas solicitações para eventos de saída de portas" na página 754
- "Solução de problemas: Credenciais não funcionam" na página 755
- "Solução de problemas: Os cartões não funcionam nos leitores" na página 756
- "Solução de problemas: A instalação do driver falha para os leitores USB HID OMNIKEY" na página 757

Visualizar eventos de saúde de controle de acesso

É possível exibir eventos de saúde relacionados a entidades de controle de acesso usando o relatório *Histórico de saúde de controle de acesso*.

O que você deve saber

Esse relatório é semelhante ao relatório de Histórico de saúde, mas a consulta só procura eventos que causam avisos e inclui apenas entidades de controle de acesso. As entidades de controle de acesso que podem produzir avisos incluem unidades de controle de acesso, portas, áreas, elevadores e zonas.

Para procurar eventos de saúde de controle de acesso:

1 Abra a tarefa **Histórico de saúde de controle de acesso**.
2 Defina os filtros de consulta para o relatório. Escolha um ou mais dos filtros abaixo:
   - **Carimbo de tempo do evento:** Definir o intervalo de tempo para consulta O intervalo pode ser definido para um período específico ou para unidades de tempo globais, como a semana ou mês anteriores.
   - **Entidade de origem:** Entidade fonte do evento.
3 Clique em **Gerar relatório**.

   Os eventos de saúde do controle de acesso são listados no painel de relatório.

Colunas de relatório para a tarefa Histórico de saúde de controle de acesso

Após gerar um relatório, os resultados da sua pesquisa são listados em um painel de relatório. Esta seção lista as colunas disponíveis para a tarefa de relatório relevante.

- **Campos personalizados:** Os campos personalizados predefinidos para a entidade. As colunas aparecem somente se os campos personalizados estiverem definidos para a entidade e se estiver visível para você, quando forem criados ou configurados pela última vez.
- **Descrição:** Relata o motivo de uma falha de atualização de firmware.
- **Dispositivo:** Dispositivo envolvido na unidade (leitor, entrada REX, módulo IO, relé de curso, etc.)
- **Evento:** Nome do evento
- **Carimbo de tempo do evento:** Data e hora em que o evento ocorreu.
- **Versão do firmware:** Versão do firmware instalada na unidade que gerou o evento
- **Endereço IP:** Endereço de IP da unidade ou computador que gerou o evento
- **Tipo de produto:** Modelo da unidade envolvida
- **Fonte:** Entidade fonte associada ao alarme ou evento.
- **Fuso horário:** Fuso horário da unidade
- **Unidade:** Controle de acesso, vídeo, detecção de invasão ou unidade LPR envolvida.

Investigar eventos relacionados a unidades de controle de acesso

É possível investigar eventos de relacionados a entidades de controle de acesso usando o relatório *Eventos de unidade de controle de acesso*.

O que você deve saber

Por exemplo, você pode usar o relatório *Eventos de unidade de controle de acesso* para ver se ocorreram eventos críticos relacionados a *unidade de controle de acesso* na última semana (por exemplo, *Violação de hardware*), procurando esse evento e definindo o intervalo de tempo.

Para investigar eventos de unidade de controle de acesso:

1 Na página inicial, abra a tarefa **Eventos de unidade de controle de acesso**.

2 Defina os filtros de consulta para o relatório. Escolha um ou mais dos filtros abaixo:

- **Unidades de controle de acesso:** Selecione as unidades de controle de acesso para investigar.
- **Campos personalizados:** Restringir a busca a campo personalizado predefinido para a entidade. Este filtro aparece somente se os campos personalizados estiverem definidos para a entidade e estavam visíveis para você, quando foi criado ou configurado pela última vez.
- **Eventos:** Selecionar os eventos de interesse. Os tipos de evento disponíveis dependem da tarefa que está usando.
- **Carimbo de tempo do evento:** Definir o intervalo de tempo para consulta O intervalo pode ser definido para um período específico ou para unidades de tempo globais, como a semana ou mês anteriores.

3 Clique em **Gerar relatório**.

Os eventos de unidade de controle de acesso são listados no painel de relatório.

NOTA: Se você tiver Access Managers offline quando você inicia a consulta, você receberá uma mensagem de erro para cada um deles, mesmo que eles não estejam relacionados às unidades de controle de acesso selecionadas. Isso ocorre porque o sistema não tem como saber se as unidades selecionadas foram ou não gerenciadas por uma delas no passado.

Colunas de relatório para a tarefa Eventos da unidade de controle de acesso

Após gerar um relatório, os resultados da sua pesquisa são listados em um painel de relatório. Esta seção lista as colunas disponíveis para a tarefa de relatório relevante.

- **Campos personalizados:** Os campos personalizados predefinidos para a entidade. As colunas aparecem somente se os campos personalizados estiverem definidos para a entidade e se estiver visível para você, quando forem criados ou configurados pela última vez.
- **Descrição:** Relata o motivo de uma falha de atualização de firmware.
- **Evento:** Nome do evento
- **Carimbo de tempo do evento:** Data e hora em que o evento ocorreu.
- **Período de ocorrência:** Período em que o evento ocorreu.
- **Tipo de produto:** Modelo da unidade envolvida
- **Violação:** Nome do módulo de interface que foi adulterado.
- **Unidade:** Controle de acesso, vídeo, detecção de invasão ou unidade LPR envolvida.

Mover unidades de controle de acesso para um Access Manager diferente

Se você quiser que uma função Access Manager diferente gerencie e controle uma unidade de controle de acesso, para distribuição de carga ou outra finalidade, você pode mover a unidade para outro Access Manager usando a ferramenta *Mover unidade*.

Antes de iniciar

Faça o seguinte:

- Certifique-se de que a função Access Manager esteja na mesma LAN que a unidade de controle de acesso controlada.
- Crie a extensão para a unidade.

Para mover uma unidade de controle de acesso para um Access Manager diferente:

1. Desative temporariamente ambos os Access Managers.
   a) Na tarefa **Controle de acesso**, clique com o botão direito no Access Manager e clique em **Manutenção** > **Desativar função** ( ).
   b) Na caixa de diálogo de confirmação que abrir, clique em **Continuar**.
   O Access Manager e todas as unidades de controle de acesso que ele controla ficam vermelhas.
2. Na página inicial, clique em **Ferramentas** > **Mover unidade**.
3. Na lista suspensa **Tipo de unidade**, selecione **Unidade de controle de acesso**.
4. Em **Access Manager**, selecione as unidades que deseja mover.
5. Em **Access Manager**, selecione a nova função Access Manager para controlar a unidade.
6. Clique em **Mover** > **Fechar**.

Preparar para substituir uma unidade de controle de acesso

Antes de substituir uma unidade de controle de acesso por uma nova, existem etapas que você deve executar.

Antes de iniciar

Você só pode substituir uma unidade de controle de acesso por uma nova se as duas forem da mesma marca e modelo. A única exceção a esta regra é se você estiver substituindo uma unidade HID VertX V1000 por uma unidade Synergis™. Em todos os casos, os mesmos módulos de interface (marca e modelo) devem ser conectados à nova unidade. Se houver qualquer diferença além da exceção mencionada, a substituição da unidade não será aceita.

Antes de substituir uma unidade de controle de acesso:

1 Faça backup do banco de dados do Directory a partir de Server Admin.

2 Desconecte fisicamente a unidade antiga e certifique-se de que ela está offline no Security Center ( ).

3 (Somente unidade Synergis™) Monte e instale a unidade Synergis™ e seus componentes de hardware. Para obter informações, consulte o *Guia de Instalação de Hardware Synergis™ Cloud Link*.

4 Desconecte fisicamente os módulos de interface da unidade antiga e conecte-os à nova unidade usando exatamente os mesmos canais.

IMPORTANTE: Não altere o endereço físico dos módulos de interface.

Se você estiver substituindo uma unidade HID VertX V1000 por uma unidade Synergis™, conecte os subpainéis (módulos de interface) encontrados em cada lado da V1000 a dois canais diferentes da unidade Synergis™, pois dois módulos de interface no mesmo canal não podem ter o mesmo endereço físico.

5 (Somente unidade Synergis™) Configure a unidade Synergis™ de acordo com os módulos de interface ligados a ela. Para mais informações, consulte o *Guia de Configuração de Aparelhos Synergis™*.

Após terminar

Substitua a unidade antiga pela nova.

Substituir unidades de controle de acesso

Se uma unidade de vídeo falhar e estiver offline no Security Center ( ), você pode substituir a unidade por uma compatível. Este processo copia as definições de configuração, associações a portas, elevadores e zonas e registros de eventos da unidade antiga, para que não seja necessário configurar a nova.

Antes de iniciar

Preparar para substituir sua unidade de controle de acesso.

CUIDADO: Nem todas as configurações são copiadas pela ferramenta de substituição de unidade. Se você estiver usando entradas supervisionadas na unidade antiga, você terá que reconfigurar as entradas na nova unidade.

Para substituir uma unidade de controle de acesso:

1 Adicione a nova unidade de controle de acesso totalmente conectada ao Access Manager que controla a unidade antiga. Para uma unidade Synergis™, consulte o *Guia de Configuração do Aparelho Synergis™*.

2 Desative temporariamente o Access Manager.

a) Na tarefa *Controle de acesso*, selecione o Access Manager e clique em **Manutenção** > **Desativar função** ( ).

b) Na caixa de diálogo de confirmação que abrir, clique em **Continuar**.

O Access Manager e todas as unidades de controle de acesso controladas pela função ficarão em vermelho.

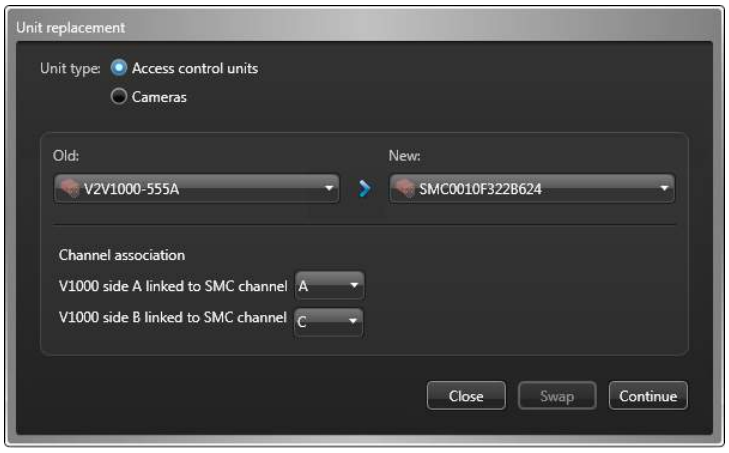
3 Na página inicial, clique em **Ferramentas** > **Substituição de unidade**.

4 Na opção **Tipo de unidade**, selecione **Unidades de controle de acesso**.

5 Selecione as unidades de controle de acesso **Antiga** e a **Nova**

6 Clique em **Trocar**.

(Somente V1000 para Synergis™) Se o V1000 possuía subpainéis (módulos de interface) usando o mesmo endereço físico, ligue os lados do V1000 aos canais da unidade Synergis™ e clique em **Continuar**.



As configurações da antiga unidade de controle de acesso são copiadas para a nova.

7 Na tarefa **Controle de acesso**, clique com o botão direito no Access Manager e clique em **Manutenção** > **Ativar função** ( ).

8 Na visualização **Funções e unidades**, selecione a nova unidade e verifique se as configurações estão todas corretas.

9 Clique com o botão direito do mouse na unidade antiga e clique em Excluir. ( ).

10 Na caixa de diálogo de confirmação que abrir, clique em **Continuar**.

Após terminar

Se as entradas na unidade antiga eram supervisionadas, reconfigure-as na nova unidade.

Tópicos relacionados

Pesquisando por entidades usando a ferramenta de pesquisa na página 75

Atualizar firmware de unidade de controle de acesso

Você pode atualizar o firmware de uma ou mais unidades de controle de acesso e seus módulos de interface conectados diretamente do Config Tool.

Antes de iniciar

- Se as unidades forem alimentadas por Power over Ethernet (PoE), elas devem incluir um backup de bateria em caso de queda da energia durante o processo de atualização.
- Faça o download de uma versão de firmware suportada para a unidade no GTAP.

  NOTA: Para obter links de download de firmware HID EVO, consulte KBA01134 no Hub TechDoc da Genetec™.
- Para unidades HID EVO, certifique-se de que a senha do *admin* esteja configurada no Config Tool nas propriedades da unidade.

O que você deve saber

- Você pode atualizar os seguintes dispositivos no Config Tool:
  - Synergis™ Cloud Link
  - Synergis™ Master Controller

    Caminho de atualização suportado: 2.x → 10.0 → qualquer versão posterior
  - Mercury EP (quando conectado a um Synergis™ Cloud Link ou Synergis™ Master Controller executando o Synergis™ Softwire 10.4 ou posterior.)
  - Mercury EP (quando conectado a um Synergis™ Cloud Link ou Synergis™ Master Controller executando o Synergis™ Softwire 10.4 ou posterior.)
  - Travas IP Assa Abloy (quando conectado a um Synergis™ Cloud Link ou Synergis™ Master Controller executando o Synergis™ Softwire 10.5 ou posterior.)
- Para atualizar unidades HID EVO de uma versão de firmware anterior (2.3.1.603 ou 2.3.1.605 para Edge EVO e 2.3.1.542 ou 2.3.1.673 para VertX EVO) para a versão de firmware recomendada, devem ser seguidos caminhos de atualização específicos.
  - HID Edge EVO: (EH400, EH400-K)

    Caminho de atualização suportado: 2.3.1.603 ou 2.3.1.605 → 2.3.1.841 → qualquer versão posterior
  - HID Vertx EVO: (V1000, V2000)

    Caminho de atualização suportado: 2.3.1.542 ou 2.3.1.673 → 2.3.1.791 → qualquer versão posterior

    CUIDADO: A atualização direta do firmware anterior para o firmware recomendado causará danos irreparáveis à sua unidade. Além disso, não pode fazer o downgrade do firmware de uma unidade HID após atualizá-lo para 2.3.1.841 em Edge EVO, ou para 2.3.1.791 em VertX EVO.
- Também é possível atualizar unidades individuais na tarefa *Controle de acesso* no Config Tool a partir da aba *Identidade* da unidade na visualização *Funções e unidades*.
- O sistema pode atualizar até dez unidades simultaneamente. Se mais de dez unidades forem selecionadas para atualização, unidades adicionais serão enfileiradas.
- Não é possível cancelar uma atualização em andamento. Só é possível cancelar uma atualização se o *status de atualização* da unidade no relatório *Inventário de hardware* for *Agendado*.
- Portas atribuídas à unidade de controle de acesso sendo atualizada não funcionam durante uma atualização de firmware.

Para atualizar o firmware de uma unidade de controle de acesso:

1 No Config Tool, gere um relatório de *Inventário de hardware* para as unidades que deseja atualizar.

2 Selecione as unidades que deseja atualizar.

O campo **Proposto** exibe a versão de firmware recomendada. Se a versão de firmware for a mesma que a versão proposta, exibirá *Atualizado*.

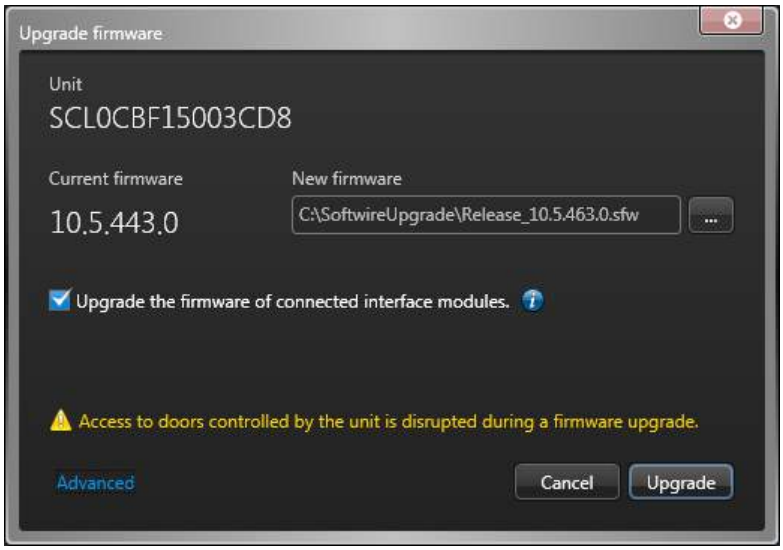
NOTA: Se você selecionar várias unidades para atualizar, todas as unidades selecionadas devem ser do mesmo tipo de produto.

3 Clique em **Atualizar firmware** ( ).

NOTA: Se o botão **Atualizar firmware** não aparecer, certifique-se de ter os privilégios de usuário necessários (exige o privilégio *Iniciar atualização de firmware de unidade de controle de acesso* e o privilégio *Ferramenta de descoberta de unidades*) e confirme se todas as unidades selecionadas são do mesmo tipo de produto.

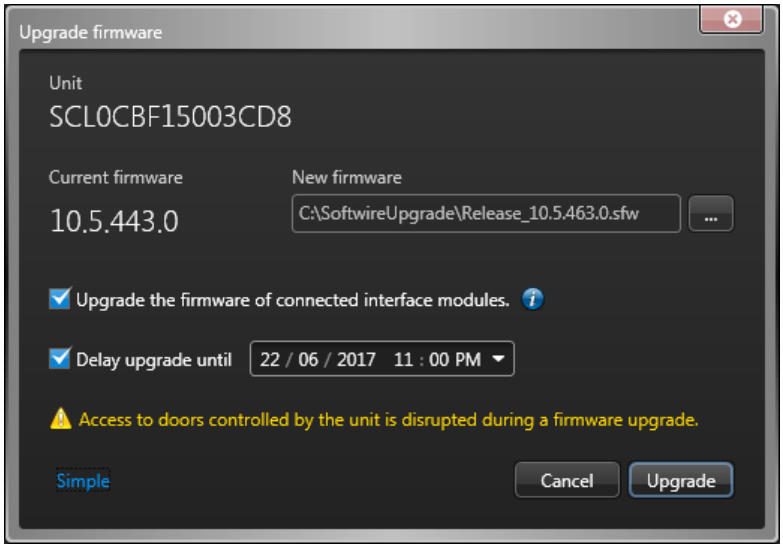
4 No navegador de arquivos, selecione o arquivo de firmware que você baixou do GTAP e clique em **Abrir**.

5 Para atualizar o firmware dos módulos de interface conectados ao controlador, selecione **Atualizar o firmware de módulos de interface conectados**.



NOTA: É recomendado que você selecione essa configuração ao atualizar os controladores HID Edge EVO ou HID VertX EVO V2000. Essa configuração é opcional para as unidades VertX EVO V1000 (até 3 minutos por interface), Synergis™ Cloud Link e Synergis™ Master Controller.

6 Para retardar a atualização, clique em **Avançado**, selecione **Retardar atualização até** e defina a data e a hora da atualização.



7 Clique em **Atualizar**.
O sistema atualiza o firmware das unidades de controle de acesso e as unidades são reiniciadas.

Exemplo

Assista a este vídeo para saber mais. Clique no ícone **Legendas** (**CC**) para ligar a legenda do vídeo em um dos idiomas disponíveis. O vídeo pode não ser exibido no Internet Explorer. Para resolver isso, abra as **Configurações de compatibilidade de exibição** e limpe **Exibir sites da intranet em Visualizar compatibilidade**.

Após terminar

- Quando as unidades voltarem a estar online, gere outro relatório de *Inventário de hardware* no Config Tool e confirme a versão de firmware exibida para as unidades.

  NOTA: Para unidades HID EVO, se **Atualizar o firmware de módulos de interface conectados** estava selecionado, a unidade permanece offline até que a atualização do firmware do módulo de interface seja concluída.
- Verifique se todas as portas controladas pelas unidades atualizadas estão operando corretamente.

Habilitar ou desabilitar registros de suporte para unidades de controle de acesso

O dispositivo Synergis™ pode manter registros detalhados para solução de problemas e suporte. É possível ativar ou desativar manualmente os registros de suporte se solicitado pelo Centro de Assistência Técnica da Genetec™.

O que você deve saber

Você pode ativar ou desativar registros de suporte para várias unidades simultaneamente no Security Center usando as instruções a seguir. Você também pode ativar registros de suporte para unidades individuais no Synergis™ Appliance Portal. Para obter mais informações sobre como configurar as opções de registro de eventos no Synergis™ Appliance Portal, consulte o *Guia de Configuração de Aparelho Synergis™*.

Para ativar ou desativar registros de suporte para unidades de controle de acesso:

1 No Config Tool, abra a tarefa *Access control* e clique na visualização *Funções e unidades*.

2 No Access Manager, selecione uma ou mais unidades de controle de acesso.

NOTA: Clicar no Access Manager seleciona todas as unidades de controle incluídas nele.

3 No menu com o botão direito do mouse, ou na barra de comandos contextual na parte inferior da tela, clique em **Manutenção** e selecione **Habilitar registros de suporte da unidade** ou **Desabilitar registros de suporte da unidade**.

Solução de problemas: problemas de descoberta e inscrição de unidade HID

Se não conseguir descobrir ou inscrever uma unidade de controle de acesso HID, existem alguns passos comuns de solução de problemas que podem ser usados para tentar resolver os problemas.

Para solucionar problemas de uma unidade HID que não pode ser descoberta ou inscrita:

1 Certifique-se de que o Config Tool e o *Access Manager* do computador estão em execução por trás de um firewall.

As portas 4050 *TCP* e 4070 *UDP* devem estar desbloqueadas.

2 Certifique-se de que todas as portas específicas do Synergis™ estejam abertas e desbloqueadas.

3 *Certifique-se de que a extensão HID VertX tenha sido adicionada ao Access Manager no Config Tool*.

4 Valide se a extensão HID VertX está devidamente carregada no Access Manager, da seguinte forma:

a) Para abrir uma sessão de console no Access Manager, abra um navegador da Web e vá para a URL `http://(server name or IP)/Genetec/console`.

NOTA: Se você não conseguir se conectar ao console, verifique se o acesso ao console está ativado no *Server Admin* , na aba **Genetec™ Server**.

b) Clique na aba **Comandos** na parte superior da página.

c) Na coluna **Comandos do Usuário**, à esquerda, expanda **Access Manager** e clique em **Status**.

d) Uma consulta de status é enviada para o Access Manager e a resposta contém as extensões que estão carregadas.

e) Certifique-se de que a seguinte linha é mostrada nos resultados de status: **HID VertX:4070 =** X **unidades**.

5 Verifique se a unidade tem um endereço IP estático.

6 Se o endereço IP da unidade for estático, você deve definir o DNS ou a unidade pode ter problemas de inscrição ou conexão.

a) Para acessar a GUI de configuração HID, digite o endereço IP da unidade em um navegador da Web.

b) Na GUI de Configuração HID, defina o DNS primário e secundário para os valores apropriados.

Se você não souber o DNS da rede, defina o endereço IP da unidade como o servidor DNS primário e secundário.

7 Certifique-se de que não existem outros aplicativos bloqueando as portas 4070, 4050 e 20:

a) Interrompa o Access Manager.

b) No Windows, clique em **Iniciar** > **Executar** e digite **cmd**para abrir o Prompt de Comando, em seguida execute **netstat -na**.

Solução de problemas: unidades HID não podem ser descobertas

Se você não conseguir descobrir uma unidade de controle de acesso HID usando a ferramenta de *Inscrição de unidade*, você pode solucionar a causa do problema.

Antes de iniciar

Realizar as etapas comuns de solução de problemas para resolver problemas de descoberta e inscrição de HID.

Para solucionar problemas de uma unidade HID que não pode ser descoberta:

1 Na página da Web Configuração avançada do HID VertX, certifique-se de que o nome do host está definido e que não tem mais do que 15 caracteres.

O nome do host deve ser definido e deve ter menos de 15 caracteres a serem descobertos.

2 Certifique-se de que a unidade está na mesma sub-rede da rede do computador em que o Config Tool está sendo executado.

Discovery só funciona dentro do mesmo domínio de *difusão*.

3 Verifique se o firmware da unidade está atualizado.

Para uma lista de versões de firmware suportadas, consulte *Notas de Lançamento do Security Center*.

Solução de problemas: unidades HID não podem ser inscritas

Se você não conseguir inscrever uma unidade de controle de acesso HID, você pode solucionar a causa do problema.

Antes de iniciar

Realizar as etapas comuns de solução de problemas para resolver problemas de descoberta e inscrição de HID.

O que você deve saber

Se você estiver enfrentando problemas de inscrição, o seguinte pode ocorrer:

- A unidade não pode ser inscrita
- A unidade é inscrita mas seu ícone permanece vermelho
- A unidade se conecta e desconecta continuamente
- Unidade começa a inscrição e falha em 67%

Para solucionar problemas de uma unidade HID que não pode ser inscrita:

1 Verifique se há conectividade com a unidade, da seguinte forma:

a) Faça o ping da unidade a partir do computador que executa o Access Manager: no Windows, clique em **Iniciar** > **Executar** e digite **cmd**para abrir o Prompt de Comando, então execute **ping w.x.y.z**.

NOTA: w.x.y.z é o endereço IP da unidade.

Um relatório é gerado. Certifique-se de que nenhum pacote foi perdido.

b) Faça o Telnet da unidade a partir do computador que executa o Access Manager para verificar suas credenciais: no Windows, clique em **Iniciar** > **Executar** e digite **cmd**para abrir o Prompt de Comando, então execute **telnet w.x.y.z**.

c) Faça o logon na unidade (Padrão: usuário=root / senha=pass).

Se o login for bem-sucedido, haverá conectividade à unidade.

2 Verifique se que a unidade está na mesma sub-rede da rede do computador em que o Access Manager está sendo executado.

Se não for, você pode inscrever a unidade manualmente desde que você saiba seu endereço IP (a unidade deve estar configurada para usar um endereço IP estático).

3 Verifique se o firmware da unidade e o firmware da placa de interface estão atualizados.

Para uma lista de versões de firmware suportadas, consulte *Notas de Lançamento do Security Center*.

4 Certifique-se de que o vínculo da placa de rede e a configuração de *banco de dados* para o Access Manager estão definidos corretamente.

5 Se o Access Manager estiver atrás de um NAT, você deve especificar o endereço do host traduzido para o Access Manager.

6 Certifique-se de que nenhum outro Access Manager esteja atualmente conectado à unidade HID, da seguinte maneira:
   a) Interrompa seu Access Manager.
   b) Faça Telnet com a unidade: no Windows, clique em **Iniciar** > **Executar**, e digite **cmd** para abrir o Prompt de Comando então execute **telnet w.x.y.z**.
   c) Faça o logon na unidade (Padrão: usuário=root / senha=pass).
   d) No prompt, digite **netstat -na**.

   Uma lista de conexões de rede é mostrada. Não deve haver nenhuma conectada à porta 4050.

7 Certifique-se de que as unidades HID (e as interfaces conectadas) estejam conectadas para não gerar alarmes de violação ou porta mantida aberta, eventos de acesso concedido ou acesso negado.

   Alarmes de violação e porta mantida aberta são disparados repetidamente. Após a conexão, tais alarmes e eventos devem ser baixados da unidade, o que pode retardar o processo de inscrição. Entre os sintomas disso estão a unidade ser difícil de se inscrever, a unidade se conectar e desconectar, ou a unidade emitir um sinal sonoro.

8 Atualize o firmware da unidade.

   Para uma lista de versões de firmware suportadas, consulte *Notas de Lançamento do Security Center*.

Solução de problemas: muitas solicitações para eventos de saída de portas

Se os registros de uma porta mostrarem um número muito grande de eventos de solicitação de saída para a quantidade real de atividade da porta, você pode tentar reduzir o número de eventos falsos de solicitação de saída nas opções da aba *Propriedades* da porta.

O que você deve saber

Se a sua porta for equipada com um dispositivo de solicitação de saída automática (com base em um sensor de *detecção de movimento*), às vezes um evento de *solicitação de saída* é disparado quando pessoas entram em uma área. Dependendo da qualidade do dispositivo de solicitação de saída automática e de como ele está instalado, o dispositivo pode disparar em qualquer atividade perto da porta.

Para reduzir o número eventos de solicitação de saída da porta:

1 Na página inicial do Config Tool, abra a tarefa *Exibição de área*.
2 Selecione a porta que está causando os problemas e clique na aba **Propriedades**.
3 Defina as seguintes opções de **Solicitação de saída** conforme necessário:
   - **Tempo para ignorar "Solicitação de saída" após acesso concedido:** Ignora quaisquer solicitações de saída para isto muito depois do acesso ter sido concedido.
   - **Destrancar pela requisição de saída:** Defina como **LIGADO** se um REX estiver sendo usado e você quiser automaticamente conceder a solicitação de saída.
   - **Ignorar eventos "Solicitação de saída" enquanto a porta estiver aberta:** Não gerar REX quando a porta estiver aberta.
   - **Tempo para ignorar "Solicitação de saída" após fechamento de porta:** Uma vez que a porta tenha fechado, espere este tempo antes de gerar mais eventos *Solicitação de saída*.
4 Clique em **Aplicar**.

Solução de problemas: Credenciais não funcionam

Se uma credencial não funcionar em uma porta ou elevador, você pode testar o motivo pelo qual o acesso é negado.

O que você deve saber

Para que uma credencial obtenha acesso a um determinado *lado da porta* ou andar de elevador, as condições a seguir devem ser cumpridas:

- O perfil da credencial deve estar ativado
- A credencial deve estar associada a um titular de cartão
- O perfil do titular de cartão deve estar ativado
- Deve haver pelo menos uma *regra de acesso* que conceda acesso especificamente para esse titular de cartão ou para o seu grupo de titulares de cartões.

Se essas configurações não estiverem corretas, o acesso é negado.

Para solucionar problemas de acesso negado:

- Use a solução de problemas de acesso para determinar porque o titular de cartão não tem acesso a uma porta ou a um elevador.

Solução de problemas: Os cartões não funcionam nos leitores

Se um cartão não estiver funcionando no leitor de uma porta, é possível solucionar a causa do problema.

Para solucionar uma credencial que não funciona em um leitor de cartão:

1 Certifique-se de que você está usando o tipo certo de tecnologia de cartão para o leitor.

Por exemplo, alguns leitores são multi-tecnologia (podem ler cartões 125 kHz e 13.56 MHz), e outros leitores só podem ler um tipo de cartão.

2 Teste se o cartão está com defeito tentando outro cartão.

3 Teste se o leitor está instalado muito perto de outro leitor desconectando um leitor da energia.

Se o outro leitor começar a operar corretamente, eles foram instalados muito próximos. Os leitores emitem um campo eletromagnético que pode interferir com outros leitores localizados nas proximidades.

4 Teste se você está usando o cabo apropriado para o leitor conectando um leitor de reserva diretamente à unidade com um cabo curto.

Se o leitor de reserva funcionar, você deve mudar o cabo do leitor original. Para obter o comprimento e tipo de cabo máximo, consulte a documentação do leitor e da unidade.

Solução de problemas: A instalação do driver falha para os leitores USB HID OMNIKEY

Se, sempre que tentar registrar uma credencial usando um leitor USB HID OMNIKEY, você vir uma mensagem de erro do Windows indicando que o driver não foi instalado, existem algumas etapas de solução de problemas que você pode usar para resolver o problema.

Antes de iniciar

- Desconecte o leitor OMNIKEY da estação de trabalho.
- FecheSecurity Desk e Config Tool.

O que você deve saber

Normalmente, este problema ocorre porque o Windows não consegue localizar o driver adequado para o leitor. Como o Windows tentará carregar o driver USB padrão, poderá parecer que o leitor funciona corretamente até que você observe algum comportamento indesejável. Para evitar tais comportamentos, recomenda-se instalar o driver específico para o tipo de leitor fornecido pelo fabricante.

Para solucionar um driver que não pode ser instalado:

1 Certifique-se de que seu leitor OMNIKEY seja compatível com o Security Center e esteja configurado corretamente.

Para obter uma lista de dispositivos compatíveis e definições de configuração, consulte o artigo da Base de Dados de Conhecimento KBA01374 no Genetec™ TechDoc Hub.

2 Instale o driver seguindo as instruções fornecidas no *Guia do Usuário do Leitor de Smart Card OMNIKEY*.

Você pode obter este guia visitando o site da HID em http://www.hidglobal.com/documents.

3 Quando a instalação estiver concluída, inicie o Security Desk e, em seguida, verifique se o leitor está ativado.

4 Tente inscrever uma credencial novamente.

A mensagem de erro não deve mais ser exibida.

Reconhecimento de placas de veículos

Esta parte inclui as seguintes chapters:

- "O LPR em um relance" na página 759
- "Funções e unidades LPR" na página 763
- "Listas de procurados" na página 787
- "Sistemas fixos AutoVu" na página 813
- "AutoVu Free-Flow" na página 829
- "Sistemas móveis AutoVu" na página 858
- "Sistemas de aplicação da lei AutoVu" na página 873
- "Sistemas de fiscalização de estacionamento na cidade e na universidade AutoVu" na página 878
- "Sistemas de inventário de placas de veículos móvel AutoVu" na página 905
- "Solução de problemas de LPR" na página 911

38

O LPR em um relance

Esta seção inclui os seguintes tópicos:

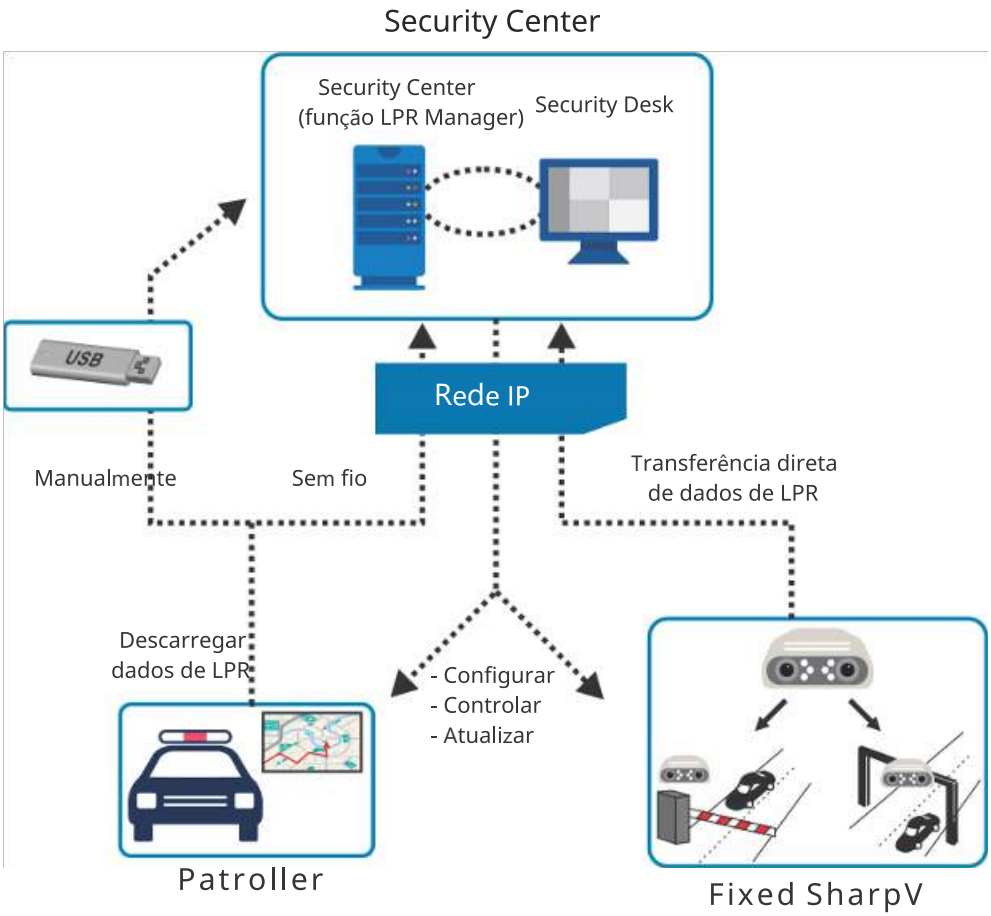
- "Sobre o Security Center AutoVu" na página 760
- "Entidades relacionadas a LPR do AutoVu" na página 762

Sobre o Security Center AutoVu™

Security Center AutoVu™ é o sistema de reconhecimento automático de placas de veículo (ALPR) que automatiza a leitura e a identificação de placas de veículo. Implantado em instalações fixas e móveis, permite estender a sua segurança física aos seus estacionamentos e perímetros, para que você esteja sempre ciente dos veículos que entram e saem das suas instalações.

As câmeras AutoVu™ Sharp capturam imagens de placas de veículos e enviam os dados para o Genetec Patroller™ ou o Security Center para comparar com listas de veículos de interesse (listas de procurados) e veículos com autorizações (listas de autorizações). É possível instalar o AutoVu™ em uma configuração fixa (por exemplo, em um poste de um estacionamento) ou móvel (por exemplo, em um carro da polícia). É possível usar o AutoVu™ para identificação de veículos procurados e pessoas que ignoram a lei, vigilância pela cidade, fiscalização de estacionamento, controle de autorizações de estacionamento, inventário de veículos, segurança e controle de acesso.

O diagrama a seguir mostra como funciona um sistema AutoVu™ típico:



Exemplo

Assista a este vídeo para saber mais. Clique no ícone **Legendas** (**CC**) para ligar a legenda do vídeo em um dos idiomas disponíveis. O vídeo pode não ser exibido no Internet Explorer. Para resolver isso, abra as **Configurações de compatibilidade de exibição** e limpe **Exibir sites da intranet em Visualizar compatibilidade**.

Entidades relacionadas a LPR do AutoVu™

O sistema de reconhecimento automático de placas de veículo (ALPR ou LPR) do AutoVu™ suporta muitas das entidades disponíveis no Security Center.

A tabela a seguir lista as entidades relacionadas ao LPR.

Ícone	Entidade	Descrição
	LPR Manager	Função que armazena todos os dados de LPR coletados das unidades LPR (Sharps fixas) e veículos de patrulha que ela gerencia.
	Unidade LPR	Dispositivo LPR baseado em IP.
	Lista de procurados	Lista de veículos.
	Regra de tempo extra	Tipo de regra de alerta que especifica um limite de tempo para estacionamento dentro de uma área restrita.
	Estacionamento	Define uma área de estacionamento ou garagem de estacionamento como um número de setores e linhas, para rastrear veículos dentro desse estacionamento.
	Regra de estacionamento	Uma regra de estacionamento define como e quando uma sessão de estacionamento é considerada como sendo válida ou uma violação.
	Patroller	Software que é executado em um computador a bordo de um veículo, que verifica placas de veículo.
	Autorização	Define uma lista de titulares de permissão de estacionamento.
	Restrição de autorização	Tipo de regra de alerta que especifica onde e quando os titulares de autorização podem estacionar.
	Usuário	Pessoa que usa aplicativos Security Center.
	Grupo de usuários	Grupo de usuários que compartilham características em comum.

39

Funções e unidades LPR

Esta seção inclui os seguintes tópicos:

- "Sobre o LPR Manager" na página 764
- "Configuração das funções do LPR Manager" na página 766
- "Configurar a função Archiver para LPR" na página 769
- "Requisitos de armazenamento para imagens de LPR" na página 772
- "Sobre unidades de LPR" na página 774
- "Equivalência de LPR" na página 775
- "Arquivo MatcherSettings.xml" na página 780
- "Boas práticas para definir configurações de equivalência de LPR" na página 782
- "Definir configurações de equivalência de LPR" na página 783
- "Atualizar o SharpV a partir do Security Center" na página 786

Sobre o LPR Manager

A função LPR Manager gerencia e controla o software do veículo de patrulha (Genetec Patroller™), câmeras Sharp e zonas de estacionamento. O LPR Manager armazena os dados de LPR (leituras, ocorrências, carimbos de data e hora, coordenadas GPS e assim por diante) coletados pelos dispositivos.

Múltiplas instâncias desta função podem ser criadas no sistema para proporcionar escalabilidade e particionamento. Por exemplo, diferentes frotas de veículo de patrulha podem ser gerenciados por diferentes *LPR Managers*.

NOTA: Você deve também registrar a unidade de processamento de LPR no Archiver para instalações do SharpX onde o controle de entrada/saída da unidade de processamento LPR é necessário.

Pasta raiz do LPR Manager

A pasta raiz é a pasta principal no computador que hospeda o LPR Manager. É onde todos os arquivos de configuração são criados, salvos e trocados entre o LPR Manager e as unidades Genetec Patroller™ que ele administra.

Quando você cria uma função LPR Manager, a pasta raiz é criada automaticamente em seu computador, localizada em: *C:\Genetec\AutoVu\RootFolder*. Se você criar vários LPR Managers, as novas pastas serão criadas no mesmo local. Por exemplo, se você criar três LPR Managers, o Security Center cria automaticamente as seguintes pastas:

- *C:\Genetec\AutoVu\RootFolder1*
- *C:\Genetec\AutoVu\RootFolder2*
- *C:\Genetec\AutoVu\RootFolder3*

A pasta raiz de cada LPR Manager inclui as seguintes subpastas:

- **ManualTransfer:** Contém os arquivos de dados e de configuração para transferir para o Genetec Patroller™ manualmente usando uma unidade USB ou dispositivo similar.
- **Offload:** Contém os dados LPR descarregados pelo Genetec Patroller™.
- **Rules:** Contém os arquivos delta usados pelo Security Center para transferir alterações em listas de procurados e lista de autorizações. **Não** copie nem mova nada nesta pasta.
- **Updates:** Esta pasta aparece quando você liga o fornecedor de atualizações pela primeira vez Contém hotfixes para Security Center e Genetec Patroller™, assim como atualizações de serviço e firmware para Sharp. Os hotfixes para Genetec Patroller™ são automaticamente baixados para o Genetec Patroller™ sempre que ele é conectado ao Security Center. As unidades Sharp móveis são atualizadas pelo Genetec Patroller™, e as unidades Sharp fixas são atualizadas pela rede.

Gerenciamento de dados de LPR

Os dados de LPR são gerenciados pela função LPR Manager e pela função Archiver. Ambas as tarefas trabalham em conjunto. Se o Archiver não puder armazenar as imagens (por exemplo, quando os discos estão cheios), o LPR Manager deixa de armazenar os dados de LPR, e as instalações de Genetec Patroller™ e unidades Sharp fixas que são controladas pelo LPR Manager armazenam temporariamente os dados em nível local até que o problema seja resolvido.

- **LPR Manager**:
  - Os dados de LPR (leituras, ocorrências, carimbos de data/hora, posições de Genetec Patroller™ e assim por diante) são armazenados pela função LPR Manager em um banco de dados do SQL Server.
  - Se você tiver muitas funções LPR Manager no seu sistema, todas elas podem ser ligadas à mesma função Archiver.
- **Archiver**:

- As imagens de LPR (capturadas por câmeras de contexto, câmeras de LPR e câmeras WMS) associadas a leituras e ocorrências são armazenadas no sistema de arquivos por uma função Archiver.
- A função Archiver segue os períodos de retenção de dados configurados para o LPR Manager.

Configuração das funções do LPR Manager

Para gerenciar leituras, ocorrências e eventos de estacionamento, você deve primeiro definir as configurações da função LPR Manager, tais como Genetec Patroller™ grupos de usuários, períodos de retenção de dados, e assim por diante, deve também atribuir uma função de Archiver para gerenciar as imagens LPR (capturadas por câmeras de contexto, câmeras LPR e câmeras WMS) associadas às leituras e ocorrências.

Antes de iniciar

Leia os seguinte antes de configurar o LPR Manager:

- Criar uma função de Archiver dedicada ao gerenciamento de imagens LRP.

O que você deve saber

- Um banco de dados do SQL Server Express pode ficar cheio antes do fim do período de retenção. Entre em contato com a GTAP para ajudá-lo a avaliar os seus requisitos de banco de dados.

  NOTA: Ao usar o SQL Server Express Edition, reduzir o período de retenção cria espaço para mais dados mas não reduz o tamanho do banco de dados.

- Quando o AutoVu™ está ativado em sua licença, uma função LPR Manager e Archiver são criadas por padrão e no servidor principal.
- Se você tiver um sistema grande, você pode distribuir a carga criando mais funções LPR Manager e hospedando-as em servidores separados.

Para configurar a função LPR Manager:

1 Na página inicial do Config Tool, abra a tarefa *LPR* e clique em **Funções e unidades**.

2 Selecione o LPR Manager que deseja configurar e clique em **Propriedades** > **Configurações gerais**.

3 Para alterar a localização da **Root folder** do LPR Manager, navegue para uma pasta diferente na máquina local ou crie uma pasta de rede.

  NOTA: Se o computador estiver hospedando mais de um LPR Manager, cada um deles deve ter uma pasta raiz diferente.

4 Se você possui grandes listas de procurados e listas de autorização associadas a unidades Genetec Patroller™ individuais, ative a opção **Otimizar o espaço em disco da pasta raiz**.

  IMPORTANTE: Se a sua pasta Raiz estiver em uma unidade de rede, o serviço Genetec™ Server deve ser configurado usando um usuário de domínio e não um usuário local.

  Ativar essa opção permite o uso de links simbólicos para reduzir o espaço em disco da pasta raiz e otimizar o desempenho da transferência de arquivos do computador do veículo. No servidor e nas máquinas clientes (exige direitos de administrador), abra o prompt de comando do Windows e digite o seguinte:

  - **Para ativar links simbólicos:** Digite `fsutil behavior set SymlinkEvaluation R2R:1`
  - **Para desativar links simbólicos:** Digite `fsutil behavior set SymlinkEvaluation R2R:0`.

5 Na lista suspensa **Grupo de usuários para Patrollers**, selecione o grupo de usuários que contém a lista de usuários com permissão para fazer logon nos veículos de patrulha gerenciados pelo LPR Manager.

  No Patroller Config Tool, se a Genetec Patroller™ *Tipo de logon* for *Nome seguro* ou *Nome e senha seguros*, o usuário do Genetec Patroller™ deve inserir o nome de usuário e senha definidos no Security Center. Se os nomes de logon seguro estiverem em uso, quando uma leitura ou um alerta ocorrer, você pode ver quem estava dirigindo o veículo no Security Desk.

6 Na seção *Período de retenção*, especifique por quanto tempo os dados relacionados a LPR podem ser mantidos:

- **Genetec Patroller™ período de retenção de rota:** Número de dias em que os dados de Genetec Patroller™ *rota* (coordenadas GPS) são mantidos no banco de dados.
- **Período de retenção de alerta:** Número de dias durante os quais os dados do alerta são mantidos na base de dados do Gerenciador LPR.
- **Período de retenção de imagem de alerta:** Número de dias durante os quais a imagem do alerta é mantida pela função do Archiver conectado. The *Período de retenção de imagem de ocorrência* não pode exceder o *Período de retenção de ocorrência* uma vez que uma imagem de ocorrência está sempre associada a uma ocorrência.
- **Período de retenção de leitura:** Número de dias durante os quais as *leituras de placa de licença* são mantidos na base de dados do Gerenciador LPR. O *período de retenção de leitura* não pode ultrapassar o *período de retenção de alerta*. Se a retenção de leitura for menor do que a retenção de alerta, apenas as leituras associadas aos alertas são mantidas.
- **Período de retenção de imagem de leitura:** Número de dias em que os dados de leitura da imagem são mantidos pela função de Archiver ligado. O *período de retenção de leitura de imagem* não pode exceder o *período de retenção de leitura*, uma vez que uma leitura de imagem está sempre associada a uma leitura.
- **Período de retenção de evento:** Número de dias durante os quais os eventos do Genetec Patroller™ (usuário conectado, desconectado e posições do veículo de patrulha) são mantidos na base de dados do LPR Manager.
- **Período de retenção da ocupação de estacionamento:** Número de dias em que os dados da ocupação do estacionamento são mantidos na base de dados do LPR Manager.
- **Período de retenção de dados de zona de estacionamento:** Número de dias em que os dados da zona de estacionamento são mantidos na base de dados do LPR Manager. Esses dados incluem informações de sessão de estacionamento, por exemplo, os horários de início da sessão de estacionamento e transições de estado, assim como informações de eventos que ocorreram dentro da zona de estacionamento. O *período de retenção de dados da zona de estacionamento* não pode ultrapassar o *período de retenção de leitura*.

O valor padrão para cada configuração é 90 dias e o máximo é 4000 dias. Dados expirados não aparecem nas consultas e relatórios do Security Center (relatórios de ocorrências, relatórios de leituras e assim por diante).

NOTA: Você não pode reduzir o tamanho do banco de dados reduzindo as configurações do período de retenção. O objetivo do algoritmo de limpeza da retenção é fazer espaço para dados novos. Contudo, o tamanho do arquivo do banco de dados em disco nunca diminuirá.

7 Clique em **Aplicar**.

8 Clique em **Recursos** > **Imagens salvas em**, e selecione o Archiver designado para gerenciar os dados de imagem para o LPR Manager.

Em uma nova instalação, o Archiver padrão é atribuído automaticamente para o LPR Manager. Se o seu sistema é usado somente para LPR, você pode deixar a configuração padrão. Caso você queira gerenciar também vídeos no seu sistema, recomendamos que crie funções de Archiver separadas para o gerenciamento de vídeo.

Em um cenário de atualização, um Archiver é automaticamente atribuído a um LPR Manager somkente se for o único Archiver no sistema e somente se o Archiver não gerenciar quaisquer unidades de vídeo.

9 Clique em **Aplicar**.

10 Se você tiver selecionado um Archiver, clique em **Pular para** ( ) ao lado do nome do Archiver.

Isso o leva diretamente à aba **Recursos** do Archiver selecionado.

11 Configure a função Archiver para LPR.

As configurações básicas do LPR Manager estão definidas. Você pode continuar a personalizar o sistema AutoVu™ definindo as outras configurações do LPR Manager.

Tópicos relacionados

Sobre o LPR Manager na página 764
LPR Manager - Aba Propriedades na página 1066

LPR Manager - Aba Recursos na página 1074
Adicionar unidades de vídeo manualmente na página 447

Configurar a função Archiver para LPR

Você deve vincular um Archiver ao LPR Manager para armazenar as imagens de LPR que estão associadas a leituras e ocorrências.

O que você deve saber

Caso seja necessário gerir dados de LPR e de vídeo, recomendamos que você crie funções Archiver separadas, cada uma processando apenas uma função.

Cada função Archiver deve armazenar vídeo em uma unidade ou partição separada de outras funções Archiver. Caso não seja possível ter funções Archiver separadas, você pode gerir dados de LPR e vídeo com o mesmo Archiver. Note que, por padrão, o Archiver exclui os arquivos mais antigos quando o disco fica cheio. Isto significa que poderão ser excluídas imagens de LPR antes de seu período de retenção expirar. Isto não afeta os metadados de LPR ou os eventos e imagens protegidos.

Para criar uma função Archiver para LPR:

1 Na página inicial do Config Tool, abra a tarefa *Vídeo*.

2 Clique no botão de menu próximo a **Unidade de vídeo** ( ) e, em seguida, clique em **Archiver** ( ).

A janela do assistente de criação de funções é aberta.

3 Na página *Informações Específicas*, defina os seguintes campos e clique em **Próximo**.

- **Servidor:** Isto só é exibido se você tiver mais de um servidor no seu sistema. Se o LPR Manager for hospedado no seu próprio servidor, sugerimos usar o mesmo servidor para hospedar a função Archiver vinculada. Caso se trate de uma atualização do Security Center 5.5 ou anterior, certifique-se de ter espaço livre em disco suficiente para armazenar imagens de LPR. Recomendamos usar um servidor onde seja possível configurar a função Archiver com a sua partição ou o seu disco local dedicado.
- **Servidor de banco de dados:** Nome do serviço SQL Server (padrão=`(local)\SQLEXPRESS`). Se o Archiver for hospedado no mesmo servidor do LPR Manager, recomendamos usar o mesmo servidor de banco de dados para os dois.
- **Banco de dados:** Nome da instância de banco de dados (padrão=`Archiver`). Sugerimos usar `LPR_Archiver` para diferenciá-lo de bancos de dados de arquivos de vídeos.

4 Na página *Informações básicas*, defina os seguintes campos e clique em **Próximo**.

- **Nome da entidade:** Nome da função Archiver (padrão=`Archiver`).

  Sugerimos usar `LPR_Archiver` para diferenciá-la da função Archiver para vídeo.
- **Descrição da entidade:** Descrição da função. Se esta função Archiver for compartilhada por muitas funções LPR Manager, liste-as aqui.
- **Partição:** Isto só é exibido se você tiver partições definidas no seu sistema. Certifique-se de criar este Archiver na mesma partição do LPR Manager ao qual está vinculado. Somente os usuários que tenham acesso à partição selecionada podem visualizar os dados de LPR geridos por estas funções.

5 Verifique se as informações exibidas na página *Resumo de criação* estão corretas e clique em **Criar**.

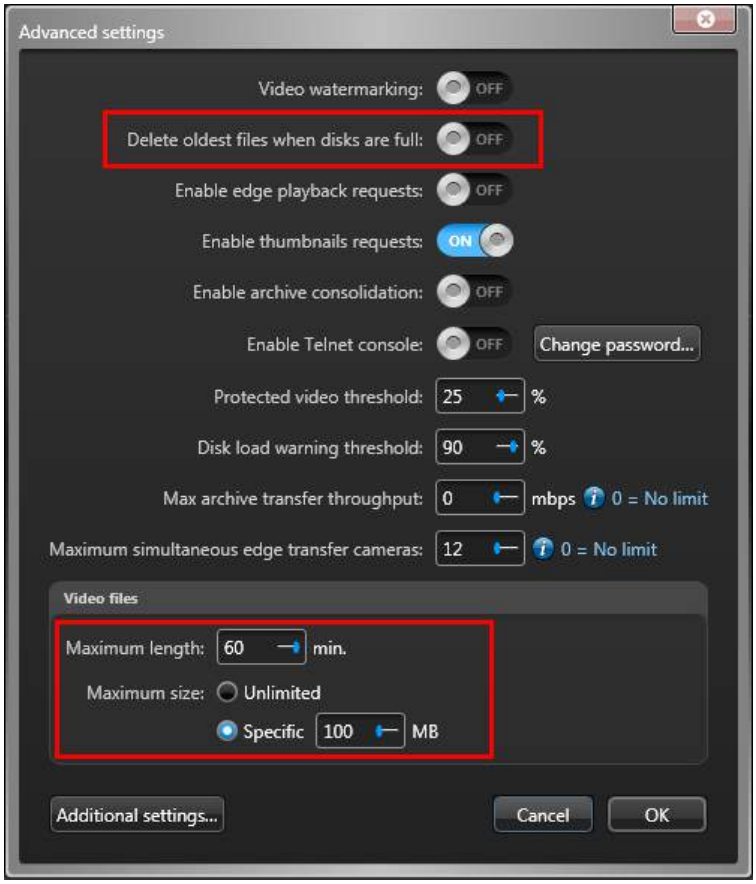
6 Clique em **Fechar**.

7 Na aba **Recursos** da função Archiver, defina as configurações de armazenamento de arquivos.

IMPORTANTE: Certifique-se de não estar usando o mesmo disco de outra função Archiver no seu sistema e de ter suficiente espaço em disco para armazenar imagens de LPR.

NOTA: O Archiver obedece ao período de retenção de imagens de **Ocorrência** e **Leitura** definido para o LPR Manager. Se houver várias funções LPR Manager vinculadas ao mesmo Archiver, o LPR Manager com o período de retenção de imagens mais longo tem precedência. Isto significa que os dados de imagens poderão ser mantidos por mais tempo do que o necessário para algumas funções LPR Manager, mas isso não afeta os metadados de LPR nem os relatórios de LPR. Nenhum dado de LPR que esteja além dos períodos de retenção especificados aparecerá em relatórios.

8 Clique em **Configurações avançadas** e otimize as configurações para armazenar dados de imagens de LPR.

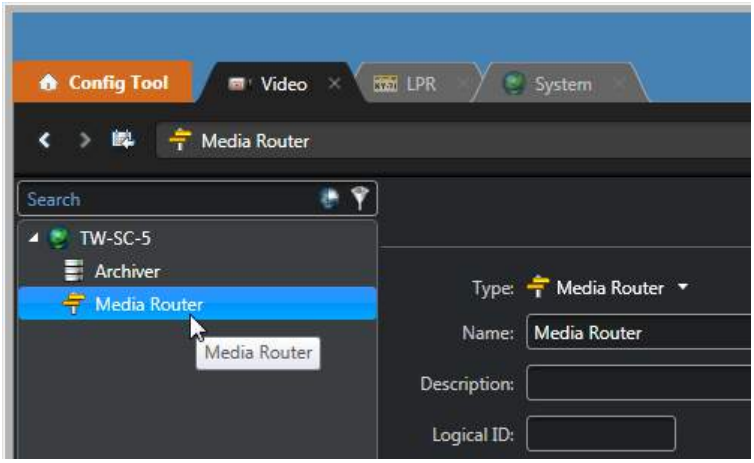


Os valores recomendados são:

- **Excluir arquivos mais antigos quando os discos estiverem cheios:** Desligado (configuração padrão para vídeo é Ligado).
- **Duração máxima:** 60 minutos (valor padrão para vídeo é 20 minutos).
- **Tamanho máximo:** 100 MB (valor padrão para vídeo é 500 MB).

9 Clique em **OK** > **Aplicar**.

10 No navegador de entidades (painel esquerdo) da tarefa *Vídeo*, certifique-se de que a função Media Router esteja em execução.



11 Clique em **Media Router** e configure as portas, os redirecionadores e as placas de rede para garantir que o Archiver possa distribuir as imagens de LPR por todas as estações de trabalho no seu sistema.

Se todos os seus servidores estiverem na mesma rede e se todos os seus servidores somente tiverem uma placa de rede, as configurações padrão deverão funcionar sem mais alterações.

Tópicos relacionados

Sobre o Media Router na página 462
Configurar a função Media Router na página 463
Adicionar redirecionadores ao Media Router na página 464
Sobre a exibição de rede na página 156
Personalizando opções de rede na página 159

Requisitos de armazenamento para imagens de LPR

As imagens associadas a leituras e ocorrências são armazenadas em disco em arquivos G64 por um Archiver. Você pode estimar o espaço em disco necessário para armazenar estas imagens se souber o número médio de leituras e ocorrências processado por dia pelo LPR Manager.

Por cada leitura de placa de veículo ou ocorrência processada pelo LPR Manager, o Archiver armazena um conjunto de quatro imagens:

- Uma imagem de câmera de contexto (em alta ou baixa resolução)
- Uma imagem de câmera de LPR (recortada para somente exibir a placa de veículo)
- Uma imagem em miniatura da câmera de contexto
- Uma imagem em miniatura da câmera de LPR

O tamanho do conjunto de imagens depende do modelo de câmera Sharp e do fato de a câmera de contexto estar configurada para obter imagens em alta ou baixa resolução.

Use a seguinte fórmula para estimar o espaço em disco necessário para os períodos de retenção de imagens desejados.

```
Disk space = (ReadsPD x ImageSize x ReadIRP) + (HitsPD x ImageSize x HitIRP)
```

onde:

- **ReadsPD:** Número médio de leituras por dia.
- **ImageSize:** Tamanho estimado de imagens por leitura (depende do modelo e da configuração do Sharp).
- **ReadIRP:** Período de retenção de imagens de leituras (consulte a aba **Propriedades** do LPR Manager).
- **HitsPD:** Número médio de ocorrências por dia.
- **HitIRP:** Período de retenção de imagens de ocorrências (consulte a aba **Propriedades** do LPR Manager).

Se os seus veículos de patrulha estiverem equipados com câmeras WMS, duplique o número de ocorrências por dia na sua fórmula (há normalmente uma imagem de roda por ocorrência).

A seguinte tabela apresenta estimativas aproximadas do tamanho de imagens por leitura com base no modelo e na configuração do Sharp.

Tipo de imagem	Sharp VGA ou XGA	SharpV
Imagem de câmera de contexto (config. de alta res.)	~50 KB	~120 KB
Imagem de câmera de contexto (config. de baixa res.)	~18 KB	-
Imagem de câmera de LPR (recortada)	~3 KB	~3 KB
Imagem em miniatura de câmera de contexto	~3 KB	~3 KB
Imagem em miniatura de câmera de LPR	~1 KB	~1 KB
Tamanho de imagem por leitura (config. de alta res.)	~57 KB	~127 KB
Tamanho de imagem por leitura (config. de baixa res.)	~25 KB	-

NOTA: Se uma leitura ou ocorrência estiver protegida e for necessário mantê-la para além do período de retenção especificado, ela exigirá mais espaço em disco para as suas imagens associadas do que o calculado para um evento simples. Como o Archiver armazena várias imagens de LPR em um único arquivo G64, se uma imagem no arquivo estiver protegida, todas as outras imagens no arquivo ficam protegidas.

Isto consome mais espaço em disco com o tempo. No entanto, uma imagem cuja leitura ou ocorrência correspondente tenha sido excluída não pode mais ser lida porque os arquivos G64 são criptografados.

Se o Archiver for atribuído a mais de um LPR Manager, adicione os números para todas as funções de LPR Manager juntas.

Sobre unidades de LPR

Uma Unidade de LPR é um dispositivo que captura números de placas de veículo. Uma Unidade de LPR inclui normalmente uma câmera de LPR e uma câmera de contexto. Essas câmeras podem ser incorporadas à unidade ser externas a ela.

AutoVu™ Sharp é a unidade de LPR usada em soluções Security Center AutoVu™. O Sharp inclui componentes de captura e processamento de placa de licença, bem como funções de processamento de vídeo digital, envolvidas em um estojo robusto. Sharps podem ser implantados em instalações móveis e fixas.

- **Instalação de AutoVu™ móveis**: A câmera Sharp é montada em um veículo e é integrado no Genetec Patroller™ (o software de bordo do sistema de LPR AutoVu™) que, por sua vez, é integrado no Security Center. O LPR Manager detecta Sharps móveis através do sistema AutoVu™ Genetec Patroller™ ao qual estão conectados.
- **Instalação de AutoVu™ fixos**: A câmera Sharp é montada em uma localização fixa, como um poste, e integrada diretamente no Security Center. O LPR Manager detecta Sharps fixos diretamente através da *porta de descoberta* do Security Center.

Equivalência de LPR

A equivalência de LPR é o mecanismo de software AutoVu™ que combina placas de veículo capturadas por câmeras Sharp com placas de veículo em uma fonte de dados, como uma lista de procurados ou lista de autorizações, ou placas de veículo previamente capturadas, como, por exemplo, para fiscalização de tempo extra. A equivalência LPR determina se uma placa lida resulta em um alerta.

Como funciona a lógica de equivalência LPR

As condições do mundo real tornam difícil o reconhecimento das placas. As placas de veículo podem ter caracteres escondidos por sujeira ou neve, enquanto que a pintura de outros caracteres pode estar desbotada ou descascada. Algumas placas de veículo têm imagens ou parafusos que podem ser mal interpretados como caracteres legítimos da placa.

Se a equivalência LPR só fosse capaz de levantar um alerta com base em uma correspondência exata, muitas placas que deveriam ser alertas seriam perdidas.

Exemplo

Uma lista de procurados contém a placa ABC123. Enquanto está em patrulha, uma câmera Sharp lê a placa ABC12, mas não consegue ler o último caractere porque a tinta do caractere está descascada.

A equivalência de LPR deve ser capaz de mais do que apenas a lógica "sim/não" porque a placa ABC12 *poderia* ser uma correspondência. Seria melhor acionar a ocorrência de lista de procurados e deixar o operador do Genetec Patroller™ decidir se a ocorrência é ou não legítima. Para fazer isso, a equivalência LPR usa diferentes níveis de lógica "talvez" para permitir mais possibilidades para uma equivalência de placas.

Técnica de equivalência de LPR: Equivalência de OCR

A equivalência de LPR usa a técnica de *equivalência de Reconhecimento Óptico de Caracteres (OCR)* para melhorar a taxa de precisão da leitura de placas de veículos.

Dependendo do modelo da fonte, alguns caracteres de placa podem parecer muito semelhantes a outros caracteres. Estes são chamados de "caracteres equivalentes de OCR".

Você pode configurar como a equivalência LPR lida com a equivalência OCR modificando o arquivo MatcherSettings.xml. Para mais informações, consulte Arquivo MatcherSettings.xml na página 780.

NOTA: Você também pode configurar as seguintes técnicas LPR no arquivo MatcherSettings.xml:

- Número de diferenças de caracteres (ver Técnica de equivalência de LPR: Número de diferenças de caracteres na página 776)
- Caracteres comuns e adjacentes (ver Técnica de equivalência de LPR: Caracteres comuns e adjacentes na página 778)

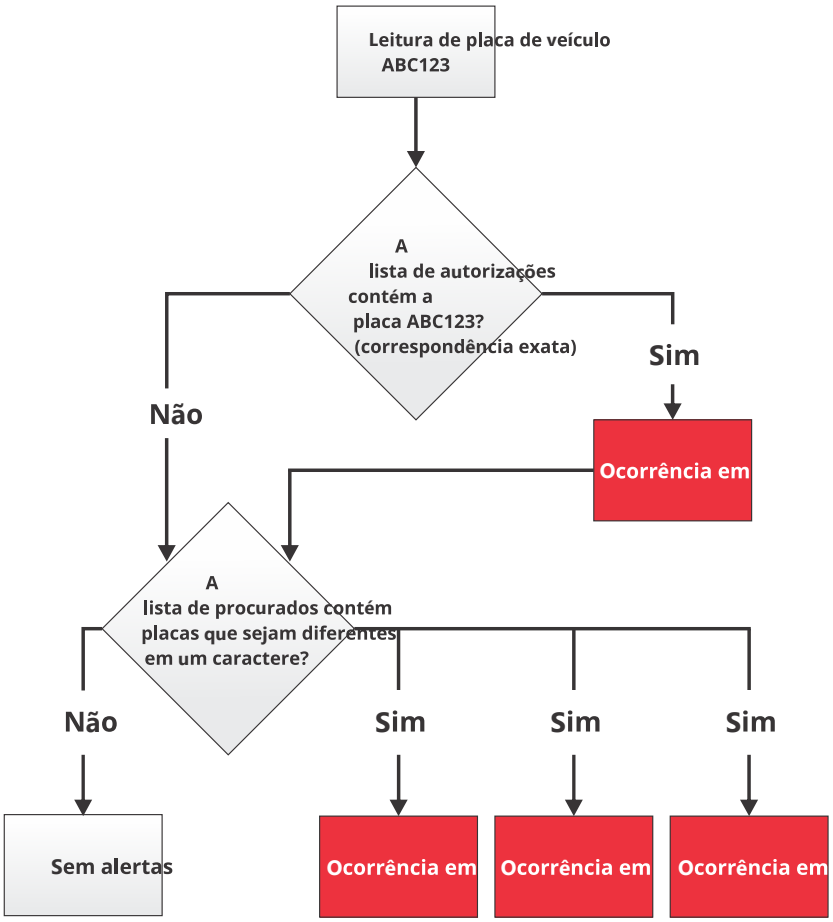
Os caracteres equivalentes ao OCR baseado em caracteres latinos são os seguintes:

- O número “0” e as letras “O”, “D”, e “Q”.
- O número “1” e a letra “I”.
- O número “2” e a letra “Z”.
- O número “5” e a letra “S”.
- O número “8” e a letra “B”.
- O número “6” e a letra “G”.

MELHOR PRÁTICA: Você não deve permitir mais de dois caracteres equivalentes de OCR porque isso acarreta muitos resultados falsos positivos.

Exemplo

O exemplo a seguir usa uma lista de procurados com a equivalência LPR configurada para permitir um caractere equivalente de OCR:



A equivalência LPR encontra a correspondência exata ABC123 no hotlist e levanta o alerta. Ela também procura placas que sejam diferentes em um caractere equivalente de OCR, e encontra A**8**C123, ABC1**Z**3 e ABC**I**23 na lista de procurados, alertando também para essas ocorrências.

Se a equivalência de LPR tivesse encontrado a placa A**8**C**IZ**3 (diferença de três caracteres equivalentes de OCR), ela não alertaria de uma ocorrência porque o sistema está configurado para aceitar, no máxima, uma diferença de OCR.

Técnica de equivalência de LPR: Número de diferenças de caracteres

A equivalência de LPR usa a técnica de "Número de diferenças de caracteres" para melhorar a taxa de precisão da leitura de placas.

Esta técnica permite uma diferença no número de caracteres entre a leitura da placa e o número da placa na lista de procurados. Isso permite que o sistema considere os caracteres na placa que não podem ser lidos (sujeira, ângulo de câmera ruim etc.) e objetos na placa que podem ser confundidos com caracteres legítimos (parafusos, imagens etc.).

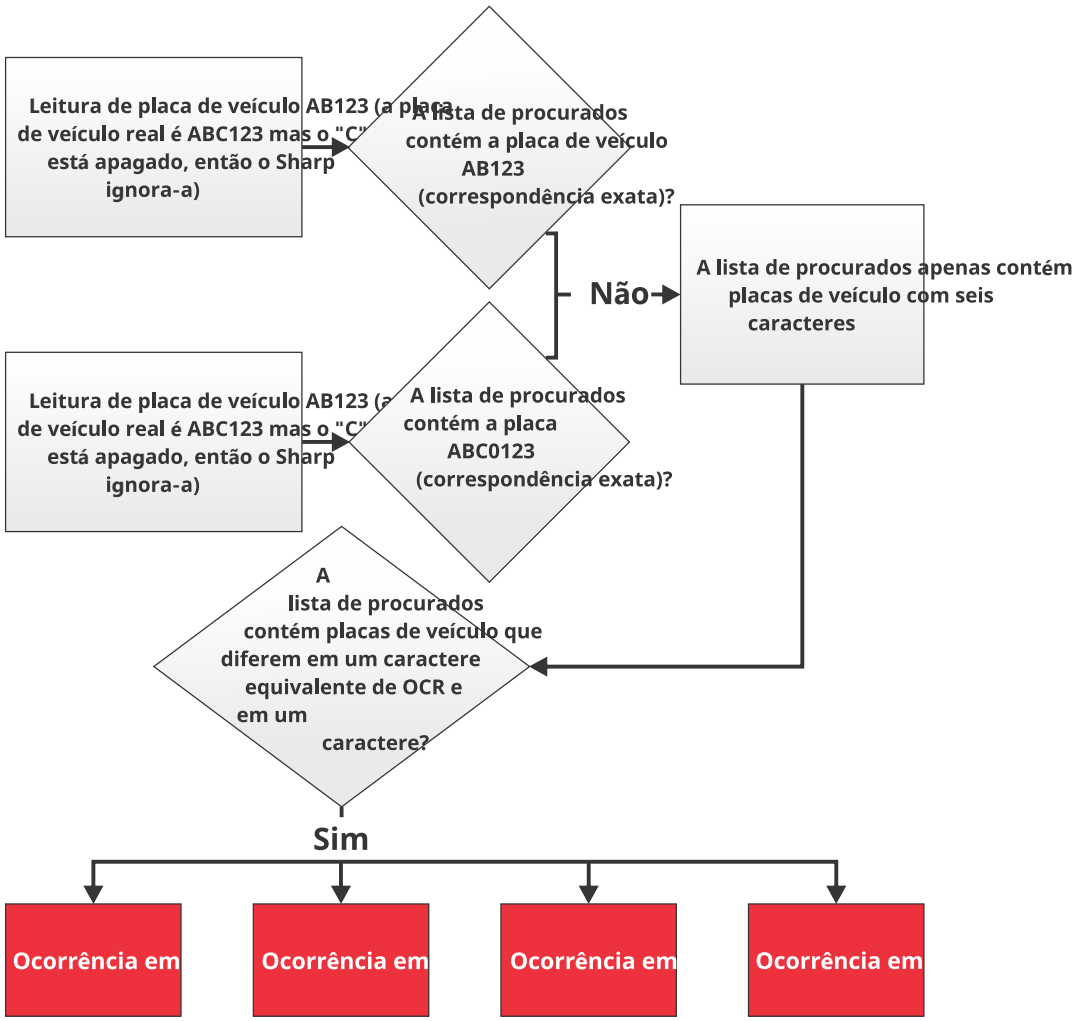
Você pode configurar como a equivalência LPR lida com as "Diferenças de números de caracteres" modificando o arquivo MatcherSettings.xml. Para mais informações, consulte Arquivo MatcherSettings.xml na página 780.

NOTA: Você também pode configurar as seguintes técnicas LPR no arquivo MatcherSettings.xml:

- Equivalência OCR (ver Técnica de equivalência de LPR: Equivalência de OCR na página 775)
- Caracteres comuns e adjacentes (ver Técnica de equivalência de LPR: Caracteres comuns e adjacentes na página 778)

Exemplo

O exemplo a seguir usa uma lista de procurados com a equivalência de LPR configurada para permitir *um* caractere equivalente de OCR e *uma* diferença no número de caracteres permitido:



Como você permitiu um caractere equivalente de OCR *e* uma diferença de caractere, a equivalência de LPR procura por ambos antes de permitir uma correspondência. Isso resulta no seguinte:

- Não há correspondência exata possível para placas de placas AB123 e ABC0123 porque a lista de procurados contém apenas placas de seis caracteres.
- As leituras de placas AB123 e ABC0123 correspondem à placa ABC123 porque você permitiu a diferença de um caractere. Não importa se é um caractere a mais ou a menos do que a placa equivalente.

- As leituras de placas AB123 e ABC0123 correspondem às placas A**8**C123, ABC**I**23 e ABC1**Z**3 porque você permitiu uma diferença de um caractere *e* um caractere equivalente de OCR.

Se você estivesse usando uma lista de autorizações em vez de uma lista de procurados, *nenhuma* das placas correspondentes no exemplo acionaria ocorrências (você recebe uma ocorrência de autorização quando uma placa *não* está na lista de autorizações).

Técnica de equivalência de LPR: Caracteres comuns e adjacentes

A equivalência de LPR usa a técnica de "Caracteres comuns e adjacentes" para melhorar a taxa de precisão da leitura de placas de veículo (por vezes chamada de "correspondência difusa").

NOTA: Este método é usado apenas para fiscalização de tempo extra em estacionamento.

Você pode configurar a forma como a equivalência de LPR lida com caracteres comuns e adjacentes modificando o arquivo MatcherSettings.xml. Para obter mais informações, consulte Arquivo MatcherSettings.xml na página 780.

NOTA: Você também pode configurar as seguintes técnicas de equivalência de LPR no arquivo MatcherSettings.xml:

- Equivalência de OCR (consulte Técnica de equivalência de LPR: Equivalência de OCR na página 775)
- Diferenças no número de caracteres (consulte Técnica de equivalência de LPR: Número de diferenças de caracteres na página 776)

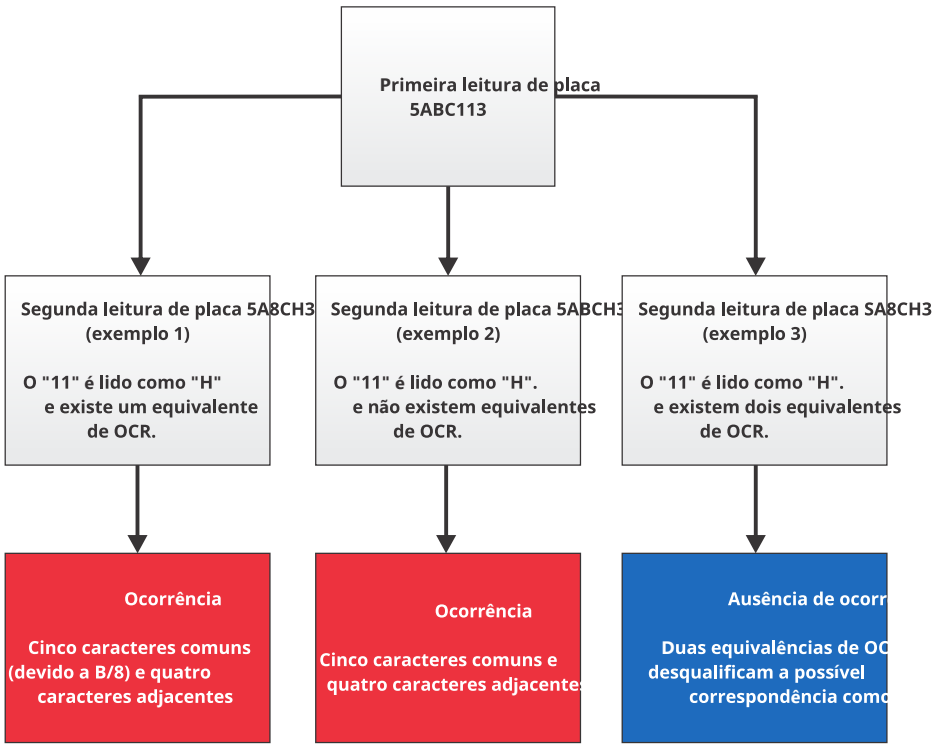
As seguintes configurações estão disponíveis ao configurar caracteres comuns e adjacentes:

- **Caracteres comuns necessários:** O número mínimo de caracteres que precisam ser comuns tanto para a primeira como para a segunda leituras de placa de veículo. Os caracteres também devem aparecer na mesma ordem na placa de veículo, mas não necessariamente em sequência.
- **Caracteres adjacentes necessários:** Comprimento mínimo da sequência de caracteres entre a primeira e a segunda leituras de placa de veículo.

  Na fiscalização de tempo extra, há uma margem de erro extra porque a equivalência de LPR está comparando uma leitura de placa com outra leitura de placa, não com uma lista de procurados ou lista de autorizações criada por uma pessoa.

Exemplo

Aqui está um exemplo com a equivalência de LPR configurada para procurar cinco caracteres comuns e quatro caracteres adjacentes (padrão). A equivalência de LPR também permite o caractere equivalente de OCR padrão, que pode contar como um caractere comum ou adjacente.



A leitura de placa 5ABC113 corresponde a 5A8CH3 (exemplo 1) e 5ABCH3 (exemplo 2) porque as seguintes condições são atendidas:

- **Equivalência de OCR:** Os equivalentes de OCR B e 8 são considerados o mesmo caractere e aplicam-se para a contagem de caracteres comuns e adjacentes.
- **Cinco caracteres comuns:** Ambas as leituras têm 5, A, B/8, C e 3 em comum, e todos eles aparecem na mesma ordem. O "3" não está em sequência, mas respeita a ordem.
- **Quatro caracteres adjacentes:** Ambas as leituras têm 5, A, B/8 e C em sequência.

A leitura de placa 5ABC113 *não* corresponde a SA8CH3 (exemplo 3) porque há dois equivalentes de OCR na segunda leitura (S/5 e B/8). Você permitiu apenas um equivalente de OCR.

O uso de caracteres comuns e adjacentes ajuda a reduzir a margem de erro envolvida quando a primeira e segunda leituras de placa de veículo são provenientes do Sharp.

Arquivo MatcherSettings.xml

O arquivo *MatcherSettings.xml* contém as configurações para as técnicas usadas pela equivalência de LPR: equivalência de OCR, número de diferenças de caractere e caracteres comuns e contíguos.

O arquivo está localizado no computador que hospeda a função Directory do Security Center, na pasta *C:\Program Files\Genetec Security Center 5.7*.

NOTA: Se você possui um sistema AutoVu™ móvel, uma cópia do mesmo arquivo está localizada no computador do veículo Genetec Patroller™. Você faz suas alterações na versão do arquivo no Security Center. O arquivo no computador do Genetec Patroller™ é substituído na próxima vez que o Genetec Patroller™ se conectar ao Security Center por conexão sem fio ou quando transferir manualmente as configurações do Genetec Patroller™ com uma unidade USB.

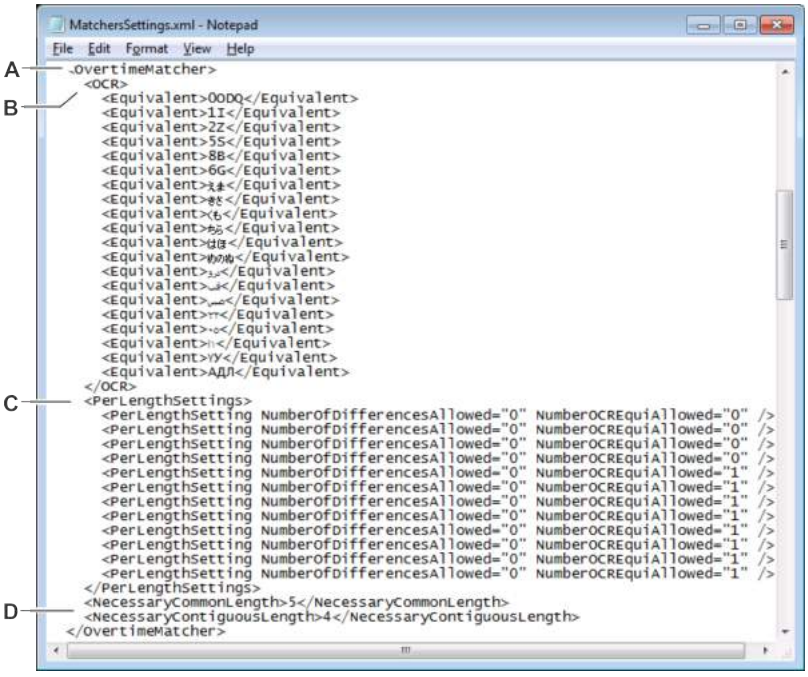
O arquivo *MatcherSettings.xml* é composto por tags `<Matcher>` que definem as configurações para cada tipo de cenário de correspondência:

- **<HotlistMatcher>:** Configurações para correspondência de leituras de placas com listas de procurados.
- **<OvertimeMatcher>:** Configurações para correspondência de leituras de placas com todas as outras leituras de placas no banco de dados do Genetec Patroller™.
- **<PermitMatcher>:** Configurações para correspondência de leituras de placas com listas de autorizações.
- **<MLPIMatcher>:** Configurações para reconciliar inventários no Security Desk.

A estrutura do arquivo *MatcherSettings.xml* permite que você tenha comportamentos diferentes para diferentes cenários de fiscalização. Por exemplo, para maximizar a taxa de precisão de leitura da placa em um cenário de fiscalização que inclua listas de autorizações *e* listas de procurados, você normalmente vai querer usar apenas a equivalência de OCR para a correspondência da lista de procurados, mas também permitir uma diferença no número de caracteres para que a correspondência de autorizações reduza a ocorrência de falsos positivos.

Exemplo de arquivo MatcherSettings.xml

Segue um exemplo do arquivo *MatcherSettings.xml*:



A: Configurações específicas da correspondência

Cada tipo de imposição (lista de procurados, autorização, horas extras e MLPI) tem suas configurações específicas listadas entre as marcas de abertura e fechamento `<Matcher>`.

Por exemplo, as configurações de correspondência de horas extras são listadas entre `<OvertimeMatcher>` e `</OvertimeMatcher>`.

B: Caracteres com equivalência OCR

Os caracteres com equivalência OCR padrão de cada tipo de imposição são listados entre `<OCR>` e `</OCR>`.

C: Configurações PerLength

Para cada correspondência, especifique o número de diferenças permitidas e o número de equivalentes OCR permitido para placas de veículo que tenham diferentes comprimentos de caracteres.

MELHOR PRÁTICA:

- Há 12 linhas de `PerLengthSetting`, cada uma contendo marcas `NumberOfDifferencesAllowed` e `NumberOCREquiAllowed`.
- Cada linha de `PerLengthSetting` corresponde a um comprimento de caracteres de placa de veículo. A linha que você edita depende do número de caracteres nas placas de veículos na sua região de patrulha.
- Ignore a primeira linha porque ela representa placas com zero caracteres. A segunda linha representa placas de veículos com um caractere, a terceira linha representa placas de veículos com dois caracteres e assim por diante, até um máximo de 11 caracteres de placas de veículos possíveis.
- Você pode editar mais de uma linha para aplicar configurações a placas de veículos com diferentes comprimentos de caracteres.

As configurações padrão são `PerLengthSettings`. Não são permitidas diferenças, e um equivalente OCR é permitido, para placas de veículos com 5 a 11 caracteres.

D: Configurações de caracteres comuns e adjacentes

Estas configurações somente se aplicam à imposição de estacionamento em horas extras.

- **<NecessaryCommonLength>:** Especifique o número mínimo de caracteres que precisam ser comuns para a primeira e a segunda placas de veículo lidas. Os caracteres também devem aparecer na mesma ordem na placa de veículo, mas não necessariamente em sequência.
- **<NecessaryContiguousLength>:** Comprimento mínimo da sequência de caracteres entre a primeira e a segunda placas de veículo lidas.

Boas práticas para definir configurações de equivalência de LPR

O modo como você configura a equivalência LPR depende do seu cenário de fiscalização. Em alguns sistemas AutoVu™, você quererá apenas uma correspondência exata. Em outros sistemas, você se beneficiará de ter um falso positivo em uma combinação potencial porque diminui as chances de perder um veículo de interesse.

Use as seguintes práticas recomendadas ao definir as configurações de equivalência LPR:

- **Correspondência exata:** A equivalência de LPR sempre procura uma correspondência exata, se possível, mas você pode configurá-la para permitir *apenas* correspondências exatas. Isso geralmente é usado quando você possui listas de procurados muito grandes (milhões de entradas). Ao limitar o número de correspondências possíveis, você alivia a carga de processamento no computador do Genetec Patroller™ e diminui a quantidade de falsos positivos que normalmente obteria de uma lista desse tamanho. Para permitir apenas correspondências exatas, ative o recurso *Simplematcher* no Genetec Patroller™ Config Toole desative a equivalência de OCR.
- **equivalência de OCR:** Por padrão, a equivalência LPR permite um caractere equivalente de OCR. Você pode permitir o máximo que quiser, mas geralmente não deve permitir mais do que dois, porque você terá muitos falsos positivos.
- **Número de diferenças permitidas:** Por padrão, a equivalência LPR não permite nenhum número de diferenças. O número que você permitir depende das placas da sua região. Quanto mais personagens em um prato, mais diferenças você pode permitir, mas geralmente você não deve permitir mais do que dois porque você terá muitos falsos positivos.
- **Caracteres comuns e adjacentes:** (Usado apenas para fiscalização de horas extras) Por padrão, a equivalência LPR procura por cinco caracteres comuns e quatro caracteres adjacentes para gerar um alerta de hora extra. O número que você especificar depende das placas da sua região. Quanto mais caracteres em uma placa, mais caracteres comuns e adjacentes que você pode permitir.

Tópicos relacionados

Definir configurações de equivalência de LPR na página 783

Definir configurações de equivalência de LPR

Para ajustar a forma como as placas de veículo capturadas pelo Sharp são correspondidas com placas de veículo em uma lista de procurados ou lista de autorizações, você deve configurar a lógica de equivalência de LPR.

Antes de iniciar

Leia as melhores práticas para definir configurações de equivalência de LPR.

IMPORTANTE: Teste seu sistema com as configurações padrão do equivalência de LPR. Se a taxa de precisão de leitura atender aos seus requisitos, **não** ajuste as configurações de equivalência de LPR.

O que você deve saber

Você define as configurações de equivalência de LPR no arquivo *MatcherSettings.xml* e aplica suas alterações ao Server Admin e ao console do Server Admin.

A equivalência de horas extras é usada como exemplo, mas os mesmos passos se aplicam a todas as equivalências no arquivo XML.

Para definir configurações de equivalência de LPR:

1. No computador que hospeda a função Directory do Security Center, abra o Windows Explorer e vá para *C:\Program Files\Genetec Security Center 5.7*.
2. Abra o *MatcherSettings.xml* no Bloco de Notas ou um editor de texto similar.
3. Adicione ou remova caracteres equivalentes de OCR da lista.

   Os caracteres equivalentes de OCR padrão são listados entre as tags <OCR> e </OCR>. Adicione novas linhas `<Equivalent>____</Equivalent>` ou exclua as linhas que não desejar.

4. Especifique o número de diferenças de caracteres que deseja permitir.

   Edite a linha `PerLengthSetting` que se aplica às placas em sua região. Por exemplo, as placas de Quebec normalmente têm seis ou sete caracteres, então edite o valor de `NumberOfDifferencesAllowed` na sexta e sétima linhas de `PerLengthSetting`.

   NOTA: Um valor "0" desativa a configuração.

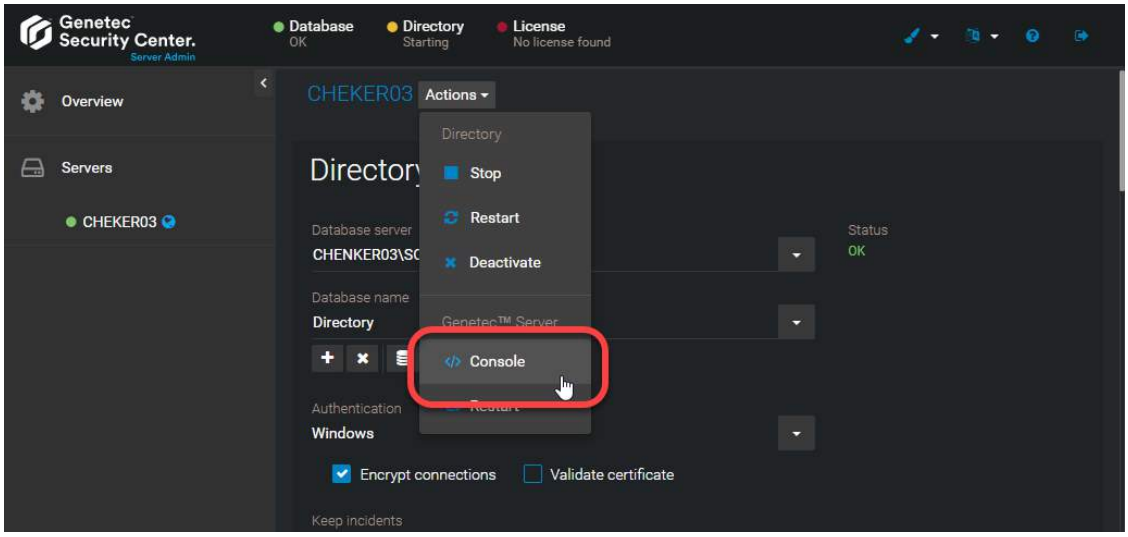
5. Especifique o número de caracteres equivalentes de OCR que você deseja permitir editando o valor `NumberOCREquiAllowed`. Isso aciona a equivalência de OCR.

   NOTA: Um valor "0" desativa a configuração.

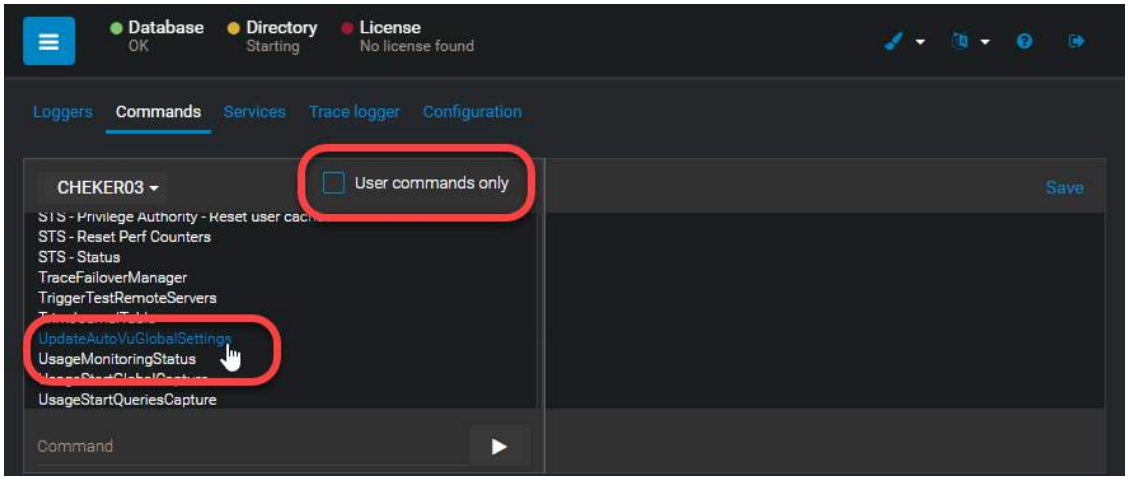
6. (Somente horas extras) Especifique o número de caracteres comuns e adjacentes.

   Para caracteres comuns, edite o valor `NecessaryCommonLength`. Para caracteres adjacentes, edite o valor `NecessaryContiguousLength`.

7. Salve e feche o editor de texto.
8. Aplique as configurações de equivalência de LPR ao Server Admin da seguinte maneira:
   a) A partir de um navegador da Web, abra o Server Admin digitando *http://<server>/genetec*.
   b) Na seção *Servidores* da página *Visão Geral*, selecione o servidor que hospeda a função Directory.
   c) Junto ao nome do servidor, clique em **Ações** > **Console**.

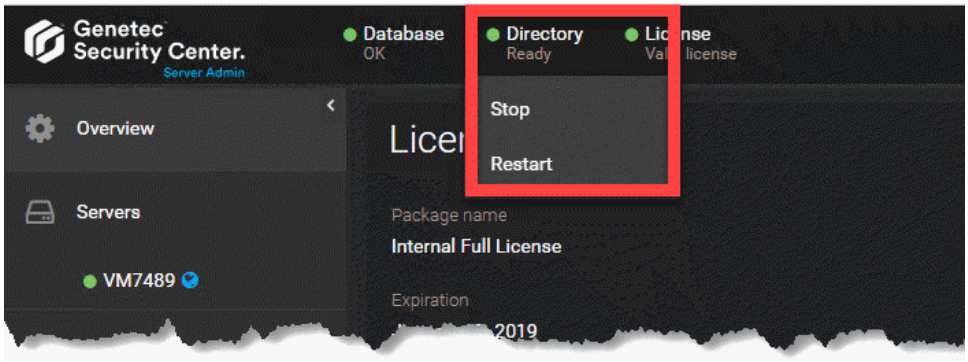


a) Clique na aba **Comandos**.
b) Desmarque a caixa de seleção **Somente comandos do usuário**.
c) Na lista de comandos, clique em **UpdateAutoVuGlobalSettings**.



d) Feche a Server Admin.

9 Reinicie a função Directory do Security Center da seguinte forma:
a) A partir de um navegador da Web, abra o Server Admin digitando *http://<server>/genetec*.
b) Clique em **Directory** e selecione **Reiniciar**.



c) Depois que o Directory tenha sido reiniciado, feche o Server Admin.

As definições de equivalência de LPR estão agora configuradas e aplicadas a todas as funções LPR Manager no seu sistema. As unidades Genetec Patroller™ serão atualizadas da próxima vez que se conectarem sem fio

ao Security Center ou quando você transferir manualmente configurações de Genetec Patroller™ usando uma chave USB.

Após terminar

Verifique se as suas funções LPR Manager foram atualizadas observando o arquivo *MatcherSettings.xml* nas respectivas pastas raiz (*C:\Genetec\AutoVu\RootFolder\ManualTransfer\General*). Você também poderá saber pelo campo *Data de modificação* do arquivo XML que ela foi atualizada.

Tópicos relacionados

Arquivo MatcherSettings.xml na página 780

Atualizar o SharpV a partir do Security Center

Se a sua câmera SharpV estiver conectada ao Security Center sem fio ou através de uma rede, você pode usar o serviço de atualização Security Center para enviar por push as atualizações para o SharpV.

O que você deve saber

As atualizações do SharpV são automaticamente instaladas após enviar por push as atualizações a partir do Security Center.

Para atualizar o SharpV usando o serviço de atualização:

1 (Somente na primeira atualização) Ative o serviço de atualização e especifique a porta de escuta no Security Center Config Tool:
   a) Faça logon no Security Center Config Tool.
   b) Na página *Início* do Security Center Config Tool, acesse **LPR** > **Funções e unidades**, selecione o LPR Manager que controla as unidades que pretende atualizar e clique em **Propriedades**.
   c) Ative o **Provedor de atualizações** e especifique a porta de escuta.

      Este número de porta deve corresponder à **Porta do provedor de atualizações** especificada na página *Extensões* no SharpV Portal.

   O Security Center cria a pasta *Updates* na *pasta raiz de LPR* do seu computador. Esta pasta está geralmente localizada em *C:\Genetec\AutoVu\RootFolder\Updates*.
2 Copie as atualizações do SharpV para a pasta *Upgrade*. Por exemplo, pasta *C:\Genetec\AutoVu\RootFolder2\Updates\SharpOS\Upgrade*:
   a) Na página *Início* do Security Center Config Tool, acesse **LPR** > **Configurações gerais** > **Atualizações** para exibir as unidades SharpV em seu sistema.
   b) Clique na aba **Unidades Genetec Patroller™ e SharpV**.
   c) Mova o cursor do mouse para a **Pasta de destino** do componente que pretende atualizar.

      Aparece uma dica de ferramenta com a localização da pasta de destino. Se você estiver no computador que hospeda a função LPR Manager, você pode clicar no ícone da **Pasta de destino** para abrir automaticamente a pasta.
   d) Copie a atualização para a **Pasta de destino**.

      Após copiar o arquivo compactado para a pasta, o nome do arquivo muda de *.zip* para *.processed*. Isto significa que o LPR Manager descompactou a atualização e está pronto para enviar a atualização para os componentes AutoVu™.
3 Envie por push as atualizações para componentes AutoVu™:
   a) Na página *Início* do Security Center Config Tool, acesse **LPR** > **Configurações gerais** > **Atualizações**.

      A aba Patrollers e unidades Sharp exibe as câmeras SharpV que são elegíveis para uma atualização.
   b) Clique em **Atualizar** para atualizar uma única câmera ou clique em **Atualizar tudo** para atualizar todas as câmeras elegíveis na lista.

      Quando o status muda de **Aguardando conexão...** para **Sincronizado**, significa que a câmera baixou a atualização com êxito.

      NOTA: O tempo que demora a transferir as atualizações depende da largura de banda da conexão e do tamanho da atualização.

   A atualização é automaticamente instalada no SharpV associado.

40

Listas de procurados

Esta seção inclui os seguintes tópicos:

- "Sobre listas de procurados" na página 788
- "Criar listas de procurados" na página 789
- "Selecionar quais listas de procurados e autorizações um veículo de patrulha monitora" na página 791
- "Instalar o plug-in Atualizador de Arquivos de Lista de Procurados e Autorizações" na página 792
- "Filtrar caracteres inválidos de listas de procurados e listas de autorização" na página 797
- "Adicionar configurações de privacidade a leituras e ocorrências" na página 798
- "Adicionar configurações de privacidade a listas de procurados" na página 799
- "Permitir que usuários editem listas de procurados e autorizações" na página 801
- "Recebendo notificações quando alertas da lista de procurados ocorrem" na página 802
- "Receber eventos de Correspondência e Não correspondência no Security Desk" na página 804
- "Listas de procurados curinga" na página 805
- "Ativar listas de procurados curinga" na página 806
- "Atributos padrão de lista de procurados e autorizações" na página 807
- "Configurando lista de procurados padrão e atributos de autorização" na página 808
- "Definir configurações avançadas de lista de procurados" na página 810
- "Configurar correspondência de leitura passada no LPR Manager" na página 811

Sobre listas de procurados

Uma lista de prioridades é uma lista de veículos procurados, na qual cada veículo é identificado por um número de placa, com o estado de emissão e com o motivo pelo qual o veículo é procurado (roubado, criminoso procurado, alerta âmbar, VIP, etc). As informações opcionais do veículo podem incluir o modelo, a cor e o número de identificação do veículo (VIN).

As listas de procurados são usadas tanto pelo AutoVu™ Genetec Patroller™ quanto pela função AutoVu™ LPR Manager para verificar placas de veículo capturadas pelas unidades de LPR para identificar veículos de interesse.

A entidade lista de procurados é um tipo de regra de alerta. Uma regra de alerta é um método usado pelo AutoVu™ para identificar veículos de interesse. Outros tipos de regras de alerta incluem *tempo extra*, *autorização* e *restrição de autorização*. Quando a leitura de uma placa corresponde uma regra de alerta, ela é chamada de alerta. Quando a leitura de uma placa corresponde a uma placa em uma lista de procurados, ela é chamada de alerta da lista de procurados.

Criar listas de procurados

Para usar uma lista de procurados no Security Center, você deve criar a lista de procurados, mapeá-la para seu arquivo de texto de origem e configurá-la para seu cenário de fiscalização.

Antes de iniciar

Crie o arquivo de texto de origem da lista de procurados (*.txt* ou *.csv*).

O que você deve saber

- As listas de procurados podem ser usadas com qualquer tipo de sistema AutoVu™ fixo ou móvel.
- O arquivo de texto de origem deve estar localizado em uma unidade acessível a partir do computador que hospeda o LPR Manager.

Para criar uma lista de procurados:

1 Na página inicial do Config Tool, clique em **LPR** > **Listas de procurados** e, em seguida, clique em **Lista de procurados** ( ).

O assistente **Criar uma lista de procurados** será aberto.

2 Na aba **Informações básicas**, no campo **Nome da entidade**, digite um nome para a lista de procurados e clique em **Próximo**.

NOTA: A **Descrição da entidade** é opcional.

3 Defina a prioridade da lista de procurados usando o controle deslizante Prioridade.

Zero (0) é a configuração de mais alta prioridade e 100 é a mais baixa. Se uma leitura de placa de veículo corresponder a mais de uma lista de procurados, a lista de procurados com a maior prioridade é exibida em primeiro lugar entre as listas de procurados encontradas.

4 Digite o **Caminho da lista de procurados** no computador onde o arquivo de texto de origem da lista de procurados se encontra.

Se você começar a digitar um caminho para uma unidade de rede, talvez seja necessário inserir um **Nome de usuário** e uma **Senha** para acessar a unidade de rede. Os campos aparecerão se este for o caso.

5 Se os campos de atributos no arquivo de texto de origem variarem em comprimento, coloque a opção **Usar delimitadores** em **Ligado** e digite o tipo de caractere (delimitador) usado para separar cada campo.

Por padrão, **Usar delimitadores** está definido como **Ligado** e o delimitador especificado é **ponto e vírgula** (;). Se o seu arquivo de texto de origem for feito de campos de comprimento fixo, defina **Usar delimitadores** para **Desligado**. O Security Center suporta os seguintes delimitadores:

- Dois pontos (:)
- Vírgula (,)
- Ponto e vírgula (;)
- Tab (digitar “Tab”)

IMPORTANTE: Se o seu arquivo de lista de origem usar Tab como delimitador, use apenas um espaço de Tab. Não use mais do que um espaço de Tab para alinhar as colunas em seu arquivo, ou o Security Center pode não ser capaz de analisar a lista de procurados.

6 (Opcional) Se você não desejar que os usuários tenham permissão para editar esta lista de procurados no Security Desk, desative **Visível no editor**,

NOTA: Para editar uma lista de procurados no Security Desk, os usuários devem ter o privilégio *Editor de lista de prioridades e autorização*.

7 Configure os **Atributos** da lista de procurados e clique em **Próximo**. Consulte Configurando lista de procurados padrão e atributos de autorização na página 808.

8 Na página **Atribuição de LPR Manager**, escolha uma das seguintes opções e clique em **Próximo**.

- **Todos os LPR Managers**. Todos os LPR Managers e todas as entidades configuradas para herdar as respectivas listas de procurados sincronizarão a nova lista de procurados.

  NOTA: LPR Managers futuros não sincronizarão automaticamente a nova lista de procurados.

- **LPR Managers específicos**. Somente os LPR Managers selecionados e as entidades que herdam as listas de procurados deles sincronizarão a nova lista de procurados.

  NOTA: As entidades criadas no futuro que forem configuradas para herdar listas de procurados de um dos LPR Managers selecionados também sincronizarão a lista de procurados.

- **Atribuir depois**. Nenhum LPR Manager e nenhuma entidade associada existente irão sincronizar a nova lista de procurados. Para obter mais informações sobre como atribuir uma listas de procurados a um LPR Manager mais tarde, consulte Selecionar quais listas de procurados e autorizações um veículo de patrulha monitora na página 791.

9 Na página **Atribuição específica de unidade**, selecione os veículos de patrulha e/ou Sharps específicos que sincronizarão a nova lista de procurados e clique em **Próximo**.

10 (Opcional) Se houver campos personalizados, insira os valores apropriados na página **Campos personalizados** e clique em **Próximo**.

NOTA: A página **Campos personalizados** não aparece se não houver campos personalizados em sua lista de procurados.

11 Na janela **Resumo de criação**, verifique se as informações da sua lista de procurados estão corretas e clique em **Próximo**.

12 Na janela **Resultado da criação de entidade**, você receberá uma notificação quanto à sua operação ter sido bem-sucedida ou não.

13 (Opcional) Escolha uma das seguintes opções:

- **Editar esta lista de procurados**. Abre o **Editor de lista de prioridades e autorização** para que você possa editar a lista de procurados.

  NOTA: Para editar uma lista de procurados, você deve ter o privilégio de *Editor de lista de prioridades e autorização*.

- **Criar uma lista de procurados baseada nesta lista de procurados:** Crie uma nova lista de procurados que use as mesmas configurações que a lista de procurados que você acabou de criar. Somente é necessário especificar o **Nome da entidade**, a **Descrição da entidade** e o **Caminho da lista de procurados**.

14 Clique em **Fechar**.

A entidade de lista de procurados é configurada e ativada no Security Center.

Selecionar quais listas de procurados e autorizações um veículo de patrulha monitora

Para que listas de procurados e listas de autorização sejam monitoradas por veículos de patrulha, elas devem ser ativadas e gerenciadas por pelo menos um LPR Manager.

O que você deve saber

- O LPR Manager envia as listas de procurados e listas de autorização ativas para os veículos de patrulha que gerencia.
- O LPR Manager também compara as listas de procurados com as leituras coletadas de câmeras Sharp para produzir ocorrências.
- Quando você cria uma nova lista de procurados ou de autorização, elas ficam ativas para todos os LPR Managers por padrão.

Somente os veículos de patrulha configurados para fiscalização de estacionamento exigem autorizações.

NOTA: Você também pode associar autorizações a veículos de patrulha individuais e listas de procurados a veículos de patrulha e unidades Sharp individuais.

Para selecionar quais listas de procurados e listas de autorização monitorar:

1 Na página inicial do Config Tool, clique em **Sistema** > **Funções**e, em seguida, clique em LPR Manager que deseja configurar.
2 Clique na guia **Propriedades**.
3 Em **Associação de arquivo**, selecione as listas de procurados e autorizações que você deseja que o LPR Manager gerencie.
4 Clique em **Aplicar**.

Instalar o plug-in Atualizador de Arquivos de Lista de Procurados e Autorizações

Em sistemas AutoVu™ Managed Services (AMS) que sejam hospedados na plataforma na nuvem Azure da Microsoft, instalar o plug-in *Atualizador de Arquivos de Lista de Procurados e Autorizações* permite enviar listas de procurados e autorizações atualizadas para a nuvem, de onde poderão ser baixadas em veículos de patrulha.

O que você deve saber

O AMS permite implantar rapidamente um sistema de reconhecimento de placas de veículos (LPR) ao reduzir a necessidade de suporte e infraestruturas informáticas no local. Com o AMS, o seu sistema de ALPR é hospedado na nuvem e é configurado e mantido por especialistas da Genetec Inc..

Para instalar e configurar o plug-in Atualizador de Arquivos de Lista de Procurados e Autorizações:

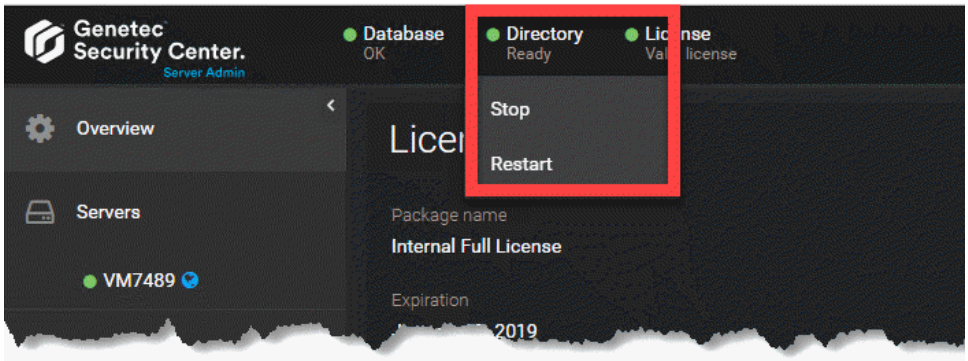
1 Baixe o pacote Atualizador de Lista de Procurados e Autorizações disponível em http://downloadcenter.genetec.com/products/AutoVu/Tools/HotlistPermitUpdater.zip.

2 Para instalar o plug-in, abra o pacote Atualizador de Lista de Procurados e Autorizações, clique duas vezes no arquivo MSI *Genetec.CS.HotListPermitFileUpdater.Setup* e siga as instruções no instalador.

3 Reinicie a função Directory do Security Center da seguinte forma:

a) A partir de um navegador da Web, abra o Server Admin digitando *http://<server>/genetec*.

b) Clique em **Directory** e selecione **Reiniciar**.



c) Depois que o Directory tenha sido reiniciado, feche o Server Admin.

4 Crie os eventos personalizados necessários.

a) No Config Tool, abra a tarefa **Sistema**, clique na visualização **Configurações gerais** e, em seguida, clique na página **Eventos**.

b) Clique em **Adicionar um item** ( ).

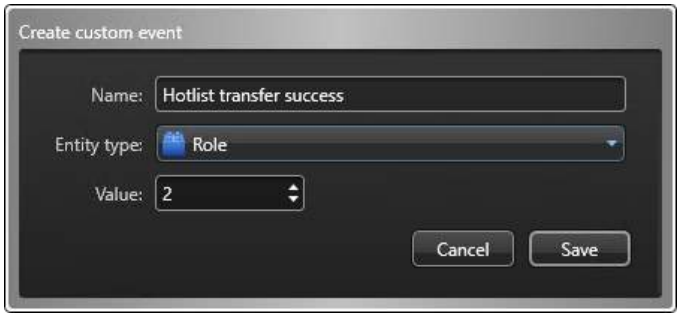
c) Na caixa de diálogo **Criar evento personalizado**, digite o **Nome** *Êxito na transferência de lista de procurados*.

d) Na lista suspensa **Tipo de entidade**, selecione **Função**.

e) No campo **Valor**, digite um número exclusivo para diferenciar este evento personalizado de outros eventos personalizados.

NOTA: Esses valores não estão relacionados à IDs lógicas das entidades.

f) Clique em **Salvar** > **Aplicar**.



g) Seguindo estas etapas, crie dois eventos adicionais:
- *Falha na transferência de lista de procurados*
- *Disparador de início de transferência de lista de procurados*

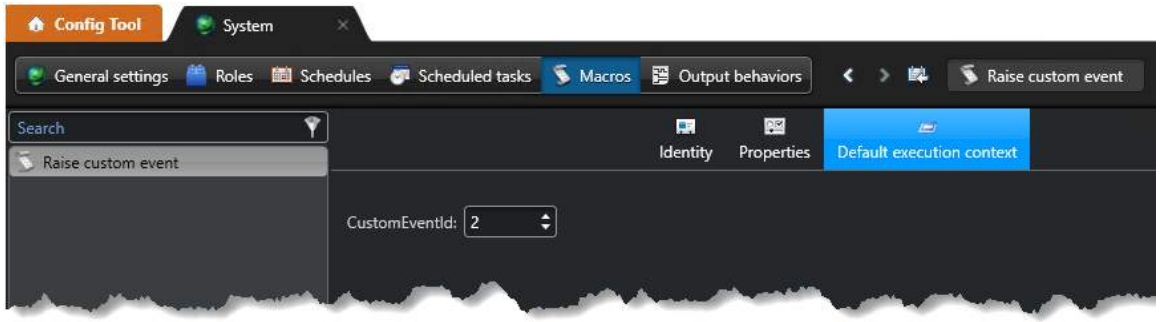
5 Instale a macro *Acionar evento personalizado* para que o Security Center possa acionar os eventos personalizados.
a) Na página inicial de Config Tool, abra a tarefa *Sistema* e clique na visualização **Macros**.
b) Clique em **Macro** (+) e nomeie a nova macro como *Acionar evento personalizado*.
c) Clique na guia **Propriedades.**
d) Clique em **Importar de arquivo**, navegue até ao arquivo TXT *RaiseCustomEventMacro* que está incluído no pacote e clique em **Abrir**.

O arquivo TXT contém o seguinte script:

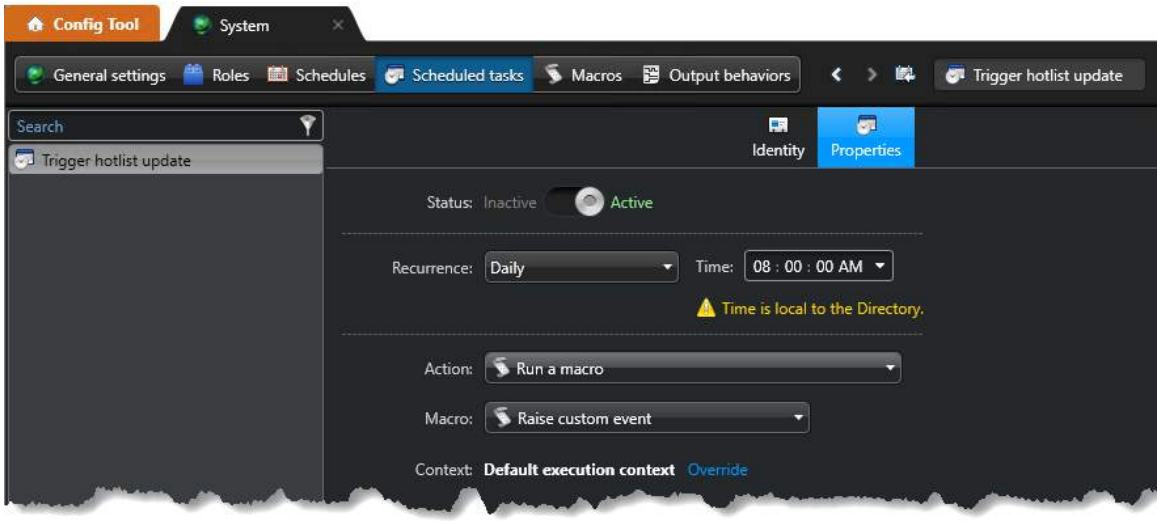
```
// ============================================================================
// Copyright (C) 2013 by Genetec, Inc.
// All rights reserved.
// May be used only in accordance with a valid Source Code License Agreement.
// ============================================================================

using Genetec.Sdk;
using Genetec.Sdk.Entities;
using Genetec.Sdk.Entities.CustomEvents;
using Genetec.Sdk.Queries;
using Genetec.Sdk.Scripting;
using Genetec.Sdk.Diagnostics.Logging.Core;
using System;
using System.Collections.Generic;
using System.Data;
using System.IO.Ports;
using System.Linq;
using System.Text;
using System.Threading;

namespace RaiseCustomEvent
{
    public class RaiseCustomEvent : UserMacro
    {
        public int CustomEventId { get; set; }

        public RaiseCustomEvent()
        {
            CustomEventId = 0;
        }
        public override void Execute()
        {
            try
            {
                if (CustomEventId > 0)
                {
                    Sdk.ActionManager.RaiseCustomEvent(new
 CustomEventId(CustomEventId),
                        SdkGuids.SystemConfiguration);
                }
            }
            catch (Exception)
```

```
            {
            }
        }

        protected override void CleanUp()
        {
        }
    }
}
```

a) Clique em **Aplicar** para salvar a macro.
b) Clique na aba **Contexto de execução padrão**.
c) No campo *ID de evento personalizado*, digite o **Valor** configurado para o evento *Disparador de início de transferência de lista de procurados*.
d) Clique em **Aplicar**.



6 Crie uma tarefa agendada para iniciar a transferência de arquivos.
a) Na página inicial do Config Tool, abra a tarefa *Sistema* e clique na visualização **Tarefas agendadas**.
b) Clique em **Tarefa agendada** ( ).
Uma nova entidade de tarefa agendada é adicionada na lista de entidades.
c) Nomeie a tarefa como *Acionar atualização de lista de procurados*.
d) Clique na aba **Propriedades** e altere a opção **Status** para **Ativo**.
e) Defina a **Recorrência** da tarefa, por exemplo, diariamente às 8:00.
f) Na lista **Ações**, selecione *Executar uma macro*.
g) Na lista **Macro**, selecione a macro *Acionar evento personalizado* criada.
h) Clique em **Aplicar**.



7 Instale a macro *Atualizador de arquivos de lista de procurados e autorizações*.
a) Na página inicial do Config Tool, abra a tarefa *Plug-ins*.
b) Clique em **Adicionar uma entidade** ( ) e selecione **Plug-in**.
c) No assistente *Criar uma função*, instale o plug-in *Atualizador de Arquivos de Lista de Procurados e Autorizações*.

d) O Atualizador de Arquivos de Lista de Procurados e Autorizações é adicionado à lista de plug-ins. Selecione-o e clique na aba **Propriedades**.
e) Configure o plug-in para usar o método de transferência HTTP, FTP ou SFTP.

HTTP ou FTP:

- Digite a URL remota do local onde se encontra o arquivo a ser transferido. Digite as credenciais se necessário. Se a origem não estiver protegida por um nome de usuário e senha, deixe os campos em branco.

SFTP:

- **Host:** Digite o host usando o seguinte formato:
  - `sftp://(nome do host ou IP):(porta)`
  - `sftp://(nome do host ou IP)` Se não for especificada uma porta, a porta padrão 22 é usada.
  - `(nome do host ou IP)` Se não for especificado um protocolo, o nome do host usa SFTP.
- **Caminho do arquivo:** Digite o caminho do arquivo de lista de procurados ou autorizações.

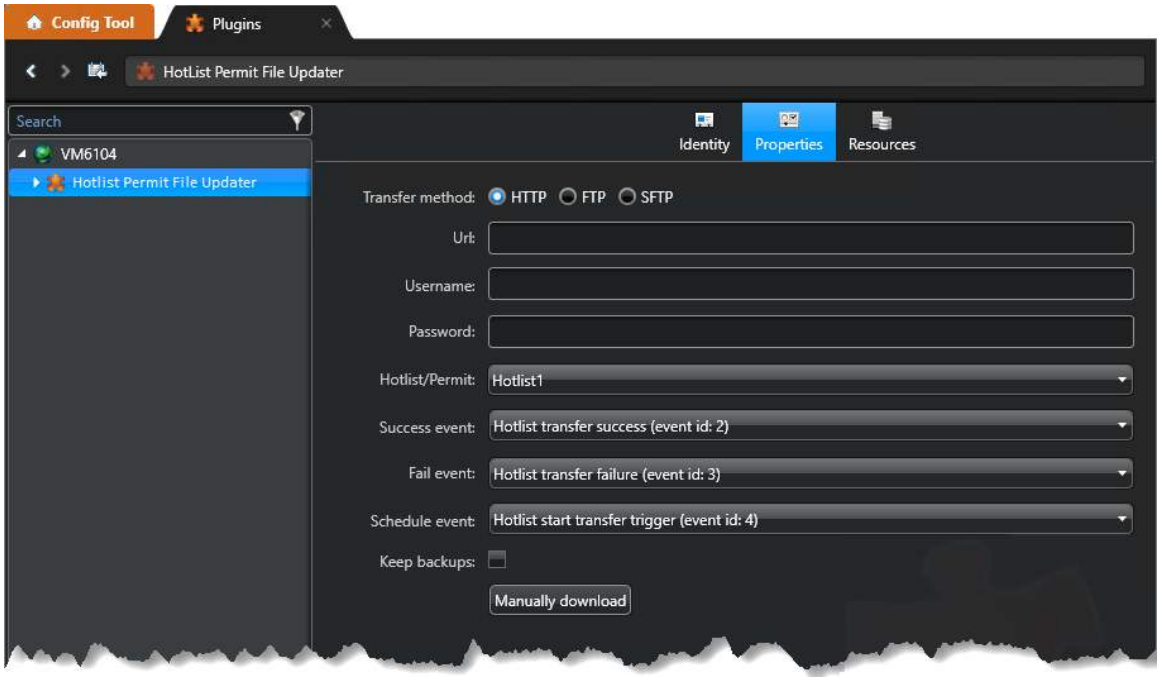
  NOTA: O caminho do arquivo é relativo ao diretório principal do usuário conectado no servidor SFTP.
- **Modo de conexão:** Selecione o modo de conexão de acordo com a configuração do local SFTP e digite o **Nome de usuário**, **Senha** e **Caminho do certificado** em função da sua seleção.

  NOTA:
  - O certificado deve estar localizado no servidor em que o plug-in está sendo executado e não no computador em que o Config Tool é usado.
  - O caminho deve também refletir a localização do arquivo no servidor.
  - O arquivo de certificado deve conter uma chave privada em um formato OpenSSH.
  - Chaves SSH-2 são compatíveis. As chaves SSH-1 são inseguras e não são compatíveis com o formato OpesSSH.

f) Na lista **Lista de procurados/Autorizações**, selecione a lista de procurados ou autorizações que deseja baixar para o veículo de patrulha.
g) Na lista **Evento de êxito**, selecione o evento *Êxito na transferência de lista de procurados* criado.
h) Na lista **Evento de falha**, selecione o evento *Falha na transferência de lista de procurados* criado.
i) Na lista **Evento de agenda**, selecione o *Disparador de início de transferência de lista de procurados* criado.
j) Se você selecionar **Manter backups**, o sistema cria um backup do arquivo de lista de procurados ou atualizações atual antes de baixar o novo. O nome de arquivo usa o nome original + a data e hora atuais + a extensão .bak, por exemplo, *hotlist2.tbl hotlist2.tbl 11-22-2017 11h10m55.bak*.

   NOTA: Para acionar a transferência imediatamente, clique em **Baixar manualmente**.

k) Clique em **Aplicar**.


Config Tool
Plugins
HotList Permit File Updater
Search
VM6104
Hotlist Permit File Updater
Identity
Properties
Resources
Transfer method:
HTTP
FTP
SFTP
Url:
Username:
Password:
Hotlist/Permit:
Hotlist1
Success event:
Hotlist transfer success (event id: 2)
Fail event:
Hotlist transfer failure (event id: 3)
Schedule event:
Hotlist start transfer trigger (event id: 4)
Keep backups:
Manually download

Filtrar caracteres inválidos de listas de procurados e listas de autorização

Quando uma lista de procurados ou de autorização é criada ou modificada, você pode especificar o conjunto de caracteres que se aplica às placas de veículo da lista com base em um idioma selecionado e o que o LPR Manager faz se detectar uma lista com caracteres inválidos (caracteres não alfanuméricos).

O que você deve saber

Para ver informações detalhadas sobre quantas entradas inválidas foram excluídas ou modificadas, você também pode salvar os registros do processo de filtragem.

Para filtrar placas de veículo ao modificar listas de procurados e listas de autorização:

1 Na página inicial do Config Tool, clique em **Sistema** > **Funções** e selecione o LPR Manager que deseja configurar.

2 Clique na guia **Propriedades.**

3 Em **Filtragem de placas de veículo**, selecione os tipos de caracteres a filtrar na lista suspensa **Conjunto de caracteres** (latino, árabe ou japonês).

4 Na seção **Número de placa de veículo inválido**, selecione uma das seguintes opções para especificar como o LPR Manager lida com registros inválidos:

- **Modificar registro:** Exclui quaisquer caracteres não alfanuméricos do número da placa de veículo. Por exemplo, o número de placa "ABC#%3" torna-se "ABC3".
- **Remover registro:** Exclui toda a entrada que contém caracteres inválidos da lista.

5 Para registrar o processo de filtragem, selecione a opção **Registar filtragem**.

Os registros de filtragem de placas de veículo são salvos na pasta raiz do AutoVu™: *C:\Genetec\AutoVu\RootFolder*.

6 Clique em **Aplicar**.

Adicionar configurações de privacidade a leituras e ocorrências

Você pode configurar o Genetec Patroller™ para obscurecer os números das placas ou para excluir as imagens de placa, contexto ou de roda das leituras e ocorrências que são recebidas no Security Center, de modo que as informações não sejam armazenadas no banco de dados do LPR Manager.

O que você deve saber

Obscurecer números de placas ou excluir dados de leituras ou alertas permite que você cumpra as leis de privacidade em sua região.

Se você precisar enviar um e-mail com dados de LPR para um destinatário específico, então você poderá ignorar as configurações de privacidade para listas de procurados individuais.

Para adicionar configurações de privacidade a leituras e alertas:

1 Na página inicial do Config Tool, clique em **LPR** > **Configurações gerais** > **Aplicativos**.

2 Em **Privacidade**, coloque em **Ligado** os tipos de dados que deseja oculta de leituras e ocorrências:

- **Imagens de placa de licença, contexto ou volante:** As imagens não são enviadas para o Security Center nem incluídas em dados descarregados.
- **Placa de licença:** Substitui a sequência de texto do número da placa por asteriscos (*) quando enviado ao Security Center ou nos dados descarregados.

3 Clique em **Aplicar**.

Adicionar configurações de privacidade a listas de procurados

Para obscurecer os números de placas de veículo, ou excluir imagens de placa, contexto ou roda das leituras e ocorrências recebidas no Security Center de uma lista de procurados específica, você pode configurar a lista de procurados como privada.

Antes de iniciar

Você deve obter um arquivo DLL especial da Genetec Inc.. Para mais informações, entre em contacto com o seu representante da Genetec Inc..

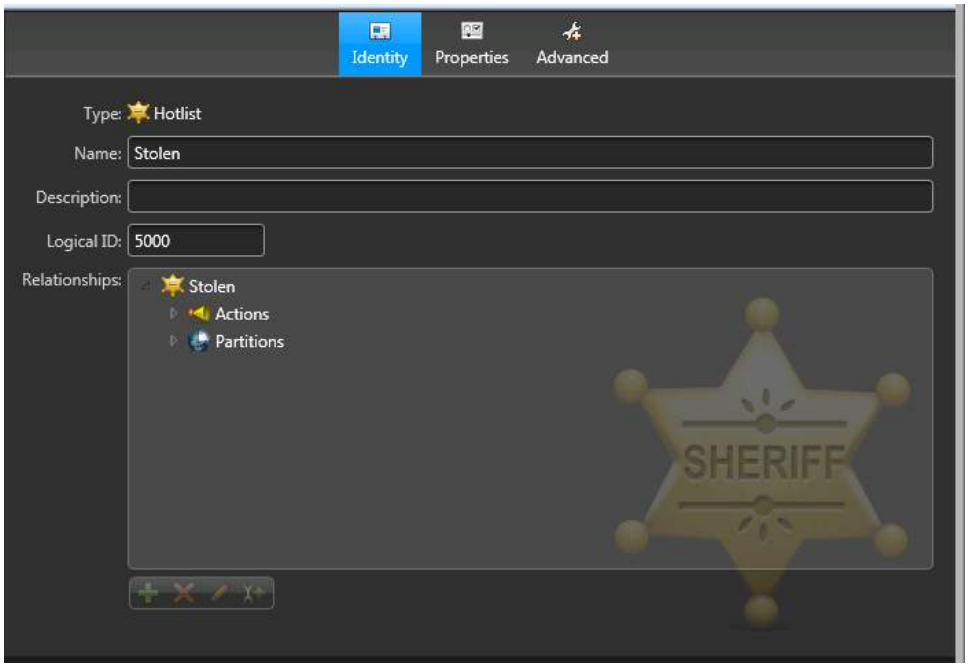
O que você deve saber

Se você adicionar configurações de privacidade a uma lista de procurados, o Security Center mantém os dados de LPR (por exemplo, números de placa, coordenadas GPS, data/hora e assim por diante), mas desassocia esses dados da lista de procurados que gerou o alerta. Por exemplo, se o Genetec Patroller™ gerar uma ocorrência de uma lista de procurados chamada "StateWideFelons", você pode manter todos os dados de LPR dessa ocorrência, mas você não poderá ver se a placa de veículo correspondida estava na lista "StateWideFelons".

As configurações de privacidade de listas de procurados específicas têm precedência sobre as configurações de privacidade globais configuradas no nível do LPR Manager. No entanto, é recomendável desligar todas as configurações de privacidade no nível do LPR Manager para evitar conflitos.

Para adicionar configurações de privacidade a leituras e alertas:

1. Copie o arquivo DLL que você recebeu da Genetec Inc. para a pasta raiz do Security Center (por exemplo, *C:\Program Files\Genetec Security Center 5.7*).
2. Reinicie a função Directory a partir do Server Admin, da seguinte forma:
   a) Abra o Internet Explorer.
   b) Na barra de endereços, digite *http://server IP address:port/Genetec* e pressione **Enter**.
   c) Faça logon no Server Admin.
   d) Em **Status do Directory**, clique em **Reiniciar**.
3. Na página inicial do Config Tool, clique em **LPR** > **Configurações gerais** > **Aplicativos**.
4. Em **Privacidade**, coloque em **Desligado** todas as configurações.
5. Clique em **Aplicar**.
6. Na página inicial, clique em **LPR** > **Listas de procurados**.
7. Selecione a lista de procurados que deseja tornar privada e clique na aba **Identidade**.



8 No campo **ID lógico**, digite o valor *5000*.

Isso marca a lista de procurados e informa o Security Center para tornar os dados de LPR privados.

9 Clique em **Aplicar**.

Após terminar

Repita para quantas listas de procurados quiser.

Permitir que usuários editem listas de procurados e autorizações

Quando você está configurando propriedades de uma lista de procurados ou autorizações, você pode selecionar se os usuários podem editar a lista usando a tarefa *Editor de lista de procurados e autorizações* no Security Desk.

O que você deve saber

Para editar uma lista de procurados ou autorizações no Security Desk, os usuários devem ter o privilégio *Editor de lista de procurados e autorizações*.

IMPORTANTE: Por favor, note o seguinte sobre o Editor de lista de procurados e permissões:

- Apenas as primeiras 100.000 linhas de uma lista são carregadas no Editor de listas de procurados e permissões.
- Se ocorrer um erro enquanto a lista de procurados está sendo carregada, o processo de carregamento é cancelado e uma mensagem de erro é exibida. No entanto, você não perderá nenhum dos dados carregados antes do erro, e você ainda pode editar os dados carregados no editor.

Para permitir que usuários editem listas de procurados e autorizações:

1 Na página inicial do Config Tool, execute uma das seguintes opções:
   - Clique em **LPR** > **Autorizações** e selecione a autorização a configurar.
   - Clique em **LPR** > **Listas de procurados** e selecione a lista a configurar.
2 Clique na guia **Propriedades.**
3 Coloque a opção **Visível no editor** em **Ligado** e clique em **Aplicar**.

Recebendo notificações quando alertas da lista de procurados ocorrem

Você pode configurar o Security Center para enviar uma notificação por e-mail quando ocorrem ocorrências da lista de procurados.

Antes de iniciar

Para garantir que a notificação de e-mail seja enviada, faça o seguinte:

- Configure o servidor de e-mail na página Server Admin - Visão geral.
- Certifique-se de que a opção **Notificação por e-mail** esteja em **Ligado** no LPR Manager - aba Propriedades.

O que você deve saber

Você pode configurar o Security Center para enviar uma notificação por e-mail quando ocorrer um dos seguintes:

- Quando qualquer placa de licença em uma lista de procurados gera um alerta.
- Quando qualquer placa de licença individual em uma lista de procurados gera um alerta. Você pode especificar um endereço de e-mail diferente para quantas placas individuais em uma lista de procurados quiser.

O e-mail contém as informações da ocorrência (número da placa correspondente, nome do Genetec Patroller™, usuário, nome da lista de procurados e prioridade) no corpo da mensagem e anexos de imagem opcionais.

Para receber notificações quando um alertas da lista de procurados ocorre:

1 Na página inicial do Config Tool, clique em **LPR** > **Listas de procurados**.
2 Selecione a lista de procurados que deseja configurar e clique na aba **Avançado**.
3 No campo **Endereços de e-mail**, especifique os endereços de e-mail que deseja notificar.

NOTA: Se você estiver inserindo mais de um endereço de e-mail, separe-os com uma vírgula, um ponto e vírgula ou um espaço.

4 Clique em **Aplicar**.

Quando qualquer placa de licença na lista de procurados selecionado gera um alerta, um e-mail de notificação é enviado para o endereço que você especificou.

Para receber notificações quando uma placa de licença gera um alerta:

1 Adicione um atributo de e-mail para a lista de procurados da seguinte maneira:
   a) Na página inicial do Config Tool, clique em **LPR** > **Listas de procurados**.
   b) Selecione a lista de procurados que deseja configurar e clique na aba **Propriedades**.
   c) Em **Atributos**, adicione um novo atributo relacionado ao e-mail (por exemplo, *E-mail*) para que o Security Center saiba que deve procurar endereços de e-mail no arquivo de origem da lista de procurados.
   d) Clique em **Aplicar**.

   O Security Center agora procurará endereços de e-mail no arquivo de origem da lista de procurados.
2 Ligue a **Notificação por e-mail** e defina as configurações relacionadas como segue:
   a) Na página inicial do Config Tool, clique em **Sistema** > **Funções**.
   b) Selecione o LPR Manager que deseja configurar, clique na aba **Propriedades** e clique em **Notificação por e-mail**.

c) No campo **Nome de atributo de e-mail**, digite o nome o mesmo nome de atributo que você criou na primeira etapa.
d) (Opcional) Em **Anexos do e-mail**, especifique quais informações deseja que o e-mail contenha.

   Por exemplo, você pode querer enviar apenas a sequência de texto da placa sem imagens para manter o tamanho do arquivo do e-mail pequeno.

e) (Opcional) No campo **Registrar e-mails em**, selecione onde armazenar os registros de notificação por e-mail.

   Os registros serão salvos na pasta raiz do AutoVu™: *C:\Genetec\AutoVu\RootFolder* e ajudarão a acompanhar quem recebeu notificações por e-mail.

f) Clique em **Aplicar**.

   O LPR Manager agora sabe que algumas listas de procurados contêm endereços de e-mail para entradas individuais de placa de licença.

3 Adicione endereços de e-mail no arquivo de origem da lista de procurados.

NOTA: Como você adicionou o atributo *E-mail* à entidade de lista de procurados, agora você pode usar o *Editor de lista de procurados e autorização* para adicionar endereços de e-mail. Você também pode adicioná-los diretamente ao arquivo de origem, se preferir.

a) Na página inicial do Config Tool, clique no **Editor de lista de procurados e autorização**.

   NOTA: A opção **Visível no editor** deve estar ligada para editar a lista de procurados.

b) Selecione a lista de procurados que deseja configurar e, em seguida, clique em **Carregar**.
c) Adicione endereços de e-mail a placas de licença conforme necessário.
d) Clique em **Salvar**.

Se uma placa com um endereço de e-mail gerar uma ocorrência, um e-mail será enviado para o destinatário especificado.

Tópicos relacionados

Server Admin - Página de visão geral na página 101
Permitir que usuários editem listas de procurados e autorizações na página 801

Receber eventos de *Correspondência* e *Não correspondência* no Security Desk

Para receber eventos de *Correspondência* e *Não correspondência* de placas de veículo no Security Desk, você precisa ativar a correspondência de lista de procurados para que as unidades Sharp possam corresponder as placas de veículo em listas de procurados e listas de autorizações ativas.

Antes de iniciar

A lista de procurados ou lista de autorizações deve estar ativa e ser gerenciada por um LPR Manager para que os eventos sejam monitorados.

O que você deve saber

Quando a correspondência de lista de procurados está ativada, você pode configurar eventos causa-efeito no Security Desk, com base em eventos de *Correspondência* (a placa de licença lida pelo Sharp estava em uma lista de procurados) e de *Não Correspondência* (a placa de licença lida pelo Sharp não foi encontrada em uma lista de procurados específica).

Tipicamente, eventos de *Não Correspondência* são usados em cenários de controle de acesso. Por exemplo, você pode associar uma lista de procurados a uma unidade Sharp específica que está monitorando o acesso a um estacionamento ou local similar. Nesse cenário, um evento causa-efeito do Security Center para uma *Ocorrência de placa de veículo* concede acesso ao veículo (abre um portão, levanta uma barreira e assim por diante), e um evento causa-efeito para uma *Não Correspondência* pode disparar um alarme ou envie um e-mail para o pessoal de segurança.

Para receber eventos de *Correspondência* **e** *Não correspondência* **no Security Desk:**

1. Na página inicial do Config Tool, clique em **Sistema** > **Funções**.
2. Selecione o LPR Manager que deseja configurar e, em seguida, clique na aba **Propriedades**.
3. Coloque a opção **Correspondência** em **Ligada**.
4. (Opcional) Para gerar eventos de "não correspondência" quando uma placa de veículo é lida por um Sharp e não faz parte de uma lista de procurados ou da lista de autorizações, coloque a opção **Gerar eventos de "Não correspondência"** em **Ligado**.
5. Clique em **Aplicar**.

Listas de procurados curinga

As listas de procurados curingas contêm entradas com apenas números de placas de licença parciais. Eles podem ser usados em situações em que testemunhas não viram ou não conseguem lembrar do número completo da placa de licença. Isso permite que o agente potencialmente intercepte veículos procurados que talvez não teriam sido detectados usando listas de procurados padrão.

Uma lista de procurados curinga inclui entradas que tenham um ou dois asteriscos (*****) no campo do número da placa de licença. Os asteriscos são os curingas que você usa quando você não conhece o caractere. Somente o campo do número da placa aceita caracteres curinga. Se o asterisco for encontrado em qualquer outro campo (por exemplo, estado ou província), ele é considerado como um caractere normal.

Observe o seguinte sobre listas de procurados curinga:

- Se você ativar curingas em uma lista de procurados, o Genetec Patroller™ ignora todas as entradas da lista de procurados que não possuem um curinga ou que tenham mais de dois caracteres curinga.
- É o número de caracteres curinga no campo *PlateNumber*, não a localização do caractere curinga, que determina quantos caracteres sem correspondência são permitidos antes que uma correspondência possa ocorrer.
- A posição dos curingas não pode ser aplicada porque, normalmente, quando as testemunhas denunciam um número de placa parcial, elas não se lembram da posição dos caracteres que perderam. A sequência dos caracteres normais no campo *PlateNumber* é respeitada, de modo que os três padrões "S*K3*7", "**SK37" e "SK37**" são equivalentes.

  Se uma lista de procurados contém a entrada da placa de licença S*K3*7:

  - As leituras de placa **N**SK3**5**7 e **A**S**D**K37 *irão* gerar uma ocorrência porque ambas as leituras não possuem mais de dois caracteres incompatíveis (em negrito) e a sequência "SK37" é respeitada.
  - A leitura de placa SUKA357 *não irá* gerar uma ocorrência porque ela contém três caracteres incompatíveis (em vermelho).
  - A leitura de placa SKU573 não gerará um alerta porque a sequência de caracteres SK37 não é encontrada na leitura.

MELHOR PRÁTICA:

- Não use mais do que uma lista de procurados com caracteres curinga por Genetec Patroller™.
- Use apenas uma lista de procurados com caracteres curinga por LPR Manager.
- Limite o número de entradas de caracteres curinga em uma lista de procurados para 100 placas.

Ativar listas de procurados curinga

Para ler placas de licença parciais, você deve configurar uma lista de procurados como lista de procurados com caracteres curinga.

Antes de iniciar

A lista de procurados deve estar ativa e ser gerenciada por um LPR Manager.

Para ativar listas de procurados curinga:

1 Na página inicial do Config Tool, clique em **LPR** > **Listas de procurados** e, em seguida, clique na lista de procurados que deseja configurar.
2 Clique na aba **Avançado** e altere a opção **Usar caracteres curinga** para **Ligado**.
3 Clique em **Aplicar**.

Tópicos relacionados

Listas de procurados curinga na página 805

Atributos padrão de lista de procurados e autorizações

Os seguintes atributos de lista de procurados e autorizações são criados por padrão no Security Center:

- **Categoria (Obrigatório):** O nome da autorização de estacionamento. Este campo no arquivo de texto de origem da lista de autorizações *deve* corresponder exatamente ao nome da entidade de autorização para que a entrada seja baixada para o Genetec Patroller™. Se você tiver várias categorias no mesmo arquivo de origem, você pode usar a mesma lista de permissões para diferentes entidades de autorização em seu sistema.

  Por exemplo, aqui está uma simples lista de autorizações com três categorias de autorização diferentes (*Estudantes*, *Docentes* e *Manutenção)*. Você pode usar esta mesma lista de autorizações para três entidades de autorização diferentes (uma entidade de autorização *Estudantes*, uma entidade de autorização *Docentes* e uma entidade de autorização *Manutenção*). Cada entidade pode apontar para o mesmo arquivo de texto de origem. O Security Center extrai as placas de veículo (e informações relacionadas) cuja categoria seja a mesma que o nome da entidade de autorização.

Campo de categoria	Estudantes	`QC;DEF228;2012-01-31;2012-05-31;PermitID_1`
	Docentes	`QC;345ABG;2012-01-31;2012-07-25;PermitID_2`
	Manutenção	`QC;244KVF;2012-01-31;2012-03-31;PermitID_3`

- **PlateState (Opcional):** Estado (ou província ou país) de emissão da placa de licença.
- **PlateNumber (Obrigatório):** O número da placa de licença.
- **EffectiveDate (Opcional):** Data a partir da qual a autorização na lista é válida.
- **ExpiryDate (Opcional):** Data a partir da qual a autorização deixa de ser válida.
- **PermitID (Opcional -** *Fiscalização de autorizações compartilhadas, geralmente Fiscalização de estacionamento na universidade e algumas aplicações de fiscalização na cidade***):** Usado quando várias entradas em uma lista de autorizações compartilham a mesma autorização (por exemplo, autorizações de carro compartilhado). Pode ser usado para identificar o número da autorização emitida para o veículo cuja placa é identificada em *PlateNumber*. No caso de autorizações compartilhadas, normalmente até quatro veículos separados teriam o mesmo número de autorização.

  Uma violação resulta em uma ocorrência de *Autorização compartilhada* no Genetec Patroller™.

Tópicos relacionados

Sobre autorizações na página 892

Configurando lista de procurados padrão e atributos de autorização

Você deve configurar os atributos de uma lista de procurados ou de permissão no Security Center da maneira como ela está escrita no seu arquivo de texto de origem, para que o Genetec Patroller™ possa analisar as informações na lista.

O que você deve saber

- Não pode haver espaços dentro de um nome de atributo.
- O arquivo de texto da lista de procurados e da lista de autorizações deve incluir os campos *Categoria* e *PlateNumber* (atributos). Estes são campos obrigatórios e não podem ser excluídos.

Para configurar lista de procurados padrão e atributos de autorização:

1 Na página inicial do Config Tool, execute uma das seguintes opções:

Se você estiver configurando atributos dos assistentes **Criação de lista de procurados** ou **Criação de uma autorização** salte para a Etapa 3.

- Clique em **LPR** > **Autorizações** e selecione a autorização a configurar.
- Clique em **LPR** > **Listas de procurados** e selecione a lista a configurar.

2 Clique na guia **Propriedades.**

3 Na seção **Atributos**, faça um dos seguintes:

- Para configurar um atributo padrão, selecione-o na lista e clique em **Editar o item** ( ).
- Para adicionar um novo atributo, clique em **Adicionar um item** ( ).

4 Se você estiver adicionando um novo atributo, digite um **Nome** para o atributo.

O nome pode conter espaços.

5 Se você quiser usar um valor padrão para o campo, digite a opção **Valor**.

O valor padrão é interpretado de forma diferente, dependendo dos delimitadores serem usados ou não.

- Se delimitadores forem usados e você adicionar um valor padrão para este campo, o campo preenchido no arquivo de origem será substituído.
- Se os delimitadores não forem usados e o campo estiver vazio no arquivo de origem, o valor padrão que você adicionar aqui será usado para o campo. No entanto, se o campo estiver preenchido no arquivo de origem, ele não será substituído.

6 Se você estiver adicionando um novo atributo e ele for obrigatório no arquivo de origem, ligue a opção **É obrigatório**.

Exemplo: If you add a mandatory attribute called *CarColor*, the column for *CarColor* no arquivo de origem deve conter texto.

7 Para mostrar campos adicionais de atributos, clique em .

8 Se o arquivo de origem usar campos de dados de comprimento fixo em vez de delimitadores, altere a opção **Comprimento fixo** para **Ligado**, defina a posição do caractere de **Início**do atributo no arquivo e seu **Comprimento**.

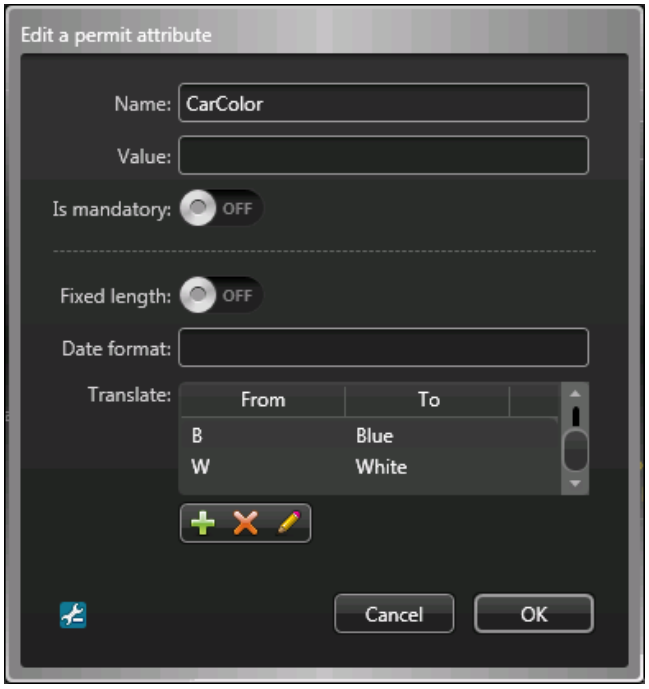
A posição do primeiro caractere no arquivo de origem é zero (0).

9 Se o campo contiver um valor de data ou hora no arquivo de origem, especifique um **Formato de data**.

Todas as sequências padrão de formato de data e hora usadas no Windows são aceitas. Se nada for especificado, o formato de tempo padrão é "aaaa-MM-dd".

10 Se quiser transformar os valores lidos no arquivo de dados, clique em **Add an item** (), em **Traduzir**, selecione um valor **De** e outro **Para**e clique em **OK**.

Exemplo: No exemplo a seguir, o novo campo é CarColor e B será traduzido para Azul e W será traduzido para Branco.



11 Clique em **OK**.

12 Para excluir um atributo que você não está usando no arquivo de origem, selecione-o na lista e clique em **Excluir** ().

Exemplo: Se as autorizações na sua lista não expirarem, você pode excluir o atributo *ExpiryDate*

Os campos de atributos da sua lista de procurados e os arquivos de texto de origem da lista de permissões agora devem corresponder aos atributos na aba **Propriedades** da entidade. Genetec Patroller™ Agora pode fazer o download da informação da lista.

Exemplo

O seguinte arquivo de origem usa dados de comprimento de campo variável e um ponto e vírgula (;) como um delimitador. As seguintes categorias são usadas: *Categoria*, *PlateState*, *PlateNumber*, *EffectiveDate*, *ExpiryDate*, e *PermitID*.

```
MyPermit;QC;DEF228;2012-01-31;2012-05-31;PermitID_1
MyPermit;QC;345ABG;2012-01-31;2012-07-25;PermitID_2
MyPermit;QC;067MMK;2012-03-31;2012-09-11;PermitID_1
MyPermit;QC;244KVF;2012-01-31;2012-03-31;PermitID_3
```

Tópicos relacionados

Atributos padrão de lista de procurados e autorizações na página 807

Definir configurações avançadas de lista de procurados

A aba **Avançado** é onde você configura as propriedades avançadas de listas de procurados, como a cor de uma ocorrência de lista de procurados e o arquivo de som que é reproduzido quando acontece uma ocorrência. Essas propriedades não são exigidas para todas as listas de procurados, mas permitem que você as personalize para cenários específicos.

Antes de iniciar

Crie a lista de procurados.

Para definir configurações avançadas de lista de procurados:

1. Na página inicial do Config Tool, clique em **LPR** > **Listas de procurados** e selecione a lista de procurados que deseja configurar.
2. Clique na aba **Avançado**.
3. Ao lado de **Cor**, clique no bloco colorido e atribua uma nova cor à autorização.

   O símbolo de mapa que marca a localização da ocorrência de lista de procurados no Security Desk e no Genetec Patroller™ aparecerá nessa cor, bem como as telas *Ocorrência de lista de procurados* e *Revisar ocorrências* do Genetec Patroller™.
4. Ative a opção **Usar curingas** para utilizar listas de procurados com curingas.
5. Ative a opção **Secreto** se quiser definir a lista de procurados como lista de procurados secreta. Quando você escolhe esta configuração, os usuários do Genetec Patroller™ não são alertados quando acontece uma ocorrência. Somente usuários com privilégios suficientes podem ver ocorrência oculta no Security Desk.
6. Insira o **Endereço de e-mail** que recebe uma notificação quando a lista de procurados que está sendo configurada gera uma ocorrência.
7. Digite o caminho para o **Arquivo de som** que o Genetec Patroller™ reproduz quando acontece uma ocorrência de lista de procurados. Se você deixar este campo em branco, o Genetec Patroller™ reproduzirá seus sons padrão. O caminho (você deve incluir o nome do arquivo) indica a localização do arquivo no computador do Genetec Patroller™ a bordo do veículo.
8. Ative a opção **Ignorar privacidade para e-mails** se você quiser ignorar configurações de privacidade que você aplicou no nível do Directory e enviar um e-mail com dados LPR reais para o endereço de e-mail que você especificou para esta lista de procurados específica.
9. Ative a opção **Desativar transferência periódica** se você somente quiser permitir que sejam baixadas alterações para o Genetec Patroller™ quando o usuário iniciar sessão no aplicativo. Esta opção exige uma conexão sem fio entre o Genetec Patroller™ e o Security Center.

   Ative a opção **Ativar modificação da transferência** se você deseja transferir modificações de lista de procurados para o Genetec Patroller™ assim que ocorrerem. Por exemplo, você pode usar essa opção em uma lista de procurados para forçar o Genetec Patroller™ a solicitar mudanças com mais frequência do que o período de transferência periódica (que se aplica a todas as listas de procurados). Isso pode ser útil para alertas AMBER, porque eles podem ser adicionados a uma lista de procurados específica e enviados para um Genetec Patroller™ quase que imediatamente. Esta opção exige uma conexão sem fio contínua entre o Genetec Patroller™ e o Security Center.

Configurar correspondência de leitura passada no LPR Manager

Quando uma lista de procurados é atualizada, o sistema pode pesquisar as leituras de placa de veículo no banco de dados do LPR Manager para ver se as novas entradas da lista de procurados foram lidas anteriormente.

Antes de iniciar

Crie uma lista de procurados que será usada para acionar a correspondência de leitura passada.

O que você deve saber

- Você pode acionar a correspondência de leitura passada usando uma ação instantânea, uma tarefa programada ou um evento causa-efeito.
- No relatório *Ocorrências* do Security Desk, as ocorrências que são geradas usando a correspondência de leitura passada são indicadas na coluna *Pós-correspondência*.
- Se o seu sistema incluir veículos de patrulha, você pode executar a correspondência de leitura passado no Genetec Patroller™. Para mais informações, consulte o *Genetec Patroller™ Guia do Administrador*.

Configurar correspondência de leitura passada no LPR Manager:

1 Associe as listas de procurados que você deseja gerenciar com o LPR Manager.

NOTA: Em etapas posteriores, você selecionará listas de procurados específicas nesta lista sobra a qual será executada a correspondência de leitura passada.

a) Na página inicial do Config Tool, clique em **Sistema** > **Funções**e, em seguida, clique em LPR Manager que deseja configurar.
b) Clique na guia **Propriedades**.
c) Em **Associação de arquivo**, selecione as listas de procurados e autorizações que você deseja que o LPR Manager gerencie.
d) Clique em **Aplicar**.

2 Habilite a correspondência de leitura passada na função LPR Manager.

a) Clique na guia **Propriedades.**
b) Coloque a opção **Correspondência** em **Ligada**.
c) (Opcional) Para gerar eventos *Não correspondência* quando uma placa é lida por um Sharp e não faz parte de uma lista de procurados ou da lista de autorizações, coloque a opção **Gerar eventos "Não correspondência"** em **Ligado**.

3 A seção **Correspondência de leitura passada** lista todas as listas de procurados que você associou à função LPR Manager. Selecione as listas de procurados para as quais você deseja habilitar a correspondência de leitura passada.

NOTA: As listas de procurados federadas não são suportadas pela correspondência de leitura passada e, portanto, não são exibidas na lista.

4 No **campo Pesquisar hora para trás**, defina o intervalo de tempo durante o qual a correspondência de leitura passada ocorrerá.

NOTA: Realizar a correspondência de leitura passada em muitas ou grandes listas de procurados e usar um tempo para trás longo pode afetar o desempenho do sistema.

5 Clique em **Aplicar**.

6 Acione a correspondência de leitura passada usando os seguintes métodos:

- Crie uma tarefa programada que use a ação *Acionar correspondência de leitura passada*.

- Crie uma evento causa-efeito que use o evento *Lista de procurados alterada* e a ação *Acionar correspondência de leitura passada*.
- Em Security Desk, crie uma ação instantânea que use a ação *Acionar correspondência de leitura passada*. Para obter mais informações sobre ações instantâneas, consulte o *Guia do Usuário do Security Desk*.

Tópicos relacionados

Agendar tarefa na página 219
Criar eventos causa-efeito na página 208

41

Sistemas fixos AutoVu™

Esta seção inclui os seguintes tópicos:

- "Preparar para implantar sistemas fixos AutoVu" na página 814
- "Implantar sistemas AutoVu fixos" na página 815
- "Configurando LPR Managers para sistemas AutoVu fixos" na página 816
- "conexões de câmeras Sharp, SharpV ou SharpX ao Security Center" na página 817
- "Adicionando uma câmera Sharp, SharpV ou SharpX ao LPR Manager" na página 819
- "Adicionar uma câmera Sharp, SharpV ou SharpX ao Archiver" na página 820
- "Substituir unidades Sharp fixas" na página 821
- "Controle de acesso baseado em LPR" na página 823
- "Configurar o AutoVu para controle de acesso" na página 825

Preparar para implantar sistemas fixos AutoVu™

Para garantir que a instalação do seu AutoVu™ fixo aconteça sem problemas, deve realizar uma série de passos de configuração prévia.

Antes de implantar sistemas fixos AutoVu™:

1 Tenha a informação da sua pesquisa inicial do local em mãos antes de instalar o hardware AutoVu™.

Por exemplo, você já deve saber a altura em que deve instalar um Sharp fixo antes de iniciar a instalação.

2 Instale os seguintes componentes de software do Security Center:

a) Software do servidor Security Center em seu servidor principal.

O *servidor principal* é o computador que hospeda a função *Directory*.

b) (Opcional) Software do servidor Security Center em servidores de expansão.

Um *servidor de expansão* é qualquer outro servidor no sistema que não hospede a função Directory. Você pode adicionar servidores de expansão a qualquer momento.

c) Software de cliente Security Center em pelo menos uma estação de trabalho.

Para obter mais informações sobre como instalar o Security Center, consulte o *Guia de Instalação e Atualização do Security Center*.

3 Instale o hardware Sharp fixo (consulte o *Guia de Instalação do Hardware AutoVu™*).

4 Atualize as unidades Sharp para o mais recente software e firmware (consulte o *Guia do Administrador do Sharp*).

NOTA: Você pode realizar certas atualizações do Security CenterConfig Tool.

Implantar sistemas AutoVu™ fixos

Para integrar diferentes capacidades de LPR no Security Center, você pode implantar um sistema AutoVu™ fixo.

Antes de iniciar

Execute as etapas de pré-configuração.

O que você deve saber

As informações sobre como configurar uma instalação AutoVu™ fixa típica são descritas aqui. Seu processo pode ser diferente dependendo das exigências específicas de sua instalação.

NOTA: As configurações que são pré-configuradas durante sua instalação não são listadas nesta tarefa. Por exemplo, quando você instala o Security Center, a pasta raiz do LPR Manager é criada automaticamente em seu computador na localização *C:\Genetec\AutoVu\RootFolder*.

Para implantar um sistema AutoVu™ fixo:

1 Faça logon no Sharp Portal e configure o Sharp para um sistema AutoVu™ fixo.

Para obter informações sobre como iniciar sessão no Sharp Portal, consulte o *Guia do Administrador Sharp*.

2 Configure o LPR Manager para que o Security Center possa descobrir unidades Sharp fixas e se comunicar com elas.

3 Conecte um Archiver ao LPR Manager para armazenar as imagens de LPR (capturadas por câmeras de contexto, câmeras de LPR e câmeras WMS) que estão associadas a leituras e ocorrências.

NOTA: Você deve também registrar a unidade de processamento de LPR no Archiver para instalações do SharpX onde o controle de entrada/saída da unidade de processamento LPR é necessário.

4 Defina o servidor do LPR Manager e as configurações do banco de dados.

NOTA: Você também pode adicionar um servidor adicional para atuar como *servidor secundário* para o LPR Manager, para configurar o failover. Para mais informações, consulte Configurar failover de função na página 165.

5 Se você estiver usando listas de procurados com sua implantação fixa, então crie e configure as entidades de lista de procurados e ative a correspondência de listas de procurados.

6 Se você estiver usando o AutoVu™ como solução de controle de acesso, então configure as câmeras Sharp para conceder ou negar acesso a um estacionamento ou uma instalação semelhante.

7 Especifique a localização e o fuso horário do Sharp.

Configurando LPR Managers para sistemas AutoVu™ fixos

Para receber dados LPR no Security Center com um sistema AutoVu™ fixo, você deve configurar a porta de escuta e descoberta do LPR Manager para encontrar unidades Sharp na rede e enviar os dados para o Security Center e selecionar quais imagens da LPR fixas as unidades Sharp devem enviar para o Security Center ao ler uma placa.

Antes de iniciar

Você deve saber o endereço IP do computador que hospeda a função LPR Manager.

O que você deve saber

Essas instruções explicam o método preferido de adicionar uma câmera Sharp se o Sharp e o Security Center estiverem na mesma sub-rede. Se eles não estiverem na mesma sub-rede, ou se eles devem se comunicar pela Internet com uma topologia de rede que inclui NATs, você deve usar um método de conexão diferente. Para mais informações, consulte conexões de câmeras Sharp, SharpV ou SharpX ao Security Center na página 817.

Para configurar um LPR Manager para um sistema AutoVu™ fixo:

1 Na página inicial do Config Tool, clique em **Sistema** > **Funções** e selecione o LPR Manager que deseja configurar.

2 Clique na aba **Propriedades** e, em seguida, clique em **Dinâmica**.

3 Em **Rede**, configure as seguintes portas:

- **Porta de escuta:** Porta usada para escutar pedidos de conexão provenientes de câmeras Sharp fixas (e veículos de patrulha). Depois que a conexão for estabelecida, o LPR Manager pode receber atualizações ao vivo das unidades LPR que gerencia. O número da porta de escuta padrão é 8731.
- **Sharpporta de descoberta:** Porta usada pelo LPR Manager para encontrar unidades Sharp fixas na rede.

  IMPORTANTE:

  - Cada unidade LPR precisa ter uma porta de descoberta exclusiva.
  - Ao configurar a porta de descoberta, não use a porta 5050, pois ela é reservada para o serviço do registrador.

4 Em **Enviar na leitura (somente Sharp fixo)**, configure os seguintes:

- **Imagem da placa de licença:** Inclui a imagem de alta resolução da placa de licença junto com os dados de leitura da placa.
- **Imagem do contexto:** Inclui a imagem de contexto de ângulo amplo junto com os dados de leitura da placa.

Essas imagens são exibidas no Security Desk ao monitorar eventos de LPR.

Após terminar

- Verifique se a porta de descoberta Sharp corresponde ao número da porta no Portal Sharp. Para obter mais informações, consulte *Guia do Administrador Sharp*.
- Para garantir que as leituras de placa tenham o carimbo de data e hora correto, configure o fuso horário das unidades Sharp fixas.
- Para traçar os eventos LPR (leituras e ocorrências) associados às unidades Sharp no *mapa* em Security Desk, configure a localização geográfica das unidades Sharp.

conexões de câmeras Sharp, SharpV ou SharpX ao Security Center

Se você estiver usando a extensão Security Center para enviar dados de LPR de uma câmera Sharp, SharpV ou SharpX para o Security Center, você deve primeiro registrar a câmera na tarefa *LPR* do Security Center em *Funções e unidades*.

A maneira mais fácil de adicionar uma câmera Sharp, SharpV ou SharpX no Security Center é configurar o LPR Manager para descobrir a câmera. Se este método de conexão não for possível, você pode adicionar a câmera manualmente no Security Center ou no portal Web da câmera.

Você pode adicionar uma câmera ao Security Center de uma das seguintes maneiras:

Método de conexão	Quando usar este método	Exigências
Configurar o LPR Manager para descobrir a câmera: Você pode configurar a *Porta de descoberta* do LPR Manager para encontrar a câmera na sub-rede.	Este é o método preferencial se a câmera e o Security Center estiverem na mesma sub-rede.	Para usar este método, você deve configurar a mesma *Porta de descoberta* na aba *Propriedades* do LPR Manager e no portal Web da câmera. A câmera e o Security Center devem estar na mesma sub-rede. Para obter mais informações sobre como configurar LPR Managers para um sistema AutoVu™ fixo, consulte o Sobre o LPR Manager na página 764.

Método de conexão	Quando usar este método	Exigências
Adicionar manualmente a câmera no Security Center: Você pode adicionar a câmera ao LPR Manager na tarefa *LPR* do Config Tool.	Use este método quando a câmera e o Security Center estiverem em sub-redes diferentes dentro da mesma LAN. Você pode usar este método se a *Porta de descoberta* não estiver disponível; porém, a *Porta de descoberta* pode ser mudada no Security Center e no portal Web da câmera. **NOTA:** • Você não pode usar esse método se a comunicação deve atravessar a Internet. • Se a câmera estiver atrás de um NAT, você deve configurar o encaminhamento da porta.	Para usar este método, você deve conhecer o endereço IP e a porta (porta de controle) para a câmera. A câmera e o Security Center devem estar na mesma rede.
Adicionar uma Sharp, SharpV ou SharpX a partir do portal Web da câmera: Você pode forçar uma conexão do portal Web da câmera ao selecionar a extensão *Security Center* e selecionar **Conectar ao Security Center**. Para obter ajuda, contate seu representante da Genetec™.	Use este método se a câmera e o Security Center tiverem que se comunicar pela Internet e a topologia da rede incluir NATs. **NOTA:** Se a câmera estiver atrás de um NAT, você deve configurar o encaminhamento da porta.	Para usar este método, você deve inserir o *Nome de host* ou o *endereço IP* e *porta* (porta de escuta) do computador do Security Center.

Adicionando uma câmera Sharp, SharpV ou SharpX ao LPR Manager

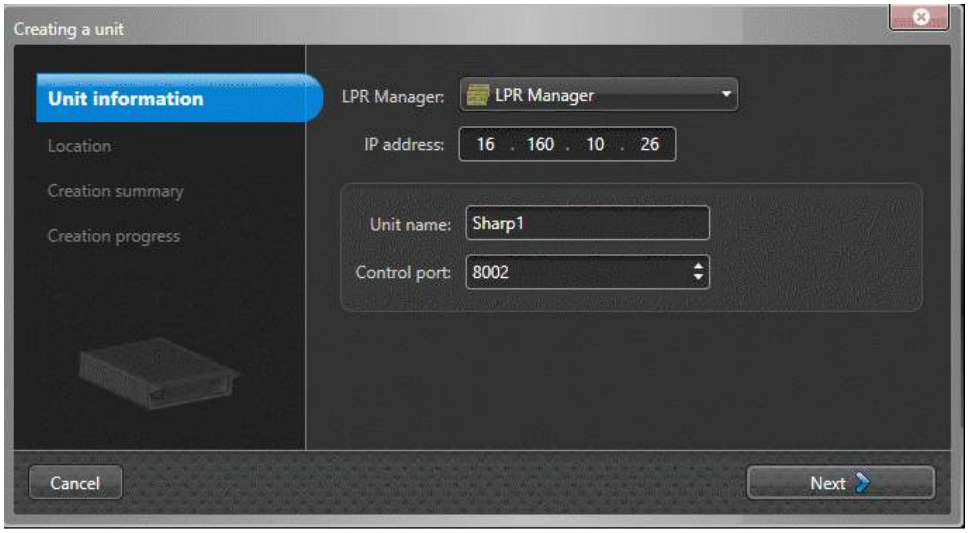
Para enviar dados de LPR da câmera para o Security Center, você deve adicionar a câmera a um LPR Manager.

Antes de iniciar

Configure um LPR Manager para o sistema AutoVu™ fixo.

Para adicionar uma câmera manualmente no Security Center:

1 Na página inicial do Config Tool, clique na tarefa *LPR* e selecione **Funções e unidades**.
2 Selecione a função **LPR Manager** na lista suspensa.
3 Clique em **Unidade de LPR**.
A caixa de diálogo **Criar uma unidade** abrirá.
4 Digite o **endereço IP** da câmera.
5 Digite um **Nome de unidade** para a câmera.
6 Digite a **Porta de controle** da câmera.
Estas informações devem corresponder às que são exibidas no portal da câmera.



7 Clique em **Próximo**.
8 Conclua todas as outras configurações conforme necessário e clique em **Criar**.

A nova câmera é incluída no LPR Manager selecionado.

Adicionar uma câmera Sharp, SharpV ou SharpX ao Archiver

Para armazenar as imagens de LPR que estão associadas a leituras e ocorrências, você deve adicionar a câmera Sharp ao Archiver.

Antes de iniciar

- Configure a função Archiver para LPR.
- Faça logon no portal da câmera e altere a senha padrão.

O que você deve saber

- Por padrão, o Archiver usa a transmissão H.264 para câmeras SharpV. Caso deseje usar a transmissão MJPEG, você pode selecioná-la na tarefa *Vídeo* na tela da câmera SharpV.
- **NOTE:** As informações sobre câmeras de contexto não são aplicáveis a câmeras SharpV ITS.

Para adicionar uma câmera manualmente a um Archiver do Security Center:

1 Na página inicial do Config Tool, abra a tarefa **Vídeo**.
2 Clique em **Unidade de vídeo** .
A caixa de dialogo **Adição manual** se abrirá.
3 Se você tiver várias funções Archiver, selecione a função Archiver que deve gerenciar a unidade de vídeo na lista suspensa **Archiver**.
4 Na lista suspensa **Fabricantes**, selecione **Genetec AutoVu**.
5 Na lista suspensa **Tipo de produto**, selecione **Todos**.
6 Digite o **endereço IP** estático da câmera.

DICA: Para adicionar várias unidades em uma única operação, digite um intervalo ( ) de endereços IP.

7 Para usar comunicação HTTP, digite **porta HTTP** 80.
Para usar comunicação HTTPS, ative **Usar HTTPS** e digite porta 443.
8 Selecione o método de **Autenticação** para a câmera.
   - **Logon padrão:** A câmera usa o logon padrão definido para o Archiver na aba *Extensões*. Usando esse método, você pode definir as mesmas credenciais de login para várias câmeras.

     IMPORTANTE: Você não pode usar o logon padrão ao adicionar uma câmera SharpV. Você deve usar as credenciais configuradas ao fazer logon pela primeira vez no portal SharpV.
   - **Específico:** Digite as credenciais de logon para a câmera. Ative **Usar HTTPS** se você tiver aplicado um certificado autoassinado ou assinado à conexão da câmera.
9 Na lista suspensa **Localização**, atribua a câmera a uma entidade de área.
10 Clique em **Adicionar**
A bandeja de notificação exibe a mensagem "Adição de unidade iniciada". Se bem-sucedida, ela exibe a mensagem "Unidade adicionada com sucesso".

A câmera é incluída no Archiver selecionado.

Substituir unidades Sharp fixas

Você pode substituir uma unidade Sharp fixa sem perder nenhuma das suas leituras de placas associadas, trocando os parâmetros de conexão da unidade antiga com uma nova unidade.

Antes de iniciar

- No Security Desk, execute um relatório *Leituras* e um relatório *Ocorrências* na unidade Sharp que deseja substituir. Você precisa desses relatórios para verificar se os dados foram transferidos para a nova unidade Sharp.

Para substituir uma unidade Sharp:

1 Adicione a nova entidade Sharp no LPR Manager.

NOTA: O nome que você usa para a nova entidade não é importante. No final do procedimento de substituição da câmera, os parâmetros de conexão das entidades serão comutados e você irá excluir a entidade que está adicionando agora.

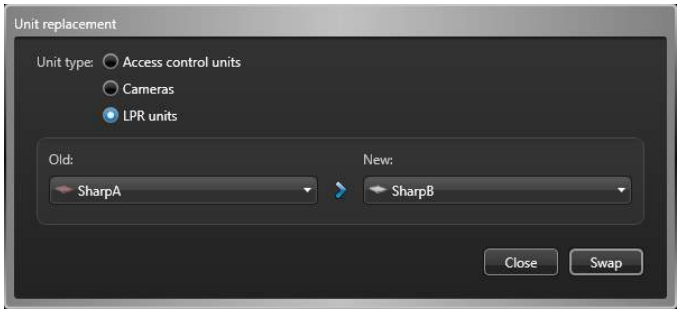
2 Copie as configurações da entidade Sharp antiga para a nova entidade Sharp usando a Ferramenta de cópia de configuração.

3 Desligue a unidade Sharp antiga.

4 No Config Tool, clique em **Ferramentas** > **Substituição de unidades**.

5 Na opção **Tipo de unidade**, selecione **Unidades de LPR**.

6 Selecione as unidades Sharp **Antiga** e **Nova**.

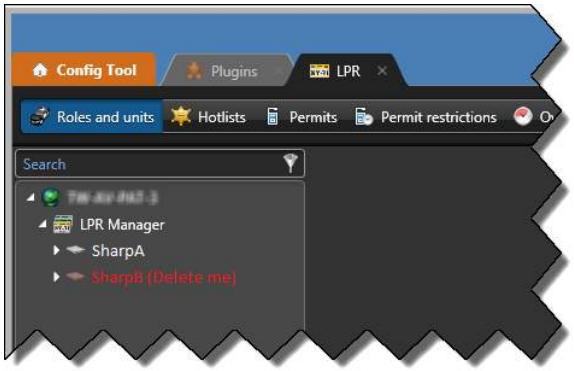


7 Clique em **Trocar**.

Quando a unidade Sharp tiver sido substituída, o sistema exibe a mensagem: "A operação foi bem-sucedida". Os parâmetros de conexão da nova unidade Sharp agora estão associados às leituras e ocorrências da antiga Sharp.

8 Verifique se as leituras e ocorrências ainda estão associados à antiga entidade Sharp executando um relatório *Leituras* e um relatório *Ocorrências* do Security Center. Compare esses relatórios com aqueles que você executou antes da operação de troca para garantir que os dados foram transferidos com sucesso.

9 As entidades Sharp foram trocadas no Security Center. A antiga unidade Sharp agora possui o novo nome da entidade e é exibida no LPR Manager com a mensagem: "Exclua-me". Clique com o botão direito do mouse na entidade Sharp e selecione **Excluir**. Na caixa de diálogo de confirmação que abrir, clique em **Excluir**.



NOTA: No Security Center 5.7, o nome da antiga unidade Sharp não é alterado e não exibe da mensagem "Exclua-me".

Tópicos relacionados

Copiar definições de configuração de uma entidade para a outra na página 77
Configurando LPR Managers para sistemas AutoVu fixos na página 816

Controle de acesso baseado em LPR

Instalando câmeras Sharp nos pontos de entrada de uma instalação (por exemplo, estacionamentos, campus universitários e assim por diante), o Reconhecimento de placas de veículo AutoVu™ (LPR, License Plate Recognition) pode ser usado para controle de acesso através da correspondência de placas de veículo a uma ou mais listas de procurados, concedendo ou negando depois o acesso a veículos que desejam entrar na instalação.

Como o controle de acesso baseado em LPR funciona

Em um cenário de controle de acesso baseado em LPR, você usa câmeras Sharp, listas de procurados e eventos causa-efeito do Security Center para automatizar o acesso a um estacionamento ou instalação similar.

Você começa por instalar suas câmeras Sharp nos pontos de entrada de uma instalação para capturar as placas de veículos que tentam entrar. Em seguida, você cria as listas de procurados que contêm as placas dos veículos que podem entrar e atribui-as ao LPR Manager ou a câmeras Sharp individuais no Config Tool.

Depois de criar e atribuir suas listas de procurados, você cria eventos causa-efeito do Security Center para os eventos *Alerta de placa de licença* e *Não combina* gerados pelos Sharps e pelas listas de procurados para conceder ou negar o acesso aos veículos.

Por exemplo, se uma placa corresponder a uma ou mais listas de procurados atribuídos a um Sharp, o Security Center desencadeia uma ação que levanta um portão ou abre uma porta de garagem, enquanto um evento de *Não combina* (a placa não corresponde a nenhuma lista de procurados atribuída) desencadeia uma ação que faz soar um alerta ou envia uma mensagem para o pessoal de segurança para que eles possam questionar o condutor do veículo.

Você também pode disparar eventos para ações em listas de veículos roubados, contraventores ou outros veículos de interesse. Essas listas são geralmente atribuídas ao LPR Manager para que o evento para ação possa ser acionado por qualquer um dos Sharps que captura a placa.

Sobre a atribuição de listas de procurados

Listas de procurados são listas de placas de veículos que podem ser atribuídas a uma função LPR Manager ou a câmeras Sharp individuais.

- **Atribuir uma lista de procurados a um LPR Manager**: Quando você atribui uma lista de procurados a um LPR Manager, todas as câmeras Sharp controladas pelo LPR Manager podem fazer correspondência com a lista de procurados e acionar um evento causa-efeito.
- **Atribuir uma lista de procurados a uma câmera Sharp**: Quando você atribui uma lista de procurados a uma câmera Sharp individual, somente essa câmera Sharp específica pode acionar um evento causa-efeito. Isto é útil para estacionamentos que tenham pontos de entrada específicos para diferentes grupos de veículos. Por exemplo, isso permite que você atribua uma lista de procurados VIP a uma câmera Sharp instalada na entrada da garagem de estacionamento VIP.

Eventos usados no controle de acesso baseado em LPR

Existem dois tipos principais de eventos do Security Center usados em um sistema de controle de acesso baseado em LPR, *Alerta de placa de licença* e *Não combina*.

NOTA: Você também pode usar eventos de *Reconhecimento de placas de veículos* para desencadear ações como iniciar a gravação de vídeo para a câmera de contexto da Sharp. No entanto, somente os eventos *Alerta de placa de licença* e *Não combina* são descritos aqui.

- **Eventos Alerta de placa de licença:** Ao ativar a *Correspondência* para um LPR Manager no Config Tool, o Security Center tenta combinar as placas capturadas pelas câmeras Sharp com placas em listas de procurados carregadas. Se uma placa corresponder a uma lista de procurados, o Security Center gera um

evento *Alerta de placa de licença*. Ao criar um evento causa-efeito que é desencadeado por esse evento, o Security Center pode conceder acesso a uma instalação abrindo um portão, uma porta de garagem e assim por diante.

- **Eventos Não combina:** Você também pode ativar eventos *Não combina* para um LPR Manager no Config Tool. Em evento *Não combina* é gerado quando uma placa *não* corresponde a uma lista de procurados. Por exemplo, você pode usar um evento *Não combina* para considerar convidados, veículos de entrega ou outros veículos que normalmente não são registrados antecipadamente em uma lista de procurados. Eventos causa-efeito para eventos *Não combina* podem ter uma lista de procurados ou uma câmera Sharp como origem do evento. Se a lista de procurados for a origem, isso significa que a placa não é encontrada naquela lista específica. No entanto, se o Sharp for a origem, isso significa que a placa não é encontrada em *nenhuma* das listas de procurados atribuídas ao Sharp. Esta é uma diferença sutil, mas importante, que você deve ter em mente ao configurar o seu sistema porque você pode ter mais de uma lista de procurados atribuída a um único Sharp.

  Eventos *Não combina* não são gerados ao comparar com listas de procurados atribuídas ao LPR Manager porque elas se aplicariam a todos os Sharps controlados pela função. Por exemplo, se você tiver uma lista de procurados de veículos roubados atribuída ao LPR Manager, qualquer placa lida que não conste daquela lista geraria um evento *Não combina*. Como a maioria das placas lidas pelo Sharp não serão de veículos roubados, eventos *Não combina* seriam gerados para praticamente todas as placas de veículo lidas.

Assista a este vídeo para saber mais. Clique no ícone **Legendas** (**CC**) para ligar a legenda do vídeo em um dos idiomas disponíveis. O vídeo pode não ser exibido no Internet Explorer. Para resolver isso, abra as **Configurações de compatibilidade de exibição** e limpe **Exibir sites da intranet em Visualizar compatibilidade**.

Configurar o AutoVu™ para controle de acesso

Para conceder ou negar o acesso de veículos a uma zona protegida (estacionamento, portão, entrada e assim por diante) com base em suas placas de veículo, você pode configurar uma solução personalizada de controle de acesso baseada em LPR.

Antes de iniciar

Faça o seguinte:

- Saiba mais sobre Controle de acesso baseado em LPR na página 823.
- Instale câmeras Sharp em cada ponto de entrada do estacionamento (consulte o *Guia de instalação de hardware AutoVu™*).
- Deixe um sistema AutoVu™ fixo preparado e em funcionamento.

O que você deve saber

Você pode implantar uma solução de controle de acesso baseada em LPR de várias maneiras. O exemplo de um campus universitário é usado para mostrar como você pode personalizar uma solução específica para sua implantação.

No hipotético campus universitário, aplicam-se as seguintes regras:

- **Docentes:** Podem estacionar nos Estacionamentos A e B.
- **Estudantes:** Podem estacionar no Estacionamento B.
- **Gerência:** Podem estacionar no Estacionamento C.
- **Manutenção:** Podem estacionar no Estacionamento B em dias da semana das 18:00 às 22:00.
- **Convidados:** Pode estacionar em qualquer estacionamento com a aprovação da segurança.
- **Contraventores:** Não podem estacionar em nenhum lugar no campus, e a segurança deve ser alertada se forem vistos.

Para configurar regras de acesso para estacionamentos:

1 Nomeie as entidades Sharp.

O Security Center detecta automaticamente todas as câmeras Sharp conectadas à rede, mas você deve nomear cada câmera de acordo com sua função ou localização. Em nosso exemplo, use os nomes *Sharp do Estacionamento A*, *Sharp do Estacionamento B* e *Sharp do Estacionamento C*.

NOTA: A configuração é mais simples quando todas as câmeras Sharp estão no mesmo LPR Manager. No entanto, se as câmeras Sharp estiverem em vários LPR Managers, você deve atribuir suas listas de procurados em conformidade.

2 Ative a correspondência de lista de procurados para o LPR Manager que controla suas câmeras Sharp.

3 Crie e configure entidades de listas de procurados.

Nomeie cada lista de procurados de acordo com seus conteúdos. No exemplo do campus universitário, use os nomes *Docentes*, *Estudantes*, *Gerência*, *Manutenção* e *Contraventores.*

NOTA: No exemplo da universidade, *Convidados* representa qualquer um que apareça sem ser anunciado. Portanto, eles não estão incluídos em nenhuma lista de procurados.

4 Crie uma agenda.

Por exemplo, se você quiser que os funcionários de *Manutenção* tenham acesso ao seu estacionamento somente entre as 18:00 e as 22:00, você deve criar uma agenda no Security Center que reflita isso. Você usará essa agenda mais tarde quando criar seus eventos de causa-efeito.

5 Adicione suas listas de procurados a câmeras Sharp e ao LPR Manager como indicado a seguir:

- *Docentes* para *Sharp do Estacionamento A* e para o *Sharp do Estacionamento B*.
- *Estudantes* para *Sharp do Estacionamento B*.
- *Gerência* para *Sharp do Estacionamento C*.
- *Contraventores* e *Manutenção* para o LPR Manager.

NOTA: A lista de procurados de *Manutenção* deve ser atribuída ao LPR Manager já que depende de uma agenda. Todas as listas de procurados que você combinar com agendas devem ser atribuídas ao LPR Manager.

6 (Opcional) Se você tiver apenas um LPR Manager no seu sistema, remova a atribuição das listas de procurados *Docentes*, *Estudantes* e *Gerência* do LPR Manager.

Quando você tem apenas um LPR Manager, novas listas de procurados são atribuídas a esse LPR Manager por padrão (novas listas de procurados são deixadas sem atribuição se você tiver vários LPR Managers). Quando você atribui uma lista de procurados a uma Sharp, o Security Center não remove automaticamente sua atribuição do LPR Manager; você deve fazê-lo manualmente. Caso contrário, você obterá eventos de correspondência duplicados das outras câmeras Sharp.

Exemplo: Se você atribuir a lista de procurados *Estudantes* a *Sharp do Estacionamento B*, mas esquecer de remover a atribuição do LPR Manager, uma leitura de placa de veículo dessa lista por *Sharp do Estacionamento B* também aciona correspondências em *Sharp do Estacionamento A* e *Sharp do Estacionamento C*.

7 Configure eventos de causa-efeito para câmeras *Sharp do Estacionamento A*, *Sharp do Estacionamento B* e *Sharp do Estacionamento C*.

8 Configure eventos de causa-efeito para as listas de procurados *Contraventores* e *Manutenção*.

O acesso ao estacionamento é agora automatizado para veículos permitidos, e são tomadas ações quando veículos desconhecidos ou de contraventores são detectados.

Criar eventos causa-efeito para eventos de LPR ou de listas de procurados

Para garantir que alguns veículos tenham acesso ao estacionamento, e que outras ações sejam tomadas para veículos desconhecidos ou de contraventores, você deve criar eventos para ações que são acionados com base em eventos de *Alerta de placa de licença* e *Não combina* gerados pelas câmeras Sharp.

O que você deve saber

- Para sistemas fixos SharpX, você pode configurar eventos causa-efeito para controlar as entradas e saídas da Unidade de Processamento LPR. As Unidades de Processamento LPR geralmente são inscritas no LPR Manager, porém, para que as saídas sejam selecionáveis ao criar eventos causa-efeito, você deve **também** inscrever a unidade de Processamento LPR no Archiver.
- Quando você atribui uma lista de procurados a um LPR Manager, todas as câmeras Sharp controladas pelo LPR Manager podem fazer correspondência com a lista de procurados e acionar um evento causa-efeito. Quando você atribui uma lista de procurados a uma câmera Sharp individual, somente essa câmera Sharp específica pode acionar um evento causa-efeito.

Para criar eventos para ação para eventos relacionados a Sharp:

1 Abra a tarefa **Sistema** e clique na visualização **Configurações gerais**.

2 Clique na página **Ações** e, em seguida, clique em **Adicionar um item** ().

3 Na lista suspensa **Quando** na caixa de diálogo *Evento causa-efeito*, selecione o tipo de evento *Alerta de placa de licença* ou *Não combina*.

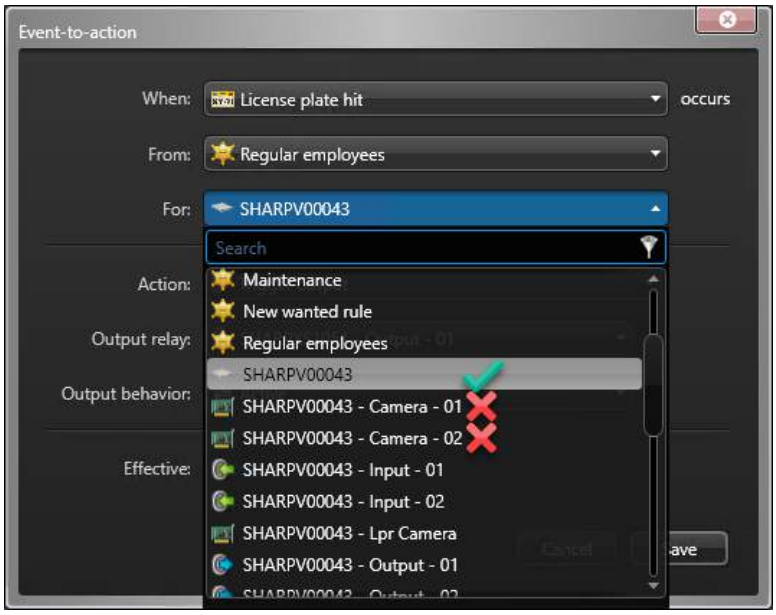
4 Da lista suspensa **De**, selecione uma lista de procurados.

Os campos **De** e **Para** podem conter tanto uma lista de procurados ou uma câmera Sharp e você não precisa preencher ambos os campos. Por exemplo, para criar um evento causa-efeito que é acionado quando uma ocorrência é detectada para a sua lista de procurados de *funcionários regulares*, não importa

em que câmera ela seja detectada, selecione a lista de procurados de *funcionários regulares* no campo **De** ou **Para** e selecione **Limpar seleção** para o outro campo para que apareça como *Qualquer entidade*.

5 Da lista suspensa **Para**, selecione a câmera Sharp para a qual você deseja atribuir a lista de procurados.

NOTA: Selecione a unidade de vídeo Sharp, não as câmeras individuais (por exemplo, *Câmera - 01*) sob a unidade.

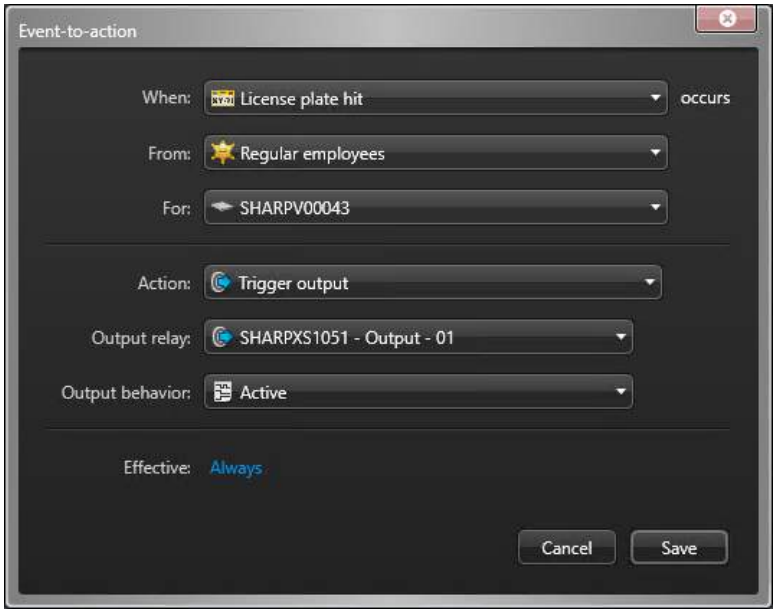


6 Selecione a **Ação** e atributos para cada tipo de evento.

- Para eventos de *Alerta de placa de licença*, selecione **Disparar saída**, em seguida selecione o **Relé de saída** e o **Comportamento de saída** exigido para conceder acesso a um estacionamento (por exemplo, abrir um portão).
  - Unidades de processamento LPR X1, X2, X2M ou X4M: inclui dois relés de saída fechados não configuráveis.
  - Unidades de processamento LPR X1S, X1SU, X2S e X2SU: inclui dois relés de saída mecânica fechados (Relé 1 e 2: 30 VDC, 8 A max., exige fusível externo) e dois relés de saída optoisolados normalmente fechados (relé 3 e 4: 30 VDC, 0,25 A max.).
  - SharpV: inclui dois relés de saída secos, optoisolados, normalmente abertos (30 V / 100 mA).
- Para eventos de *Não combina*, selecione a ação que deseja que o Security Center tome. Por exemplo, você pode enviar uma mensagem para um usuário particular do Security Center ou usar outra ação de *Disparar saída* para ativar um interfone de segurança no portão.

7 Na opção **Efetivo**, clique em **Sempre** e selecione uma agenda de quando este evento causa-efeito está ativo.

8 Clique em **Salvar**.



Tópicos relacionados

Controle de acesso baseado em LPR na página 823
Criar eventos causa-efeito na página 208

42

AutoVu™ Free-Flow

Esta seção inclui os seguintes tópicos:

- "Sobre AutoVu Free-Flow" na página 830
- "Sobre sessões de estacionamento" na página 832
- "Configurar o AutoVu Free-Flow" na página 837
- "Adicionar e configurar regras de estacionamento" na página 840
- "Adicionar e configurar zonas de estacionamento" na página 842
- "Como a ocupação da zona é calculada" na página 846
- "Sobre autorizações compartilhadas no AutoVu Free-Flow" na página 848
- "Atribuir um mapa a uma zona de estacionamento" na página 850
- "Adicionar uma zona de estacionamento a um mapa" na página 851
- "Adicionar visualizações drill-down a mapas" na página 853

Sobre AutoVu™ Free-Flow

O recurso AutoVu™ Free-Flow no Security Center aumenta a eficácia da fiscalização do estacionamento ao fornecer um inventário em tempo real das violações de estacionamento em zonas de estacionamento monitoradas.

Usando o AutoVu™ Free-Flow, você pode gerir *estacionamento temporário* e *estacionamento autorizado contratual* em zonas de estacionamento que tenham unidades Sharp fixas monitorando as entradas e saídas. O sistema registra as placas dos veículo que entram e saem do estacionamento e compara-as com a lista de titulares de autorizações e pagamentos recebidos através estações de pagamento equipadas com Pay-by-Plate Sync e aplicativos de estacionamento móveis. Os veículos cujo estacionamento ultrapasse o tempo comprado são automaticamente marcados como violações aguardando fiscalização. Se o funcionário do estacionamento for responsável por passar multas manualmente, esta informação ajuda o funcionário a decidir quando e para onde destacar patrulhas de zona de estacionamento.

O AutoVu™ Free-Flow permite fazer o seguinte:

- Usando o plug-in Pay-by-Plate Sync, o AutoVu™ Free-Flow também pode ser integrado com provedores terceiros de autorizações de estacionamento. Você pode consolidar vários sistemas de estacionamento habilitado por placa (LEP) de terceiros em uma única solução de estacionamento. Os proprietários de veículos terão assim a opção de pagar estacionamento por parquímetro e prolongar o seu tempo de estacionamento antes de entrarem em violação.
- Você pode mesclar autorizações dinâmicas Pay-by-Plate Sync com autorizações estáticas Security Center. Isto permite definir autorizações semanais ou mensais e também usar autorizações de provedores terceiros.
- O sistema tem capacidade para gerar um arquivo XML de violações que pode ser usado no seu sistema de gerenciamento de multas.
- Você pode gerar relatórios de violações nos formatos PDF, CSV e Excel, bem como relatórios na tela. Se a sua instalação de estacionamento incluir uma unidade Genetec Patroller™ (o aplicativo de bordo), o sistema pode gerar uma lista de veículos procurados em violação para ser usada em fiscalização móvel.

Exemplo

Assista a este vídeo para saber mais. Clique no ícone **Legendas** (**CC**) para ligar a legenda do vídeo em um dos idiomas disponíveis. O vídeo pode não ser exibido no Internet Explorer. Para resolver isso, abra

as **Configurações de compatibilidade de exibição** e limpe **Exibir sites da intranet em Visualizar compatibilidade**.

Sobre sessões de estacionamento

O recurso AutoVu™ Free-Flow no Security Center usa sessões de estacionamento para rastrear a permanência de cada veículo em uma zona de estacionamento.

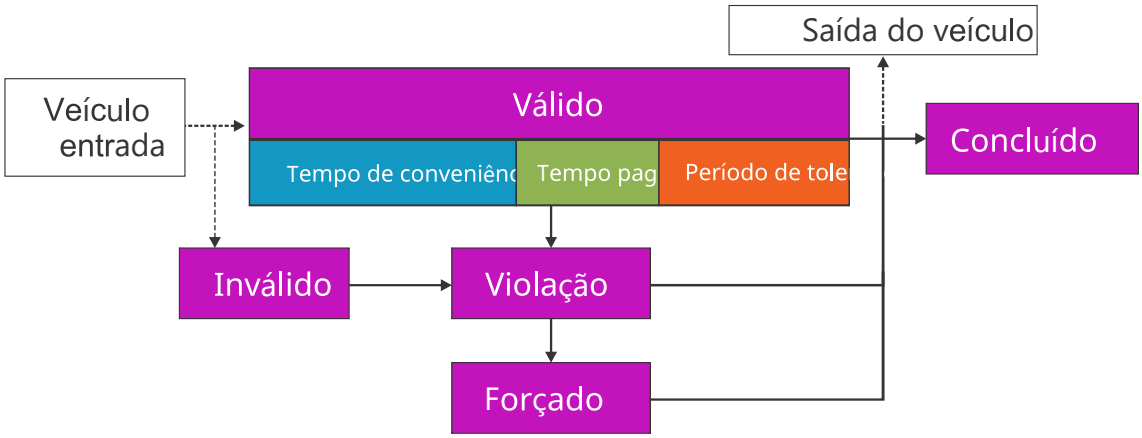
Os seguintes termos são importantes ao configurar zonas de estacionamento AutoVu™ Free-Flow:

- **Tempo de conveniência:** O tempo de conveniência é um tempo de leniência configurável que é aplicável antes de um veículo começar a ser cobrado após entrar na zona de estacionamento. Por exemplo, se você precisar configurar um período de estacionamento grátis de 2 horas que é aplicável antes de o tempo pago ou a fiscalização de estacionamento entrar em vigor, você deverá definir do tempo de conveniência para 2 horas. Para estacionamentos onde a fiscalização de estacionamento começa imediatamente, você precisaria definir um breve tempo de conveniência para dar tempo aos proprietários dos veículos encontrarem um lugar de estacionamento e adquirirem tempo de estacionamento antes que a fiscalização de estacionamento comece.
- **Atraso de expiração padrão:** O atraso padrão da expiração é usado para autorizações fornecidas pelo Pay-by-Plate Sync que não incluem uma expiração. Neste caso, o AutoVu™ Free-Flow verifica junto do provedor de autorização de estacionamento se a autorização permanece válida. Aumentar este valor reduz a frequência das verificações de autorização. Por exemplo, se o estacionamento for cobrado em incrementos de 15 minutos e você também definir o atraso padrão da expiração para 15 minutos, o sistema valida a autorização junto do provedor de estacionamento a cada 15 minutos.
- **Período de tolerância:** Você pode adicionar um período de cortesia a uma sessão de estacionamento para fins de fiscalização leniente. Após o término do tempo pago ou do tempo de conveniência do veículo, o período de cortesia é o tempo extra dado antes de uma sessão de estacionamento ser identificada como uma *Violação*.
- **Tempo máximo da sessão:** Definir um tempo máximo da sessão ajuda a melhorar as estatísticas de ocupação de estacionamentos. Quando um veículo excede o tempo máximo da sessão, presume-se que a placa do veículo não foi lida à saída e que o veículo já não se encontra na zona de estacionamento. A sessão de estacionamento aparece em relatórios gerados a partir da tarefa *Sessões de estacionamento* com o *Motivo do estado: tempo máximo da sessão excedido*.
- **Tempo pago:** A etapa de tempo pago de uma sessão de estacionamento começa quando o *tempo de conveniência* expira. Os proprietários de veículos podem adquirir tempo de estacionamento através de uma estação de pagamento ou um aplicativo móvel e o sistema de pagamento pode ser fornecido por provedores terceiros de autorização de estacionamento integrados.
- **Regra de estacionamento:** Uma regra de estacionamento define como e quando uma sessão de estacionamento é considerada como sendo válida ou uma violação.
- **Estados da sessão de estacionamento:** A sessão de estacionamento de um veículo é dividida em quatro estados: *Válido* (incluindo tempo de conveniência, tempo pago e período de cortesia), *Violação*, *Fiscalizado* e *Concluído*. Quando um veículo estaciona em uma zona de estacionamento, a sua sessão de estacionamento progride pelos estados da sessão de estacionamento com base no tempo configurado para a regra de estacionamento, a validade do tempo pago e se a sessão de estacionamento do veículo incorre em violação.
- **Zona de estacionamento:** As zonas de estacionamento que você define no Security Center representam estacionamentos fora da rua cujas entradas e saídas são monitoradas por câmeras Sharp.
- **Capacidade da zona de estacionamento:** A capacidade da zona de estacionamento é o número máximo de veículos que podem ser estacionados em uma zona de estacionamento.
- **Limite de capacidade da zona de estacionamento:** A definição de limite de capacidade da zona de estacionamento determina em que ponto um evento de *limite de capacidade atingido* é gerado. Por exemplo, se diminuir o limite para 90%, o sistema gera um evento quando a zona de estacionamento atinge a capacidade de 90%.

Estados da sessão de estacionamento

A sessão de estacionamento de um veículo é dividida em estados, para mostrar a progressão da visita de estacionamento do proprietário. Se você precisar monitorar e investigar zonas de estacionamento ou se você configurar zonas e regras de estacionamento, é importante entender como uma sessão de estacionamento progride por esses estados.

Quando um veículo estacionar em uma zona de estacionamento, os estados pelos quais uma sessão de estacionamento passa depende de haver ou não uma violação de estacionamento. O seguinte diagrama mostra os estados possíveis de uma sessão de estacionamento:



- **Válido:** Um sessão de estacionamento passa para o estado *válido* porque:
  - A placa do veículo é lida na entrada da zona de estacionamento.
    NOTA: Dependendo de como a regra de estacionamento for configurada, o estado *válido*pode incluir *tempo de conveniência*, *tempo pago* e *período de cortesia*.
- **Violação:** Um sessão de estacionamento passa para o estado *violação* porque:
  - O tempo válido expira. Isso pode incluir uma combinação do *tempo de conveniência*, *tempo pago* e *período de cortesia* que são configurados para a regra de estacionamento.
- **Imposto:** Um sessão de estacionamento passa para o estado *imposto* porque:
  - O operadora de estacionamento impõe manualmente a violação no Security Desk.
- **Concluído:** Um sessão de estacionamento passa para o estado *concluído* porque:
  - O veículo sai da zona de estacionamento. O estado da zona de estacionamento é *concluído* não importa em que estado esteja quando o veículo sai da zona de estacionamento.
  - O inventário da zona de estacionamento é atualizado.
  - O veículo entra novamente na zona de estacionamento. Isso pode indicar que na sessão de estacionamento anterior do veículo, a placa não foi lida na saída da zona de estacionamento.
  - O veículo excedeu o *tempo máximo da sessão* que está definido para a zona de estacionamento.

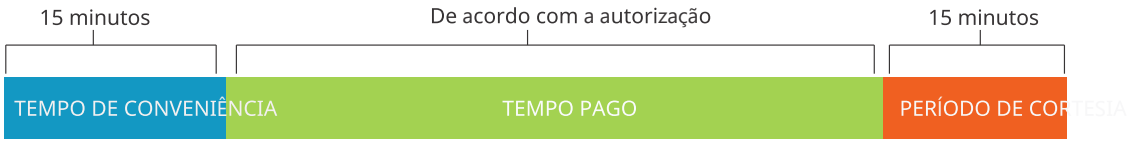
Cenários de estacionamento comuns para AutoVu™ Free-Flow

Ao usar o recurso AutoVu™ Free-Flowno Security Center, você pode personalizar o sistema para atender aos requisitos de suas regras de estacionamento.

Os seguintes exemplos mostram como o AutoVu™ Free-Flow pode ser usado para se adequar a cenários de estacionamento comuns.

Estacionamento temporário

No cenário de *estacionamento temporário*, quando o veículo entra no estacionamento, o proprietário deve imediatamente comprar tempo de estacionamento.

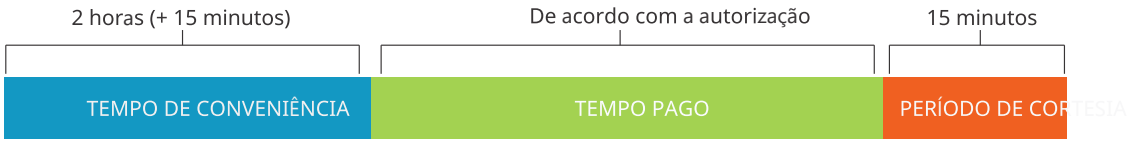


Sobre este cenário:

- Um *tempo de conveniência* curto pode ser adicionado para permitir que o proprietário do veículo tenha tempo para encontrar uma vaga de estacionamento e comprar o tempo de estacionamento.
- Se o proprietário não tiver comprado o tempo de estacionamento ao fim dos 15 minutos do tempo de conveniência e do período de cortesia, a sessão de estacionamento será sinalizada como uma *Violação*.
- Se o proprietário comprar o tempo de estacionamento, mas exceder o tempo comprado e o período de cortesia, o veículo será sinalizado como uma *violação*.

Estacionamento temporário com um período de estacionamento grátis

No cenário de estacionamento temporário, os veículos podem estacionar sem uma permissão durante as primeiras 2 horas. Se o proprietário do veículo planeja estacionar o veículo no estacionamento durante mais de 2 horas, o tempo de estacionamento deve ser comprado.

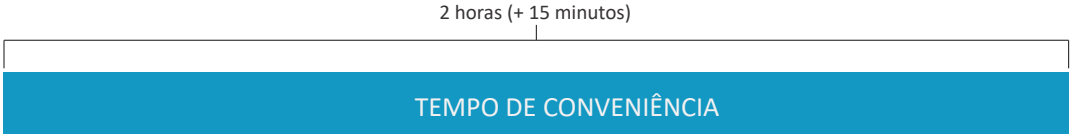


Sobre este cenário:

- O tempo de conveniência é configurado para 2 horas.
- Se o proprietário não tiver comprado o tempo de estacionamento ao fim das 2 horas do tempo de conveniência e dos 15 minutos do período de cortesia, a sessão de estacionamento será sinalizada como uma *Violação*.
- Se o proprietário comprar o tempo de estacionamento, mas exceder o tempo comprado e o período de cortesia, o veículo será sinalizado como *uma violação*.

Estacionamento em tempo extra

Em um cenário de *tempo extra*, qualquer veículo pode estacionar durante, no máximo, 2 horas. Os motoristas podem comprar um tempo de estacionamento adicional.

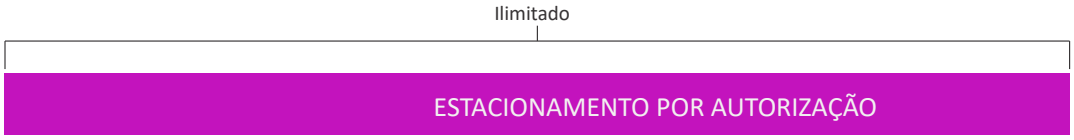


Sobre este cenário:

- O tempo de conveniência é configurado para 2 horas.
- Se o proprietário estacionar o carro durante mais de 2 horas do tempo de conveniência e de 15 minutos do período de cortesia, a sessão de estacionamento será sinalizada como uma *Violação*.

Estacionamento autorizado contratual

No cenário de *estacionamento autorizado contratual*, somente os motoristas com autorizações mensais podem estacionar em uma zona de estacionamento. Uma lista de permissões é usada para conceder aos titulares de autorização acesso à zona de estacionamento.

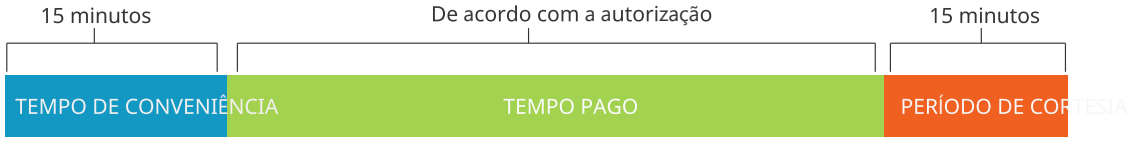


Sobre este cenário:

- Como não há tempo pago, a regra de estacionamento inclui apenas o padrão mínimo de 1 minuto, e não está configurado um período de cortesia.
- Ao usar esta configuração, você pode monitorar o tempo que cada veículo permanece na zona de estacionamento.

Autorização estática e estacionamento temporário

Neste cenário, uma *lista de permissões* é usada para conceder aos titulares de autorizações acesso à zona de estacionamento e, quando um veículo desconhecido entra no estacionamento, o motorista deve comprar imediatamente o tempo de estacionamento.



Sobre este cenário:

- O estacionamento temporário está configurado como no exemplo *Estacionamento temporário com um período de estacionamento grátis*.
- Para sessões de estacionamento que usam uma autorização estática Pay-by-Plate Sync, a autorização estática segue o mesmo tempo de conveniência e período de cortesia configurados para a regra de estacionamento temporário. Contudo, uma vez que não se aplicam a autorizações temporárias, a autorização não entrará em violação, contanto que a autorização seja válida.

Eventos de zona de estacionamento

Durante a sessão de estacionamento de um veículo, vários eventos e eventos secundários são acionados com base nas regras de estacionamento que são aplicadas à zona de estacionamento.

- **Eventos:** Os administradores podem usar eventos para criar eventos causa-efeito para a zona de estacionamento. Por exemplo, você pode configurar um evento causa-efeito que envia um e-mail ou aciona um alarme quando um evento de *violação detectada* é gerado.

- **Eventos secundários:** Os eventos secundários aparecem no relatório *Atividades da zona de estacionamento* do Security Desk. Você pode filtrar o relatório por eventos secundários específicos, mas não pode incluir eventos secundários em um evento causa-efeito.

Os seguintes eventos e eventos secundários estão disponíveis:

Eventos	Eventos secundários
Limite de capacidade atingido	Não se aplica
Tempo de gratuidade iniciado	Não se aplica
Período de gratuidade iniciado	• Tempo de conveniência expirado • Tempo pago inválido
Inventário redefinido	Não se aplica
Tempo pago iniciado	• Tempo pago válido • Não é possível validar o tempo pago
Sessão concluída	• Inventário redefinido • O tempo máximo de sessão expirou • Veículo desconhecido saiu • Veículo saiu • Veículo entrou novamente • Leitura editada • Regra excluída
Sessão iniciada	• Veículo desconhecido saiu • Veículo entrou
Validando tempo pago	• Tempo de conveniência expirado • Tempo pago expirado • Leitura editada
Violação detectada	• Tempo de conveniência expirado • Período de gratuidade expirado • Tempo pago inválido • A autorização compartilhada corresponde
Violação forçada	Não se aplica

Configurar o AutoVu™ Free-Flow

Para usar o AutoVu™ Free-Flow, você deve definir configurações gerais que definem como o sistema processa leituras de placas de veículo e como o AutoVu™ Free-Flow trabalha com o Pay-by-Plate Sync.

O que você deve saber

Para usar o AutoVu™ Free-Flow, você deve também configurar regras de estacionamento e zonas de estacionamento.

Para configurar o AutoVu™ Free-Flow:

1 Na página inicial do Config Tool, clique em **Sistema > Funções**.

2 Selecione o **LPR Manager** que deseja configurar e, em seguida, clique na aba **Propriedades**.

3 Selecione **Free-Flow**.

4 Configure a correspondência de placas.

- **Corresponder o limite de tolerância:** Este valor indica o número de diferenças de caractere simples entre leituras de placa de entrada e saída que serão ainda consideradas uma correspondência. Definir o valor para 0 é equivalente a uma correspondência exata.

  IMPORTANTE: Definir para um valor demasiado elevado faz com que leituras de placa sejam associadas ao veículo errado. O valor padrão é 1.

5 (Opcional) Defina as configurações de Pay-by-Plate Sync se estiver usando um provedor terceiro de pagamentos.

- **Servidor:** Digite o endereço IP da máquina onde o Pay-by-Plate Sync está instalado.
- **Porta:** Digite o número de porta para a conexão do Pay-by-Plate Sync (padrão: 8787).

6 (Opcional) Defina as configurações de exportação XML se estiver enviando leituras de placas para um sistema terceiro.

- **Pasta de exportação XML:** Especifique a pasta de exportação para dados XML do AutoVu™ Free-Flow.
- **Incluir imagens do veículo na exportação:** Por padrão, as imagens de veículos não são incluídas em arquivos XML exportados.

  NOTA: Incluir imagens de veículos aumenta o tamanho do arquivo de exportação XML.
- **Exportar ocupação:** Exporta dados de ocupação de zona de estacionamento para um arquivo XML separado.

  NOTA: É exportado um único arquivo XML para todas as zonas de estacionamento. Este arquivo é sobrescrito uma vez por minuto.

  O seguinte é um exemplo de um arquivo XML de ocupação:

```
<?xml version="1.0" encoding="utf-8"?>
<OccupancyExport>
  <RoleId>8817e652-a9ca-4d06-81d7-8db93b5e3819</RoleId>
  <RoleName>LPR Manager</RoleName>
  <ParkingOccupancies>
    <Occupancy>
      <Capacity>100</Capacity>
      <ParkingZoneId>293b9997-19ac-4fd9-99a4-c713fbbe1b96</ParkingZoneId>
      <ParkingZoneName>P1</ParkingZoneName>
      <TimestampUtc>2017-04-05T20:15:00Z</TimestampUtc>
      <Vehicles>5</Vehicles>
      <Violations>1</Violations>
      <EnforcedVehicles>0</EnforcedVehicles>
    </Occupancy>
    <Occupancy>
      <Capacity>200</Capacity>
      <ParkingZoneId>9dab3ef5-197f-4a33-87ae-e85dfa01c0b2</ParkingZoneId>
      <ParkingZoneName>P2</ParkingZoneName>
```

```
      <TimestampUtc>2017-04-05T20:15:00Z</TimestampUtc>
      <Vehicles>4</Vehicles>
      <Violations>0</Violations>
      <EnforcedVehicles>0</EnforcedVehicles>
    </Occupancy>
  </ParkingOccupancies>
</OccupancyExport>
```

- **Exportar violações:** Quando um veículo está em violação, as informações do veículo são exportadas como um arquivo XML separado.

  O seguinte é um exemplo de um arquivo XML de violações:

```
<?xml version="1.0" encoding="utf-8"?>
<InLotViolation>
  <ParkingZoneName>P1</ParkingZoneName>
  <ParkingRuleName>Default parking rule</ParkingRuleName>
  <ParkingZoneId>293b9997-19ac-4fd9-99a4-c713fbbe1b96</ParkingZoneId>
  <SessionId>e6abdbb3-3b1a-e711-8b70-001018e35f7c</SessionId>
  <ParkingRuleId>09e29d39-83da-4cdc-81cc-0191833cb9a6</ParkingRuleId>
  <EntranceRead>
    <DeviceId>1775e575-af23-4387-9546-23ab6c67e619</DeviceId>
    <PlateNumber>L8NJI4</PlateNumber>
    <PlateState>DP</PlateState>
    <ReadId>e4063dad-8264-410b-a50a-c3fdc9375e5c</ReadId>
    <ReadTimestampUtc>2017-04-05T20:08:57.7919418Z</ReadTimestampUtc>
    <UnitId>95b71795-735e-497d-8955-5acc3a0c9388</UnitId>
  </EntranceRead>
  <ViolationReason>ConvenienceTimeExpired</ViolationReason>
  <TimestampUtc>2017-04-05T20:09:57.7919418Z</TimestampUtc>
</InLotViolation>
```

- **Exportar sessões concluídas:** Quando um veículo sai do parque de estacionamento, as informações da sessão de estacionamento são exportadas como um arquivo XML separado.

  O seguinte é um exemplo de um arquivo XML de sessões concluídas.

```
<?xml version="1.0" encoding="utf-8"?>
<ParkingSessionCompleted>
  <ParkingZoneName>P1</ParkingZoneName>
  <ParkingRuleName>Default parking rule</ParkingRuleName>
  <ParkingZoneId>293b9997-19ac-4fd9-99a4-c713fbbe1b96</ParkingZoneId>
  <SessionId>e6abdbb3-3b1a-e711-8b70-001018e35f7c</SessionId>
  <ParkingRuleId>09e29d39-83da-4cdc-81cc-0191833cb9a6</ParkingRuleId>
  <EntranceRead>
    <DeviceId>1775e575-af23-4387-9546-23ab6c67e619</DeviceId>
    <PlateNumber>L8NJI4</PlateNumber>
    <PlateState>DP</PlateState>
    <ReadId>e4063dad-8264-410b-a50a-c3fdc9375e5c</ReadId>
    <ReadTimestampUtc>2017-04-05T20:08:57.7919418Z</ReadTimestampUtc>
    <UnitId>95b71795-735e-497d-8955-5acc3a0c9388</UnitId>
  </EntranceRead>
  <ExitRead>
    <DeviceId>cefe75b2-7152-45a9-b657-07f10c2880cd</DeviceId>
    <PlateNumber>L8NJI4</PlateNumber>
    <PlateState>QC</PlateState>
    <ReadId>1670f981-7138-47e8-babd-d9e7ab631122</ReadId>
    <ReadTimestampUtc>2017-04-05T20:12:41.663817Z</ReadTimestampUtc>
    <UnitId>0b1a978f-8a45-45a3-9123-263a5f7004de</UnitId>
  </ExitRead>
  <StartTimestampUtc>2017-04-05T20:08:57.7919418Z</StartTimestampUtc>
  <ConvenienceTimestampUtc>2017-04-05T20:08:57.7919418Z</
ConvenienceTimestampUtc>
  <ViolationTimestampUtc>2017-04-05T20:09:57.7919418Z</ViolationTimestampUtc>
  <CompletedTimestampUtc>2017-04-05T20:12:41.663817Z</CompletedTimestampUtc>
  <ConvenienceTimeDuration>00:01:00</ConvenienceTimeDuration>
  <GracePeriodDuration>00:00:00</GracePeriodDuration>
  <PaidDuration>00:00:00</PaidDuration>
  <ViolationDuration>00:02:43.8718752</ViolationDuration>
  <EnforcedDuration>00:00:00</EnforcedDuration>
  <TotalDuration>00:03:43.8718752</TotalDuration>
  <CompletedReason>VehicleExited</CompletedReason>
```

```
</ParkingSessionCompleted>
```

7 Defina configurações de eventos.

- **Limite de capacidade:** Especifica o limite de capacidade da zona de estacionamento para o qual um evento de *limite de capacidade atingido* é gerado.

8 Clique em **Aplicar**.

Adicionar e configurar regras de estacionamento

As regras de estacionamento que definem como e quando um veículo pode ser estacionado podem variar significativamente entre zonas de estacionamento. As regras de estacionamento que você configurar podem ser atribuídas a uma ou mais zonas de estacionamento.

Antes de iniciar

Se você desejar incorporar sistemas terceiros de pagamento de estacionamento habilitado por placa de veículo, você deve instalar o plug-in Pay-by-Plate Sync em todos os servidores e estações de trabalho cliente que devem usar o plug-in. Para obter mais informações, consulte o *Guia do Plug-in Pay-by-Plate Sync*.

O que você deve saber

Os seguintes cenários de estacionamento são compatíveis:

- *Estacionamento em tempo extra* (por exemplo, estacionamento grátis até um máximo de 2 horas).
- *Estacionamento temporário* usando provedores de pagamento habilitados por Pay-by-Plate Sync.
- *Estacionamento contratado* uando autorizações Pay-by-Plate Sync.

Para adicionar uma nova regra de estacionamento:

1 Na página inicial do Config Tool, abra a tarefa *LPR* e clique em **Regras de estacionamento**.

2 Clique em **Regra de estacionamento** ( ).

3 Na aba *Identidade*, renomeie a sua regra de estacionamento e adicione **Descrição** e **ID lógico** (opcional).

4 Você pode definir **Relações** para vincular zonas de estacionamento e ações à sua regra de estacionamento.

5 Na aba **Propriedades**, configure o seguinte:

- **Tempo de conveniência:** O tempo de conveniência é um tempo de leniência configurável que é aplicável antes de um veículo começar a ser cobrado após entrar na zona de estacionamento. Por exemplo, se você precisar configurar um período de estacionamento grátis de 2 horas que é aplicável antes de o tempo pago ou a fiscalização de estacionamento entrar em vigor, você deverá definir do tempo de conveniência para 2 horas. Para estacionamentos onde a fiscalização de estacionamento começa imediatamente, você precisaria definir um breve tempo de conveniência para dar tempo aos proprietários dos veículos encontrarem um lugar de estacionamento e adquirirem tempo de estacionamento antes que a fiscalização de estacionamento comece.

  NOTA:

  - Se estiver configurando um estacionamento que utiliza autorizações, você pode definir o tempo de conveniência para 10 minutos. Isso dá aos clientes tempo suficiente para estacionar e comprar uma autorização antes de entrarem em violação. Você também pode conceder tolerância ao cliente na saída configurando um período de cortesia.
  - Se estiver configurando um estacionamento que é grátis, mas com um limite de tempo de 1 hora, você deve configurar um tempo de conveniência de 1 hora. Observe que este cenário não utiliza autorizações de estacionamento de terceiros e não exige o plug-in Pay-by-Plate Sync.

- **Período de tolerância:** Um período de cortesia pode ser adicionado a uma sessão de estacionamento para efeitos de imposição de tolerância. Após o vencimento do tempo de estacionamento do veículo, é dado tempo extra antes de a sessão de estacionamento de um veículo ser identificada como violação.

6 Se o seu sistema usa o plug-in Pay-by-Plate Sync para incorporar sistemas de pagamento de terceiros, ative o recurso e configure o seguinte:

- **Autorização:** Selecione a autorização Pay-by-Plate Sync que deseja aplicar.
- **Atraso padrão da expiração:** É recomendado que você configure uma *EffectiveDate* e uma *ExpiryDate* para autorizações Pay-by-Plate Sync (se compatível com os provedores de pagamento). Isso reduz

o volume de consultas para os provedores terceiros. O *Atraso padrão da expiração* é usado para autorizações que não incluem uma expiração. Neste caso, o AutoVu™ Free-Flow verifica junto do provedor de autorização de estacionamento se a autorização permanece válida. Aumentar este valor reduz a frequência das verificações de autorização. Por exemplo, se o estacionamento mudar para estacionamento em incrementos de 15 minutos, você pode definir o *Atraso padrão da expiração* para 15 minutos.

Para obter mais informações sobre os atributos *EffectiveDate* e *ExpiryDate*, consulte as instruções sobre como criar autorizações Security Center no *Guia do Plug-in Pay-by-Plate Sync*.

- **Tempo de conveniência e período de cortesia:** Ao utilizar Pay-by-Plate Sync para estacionamento temporário, você também pode configurar tempo de conveniência e um período de cortesia para efeitos de imposição de tolerância.

Adicionar e configurar zonas de estacionamento

Para gerenciar estacionamentos físicos no Security Center usando o AutoVu™ Free-Flow, você deve primeiro definir zonas de estacionamento e atribuir câmeras Sharp como câmeras de entrada ou saída.

Antes de iniciar

- Adicione as câmeras Sharp que estão monitorando a zona de estacionamento ao LPR Manager.
- Para tornar o feed de vídeo disponível, adicione as câmeras Sharp que estão monitorando a zona de estacionamento ao Archiver.
- Crie uma regra de estacionamento.

Para adicionar uma nova zona de estacionamento

1 Na página inicial de Config Tool, clique na tarefa *Exibição de área*.
2 Na árvore de entidades, clique na área à qual deseja anexar a zona de estacionamento.
3 Clique em **Adicionar uma entidade** () e selecione **Zona de estacionamento**.
Uma nova zona de estacionamento é adicionada abaixo da área.

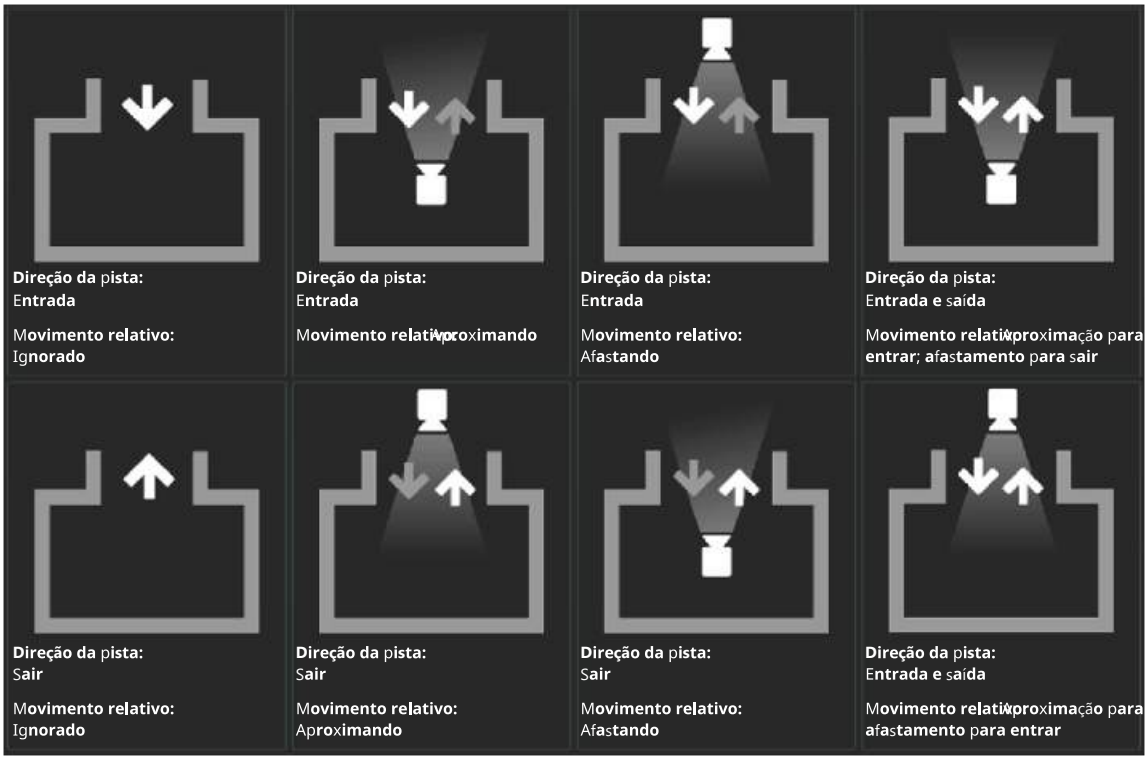
Para configurar a zona de estacionamento:

1 Na aba *Identidade*, renomeie a sua regra de estacionamento e adicione **Descrição** e **ID lógico** (opcional).
2 Clique na aba **Propriedades** da zona de estacionamento.
3 Na lista suspensa **LPR Manager**, selecione o LPR Manager ao qual a zona de estacionamento está atribuída.

ADVERTÊNCIA: Se você eliminar um LPR Manager, todas as zonas de estacionamento atribuídas a ele são também excluídas e todos os dados de estacionamento relacionados são perdidos.

NOTA: Somente as câmeras Sharp associadas ao LPR Manager selecionado ficam disponíveis para monitorar a zona de estacionamento.

4 Na seção **Câmeras de LPR**, clique em **Adicionar um item** (). Selecione as câmeras Sharp que estão instaladas na zona de estacionamento e clique em **OK**.
5 Para cada câmera Sharp que esteja monitorando a zona de estacionamento, você deve especificar se a pista monitorada é uma saída, uma entrada ou se a pista serve tanto de entrada como saída.



Defina a direção da pista usando o seguinte parâmetro:

Direção da pista:

- **Entrada:** A câmera Sharp está monitorando uma pista de entrada do estacionamento.
- **Saída:** A câmera Sharp está monitorando uma pista de saída do estacionamento.
- **Entrada e saída:** Uma câmara Sharp pode detectar se um veículo está se aproximando ou afastando dela. Como resultado, se os veículos tiverem uma placa de veículo dianteira e traseira, você pode usar uma única câmera Sharp para monitorar uma pista que é usada como entrada e saída de uma zona de estacionamento.

6 Para cada câmera Sharp que esteja monitorando a zona de estacionamento, você deve especificar a direção em que o trânsito se move em relação à câmera.

Defina o movimento relativo usando o seguinte parâmetro:

Movimento relativo: Uma câmera Sharp pode detectar se um veículo está se aproximando ou afastando dela. Usando esta informação, a zona de estacionamento pode ignorar veículos que passem em determinada direção.

IMPORTANTE: Somente filtre por movimento relativo se necessário. Se você posicionar a câmera de modo que somente uma pista esteja visível, e a pista apenas tiver uma direção de passagem, não é necessário usar o recurso de movimento relativo. Para obter mais informações sobre como definir uma região de interesse, consulte o *Guia do Administrador Sharp*.

As seguintes opções estão disponíveis se você selecionar a direção de uma pista como **Entrada** ou **Saída**.

- **Ignorado:** Use esta opção se somente uma pista estiver visível na imagem de contexto com apenas uma direção de passagem.
- **Aproximando:** Se a câmera puder detectar veículos passando em ambas as direções, use esta definição para somente registrar veículos se eles estiverem se aproximando da câmera ou se a direção de passagem não puder ser detectada.
- **Afastando:** Se a câmera puder detectar veículos passando em ambas as direções, use esta definição para somente registrar veículos se eles estiverem se afastando da câmera ou se a direção de passagem não puder ser detectada.

As seguintes opções estão disponíveis se você selecionar a direção de uma pista como **Entrada e saída**.

- **Aproximação para entrar:** Use esta opção se uma câmera for usada para detectar veículos entrando e saindo e se os veículos se aproximam da câmera à medida que entram no estacionamento.
- **Aproximação para sair:** Use esta opção se uma câmera for usada para detectar veículos entrando e saindo e se os veículos se aproximam da câmera à medida que saem no estacionamento.

7 Na seção **Definição**, configure os seguintes parâmetros para o estacionamento:

- **Capacidade:** O número de vagas físicas no estacionamento.

  NOTA: A capacidade da zona de estacionamento funciona em conjunto com a definição *Limiar de capacidade* do LPR Manager. Quando o limiar de capacidade é alcançado, um evento de *limiar de capacidade alcançado* é gerado.
- **Tempo máximo da sessão:** Este é o período de tempo antes de se considerar que a *sessão de estacionamento* de um veículo excedeu o limite de permanência no *zona de estacionamento*. A partir deste ponto, presume-se que a placa do veículo não foi lida à saída e que o veículo já não se encontra na zona de estacionamento. O veículo deixa de aparecer em relatórios de sessão de estacionamento criados na tarefa Security Desk do *Sessões de estacionamento*.
- **Regra de estacionamento:** Selecione uma regra de estacionamento para aplicar à zona de estacionamento.

  Para saltar para a página de configuração de uma regra de estacionamento, selecione a regra e clique em  .

8 Na seção **Aplicação**, defina os seguintes parâmetros para o estacionamento:

- **Lista de procurados por violação:** Selecione uma lista de procurados a ser preenchida com as informações de veículos cujas sessões de estacionamento chegaram a um estado de *Violação*. A lista de procurados selecionada é atualizada a cada minuto e pode ser usada para impor violações usando um veículo Genetec Patroller™.

9 Clique em **Aplicar**.

Após terminar

(Opcional) A certa altura (por exemplo, quando o estacionamento fecha), você pode assumir que todas as sessões de estacionamento terminaram e que todos os veículos que permanecem na zona de estacionamento foram multados ou devem ser rebocados. Você pode redefinir o inventário de zonas de estacionamento usando a ação *Redefinir inventário de zonas de estacionamento*.

Tópicos relacionados

Configurar estacionamentos no Security Center na página 901

Vincular câmeras a zonas de estacionamento

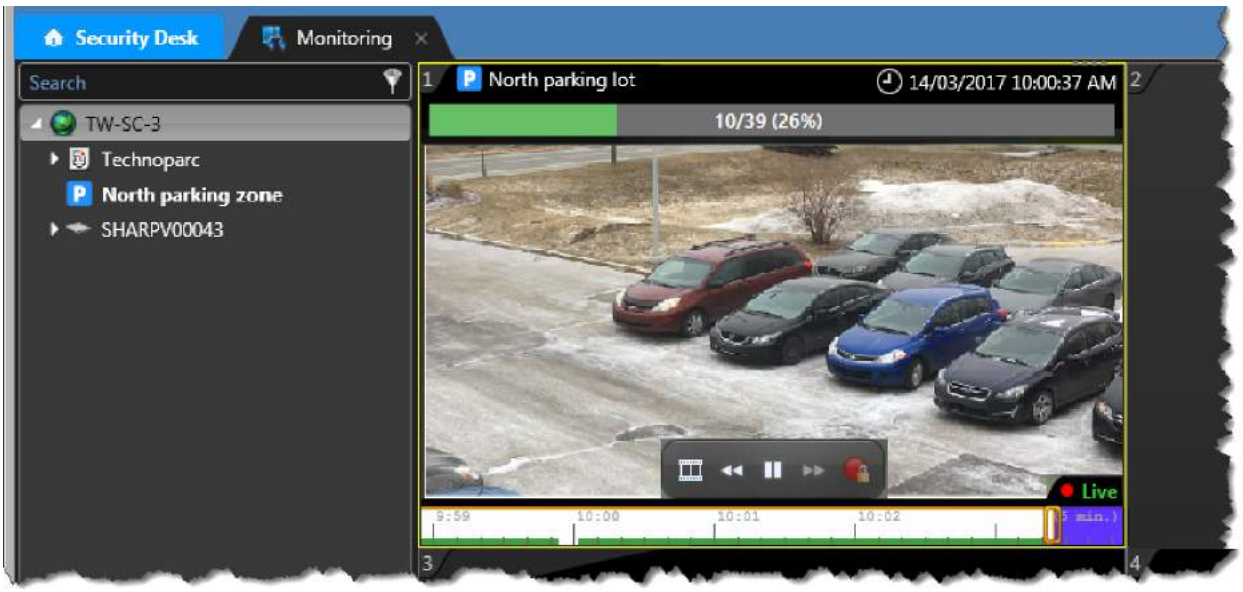
Para além das câmeras Sharp que leem as placas dos veículos que entram numa zona de estacionamento, você pode também associar uma ou mais câmeras de vídeo adicionais à zona de estacionamento. Isto permite que o operador vigie e também monitore a ocupação da zona de estacionamento.

Antes de iniciar

- Crie uma zona de estacionamento.

O que você deve saber

Quando vincula câmeras a uma zona de estacionamento, as informações de ocupação da zona de estacionamento são exibidas como um gráfico de barras acima do feed de vídeo na tarefa *Monitoramento*.



Para monitorar uma zona de estacionamento com câmeras, você deve ter uma das seguintes configurações Security Center:

- Uma função Archiver com câmeras disponíveis.
- Uma função Omnicast™ Federation™ para conexão a um sistema Omnicast™ externo.
- Uma função Security Center Federation™ para conexão a um sistema Security Center externo com câmeras.

Para vincular uma câmera a uma zona de estacionamento:

1 Na página inicial de Config Tool, clique na tarefa *Exibição de área*.
2 Na árvore de entidades, clique na zona de estacionamento à qual deseja vincular câmeras.
3 Na seção *Relacionamentos* da aba **Identidade**, selecione **Câmeras**.
4 Clique em **Adicionar um item** ( ).
5 Na janela de **Pesquisa**, clique na entidade de câmera que deseja adicionar e, em seguida, clique em **Selecionar**.
6 Clique em **Aplicar**.
7 Na seção *Relacionamentos* da aba *Identidade*, expanda **Câmeras** e verifique se a câmera foi adicionada.

Como a ocupação da zona é calculada

À medida que as câmeras Sharp detectam veículos entrando e saindo de uma zona de estacionamento, o sistema AutoVu™ Free-Flow calcula a ocupação da zona de estacionamento. Você pode depois exibir estas informações em ladrilhos de tarefas de *Monitoramento* no Security Desk.

Evento	Contagem de veículos
O veículo entra Isto pode incluir veículos com: • Leituras de placas de veículo precisas • Placas de veículos que não são corretamente lidas • Leituras NOPLATE • Placas de veículos que não foram capturadas à saída da zona de estacionamento e que estão reentrando na zona de estacionamento	A ocupação da zona de estacionamento aumenta um valor.
O veículo sai Isto pode incluir veículos com: • Leituras de placas de veículo precisas • Placas de veículos que não são corretamente lidas • Leituras NOPLATE • Veículo desconhecido saiu (indicando que a leitura de saída não corresponde à leitura de entrada)	A ocupação da zona de estacionamento diminui um valor.
Redefinição de inventário Você pode redefinir o inventário de uma zona de estacionamento usando a ação *Redefinir inventário de zona de estacionamento*. Esta ação pode ser desencadeada por uma *ação instantânea* ou uma *tarefa agendada*. Para obter mais informações sobre ações instantâneas, consulte o *Guia do Usuário do Security Desk*.	A ocupação da zona de estacionamento é zerada.

NOTA: Se uma sessão de estacionamento for fechada devido ao tempo máximo da sessão ter sido excedido, a contagem de ocupação da zona de estacionamento não sofre alterações.

Como a edição de leituras de placas afeta sessões de estacionamento e a ocupação da zona de estacionamento

- **Editar uma leitura de placa de entrada:**
  - Se você editar a leitura de placa de entrada de um veículo que tenha uma sessão de estacionamento ativa, a sessão de estacionamento é atualizada com o número de placa correto. Neste caso, a ocupação da zona de estacionamento não é afetada. Se o sistema usar autorizações de estacionamento Pay-by-Plate Sync, o estado de *tempo pago*, *violação* ou *período de cortesia* da sessão de estacionamento é reavaliada com Pay-by-Plate Sync.

- Se a placa de um veículo for lida incorretamente ao entrar na zona de estacionamento, uma sessão de estacionamento é criada e a ocupação da zona de estacionamento é aumentada. Neste caso, você deve editar a leitura de placa de entrada antes que o veículo abandone a zona de estacionamento ou antes que a sessão de estacionamento exceda o *tempo máximo da sessão* porque, nesse momento, a sessão está fechada e atualizar a leitura de placa não atualiza a sessão de estacionamento. No entanto, esta situação não afeta a ocupação. Quando a placa do veículo é lida corretamente à saída da zona de estacionamento, o veículo será sinalizada como um *veículo desconhecido* e a ocupação da zona de estacionamento é reduzida.
- Se a leitura de entrada for uma leitura NOPLATE, o veículo é incluído na ocupação da zona de estacionamento, mas não é criada uma sessão de estacionamento. Editar a leitura cria uma sessão de estacionamento para o veículo e a autorização é avaliada com base na hora de entrada do veículo.

- **Editar uma leitura de placa de saída:**
  - Se você editar uma leitura de placa de saída que corresponda ao número de placa de uma sessão de estacionamento ativa, o sistema fecha a sessão e a ocupação da zona de estacionamento é atualizada em conformidade.
  - Quando uma leitura NOPLATE é gerada à saída de uma zona de estacionamento, a contagem de ocupação para essa zona é reduzida. Se esse evento for editado para um número de placa que corresponda a uma sessão ativa na zona de estacionamento, a sessão de estacionamento é fechada porque sabemos que a leitura NOPLATE é do mesmo veículo.

Recomendações para melhoria das métricas da ocupação de zona de estacionamento

Para garantir que as métricas da ocupação de zona de estacionamento AutoVu™ Free-Flow são precisas, você pode criar alertas para notificar os operadores de zonas de estacionamento quando um reconhecimento de placa de veículo precisa ser editado. Você pode também automatizar a redefinição de inventário da zona de estacionamento.

Ao usar o AutoVu™ Free-Flow, nós recomendamos que você configure as seguintes ações:

Configurar eventos causa-efeito para baixos níveis de confiança e leituras NOPLATE

Para assegurar que a ocupação da zona de estacionamento é precisa, é importante que os operadores editem todas as leituras de placas NOPLATE (se habilitado no Sharp) e leituras de placa com baixo nível de confiança. Recomenda-se que você configure *eventos causa-efeito* para notificar operadores quando uma leitura de placa deve ser editada.

- **Nível de confiança:** Criar um evento causa-efeito usando *Quando: reconhecimento de placas de veículos* com *E: [nível de confiança] < 50*.

  NOTA: Um nível de confiança aceitável depende do ambiente e do contexto LPR usado.
- **NOPLATE:** Criar um evento causa-efeito usando *Quando: Reconhecimento de placas de veículos* com *E: [PlateNumber] = "NOPLATE"*.

Configure uma tarefa agendada para redefinir o inventário da zona de estacionamento

A certa altura durante o dia (por exemplo, quando o estacionamento fecha), você pode assumir que todas as sessões de estacionamento terminaram e que todos os veículos que permanecem na zona de estacionamento foram multados ou devem ser rebocados. Você pode redefinir o inventário de zonas de estacionamento criando uma *tarefa agendada* com a *Ação: redefinir inventário de zonas de estacionamento*.

Sobre autorizações compartilhadas no AutoVu™ Free-Flow

Se o seu sistema AutoVu™ Free-Flow estiver configurado para permitir autorizações de estacionamento compartilhadas, então a mesma autorização de estacionamento pode ser associada a vários veículos. As autorizações compartilhadas são geralmente usadas se o proprietário da autorização possuir mais de um veículo, ou para motoristas que fazem carona solidária.

As autorizações compartilhadas são aplicadas a um veículo de cada vez. Por exemplo, se os quatro membros de uma carona solidária que compartilham uma autorização decidirem dirigir seus próprios veículos em determinado dia, somente o primeiro veículo que entrar na zona de estacionamento poderia estacionar usando a autorização. Os outros três veículos gerariam ocorrências de *autorização compartilhada* se entrassem na zona de estacionamento enquanto o primeiro veículo está estacionado.

Usar Pay-by-Plate Sync

Considere o seguinte ao configurar autorizações compartilhadas:

- Para usar autorizações compartilhadas, as autorizações devem ser de um provedor terceiro de autorizações de estacionamento que use o plug-in Pay-by-Plate Sync. Você pode definir autorizações estáticas para veículos no Security Center, mas essas autorizações não podem ser compartilhadas entre veículos.
- Para usar este recurso, o provedor de autorizações Pay-by-Plate Sync deve suportar autorizações compartilhadas.
- Considera-se que os veículos compartilham uma autorização se eles tiverem o mesmo ID de autorização. Por esse motivo, certifique-se de que todas as autorizações tenham um ID de autorização exclusivo. Se duas autorizações compartilharem o mesmo ID de autorização quando este recurso é habilitado, elas podem gerar ocorrências de autorização compartilhada.

Como funcionam as autorizações compartilhadas

1 Quando um veículo entra numa zona de estacionamento, o sistema inicia uma sessão de estacionamento para o veículo e valida a autorização de estacionamento associada à placa de veículo.

NOTA: Se a câmara Sharp ler incorretamente determinados caracteres da placa do veículo, o sistema continua a poder associar a placa do veículo à autorização de estacionamento. O sistema faz isso usando uma técnica de equivalência de LPR que somente exige cinco caracteres comuns e quatro caracteres adjacentes.

2 O sistema compara o *ID de autorização* com veículos que já estão na zona de estacionamento.

- Se nenhuma outra placa de veículo compartilhar o mesmo ID de autorização, a etapa de tempo pago da sessão de estacionamento é iniciada.
- Se uma outra placa de estacionamento compartilhar o mesmo ID de autorização, então a sessão de estacionamento entra em violação.
- Se a placa de estacionamento não tiver uma autorização, então o tempo de conveniência da sessão de estacionamento é iniciado.
- Se o sistema não conseguir comunicar com o provedor de autorização Pay-by-Plate Sync para validar a autorização, o tempo de conveniência da sessão de estacionamento é iniciado. O sistema tenta validar a autorização novamente no final da sessão de estacionamento do veículo.

Habilitar autorizações de estacionamento compartilhadas

Em um sistema de estacionamento AutoVu™ Free-Flow, para usar a mesma autorização de estacionamento para mais de um veículo, você deve habilitar autorizações compartilhadas no Security Center.

O que você deve saber

- Quando você habilita autorizações compartilhadas, a configuração é aplicada a todas as zonas de estacionamento que estão configuradas no Security Center.
- Para usar autorizações compartilhadas, as autorizações devem ser de um provedor terceiro de autorizações de estacionamento que use o plug-in Pay-by-Plate Sync. Você pode definir autorizações estáticas para veículos no Security Center, mas essas autorizações não podem ser compartilhadas entre veículos.
- Para usar este recurso, o provedor de autorizações Pay-by-Plate Sync deve suportar autorizações compartilhadas.

Para habilitar autorizações compartilhadas:

1 Inicie o aplicativo **Security Center Server Admin** ( ).
2 Digite a senha do servidor que definiu durante a instalação do servidor e clique em **Log on**.
A página *Visão geral* de Server Admin é exibida.
3 Selecione o seu servidor na lista suspensa *Servidores*.
4 Na lista suspensa *Ações*, selecione **</> Console**.
5 Selecione a aba *Comandos*.
6 Na lista de comandos, expanda **Comandos de gerenciamento de estacionamento**.
7 Clique em uma das seguintes opções para executar o comando associado:
   - **Desabilitar o recurso de autorizações compartilhadas:** Desabilitar este recurso desativa o processamento de ocorrências de autorização compartilhada. Os veículos com o mesmo ID de autorização não são considerados violação.
   - **Habilitar o recurso de autorizações compartilhadas:** Habilitar este recurso ativa o processamento de ocorrências de autorização compartilhada nas zonas de estacionamento que tenham a mesma entidade de autorização Pay-by-Plate Sync. Os veículos com o mesmo ID de autorização são considerados violação.

     DICA: Executar o comando **Configurações do módulo de impressão** exibe o status atual de várias configurações, incluindo o recurso de autorizações compartilhadas.

Atribuir um mapa a uma zona de estacionamento

Quando atribui um mapa a uma zona de estacionamento, você dá a essa entidade uma representação em mapa que pode ser usada para fins de monitoramento. Você pode atribuir um mapa a uma zona de estacionamento na tarefa *Exibição de área* ou na tarefa *Map designer* do Config Tool.

Antes de iniciar

Adicione e configure uma zona de estacionamento.

O que você deve saber

- Você pode adicionar uma entidade de zona de estacionamento (representada como um polígono) a um mapa existente. Você pode depois sobrepor a localização da entidade em um mapa geográfico.
- Você pode adicionar uma visualização drill-down a um mapa para que o operador possa, por exemplo, clicar em um estacionamento de vários pisos para ter uma visão de cada piso de estacionamento.
- Como alternativa a atribuir um mapa a uma zona de estacionamento, você pode também adicionar uma zona de estacionamento a um mapa.

Para atribuir um mapa a uma zona de estacionamento na tarefa *Exibição de área*:

1 Na página inicial de Config Tool, abra a tarefa *Exibição de área*.
2 Na árvore de entidades, selecione a zona de estacionamento à qual pretende atribuir um mapa.
3 Clique na aba **Identidade** e, em seguida, clique em **Criar mapa**.
4 Selecione um dos seguintes métodos para criar o plano de fundo do mapa.
   - **Imagem:** Importe o fundo do mapa de um arquivo de imagem.
   - **Geográfico:** Estabeleça conexão com um provedor de mapas.
5 Configure a visualização de mapa padrão e outras predefinições.
6 Configure as informações padrão a serem exibidas quando alguém abrir este mapa.
7 Clique em **Criar**.
8 Para adicionar uma câmera Sharp que esteja monitorando a zona de estacionamento, clique em **Exibição de área** ( ) e arraste a Câmera de LPR para o mapa.

Para atribuir um mapa a uma zona de estacionamento na tarefa *Map designer*:

1 Na página inicial do Config Tool, abra a tarefa *Map designer*.
   O assistente do Map designer exibe uma lista de mapas recentes.
2 Clique em **Criar** ( ).
3 Na árvore de áreas, selecione a zona de estacionamento para a qual está criando um mapa.
4 Clique em **Próximo**.
5 Selecione um dos seguintes métodos para criar o plano de fundo do mapa.
   - **Imagem:** Importe o fundo do mapa de um arquivo de imagem.
   - **Geográfico:** Estabeleça conexão com um provedor de mapas.
6 Configure a visualização de mapa padrão e outras predefinições.
7 Configure as informações padrão a serem exibidas quando alguém abrir este mapa.
8 Clique em **Criar**.
9 Para adicionar uma câmera Sharp que esteja monitorando a zona de estacionamento, clique em **Exibição de área** ( ) e arraste a Câmera de LPR para o mapa.

Adicionar uma zona de estacionamento a um mapa

Se tiver criado uma zona de estacionamento no sistema AutoVu™ Free-Flow, você pode adicionar a entidade de zona estacionamento a um mapa existente ou criar um novo mapa para exibir a zona. Fazer isso permite que os operadores vejam a ocupação da zona de estacionamento na tarefa *Mapas* Security Desk.

Antes de iniciar

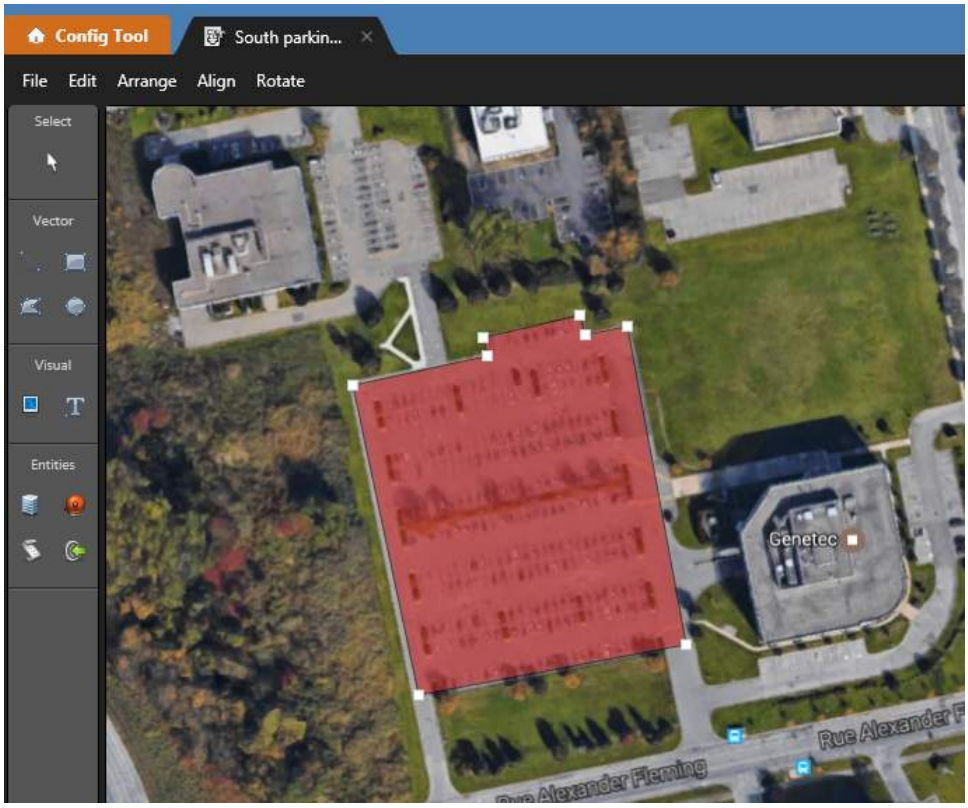
- Crie um mapa no Map designer.
- Adicione e configure uma zona de estacionamento.

O que você deve saber

- Você pode adicionar uma visualização drill-down a um mapa para que o operador possa, por exemplo, clicar em um estacionamento de vários pisos para ter uma visão de cada piso de estacionamento.
- Como alternativa a adicionar uma zona de estacionamento a um mapa, você pode também atribuir um mapa a uma zona de estacionamento.

Para adicionar uma zona de estacionamento a um mapa usando a entidade de zona de estacionamento:

1 Abra a tarefa *Map designer* e selecione o mapa que inclui uma imagem de, por exemplo, o estacionamento ou a região geográfica.
2 Na barra de ferramentas de **Entidades**, selecione **Exibição de área**.
3 Clique na zona de estacionamento na lista e arraste-a para o mapa.
A zona de estacionamento aparece como um quadrado no mapa.
4 Modifique os pontos do quadrado até que o objeto de zona de estacionamento corresponda à forma do estacionamento.
DICA: Pressione `Shift` e clique para adicionar ou remover pontos na borda do objeto de zona de estacionamento.
5 Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).



Para adicionar uma zona de estacionamento a um mapa desenhando um polígono:

1 Abra a tarefa *Map Designer* e selecione o mapa que inclui uma imagem do estacionamento.

2 Na barra de ferramentas **Vetor**, selecione **Desenhar polígono**.

3 No mapa, clique nos cantos do estacionamento para desenhar o polígono.

DICA: Após concluir o desenho do polígono, você pode pressionar `Shift` e clicar para adicionar ou remover pontos na borda do polígono.

4 Clique em **Não atribuído** no widget *Links* e selecione a zona de estacionamento que deseja atribuir ao polígono.

5 Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

Adicionar visualizações drill-down a mapas

QuandoSecurity Desk operadores precisam monitorar uma grande área geográfica com muitas entidades, criar uma visualização drill-down pode facilitar o gerenciamento da área para o operador. Isso pode ser especialmente útil ao gerenciar zonas de estacionamento.

O que você deve saber

No exemplo a seguir nós criaremos uma visualização drill-down a partir do nível da cidade para um estacionamento multinível, até um nível de dentro do estacionamento.

Configurar uma visualização drill-down em um mapa:

1 Em Config Tool, abra a tarefa *exibição de área* e crie as áreas necessárias para o drill-down.

Este exemplo usa as áreas a seguir:

Estacionamento do aeroporto (adicionado como uma entidade de *Área*)

Estacionamento multinível (adicionado como uma entidade de *Área*)

Piso 3 do estacionamento (adicionado como uma entidade de *zona de estacionamento*)

Piso 2 do estacionamento (adicionado como uma entidade de *zona de estacionamento*)

Piso 1 do estacionamento (adicionado como uma entidade de *zona de estacionamento*)

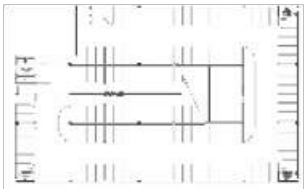
2 Para adicionar mapas às áreas, na aba **Identidade** de cada uma das áreas, clique em **Criar mapa** e adicionar mapa da área.

Este exemplo usa os mapas de áreas a seguir:

Estacionamento em aeroporto

Estacionamento multinível

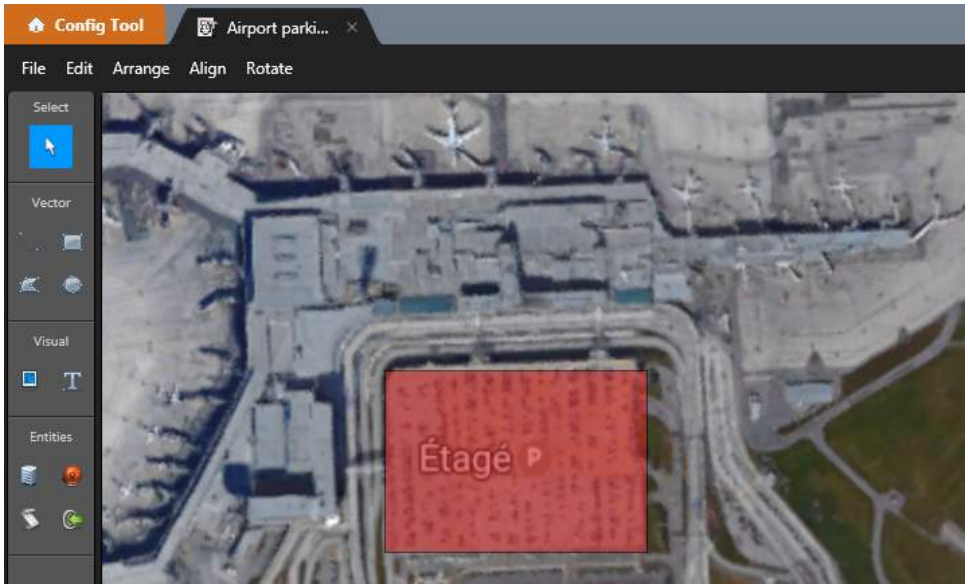
Níveis de estacionamento



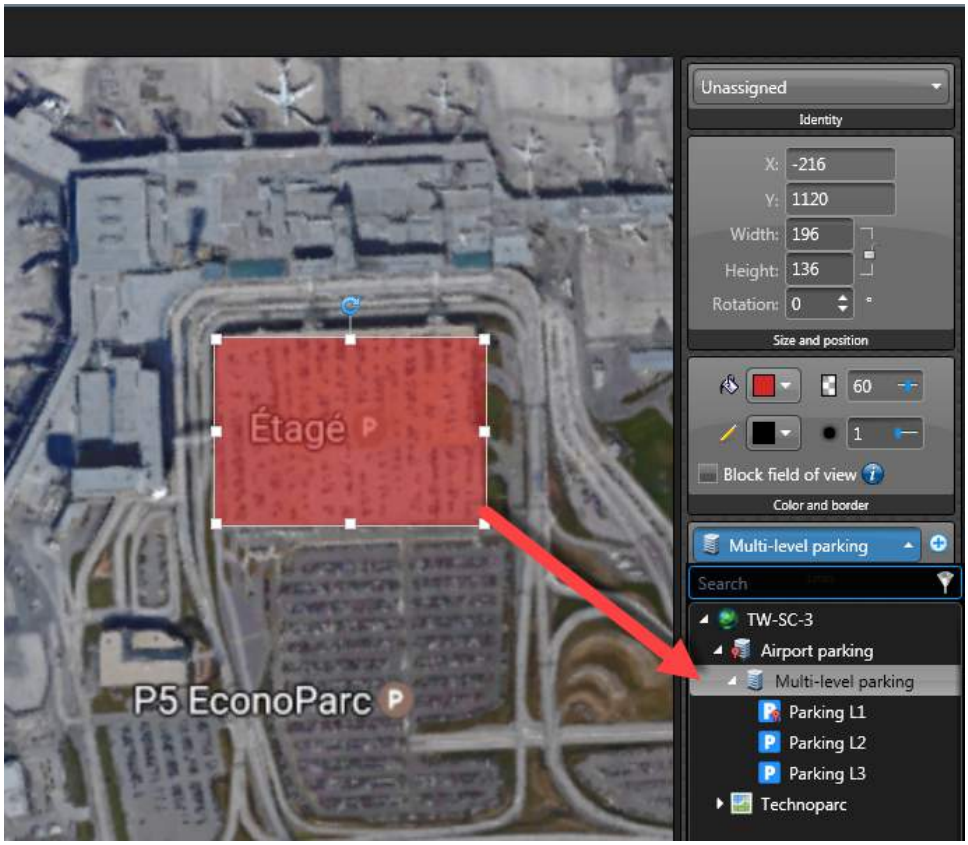
3 Crie *link para mapas* para fazer o drill-down pelas áreas. Para este exemplo, estamos fazendo o drill-down a partir do mapa de estacionamento do aeroporto para o mapa de estacionamento multinível, até o mapa de piso do estacionamento.

a) Na tarefa *Map designer*, abra o mapa do *estacionamento do aeroporto*.

b) Usando as ferramentas de **Vetor**, desenhe um polígono sobre o estacionamento multinível.



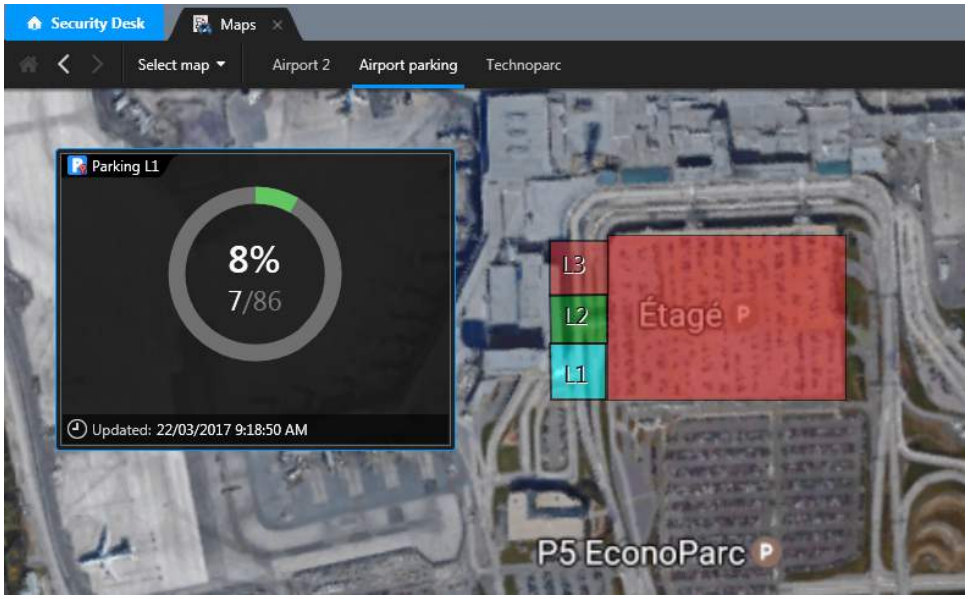
c) A partir do widget **Links**, atribua a área do estacionamento multinível para o polígono.



NOTA: Você pode selecionar uma cor para o polígono a partir do widget **Cor e borda**.

d) Para exibir a ocupação em cada uma das zonas de estacionamento no mapa, clique em **exibição de área** ( ) na barra de ferramentas e arraste as zonas de estacionamento para o mapa. As zonas de estacionamento aparecem como polígonos no mapa. Você pode selecionar a cor de cada um dos polígonos e usar a ferramenta **Adicionar texto** ( ) para identificar a zona de estacionamento.

e) Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

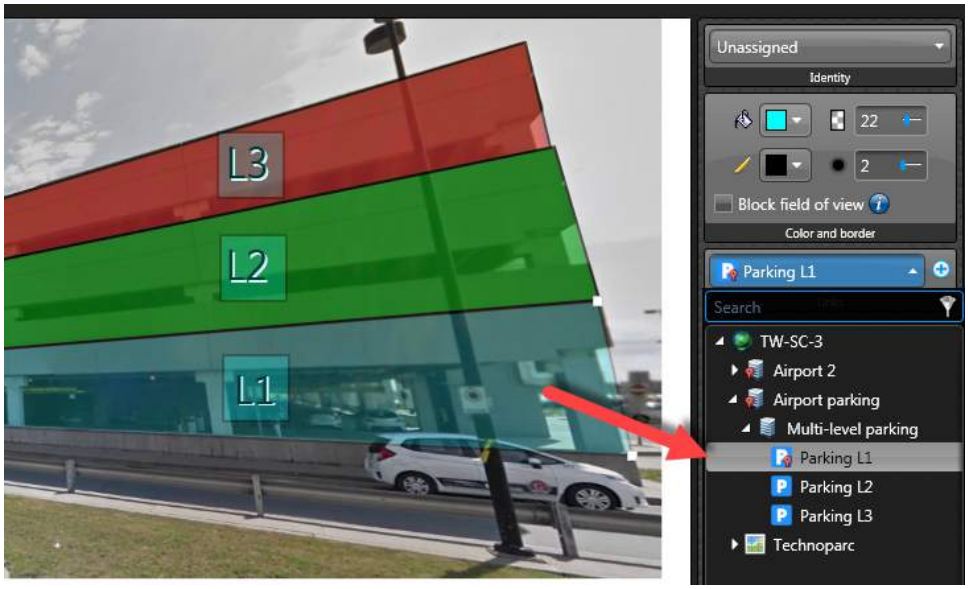


Quando este mapa é exibido em Security Desk, ao clicar em um dos polígonos da zona de estacionamento exibe a ocupação da zona de estacionamento. Clicar no polígono do estacionamento multinível faz o drill-down para o mapa do estacionamento multinível.

f) Na tarefa *Map designer*, abra o mapa do *estacionamento multinível*.

g) Usando as ferramentas de **Vetor**, desenhe um polígono sobre cada piso do estacionamento.

h) A partir do widget **Links**, atribua a zona de estacionamento que corresponde a cada polígono.



i) Para exibir a ocupação em cada uma das zonas de estacionamento no mapa, arreste todas as zonas de estacionamento para o mapa a partir da **exibição de área**, tal como fez para o primeiro mapa.

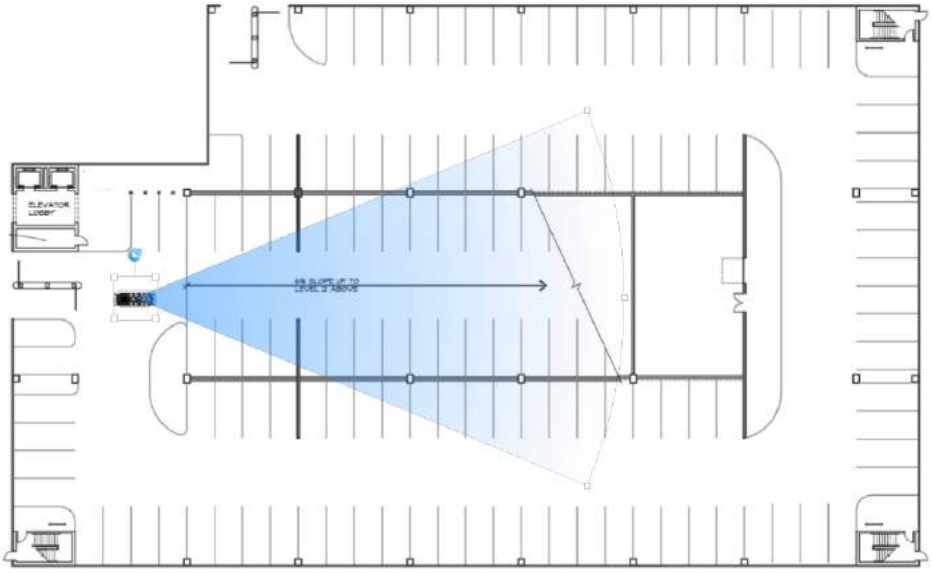
j) Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

k) Na tarefa *Map designer*, abra o mapa do *Piso 1 do estacionamento*.

NOTA: Não é necessário vincular os polígonos a quaisquer mapas adicionais pois neste exemplo a zona de estacionamento é o nível mais baixo desse drill-down.

l) Para adicionar uma unidade de vídeo Sharp que esteja monitorando a zona de estacionamento, clique em **Exibição de área** ( ) e arraste a Sharp para o mapa.

- Caso queira exibir reconhecimento de placas de veículos, arreste para a unidade Sharp.
- Caso queira exibir uma representação do campo de visão da Sharp, arraste a Câmera de LPR listada sob a unidade Sharp, tal como mostrado na imagem a seguir. Selecione **Exibir campo de visão** a partir do widget *Campo de visão*.



m) Na barra de ferramentas *Map designer*, clique em **Salvar** ( ).

43

Sistemas móveis AutoVu™

Esta seção inclui os seguintes tópicos:

- "Preparar para implantar sistemas móveis AutoVu" na página 859
- "Implantar sistemas AutoVu móveis" na página 860
- "Sobre Genetec Patroller" na página 861
- "Conectar o Genetec Patroller ao Security Center" na página 862
- "Configurar a entidade de Genetec Patroller no Security Center" na página 864
- "Adicionar campos personalizados pelo usuário a leituras e ocorrências" na página 866
- "Arquivos de som usados no Genetec Patroller" na página 870
- "Alterar arquivos de som para eventos de LPR" na página 871

Preparar para implantar sistemas móveis AutoVu™

Para garantir que a implantação do seu AutoVu™ móvel aconteça sem problemas, deve realizar uma série de passos de configuração prévia.

Antes de implantar um sistema móvel AutoVu™:

1 Instale os seguintes componentes de software do Security Center:
   a) Instale o software do Servidor Security Center no seu *servidor principal*.
   b) (Opcional) Instale o software do servidor Security Center em *servidores de expansão*.
      Você pode adicionar servidores de expansão a qualquer momento.
   c) Instale o software de cliente Security Center em pelo menos uma estação de trabalho.
      Para obter mais informações sobre a instalação do Security Center, consulte o *Guia de Instalação e Atualização do Security Center*.
2 Instale o hardware Sharp móvel (consulte o *Guia de implantação na cidade AutoVu™* ou*Guia de implantação na universidade AutoVu™*).
3 Instale Genetec Patroller™ e hotfixes relacionados (consulte o *Guia do administrador Genetec Patroller™)*.
4 Atualize AutoVu™ Genetec Patroller™ e as unidades Sharp para o mais recente software e firmware (consulte o *Guia do Administrador do Genetec Patroller™* e o *Guia do Administrador do Sharp.*

   NOTA: Você pode realizar certas atualizações do Security CenterConfig Tool.

Tópicos relacionados

Atualizar o SharpV a partir do Security Center na página 786

Implantar sistemas AutoVu™ móveis

Para integrar veículos de patrulha equipados com LPR no Security Center, você pode implantar um sistema AutoVu™ móvel.

Antes de iniciar

Execute as etapas de pré-configuração.

O que você deve saber

As informações sobre como configurar uma instalação AutoVu™ móvel típica são descritas aqui. Seu processo pode ser diferente dependendo das exigências específicas de sua instalação.

NOTA: As configurações que são pré-configuradas durante sua instalação não são listadas nesta tarefa. Por exemplo, quando você instala o Security Center, a pasta raiz do LPR Manager é criada automaticamente em seu computador na localização *C:\Genetec\AutoVu\RootFolder*.

Para implantar um sistema AutoVu™ móvel:

1 Faça logon no Sharp Portal e configure o Sharp para um sistema AutoVu™ móvel. Para obter informações sobre como iniciar sessão no Sharp Portal, consulte o *Guia do Administrador Sharp*.

2 Conecte o Genetec Patroller™ ao Security Center para que o Genetec Patroller™ seja descoberto pelo LPR Manager.

3 Conecte unidades Sharp móveis ao Genetec Patroller™ (consulte o *Guia do Administrador do Genetec Patroller™*).

4 Defina o servidor do LPR Manager e as configurações do banco de dados.

NOTA: Você também pode adicionar um servidor adicional para atuar como *servidor secundário* para o LPR Manager, para configurar o failover. Para mais informações, consulte Configurar failover de função na página 165.

5 Crie e configure entidades de lista de procurados.

6 Configure o Genetec Patroller™ (consulte o *Guia do Administrador do Genetec Patroller™*).

Após terminar

Defina as configurações adicionais para o seu tipo de instalação do AutoVu™ móvel:

- Aplicação da lei.
- Fiscalização de estacionamento na cidade e na universidade.
- Inventário de placas de veículos móvel.

Sobre Genetec Patroller™

Uma entidade *Genetec Patroller*™ representa o software no veículo que é executado em um computador de bordo do veículo de patrulha. O software verifica as placas de licença captadas por unidades LPR montadas no veículo contra listas de veículos de interesse e veículos com autorizações. Ele também coleta dados para a fiscalização de estacionamento com limitação de tempo.

A interface do *Genetec Patroller*™ alerta usuários sobre placas de licença que correspondam às regras acima para que ação imediata possa ser tomada.

Dependendo da sua solução AutoVu™ o Genetec Patroller™ poderá ser usado para fazer o seguinte:

- Verificar leitura de placa de veículo de *Câmera de LPR* com relação a listas de veículos de interesse (listas de procurados) e de veículos com autorizações (listas de autorizações).
- Informá-lo sobre alertas de listas de procurados, de autorizações ou de horas extras para que você possa agir imediatamente.
- Coletar dados para fiscalização de estacionamento limitada pelo tempo.
- Coletar leituras de placas para criar e manter um inventário de placas de uma instalação de estacionamento.

Conectar o Genetec Patroller™ ao Security Center

Você deve configurar o Genetec Patroller™ e o Security Center para que o LPR Manager possa descobrir e se comunicar com as unidades Genetec Patroller™ que ele controla.

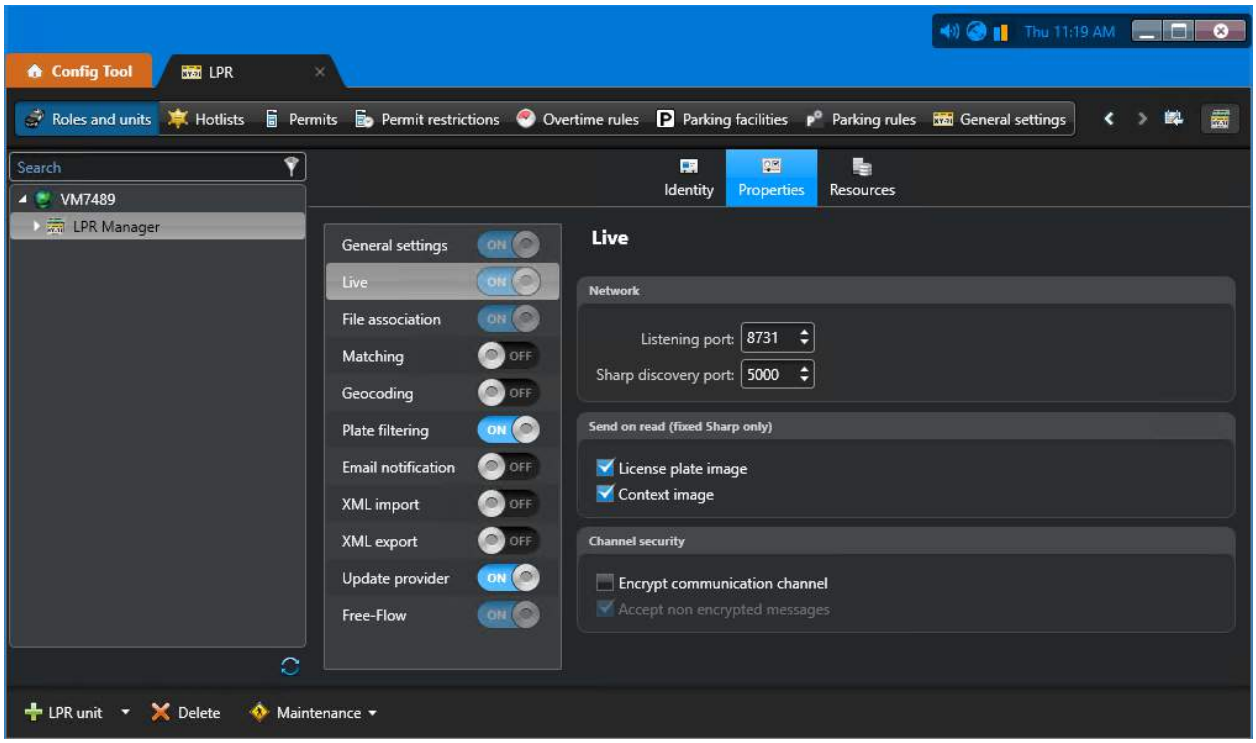
Para conectar o Genetec Patroller™ ao Security Center:

1 Na página inicial do Config Tool, clique em **Sistema** > **Funções** e selecione o LPR Manager que deseja configurar.

2 Clique na aba **Propriedades** e, em seguida, clique em **Dinâmica**.

3 Na opção **Porta de escuta**, selecione a porta para escutar solicitações de conexão vindas de veículos de patrulha.

NOTA: A **Porta de escuta** (padrão: 8731) deve corresponder ao número de **Porta** inserido para Patroller Config Tool (padrão: 8731) na etapa 10.



4 Para criptografar a comunicação entre o Security Center e o Patroller Config Tool, selecione a opção **Criptografar canal de comunicação**.

IMPORTANTE: Esta definição também deve ser aplicada no Patroller Config Tool.

5 Para permitir que o Security Center ainda aceite as conexões recebidas de veículos de patrulha que não possuem a opção de criptografia ativada, selecione a opção **Acessar mensagens não criptografadas** .

6 Clique em **Aplicar**.

7 Abra o Patroller Config Tool.

8 Clique na aba Security Center e ative a opção **Conectar ao Security Center**.

9 Digite o **endereço IP** da máquina Security Center que hospeda a função LPR Manager.

10 Digite o número da **Porta** (padrão: 8731) que o Genetec Patroller™ deve usar para se conectar à função LPR Manager.

11 Se você tiver habilitado a opção **Criptografar canal de comunicação** no Security Center do Config Tool, habilite a opção no Patroller Config Tool.

12 (Opcional) Para configurar a atualização centralizada de todas as unidades Sharp conectadas ao LPR Manager, digite a **Porta de provedor de atualizações** que o Security Center usa para enviar atualizações para o Genetec Patroller™ e unidades Sharp conectadas.

NOTA: Digite a mesma *Porta de escuta* de **Provedor de atualizações** que está configurada na aba Propriedades do LPR Manager no Security Center do Config Tool. Não confunda a *Porta de escuta* de **Provedor de atualizações** com a *Porta de escuta* **Dinâmica**.

13 Selecione que **Eventos dinâmicos** pretende enviar ao Security Center.

14 Ao lado de **Transferência periódica**, especifique a frequência com que as alterações de listas de procurados e listas de autorização são baixadas para o Genetec Patroller™ (se você tiver uma conexão dinâmica). O período de transferência padrão é a cada 240 minutos. Você pode desativar a transferência periódica em listas de procurados específicas (não em listas de autorização) no Security Center do Config Tool na página *Avançado* da lista de procurados.

15 Clique em **Aplicar**.

Tópicos relacionados

Definir configurações avançadas de lista de procurados na página 810

Configurar a entidade de Genetec Patroller™ no Security Center

Na tarefa *LPR*, você pode configurar o gerenciamento de som, as definições do buffer de confirmação e um retardo das ocorrências para o veículo de patrulha.

Antes de iniciar

Conecte o Genetec Patroller™ ao Security Center.

O que você deve saber

- Quando seleciona a entidade Genetec Patroller™ que adicionou ao Security Center, você não pode modificar as configurações do computador na aba **Propriedades** do computador.
- As informações sobre o computador que hospeda a entidade Genetec Patroller™ em **Propriedades** não podem ser modificadas.

Para configurar a entidade de Genetec Patroller™:

1 Na página inicial do Config Tool, abra a tarefa *LPR* e clique em **Funções e unidades**.

2 No LPR Manager, selecione a entidade Genetec Patroller™ que deseja configurar e, em seguida, clique na aba **Propriedades**.

3 Em **Associação de arquivos**, configure como as listas de procurados e autorizações devem ser usadas.

- **Herdar da função LPR Manager:** O Genetec Patroller™ usa as listas de procurados e listas de autorizações associadas ao seu LPR Manager pai. Esta é a configuração padrão.
- **Específico:** Associe listas de procurados ou listas de autorizações específicas à unidade Genetec Patroller™ em vez de ao LPR Manager. Se você mover a entidade Genetec Patroller™ para outro LPR Manager, a lista de procurados ou de autorizações acompanhará.

4 Em **Gerenciamento de som**, configure o Genetec Patroller™ para reproduzir um som ao ler uma placa e/ou ao gerar uma ocorrência e selecione se sons devem ser tocados mesmo quando o aplicativo está minimizado.

- **Tocar som por alerta:** Toca um som quando o Genetec Patroller™ gera uma ocorrência.
- **Tocar som por leitura:** Toca um som quando o Genetec Patroller™ lê uma placa.
- **Tocar sons mesmo quando minimizado:** Permita a reprodução de sons mesmo quando a janela do Genetec Patroller™ está minimizada.

5 Em **Buffer de confirmação**, especifique uma restrição de buffer que limite a quantidade de ocorrências que podem ser ignorados (não confirmados ou rejeitados) antes que o Genetec Patroller™ comece automaticamente a rejeitar todas as ocorrências subsequentes. Você também pode escolher (por prioridade) quais listas de procurados devem cumprir esta restrição

- **Contagem de rejeição:** Quantos alertas não confirmados são permitidos.
- **Prioridade de rejeição:** Quando você cria uma entidade de lista de procurados, você pode especificar uma prioridade para aquela lista de procurados. Esta definição diz ao Genetec Patroller™ quais listas de procurados devem atender a restrição do buffer.

6 Em **Lista de procurados e autorizações**, especifique o **Retardo de ocorrência duplicada** que informa o Genetec Patroller™ para ignorar múltiplas ocorrências da mesma placa durante o período de retardo. Por exemplo, se você definir um atraso de 10 minutos, não importa quantas vezes o Genetec Patroller™ leia a mesma placa durante esses 10 minutos, ele gerará apenas uma ocorrência.

A entidade Genetec Patroller™ é configurada no Security Center. As configurações serão transferidas por push para o Genetec Patroller™ em execução no computador de bordo na próxima vez que ele se conectar ao Security Center.

Após terminar

Configure o Genetec Patroller™ usando o Patroller Config Tool (consulte o *Guia do Administrador do Genetec Patroller™)*.

Adicionar campos personalizados pelo usuário a leituras e ocorrências

Para associar os metadados de um usuário a leituras e ocorrências de um Genetec Patroller™ individual para que você possa consultar e filtrar esses campos personalizados do usuário nos relatórios de *Leituras* e *Ocorrências* do Security Desk, você pode adicionar campos de usuário personalizados a campos de anotação de LPR.

Antes de iniciar

- Configure o Genetec Patroller™ para que seja exigido um nome de usuário e/ou senha para fazer logon (consulte o *Guia do Administrador do Genetec Patroller™*).

O que você deve saber

Você não pode adicionar campos personalizados a leituras e ocorrências se o Genetec Patroller™ estiver configurado para "Sem logon", porque as leituras e as ocorrências devem ser anexadas a um nome de usuário válido.

Para adicionar campos personalizados relacionados ao usuário a leituras e ocorrências:

1 Crie o campo personalizado que se aplica a entidades de usuário.
2 Defina o campo personalizado para seus usuários do Genetec Patroller™.
3 Adicione o campo personalizado como um campo de anotação

O campo personalizado está agora disponível como duas colunas separadas nos relatórios "Leituras" e "Ocorrências" do Security Desk. Uma é uma coluna de *Campo personalizado* que exibe o último valor configurado para a entidade de usuário. A outra coluna é um *Campo de anotação* que exibe o valor da entidade de usuário quando a leitura ou ocorrência é armazenado pela função LPR Manager. Para obter mais informações sobre a visualização de eventos de LPR no Security Desk, consulte o *Guia do Usuário do Security Desk*.

Exemplo

Você tem vários usuários do Genetec Patroller™ que alternam entre diferentes equipes de patrulha, como policiais que se deslocam entre diferentes zonas da cidade. Ao definir cada equipe de patrulha como um campo personalizado do usuário, você pode gerar um relatório no Security Desk que exibe leituras ou ocorrências coletadas quando o oficial estava na equipe de patrulha A, equipe de patrulha B e assim por diante.

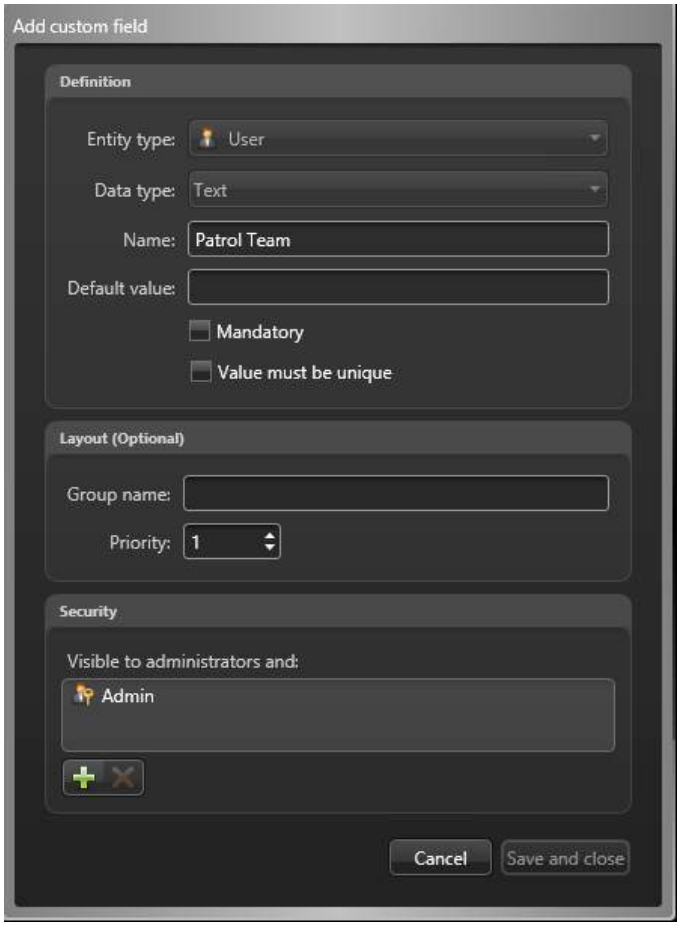
Tópicos relacionados
Sobre campos personalizados na página 86

Criando campos personalizados do usuário

Para usar campos personalizados com alertas e leituras, primeiro você deve criar um campo personalizado que se aplique às entidades de usuário.

Para criar um campo personalizado do usuário:

1 Na página inicial de Config Tool, abra a tarefa **Sistema** e clique na visualização **Macros**.
2 Clique na página **Ações personalizadas** e, em seguida, clique em **Adicionar um item**  .
3 Na lista suspensa **Tipo de entidade** na caixa de diálogo **Adicionar campo personalizado**, selecione **Usuário**.



4 Na lista suspensa **Tipo de dado**, selecione um tipo de dado personalizado ou padrão para o campo personalizado.

   Por exemplo, selecione **Texto**.

5 No campo **Nome**, digite o nome para o campo personalizado.

   Por exemplo, digite **ID do usuário**.

6 (Opcional) No campo **Valor padrão**, digite ou selecione o valor padrão para este campo.

7 Dependendo do tipo de dado selecionado, as seguintes opções adicionais estão disponíveis:

   - **Obrigatório:** Selecione-o se este campo personalizado não puder ficar vazio.
   - **O valor deve ser único:** Selecione-o se o valor deste campo personalizado dever ser exclusivo.

     NOTA: A opção de *valor exclusivo* somente pode ser aplicada após o campo ter sido criado. Para aplicar esta opção, você deve primeiro certificar-se de que todas as entidades no seu sistema tenham um valor distinto para este campo personalizado, em seguida, volte para esta aba para aplicar a opção de valor único a ela.

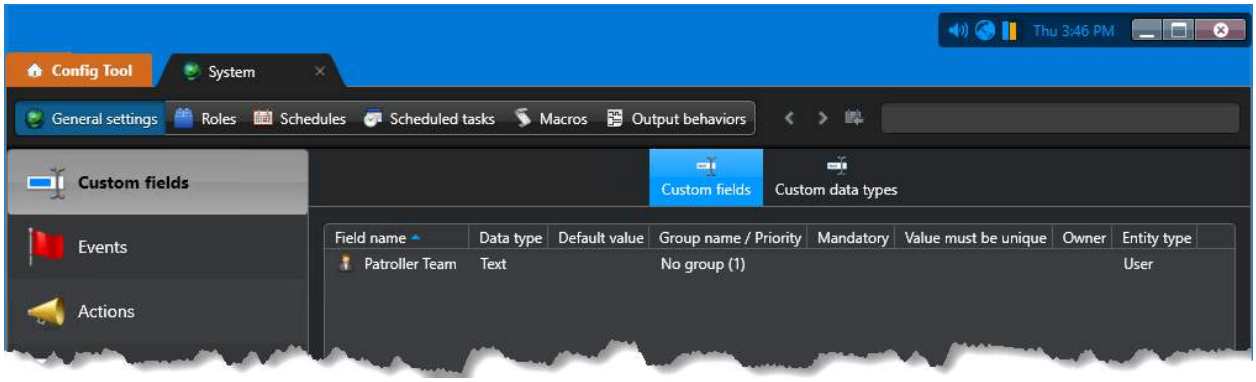
8 (Opcional) Na seção **Layout**, digite o **Nome do grupo** e selecione a **Prioridade** da lista suspensa.

   Esses dois atributos são usados ao exibir o campo na aba **Campos personalizados** da entidade associada. O nome do grupo é usado como o cabeçalho do grupo e a prioridade define a ordem de exibição do campo dentro do grupo.

9 (Opcional) Na seção **Segurança**, clique em ✚ para adicionar usuários e grupos de usuários que serão capazes de visualizar este campo personalizado. Como padrão, somente usuários administrativos podem ver um campo personalizado.

10 Clique em **Salvar e fechar**.

11 Clique em **Aplicar**.



O novo campo personalizado do usuário **ID do usuário** está disponível na aba **Campos personalizados** do seu usuário.

Adicionando campos personalizados como campos de anotação

Depois de ter criado e definido campos personalizados para usuários do Genetec Patroller™, você deve adicionar esses campos personalizados à lista de campos de anotação para leituras e alertas do Genetec Patroller™.

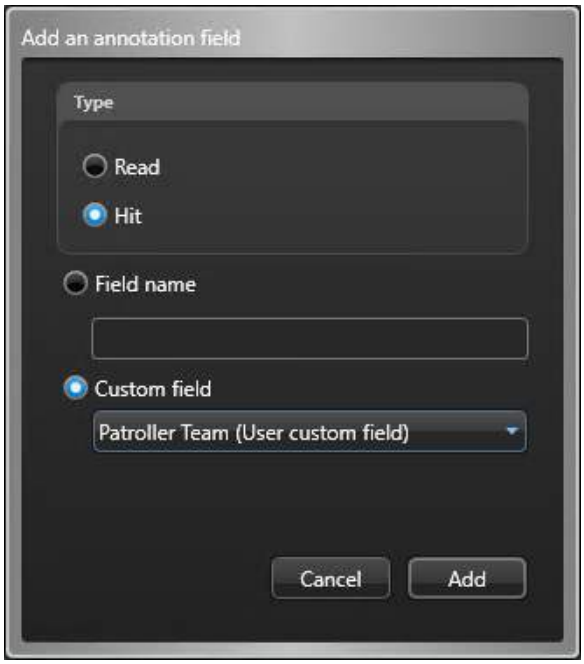
Para adicionar um campo personalizado como um campo de anotação:

1 Na página inicial do Config Tool, clique em **LPR** > **Configurações gerais** > **Campos de anotação**.

2 Clique em **Adicionar um item** ( ).

A janela **Adicionar um campo de anotação** aparecerá.

3 Em **Tipo**, na caixa de diálogo **Adicionar um campo de anotação**, selecione **Leitura** ou **Ocorrência**.



4 Selecione **Campo personalizado** e, em seguida, selecione o campo personalizado do usuário que você criou.

5 Clique em **Adicionar**

O seu campo personalizado do usuário é adicionado à lista de campos de anotação para todas as leituras e ocorrências do Genetec Patroller™. O Security Center agora associa leituras e ocorrências ao campo de usuário personalizado (o **ID de usuário** neste caso**)** que foi conectado ao Genetec Patroller™ no momento da ocorrência do evento. Esse valor é armazenado no banco de dados para cada leitura ou alerta.

NOTA: Se você quiser o mesmo campo personalizado do usuário para leituras *e* ocorrências, você deve defini-lo como um campo de anotação duas vezes, uma vez para ocorrência e uma vez para leituras.

Tópicos relacionados

Criando campos personalizados do usuário na página 866

Definir campos personalizado para usuários do Genetec Patroller™

Depois de criar campos personalizados de usuário no Security Center, você pode defini-los na aba *Campos personalizados* dos usuários do Genetec Patroller™.

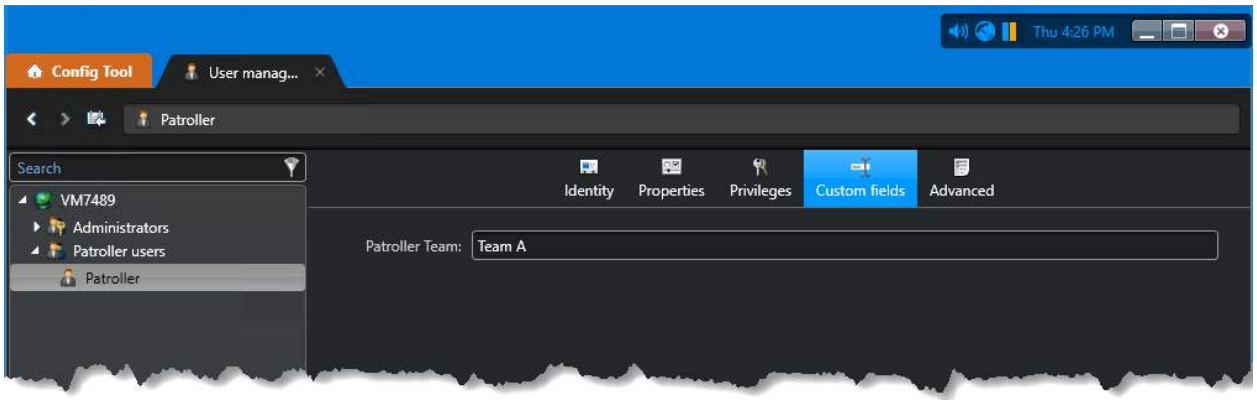
Antes de iniciar

Para definir um campo personalizado para um usuário do Genetec Patroller™:

1 Na página inicial do Config Tool, clique em **Segurança** > **Usuários** e selecione o LPR Manager que deseja configurar.

2 Selecione a aba **Campos personalizados**.

Os campos personalizados que já foram criados para entidades de usuário são exibidos.



3 Digite a **Equipe Patroller** para o usuário atual do Genetec Patroller™.

Por exemplo, digite **Equipe A**.

4 Clique em **Aplicar**.

Este usuário do Genetec Patroller™ tem agora um ID de Usuário da *Equipe A*. Agora você pode adicionar este campo personalizado como um campo de anotação para leituras e alertas.

Tópicos relacionados

Criando campos personalizados do usuário na página 866

Arquivos de som usados no Genetec Patroller™

O Genetec Patroller™ usa sons para comunicar informações e para incitar o operador do veículo de patrulha a tomar uma ação. Os arquivos de som estão localizados no computador de bordo na pasta: *C:\Program Files \Genetec AutoVu X.Y\MobileClient\Config\Sounds* (localização padrão).

Os seguintes arquivos de som *.wav* estão incluídos:

- **Ambiguity:** Indica que o Genetec Patroller™ está configurado para selecionar automaticamente a zona, mas é necessária confirmação do operador
- **CalibrationError:** Indica que a etapa de calibração de um sistema de Navegação AutoVu™ não teve êxito
- **CalibrationInstruction:** Indica a etapa seguinte na calibração da Navegação AutoVu™
- **EnterZone:** Indica que o veículo de patrulha entrou em uma zona de estacionamento ou zona de tempo extra
- **ExitZone:** Indica que o veículo de patrulha saiu de uma zona de estacionamento ou zona de tempo extra
- **HotlistHitEvent:** Indica que a placa de veículo está incluída em uma lista de procurados
- **NotificationError:** Indica que ocorreu um erro.
- **OvertimeHitEvent:** Indica que o veículo estacionado tem uma violação de tempo extra
- **PermitHitEvent:** Indica que o veículo estacionado não tem a autorização necessária para estacionar na zona de estacionamento
- **TooManyReadsEvent:** Indica que o número máximo de placas no Inventário de placas de veículos móvel foi excedido
- **VehicleEvent:** Indica que uma placa de veículo foi lida

Alterar arquivos de som para eventos de LPR

Você pode adicionar novos arquivos de som ao Genetec Patroller™ para serem usados em eventos de LPR copiando manualmente os arquivos para o computador de bordo do Genetec Patroller™.

Antes de iniciar

O que você deve saber

- Os arquivos de som devem estar no formato *.wav*.
- Você pode substituir um arquivo de som padrão por um novo arquivo de som que tenha o mesmo nome de arquivo.

  Exemplo: Se você tiver um arquivo chamado *alert.wav* e quiser usá-lo para uma ocorrência de autorização, você deve renomear seu arquivo para *PermitHitEvent* para corresponder ao nome do arquivo de som padrão antes de copiá-lo para a pasta *Sounds* (manualmente ou através do serviço de atualização). Desta forma, ele sobrescreve o arquivo de som padrão e o Genetec Patroller™ pode reproduzi-lo.
- Os sons de alertas da lista de procurados têm mais flexibilidade. Você pode substituir o som padrão *HotlistHitEvent* na pasta *Sounds* ou você pode usar um nome de arquivo diferente para cada lista de procurados carregada no Genetec Patroller™, desde que você especifique o caminho para cada arquivo de som de lista de procurados no Security Center do Config Tool.

  MELHOR PRÁTICA: Os novos arquivos de som de lista de procurados podem ser armazenados em qualquer local no computador de bordo, mas você deve mantê-los na mesma pasta *Sounds* dos arquivos de som padrão. Isso torna mais fácil atualizá-los mais tarde.

Para substituir um arquivo de som:

1 Para sobrescrever os arquivos de som padrão, faça o seguinte:
   a) Abra a pasta *C:\Program Files\Genetec AutoVu X.Y\MobileClient\Config\Sounds*.
   b) Renomeie seu arquivo de som para corresponder ao arquivo padrão que deseja substituir.
   c) Copie seu arquivo de som renomeado para a pasta *Sounds* para que ele sobrescreva o arquivo padrão.
2 Reinicie o Genetec Patroller™ para que suas alterações entrem em vigor.

Para configurar um som exclusivo para cada lista de procurados:

1 Copie seu novo arquivo de som para qualquer local no computador no veículo.
2 Abra o Config Tool e selecione a tarefa **LPR**.
3 Selecione a lista de procurados a configurar e clique na aba **Avançado**.
4 No campo **Arquivo de som**, especifique o caminho e o nome de arquivo para o arquivo de som no computador de bordo.

  Para configurar sons para outras listas de procurados, repita as Etapas 3 e 4.

Tópicos relacionados

Arquivos de som usados no Genetec Patroller na página 870

Alterar arquivos de som para eventos LPR usando o serviço de atualização

Você pode enviar diferentes arquivos de som para a pasta *MobileClient* do veículo de patrulha usando o serviço de atualização do Security Center.

O que você deve saber

Os arquivos de som para ocorrências de autorização, ocorrências de tempo extra e leituras de placa devem estar na pasta padrão *Sounds* para que o Genetec Patroller™ possa reproduzi-los.

Depois de enviar os arquivos para a pasta *MobileClient*, você pode mover manualmente os arquivos para a pasta *Sounds* se escolher fazer isso, mas você também pode compactar seu arquivo de som para que o Windows o extraia automaticamente para a pasta *Sounds*.

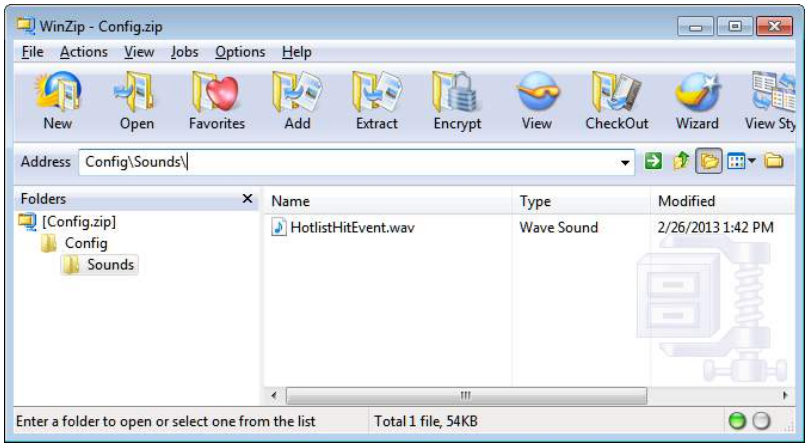
Para alterar arquivos de som para eventos LPR usando o serviço de atualização:

1 (Opcional) Se você deseja substituir um arquivo de som padrão, renomeie seu novo arquivo de som para o mesmo nome do arquivo padrão que deseja substituir (por exemplo, *HotlistHitEvent.wav*).

2 No computador do Security Center, crie a mesma estrutura de arquivos do Windows Explorer encontrada no computador de bordo do Genetec Patroller™ (por exemplo, *C:\Program Files\Genetec AutoVu X.Y \MobileClient\Config\Sounds*).

3 Copie seu novo arquivo de som para a pasta *Sounds* que você criou.

4 Compacte o arquivo de som no nível *Config* de modo que espelhe o caminho relativo da pasta *MobileClient* até a pasta *Sounds* no computador de bordo.



O arquivo é extraído para o destino definido no caminho do arquivo compactado (pasta *Sounds*).

5 (Opcional para sons da lista de procurados) Se o arquivo tiver um nome de arquivo diferente do padrão *HotlistHitEvent*, você deve especificar o caminho completo para o arquivo, incluindo o novo nome do arquivo:

a) Na página inicial do Config Tool, abra a tarefa **LPR**.
b) Selecione a lista de procurados a configurar e clique na aba **Avançado**.
c) No campo **Arquivo de som**, especifique o caminho e o nome de arquivo para o arquivo de som no computador de bordo.
d) Repita as etapas para quantas listas de procurados quiser.

6 Envie o arquivo de som para o Genetec Patroller™ como se estivesse instalando uma atualização sem fio. Para mais informações, consulte o *Genetec Patroller™ Guia do Administrador*.

O Genetec Patroller™ reinicia após instalar a atualização e agora usa o novo arquivo de som para o seu evento LPR escolhido.

Tópicos relacionados

Arquivos de som usados no Genetec Patroller na página 870

44

Sistemas de aplicação da lei AutoVu™

Esta seção inclui os seguintes tópicos:

- "Sobre a Aplicação da lei" na página 874
- "Criar motivos de aceitação de ocorrência e rejeição de ocorrência para ocorrências de lista de procurados" na página 875
- "Criar atributos e categorias de Novo procurado" na página 876

Sobre a Aplicação da lei

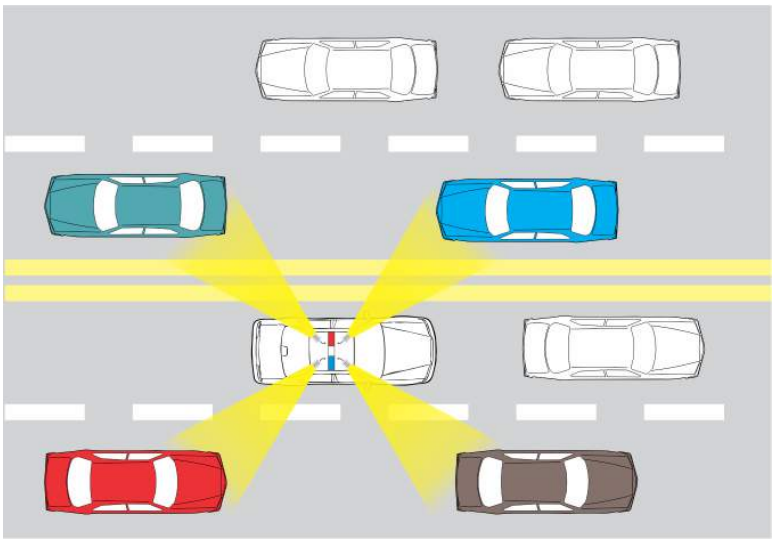
Aplicação da lei é uma instalação de software do Genetec Patroller™ que está configurada para fiscalizar a lei: a correspondência entre leituras de placas de veículo e listas de placas de veículo procuradas (listas de procurados). O uso de mapas é opcional.

À medida que você patrulha, as câmeras Sharp instaladas no veículo leem placas automaticamente e enviam as informações para o Genetec Patroller™. Se uma placa estiver em uma lista de procurados carregada, o Genetec Patroller™ o alerta e você pode tomar medidas imediatas.

As listas de procurados normalmente contêm informações sobre veículos roubados, suspeitos de contravenção, crianças desaparecidas e assim por diante. O uso do mapeamento no veículo com uma instalação de Fiscalização da lei é opcional.

Exemplo

Você pode ter até seis câmeras Sharp instaladas em um veículo de patrulha. Isso permite que você capture o número máximo de placas em veículos em diferentes pistas e mesmo aqueles que viajam na direção oposta. O diagrama a seguir mostra um veículo Genetec Patroller™ de aplicação da lei equipado com quatro câmeras:



Criar motivos de aceitação de ocorrência e rejeição de ocorrência para ocorrências de lista de procurados

Quando um operador escolhe aceitar ou rejeitar uma ocorrência de placa de veículo, além dos motivos predefinidos que o operador pode escolher, você também pode definir motivos de aceitação de ocorrência e rejeição de ocorrência personalizados que podem ser selecionados pelo operador.

O que você deve saber

- **Motivos de rejeição de ocorrência:** Lista de motivos para rejeitar ocorrências de lista de procurados. Esses valores também ficam disponíveis como opções de filtragem de motivos de Rejeição para gerar relatórios de ocorrências no Security Desk. Várias categorias são pré-configuradas para você ao instalar o Security Center.
- **Motivos de aceitação de ocorrência:** Um formulário que contém uma lista de perguntas que os usuários do Genetec Patroller™ devem responder quando aceitam uma ocorrência. As informações do formulário de ocorrências podem ser consultadas no relatório de Ocorrências do Security Desk. Não há categorias pré-configuradas.
- As configurações são baixadas juntamente com as listas de procurados e listas de autorização selecionadas para Genetec Patroller™ quando o usuário faz logon.
- Os motivos de rejeição e aceitação de ocorrências são aplicados no nível do Directory, o que significa que todos os LPR Managers em seu sistema compartilham as mesmas configurações.
- Os atributos que você cria também ficam disponíveis como opções de filtragem de relatórios de ocorrências no Security Desk.

Para criar um motivo de aceitação de ocorrência ou rejeição de ocorrência:

1 Na página inicial do Config Tool, clique em **LPR** > **Configurações gerais** > **Lista de procurados**.
2 Adicione **Motivos de aceitação de ocorrência** ou **Motivos de rejeição de ocorrência** conforme necessário.
3 Clique em **Aplicar**.

Os novos motivos de aceitação e rejeição de ocorrências são baixados para o Genetec Patroller™ na próxima vez que ele for conectado ao Security Center.

Criar atributos e categorias de *Novo procurado*

É possível criar atributos e categorias personalizados de placas de veículos para serem exibidos no Genetec Patroller™. Os operadores de veículos de patrulha podem selecionar esses atributos quando adicionam uma placa de veículo *Novo procurado*.

O que você deve saber

- Se um veículo de patrulha tiver uma conexão sem fio, é possível obter listas de procurados atualizadas para o Genetec Patroller™. Contudo, se o veículo não tiver uma conexão sem fio, o operador pode adicionar manualmente uma placa de veículo a uma lista de procurados local criando uma entrada de placa de veículo *Novo procurado*. No Security Center, é possível configurar atributos e categorias que ficam visíveis para o operador quando ele cria uma entrada de *Novo procurado*.
  - **Atributos de Novo procurado:** Atributos diferentes dos padrões (número de placa de veículo, estado de emissão da placa de veículo, categoria) que um usuário do Genetec Patroller™ deve especificar ao inserir um item novo procurado no Genetec Patroller™. Uma categoria é pré-configurada para você quando você instala o Security Center.
  - **Categorias de *Novo procurado*:** Lista de categorias que um usuário do Genetec Patroller™ pode escolher ao inserir um novo item procurado. A categoria é o atributo que diz por que um número de placa de licença de veículo é procurado em uma lista de procurados. Várias categorias são pré-configuradas para você ao instalar o Security Center.

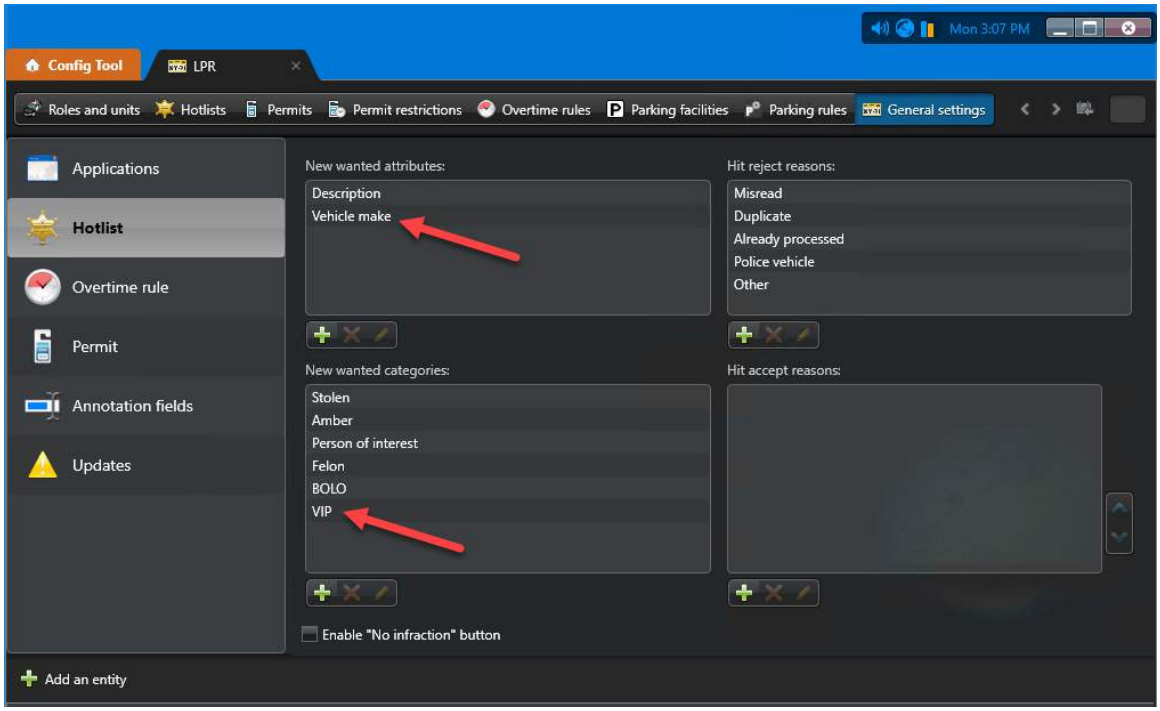
    NOTA: BOLO é uma sigla para "Be On The Lookout" (estar atento), às vezes referido como um boletim de todos os pontos (APB).
- As categorias e atributos de *Novo procurado* são aplicados no nível de Diretório, o que significa que todos os LPR Managers em seu sistema compartilham as mesmas configurações.

Para criar atributos e categorias de *Novo procurado*:

1 Na página inicial do Config Tool, clique em **LPR** > **Configurações gerais** > **Lista de procurados**.

2 Adicione **atributos de Novo procurado** ou **categorias de Novo procurado** conforme necessário.

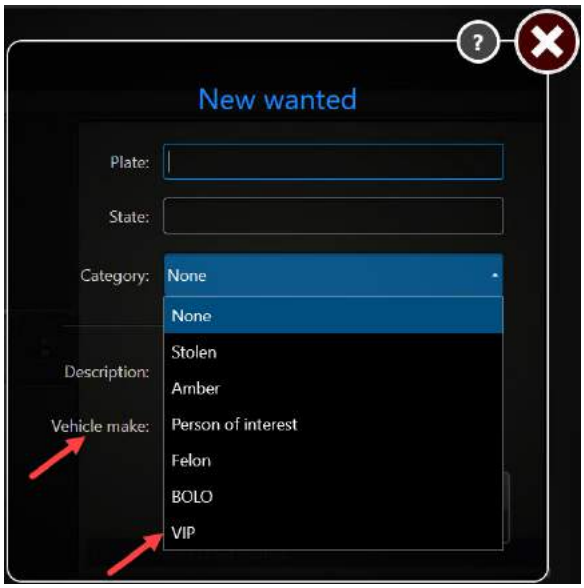
Neste exemplo, foi adicionado o **Atributo:** *Marca do veículo* e a **Categoria:** *VIP*.



3 Clique em **Aplicar**.

O novo atributo e a nova categoria são carregados para o Genetec Patroller™ quando ele for novamente conectado ao Security Center.

Quando o operador adiciona uma placa de veículo *Novo procurado*, o novo campo de Marca do veículo e a opção de categoria VIP estão disponíveis.



Após terminar

Configure os atributos e as categorias de *Novo procurado* no Genetec Patroller™ do Config Tool. Para mais informações, consulte o *Guia do Administrador do Genetec Patroller™*.

45

Sistemas de fiscalização de estacionamento na cidade e na universidade AutoVu™

Esta seção inclui os seguintes tópicos:

- "Sobre a fiscalização municipal de estacionamento" na página 879
- "Sobre a Fiscalização de estacionamento na universidade" na página 881
- "Diferenças entre fiscalização de estacionamento na cidade e na universidade" na página 882
- "Implementar sistemas de fiscalização de estacionamento na cidade e na universidade AutoVu" na página 883
- "Sobre regras de tempo extra" na página 884
- "Criando regras de horas extras" na página 888
- "Configurar regras de tempo extra" na página 889
- "Sobre autorizações" na página 892
- "Criar autorizações de estacionamento" na página 894
- "Configurar autorizações" na página 896
- "Sobre restrições de autorização" na página 897
- "Criando restrições de autorização" na página 898
- "Configurar restrições de autorização" na página 899
- "Configurar estacionamentos no Security Center" na página 901
- "Definir configurações avançadas de autorização" na página 904

Sobre a fiscalização municipal de estacionamento

Fiscalização de estacionamento da cidade é uma instalação de software do Genetec Patroller™ configurada para a fiscalização de autorizações de estacionamento e restrições de tempo extra.

Na fiscalização de estacionamento da cidade, o Genetec Patroller™ combina placas em veículos estacionados para regras de horas extras (regras sobre quanto tempo os veículos estão autorizados a estacionar), listas de autorização (listas de veículos que estão autorizados a estacionar) ou para ambos, regras de horas extra e listas de autorização.

Você também pode usar a Fiscalização Municipal de Estacionamento com imagens de roda para fornecer evidências adicionais de um veículo ter se movido ou não.

Exemplo

Aqui estão alguns exemplos de quando você usaria cada tipo de regra de fiscalização:

- **Regra de hora extra isoladamente:** Para maximizar o rendimento e evitar o abuso de estacionamento gratuito em uma área comercial, os veículos podem estacionar por apenas duas horas nas ruas principais entre as 8:00 e 18:00. Qualquer veículo estacionado por mais de duas horas é uma violação da regra de horas extras. Isso resulta em uma ocorrência de tempo extra no Genetec Patroller™. Neste exemplo, você não precisa de uma lista de autorizações porque não há exceções à regra.
- **Lista de autorizações isolada:** Algumas áreas residenciais permitem que apenas os titulares de autorizações estacionem nas ruas do bairro. Qualquer veículo estacionado na área sem uma licença viola a lista de autorizações. Isso resulta em uma ocorrência de autorização Genetec Patroller™. Neste exemplo, você não precisa de uma regra de horas extras porque não há limites de tempo. Qualquer veículo estacionado sem uma licença válida (por exemplo, licença vencida ou sem autorização) está em violação, independentemente do dia ou hora.
- **Regra de horas extras e lista de autorizações em conjunto:** Algumas áreas residenciais permitem que os titulares de permissões estacionem indefinidamente, e os titulares sem autorizações estacionem por tempo limitado. Qualquer veículo sem autorização que esteja estacionado na área por mais tempo que o permitido pelo limite, viola a regra de horas extras. Isso resulta em um alerta de horas extras. Neste exemplo, você precisa de uma regra de horas extras e uma lista de autorizações para determinar se um veículo estacionado está em violação.

Exemplo

Assista a este vídeo para saber mais. Clique no ícone **Legendas** (**CC**) para ligar a legenda do vídeo em um dos idiomas disponíveis. O vídeo pode não ser exibido no Internet Explorer. Para resolver isso, abra as **Configurações de compatibilidade de exibição** e limpe **Exibir sites da intranet em Visualizar compatibilidade**.

Sobre a fiscalização municipal de estacionamento com imagens da roda

Em um sistema de Fiscalização de estacionamento da cidade com imagens das rodas, o Genetec Patroller™ usa imagens de roda tomadas por "câmeras de pneus" como evidência adicional quanto a um veículo estacionado ter ou não se movido mesmo que por uma pequena distância.

Por exemplo, quando você recebe uma ocorrência de horas extras, você pode observar uma imagem das rodas do veículo e ver pela haste da válvula ou outro ponto de referência (por ex. uma rachadura na calota), que o veículo não se moveu. Esta evidência fotográfica pode ajudar a provar a ofensa de horas extras se o condutor alegar ter deslocado o veículo e depois estacionado novamente na mesma área.

Exemplo

Aqui está um veículo Genetec Patroller™ com uma câmera Sharp e uma única câmera de pneu.

Você não pode fazer imagens de roda em ambos os lados de uma rua ao mesmo tempo.

Para instalações do AutoVu™ que incluam câmeras WMS, a Unidade de Processamento de LPR deve incluir a opção de Navegação. Isto fornece ao sistema informações de navegação adicionais para garantir que a roda do veículo é visível na imagem.

Exemplo

Assista a este vídeo para saber mais. Clique no ícone **Legendas** (**CC**) para ligar a legenda do vídeo em um dos idiomas disponíveis. O vídeo pode não ser exibido no Internet Explorer. Para resolver isso, abra as **Configurações de compatibilidade de exibição** e limpe **Exibir sites da intranet em Visualizar compatibilidade**.

Horas extras a longo prazo

As horas extras a longo prazo são usadas para o estacionamento a longo prazo; isto é, quando os veículos podem estacionar no mesmo espaço por mais de 24 horas. Com as horas extras a longo prazo, você pode especificar um limite de tempo entre 2 a 5 dias. Esta opção define automaticamente a categoria de regra de tempo extra para *Mesma posição*, o que significa que o veículo está em violação se estiver estacionado no mesmo espaço de estacionamento além do limite de tempo especificado.

IMPORTANTE: Você só pode impor uma regra de tempo extra a longo prazo por veículo de patrulha. Se você tiver mais de uma zona de horas extras a longa prazo configurada no Security Center, você deve especificar o nome da zona que deseja que o Genetec Patroller™ exiba. Esta configuração é definida nas configurações avançadas de horas extras do Patroller Config Tool (consulte o *Guia do Administrador do Genetec Patroller™*.

Sobre a Fiscalização de estacionamento na universidade

Fiscalização de estacionamento na universidade é uma instalação de software do Genetec Patroller™ configurada para a fiscalização de estacionamento na universidade: a fiscalização de autorizações de estacionamento agendadas ou restrições de tempo extra. O uso de mapas é obrigatório. O recurso da lista de procurados não está incluído.

O estacionamento na universidade difere do estacionamento na cidade em muitos aspetos. Com estacionamento na universidade:

- Você aplica uma restrição de autorizações a uma ou mais listas de autorizações, para especificar onde e quando as autorizações se aplicam.
- Você pode impor regras de horas extras ou restrições de autorizações para um estacionamento selecionado, mas não ambos ao mesmo tempo.
- As imagens da roda não são suportadas.

Exemplo

Os exemplos a seguir mostram quando você usaria uma regra de horas extras e quando você usaria uma restrição de autorização:

- **Regra para horas extras:** Um campus universitário tem vários lotes de estacionamento reservados para estudantes e docentes, mas também tem áreas de estacionamento convenientemente localizadas que são usadas pelos veículos de entrega para o carregamento ou descarregamento de equipamentos.

  Usando uma regra de tempo extra, você pode permitir que qualquer veículo estacione na área de carregamento a qualquer hora do dia, mas apenas por um tempo limitado (por exemplo, 20 minutos). Um veículo estacionado por mais de 20 minutos é uma violação da regra de tempo extra. Isso resulta em uma ocorrência de tempo extra no Genetec Patroller™. Neste exemplo, você não precisa de uma restrição de permissão porque qualquer veículo pode estacionar, mas apenas por um tempo limitado.
- **Restrição de autorização:** Um estacionamento universitário pode ser usado tanto por professores como por estudantes, mas em momentos diferentes. Professores podem estacionar nos dias da semana das 8:00 às 18:00, enquanto os alunos podem estacionar das 10:00 às 16:00. Isso reserva os espaços de estacionamento privilegiados para os docentes da universidade, mas ainda permite aos estudantes estacionamento conveniente durante aulas em horário de pico. Você não poderá criar este cenário de estacionamento com uma regra de horas extras. Você precisa de uma restrição de autorização e listas de autorizações associadas. Veículos sem autorização, com licença vencida ou estacionados na hora errada, violam a restrição de autorização. Isso resulta em uma ocorrência de autorização Genetec Patroller™.

Tópicos relacionados

Sobre autorizações na página 892

Diferenças entre fiscalização de estacionamento na cidade e na universidade

As regras de fiscalização que você usa, e como você as configura, variam consoante o seu sistema esteja configurado para fiscalização na cidade ou na universidade.

A tabela a seguir mostra quais os conceitos e recursos de fiscalização de estacionamento usados com cada tipo de sistema:

Conceito ou recurso	Fiscalização de Estacionamento Municipal	Fiscalização de Estacionamento Universitário
Fiscalizar autorizações e horas extras simultaneamente	Sim	Não
Horas extras distritais	Sim	Sim
Horas extras de fachada	Sim	Suportado, mas não tipicamente usado.
Horas extras na mesma posição	Sim	Suportado, mas não tipicamente usado.
Múltiplas violações	Sim	Sim
Autorizações	Sim	Sim[1]
Restrições de autorização	Não	Sim
Autorizações compartilhadas	Sim	Sim
Estacionamentos (“zonas”)	Sim	Sim
Imagem da roda	Sim[2]	Não
Hora extra ao longo prazo	Sim[3]	Não
Alertas da lista de procurados	Sim	Sim

[1] As autorizações devem ter restrições de autorização aplicadas a elas na Fiscalização de estacionamento na universidade.

[2] Usado para fornecer provas adicionais de que um veículo não se moveu.

[3] Requer a opção Fiscalização de estacionamento da cidade com imagens das rodas para determinar se um veículo estacionado não se moveu durante o período de tempo extra.

Implementar sistemas de fiscalização de estacionamento na cidade e na universidade AutoVu™

Você pode configurar o seu sistema AutoVu™ móvel especificamente para Fiscalização de estacionamento da cidade (com ou sem imagens de roda) ou para Fiscalização de estacionamento na universidade.

Antes de iniciar

- Realize as tarefas de configuração geral para os sistemas AutoVu™ móveis.

O que você deve saber

- Todos os sistemas de fiscalização de estacionamento exigem capacitação de GPS e mapeamento.

Para implementar um sistema de fiscalização de estacionamento na cidade e na universidade AutoVu™

1 Crie as regras de tempo extra.
2 Crie as listas de autorizações.
3 (Somente *Fiscalização de estacionamento na universidade*) Crie as restrições de autorização.
4 Crie estacionamentos para as suas regras de tempo extra e restrições de autorização.
5 (Somente *Fiscalização de estacionamento da cidade com imagens das rodas*) Para fornecer leituras exatas de odometria ao Genetec Patroller™, calibre as configurações de Navegação AutoVu™ (consulte o *Guia de Instalação de Hardware AutoVu™*).
6 Ative e configure configurações de tempo extra no Genetec Patroller™. Para mais informações, consulte o *Genetec Patroller™ Guia do Administrador*.
7 Ative e configure listas de autorizações no Genetec Patroller™. Para mais informações, consulte o *Genetec Patroller™ Guia do Administrador*.
8 (Somente *Fiscalização de estacionamento da cidade com imagens das rodas*) Defina as configurações do Genetec Patroller™ relacionadas com imagens de rodas. Para mais informações, consulte o *Genetec Patroller™ Guia do Administrador*.
9 Defina as configurações de GPS e Mapas do Genetec Patroller™. Para mais informações, consulte o *Guia do Administrador do Genetec Patroller™*.

Sobre regras de tempo extra

Uma regra de tempo extra é um tipo de entidade que define um limite de tempo estacionado e o número máximo de violações a fiscalizar em um único dia. As regras de tempo extra são usadas na fiscalização de estacionamentos municipais e universitários. Para estacionamentos universitários, uma regra de tempo extra também define a zona de estacionamento em que essas restrições se aplicam.

A regra de tempo extra é baixada para o Genetec Patroller™. No Genetec Patroller™, ocorre um alerta de tempo extra quando o tempo entre duas leituras da mesma placa de veículo está além do limite de tempo especificado na regra de tempo extra. Por exemplo, sua regra de tempo extra especifica um limite de estacionamento de **quatro horas** dentro de um distrito da cidade. O operador do Genetec Patroller™ faz uma primeira passagem pelo distrito às 9:00 da manhã coletando leituras de placas de viatura. O operador faz uma segunda passagem pelo distrito às 13:05 Se uma placa de veículo tiver sido lida durante a primeira e a segunda passagens, o Genetec Patroller™ gera um alerta de tempo extra.

Uma regra de tempo extra é um tipo de regra de alerta. Uma regra de alerta é um método usado pelo AutoVu™ para identificar veículos de interesse. Outros tipos de regras de alerta incluem *lista de procurados*, *autorização* e *restrição de autorização*. Quando a leitura de uma placa de veículo corresponde a uma regra de alerta, ela é chamada de *alerta*. Quando um par de leituras de placa de veículo (mesmo placa lida em dois momentos diferentes) viola uma regra de tempo extra, é chamado de *alerta de tempo extra*.

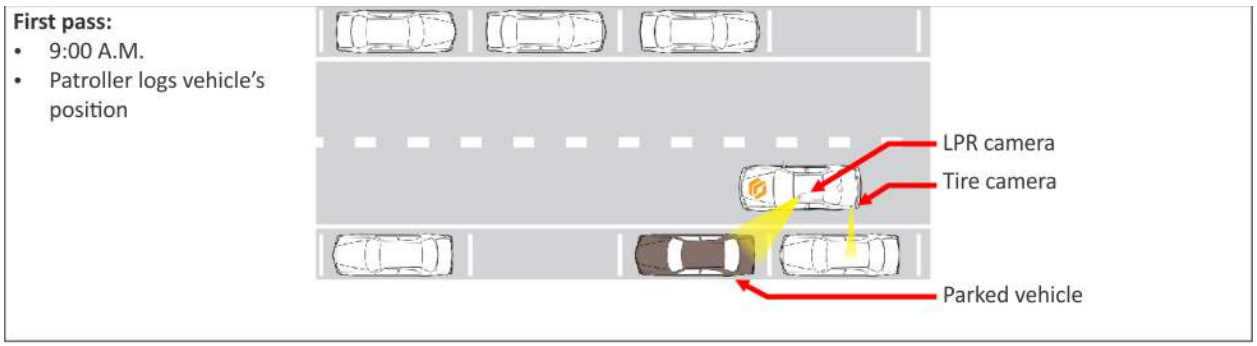
Na fiscalização municipal, a opção de WMS pode ser usada para fornecer evidências adicionais da violação, mostrando se o veículo se moveu ou não mesmo que por uma pequena distância.

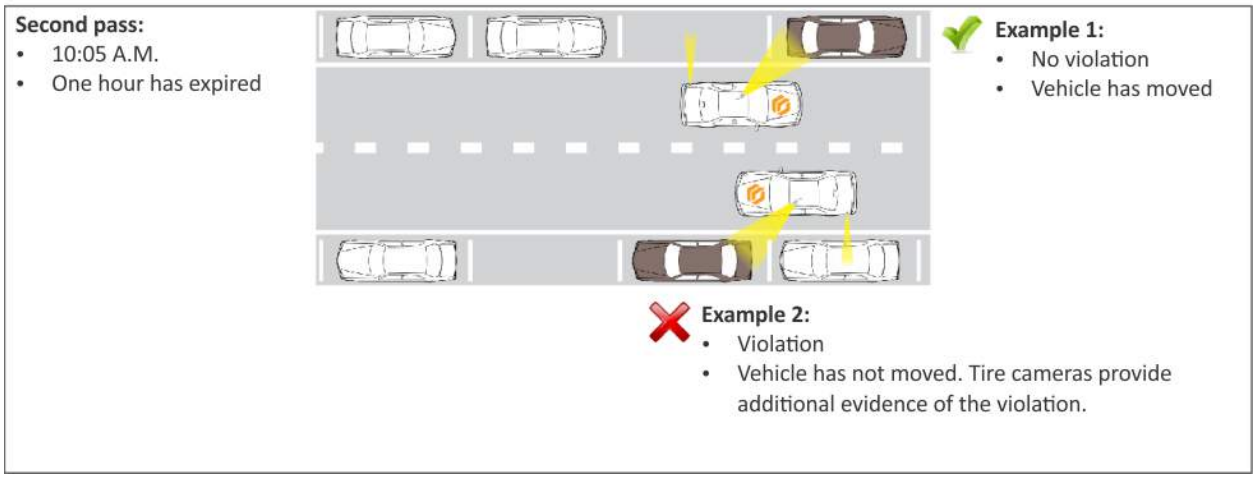
Regras de tempo extra na mesma posição

As regras de tempo extra na *Mesma posição* especificam quanto tempo um veículo pode estacionar em um *espaço de estacionamento individual* em uma rua específica.

Exemplo

A regra de tempo extra indica que os veículos podem estacionar por uma hora em qualquer espaço de estacionamento na rua X. Você faz uma primeira passagem às 9:00 coletando leituras de placas de veículo. Você então faz uma segunda passagem às 10:05. Se o Genetec Patroller™ ler a mesma placa no mesmo espaço de estacionamento, o Genetec Patroller™ gera um alerta de tempo extra.





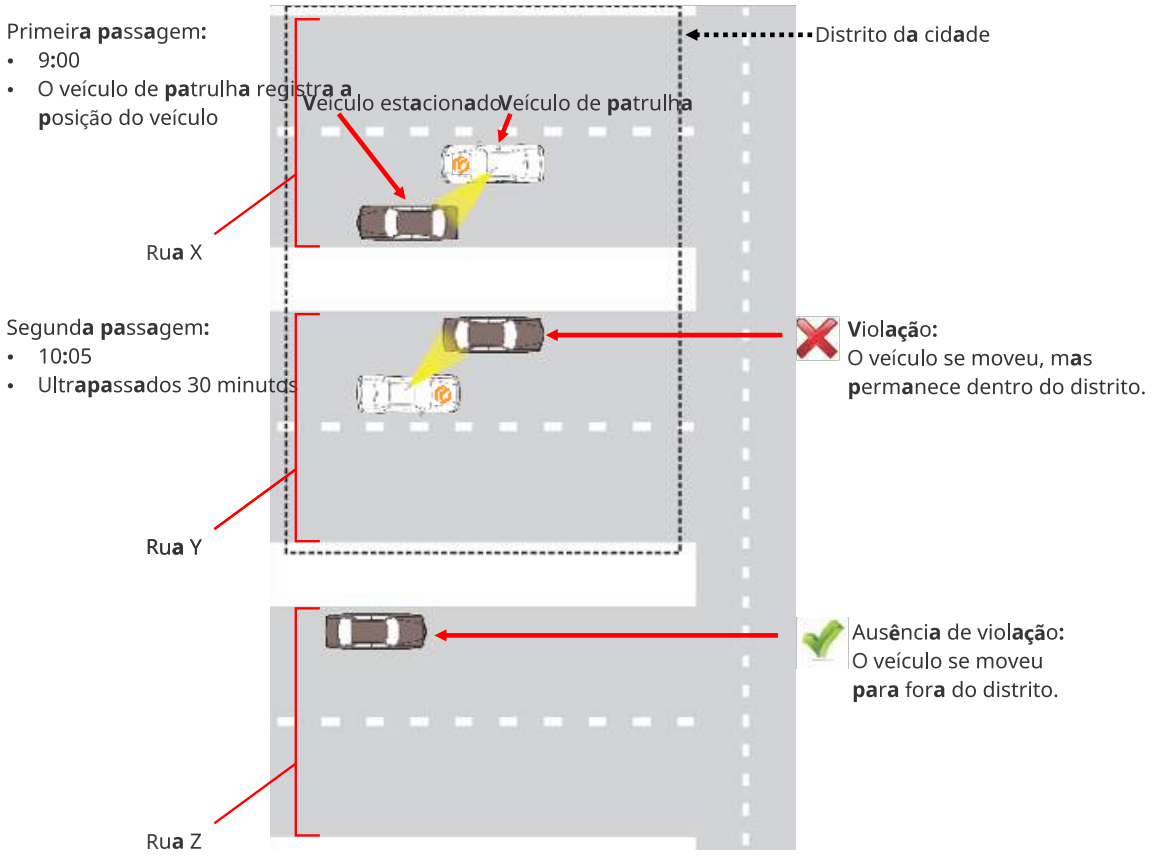
Regras de tempo extra distritais

A fiscalização de *Estacionamento distrital* é um tipo de regra de tempo extra que especifica quando um veículo está autorizado a estacionar *dentro de uma localização geográfica específica* (por exemplo, um distrito da cidade).

As fronteiras de um "distrito" não são definidas em Security Center do Config Tool (por exemplo, desenhando um polígono em um mapa) e não há correlação com regiões ou municípios formais de uma cidade. Existe um distrito onde o usuário do Genetec Patroller™ opta por fazer a fiscalização.

Exemplo

A regra de tempo extra indica que, entre as 9:00 e as 17:00 da manhã nos dias da semana, os veículos podem estacionar por apenas 30 minutos dentro do distrito definido pela Rua X e Rua Y. Você faz uma primeira passagem pelo distrito às 9:30 coletando leituras de placa de veículos. Você então faz uma segunda passagem pelo distrito às 10:05. Se o veículo de patrulha ler a mesma placa dentro do mesmo distrito (independentemente de o veículo ter se movido ou não), o veículo está em violação da regra de tempo extra e você recebe um alerta de tempo extra.



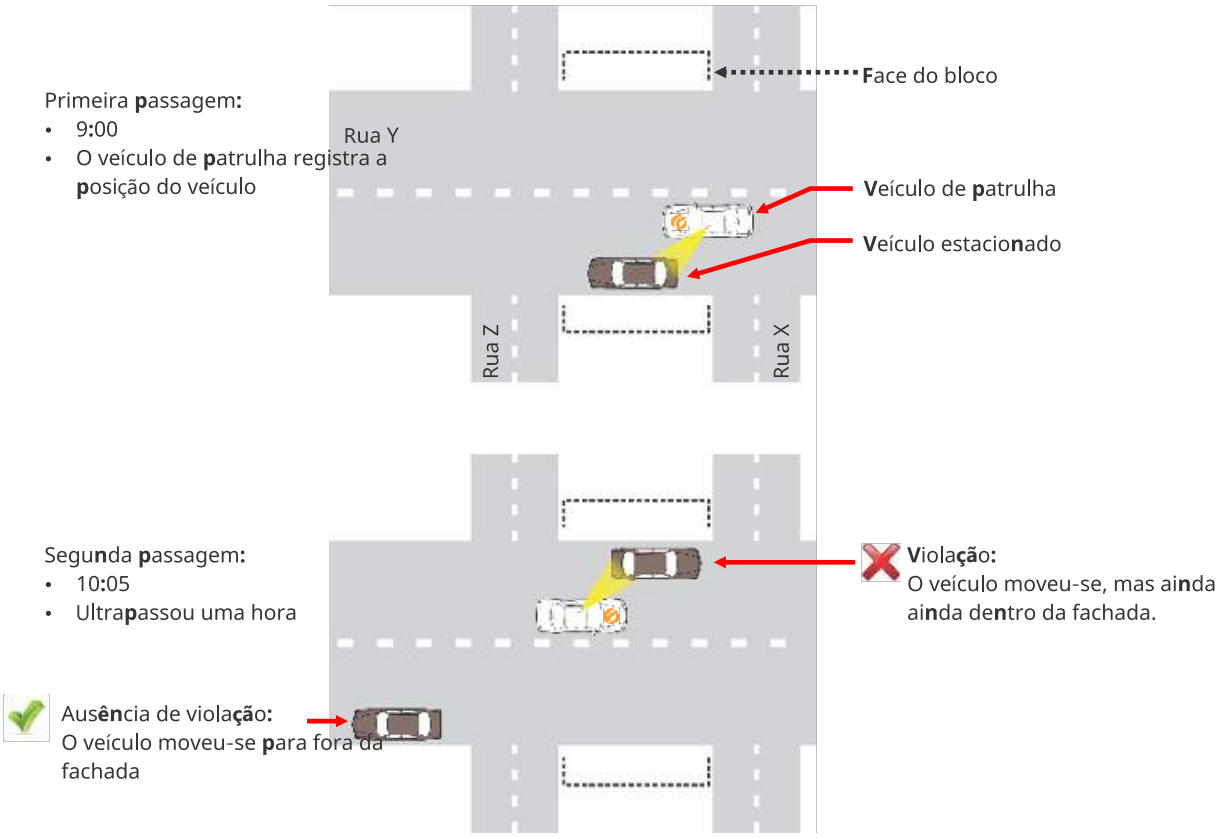
Regras de tempo extra de fachada

A fiscalização de *Estacionamento de fachada* é um tipo de regra de tempo extra que especifica quando um veículo tem permissão para estacionar *em ambos os lados de uma rua*, entre ruas interseccionadas.

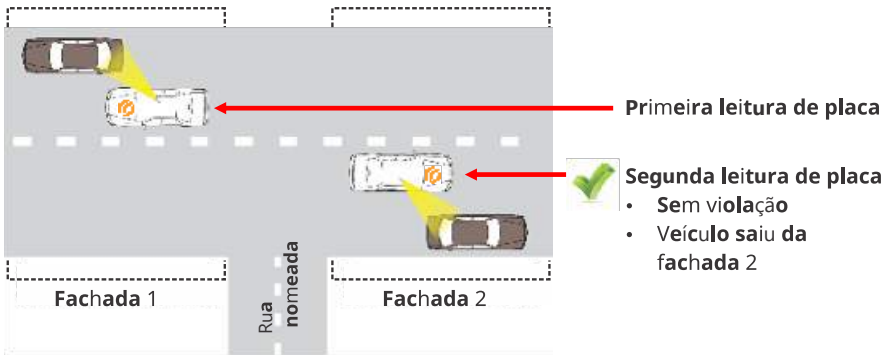
As fronteiras de uma "fachada" não são definidas em Config Tool (por exemplo, desenhando um polígono em um mapa). Elas são definidas no local para cada leitura de placa de veículo individual. Por exemplo, quando um usuário do Genetec Patroller™ seleciona uma regra de tempo extra de fachada e, em seguida, lê uma placa de veículo, o Genetec Patroller™ usa o GPS para determinar a fachada para essa leitura da placa de veículo em particular, com base nos cruzamentos mais próximos da posição do veículo estacionado.

Exemplo

A regra de tempo extra indica que os veículos podem estacionar por uma hora em qualquer lado da Rua Y, entre as Ruas X e Z. Você faz uma primeira passagem às 9:00 coletando leituras de placas de veículo. Você então faz uma segunda passagem pela fachada às 10:05. Se o Genetec Patroller™ ler a mesma placa dentro da mesma fachada (independentemente de o veículo ter se movido ou não), o veículo está em violação da regra de tempo extra e você recebe um alerta de tempo extra.



NOTA: O Genetec Patroller™ considera as "intersecções em T" como fronteiras válidas de uma fachada. Por exemplo, no seguinte cenário, o Genetec Patroller™ *não* acionaria um alerta de tempo extra, porque a interseção em T é vista como o fim da *Fachada 1* e o começo da *Fachada 2*.



Criando regras de horas extras

Você pode criar uma entidade de regra de hora extra em Security Center Config Tool. Depois de criar a entidade, você deve definir suas configurações para o seu cenário de fiscalização.

O que você deve saber

Você pode usar as regras de horas extras tanto para Fiscalização Municipal de Estacionamento quanto para Fiscalização de Estacionamento Universitário.

Para criar uma regra de horas extras:

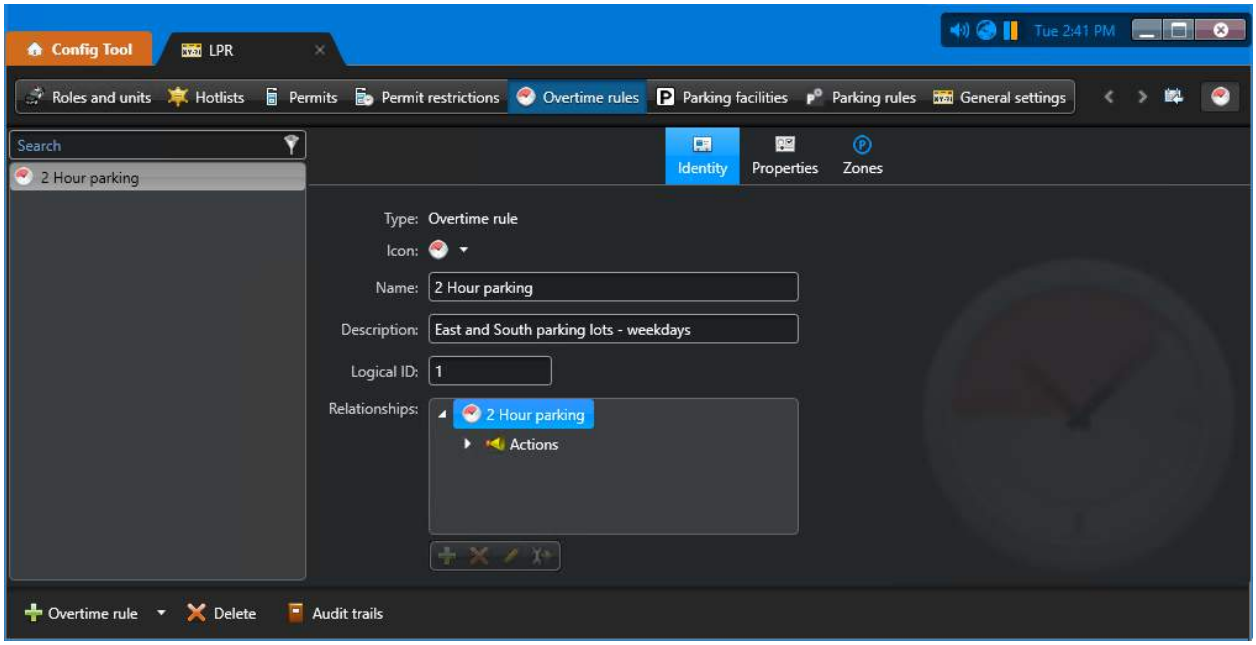
1 Na página inicial do Config Tool, clique em **LPR** > **Regras de tempo extra**e, em seguida, clique em **Regra de tempo extra** ( ).

2 Na aba **Identidade**, digite as informações exigidas:

- **Nome:** Em Fiscalização de estacionamento da cidade, este nome aparece no Genetec Patroller™ na página de seleção de regra de tempo extra. Na Fiscalização de estacionamento universitário, este nome aparece junto ao nome do estacionamento na página de seleção de zona.

  DICA: Selecione um nome que descreva os detalhes do cenário de fiscalização. Isso torna mais fácil selecionar no Genetec Patroller™ quando você tem mais de um disponível.
- **(Opcional) Descrição:** Você pode adicionar uma descrição mais longa para a regra. Este campo não aparece no Genetec Patroller™.
- **(Opcional) ID Lógica:** Digite uma ID Lógica, se aplicável.

3 Clique em **Aplicar**.



A regra de tempo extra aparece em uma visualização de lista simples que exibe todas as regras de tempo extra em seu sistema. O Genetec Patroller™ baixa regras de tempo extra quando se conecta ao Security Center.

Após terminar

Configure a regra de tempo extra.

Configurar regras de tempo extra

Para usar uma entidade de regra de tempo extra depois de tê-la adicionado no Security Center, você deve configurá-la para o seu cenário de fiscalização.

Antes de iniciar

Crie a regra de tempo extra.

O que você deve saber

Você deve configurar uma área de fiscalização (ou estacionamento) para cada restrição de autorização e regra de tempo extra que você criar.

Para configurar uma regra de horas extras:

1 Na página inicial do Config Tool, clique em **LPR** > **Regras de tempo extra**e selecione a regra de tempo extra que deseja configurar.

2 Clique na guia **Propriedades.**

3 Selecione uma **Cor** para a regra de tempo extra.

Esta será a cor da tela de ocorrências de tempo extra no Genetec Patroller™ e no Security Desk, bem como das leituras de placas pendentes de fiscalização no mapa do Genetec Patroller™.

4 (Somente Fiscalização de estacionamento da cidade com imagens das rodas) Selecione a **Posição de estacionamento do veículo**.

Esta opção informa ao Genetec Patroller™ quais parâmetros usar para imagens de roda: Paralelo ou Em ângulo (45 graus).

NOTA: Você não pode usar a mesma regra de horas extras para a fiscalização de estacionamento em paralelo e em ângulo. Se você estiver fazendo ambos os tipos de fiscalização, você deve criar entidades separadas de regras de horas extras para cada.

5 (Opcional) Selecione **Tempo extra de longo prazo** para permitir que veículos estacionem no mesmo local por mais de 24 horas.

Quando selecionado, o limite de tempo de estacionamento é especificado em dias (2 a 5 dias) e a opção *Fiscalização de estacionamento* é automaticamente definida para *Mesma posição*. Esta opção define automaticamente o regulamento de estacionamento como mesma posição, o que significa que o veículo estaciona por horas extras quando permanece no mesmo espaço de estacionamento além do limite de tempo de estacionamento definido para esse espaço.

NOTA: Esta configuração se aplica a Fiscalização de estacionamento da cidade com ou sem imagens das rodas do AutoVu™ Genetec Patroller™. *Imagens de rodas* é recomendado se você planeja usar esta regra para detectar veículos estacionados por longo prazo para que você possa distinguir entre alguém que estaciona na mesma posição e um veículo que foi abandonado.

IMPORTANTE: Você só pode impor uma regra de *Tempo extra de longo prazo* por Directory.

6 Na lista de **Fiscalização de estacionamento**, selecione o tipo de área de estacionamento restrito que se aplica ao limite de tempo: um único lugar de estacionamento, um bairro da cidade ou ambos os lados de um quarteirão:

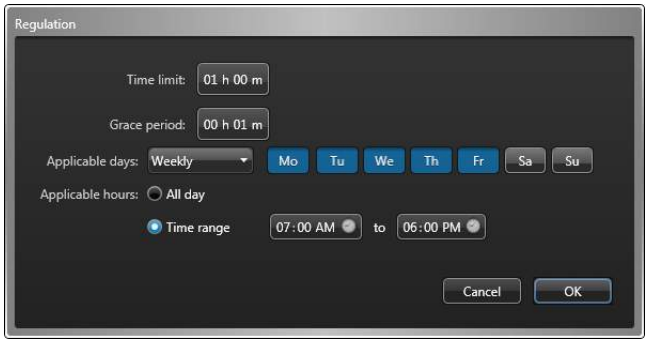
- **Mesma posição:** Um veículo está estacionado em tempo extra se estacionar no mesmo local por mais tempo do que o limite de tempo especificado. Por exemplo, sua regra de horas extras especifica um limite de estacionamento de uma hora para um único espaço de estacionamento. O operador do Genetec Patroller™ faz uma primeira passagem pelo distrito às 9:00 da manhã coletando leituras de placas de viatura. Você então faz uma segunda passagem às 10:05. Se ler a mesma placa no mesmo local duas vezes, o Genetec Patroller™ gera uma ocorrência de tempo extra.

  IMPORTANTE: Para que este recurso funcione, o Genetec Patroller™ precisa de capacidade GPS.

- **Distrito:** Um veículo está estacionado em tempo extra se estiver estacionado em qualquer lugar dentro de um bairro da cidade (uma área geográfica) por mais tempo do que o prazo especificado. Por exemplo, sua regra de horas extras especifica um limite de estacionamento de quatro horas dentro de um distrito da cidade. O usuário do Genetec Patroller™ faz uma primeira passagem pelo bairro às 9:00 da manhã coletando leituras de placa de veículo. O operador faz uma segunda passagem pelo distrito às 13:05 Se ler a mesma placa no mesmo bairro duas vezes, o Genetec Patroller™ gera uma ocorrência de tempo extra.
- **Fachada (2 lados):** Um veículo está estacionado em tempo extra se estiver estacionado em qualquer um dos lados de uma estrada entre duas interseções por mais tempo do que o limite de tempo especificado. Por exemplo, sua regra de tempo extra especifica um limite de estacionamento de 1 hora no espaço de uma fachada. O operador do Genetec Patroller™ faz uma primeira passagem pela fachada às 9:00 da manhã coletando leituras de placas de viatura. O operador faz uma segunda passagem na fachada às 10:05 Se ler a mesma placa no espaço da mesma fachada duas vezes, o Genetec Patroller™ gera uma ocorrência de tempo extra.

7 Para definir os parâmetros da regra de tempo extra (por exemplo, limite de tempo, período de cortesia, dias aplicáveis etc.), em **Regulamentação**, clique em **Adicionar um item** ( ).

8 Na caixa de diálogo **Regulamentação**, configure o seguinte e clique em **OK**:



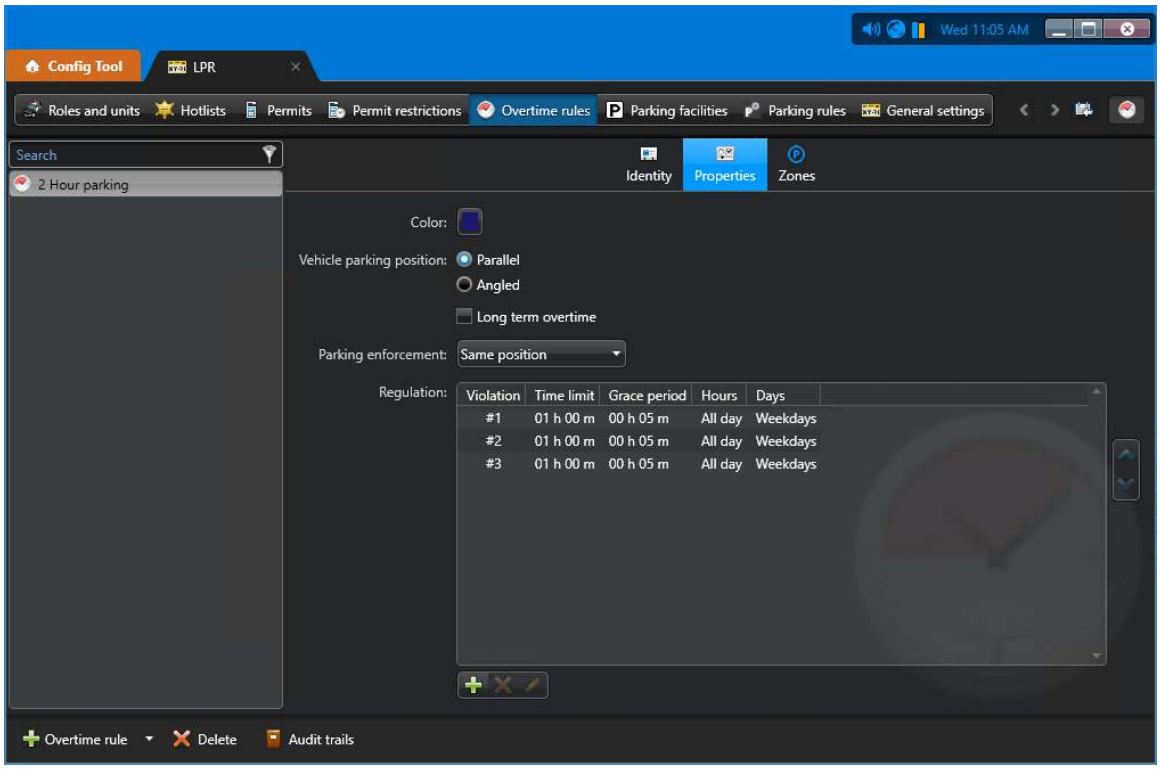
- **Limite de horário:** O limite de tempo de estacionamento em horas e minutos.
- **Período de tolerância:** Para efeitos de fiscalização de leniência, o período de cortesia é o tempo além do limite de tempo de estacionamento durante o qual a violação de tempo extra é dispensada. Por exemplo, o Genetec Patroller™ gerará uma ocorrência de tempo extra para uma placa quando o tempo entre a captura da mesma placa exceder o **Limite de tempo** mais o **Período de cortesia**.
- **Dias aplicáveis:** Dias da semana em que o prazo é aplicado. Você pode selecionar um intervalo de tempo semanal na lista suspensa:
  - **Sempre:** 7 dias por semana
  - **Dias úteis:** De segunda a sexta
  - **Personalizado:** Para criar um intervalo de tempo personalizado, clique nos dias.
- **Horas aplicáveis:** Selecione quando o limite de tempo é aplicado.
  - **Dia inteiro:** 24 horas por dia
  - **Intervalo de tempo:** Clique no campo seletor de data e use o campo de texto ou o relógio gráfico para especificar a hora.

9 (Opcional) Para definir o número máximo de citações que podem ser emitidas para o mesmo veículo e mesma infração de tempo extra, adicione regulamentações adicionais. No seguinte exemplo, um veículo pode ser sancionado com três violações da regra de tempo extra de uma hora em um dia:

Aqui estão dois exemplos para explicar a diferença entre ter uma regra de horas extras com uma violação e uma regra de horas extras com múltiplas violações:

- **Regra de horas extras com uma violação:** Sua regra de horas extras permite que os veículos estacionem por uma hora em uma rua específica. Se um veículo estiver estacionado naquela área por mais de uma hora, ele viola a regra de horas extras. Isso resulta em uma ocorrência de tempo extra no Genetec Patroller™. No entanto, uma vez que a regra de horas extras permite apenas uma violação, mesmo que o veículo esteja estacionado no mesmo lugar o dia todo, você só receberá um alerta de hora extra para ele. Nesse cenário, você emitiria uma multa para a violação.

- **Regra de horas extras com várias violações:** Sua regra de tempo extra permite que veículos estacionem por uma hora em uma rua específica, mas seu sistema está configurado para permitir que um veículo acumule, por exemplo, até três violações da regra de uma hora. Se um veículo estiver estacionado naquela área o dia todo, e você patrulhar a área três vezes durante o turno, você receberá três violações da regra de tempo extra e três ocorrências de tempo extra separadas no Genetec Patroller™. Nesse cenário, você emitiria três multas para a mesma violação.



DICA: Observe que, neste exemplo, as três regulamentações somente são válidas em dias úteis. Isto garante que, se o operador do Genetec Patroller™ selecionar erradamente esta zona de tempo extra no fim de semana, nenhuma citação será emitida.

10 Clique em **Aplicar**.

A regra de tempo extra está configurada e será baixada para o Genetec Patroller™ na próxima vez que ele se conectar ao Security Center.

Sobre autorizações

Uma autorização é um tipo de entidade que define uma lista única de detentores de autorização de estacionamento. Cada detentor de autorização é caracterizado por uma categoria (zona de autorização), um número de placa de licença, um estado emissor da licença e, opcionalmente, um período de validade da autorização (data de entrada em vigor e data de expiração). As autorizações são usadas na fiscalização de estacionamento tanto municipal quanto universitário.

A entidade de autorização pertence a uma família de métodos usados pelo AutoVu™ para identificar veículos de interesse, chamados regras de ocorrências. Outros tipos de regras de ocorrências incluem *lista de procurados*, *horas extras*, e *restrição de autorização*. Quando a leitura de uma placa de veículo corresponde a uma regra de alerta, ela é chamada de *alerta*. Quando uma leitura não corresponde a nenhuma autorização carregada no Genetec Patroller™, ela gera uma *ocorrência de autorização*.

Autorizações na Fiscalização Municipal de Estacionamento

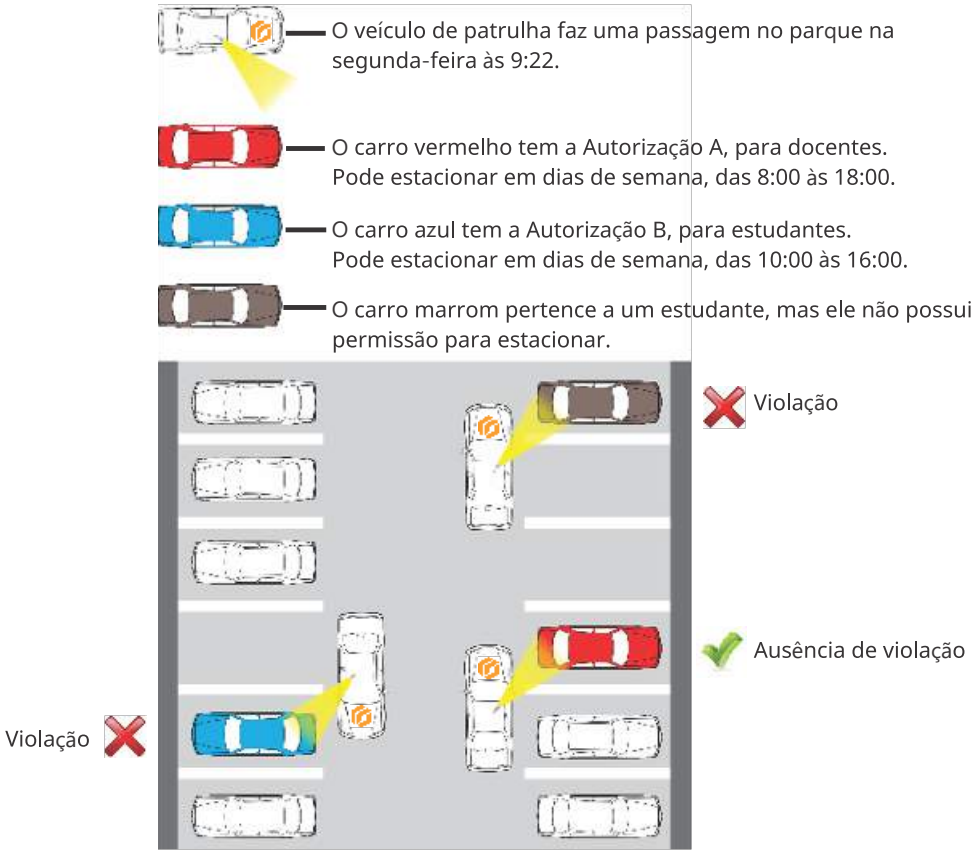
Na Fiscalização Municipal de Estacionamento, você cria a lista de autorizações e configura suas propriedades básicas, mas não precisa definir uma restrição estacionamento ou de autorização. É a cidade ou município que decide quando e onde a autorização é aplicável. O operador do veículo de patrulha escolhe qual autorização deve impor no Genetec Patroller™ com base nas placas de regra de estacionamento que aparecem na rua.

Autorizações na Fiscalização de Estacionamento Universitário

Na Fiscalização de estacionamento na universidade, você cria e configura uma lista de autorizações da mesma forma que você faria na Fiscalização de estacionamento da cidade, mas você também precisa atribuir *restrições de autorização* e estacionamentos para criar uma "zona" de fiscalização que é baixada para o Genetec Patroller™. Esta configuração adicional é necessária porque o veículo de patrulha está monitorando lotes de estacionamento individuais, não as ruas da cidade com regulamentos específicos já existentes.

Exemplo

Neste exemplo, você usa uma restrição de autorização para especificar diferentes limites de tempo para diferentes titulares de autorizações.



Autorizações compartilhadas

Uma lista de autorizações inclui um campo chamado*ID da Autorização*, que permite que diferentes veículos compartilhem a mesma licença ao ter o mesmo valor de *ID da Autorização* no arquivo de origem da lista de autorização. Por exemplo, uma autorização de carro compartilhado poderia ser compartilhada entre vários veículos. Cada membro do compartilhamento tem um turno levando os outros membros para o trabalho ou para a escola, portanto, cada membro precisa compartilhar a mesma autorização para estacionar.

No entanto, a autorização ainda se aplica a *um veículo por vez*. Por exemplo, se todos os quatro membros do compartilhamento de carro decidirem levar os seus próprios veículos um dia, eles não poderão todos usar aquela autorização de carro compartilhado ao mesmo tempo. Genetec Patroller™ Permite que um veículo com a autorização de carro compartilhado estacione (a primeira placa de veículo detectada), mas vai gerar uma ocorrência de *Autorização compartilhada* para todos os outros veículos vistos com a mesma autorização.

NOTA: Para obter mais informações sobre como funcionam autorizações compartilhadas em instalações AutoVu™ Free-Flow, consulte Sobre autorizações compartilhadas no AutoVu™ Free-Flow na página 848.

Tópicos relacionados

Sobre restrições de autorização na página 897

Criar autorizações de estacionamento

Para usar as entidades de autorização no Security Center, você deve criar a autorização, mapeá-la em seu arquivo de texto de origem e configurá-la para seu cenário de fiscalização.

O que você deve saber

Se você estiver usando a Fiscalização de estacionamento na universidade, você também deve aplicar restrições às autorizações para criar uma regra de fiscalização.

Para criar uma autorização:

1 Na página inicial do Config Tool, clique em **LPR > Autorizações**e, em seguida, clique em **Autorização** ( ).

O assistente **Criar uma autorização** será aberto.

2 Na página **Informações básicas**, no campo **Nome da entidade**, digite um nome para a autorização.

Este nome aparece no Genetec Patroller™ na página de seleção da autorização.

IMPORTANTE: O nome da entidade de autorizações deve coincidir com o campo **Categoria** do arquivo de origem da lista de autorizações.

3 (Opcional) No campo **Descrição da entidade**, digite uma descrição para a nova autorização e clique em **Próximo**.

Este campo não aparece no Genetec Patroller™.

4 Digite o **Caminho** no computador onde o arquivo de origem da lista de autorizações está localizado.

Se você começar a digitar um caminho para uma unidade de rede, os campos **Nome do usuário** e **Senha** aparecem e você precisará digitar o nome de usuário e a senha para acessar a unidade de rede.

5 Se os campos de atributos no arquivo de texto de origem variarem em comprimento, coloque a opção **Usar delimitadores** em **Ligado** e digite o tipo de caractere (delimitador) usado para separar cada campo.

Por padrão, **Usar delimitadores** está definido como **Ligado** e o delimitador especificado é **ponto e vírgula** (;). Se o seu arquivo de texto de origem for feito de campos de comprimento fixo, defina **Usar delimitadores**para **Desligado**. O Security Center suporta os seguintes delimitadores:

- Dois pontos (:)
- Vírgula (,)
- Ponto e vírgula (;)
- Tab (digitar “Tab”)

IMPORTANTE: Se o seu arquivo de origem da lista usar Tab como delimitador, use apenas um espaço de Tab. Não use mais do que um espaço de Tab para alinhar as colunas em seu arquivo ou o Security Center pode não ser capaz de analisar a lista de autorizações.

NOTA: O número máximo de entradas é de 1,8 milhões ao usar o Genetec Patroller™ no modo de 64 bits. Adicionar mais entradas faz com que o sistema responda lentamente.

6 (Opcional) Se você não desejar que os usuários tenham permissão para editar esta autorização no Security Desk, desative **Visível no editor**.

NOTA: Para editar uma autorização no Security Desk, os usuários devem ter o privilégio *Editor de lista de procurados e autorização*.

7 Configure os **Atributos** da autorização e clique em **Próximo**. Veja Configurando lista de procurados padrão e atributos de autorização na página 808.

8 Na página **Atribuição de LPR Manager**, escolha uma das seguintes opções e clique em **Próximo**.

- **Todos os LPR Managers**. Todos os LPR Managers e todas as entidades configuradas para herdar as suas listas de procurados suas autorizações sincronizarão a nova autorização.

NOTA: LPR Managers futuros não sincronizarão automaticamente a nova autorização.

- **LPR Managers específicos**. Somente os LPR Managers selecionados e as entidades que herdam as autorizações deles sincronizarão a nova autorização.

  NOTA: As entidades criadas no futuro que forem configuradas para herdar autorizações de um dos LPR Managers selecionados também sincronizarão a autorização.

- **Atribuir depois**. Nenhum LPR Manager ou nenhuma entidade associada existente irão sincronizar a nova autorização. Para obter mais informações sobre como atribuir uma autorização a um LPR Manager mais tarde, consulte Selecionar quais listas de procurados e autorizações um veículo de patrulha monitora na página 791.

9 Na página **Atribuição específica de unidade**, selecione os veículos de patrulha e/ou câmeras Sharp específicos que sincronizarão a nova autorização e clique em **Próximo**.

10 (Opcional) Se você possuir campos personalizados em sua autorização, insira os valores apropriados na página **Campos personalizados** e clique em **Próximo**.

NOTA: A página **Campos personalizados** somente aparece se houver campos personalizados em sua lista de procurados.

11 Na janela **Resumo de criação**, verifique se as informações da sua autorização estão corretas e clique em **Próximo**.

12 Na janela **Resultado da criação de entidade**, você receberá uma notificação quanto à sua operação ter sido bem-sucedida ou não.

13 (Opcional) Escolha um dos seguintes:

- **Editar esta autorização**. Abre a tarefa **Editor de lista de procurados e autorização** para que você possa editar a autorização.

  NOTA: Para editar uma autorização, você deve ter o privilégio *Editor de lista de procurados e autorização*.

- **Criar uma autorização com base nesta autorização:** Crie uma nova autorização que use as mesmas configurações que a autorização que você acabou de criar. Só é necessário especificar **Nome da entidade**, **Descrição da entidade** e **Caminho da autorização**.

14 Clique em **Fechar**.

A entidade de autorização é configurada e ativada no Security Center.

Configurar autorizações

Você pode modificar suas definições de configuração de autorizações após uma entidade de autorização ter sido adicionada ao Security Center.

Antes de iniciar

Crie a autorização.

O que você deve saber

O arquivo de texto de origem deve estar localizado na unidade local do computador do LPR Manager (por exemplo, a unidade C) ou em uma unidade de rede acessível a partir do computador que hospeda o LPR Manager.

Para configurar uma autorização:

1 Na página inicial do Config Tool, clique em **LPR** > **Autorizações** e selecione a autorização que deseja configurar.

2 Na aba **Identidade**, digite uma **Descrição** para a autorização e clique em **Aplicar**.

Você pode adicionar uma descrição mais longa para a autorização. Este campo não aparece no Genetec Patroller™.

3 Na aba **Propriedades**, digite o **Caminho** no computador onde o arquivo de texto de origem da lista de autorizações se encontra.

Se você começar a digitar um caminho para uma unidade de rede, os campos **Nome do usuário** e **Senha** aparecem e você precisará digitar o nome de usuário e a senha para acessar a unidade de rede.

4 Se os campos de atributos no arquivo de texto de origem variarem em comprimento, coloque a opção **Usar delimitadores** em **Ligado** e digite o tipo de caractere (delimitador) usado para separar cada campo.

Por padrão, **Usar delimitadores** está definido como **Ligado** e o delimitador especificado é **ponto e vírgula** (;). Se o seu arquivo de texto de origem for feito de campos de comprimento fixo, defina **Usar delimitadores**para **Desligado**. O Security Center suporta os seguintes delimitadores:

- Dois pontos (:)
- Vírgula (,)
- Ponto e vírgula (;)
- Tab (digite "Tab")

IMPORTANTE: Se o seu arquivo de origem da lista usar Tab como delimitador, use apenas um espaço de Tab. Não use mais do que um espaço de Tab para alinhar as colunas em seu arquivo ou o Security Center poderá não ser capaz de analisar a lista de autorizações.

5 Decida se os usuários podem editar essa autorização no Security Desk.

6 Configure os **Atributos** do arquivo de texto da lista de autorizações para que o Genetec Patroller™ possa analisar as informações da lista.

7 Clique em **Aplicar**.

Sobre restrições de autorização

Uma restrição de autorização é um tipo de entidade que aplica restrições de tempo a uma série de autorizações de estacionamento para uma dada zona de estacionamento. As restrições de autorização são apenas usadas por veículos de patrulha configurados para Fiscalização de estacionamento na universidade.

Diferentes restrições de horário podem ser aplicadas a diferentes *autorizações*. Por exemplo, uma restrição de autorização pode limitar o estacionamento na zona A de segunda a quarta-feira para detentores da autorização P1, e de quinta a domingo para detentores da autorização P2.

A entidade restrição de autorização é um tipo de regra de alerta. Uma regra de alerta é um método usado pelo AutoVu™ para identificar veículos de interesse. Outros tipos de regras de ocorrências incluem *lista de procurados, hora extra* e *autorização*. Quando a leitura de uma placa de veículo corresponde a uma regra de alerta, ela é chamada de *alerta*. Quando a leitura de placa corresponde à restrição da autorização, ela gera uma *ocorrência de autorização*. Além disso, uma *ocorrência de autorização compartilhada* ocorre quando duas placas que compartilham o mesmo ID de autorização são lidas na mesma área de estacionamento dentro de um período específico.

Tópicos relacionados

Sobre autorizações na página 892

Criando restrições de autorização

Você pode adicionar uma entidade de restrição de autorização no Security Center do Config Tool para aplicar restrições a uma autorização. Depois de criar a entidade, você definirá as configurações para o seu cenário de fiscalização.

Antes de iniciar

Crie a autorização e configure a autorização.

O que você deve saber

Se você estiver usando a Fiscalização de estacionamento na universidade, você deve aplicar restrições às autorizações que adicionar para criar uma regra de fiscalização. Genetec Patroller™ baixa restrições de autorização quando se conecta ao Security Center.

Para criar uma restrição de autorização:

1 Na página inicial do Config Tool, clique em **LPR** > **Restrições de autorização**e, em seguida, clique em **Restrição de autorização** ( ).

Uma nova entidade de restrição de autorização é adicionada na lista de todas as restrições de autorização em seu sistema.

2 Na aba **Identidade**, digite as informações exigidas:

- **Nome:** Em Fiscalização de estacionamento da cidade, este nome aparece no Genetec Patroller™ na página de seleção de regra de tempo extra. Na Fiscalização de estacionamento universitário, este nome aparece junto ao nome do estacionamento na página de seleção de zona.

  DICA: Selecione um nome que descreva os detalhes do cenário de fiscalização. Isso torna mais fácil selecionar no Genetec Patroller™ quando você tem mais de um disponível.
- **(Opcional) Descrição:** Você pode adicionar uma descrição mais longa para a regra. Este campo não aparece no Genetec Patroller™.
- **(Opcional) ID Lógica:** Digite uma ID Lógica, se aplicável.

3 Clique em **Aplicar**.

Após terminar

Configure as restrições de autorização.

Configurar restrições de autorização

Depois de ter criado uma entidade de restrição de autorização no Security Center do Config Tool, você precisa configurá-la para seu cenário de fiscalização.

Antes de iniciar

Crie a restrição de autorização.

O que você deve saber

Você deve configurar uma área de fiscalização (ou estacionamento) para cada restrição de autorização e regra de tempo extra que você criar.

Para configurar uma restrição de autorização:

1 Na página inicial do Config Tool, clique em **LPR** > **Restrições de autorização**.

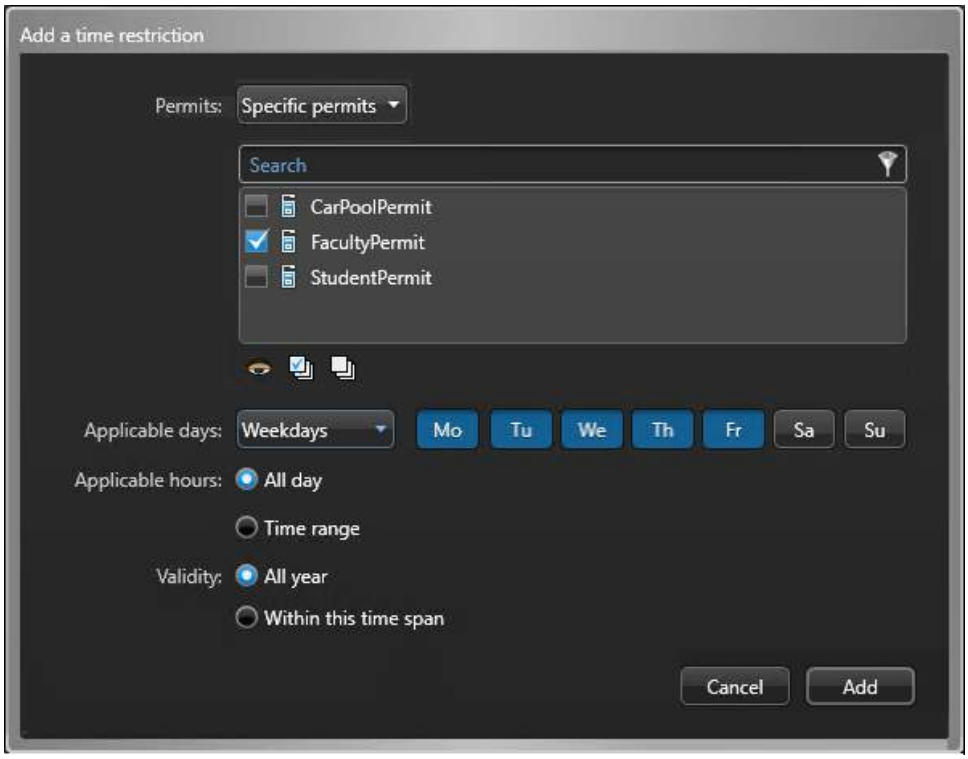
2 Selecione a restrição de autorização a configurar e clique na aba **Propriedades**.

3 Para atribuir uma cor à restrição de autorização, clique no ícone **Cor**, selecione uma cor e clique em **OK**.

A cor é exibida na tela de ocorrências de autorização no Genetec Patroller™ e no Security Desk, bem como nas leituras de placas pendentes de fiscalização no mapa do Genetec Patroller™.

4 Para selecionar quando esta restrição se aplica, clique em **Adicionar um item** ( ).

A janela **Adicionar uma restrição de tempo** é aberta.



5 Na lista suspensa **Autorizações**, selecione a quais autorizações a restrição se aplica:

- **Todo mundo:** O estacionamento fica disponível para todos, independentemente deles terem ou não uma autorização. Nenhuma restrição é fiscalizada durante o período especificado. Esta restrição é usada com outras restrições como uma substituição temporária. Por exemplo, se uma universidade estiver promovendo um jogo, o estacionamento poderá ser disponibilizado para todos durante o jogo em vez de titulares de autorizações específicas.

- **Nenhuma autorização:** Somente veículos sem autorizações podem estacionar. Por exemplo, você pode usar esse tipo de restrição para reservar uma zona para o estacionamento dos visitantes. Um leitura de placa que corresponda a qualquer uma das autorizações baixadas para o Genetec Patroller™ aciona uma ocorrência.
- **Todas as autorizações:** Somente veículos com autorização podem estacionar. Um leitura de placa que não corresponda a qualquer uma das autorizações baixadas para o Genetec Patroller™ aciona uma ocorrência.
- **Autorizações específicas:** Somente veículos que tenham uma ou mais das autorizações especificadas podem estacionar. Um leitura de placa que não corresponda a nenhuma das autorizações especificadas levanta um alerta.

Quando várias restrições de tempo se aplicam em um determinado momento, os conflitos são resolvidos avaliando as restrições na seguinte ordem: 1. *Todos*, 2. *Sem autorização*, 3. *Todas as autorizações*, 4. *Autorizações específicas*. Além disso, um alerta é levantado quando uma licença correspondente não é válida (ainda não é efetiva ou já expirou).

6 Na opção **Dias aplicáveis**, selecione os dias da semana em que o estacionamento é permitido.
- **Sempre:** Sete dias por semana.
- **Semanalmente:** Segunda-feira a sexta-feira.
- **Fim de semana:** Sábado e domingo.
- **Personalizar:** Selecione os dias que se aplicam.

7 Na opção **Horas aplicáveis**, selecione as horas durante o dia da semana em que o estacionamento é permitido.

8 Na opção **Validade**, selecione as datas durante o ano em que o estacionamento é permitido.

Selecione **O ano inteiro** ou selecione um intervalo de tempo específico usando o seletor de datas.

NOTA: O intervalo de data deve ser maior do que um dia.

9 Clique em **Adicionar** e, em seguida, clique em **Aplicar**.

A entidade de restrição de autorização é configurada e ativada no Security Center.

Após terminar

Configure um estacionamento no Security Center para a restrição de autorização.

Configurar estacionamentos no Security Center

Você deve configurar uma área de fiscalização (ou estacionamento) para cada restrição de autorização e regra de tempo extra que você criar.

O que você deve saber

- Uma vez que você tenha uma regra de fiscalização e um estacionamento definidos, isso perfaz o *estacionamento* que é exibido no Genetec Patroller™. Você cria estacionamentos no Security Center do Config Tool desenhando um polígono em torno da localização geográfica do estacionamento no mapa. Você pode adicionar múltiplos estacionamentos a um mapa.
- Você também pode importar para o seu mapa *arquivos KML* que foram criados em outro aplicativo de mapas, como o Google Earth.

Para configurar um estacionamento no Security Center:

1 Na página inicial do Config Tool, clique em **LPR** > **Autorizações**, **Restrições de autorização** ou **Regras de tempo extra**.

2 Selecione a autorização, restrição de autorização ou regra de tempo extra que deseja configurar e, em seguida, clique em **Zonas**.

O mapa aparecerá.

3 Amplie a área do mapa onde o seu estacionamento está localizado.

4 Clique no botão de **Vetor** e coloque o cursor no mapa.

O cursor muda para uma cruz.

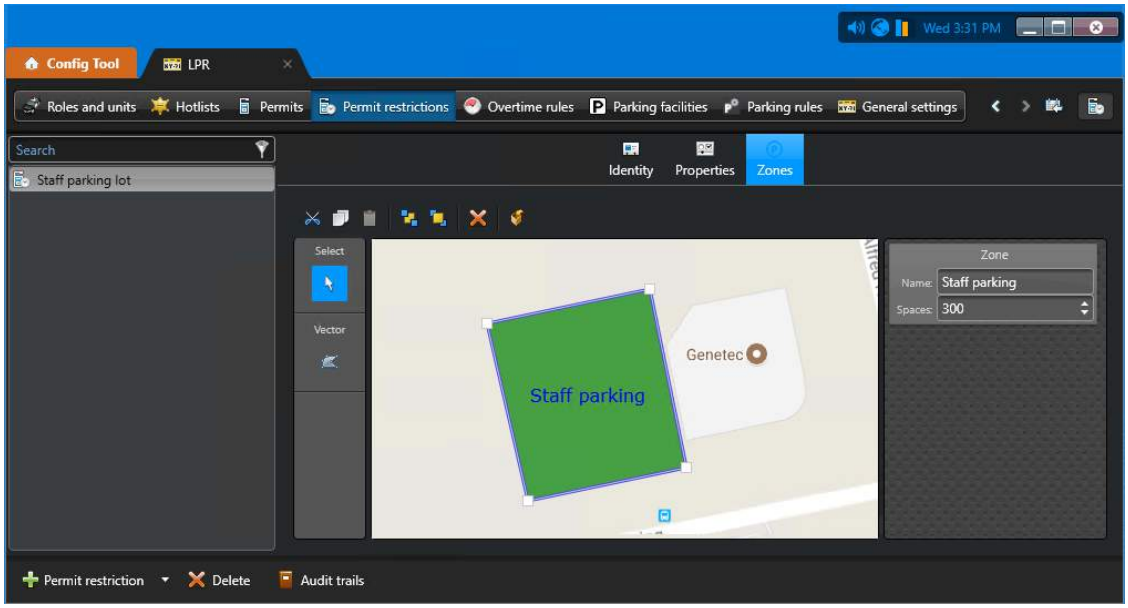
5 No mapa, clique em cada canto do estacionamento para criar o polígono (clique no ponto inicial para concluir o desenho).

Um estacionamento aparecerá com o nome **Nova zona 1**.

6 Clique no estacionamento **Nova zona 1** e, na caixa de diálogo que aparecerá, digite um novo **Nome** e o número de **Espaços** no estacionamento.

Este nome aparecerá em Genetec Patroller™ juntamente com o nome da *Autorização*, *Regra de tempo extra* ou *Restrição de estacionamento* para exibir uma zona de fiscalização.

DICA: Escolha um nome que descreva onde o estacionamento está. Isso torna mais fácil selecionar a zona de fiscalização em Genetec Patroller™ quando várias zonas estão disponíveis.



7 Clique em **Aplicar**.

O estacionamento aparece como um polígono preenchido com uma grossa borda azul no mapa. O nome do estacionamento é exibido no centro.

8 (Opcional) Para redimensionar um estacionamento, selecione-o no mapa e use as alças para arrastá-lo para o tamanho desejado.

DICA: Para selecionar um estacionamento, você pode clicar diretamente no estacionamento, ou clicar no botão Selecionar e selecionar o lote.

9 (Opcional) Para editar um estacionamento, selecione o lote e use os botões localizados na parte superior esquerda do mapa:

- **Recortar** : Corte o estacionamento selecionado da entidade atual e cole-o em outro. Por exemplo, você pode querer cortar o estacionamento de uma entidade de autorização e colá-lo no mapa ao criar um estacionamento para uma regra de horas extras.
- **Copiar** : Copie o estacionamento selecionado da entidade atual e cole-o em outro. Por exemplo, você pode querer usar as mesmas dimensões do estacionamento que foram criadas para um estacionamento de autorização em uma regra de hora extra em um estacionamento.
- **Colar** : Cole o estacionamento selecionado em outra entidade.
- **Enviar para trás** : Envie o estacionamento selecionado para o segundo plano.
- **Trazer para a frente** : Envie o estacionamento selecionado para o segundo plano.
- **Remover** : Exclua o estacionamento.

Tópicos relacionados

Adicionar e configurar zonas de estacionamento na página 842

Importar arquivos KML no Security Center

A aba **Zonas** no Config Tool permite que você importe arquivos KML (Keyhole Markup Language) para que você possa facilmente criar estacionamentos no Security Center.

Antes de iniciar

Crie um arquivo KML para o seu mapa. Isso pode ser feito usando o Google Earth.

O que você deve saber

- Se o arquivo KML que deseja importar não for suportado ou não for válido, você receberá uma mensagem de erro.
- Se você quiser atualizar um estacionamento KML no Security Center reimportando um arquivo KML atualizado, exclua o estacionamento KML original primeiro para não obter uma duplicata.

Para importar um arquivo KML:

1 Na página inicial do Config Tool, clique em **LPR** > **Autorizações**, **Restrições de autorização** ou **Regras de tempo extra**.

2 Selecione a autorização, restrição de autorização ou regra de tempo extra que deseja configurar e, em seguida, clique em **Zonas**.

O mapa aparecerá.

3 Clique em **Importar KML** ( ) e navegue até a pasta que contém o seu arquivo KML.

4 Selecione o arquivo KML e clique em **Abrir**.

O estacionamento aparece em seu mapa como um polígono preenchido com uma grossa borda azul no mapa. O nome do estacionamento está escrito no centro.

5 Selecione o ícone do estacionamento no mapa. Na caixa de diálogo que aparecer, digite o número de **Espaços** existentes no estacionamento.
6 Clique em **Aplicar**.

Definir configurações avançadas de autorização

A aba **Avançado** é onde você configura as propriedades avançadas de autorização, como a cor e a frequência de download. Essas propriedades não são exigidas para todas as autorizações, mas permitem que você personalize determinadas autorizações para cenários específicos.

Antes de iniciar

Crie a autorização.

Para definir configurações avançadas de autorização:

1. Na página inicial do Config Tool, clique em **LPR** > **Autorizações** e selecione a autorização que deseja configurar.
2. Clique na aba **Avançado**.
3. Ao lado de **Cor**, clique no bloco colorido e use a caixa de diálogo **Selecionar cor** para atribuir uma nova cor à autorização.

   O símbolo de mapa que marca a localização da ocorrência de autorização no Security Desk e no Genetec Patroller™ aparecerá nessa cor, bem como as telas Ocorrência de autorização e *Revisar ocorrências* no Genetec Patroller™.
4. Ative a opção **Desativar transferência periódica** se você somente quiser permitir que sejam baixadas alterações para o Genetec Patroller™ quando o usuário iniciar sessão no aplicativo. Esta opção exige uma conexão sem fio entre o Genetec Patroller™ e o Security Center.
5. Ative a opção **Ativar modificação da transferência** se você deseja transferir modificações de autorizações para o Genetec Patroller™ assim que ocorrerem. Por exemplo, você pode usar essa opção em uma autorização para forçar o Genetec Patroller™ a solicitar mudanças com mais frequência do que o período de transferência periódica (que se aplica a todas as autorizações). Esta opção exige uma conexão sem fio contínua entre o Genetec Patroller™ e o Security Center.
6. Clique em **Aplicar**.

46

Sistemas de inventário de placas de veículos móvel AutoVu™

Esta seção inclui os seguintes tópicos:

- "Inventário Móvel de Placas de Licença" na página 906
- "Sobre estacionamentos" na página 907
- "Criando instalações de estacionamento" na página 908
- "Configurar instalações de estacionamento" na página 909

Inventário Móvel de Placas de Licença

O Inventário de placas de veículos móvel (MLPI) é a instalação do software Genetec Patroller™ que está configurado para coletar placas de veículo e outras informações do veículo para criar e manter um inventário de placas de veículo para uma área de estacionamento ou garagem grande.

O inventário pode ser usado para relatar o seguinte:

- O número de dias em que um veículo foi estacionado na instalação.
- A localização (setor e linha) do veículo na instalação.
- Todos os veículos estacionados na instalação.
- Todos os veículos que deixaram a instalação ou entraram nela.

As leituras de placa de licença podem ser coletadas de três maneiras:

- Leitura automática usando o aplicativo Genetec Patroller™ e uma câmera (ou câmeras) Sharp.
- Entrada manual usando o recurso de *Captura manual* do aplicativo Genetec Patroller™.
- (Opcional) Captura manual usando o computador portátil aprovado pela Genetec Inc. que está executando o aplicativo Genetec Patroller™ MLPI.

Inventário de placas de licença

O inventário da placa de licença inclui leituras de placas de todos os veículos estacionados no estacionamento. É criado a partir dos dados de descarga da coleção de placas do Genetec Patroller™ e do computador portátil aprovado pela Genetec Inc. (se aplicável). O inventário pode ser usado para monitorar a atividade da instalação de estacionamento durante um período de tempo específico. Por exemplo, um veículo de patrulha pode coletar as leituras de placa de licença no início da manhã e depois fazer outra coleta à noite para ver quantos veículos deixaram a instalação. A tarefa *Gerenciamento de inventário* do Security Desk é usada para criar o inventário a partir dos dados de descarregamento, e a tarefa *Relatório de inventário* do Security Desk é usada para consultar quaisquer alterações a um inventário.

Para obter mais informações, consulte os tópicos *Gerenciamento de inventário* e *Relatório de inventário* no *Guia de Usuário do Security Desk*.

Como as leituras são reconciliadas

A maioria das leituras dos dados de descarregamento de uma coleta de placas de licença são automaticamente reconciliadas (validadas e adicionadas) ao inventário de placas de licença pelo Security Center. No entanto, algumas delas podem exigir reconciliação manual se um conflito for detectado. Por exemplo, um veículo pode ter os mesmos números da placa de licença que outro veículo, mas ser de um estado diferente. Neste caso, a tarefa *Gerenciamento de inventário* do Security Desk exibirá uma caixa de diálogo pedindo que você reconcilie a leitura (confirme o número da placa e o estado do veículo).

Para mais informações sobre a tarefa *Gerenciamento de inventário*, consulte o *Guia de Usuário do Security Desk*.

Sobre estacionamentos

É um tipo de entidade que define uma grande área de estacionamento como um número de setores e filas para fins de rastreamento de inventário. É usado no aplicativo *Inventário de placas de veículos móvel* (MLPI) do AutoVu™.

O inventário de placas de veículos é a lista de veículos presentes em um estacionamento dentro de um determinado período de tempo.

Antes de as unidades MLPI do AutoVu™ (veículos de patrulha e dispositivos portáteis) poderem coletar placas de veículos para o inventário, você deve definir sua rota de coleta como uma sequência de setores e linhas configurada no estacionamento. O setor e a linha onde uma placa de veículo é reconhecida representam a localização do veículo dentro do estacionamento.

O Security Center coleta *reconhecimentos de placas de veículos* das unidades MLPI e cria um inventário para a data atual. Usando o Security Desk, você pode saber onde um veículo está estacionado (setor e linha) e há quanto tempo ele está estacionado ali no inventário atual. Você também pode comparar dois inventários de datas diferentes para ver os movimentos do veículo (veículos que chegaram, foram movidos ou saíram).

Criando instalações de estacionamento

Para rastrear a localização dos veículos em um sistema de inventário de placas de veículos móvel AutoVu™, você deve criar um estacionamento.

Para criar uma instalação de estacionamento:

1 Na página inicial do Config Tool, clique em **LPR** > **Instalações de estacionamento** e, em seguida, clique em **Instalação de estacionamento** ( ).

2 Na aba **Identidade**, digite as informações exigidas:

- **Nome:** No Inventário de Placas de Veículos Móvel, este nome aparecerá no Genetec Patroller™ na página de seleção de zona de estacionamento.
- **(Opcional) Descrição:** Você pode adicionar uma descrição mais longa para a regra. Este campo não aparece no Genetec Patroller™.
- **(Opcional) ID Lógica:** Digite uma ID Lógica, se aplicável.

3 Clique em **Aplicar**.

A instalação de estacionamento aparece em uma visualização de lista simples que exibe todas as instalações em seu sistema.

Após terminar

Defina o estacionamento para o seu cenário de estacionamento criando setores e linhas.

Configurar instalações de estacionamento

Depois de ter criado uma instalação de estacionamento no Security Center, você deve definir a instalação para o seu cenário de estacionamento criando setores e linhas para a rota de coleta de placas de veículo.

Antes de iniciar

Crie a instalação de estacionamento.

O que você deve saber

O espaço de estacionamento de um estacionamento é dividido em setores (ou níveis no caso de uma garagem) para facilidade de referência. Cada setor contém x número de linhas, e cada linha contém x número de espaços. Você pode configurar o Genetec Patroller™ para acionar um alarme (som ou mensagem de advertência) se as leituras coletadas durante a varredura de uma linha excederem a contagem de espaços para essa linha.

A *rota* é a rota de coleta de placas de veículo seguida pelas unidades MLPI responsáveis pela coleta de placas para o inventário. A rota é baixada pelos veículos de patrulha e dispositivos portáteis atribuídos a esta instalação de estacionamento.

NOTA: Apenas uma rota pode ser definida por estacionamento, mas cada dispositivo MLPI pode começar a rodar em um ponto diferente da rota. A rota forma um circuito fechado.

Para configurar uma instalação de estacionamento:

1 Na página inicial do Config Tool, clique em **LPR** > **Instalações de estacionamento** e selecione a instalação que deseja configurar.

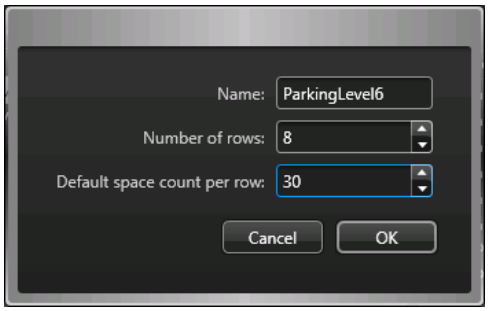
2 Clique na guia **Propriedades.**

3 Na lista suspensa **LPR Manager**, selecione o LPR Manager que criará e gerenciará o inventário de placas de veículo para a instalação de estacionamento selecionada.

Somente descarregamentos de veículos de patrulha MLPI gerenciados pelo mesmo LPR Manager são usados para construir o inventário para esta instalação de estacionamento. Um descarregamento de um Genetec Patroller™ MLPI pode incluir o inventário de veículos de várias instalações de estacionamento, mas somente as leituras marcadas para esta instalação de estacionamento são usadas para construir o inventário.

4 Em **Configuração**, clique em **Criar** () para adicionar um novo setor.

O espaço de estacionamento de um estacionamento é dividido em setores (ou níveis no caso de uma garagem) para facilidade de referência. Cada setor contém x número de linhas.

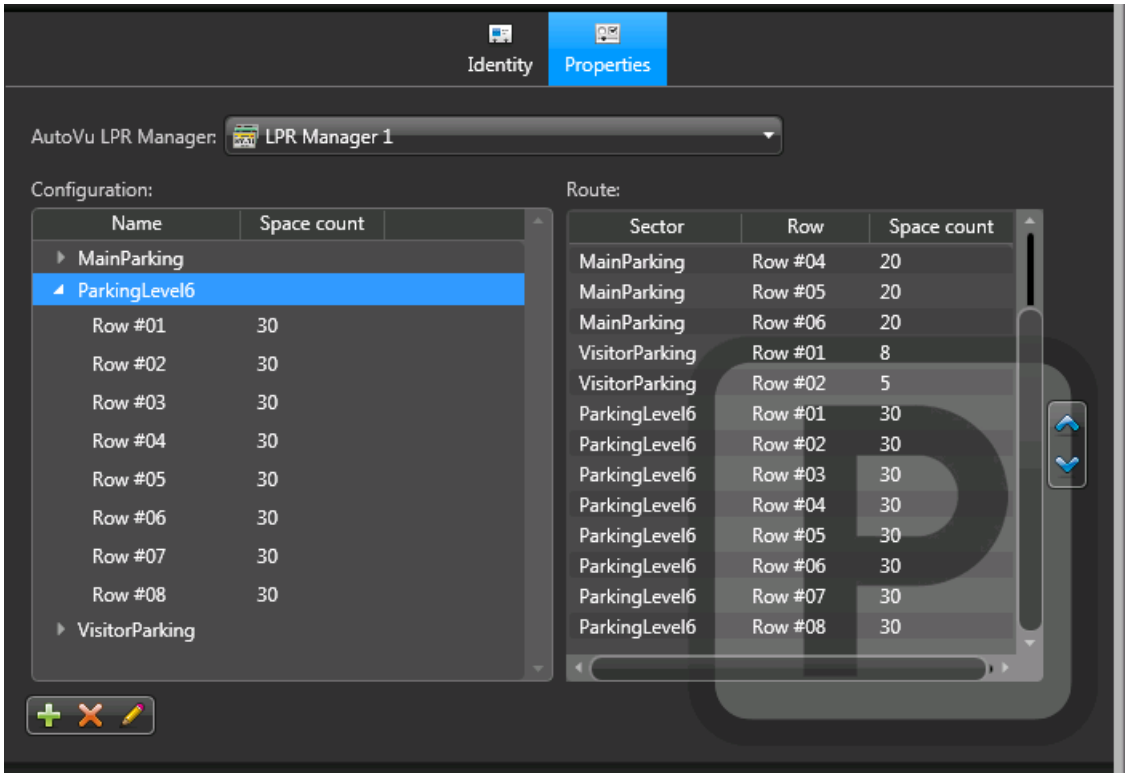


5 Digite o **Nome** do setor (ou nível, se for uma garagem de estacionamento).

6 Digite o **Número de linhas** no setor.

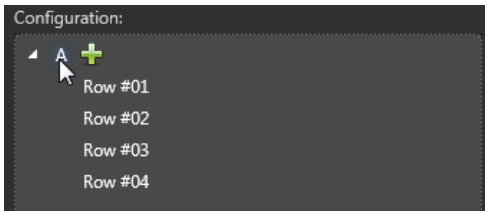
7 Clique em **OK**.

O setor que você criou aparece nas seções **Configuração** e **Rota**.



8 Para adicionar linhas a um setor, faça o seguinte:

a) Em **Configuração**, passe o mouse sobre o nome do setor e clique em **Criar** ( ).



b) Insira o **Número de linhas** a adicionar e clique em **OK** > **Aplicar**.

9 (Opcional) Para renomear um setor, faça o seguinte:

a) Em **Configuração**, clique no nome do setor que deseja renomear e, em seguida, clique em **Editar** ( ).

b) Digite o novo nome e clique em **OK** > **Aplicar**.

10 (Opcional) Para excluir um setor, clique no nome do setor que deseja excluir em **Configuração** e, em seguida, clique em **Excluir** ( ) > **Aplicar**.

11 Para alterar a ordem dos setores e das linhas na rota, clique nas setas para cima ( ) e para baixo ( ) em **Rota**.

Após terminar

Você deve configurar o *Período de retenção de leituras* do LPR Manager de acordo com o período de tempo durante o qual você deseja manter os inventários de placas de veículo no banco de dados. O período de retenção padrão é de 90 dias.

47

Solução de problemas de LPR

Esta seção inclui os seguintes tópicos:

- "Mover unidades Genetec Patroller ou LPR para um LPR Manager diferente" na página 912

Mover unidades Genetec Patroller™ ou LPR para um LPR Manager diferente

Se você quiser que uma função LPR Manager diferente gerencie e controle uma unidade LPR ou Genetec Patroller™ para balanceamento de carga ou outra finalidade, você pode mover a unidade para outro LPR Manager usando a ferramenta *Mover unidade*. Depois que a unidade é movida, o LPR Manager antigo continua a gerenciar os dados da unidade coletados antes da mudança.

O que você deve saber

Depois de mover uma unidade no Config Tool, você precisa atualizar as configurações de rede da unidade no Genetec Patroller™ Config Tool e no Sharp Portal para que a unidade possa se comunicar com o seu novo LPR Manager. As configurações específicas da unidade (por exemplo, nome da unidade, ID lógica, etc.) são transferidas automaticamente para o novo LPR Manager.

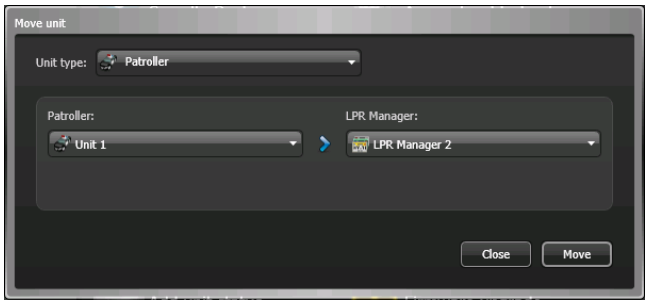
Por exemplo, se você mover uma unidade Genetec Patroller™ do *LPR Manager* para o *LPR Manager 2*, você deve configurar a unidade Genetec Patroller™ para se comunicar com o *LPR Manager 2* da mesma forma que fez quando originalmente adicionou a unidade no *LPR Manager*. Isso requer a alteração das configurações de rede no Genetec Patroller™ Config Tool para que elas correspondam às configurações de rede do *LPR Manager 2* no Security Center do Config Tool.

Para mover uma unidade LPR ou Genetec Patroller™ para um LPR Manager diferente:

1 Na página inicial do Config Tool, clique em **Ferramentas** > **Mover unidade**.

2 Na lista suspensa **Tipo de unidade**, na caixa de diálogo **Mover unidade**, selecione a unidade Genetec Patroller™ ou LPR que deseja mover.

Uma unidade Genetec Patroller™ é mostrada como exemplo.



3 Selecione os dados que deseja mover.

4 Na lista suspensa **LPR Manager**, selecione o novo LPR Manager para controlar a unidade.

5 Clique em **Mover** > **Fechar**.

A unidade agora está adicionada no novo LPR Manager

Após terminar

Verifique se a unidade pode se comunicar com o novo LPR Manager, da seguinte forma:

- Para listas de procurados, listas de autorização e grupos de usuários do Genetec Patroller™, faça o seguinte:

  1 Na página inicial, clique em **Sistema** > **Funções** e selecione o LPR Manager que agora controla a unidade que você moveu.

  2 Clique em **Propriedades** > **Associação de arquivos**.

  3 Ative as listas de procurados e listas de autorização e atribua um grupo de usuários do Genetec Patroller™ para este LPR Manager.

- Atualize as configurações de rede das unidades Genetec Patroller™ para se comunicarem com o novo LPR Manager (consulte o *Guia do Administrador do Genetec Patroller™*).
- Atualize as configurações de rede das unidades LPR para se comunicar com o novo LPR Manager. Para obter mais informações, consulte *Guia do Administrador Sharp*.

Alarmes e eventos críticos

Esta parte inclui as seguintes chapters:

- "Alarmes" na página 915
- "Níveis de ameaça" na página 928
- "Zonas e detecção de intrusão" na página 938

48

Alarmes

Esta seção inclui os seguintes tópicos:

- "Sobre alarmes" na página 916
- "Criando alarmes" na página 918
- "Testar alarmes" na página 922
- "Solução de problemas: Alarmes não recebidos" na página 923
- "Configurar alarmes usando eventos de causa-efeito" na página 924
- "Acionar alarmes manualmente" na página 927

Sobre alarmes

Um alarme é um tipo de entidade que descreve uma situação de problema particular que requer atenção imediata e como pode ser tratada no Security Center. Por exemplo, um alarme pode indicar quais entidades (geralmente câmeras e portas) melhor descrevem, quem deve ser notificado, como deve ser exibido para o usuário, etc.

As propriedades básicas de um alarme são:

- **Nome:** Nome do alarme.
- **Prioridade:** Prioridade do alarme (1-255), baseado na urgência da situação. Os alarmes com prioridade mais altas são exibidos primeiro no Security Desk.
- **Destinatários:** Usuários, grupos de usuários e grupos de monitor analógico que são notificados quando ocorre o alarme e são responsáveis por responder à situação do alarme.
- **Modo de difusão:** Como os destinatários do alarme são notificados sobre o alarme.
  - **Todos ao mesmo tempo:** (Padrão) Todos os destinatários são notificados ao mesmo tempo, imediatamente após o alarme ser disparado.
  - **Sequencial:** Os destinatários são notificados individualmente, cada um após um atraso específico (em segundos) calculado a partir do momento que o alarme é disparado. Se o destinatário é um grupo de usuários, todos os membros do grupo serão notificados ao mesmo tempo.
- **Entidades anexas:** Entidades que ajudam a descrever a situação de alarme (por exemplo, câmeras, área, portas, procedimento de alarme, etc.). Quando o alarme é recebido em Security Desk, as entidades relacionadas podem ser exibidas uma depois da outra, em uma sequência, ou de uma vez, na *tela*, para ajudar a revisar a situação. Se uma entidade composta estiver anexada ao alarme, as entidades que a compõem também estão vinculadas ao alarme. Por exemplo, se uma entidade de porta estiver anexada ao alarme, as câmeras associadas à porta também estão.

Para informações sobre monitoramento, confirmação e investigação de alarmes no Security Desk, consulte o *Guia do Usuário Security Desk*.

Prioridade do alarme

No Security Desk, os alarmes são exibidos na tarefa *Monitoramento de alarme* e *Monitoramento* por ordem de prioridade (isso é avaliado sempre que um novo alarme é recebido). O alarme de maior prioridade é mostrado no ladrilho nº 1, seguido pelo segundo maior no ladrilho nº 2 e assim por diante. Quando dois alarmes têm o mesmo valor de prioridade, a prioridade é dada ao mais novo.

Quando um novo alarme é recebido no Security Desk com um nível de prioridade idêntico ou maior que os alarmes atuais exibidos, ele empurra os outros alarmes para baixo na lista de ladrilhos.

Quando um alarme é *confirmado* no Security Desk, ele libera um ladrilho para os alarmes de prioridade mais baixa subirem.

Gravação de vídeo em alarmes

Quando um alarme com câmeras é disparado, é possível se certificar que o vídeo relacionado ao alarme seja gravado e esteja disponível para investigações futuras de alarme.

O tempo em que o vídeo é gravado (chamado *intervalo de gravação garantida*) é definido por duas configurações:

- **Duração de gravação do alarme:** Número de segundos que o Archiver grava o vídeo após o alarme ser disparado. Essa opção (*Gravação automática de vídeo*) é configurada na aba *Avançado* do alarme.
- **Buffer de gravação:** Número de segundos que o Archiver grava o vídeo antes do alarme ser disparado, para se certificar que o que disparou o alarme também seja gravado. Essa opção (*Tempo para gravar*

antes de um evento) é definida na aba *Configurações padrão da câmera* do Archiver ou para cada câmera individualmente.

Se um alarme for disparado de um evento de câmera (por exemplo, *Objeto removido*), depois, a câmera que causou o evento também é vinculada ao alarme e começa a gravação.

IMPORTANTE: As gravações dependem dos agendamentos de arquivamento. Se a gravação estiver desabilitada quando o alarme for disparado, nenhum vídeo é gravado.

Tópicos relacionados

Archiver - Aba Configurações padrão de câmera na página 1048
Diferenças entre níveis de ameaça e alarmes na página 930

Criando alarmes

Para que os alarmes sejam acionados no seu sistema, você deve criar uma entidade de alarme e configurar suas propriedades.

O que você deve saber

Como prática recomendada, dê nomes aos alarmes que melhor descrevem a situação, para que seja fácil determinar o que aconteceu quando o alarme foi disparado.

Para criar um alarme:

1 Na página inicial do Config Tool, abra a tarefa *Alarmes* e clique na visualização **Alarmes**.

2 Clique em **Alarme** ( ).

Uma nova entidade de alarme ( ) aparecerá na visualização **Alarmes**.

3 Digite um nome para o alarme e pressione **ENTER**.

4 Clique na guia **Propriedades.**

5 Na opção **Prioridade**, defina a prioridade do alarme, com base na urgência da situação.

Os alarmes com prioridade mais altas são exibidos primeiro no Security Desk.

6 Para adicionar destinatários para o alarme, clique em **Adicionar um item** ( ) na seção **Destinatários**, selecione os usuários, grupos de usuários ou grupos de monitores analógicos e clique em **Adicionar**.

Os destinatários são notificados quando ocorre o alarme e são responsáveis por responder à situação.

7 Se você escolher mais de um destinatário, selecione como eles são notificados sobre o alarme na opção **Modo de transmissão**:

- **Todos ao mesmo tempo:** Todos os destinatários são notificados ao mesmo tempo, imediatamente depois que o alarme é disparado.
- **Sequencial:** Os destinatários são notificados individualmente, cada um após um atraso específico (em segundos) calculado a partir do momento que o alarme é disparado. Se o destinatário é um grupo de usuários, todos os membros do grupo serão notificados ao mesmo tempo.

8 Para adicionar entidades para ajudar a descrever o alarme, clique em **Adicionar um item** ( ) na seção **Entidades anexas**, selecione as entidades e clique em **Selecionar**.

As entidades anexas ajudam os usuários a reagir à situação de alarme. Quando o alarme é recebido no Security Desk, as entidades anexas (câmeras, portas, áreas, procedimento de alarme e assim por diante) são exibidas na tela na tarefa Monitoramento de alarme.

9 Na lista suspensa **Opções de vídeo**, selecione as opções de vídeo quando o alarme é disparado.

10 Para girar automaticamente as entidades anexadas dentro de um ladrilho na tarefa *Monitoramento de alarme* quando o alarme é disparado, mude a opção **Ciclo de conteúdo** para **Ligado** e defina o número de segundos durante os quais cada entidade é exibida.

NOTA: A ordem das entidades na lista é a ordem em que elas são exibidas no Security Desk. Quando o alarme é acionado por um evento, a entidade que causou o evento também é conectada ao alarme e é exibida primeiro.

11 Clique em **Aplicar**.

12 Clique na aba **Avançado** e defina as configurações opcionais do alarme.

Após terminar

Faça o seguinte:

- Certifique-se de que os destinatários de alarme tenham os privilégios de usuário *Confirmar alarmes* e *Monitoramento de alarme*.

- Teste o alarme que você criou.

Selecionar opções de exibição de vídeo para alarmes

Se uma câmera estiver conectada a um alarme, você deve configurar como o vídeo é exibido quando o alarme é acionado e exibido na tela da tarefa Monitoramento de alarme.

O que você deve saber

A opção de exibição de vídeo padrão é o vídeo ao vivo. Você pode selecionar vídeo ao vivo, reprodução de vídeo, uma série de quadros fixos antes, durante ou após o alarme ser disparado ou uma combinação dos três. O vídeo ou os quadros fixos são exibidos pelo número de segundos configurado na opção **Ciclo de conteúdo** na aba **Propriedades** do alarme.

As opções que você configura são aplicadas a todas as câmeras conectadas ao alarme.

Para selecionar as opções de exibição de vídeo para um alarme:

1 Abra a tarefa **Alarmes** e clique na visualização **Alarmes**.
2 Selecione o alarme a configurar e clique na aba **Propriedades**.
3 Na lista suspensa **Opção de exibição de vídeo**, selecione um dos seguintes itens:
   - **Ao vivo:** Exibir vídeo ao vivo.
   - **Reprodução:** Exibir reprodução de vídeo.
   - **Ao vivo e reprodução:** Circule entre a exibição de vídeo ao vivo e reprodução. Quando você descompacta o ladrilho, um ladrilho exibe vídeo ao vivo e outro exibe a reprodução. Você também pode clicar no ícone **Propriedades** (⚙) e configurar **Picture-in-picture** para que você possa visualizar vídeo ao vivo e de reprodução no mesmo ladrilho.
   - **Ao vivo e quadros estáticos:** Circule entre a exibição de vídeo ao vivo e uma série de quadros fixos. Quando você descompacta o ladrilho, um ladrilho exibe vídeo ao vivo e outro exibe quadros estáticos. Você também pode clicar no ícone **Propriedades** (⚙) e configurar **Picture-in-picture** para que você possa visualizar vídeo ao vivo e quadros estáticos no mesmo ladrilho.

     NOTA: Os quadros estáticas não são suportados quando a câmera é criptografada.
   - **Quadros estáticos:** Exibe uma série de quadros estáticos. Ver nota anterior.
4 Se você selecionar uma opção de exibição que inclua reprodução de vídeo, selecione quantos segundos antes do alarme ser ativado para iniciar a reprodução.

   NOTA: Para garantir que o vídeo de reprodução esteja disponível durante o período de tempo que você configurou, o buffer de gravação de eventos deve ter um valor igual ou superior.
5 Se você selecionar uma opção de exibição que inclua quadros estáticos, clique no ícone **Propriedades** (⚙).
6 Na caixa de diálogo **Quadros estáticos**, selecione se deseja que cada quadro estático seja exibido pela mesma duração ou por uma duração independente (**Mesmas durações** ou **Durações independentes**).
7 Se você selecionar **Mesmas durações**, defina as seguintes opções:
   - **Número de quadros:** Selecione o número de quadros estáticos para exibir dentro de uma duração total do ciclo do conteúdo.
   - **Reproduzir:** Selecione quantos segundos antes de o alarme ter sido disparado para começar o primeiro quadro estático.
8 Se você selecionar **Durações independentes**, faça o seguinte:
   a) Clique em **Adicionar um item** (➕).
   b) Na opção **Tempo relativo**, selecione quantos segundos antes ou depois de alarme ser acionado o quadro é exibido.
   c) Na opção **Duração**, selecione por quanto tempo a imagem estática será exibida.
   d) Clique em **Adicionar**

e) Adicione quadros estáticos adicionais.

A duração de todos os quadros fixos não pode exceder o valor da **Duração total**.

9 Se você selecionar a opção **Ao vivo e de reprodução** ou **Ao vivo e quadros estáticos**, você pode configurar picture-in-picture para exibir vídeo ao vivo e de reprodução ou vídeo ao vivo e em quadros estáticos no mesmo ladrilho.

a) Clique no ícone **Propriedades** ( ).

b) Na caixa de diálogo **Configuração de exibição de vídeo**, na lista **Picture-in-picture**, escolha o tipo de vídeo que gostaria que fosse exibido na janela menor.

c) Na lista **Exibido em**, selecione onde você gostaria que a janela menor fosse exibida.

10 Clique em **OK** > **Aplicar**.

Configurar propriedades opcionais de alarmes

Depois de criar um alarme e configurar suas propriedades básicas, existem outras propriedades que você pode definir.

Para definir propriedades opcionais para um alarme:

1 Abra a tarefa **Alarmes** e clique na visualização **Alarmes**.

2 Selecione o alarme a configurar e clique na aba **Avançado**.

3 Definir as seguintes opções:

- **Limiar de reativação:** O tempo mínimo que o Security Center precisa esperar depois de disparar o alarme antes de ser disparado novamente. Essa opção evita que o sistema fique disparando repetidamente o mesmo alarme antes que seja resolvido.
- **Procedimento de alarme (URL):** Entre a URL ou o endereço de página da Web correspondente ao *procedimento de alarme*, que oferece instruções de funcionamento do alarme aos operadores. A página da web é exibida quando o usuário clica em *Exibir procedimento de alarme* ( ) no widget de alarme no Security Desk.
- **Agendamento:** Defina quando esse alarme estará operando. Fora dos períodos definidos por esse agendamento, disparar esse alarme não tem nenhum efeito.

  NOTA: É possível adicionar múltiplos agendamentos ao alarme. Conflitos de agendamento que não possam ser resolvidos serão notificados.
- **Confirmação automática:** Ative essa opção para permitir que o sistema confirme automaticamente esse alarme se não for confirmado antes do tempo especificado (em segundos). Essa opção é recomendada para alarmes de baixa prioridade que servem para alertar o operador de segurança, mas não exige nenhuma ação. Quando esta opção está desativada, o sistema segue a opção **Confirmar alarmes automaticamente após** configurada no nível do sistema no Server Admin.

  NOTA: A confirmação automática não se aplica a alarmes que têm uma condição ativa anexa. Para confirmar esses alarmes, é necessário confirmá-los à força (o que exige o privilégio de *Confirmar alarmes à força*). Para obter mais informações sobre confirmação de alarmes, consulte o *Guia do Usuário do Security Desk*.
- **Criar um incidente da confirmação:** Ative essa opção para estimular o usuário Security Desk a relatar um *incidente* sempre que confirmar um alarme.

  NOTA: Ativar essa opção desliga a opção *confirmação automática*.
- **Gravação automática de vídeo:** Desative essa opção (padrão=ligado) se não desejar começar a gravar o vídeo quando o alarme é disparado.
- **Proteger vídeo gravado:** Ative essa opção (padrão=desligado) para proteger as gravações de vídeo associadas a esse alarme por um número específico de dias.
- **Som do alarme:** Selecione o trecho de som para reproduzir quando ocorre um novo alarme, se os alarmes estiverem configurados para tocar um som no Security Desk. Por padrão, o trecho de som configurado na caixa de diálogo do Security Desk *Opções* é usado.

- **Cor:** Selecione uma cor para o alarme. A cor é usada para a sobreposição do vídeo de alarme quando ele é exibido em um ladrilho na tarefa *Monitoramento de alarme* ou *Monitoramento*, bem como quando o alarme é acionado em um mapa.

4 Clique em **Aplicar**.

Tópicos relacionados

Archiver - Aba Configurações padrão de câmera na página 1048
Proteger arquivos de vídeo contra exclusão na página 537
Server Admin - Página do servidor principal na página 104

Testar alarmes

Para testar se um alarme que você acabou de criar funciona, você pode ativá-lo manualmente a partir do Config Tool e certificar-se de recebê-lo no Security Desk.

Antes de iniciar

Faça logon no Security Desk como um dos destinatários dos alarmes.

O que você deve saber

Você pode configurar a tarefa *Monitoramento de alarmes* no Security Desk para abrir automaticamente quando um alarme é acionado. Para obter mais informações sobre como personalizar o comportamento de alarmes, consulte o *Guia do Usuário do Security Desk*.

Para testar um alarme:

1. No Config Tool, abra a tarefa **Alarmes**.
2. Clique na visualização **Alarmes** e selecione o alarme a ser testado.
3. Na barra de ferramentas na parte inferior da área de trabalho, clique em **Acionar alarme** ( ).

   O alarme deve aparecer na bandeja de notificação do Security Desk e na lista de alarmes na tarefa Monitoramento de alarmes.
4. Se a tarefa de monitoramento de alarmes não abrir automaticamente, clique duas vezes no ícone de alarme ( ) na bandeja de notificação do Security Desk.
5. Na tarefa Monitoramento de alarme, verifique se o alarme aparece na lista de alarmes.

Após terminar

Se você não receber o alarme, você pode solucionar problemas de alarmes.

Solução de problemas: Alarmes não recebidos

Se você não receber um alarme no Security Desk, você pode solucionar a causa do problema.

Para solucionar o problema de um alarme que não é recebido:

1. Verifique se o usuário que está tentando receber o alarme é um destinatário do alarme, da seguinte forma:
   a) Abra a tarefa **Alarmes** e clique na visualização **Alarmes**.
   b) Selecione o alarme e clique na aba **Propriedades**.
   c) Certifique-se de que o usuário, ou o grupo de usuários de que ele é membro, está na lista de **Destinatários**.
2. Certifique-se de que a agenda de alarmes não o impede de acionar o alarme neste momento, da seguinte forma:
   a) Clique na aba **Avançado** do alarme.
   b) Certifique-se de que a agenda listada na lista suspensa **Agenda** se aplica neste momento.
3. Certifique-se de que o destinatário do alarme tenha os privilégios de usuário corretos para receber alarmes, da seguinte maneira:
   a) Na página inicial Config Tool, abra a tarefa *Gerenciamento de usuários*.
   b) Selecione o usuário a configurar e clique na aba **Privilégios**.
   c) Certifique-se de que os privilégios de usuário *Monitoramento de alarmes* e *Confirmar alarmes* estejam definidos como **Permitir**.
   d) Clique em **Aplicar**.

Configurar alarmes usando eventos de causa-efeito

Você pode configurar alarmes para que eles sejam acionados quando ocorre um evento, usando eventos de causa-efeito.

Para configurar um alarme usando um evento de causa-efeito:

1 Abra a tarefa **Sistema** e clique na visualização **Configurações gerais**.
2 Clique na aba **Ações** e, em seguida, clique em .
3 Na página **Tipo de entidade**, selecione um tipo de entidade e clique em **Próximo**.
A *entidade de origem* é aquela à qual o evento está anexado.
4 Na página **Origem**, selecione a entidade de origem e clique em **Próximo**.
5 Na página **Evento**, selecione um tipo de evento.
Somente eventos relacionados ao tipo de entidade selecionada são listados.
6 Selecione uma agenda e clique em **Próximo**.
A agenda determina quando o evento irá desencadear a ação. Por exemplo, você pode querer acionar um alarme apenas se uma janela for aberta durante o fim de semana. Por padrão, *Sempre* fica selecionado.
7 Na página **Ação**, selecione **Disparar alarme**.
8 Na lista suspensa **Alarme**, selecione um alarme a ser acionado.
9 (Opcional) Na lista suspensa **Condição de confirmação**, selecione um evento que deva ser acionado antes que o alarme possa ser confirmado.
Esta opção está disponível somente para alguns tipos de eventos.
10 Para exigir que um usuário confirme o alarme após a condição de confirmação ser atendida, selecione a opção **Necessária confirmação do usuário**.
Se você limpar esta opção, o alarme será automaticamente confirmado quando a condição de confirmação for apagada.
11 Clique em **Próximo** > **Criar** > **Fechar**.

Tópicos relacionados

Criar eventos causa-efeito na página 208
Tipos de evento na página 1101

Tipos de eventos que podem exigir condições de confirmação

Alguns eventos para ações podem ser configurados para que um segundo evento seja acionado antes que o alarme que foi disparado possa ser confirmado. O segundo evento é a *condição de confirmação*.

Por exemplo, você pode configurar um evento *Sinal perdido* para acionar um alarme e especificar que o alarme só pode ser confirmado após o evento *Sinal recuperado* ser gerado.

A tabela a seguir lista os tipos de eventos que dão a você a opção de configurar uma condição de confirmação que deve ser limpa antes que o alarme possa ser confirmado.

Tipo de evento de origem	Tipo da entidade	Condição de confirmação
Falha de CA	Unidade de controle de acesso, unidade de detecção de intrusão	Pronto para CC
Aplicativo perdido	Funções	Aplicativo online
O ativo está offline	Ativo	O ativo está online

Tipo de evento de origem	Tipo da entidade	Condição de confirmação
O ativo está online	Ativo	O ativo está offline
Falha de bateria	Unidade de controle de acesso, unidade de detecção de intrusão	Pronto para bateria
Porta fechada	Porta	Entrada (*Normal* ou *Ativo*)
A porta forçada para abrir	Porta	Porta fechada • Entrada *Normal* • Entrada *Ativo*
Porta aberta	Porta	Porta fechada • Entrada *Normal* • Entrada *Ativo*
Porta aberta por muito tempo	Porta	Porta fechada
Violação de hardware	Unidade de controle de acesso, unidade de detecção de intrusão, zona (hardware)	Adulteração normal
Alarme da área de detecção de intrusão ativado	Área de detecção de intrusão	• Não em atenção (não pronta) • Não em atenção (pronta para entrar em atenção) • Mestre armado • Perímetro armado
Desvio de entrada da área de detecção de intrusão ativado	Área de detecção de intrusão	Entrada normal
Violação de unidade de detecção de intrusão	Unidade de detecção de intrusão:	Adulteração normal
Estação manual ativada	Porta	Estação manual normal • Entrada *Normal* • Entrada *Ativo*
Problema de gravação	Câmera	Problema de gravação resolvido (corresponde a *Gravação ativa* ou *Gravação inativa*)
Perda de Sinal	Câmera	Sinal recuperado

Tipo de evento de origem	Tipo da entidade	Condição de confirmação
Perda de unidade	Unidade de controle de acesso, Unidade de detecção de intrusão, unidade LPR, Unidade de vídeo	Unidade online
Zona colocada em atenção / Zona colocada fora de atenção[1]	Zona	• Estado da zona normal • Estado da zona ativo

[1] Os eventos associados aos estados normal, ativo e problema de uma zona também podem ser configurados com uma condição de confirmação.

Acionar alarmes manualmente

Para testar um alarme recém-criado ou se algo crítico ocorrer e você desejar ativar um alarme, é possível acionar o alarme manualmente.

Antes de iniciar

- O alarme deve estar configurado no Config Tool.
- Se desejar acionar alarmes a partir da tarefa *Monitoramento*, é necessário habilitar o monitoramento de alarmes.

Para acionar um alarme manualmente:

- Tome uma das seguintes ações:
  - Na tarefa **Alarmes** de Config Tool, selecione um alarme e clique em **Acionar alarme** () na barra de ferramentas na parte inferior do espaço de trabalho.
  - Na bandeja de notificação de Security Desk, clique em **Ações instantâneas (**  **)** > **Ação manual** . Clique em **Acionar alarme** (), selecione um alarme e clique **OK**.
  - Na tarefa *Monitoramento de alarmes* de Security Desk ou *Monitoramento*, clique em **Disparar alarme** (), selecione um alarme e clique em **Disparar alarme**.

Todos os destinatários de alarme pré-configurados recebem o alarme, caso tenham sessão iniciada no Security Desk.

49

Níveis de ameaça

Esta seção inclui os seguintes tópicos:

- "Sobre níveis de ameaça" na página 929
- "Definir níveis de ameaça" na página 933
- "Cenário de nível de ameaça: Incêndio" na página 934
- "Cenário de nível de ameaça: pessoa armada" na página 936

Sobre níveis de ameaça

Uma *ameaça* é uma situação potencialmente perigosa, como incêndio ou tiroteio, que exige uma resposta imediata do sistema e do pessoal de segurança.

Cada nível de ameaça é caracterizado por um nome e uma cor e está associado a duas listas de ações que determinam o comportamento do sistema. Uma lista é executada quando o nível de ameaça é definido e a outra lista é executada quando a ameaça é desmarcada. Você pode escolher entre as ações do Security Center para definir o nível de ameaça, além de algumas ações adicionais que são exclusivas dos níveis de ameaça, como negar a certos titulares de cartão o acesso a áreas em seu sistema ou forçar certos usuários a se desconectar do sistema.

Os níveis de ameaça são definidos pelos usuários do Security Desk que possuem o privilégio *Definir nível de ameaça* quando uma situação perigosa ocorre. Os operadores podem definir um nível de ameaça em uma área ou em todo o sistema (inclui todas as áreas).

Agendamentos de desbloqueio durante um nível de ameaça ativo

As áreas são configuradas com uma autorização de segurança que varia de 0 a 7 (0 = maior segurança, 7 = menor). Uma autorização de segurança 7 é o valor padrão, geralmente significando que a área não requer uma autorização especial. Os horários de desbloqueio para áreas configuradas com um nível de segurança diferente de sete são ignorados pela duração da ameaça. Uma vez que o nível de ameaça seja liberado, os horários de desbloqueio para essas áreas retomam.

Definir um nível de ameaça não tem efeito sobre o seguinte:

- Comandos *Ignorar manualmente agenda de desbloqueio* no Security Desk
- Comandos *Desbloquear manualmente* para portas específicas no widget de porta do Security Desk.
- Evento causa-efeito *Ignorar temporariamente agenda de desbloqueio*
- Ativação do REX, o que significa que a ativação do REX ainda desbloqueará a porta
- Desbloquear portas de dentro da área, o que significa que as regras de acesso para sair da área não são afetadas
- Portas cativas dentro da área
- Conexão de E/S da Zona de Hardware

Limitações dos níveis de ameaça

As seguintes limitações se aplicam ao usar o recurso de nível de ameaça:

- Os níveis de ameaça funcionam independentemente das partições. Portanto, um nível de ameaça definido no nível do sistema pelos usuários de uma partição pode afetar as entidades pertencentes a outra partição se as ações tiverem um alcance genérico (aplicado a *Todas as entidades*).
- Os níveis de ameaça não podem ser aplicados às áreas federadas.

Ações de nível de ameaça

Normalmente, as ações são aplicadas a uma entidade específica. Porém, as ações que você configurar para um *nível de ameaça* podem ser aplicadas a uma entidade específica ou a todas as entidades do tipo de entidade relacionado a essa ação.

Por exemplo, a ação *Iniciar gravação* normalmente se aplica a uma câmera. No entanto, quando você está configurando um nível de ameaça, você pode selecionar *Todas as entidades* para que todas as câmeras comecem a gravar quando o nível de ameaça estiver definido.

NOTA: Se você selecionar uma entidade específica para sua ação, a ação será aplicada à entidade selecionada independentemente de a entidade ser encontrada na área onde o nível de ameaça está definido ou não.

Ações exclusivas para níveis de ameaça

As seguintes ações são exclusivas para a configuração de nível de ameaça.

Nome da ação	Entidade de destino	Descrição
Definir permissão mínima de segurança	área (Localização)	Define a autorização de segurança mínima exigida dos titulares para entrar em áreas específicas, além das restrições impostas pelas regras de acesso. Parâmetro adicional: • **Folga de segurança:** O nível de certificado de segurança mínimo necessário para entrar na área selecionada. (0=nível mais elevado, 7=nível mais baixo ou nenhum certificado especial necessário). A opção *certificado de segurança* só é visível para usuários administrativos. Esta ação funciona somente com os controladores de portas que suportam este recurso. O intervalo de valores suportados pode variar, dependendo do hardware de controle de acesso.
Definir nível mínimo de usuário	N/A	Desconecta usuários com um nível de usuário inferior ao que você especifica quando um nível de ameaça está configurado e impede que eles façam o login novamente. Parâmetro adicional: • **Nível de usuário:** O nível mínimo de usuário (1 = nível mais alto, 254 = nível mais baixo) necessário para fazer logon no sistema ou para manter logado no sistema. Esta ação só é executada quando o nível de ameaça é definido no nível do sistema. Se o usuário que define o nível de ameaça tiver um nível de usuário abaixo do mínimo exigido, esse usuário é desconectado do sistema no momento em que o nível de ameaça é definido.
Definir modo do leitor	área, porta (Localização)	Define o modo do leitor para acesso às portas. Parâmetro adicional: • **Modo do leitor:** Seleciona se o acesso é concedido usando *Cartão e PIN* ou *Cartão ou PIN* para as áreas selecionadas. Esta ação funciona somente com os controladores de portas e os leitores que suportam este recurso.

Diferenças entre níveis de ameaça e alarmes

Existem diferenças importantes entre os níveis de ameaça e os alarmes, como por que eles são acionados, como eles são ativados e assim por diante.

A tabela a seguir destaca as diferenças entre níveis de ameaça e alarmes.

Características	Alarme	Nível de ameaça
Finalidade	Oferece eventos localizados, como uma entrada forçada ou um objeto deixado sem vigilância em uma área pública.	Lida com eventos generalizados que afetam uma área inteira ou todo o sistema, como incêndio ou tiroteio.
Privilégios de configuração	• Config Tool • Adicionar/excluir alarmes • Modificar alarmes	Somente usuários administrativos podem configurar níveis de ameaça.
Ativação	Normalmente disparada por um evento para ação. Também pode ser disparada por uma ação manual.	Normalmente, configurado manualmente por um operador do Security Desk. Também pode ser disparada por um evento para ação.
Resposta do sistema na ativação	A gravação começa automaticamente em câmeras associadas ao alarme.	A lista de ação de ativação do nível de ameaça é executada automaticamente.
Método de notificação	O ícone de alarme fica vermelho na bandeja de notificação do Security Desk. Dependendo de sua configuração do Security Desk, a tarefa *Monitoramento de alarmes* pode ser colocada em primeiro plano.	O ícone de nível de ameaça fica vermelho na bandeja de notificação do Security Desk. Quando um nível de ameaça está definido no nível do sistema, o fundo do Security Desk muda para a cor do nível de ameaça.
Destinatários	Usuários do Security Desk configurados como destinatários de alarme.	Todos os usuários do Security Desk.
Classificação do evento	Alarmes são classificados de acordo com seu nível de prioridade (1=mais alto, 255=mais baixo). Os alarmes com prioridade mais altas são exibidos primeiro. Quando o nível de prioridade é o mesmo, o mais recente é exibido primeiro.	Os níveis de ameaça são independentes um do outro. Somente um nível de ameaça pode ser definido em uma área em dado momento. O último nível de ameaça definido substitui o anterior.
Desativação	Um usuário do Security Desk (destinatário do alarme) deve confirmar o alarme. Alarmes também podem ser confirmados automaticamente pelo sistema após um atraso especificado ou quando a condição de confirmação é atendida.	Um usuário do Security Desk deve limpar manualmente o nível de ameaça ou definir um nível de ameaça diferente. Um nível de ameaça também pode ser apagado automaticamente usando um evento causa-efeito (*Definir o nível de ameaça*para *Nenhum*).
Resposta do sistema na desativação	O alarme confirmado é removido de toda a lista de alarmes ativos (tarefa *Monitoramento de alarmes* no Security Desk).	A lista de ação de desativação do nível de ameaça é executada automaticamente.

Características	Alarme	Nível de ameaça
Eventos relacionados	• *Alarme disparado* • *Alarme sob investigação* • *Condição de alarme apagada* • *Alarme confirmado* • *Alarme confirmado (Alternativo)* • *Alarme confirmado forçadamente*	• Nível da ameaça definido • Nível de ameaça apagado
Privilégios do operador	• Security Desk (Aplicativo) • Monitoramento de alarme (Tarefa) • Relatório de alarme (Tarefa) • Disparar alarmes (Ação) • Colocar alarmes em espera (Ação) • Encaminhar alarmes (Ação) • Confirmar alarmes (Ação)	• Security Desk (Aplicativo) • *Definir o nível de ameaça* (Ação) O mesmo privilégio é usado para definir e eliminar os níveis de ameaça. Limpar um nível de ameaça é defini-lo para *Nenhum*. **NOTA:** As ações de ativação e desativação do nível de ameaça são realizadas pelo sistema, independentemente dos privilégios do operador.
Ações exclusivas	Nenhum.	• Definir permissão mínima de segurança • Definir nível mínimo de usuário • Definir modo do leitor

Tópicos relacionados

Sobre alarmes na página 916
Ações de nível de ameaça na página 929

Definir níveis de ameaça

Para ajudar seu pessoal de segurança a responder rapidamente a uma situação ameaçadora, você pode definir níveis de ameaça.

O que você deve saber

Somente usuários administrativos podem definir níveis de ameaça.

CUIDADO: O sistema não reverte automaticamente para o estado em que estava antes que o nível de ameaça fosse definido. Você deve definir explicitamente as ações que são acionadas quando a ameaça é desmarcada.

Para definir um nível de ameaça:

1. Abra a tarefa **Sistema**, clique na visualização **Configurações gerais** e, em seguida, clique na página **Níveis de ameaça**.
2. No fim da lista de níveis de ameaça, clique em **Adicionar um item** ().
3. Na caixa de diálogo **Configuração do nível de ameaça**, digite **Nome**, **Descrição**, **ID lógico** (opcional) e **Cor** do nível de ameaça.

   DICA: Escolha uma cor distinta para cada nível de ameaça, de modo que, quando o nível de ameaça estiver definido no nível do sistema e o fundo do Security Desk ficar nessa cor, os usuários podem facilmente identificar a ameaça.

4. Configure as **Ações de ativação** do nível de ameaça.

   Essas ações são executadas pelo sistema quando o nível de ameaça é definido, independentemente dos privilégios e permissões do usuário que definiu o nível de ameaça.

5. Configure as **Ações de desativação** do nível de ameaça.

   Essas ações são executadas pelo sistema quando o nível de ameaça é liberado ou sobrescrito por outro, independentemente dos privilégios e permissões do usuário que definiu o nível de ameaça.

6. Clique em **OK**.

   Aparece um novo nível de ameaça na lista de níveis de ameaça. 

7. Clique em **Aplicar**.

Após terminar

Para todos os usuários que precisam definir níveis de ameaça, certifique-se de que fazem parte da *partição pública* e certifique-se de que têm o privilégio de usuário *Definir nível de ameaça*.

- Para ver quais níveis de ameaça e certificados de segurança estão definidos em cada área, use a tarefa *Status do sistema*.
- Para descobrir quando os níveis de ameaça foram definidos e liberados e quem o fez, use a tarefa Trilhas da atividade.

Tópicos relacionados

Ações de nível de ameaça na página 929
Monitorar o status do seu sistema Security Center na página 316
Investigar atividades relacionadas a usuários no seu sistema Security Center na página 319

Cenário de nível de ameaça: Incêndio

Um cenário para criar níveis de ameaça é no caso de um incêndio.

Se um incêndio surgir, algumas ações com as quais o sistema responde são as seguintes:

- Soar o alarme de incêndio.

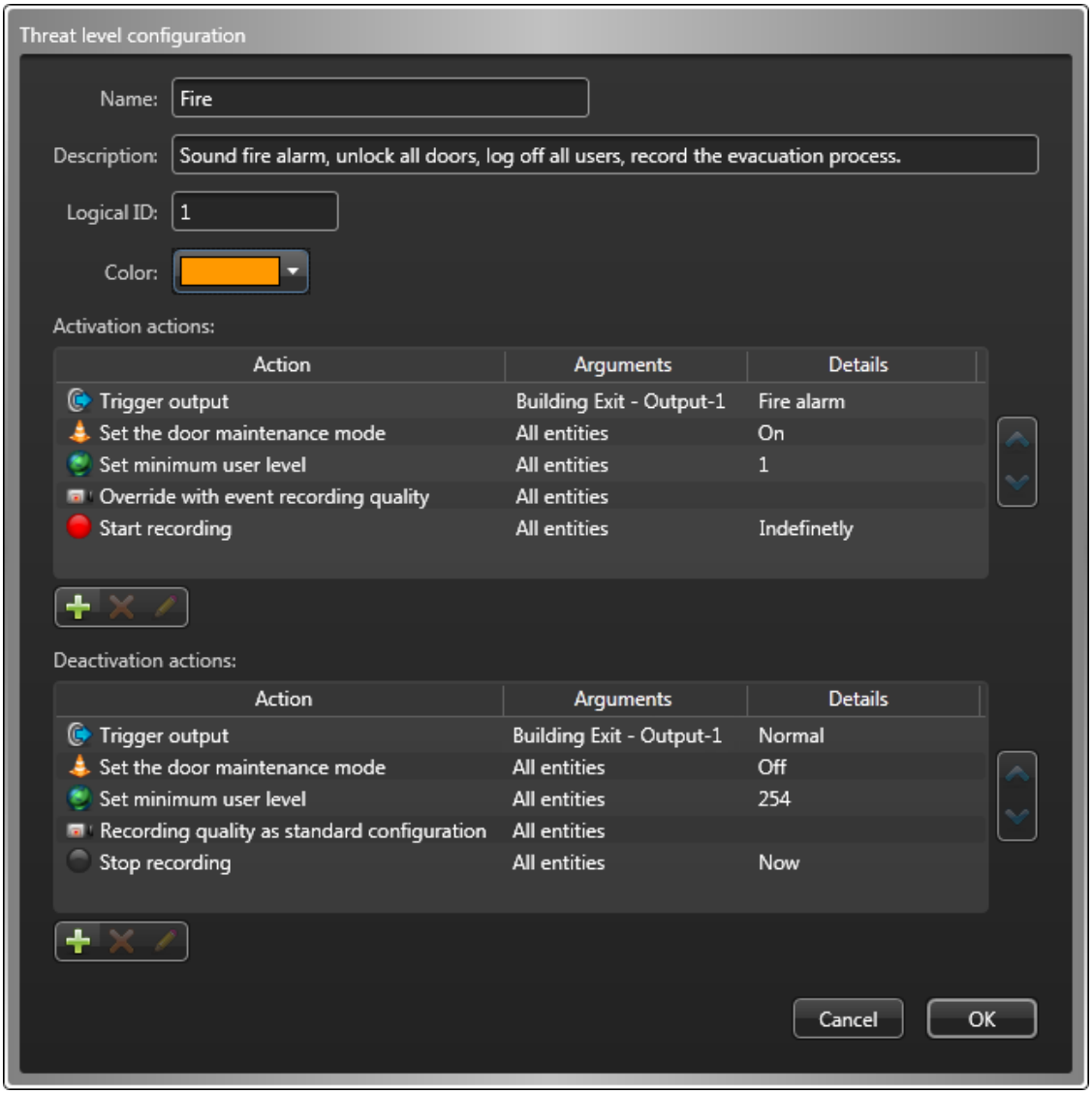
  NOTA: Para fins meramente ilustrativos. Não é uma prática recomendada.

- Desbloquear todas as portas para permitir que as pessoas evacuem.

  NOTA: Para fins meramente ilustrativos. Não é uma prática recomendada.

- Desconectar todos os usuários de baixa prioridade para liberar seus recursos (especialmente a largura de banda da rede), para usuários de alta prioridade gerenciarem a ameaça atual.
- Registrar todo o processo de evacuação com alta qualidade de vídeo, pelo tempo que durar.

Um nível de ameaça para responder a um incêndio pode ser configurado da seguinte forma:



Quando um operador configura este nível de ameaça, as seguintes ações são executadas pelo sistema:

- **Disparar saída:** Soa o alarme de incêndio através do envio do comportamento de saída *Alarme de incêndio* para o relé de saída *Saída do edifício - Saída-1*, supondo que seja onde a campainha de alarme está conectada.
- **Definir modo de manutenção da porta:** Define todas as portas dentro da área onde o nível de ameaça está configurado no modo de manutenção, efetivamente desbloqueando-as por um período de tempo indefinido. Isso é melhor do que usar a ação *Desbloquear a porta explicitamente*, que só desbloqueia as portas por alguns segundos.
- **Definir nível mínimo de usuário:** Imediatamente, desconecta todos os usuários com um nível de usuário inferior a 1, basicamente cada um que não é um administrador, encorajando-os a deixar suas mesas ao mesmo tempo, além de interromper toda atividade desnecessária na rede, para que os administradores possam ter toda largura de banda possível à disposição para lidar com a situação.

  NOTA: Esta ação só é executada quando o nível de ameaça é definido no nível do sistema. Então, se o incêndio estiver limitado a uma área, não queremos que todos saiam do sistema.
- **Sobrepor com a qualidade de gravação do evento:** Aumenta a qualidade de gravação de todas as câmeras dentro da área em que nível de ameaça está definido para a qualidade de gravação de evento.
- **Iniciar gravação:** Começa a gravação em todas as câmeras dentro da área em que o nível de ameaça está definido para uma duração infinita, ou até o comando *Interromper gravação* ser emitido.

Quando um operador libera este nível de ameaça, as seguintes ações são executadas pelo sistema:

- **Disparar saída:** Interrompe o alarme de incêndio através do envio do comportamento de saída *Normal* para o relé de saída *Saída do edifício - Saída-1*.
- **Definir modo de manutenção da porta:** Desliga o modo de manutenção em todas as portas dentro da área em que o nível de ameaça está definido. Isso efetivamente restaura todas as portas ao seu comportamento normal.
- **Definir nível mínimo de usuário:** Redefine o nível mínimo de usuário para 254 (o valor mais baixo), permitindo que todos os usuários façam logon novamente.
- **Qualidade da gravação como configuração padrão:** Restaura a qualidade de gravação padrão de todas as câmeras dentro da área em que nível de ameaça está definido.
- **Interromper gravação:** Interrompe a gravação de todas as câmeras dentro da área em que o nível de ameaça está definido. Esta ação não interromperá a gravação em câmeras que estejam em uma programação de gravação contínua.

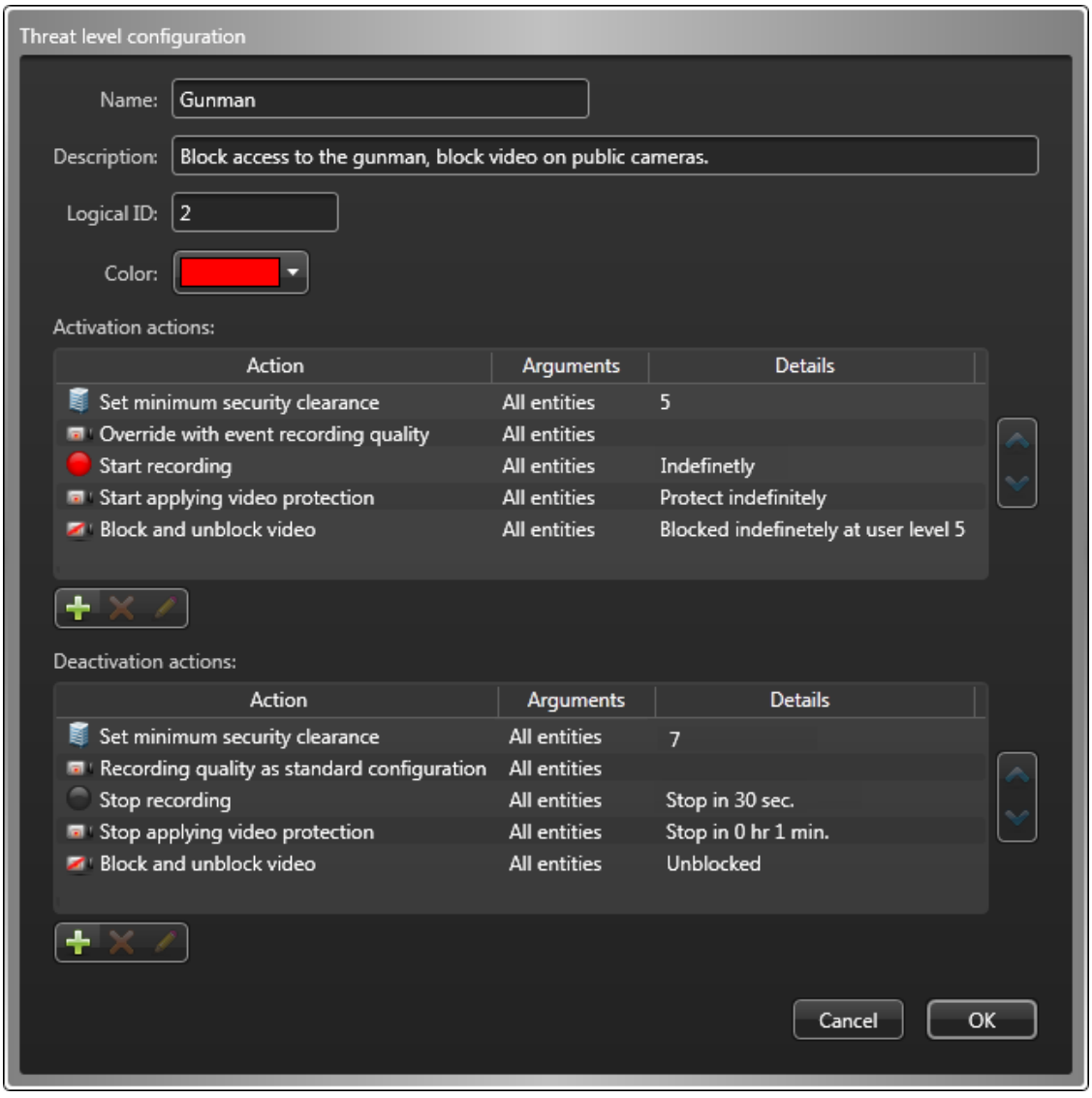
Cenário de nível de ameaça: pessoa armada

Um cenário para criar níveis de ameaça é no caso de uma pessoa armada.

Se uma pessoa armada ou um atirador for vista, algumas ações com as quais o sistema responde são as seguintes:

- Bloquear o acesso ao local onde o atirador está para transeuntes inocentes.
- Registrar o incidente com filmagem em vídeo de alta qualidade como prova no tribunal.
- Proteger as gravações de vídeo de todo o evento contra exclusão acidental.
- Bloquear as imagens de vídeo sensíveis para o público, caso alguns fluxos de vídeo sejam exibidos em sites públicos.

Um nível de ameaça para responder à presença de uma pessoa armada ou um atirador pode ser configurado da seguinte forma:



Quando um operador configura este nível de ameaça, as seguintes ações são executadas pelo sistema:

- **Definir permissão mínima de segurança:** Reduz a mobilidade da pessoa armada, assumindo que sua credencial tem uma autorização de segurança inferior a 5 (entre 6-7).

NOTA: Esta configuração pressupõe que apenas o pessoal de segurança armado possui um nível de autorização superior a 5 (entre 0 a 5) e que os operadores de segurança continuam a monitorar todas as portas para que possam abri-las quando necessário para permitir que pessoas inocentes se escondam em áreas protegidas onde a pessoa armada não tenha acesso.

- **Sobrepor com a qualidade de gravação do evento:** Aumenta a qualidade de gravação de todas as câmeras dentro da área em que nível de ameaça está definido para a qualidade de gravação de evento.
- **Iniciar gravação:** Começa a gravação em todas as câmeras dentro da área em que o nível de ameaça está definido para uma duração infinita, ou até o comando *Interromper gravação* ser emitido.
- **Iniciar a aplicação da proteção do vídeo:** Inicia a proteção dos vídeos gravados nas câmeras dentro da área onde o nível de ameaça está configurado, de agora até o comando *Parar aplicação de proteção de vídeo* ser emitido, por um período de tempo ilimitado.
- **Bloquear e desbloquear vídeo:** Bloqueie todos os usuários com nível de usuário inferior a 5 de exibir o vídeo das câmeras dentro da área onde o nível de ameaça está definido, de agora até o bloqueio de vídeo ser parado explicitamente, por um período de tempo ilimitado.

  NOTA: Esta configuração pressupõe que todo o pessoal de segurança possui nível de usuário superior a 5 e pode continuar a monitorar a cena.

Quando um operador libera este nível de ameaça, as seguintes ações são executadas pelo sistema:

- **Definir permissão mínima de segurança:** Restaura o acesso normal à área para todos os titulares de cartões, definindo a autorização de segurança para 7 (o nível mais baixo).
- **Qualidade da gravação como configuração padrão:** Restaura a qualidade de gravação padrão de todas as câmeras dentro da área em que nível de ameaça está definido.
- **Interromper gravação:** Interrompe a gravação de todas as câmeras dentro da área em que o nível de ameaça está definido após 30 segundos. Esta ação não interromperá a gravação em câmeras que estejam em uma programação de gravação contínua.
- **Parar aplicação de proteção de vídeo:** Interrompe a proteção de vídeos gravados de todas as câmeras dentro da área em que o nível de ameaça está definido após um minuto.
- **Bloquear e desbloquear vídeo:** Desbloqueia todas as câmeras dentro da área em que o nível de ameaça está definido. O vídeo gravado durante o tempo em que o nível de ameaça estava ativo permanecerá bloqueado para reprodução para usuários cujo nível de usuário seja inferior a 5.

50

Zonas e detecção de intrusão

Esta seção inclui os seguintes tópicos:

- "Sobre zonas" na página 939
- "Sobre Zone Managers" na página 942
- "Acerca de comportamentos de saída" na página 943
- "Criar zonas de hardware" na página 944
- "Definição de configurações de área de hardware" na página 945
- "Criar áreas virtuais" na página 947
- "Definir configurações de área virtuais" na página 948
- "Criar zonas de E/S" na página 950
- "Definição de configurações de área de E/S" na página 951
- "Integração do painel de intrusão" na página 953
- "Sobre Intrusion Managers" na página 954
- "Criar a função Intrusion Manager" na página 955
- "Sobre unidades de detecção de intrusão" na página 957
- "Sobre áreas de detecção de intrusão" na página 958
- "Criando áreas de detecção de intrusão" na página 959
- "Mover unidades de detecção de intrusão para um Intrusion Manager diferente" na página 960

Sobre zonas

É um tipo de entidade que monitora um conjunto de entradas e dispara eventos com base nos estados combinados. Esses eventos podem ser usados para controlar relés de saída.

O conceito de uma zona é emprestado do mundo dos *painéis de alarme*, onde entradas elétricas são associadas a zonas para desencadear alarmes específicos. No Security Center, as entradas elétricas são associadas a zonas para acionar eventos. Usando *eventos causa-efeito*, estes eventos podem ser usados não apenas para acionar saídas, mas também para acionar alarmes, enviar e-mails, iniciar gravações de câmeras e assim por diante.

DICA: Você também pode definir eventos personalizados para corresponder a cada combinação de entradas especiais.

Uma zona pode ser armada (dispara ativada) ou desarmada (dispara desativada) usando um interruptor de chave, um comando de software ou uma programação. Uma zona pode ser armada por software (usando um comando de ação ou de acordo com uma programação), ou por hardware (para unidades que suportam esse recurso).

Vinculação de I/O

A ligação de E/S é o controle de relés de saída específicos com base no resultado combinado de um conjunto específico de entradas elétricas. Cada entrada pode ser conectada a um dispositivo de monitoramento específico, como um sensor de movimento, um detector de fumaça, um contato de porta ou janela e assim por diante.

Por exemplo, se uma janela quebrar, o sensor de *vidro quebrado* em uma janela conectado a uma entrada em uma *unidade* pode ser vinculado a uma saída que aciona uma campainha.

CUIDADO: Em unidades HID VertX, algumas entradas, como *Falha de CA* e *Falha de bateria*, devem ser configuradas para algo diferente do seu propósito inicial (deixar as caixas de seleção vazias) antes que elas possam ser usadas para vinculação de E/S. No entanto, outras entradas, como *Monitor de porta*, só podem ser usadas para o propósito designado. Se você usar uma entrada de propósito específico como propósito geral, sua configuração não funcionará. Não exceda 20 entradas por zona com unidades HID VertX. Exceder este limite pode levar a problemas de sincronização da unidade.

Estados da zona

Os estados de zona são determinados por uma combinação (AND/OR) de entradas associadas à zona.

Os seguintes estados de zona estão disponíveis:

- **Normal:** Quando a combinação de entradas resulta em zero (0).
- **Ativo:** Quando a combinação de entradas resulta em um (1).
- **Problema:** Exige ter pelo menos uma entrada supervisionada. A zona fica no estado de *Problema* quando pelo menos uma das entradas está no estado *Problema*. O estado *Problema* supera todos os outros estados.

Zonas de hardware

Uma zona de hardware é um tipo de zona onde o vínculo de E/S é feito por uma única unidade de controle de acesso. Uma zona de hardware funciona independentemente do Access Manager e, consequentemente, não pode ser ativada ou desativada pelo Security Desk.

As zonas de hardware são recomendadas quando as respostas rápidas e as operações offline são cruciais para o seu sistema de segurança. O *unidade de controle de acesso* controlando a zona não deve ser operado

em *modo de servidor*. Uma vez que a unidade esteja configurada no Security Center, ela deve ser capaz de atuar sozinha sem ser conectada ao Security Center ou sem ser controlada por ele.

As zonas de hardware podem ser armadas usando uma chave (entrada) ou em programação.

Zonas virtuais

Uma zona virtual é um tipo de zona onde o vínculo de E/S é feito pelo software. Os dispositivos de entrada e saída podem pertencer a diferentes unidades de diferentes tipos. Uma zona virtual é controlada pelo Zone Manager e somente funciona quando todas as unidades estão online. Ela pode ser armada e desarmada pelo Security Desk.

As zonas virtuais são recomendadas quando a flexibilidade é exigida e quando as unidades de controle de acesso não estão disponíveis.

Zonas de E/S

Uma zona de E/S é uma entidade de zona na qual a ligação E/S pode ser distribuída a várias unidades Synergis™, enquanto uma unidade age como a unidade principal. Todas as unidades Synergis™ envolvidas em uma zona de E/S devem ser gerenciadas pelo mesmo Access Manager. A zona I/O trabalha independentemente do Access Manager, mas para de funcionar se a unidade mestra está desativada. Uma zona de E/S pode ser ativada e desativada pelo

As zonas de E/S são recomendadas quando são necessárias respostas rápidas, operação offline e ligação de E/S em várias unidades.

Diferenças entre os tipos de área

A tabela a seguir lista as diferenças entre uma zona de hardware, uma zona virtual e uma zona de E/S e pode ajudá-lo a decidir qual o tipo de zona que você precisa criar.

Características	Zona de hardware	Zona virtual	Zona de E/S
Uso recomendado	As zonas de hardware são recomendadas quando as respostas rápidas e as operações offline são cruciais para o seu sistema de segurança.	As zonas virtuais são recomendadas quando a flexibilidade é exigida e quando as unidades de controle de acesso não estão disponíveis.	As zonas de E/S são recomendadas quando são necessárias respostas rápidas, operação offline e ligação de E/S em várias unidades.
Função	Gestor de Acesso	Gerenciador de Zona	Gestor de Acesso
Tipo de unidade requerido	HID ou unidade Synergis™	Qualquer tipo de unidade com entradas e saídas[1]	Unidades Synergis™[2]
Modo de operação da unidade	Online e Offline	Online	Online e Offline
Execução de ligação de E/S	Unidade de controle de acesso	Gerenciador de Zona	Unidade mestre[3]
Ligação de E/S (entradas)	Todas as entradas são da mesma unidade	Pode combinar entradas de qualquer unidade de qualquer tipo	Pode combinar entradas de qualquer unidade

Características	Zona de hardware	Zona virtual	Zona de E/S
Operador lógico (entradas)	**OR**/AND	**OR**/AND	OU
Ligação de E/S (saídas)	Todas as saídas são da mesma unidade que as entradas	Pode disparar saídas de qualquer unidade de qualquer tipo	Pode disparar saídas em qualquer unidade
Configuração de ligação de E/S	Configuração de zona + eventos para ação	Configuração de zona + eventos para ação	Configuração de zona isoladamente
Ponto a ponto	Não	Não	Sim[4]
Armar/desarmar do Security Desk	Não	Sim	Sim[5]
Armar/desarmar usando ações	Não	Sim	Sim[5]
Armar/desarmar usando chave	Sim[6]	Não	Não
Armar/desarmar com cronograma	Sim[7]	Sim[8]	Sim[9]
Atraso de armamento	**Desligado**/Ligado (mm:ss)	**Desligado**/Ligado (mm:ss)	Não
Atraso na entrada	**Desligado**/Ligado (mm:ss)	**Desligado**/Ligado (mm:ss)	Não
Modo de manutenção	Não	Não	Sim

[1] Não é recomendado o uso de zonas para monitorar as entradas de unidades de detecção de intrusão.

[2] Requer o Security Center 5.5 e posteriores e o Synergis™ Softwire 10.2 e posteriores.

[3] A unidade mestre é a unidade Synergis™ que você seleciona para fazer vinculação de E/S.

[4] Até 15 unidades Synergis™ podem se comunicar diretamente entre si, desde que estejam todas no mesmo Access Manager.

[5] A unidade mestre deve estar online.

[6] O interruptor de chave deve ser conectado a uma entrada na mesma unidade de controle de acesso.

[7] Apenas uma agenda por vez, e não pode ser combinada com a abordagem de interruptor de chave.

[8] Suporta múltiplas agendas.

[9] Suporta múltiplas agendas, inclusive agendas de exceção.

Sobre Zone Managers

É um tipo de função que gerencia as zonas virtuais e dispara eventos ou relés de saída com base nas entradas configuradas por cada zona. Também registra os eventos de zona em um banco de dados para relatórios de atividades de zona.

Múltiplas instâncias desta função podem ser criadas no sistema.

Acerca de comportamentos de saída

É um tipo de entidade que define um formato de sinal de saída personalizado, como um pulso com atraso e duração.

Alguns exemplos de comportamentos de saída podem incluir o controle de um portão de estacionamento, piscar uma luz no armazém e assim por diante.

Os comportamentos de saída são usados para controlar relés de saída ou unidades de controle de acesso, unidades de vídeo e zonas que não estão sendo usadas para controlar bloqueios de portas. Eles podem ser desencadeados por eventos de causa-efeito automáticos, manualmente através de *ações instantâneas* no Security Desk, ou por meio de *Vinculação de I/O*.

Criar zonas de hardware

Para ter uma zona que possa operar por conta própria mesmo quando a unidade de controle de acesso não está conectada ao Access Manager, você deve criar uma no Security Center.

Antes de iniciar

Faça o seguinte:

- Configure a função Access Manager que gerenciará a zona.
- Adicione a unidade de controle de acesso que controlará a zona em seu sistema.

O que você deve saber

Uma *zona de hardware* permite que você programe o comportamento de ligação de E/S em uma unidade de controle de acesso para que ela possa operar por conta própria. As zonas de hardware só podem ser controladas por uma única unidade de controle de acesso.

Criar uma zona de hardware:

1 Abra a tarefa **Exibição de área**.
2 Clique em **Adicionar uma entidade** () > **Zona**.
3 No assistente de criação de zonas, digite um nome e uma descrição para a zona.
4 Selecione a área da qual esta zona faz parte em **Local** e clique em **Próximo**.
5 Na página **Informações da zona**, clique em **Zona de hardware**.
6 Na caixa de diálogo, selecione a unidade de controle de acesso para controlar esta zona e clique em **OK**.
7 Clique em **Criar** > **Fechar**.

Após terminar

Configure a zona de hardware.

Tópicos relacionados

Sobre zonas na página 939

Definição de configurações de área de hardware

Para monitorar e configurar a vinculação de E/S para zonas de hardware no Security Center, você deve decidir como o estado da zona é avaliado, quais eventos são acionados com base nas entradas associadas à zona e quando a zona está armada.

Antes de iniciar

Faça o seguinte:

- Para armar a zona segundo uma agenda, já deve existir uma agenda criada.
- Para armar a zona usando um interruptor de chave, uma das entradas da unidade de controle de acesso deve ser conectada ao interruptor de chave.

O que você deve saber

Todos os pontos de entrada e relés de saída configurados para esta zona devem pertencer à mesma unidade de controle de acesso que está controlando a zona.

Você não pode armar ou desarmar uma zona de hardware do Security Desk, ou usando um comando de software (evento para ações).

Para definir configurações de área de hardware:

1 Abra a tarefa **Exibição de área**.
2 Selecione zona de hardware a configurar e clique na aba **Propriedades**.
3 Na lista, selecione as entradas para determinar o estado da zona.
4 Coloque a chave **Operador** na posição desejada.
   - **E:** Combine os estados de entrada com o operador lógico AND.
   - **OU:** (Padrão) Combine os estados de entrada com o operador lógico OR

   Exemplo: Se você selecionar o operador **AND**, a zona é considerada como estando em um estado *Ativo* quando todas as entradas selecionadas estão no estado *Ativo*. Se você selecionar o operador **OR**, a zona é considerada como estando em um estado *Ativo* se uma das entradas selecionadas estiver no estado *Ativo*.
5 Na seção **Eventos associados**, selecione nas listas suspensas abaixo quais eventos disparar quando o estado de zona mudar:

   Esses eventos são disparados somente quando a zona está armada. Selecione *Nenhum* caso um estado de zona deva ser ignorado.
   - **Normal:** Quando a combinação de entradas resulta em zero (0).
   - **Ativo:** Quando a combinação de entradas resulta em um (1).
   - **Problema:** Exige ter pelo menos uma entrada supervisionada. A zona fica no estado de *Problema* quando pelo menos uma das entradas está no estado *Problema*. O estado *Problema* supera todos os outros estados.
6 Digite em **Limiar de reativação** quantos milissegundos devem se passar antes do evento associado ao estado de zona podem ser disparados novamente e clique em **Aplicar**.
7 Clique na aba **Armamento** e configure a forma como a zona é armada.
8 Na seção *Origem do armamento*, selecione se a zona é armada usando um interruptor de chave ou um cronograma:
   - **Cronograma:** Selecione uma programação predefinida para armar a zona.
   - **Ponto de entrada:** Selecione a entrada que é ligada à chave de acionamento.
9 (Opcional) Para que as pessoas tenham mais tempo para sair de uma zona que acabaram de armar, ou desarmar uma zona na qual entraram, deixe as seguintes opções como **Ligado**:

- **Atraso de armamento:** Duração (mm:ss) que você deseja entre o tempo em que a zona é armada e o tempo em que os disparos de evento se tornam ativos.
- **Atraso na entrada:** Duração (mm:ss) que você deseja entre o tempo em que o sensor de entrada é disparado e o tempo em que os eventos são disparados. Esta opção permite desarmar a zona antes de disparar os relés de saída.

10 (Opcional) Selecione uma **Campainha de contagem regressiva** para usar durante o período de atraso de armamento, da seguinte forma:

NOTA: Esta opção só está disponível quando a zona é armada usando um interruptor de chave.

a) Na lista suspensa **Campainha de contagem regressiva**, selecione um relé de saída.
b) Na lista suspensa **Comportamento de saída**, selecione uma entidade de comportamento de saída para determinar o padrão do sinal a enviar à campainha.

11 Clique em **Aplicar**.

Após terminar

- Teste a sua zona verificando se os eventos gerados aparecem no relatório *Atividades de zona* no Security Desk. Para obter mais informações, consulte o *Guia do Usuário do Security Desk*.
- Para cada evento associado configurado para esta zona,crie eventos para ação para disparar os relés de saída desejados para completar as configurações de vinculações de E/S.

  NOTA: Para que a zona de hardware funcione, os relés de saída devem estar entre os periféricos da unidade que controla a zona.

Tópicos relacionados

Considerações sobre conexão de E/S do HID na página 1161
Abas de configuração de zonas de hardware na página 1010

Criar áreas virtuais

Para monitorar dispositivos de entrada (sensores, interruptores e assim por diante) usando o Security Desk e para usá-los para desencadear eventos, você deve criar uma zona virtual no Security Center.

Antes de iniciar

Configure a função Zone Manager que gerenciará a zona.

O que você deve saber

Uma zona virtual permite ativar/desativar o monitoramento nos vários dispositivos de entrada (sensores, interruptores, etc.) em seu sistema usando o Security Desk e usá-los para desencadear eventos.

Para criar uma zona virtual:

1 Abra a tarefa **Exibição de área**.
2 Clique em **Adicionar uma entidade** () > **Zona**.
3 No assistente de criação de zonas, digite um nome e uma descrição para a zona.
4 Selecione a área da qual esta zona faz parte em **Local** e clique em **Próximo**.
5 Na página **Informações da zona**, clique em **Zona virtual**.

   Se você tiver várias funções Zone Manager, você será solicitado a selecionar uma.

6 Clique em **Criar** > **Fechar**.

Após terminar

Configure a zona virtual.

Tópicos relacionados

Sobre zonas na página 939

Definir configurações de área virtuais

Para monitorar dispositivos de entrada e usá-los para acionar eventos de zonas virtuais no Security Center, você deve decidir como o estado da zona é avaliado, quais eventos são acionados com base nas entradas associadas à zona e quando a zona está armada.

Antes de iniciar

Para armar a zona segundo uma agenda, já deve existir uma agenda criada.

O que você deve saber

Uma zona virtual pode ser armada a qualquer momento por um operador do Security Desk ou pela ação *Armar zona*. O horário de armamento é opcional e só é necessário se você deseja que a zona seja armada automaticamente em um determinado momento. Uma zona virtual pode ser desarmada a qualquer momento por um operador do Security Desk ou pela ação *Desarmar zona* desencadeada por um evento.

Para definir configurações de zonas virtuais:

1 Abra a tarefa **Exibição de área**.

2 Selecione a zona virtual a configurar e clique na aba **Propriedades**.

3 Na lista **Entradas**, clique em **Adicionar um item** (), selecione as entradas que determinam o estado da zona e clique em **Selecionar**.

DICA: Mantenha pressionado **Ctrl** ou **Shift** para selecionar várias entradas.

4 Coloque a chave **Operador** na posição desejada.

- **E:** Combine os estados de entrada com o operador lógico AND.
- **OU:** (Padrão) Combine os estados de entrada com o operador lógico OR

Exemplo: Se você selecionar o operador **AND**, a zona é considerada como estando em um estado *Ativo* quando todas as entradas selecionadas estão no estado *Ativo*. Se você selecionar o operador **OR**, a zona é considerada como estando em um estado *Ativo* se uma das entradas selecionadas estiver no estado *Ativo*.

5 Na seção **Eventos associados**, selecione nas listas suspensas abaixo quais eventos disparar quando o estado de zona mudar:

Esses eventos são disparados somente quando a zona está armada. Selecione *Nenhum* caso um estado de zona deva ser ignorado.

- **Normal:** Quando a combinação de entradas resulta em zero (0).
- **Ativo:** Quando a combinação de entradas resulta em um (1).
- **Problema:** Exige ter pelo menos uma entrada supervisionada. A zona fica no estado de *Problema* quando pelo menos uma das entradas está no estado *Problema*. O estado *Problema* supera todos os outros estados.

6 Digite em **Limiar de reativação** quantos milissegundos devem se passar antes do evento associado ao estado de zona podem ser disparados novamente e clique em **Aplicar**.

7 Clique na aba **Armamento** e configure a forma como a zona é armada.

8 Na seção *Origem do armamento*, clique em **Adicionar um item** (), selecione uma agenda predefinida para quando a zona deve ser armada e clique em **Selecionar**.

9 (Opcional) Para que as pessoas tenham mais tempo para sair de uma zona que acabaram de armar, ou desarmar uma zona na qual entraram, deixe as seguintes opções como **Ligado**:

- **Atraso de armamento:** Duração (mm:ss) que você deseja entre o tempo em que a zona é armada e o tempo em que os disparos de evento se tornam ativos.

- **Atraso na entrada:** Duração (mm:ss) que você deseja entre o tempo em que o sensor de entrada é disparado e o tempo em que os eventos são disparados. Esta opção permite desarmar a zona antes de disparar os relés de saída.

10 Clique em **Aplicar**.

Após terminar

- Teste a sua zona verificando se os eventos gerados aparecem no relatório *Atividades de zona* no Security Desk. Para obter mais informações, consulte o *Guia do Usuário do Security Desk*.
- Para cada evento associado configurado para esta zona,crie eventos para ação para disparar os relés de saída desejados para completar as configurações de vinculações de E/S.

Tópicos relacionados

Abas de configuração de zona virtual na página 1041

Criar zonas de E/S

Para que as entradas de uma unidade Synergis™ acionem relés de saída em outras unidades Synergis™ (mesmo que algumas, ou nenhuma delas, estejam conectadas ao Access Manager), você deve criar uma zona de E/S no Security Center.

Antes de iniciar

Faça o seguinte:

- Configure a função Access Manager que gerenciará a zona.
- Adicione as unidades Synergis™ que serão vinculadas pela zona.
- Verifique se todas as unidades estão executando o Synergis™ Softwire versão 10.2 ou posterior.

O que você deve saber

Uma *Zona de E/S* permite que você programe o comportamento de vinculação de E/S em várias unidades Synergis™, com uma unidade designada como a unidade mestre. Todas as unidades devem ser gerenciadas pelo mesmo Access Manager. Uma Zona de E/S pode ser ativada e desativada pelo Security Desk, desde que a unidade mestre esteja online.

Para criar uma zona de hardware:

1 Abra a tarefa **Exibição de área**.
2 Clique em **Adicionar uma entidade** ( ) > **Zona**.
3 No assistente de criação de zonas, digite um nome e uma descrição para a zona.
4 Selecione a área da qual esta zona faz parte em **Local** e clique em **Próximo**.
5 Na página **Informações da zona**, clique em **Zona de E/S**.
6 Na caixa de diálogo, selecione a unidade Synergis™ que desempenhará a função de *unidade mestre* entre as suas semelhantes e clique em **OK**.

   A unidade mestre é a unidade Synergis™ que você seleciona para fazer vinculação de E/S. Uma vez que sua escolha seja feita, ela não pode ser alterada após a criação da Zona de E/S.
7 Clique em **Criar** > **Fechar**.

Após terminar

Configure a Zona de E/S.

Tópicos relacionados

Sobre zonas na página 939

Definição de configurações de área de E/S

Para monitorar e configurar a ligação de E/S para zonas de E/S no Security Center, você deve decidir como o estado da zona é avaliado, quais relés de saída são acionados com base nas entradas associadas à zona e quando a zona está armada.

Antes de iniciar

Faça o seguinte:

- Para armar a zona segundo uma agenda, já deve existir uma agenda criada.
- Para disparar um relé de saída, umcomportamento de saída já deve ter sido criado.

O que você deve saber

Todos os pontos de entrada e relés de saída configurados para esta zona devem pertencer às unidades Synergis™ gerenciadas pelo mesmo Access Manager.

Você pode configurar a ligação de E/S a partir da aba **Propriedades** da zona de E/S. Você não precisa criar *eventos causa-efeito* para disparar relés de saída.

IMPORTANTE: Se as entradas e saídas configuradas para esta zona não pertencem à mesma unidade Synergis™, você deve habilitar a opção **Ativar ponto a ponto** no Access Manager.

Para definir configurações de zona de E/S:

1 Abra a tarefa **Exibição de área**.
2 Selecione zona de E/S a configurar e clique na aba **Propriedades**.
3 Na lista suspensa **Cronograma de armamento**, selecione um cronograma predefinido para quando a zona estiver armada.

   Para adicionar mais agendamentos predefinidos para definir a programação de armar, clique em **Avançado** ( ) e clique em **Adicionar um item** ( ).
4 (Opcional) Clique em **Exceções** para definir períodos dentro do horário de armamento quando a zona não deve ser armada.
5 Na lista **Entradas**, clique em **Adicionar um item** ( ), e selecione as entradas que determinam o estado da zona.

   A zona fica no estado de *Problema* quando pelo menos uma das entradas está no estado Problema.
6 Na lista **Saídas**, clique em **Adicionar um item** ( ), e selecione os relés de saída para os quais deseja enviar o comportamento de saída configurado, quando a zona estiver armada e no estado *Ativo*, ou quando a zona estiver no estado de *Problema*.

   MELHOR PRÁTICA: O tanto quanto possível, use os relés de saída na unidade mestre. Isso permite que a zona E/S continue a funcionar quando uma ou mais unidades escravas estiverem desligadas.
7 Na lista suspensa **Comportamento de saída**, selecione o comportamento de saída para enviar aos relés de saída.
8 Selecione **Ativar saída em problema quando a zona está desarmada** se quiser que os relés de saída sejam acionados quando a zona estiver em estado de *Problema*.
9 Na lista suspensa **Reverter para**, selecione o comportamento de saída para enviar para os relés de saída quando a zona retornar ao estado *Normal*.
10 Na seção **Eventos associados**, selecione nas listas suspensas abaixo quais eventos disparar quando o estado de zona mudar:

   Esses eventos são disparados somente quando a zona está armada. Selecione *Nenhum* caso um estado de zona deva ser ignorado.

   - **Normal:** Quando a combinação de entradas resulta em zero (0).
   - **Ativo:** Quando a combinação de entradas resulta em um (1).

- **Problema:** Exige ter pelo menos uma entrada supervisionada. A zona fica no estado de *Problema* quando pelo menos uma das entradas está no estado *Problema*. O estado *Problema* supera todos os outros estados.

11 Digite em **Limiar de reativação** quantos milissegundos devem se passar antes do evento associado ao estado de zona podem ser disparados novamente e clique em **Aplicar**.

Após terminar

Teste a sua zona verificando se os eventos gerados aparecem no relatório *Atividades de zona* no Security Desk. Para obter mais informações, consulte o *Guia do Usuário do Security Desk*.

Tópicos relacionados

Zona de E/S - Aba Propriedades na página 1013

Integração do painel de intrusão

Os painéis de intrusão (também conhecidos como *painéis de alarme* ou *painéis de controle*) podem ser integrados ao Security Center usando a função Intrusion Manager, que permite monitorar o status de cada zona (ou grupo de sensores) em tempo real, gerar relatórios de atividades detalhados e armar/desarmar zonas (ou partições) definidas nos painéis de intrusão no Security Desk.

O Security Center suporta painéis de intrusão Bosch, DSC PowerSeries, Honeywell Galaxy Dimension e DMP, bem como sensores de proteção de perímetro Southwest Microwave. Para obter informações sobre como integrar unidades de detecção de intrusão no Security Center, consulte o *Guia de Extensões de Painel de Intrusão Bosch*, o *Guia de Extensões do Painel de Intrusão Honeywell Galaxy*, o *Guia de Integração do Painel de Controle DMP*, o *Guia de Extensões de Painel de Intrusão DSC PowerSeries* e o *Guia de Extensões Southwest Microwave RPM II*.

Como a integração de painéis de intrusão funciona

A função Intrusion Manager recebe eventos do painel através de uma rede IP ou conexão serial, os relata ao vivo no Security Desk e os registra em um banco de dados para relatórios futuros. A função também retransmite comandos do usuário para o painel (como armar e desarmar as áreas de detecção de intrusão) e aciona as saídas conectadas ao painel através de eventos causa-efeito (por exemplo, um evento *Master da área de detecção de intrusão colocado em atenção* no Security Center pode acionar uma saída no painel).

Para obter mais informações sobre como monitorar eventos, alarmes ou unidades de detecção de intrusão, o widget de área de detecção de intrusão, desencadear ações instantâneas, monitorar o status de entidades no seu sistema usando a tarefa *Status do sistema*, ou usando as tarefas *Atividades de área de detecção de intrusão* ou *Eventos de unidade de detecção de intrusão*, consulte o *Guia do Usuário do Security Desk*. Você pode acessar esse guia pressionando **F1** no Security Desk.

Sobre Intrusion Managers

A função Gerenciador de intrusão monitora e controla as unidades de detecção de intrusão. Ele ouve os eventos relatados pelas unidades, oferece relatórios ao vivo para o Security Center e registra os eventos em um banco de dados para relatório futuro.

O Intrusion Manager também transmite comandos de usuários para painéis de intrusão, como armar as *áreas de detecção de intrusão* (ou zonas) e acionar saídas conectadas ao painel usando *eventos causa-efeito*.

Múltiplas instâncias desta função podem ser criadas no sistema.

Limitações da função Intrusion Manager

Para fins de *failover*, o Intrusion Manager pode ser atribuído a mais de um servidor. No entanto, o Intrusion Manager só suporta failover quando os painéis de intrusão estão conectados via IP. O failover não é suportado se o seu painel de intrusão estiver diretamente conectado ao seu servidor via porta serial.

Criar a função Intrusion Manager

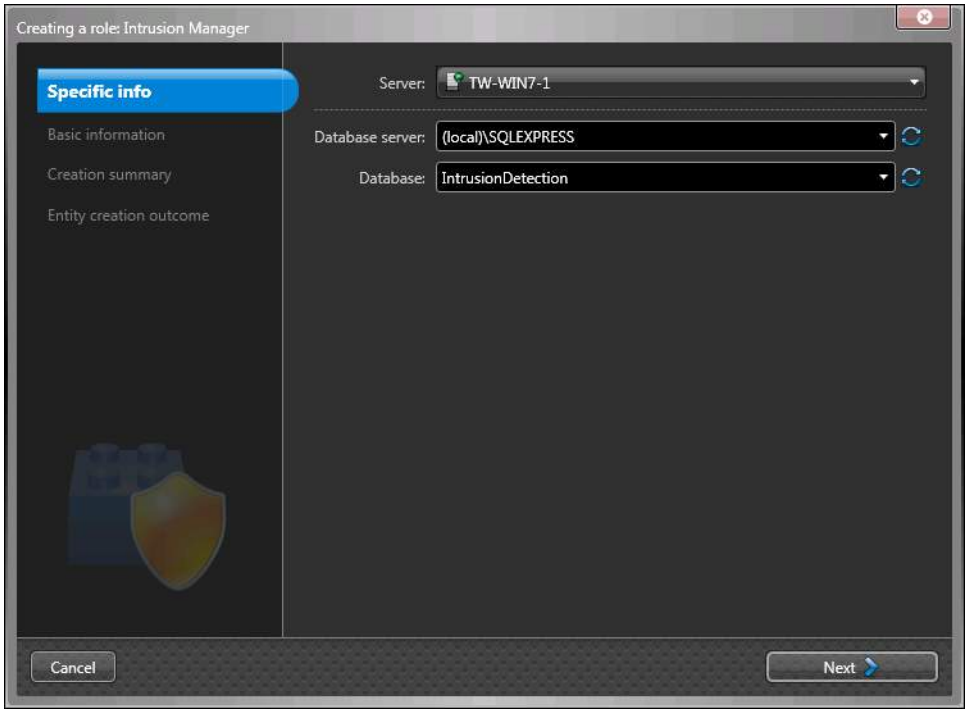
Você deve criar uma função Intrusion Manager em Config Tool para gerenciar a unidade de detecção de intrusão.

Para criar uma função Intrusion Manager:

1 Na página inicial do Config Tool, abra a tarefa *Sistema*.

2 Clique em **Adicionar uma entidade** () e, em seguida, clique em **Intrusion Manager**.

A janela *Criar uma tarefa: Intrusion Manager* é aberta.



3 Na página **Informações específicas**, faça o seguinte:

a) Na lista suspensa **Servidor**, selecione o servidor atribuído a esta função.

NOTA: Se nenhum servidor de expansão estiver presente, esta opção não estará disponível.

b) No campo **Servidor do banco de dados**, digite ou selecione o nome do servidor de banco de dados.

c) No campo **Banco de dados**, digite ou selecione o nome do banco de dados (por exemplo, **IntrusionDetection**).

d) Clique em **Próximo**.

4 Na página **Informações básicas**, faça o seguinte:

a) Digite o **Nome da entidade** (**Intrusion Manager**).

b) Digite uma **Descrição da entidade** para a função.

c) Clique em **Próximo**.

5 Na página **Resumo de criação**, faça o seguinte:

a) Verifique as informações que você digitou.

b) Se tudo estiver correto, clique em **Criar**, ou clique em **Voltar** para modificar suas configurações.

Quando a função estiver criada, verá a seguinte mensagem: *A operação foi bem-sucedida.*

6 Clique em **Fechar**.

A função Intrusion Manager é exibida no navegador de entidades.

Após terminar

Adicione as unidades de detecção de intrusão em Security Center.

Sobre unidades de detecção de intrusão

Uma unidade de detecção de intrusão é uma entidade que representa um dispositivo de intrusão (painel de intrusão, painel de controle, receptor e assim por diante) que é monitorado e controlado pela função Gerenciador de intrusão.

Um *painel de intrusão* (também conhecido como *painel de alarme* ou *painel de controle*) é uma unidade montada na parede onde os sensores de alarme (sensores de movimento, detectores de fumaça, sensores de porta etc.) e os fios dos alarmes de intrusão estão conectados e são gerenciados.

Para obter uma lista de painéis de detecção de intrusão suportados no Security Center, consulte as *Notas de Versão do Security Center*.

Para monitorar e controlar áreas de detecção de intrusão (zonas ou partições) no Security Desk, você deve inscrever o painel de intrusão que os controla adicionando uma unidade de detecção de intrusão. Para obter informações sobre como criar unidades de detecção de intrusão no Security Center, consulte o *Guia de Extensões de Painel de Intrusão Bosch*, o *Guia de Integração do Painel de Controle Honeywell Galaxy*, o *Guia de Integração do Painel de Controle DMP* ou o *Guia de Extensões de Painel de Intrusão DSC PowerSeries*.

Limitações no monitoramento de entradas do painel de intrusão

Recomendamos que você use painéis de intrusão somente para monitoramento de intrusão.

Os painéis de intrusão não são projetados para capturar mudanças rápidas consecutivas em seus estados de entrada, como portas abertas e fechadas rapidamente, ou sensores de movimento que detectam movimentos constantes.

O objetivo principal de uma entrada em um painel de intrusão é disparar um alarme quando seu estado mudar. Quando a entrada se torna ativa enquanto a sua área de detecção de intrusão está armada, o painel aciona um alarme. O Security Center usa este alarme para acionar um *Alarme de área de detecção de intrusão ativado*.

- Os painéis de intrusão são limitados na quantidade de eventos que podem reportar; eles também são limitados quanto à velocidade em que podem transmiti-los.
- Pode levar alguns minutos para receber as alterações aos estados das entradas no Security Center.
- Algumas das alterações aos estados das entradas podem não ser relatadas no Security Center mesmo que o painel acione alarmes de intrusão.

Sobre áreas de detecção de intrusão

É um tipo de entidade que corresponde a uma zona ou divisão (grupo de sensores) em um painel de invasão.

As áreas de detecção de intrusão podem ser criadas automaticamente pela função Intrusion Manager quando os painéis de intrusão em que elas estão configuradas estão inscritos em seu sistema.

As áreas de detecção de intrusão não são configuráveis na sua maior parte, exceto para as câmeras atribuídas a elas para fins de monitoramento no Security Desk e para *eventos causa-efeito*. Elas são atualizadas automaticamente quando as zonas correspondentes são atualizadas nos painéis de intrusão.

Os usuários podem realizar as seguintes ações nas áreas de detecção de intrusão:

NOTA: Você pode não ser capaz de executar algumas dessas ações, dependendo do tipo de painel de intrusão que você está usando.

- **Armação mestre:** O armamento mestre é armar uma área de detecção de intrusão de modo que todos os sensores atribuídos à área disparem o alarme se um deles for disparado. Alguns dos fabricantes chamam este modo de "Armação distante".
- **Armação do perímetro:** Ela arma uma área de detecção de invasão de um modo que somente os sensores atribuídos compensariam o alarme se um deles fosse disparado. Outros sensores, como o de movimento dentro da área, são ignorados.
- **Desarmar:** Desarma a área, fazendo com que todos os sensores atribuídos à área de detecção de intrusão selecionada sejam ignorados pelo painel de intrusão.
- **Aciona um alarme de intrusão:** Disparar um alarme de invasão na área de detecção de invasão selecionada.
- **Silenciar alarme:** Se houver um alarme ativo na área de detecção de intrusão selecionada, faz com que a sirene no painel de intrusão pare de soar. Dependendo do seu painel de intrusão e do tipo de alarme, clicar em **Silenciar alarme** também pode confirmar o alarme.
- **Confirmar recepção do alarme:** Reconhecer um alarme de intrusão na área de detecção de intrusão selecionada.

Criando áreas de detecção de intrusão

Se as áreas de detecção de intrusão não foram criadas automaticamente após a inscrição na unidade de detecção de intrusão, você deve criá-las manualmente, para que as áreas possam ser armadas, desarmadas e assim por diante.

Antes de iniciar

Adicione a unidade de detecção de intrusão para controlar as áreas.

Para criar uma área de detecção de intrusão.

1. Abra a tarefa **Detecção de intrusão**.
2. Clique em **Adicionar uma entidade** ( ) > **Mostrar todas** > **Área de detecção de intrusão**.
3. Na página **Informações básicas**, insira um nome e uma descrição para a área.
4. Selecione uma **Partição** da qual esta área seja membro e clique em **Próximo**.

   As partições determinam quais usuários do Security Center têm acesso a essa entidade. Somente usuários que sejam parte da partição poderão visualizar ou modificar a área de detecção de intrusão.
5. Na lista suspensa **Unidade de detecção de intrusão**, selecione a unidade de detecção de intrusão para controlar esta área.
6. Em **ID exclusiva da área de detecção de intrusão**, insira o ID ou o nome da área conforme configurado no painel de intrusão.
7. Clique em **Próximo** > **Criar** > **Fechar**.

Tópicos relacionados

Sobre áreas de detecção de intrusão na página 958

Mover unidades de detecção de intrusão para um Intrusion Manager diferente

Se você quiser que uma função Intrusion Manager diferente gerencie e controle uma unidade de detecção de intrusão, para balanceamento de carga ou outra finalidade, você pode mover a unidade para outro Intrusion Manager usando a ferramenta *Mover unidade*.

Antes de iniciar

- A função Intrusion Manager deve estar na mesma LAN que a unidade de detecção de intrusão que controla.
- Se a extensão da unidade não for criada automaticamente, você deve adicioná-la.
- Se o painel de intrusão estiver fisicamente conectado a uma porta serial no servidor que hospeda a função original, certifique-se de fazer o mesmo com o servidor que hospeda a nova função.

Mover unidades detecção de intrusão para um Intrusion Manager diferente .

1 Na página inicial, clique em **Ferramentas** > **Mover unidade**.
2 Na lista suspensa **Tipo de unidade**, selecione **Unidade de detecção de intrusão**.
3 Selecione os dados que deseja mover.
4 Em **Intrusion Manager**, selecione a nova função Intrusion Manager para controlar a unidade.
5 Clique em **Mover** > **Fechar**.

Tópicos relacionados

Abas de configuração do Intrusion Manager na página 1065

Referência do Config Tool

Esta parte inclui as seguintes chapters:

- "Tipos de entidade" na página 962
- "Tipos de função" na página 1042
- "Tarefas de administração" na página 1085
- "Eventos e ações" na página 1100

51

Tipos de entidade

Esta seção inclui os seguintes tópicos:

- "Abas de configuração comum" na página 964
- "Unidade de controle de acesso - HID - Aba Identidade" na página 967
- "Unidade de controle de acesso - HID - Aba Propriedades" na página 968
- "Unidade de controle de acesso - HID - Aba Sincronização" na página 969
- "Unidade de controle de acesso - HID - Aba Periféricos" na página 970
- "Unidade de controle de acesso - Synergis – Aba Identidade" na página 972
- "Unidade de controle de acesso - Synergis – Aba Propriedades" na página 973
- "Unidade de controle de acesso - Synergis – Aba Portal" na página 974
- "Unidade de controle de acesso - Synergis – Aba Hardware" na página 975
- "Unidade de controle de acesso - Synergis – Aba Sincronização" na página 976
- "Unidade de controle de acesso - Synergis - Aba Periféricos" na página 977
- "Regra de acesso - Aba Propriedades" na página 979
- "Abas Configuração de alarmes" na página 980
- "Monitor analógico - Aba Propriedades" na página 982
- "Abas de configuração de área" na página 984
- "Modelo de crachá - Aba Designer de crachás" na página 987
- "Câmera - Aba vídeo" na página 989
- "Câmera - Aba Gravação" na página 993
- "Câmera - Aba Detecção de movimento" na página 994
- "Câmera - Aba Cor" na página 996
- "Câmera - Aba Rastreamento visual" na página 997
- "Câmera - Aba hardware" na página 998
- "Sequência de câmeras - Aba Câmeras" na página 1001
- "Abas de configuração de titulares de cartão" na página 1002
- "Grupo de titulares de cartão - Aba Propriedades" na página 1003
- "Abas de configuração de credencial" na página 1004
- "Abas Configuração de portas" na página 1005
- "Abas de configuração de elevador" na página 1008
- "Abas de configuração de zonas de hardware" na página 1010
- "Abas de configuração de lista de procurados" na página 1011

- "Zona de E/S - Aba Propriedades" na página 1013
- "Área de detecção de intrusão - Aba Propriedades" na página 1014
- "Abas de configuração da unidade de detecção de intrusão" na página 1015
- "Unidade de LPR - Aba Propriedades" na página 1016
- "Abas de configuração de macro" na página 1017
- "Grupo de monitores - Aba Monitores" na página 1018
- "Rede - Aba Propriedades" na página 1019
- "Comportamento de saída - Aba Propriedades" na página 1020
- "Abas de configuração de regra de horas extras" na página 1021
- "Instalação de estacionamento - Aba Propriedades" na página 1022
- "Partição - Aba Propriedades" na página 1023
- "Genetec Patroller - Aba Propriedades" na página 1024
- "Autorização - Aba Propriedades" na página 1025
- "Abas de configuração de restrição de autorização" na página 1026
- "Agendamento - Aba Propriedades" na página 1027
- "Tarefa agendada - Aba Propriedades" na página 1028
- "Servidor - Aba Propriedades" na página 1029
- "Plug-in de Ladrilho - Aba Propriedades" na página 1030
- "Abas de configuração do usuário" na página 1031
- "Abas de configuração Grupo de usuários" na página 1034
- "Unidade de vídeo - Aba Identidade" na página 1036
- "Unidade de vídeo - Aba Propriedades" na página 1037
- "Unidade de vídeo - Aba Periféricos" na página 1039
- "Abas de configuração de zona virtual" na página 1041

Abas de configuração comum

Algumas das abas de configuração são comumente usadas pela maioria das entidades do Security Center.

Aba de Identidade

A aba **Identidade** fornece informações descritivas sobre a entidade, como seu nome, descrição, ID lógica e permite que você passe para a página de configuração de entidades relacionadas.

- **Tipo:** Tipo da entidade
- **Ícone:** O ícone atribuído à entidade para ajudar a identificar visualmente a entidade na exibição de área, aba Identidade, e assim por diante.

  Clique na lista suspensa do **ícone Alterar** para alterar as configurações do ícone:

  - Clique em **Procurar...** para navegar para ou selecionar seu próprio ícone personalizado favorito.
  - Clique em **Redefinir** para restaurar o ícone padrão.
- **Nome:** Nome da entidadeSecurity Center. É recomendado criar um nome único e descritivo para cada entidade. Em alguns casos, um nome padrão é criado, que pode ser alterado. Os nomes das entidades são editáveis, exceto nos seguintes casos:
  - **Entidades do servidor:** O nome da entidade corresponde ao nome da máquina e não pode ser alterado.
  - **Entidades confederadas:** O nome da entidade é definido no sistema original e não pode ser alterado na federação.
- **Descrição:** Informações opcionais sobre a entidade.
- **ID lógico:** Número exclusivo atribuído à entidade para identificar facilmente no sistema (principalmente para operações de teclados de CCTV).
- **Relacionamentos:**

  Lista de relações entre esta entidade e as outras no sistema.

  Você pode usar os botões de comando encontrados na parte inferior da lista para gerenciar a relação entre essa entidade e outras entidades no sistema.

  - Para adicionar um novo relacionamento, clique em .
  - Para remover um relacionamento, selecione uma entidade relacionada e clique em .
  - Para saltar para a página de configuração de uma entidade relacionada, selecione a entidade e clique em .
- **Informações específicas:** Certos tipos de entidade, como unidades de vídeo, podem mostrar informações adicionais nesta guia.

Aba câmeras

A aba **Câmeras** permite que você associe câmeras à entidade para que, quando seja visualizado no Security Desk, as câmeras sejam exibidas em vez do ícone da entidade.

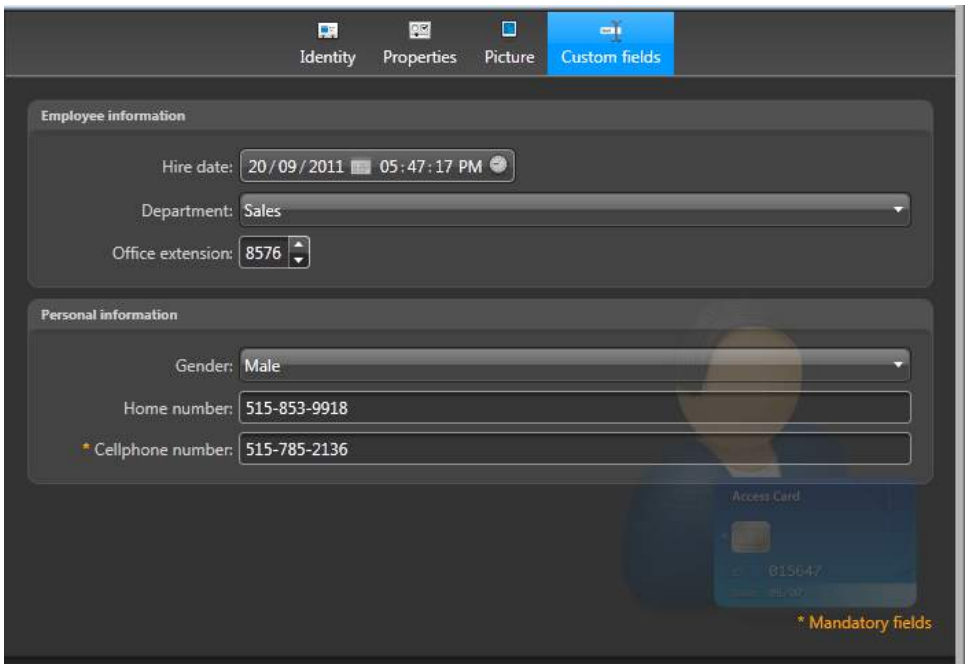
Nesta aba você pode executar as seguintes ações:

- Para adicionar uma nova câmera, clique em .
- Para remover a câmera selecionada, clique em .

Campos personalizados

A aba **Campos personalizados** permite visualizar e modificar os campos personalizados definidos para a entidade. A captura de tela de exemplo abaixo é a de uma entidade *titular de cartão*.

Esta aba só aparece quando os campos personalizados são criados para esse tipo de entidade.



No exemplo acima, cinco campos personalizados foram definidos para a entidade do titular de cartão, separados em dois grupos:

- Informações do funcionário
  - Data de contratação
  - Departamento
  - Ramal do escritório
- Informações pessoais
  - Sexo
  - Telefone residencial
  - Número do celular (identificado como obrigatório)

Aba da localização

A aba **Localização** fornece informações sobre fuso horário e localização geográfica da entidade. Isso não afeta a localização real das entidades em mapas.

- **Fuso horário:** O fuso horário é usado para exibir os eventos da entidade no fuso horário local da entidade. No Security Center, todos os horários são armazenados em UTC nos *bancos de dados*, mas são exibidos de acordo com o fuso horário local das entidades. A hora local da entidade é exibida abaixo da seleção do fuso horário.
- **Localização:** A localização geográfica (latitude e longitude) da entidade. Esta configuração de localização apenas é usada para os seguintes tipos de entidades:
  - Para unidades de vídeo, a localização é usada para o cálculo automático da hora em que o sol nasce e se põe em uma determinada data.

- Para Unidades de LPR fixas que não sejam equipadas com um receptor GPS, a localização geográfica é usada para traçar os eventos LPR (*leituras* e *ocorrências*) associados com a unidade de LPR no mapa no Security Desk.

Unidade de controle de acesso - HID - Aba Identidade

Esta seção lista as configurações encontradas na aba **Identidade** da unidade de controle de acesso HID, na tarefa *Controle de acesso*. Esta aba permite visualizar informações específicas do hardware, além das informações de entidade padrão (nome, descrição, ID lógica, etc.).

- **Fabricante:** Fabricante da unidade de controle de acesso.
- **Tipo de produto:** Modelo da unidade de controle de acesso.
- **Endereço MAC:** Endereço MAC da unidade de controle de acesso
- **Versão do firmware:** Versão de firmware atual instalada na unidade de controle de acesso.

  NOTA: O botão **Atualização** (☢) só aparece se for uma unidade HID EVO.
- **Proposta:** Exibe a versão de firmware recomendada. Se a versão de firmware for a mesma que a versão proposta, exibirá *Atualizado*.
- **Número de credenciais:** (Quando o **Modo seguro** está habilitado) Número de credenciais armazenadas na unidade.

  (Quando o **Modo seguro** está desabilitado) Número de credenciais armazenados na unidade comparado ao número total de credenciais que a unidade consegue armazenar, com base na memória disponível e na média de bytes por credencial.
- **Memória principal:** (Apenas quando o **Modo seguro** está desativado) Memória disponível na unidade.
- **Memória secundária:** (Apenas quando o **Modo seguro** está desativado) Memória secundária disponível na unidade (quando se aplicar).

Unidade de controle de acesso - HID - Aba Propriedades

Esta seção lista as configurações encontradas na aba **Propriedades** da unidade de controle de acesso HID, na tarefa *Controle de acesso*. Esta aba permite atualizar os parâmetros de conexão após a descoberta da unidade HID, como as credenciais de logon e o uso de determinadas entradas específicas.

Configurações de conexão

Esta seção mostra os parâmetros de conexão para o Access Manager se comunicar com a unidade. Essas configurações são inicializadas quando a unidade HID é adicionada ao seu sistema. Não altere essas configurações, a menos que você as tenha alterado na unidade através da página Web da unidade ou usando a GUI de Descoberta HID após a inscrição da unidade, ou um dos nossos representantes instruir você a fazê-lo.

- **Nome de usuário e senha:** Nome de usuário e senha usados para fazer logon à unidade HID.
- **Usar endereço de host traduzido:** Selecione essa opção quando houver um roteador NAT entre a unidade e seu Gerenciador de Acesso. O IP do roteador NAT que é visível da unidade seria definido aqui.
- **IP Estático:** Selecione esta opção e configure o endereço de IP, Gateway e máscara de sub-rede manualmente, caso a unidade HID use um endereço de IP fixo (recomendado).
- **Usar DHCP:** Selecione essa opção se a unidade HID será atribuída à sua configuração de IP por um servidor DHCP. Ao usar a opção DHCP, o servidor DHCP deve ser configurado para sempre atribuir o mesmo endereço de IP à unidade.

Configurações gerais

Esta seção exibe as configurações gerais da unidade HID.

- **Modo de servidor:** Esta opção sempre fica apagada porque as unidades HID não suportam o *modo de servidor*.
- **Modo seguro:** Ativar o modo seguro desativa os protocolos não seguros de FTP e Telnet. Ele também deixa a conexão entre o Access Manager e unidades HID menos suscetível a problemas de rede. Essa opção está disponível somente se a unidade HID atende aos requisitos de firmware para modo seguro.
- **Falha de AC do monitor :** Selecione esta opção, caso a entrada de *falha de AC* seja usada para monitorar as falhas de AC ou pra qualquer outro objetivo geral.
- **Falha da bateria do monitor :** Selecione esta opção, caso a entrada de *falha da bateria* seja usada para monitorar a bateria reserva ou pra qualquer outro objetivo geral.
- **Supervisão de leitor:** Selecione essa opção para habilitar a supervisão de leitor (habilitar para detectar a desconexão do leitor ou falta de energia no Security Desk e Config Tool). Para esse recurso funcionar, todos os leitores conectados a essa unidade HID devem ser configurados para supervisão. Também é necessário habilitar o modo de supervisão em cada leitor físico ao apresentar o cartão de configuração HID.
- **Tempo limite:** (Somente se a *Supervisão de leitor* for selecionada) Tempo limite usado para detectar que o leitor está conectado. É recomendado que seja definido um valor de tempo limite pelo menos três vezes o tempo de rotação do sinal *Estou aqui* (padrão=10 segundos) configurado no leitor.

Tópicos relacionados

Habilitar a supervisão de leitores no HID VertX na página 611

Unidade de controle de acesso - HID - Aba Sincronização

Esta seção lista as configurações encontradas na aba **Sincronização** da unidade de controle de acesso HID, na tarefa *Controle de acesso*. Esta aba permite configurar o tipo de sincronização que deseja entre a unidade e o Access Manager.

- **Última atualização:** Indica data e hora da última sincronização de sucesso com a unidade.
- **Próxima atualização:** Data e hora da próxima sincronização agendada com a unidade.
- **Configuração expira em:** Depende se regras de acesso temporário são usadas ou não.
  - Se nenhuma regra de acesso temporário é usada: Indica o dia e a hora em que a unidade não poderá mais funcionar completamente independente do Access Manager. Isso ocorre devido à capacidade limitada de agendamento da unidade de controle de acesso HID. É necessário sincronizar antes da data de vencimento para garantir que a unidade funcione adequadamente sozinha.
  - Suas regras de acesso temporário são usadas: Indica a data e hora que a próxima sincronização deve ocorrer baseado na regra de data de ativação e vencimento das regras de acesso temporário.

  CUIDADO: As unidades HID VertX expiram após um ano. Após a data de validade, a unidade para de funcionar adequadamente.
- **Sincronizar:** Clique nesse botão para enviar tudo que foi alterado desde a última sincronização à unidade. Essa operação pode causar uma curta interrupção se houver mudanças a agendamentos de destravamento de porta.
- **Sincronizar e reiniciar:** Clique nesse botão para enviar a configuração completa à unidade e reiniciar a unidade. Essa operação causará a interrupção do serviço.

Opções de sincronização

Você pode selecionar a frequência com que deseja que a sincronização da unidade ocorra.

- **Automaticamente:** Essa é a configuração recomendada.

  Qualquer alteração de configuração é enviada para a unidade de controle de acesso 15 segundos depois que a alteração é salva pelo Config Tool, Web Client ou Security Desk. Somente configurações que afetam aquela unidade específica são enviadas.
- **Diariamente:** A unidade é sincronizada diariamente, nas horas especificadas.
- **A cada:** A unidade é sincronizada semanalmente, no dia e horas especificadas.
- **Manual:** A unidade é sincronizada apenas quando você clica em **Sincronizar agora**.

  Certifique-se de sincronizar a unidade antes que a configuração expire.

Unidade de controle de acesso - HID - Aba Periféricos

Esta seção lista as configurações encontradas na aba **Periféricos** da unidade de controle de acesso HID, na tarefa *Controle de acesso* task. Nesta aba, você pode visualizar e alterar o nome e as configurações dos periféricos (leitores e dispositivos de E/S) controlados pela unidade.

As informações exibidas nesta página são:

- **Nome:** Nome do periférico ou módulo de interface. Os periféricos são exibidos em uma visualização hierárquica por padrão.

  Clique em **Modo de visualização** () para selecionar a *Visualização plana* se essa for sua preferência.

- **Tipo:** Tipo de periférico: *In* (Entrada), *Out* (Saída), *Leitor*. Em branco se não for um periférico.

  (Somente relés de saída) Clique em **Acionar saída** () na parte inferior da lista para enviar um comportamento de saída (*Ativo*, *Normal* ou *Pulso*) para o dispositivo selecionado.

- **Estado:** Estado do periférico ao vivo: *Ativo*, *Normal*, *Desabilitado* (somente entradas), *Problema* (somente entradas) ou *Desconhecido*.

  Use esta coluna para testar os módulos de interface conectados e validar a configurações de fiação dos dispositivos de E/S.

- **Informações adicionais:** Configurações específicas do tipo de periférico.

  Clique duas vezes em um periférico ou clique em **Editar** () na parte inferior da lista para editar as configurações do periférico selecionado.

- **Controle:** Entidade (porta, elevador, zona) controlada por este periférico.

  Clique em **Saltar para** () na parte inferior da lista para visualizar as abas de configuração da entidade controlada pelo periférico selecionado.

- **ID lógico:** (Oculta por padrão) ID lógico atribuída a este periférico para facilidade de referência em macros e programas do SDK.
- **Nome físico:** (Oculto por padrão) Nome estático atribuídos a este periférico pelo sistema.

DICA: As informações desta página também ficam disponíveis para os usuários do Security Desk através da tarefa *Status do sistema* ao monitorar periféricos.

Configurações editáveis de leitores

As configurações editáveis de leitores são:

- **Nome:** Nome do leitor.
- **ID lógico:** Deve ser único entre todos os periféricos anexados à mesma unidade.
- **Desabilitado:** Este recurso não é suportado por unidades HID.
- **Tipo de leitor:** Selecione um dos seguintes.
  - *Wiegand*
  - *Clock & Data*
  - *Wiegand (Dorado)*
  - *Clock & Data (Dorado)*

Descobrir interfaces

Se a unidade HID estiver operando com **Modo seguro** ativado, as novas interfaces que você associar à unidade não aparecerão automaticamente na aba **Periféricos** após reiniciar a unidade. Para exibi-las, clique

no botão **Descobrir interfaces** () na parte inferior da página. Note que clicar neste botão faz com que a unidade fique por momentos desativada.

Configurações editáveis de entradas

As configurações editáveis de entradas são:

- **Nome:** Nome do dispositivo de entrada.
- **ID lógico:** Deve ser único entre todos os periféricos anexados à mesma unidade.
- **Desabilitado:** Selecione esta opção para ignorar as entradas. Uma vez desabilitada, o estado da entrada permanece em *Normal*, independentemente de como você a acionar.
- **Filtrar variação:** O período de tempo que uma entrada pode estar em um estado alterado (por exemplo, alterado de *Ativo* para *Normal*) antes que a alteração do estado seja relatada. Esta opção filtra os sinais que estão instáveis.
- **Tipo de contato/predefinições:** Configure o estado normal do contato de entrada e seu modo de supervisão.
  - **Não supervisionado/Normalmente fechado:** O estado normal do contato de entrada é fechado e a unidade de controle de acesso não relata se a entrada estiver no estado de problema.
  - **Não supervisionado/Normalmente aberto:** O estado normal do contato de entrada é aberto e a unidade de controle de acesso não relata se a entrada estiver no estado de problema.
  - **Supervisionado em 4 estados/Normalmente fechado:** O estado normal do contato de entrada é fechado e a unidade de controle de acesso relata quando entrada está no estado de problema.
  - **Supervisionado em 4 estados/Normalmente aberto:** O estado normal do contato de entrada é aberto e a unidade de controle de acesso relata quando entrada está no estado de problema.
- **Tipo de contato/manual:** Configurações manuais. Permite definir seu intervalo personalizado de valores para estados de entrada *Ativo* e *Normal*.

Configurações editáveis de saídas

As configurações editáveis de saídas são:

- **Nome:** Nome do dispositivo de saída.
- **ID lógico:** Deve ser único entre todos os periféricos anexados à mesma unidade.
- **Tempo mínimo (Ação):** Se o relé estiver sendo usado como parte de uma zona (seja hardware ou virtual), estabeleça um número mínimo de segundos em que o relé fica fechado, quando acionado por um evento (por exemplo, *Solicitação de saída*).

Unidade de controle de acesso - Synergis™ – Aba Identidade

Esta seção lista as configurações encontradas na aba **Identidade** da unidade de controle de acesso Synergis™, na tarefa *Controle de acesso*. Esta aba permite visualizar informações específicas do hardware, além das informações de entidade padrão (nome, descrição, ID lógico etc.).

- **Fabricante:** Fabricante da unidade de controle de acesso.
- **Tipo de produto:** Modelo da unidade de controle de acesso.
- **Endereço MAC:** Endereço MAC da unidade de controle de acesso
- **Porta de descoberta:** Porta usada pelo Access Manager para conversar com essa unidade. Ela deve corresponder a uma das portas de descoberta configuradas para a extensão Genetec™ Synergis™ do Access Manager.
- **Versão do firmware:** Versão de firmware atual instalada na unidade de controle de acesso.
- **Número de titulares de cartão.:** Número de titulares de cartão (credenciais distintas) armazenadas na unidade.

Unidade de controle de acesso - Synergis™ – Aba Propriedades

Esta seção lista as configurações encontradas na aba **Propriedades** da unidade de controle de acesso Synergis™, na tarefa *Controle de acesso*. Esta aba permite atualizar os parâmetros de conexão após a descoberta da unidade Synergis™, como as respectivas credenciais de logon.

Configurações de conexão

As configurações de conexão são inicializadas quando a unidade Synergis™ é inscrita no seu sistema. Não altere essas configurações, a menos que você tenha alterado as configurações da unidade com o Synergis™ Appliance Portal após a inscrição da unidade ou um dos nossos representante tenha instruído você a fazê-lo.

- **Endereço da Web:** Endereço da web para contatar Synergis™ Appliance Portal.
- **Nome de usuário e senha:** Nome de usuário e senha de logon.
- **Usar DHCP:** Não altere este parâmetro, a menos que seja solicitado pelo representante local da Assistência Técnica da Genetec™. Este parâmetro é redefinido sempre que o Access Manager se reconecta à unidade Synergis™.
- **Ignorar o proxy da web:** Selecione essa opção para instruir o Access Manager a ignorar as configurações de Servidor de Proxy do servidor que é o host atual da função. Limpe essa opção para instruir o Access Manager a seguir as configurações do Servidor de Proxy (padrão=limpo).
- **Reiniciar certificado confiável:** (Habilitado somente quando a unidade está desligada) Clique nesse botão para fazer com que o Access Manager esqueça do certificado confiável para essa unidade e um novo possa ser aceito. Use esse recurso quando trocar o certificado digital da unidade após a inscrição.

Unidade de controle de acesso - Synergis™ – Aba Portal

Esta seção lista as configurações encontradas na aba **Portal** da unidade de controle de acesso Synergis™, na tarefa *Controle de acesso*. Esta aba abre uma janela para a interface baseada na web da unidade Synergis™ (Synergis™ Appliance Portal) que permite configurar e manter a unidade.

O Portal de Dispositivos Synergis™ permite que você execute as seguintes tarefas:

- Alterar a senha de segurança necessária para fazer logon na unidade Synergis™.
- Definir as configurações de rede na unidade Synergis™ para que ela funcione em seu sistema.
- Configurar a unidade Synergis™ para aceitar conexões de Access Managers específicos.
- Inscrever e configurar os módulos de interface acoplados à unidade Synergis™.

  NOTA: Existe uma exceção à regra. Os controladores Mercury (EP e M5-IC) devem ser inscritos e configurados a partir do Security Center do Config Tool na aba **Periféricos** da unidade de controle de acesso. Para obter mais informações, consulte o capítulo sobre controladores Mercury no *Guia de Integração do Synergis™ Softwire*.
- Configure o comportamento de controle de acesso da unidade Synergis™, tanto para operações online quanto offline.
- Visualize os registros de atividade armazenados na unidade Synergis™.
- Teste e diagnostique as conexões dos módulos de interface à unidade Synergis™.
- Visualize e exporte o status e a configuração da unidade Synergis™.
- Atualize o firmware da unidade Synergis™ (Synergis™ Softwire).
- Reinicie o hardware ou o software da unidade Synergis™.
- Atualize os níveis de certificado de segurança atribuídos a áreas do Security Center manualmente no aparelho quando a conexão com o Access Manager for perdida.

Tópicos relacionados

Unidade de controle de acesso - Synergis – Aba Hardware na página 975

Unidade de controle de acesso - Synergis™ – Aba Hardware

Esta seção lista as configurações encontradas na aba **Hardware** da unidade de controle de acesso Synergis™, na tarefa *Controle de acesso*. Esta aba só aparece se sua unidade estiver executando o Synergis™ Softwire versão 10.0 ou mais recente. Ela permite configurar os módulos de interface conectados à unidade Synergis™.

A unidade Synergis™ (Synergis™ Cloud Link ou Synergis™ Master Controller) suporta as seguintes integrações de hardware de terceiros:

- Travas Assa Abloy com Aperio.
- Travas IP Assa Abloy (PoE e sem fio).
- Controladores IP inteligentes Axis.
- Controladores DDS TPL e TPL-P4 RS-485 e IP.
- Travas sem fio Salto Sallis.
- Leitores de cartão inteligente STid.
- Módulos de interface HID VertX (V100, V200, V300).

Para obter mais informações sobre cada uma dessas integrações, consulte os respectivos *Guias de Integração do Synergis™ Softwire*.

Tópicos relacionados

Unidade de controle de acesso - Synergis – Aba Portal na página 974

Unidade de controle de acesso - Synergis™ – Aba Sincronização

Esta seção lista as configurações encontradas na aba **Sincronização** da unidade de controle de acesso Synergis™, na tarefa *Controle de acesso*. Esta aba permite acionar manualmente a sincronização entre a unidade e o respectivo Access Manager.

- **Última atualização:** Indica o dia e a hora da última sincronização bem-sucedida entre a unidade e o respectivo Access Manager.
- **Próxima atualização:** Não se aplica. As alterações que afetam a unidade Synergis™ são sempre enviadas automaticamente no momento em que são salvas.
- **A configuração expira em:** Os dados sincronizados da unidade Synergis™ nunca expiram porque ela entende o esquema de agendamento usado no Security Center.
- **Sincronizar:** Clique nesse botão para enviar tudo que foi alterado desde a última sincronização à unidade.

  Esta ação sempre executa uma sincronização completa. A sincronização de uma unidade Synergis™ não causa nenhuma interrupção do serviço.

Unidade de controle de acesso - Synergis™ - Aba Periféricos

Esta seção lista as configurações encontradas na aba **Periféricos** da unidade de controle de acesso Synergis™, na tarefa *Controle de acesso*. Esta aba exibe, em visualização hierárquica, todos os módulos de interface acoplados à unidade, juntamente com todos os painéis subordinados anexos a eles.

Na aba **Periféricos**, você pode adicionar e excluir módulos de interface e alterar o nome e as configurações dos periféricos (leitores e dispositivos de E/S) anexos à unidade.

As informações exibidas nesta página são:

- **Nome:** Nome do periférico ou módulo de interface. Os periféricos são exibidos em uma visualização hierárquica por padrão.

  Clique em **Modo de visualização** () para selecionar a *Visualização plana* se essa for sua preferência.

- **Tipo:** Tipo de periférico: *In* (Entrada), *Out* (Saída), *Leitor*. Em branco se não for um periférico.

  (Somente relés de saída) Clique em **Acionar saída** () na parte inferior da lista para enviar um comportamento de saída (*Ativo*, *Normal* ou *Pulso*) para o dispositivo selecionado.

- **Estado:** Estado do periférico ao vivo: *Ativo*, *Normal*, *Desabilitado* (somente entradas e leitores), *Problema* (somente entradas) ou *Desconhecido*.

  Use esta coluna para testar os módulos de interface conectados e validar a configurações de fiação dos dispositivos de E/S.

- **Informações adicionais:** Configurações específicas do tipo de periférico.

  Clique duas vezes em um periférico ou clique em **Editar** () na parte inferior da lista para editar as configurações do periférico selecionado.

- **Controle:** Entidade (porta, elevador, zona) controlada por este periférico.

  Clique em **Saltar para** () na parte inferior da lista para visualizar as abas de configuração da entidade controlada pelo periférico selecionado.

- **ID lógico:** (Oculta por padrão) ID lógico atribuída a este periférico para facilidade de referência em macros e programas do SDK.

- **Nome físico:** (Oculto por padrão) Nome estático atribuídos a este periférico pelo sistema.

DICA: As informações desta página também ficam disponíveis para os usuários do Security Desk através da tarefa *Status do sistema* ao monitorar periféricos.

Módulos de interface que você pode adicionar e excluir

Você só pode adicionar e excluir controladores Mercury (EP e M5-IC) conectados à sua unidade Synergis™ pela aba **Periféricos**. Para todos os outros tipos de módulos de interface, você deve adicioná-los através da aba **Hardware** ou pela página *Hardware* do Synergis™ Appliance Portal. Para mais informações, consulte o *Guia de Integração para Controladores Mercury Synergis™ Softwire*.

Configurações editáveis do leitor

As configurações editáveis do leitor são:

- **Nome:** Nome do leitor.
- **ID lógico:** Deve ser único entre todos os periféricos anexados à mesma unidade.
- **Desabilitado:** Selecione esta opção para ignorar as leituras.

Esta ação também pode ser emitida pelo Security Desk.

- **Tipo de leitor:** Selecione o tipo correspondente ao seu leitor. A lista de tipos de leitores disponíveis depende do tipo de módulo de interface que você possui. Selecionar o tipo de leitor *Personalizado* permite que você configure todas as opções do leitor manualmente.

Configurações editáveis de entrada

As configurações editáveis de entrada são:

- **Nome:** Nome do dispositivo de entrada.
- **Descrição:** (Somente leitura) Descrição da entrada.
- **ID lógico:** Deve ser único entre todos os periféricos anexados à mesma unidade.
- **Desabilitado:** Selecione esta opção para ignorar as entradas. Uma vez desabilitado, o estado da entrada permanece em *Normal*, independentemente de como você a acionar.
- **Filtrar variação:** O tempo que uma entrada pode estar em um estado alterado (por exemplo, alterado de *Ativo* para *Normal*) antes que a alteração do estado seja relatada. Esta opção filtra os sinais que são instáveis.
- **Tipo de contato:** Configura o estado normal do contato de entrada e seu modo de supervisão.
  - **Não supervisionado/Normalmente fechado:** O estado normal do contato de entrada é fechado e a unidade de controle de acesso não relata que a entrada está no estado de problema.
  - **Não supervisionado/Normalmente aberto:** O estado normal do contato de entrada é aberto e a unidade de controle de acesso não relata se a entrada estiver no estado de problema.
  - **Supervisionado em 4 estados/Normalmente fechado:** O estado normal do contato de entrada é fechado e a unidade de controle de acesso relata quando a entrada está no estado de problema.
  - **Supervisionado em 4 estados/Normalmente aberto:** O estado normal do contato de entrada é aberto e a unidade de controle de acesso relata quando a entrada está no estado de problema.
  - **Personalizar:** Permite definir seu intervalo personalizado de valores para estados de entrada *Ativo* e *Normal*. Os valores reais são definidos em Configurações avançadas do controlador Mercury.

Configurações editáveis de saída

As configurações editáveis do leitor são:

- **Nome:** Nome do dispositivo de saída.
- **ID lógico:** Deve ser único entre todos os periféricos anexados à mesma unidade.

Regra de acesso - Aba Propriedades

Esta seção lista as configurações encontradas na aba **Propriedades** da regra de acesso, na tarefa *Controle de acesso*.

Na aba *Propriedades*, você pode associar os 3 critérios de uma regra de acesso: “Quem”, “Quando” e “O quê”. Por exemplo, "Todos os funcionários", "Horário de expediente" e "Acesso concedido".

- **Cronograma:** Escolha quando essa regra de acesso estiver ativada.
- **Ativação:** (Apenas para regras acesso temporário) Data e hora de ativação ou quando a regra de agendamento de regra se aplicar.
- **Validade:** (Apenas para regras acesso temporário) Data e hora de vencimento ou quando a regra de agendamento deixar de se aplicar.
- **Quando o agendamento está ativo:** Selecione o que a regra faz (concede ou nega acesso a titulares de cartão) quando está ativada.
- **Titulares de cartão afetados por essa regra:** Selecione os titulares de cartão e grupos de titulares afetados por esta regra.

Abas Configuração de alarmes

Esta seção lista as configurações encontradas nas guias Configuração de alarmes, na tarefa *Alarme*.

Alarme - Aba propriedades

Na aba *Propriedades*, é possível definir as propriedades essenciais do alarme.

- **Prioridade:** Prioridade do alarme (1-255), baseado na urgência da situação. Os alarmes com prioridade mais altas são exibidos primeiro no Security Desk.
- **Destinatários:** Usuários, grupos de usuários e grupos de monitor analógico que são notificados quando ocorre o alarme e são responsáveis por responder à situação do alarme.
- **Modo de difusão:** Como os destinatários do alarme são notificados sobre o alarme.
  - **Todos ao mesmo tempo:** (Padrão) Todos os destinatários são notificados ao mesmo tempo, imediatamente após o alarme ser disparado.
  - **Sequencial:** Os destinatários são notificados individualmente, cada um após um atraso específico (em segundos) calculado a partir do momento que o alarme é disparado. Se o destinatário é um grupo de usuários, todos os membros do grupo serão notificados ao mesmo tempo.
- **Entidades anexas:** Entidades que ajudam a descrever a situação de alarme (por exemplo, câmeras, área, portas, procedimento de alarme, etc.). Quando o alarme é recebido em Security Desk, as entidades relacionadas podem ser exibidas uma depois da outra, em uma sequência, ou de uma vez, na *tela*, para ajudar a revisar a situação. Se uma entidade composta estiver anexada ao alarme, as entidades que a compõem também estão vinculadas ao alarme. Por exemplo, se uma entidade de porta estiver anexada ao alarme, as câmeras associadas à porta também estão.
- **Opções de exibição de vídeo:** Se as câmeras estiverem anexadas ao alarme, selecione se exibirá o vídeo ao vivo, reprodução, uma série de quadros estáticos ou uma combinação dos três quando o alarme for disparado.
  - **Ao vivo:** Exibir vídeo ao vivo.
  - **Reprodução:** Exibir reprodução de vídeo.
  - **Ao vivo e reprodução:** Alterna entre a exibição de vídeo ao vivo e a reprodução.
  - **Ao vivo e quadros estáticos:** Alterna entre a exibição de vídeo ao vivo e uma série de quadros estáticos.
  - **Quadros estáticos:** Exibe uma série de quadros estáticos.
- **Duração de quadros estáticos:** Selecione se deseja que cada quadro estático seja exibido pela mesma duração ou por um período independente de tempo.
  - **Mesmas durações:** Exibe cada quadro estáticos pela mesma quantidade de tempo.
    - **Número de quadros:** Selecione o número de quadros estáticos para exibir dentro de uma duração total do ciclo do conteúdo.
    - **Reproduzir:** Selecione quantos segundos antes de o alarme ter sido disparado para começar o primeiro quadro estático.
  - **Durações independentes:** Exiba cada quadro estático por uma duração de tempo independente.
    - **Tempo relativo:** Seleciona quantos segundos antes ou depois do alarme ser disparado, o quadro estático é exibido.
    - **Duração:** Seleciona por quanto tempo o quadro estático será exibido.

- **Ciclo de conteúdo:** Ative esta opção para alternar automaticamente as entidades anexas ao alarme em um ladrilho de exibição pela mesma quantidade de tempo. As entidades anexas estão listadas na ordem em que são exibidas no Security Desk.

Alarme - Aba avançado

Na aba *Configurações avançadas* , é possível configurar as propriedades de alarme opcionais.

- **Limiar de reativação:** O tempo mínimo que o Security Center precisa esperar depois de disparar o alarme antes de ser disparado novamente. Essa opção evita que o sistema fique disparando repetidamente o mesmo alarme antes que seja resolvido.
- **Procedimento de alarme (URL):** Entre a URL ou o endereço de página da Web correspondente ao *procedimento de alarme*, que oferece instruções de funcionamento do alarme aos operadores. A página da web é exibida quando o usuário clica em *Exibir procedimento de alarme* ( ) no widget de alarme no Security Desk.
- **Agendamento:** Defina quando esse alarme estará operando. Fora dos períodos definidos por esse agendamento, disparar esse alarme não tem nenhum efeito.

  NOTA: É possível adicionar múltiplos agendamentos ao alarme. Conflitos de agendamento que não possam ser resolvidos serão notificados.
- **Confirmação automática:** Ative essa opção para permitir que o sistema confirme automaticamente esse alarme se não for confirmado antes do tempo especificado (em segundos). Essa opção é recomendada para alarmes de baixa prioridade que servem para alertar o operador de segurança, mas não exige nenhuma ação. Quando esta opção está desativada, o sistema segue a opção **Confirmar alarmes automaticamente após** configurada no nível do sistema no Server Admin.

  NOTA: A confirmação automática não se aplica a alarmes que têm uma condição ativa anexa. Para confirmar esses alarmes, é necessário confirmá-los à força (o que exige o privilégio de *Confirmar alarmes à força*). Para obter mais informações sobre confirmação de alarmes, consulte o *Guia do Usuário do Security Desk*.
- **Criar um incidente da confirmação:** Ative essa opção para estimular o usuário Security Desk a relatar um *incidente* sempre que confirmar um alarme.

  NOTA: Ativar essa opção desliga a opção *confirmação automática*.
- **Gravação automática de vídeo:** Desative essa opção (padrão=ligado) se não desejar começar a gravar o vídeo quando o alarme é disparado.
- **Proteger vídeo gravado:** Ative essa opção (padrão=desligado) para proteger as gravações de vídeo associadas a esse alarme por um número específico de dias.
- **Som do alarme:** Selecione o trecho de som para reproduzir quando ocorre um novo alarme, se os alarmes estiverem configurados para tocar um som no Security Desk. Por padrão, o trecho de som configurado na caixa de diálogo do Security Desk *Opções* é usado.
- **Cor:** Selecione uma cor para o alarme. A cor é usada para a sobreposição do vídeo de alarme quando ele é exibido em um ladrilho na tarefa *Monitoramento de alarme* ou *Monitoramento*, bem como quando o alarme é acionado em um mapa.

Monitor analógico - Aba Propriedades

Esta seção lista as configurações encontradas na aba **Propriedades** de Monitor analógico, na tarefa *Vídeo*.

A aba *Propriedades* permite configurar o uso (ou função) da transmissão de vídeo e as configurações de rede específicas para o monitor analógico.

Vídeo

Na seção *Vídeo*, você pode definir as configurações que afetam a qualidade do vídeo.

- **Uso do stream:** Selecione o stream de vídeo para usar para câmeras exibidas no monitor analógico. Essa opção está disponível somente para os decodificadores capazes de gerar vários fluxos de vídeo. As opções de uso do stream são:
- **Ao vivo:** Transmissão padrão para ver vídeos ao vivo no Security Desk.
- **Gravando:** Stream gravado pelo Archiver para futura investigação.
- **Remoto:** Stream utilizado para ver vídeos quando a largura de banda de internet é limitada.
- **Baixa resolução:** Transmissão utilizada em vez da transmissão *Ao vivo* quando o ladrilho utilizado para visualizar a transmissão no Security Desk é pequeno.
- **Alta resolução:** Transmissão utilizada em vez da transmissão *Ao vivo* quando o ladrilho utilizado para visualizar a transmissão no Security Desk é grande.
- **Formato analógico:** Selecione o formato analógico NTSC (National Television System Committee) ou PAL (Phase Alternating Line) para o sinal de vídeo. O formato PAL geralmente transmite vídeo a uma velocidade de quadro mais baixa, mas com maior resolução.
- **Exibir nome da câmera:** Ative esta opção se desejar que o nome da câmera seja exibido quando ela for exibida no monitor analógico em um ladrilho do Security Desk.

Configurações de rede

Na seção *Configurações de rede*, você pode configurar o tipo de conexão usado pelo decodificador de vídeo.

- **Porta UDP:** Número da porta usada quando o tipo de conexão é *UDP* unicast. Se o codificador suportar múltiplos streams de vídeos, este parâmetro é diferente para cada stream.
- **Tipo de conexão:** Define como a comunicação é estabelecida entre o Archiver e a unidade para enviar ou receber fluxos de vídeo. Cada dispositivo na mesma unidade pode suportar diferentes tipos de conexão.
- **Melhor disponível:** Permite que o Archiver selecione o melhor tipo de conexão disponível para o stream. Os melhores tipos disponíveis são classificados nesta ordem, de acordo com a disponibilidade: *Multicast*, *UDP* e *TCP*. Quando o fluxo é solicitado apenas para gravação, o multicast é removido da lista, então os melhores tipos disponíveis começam com o UDP.
  - **Multicast:** Comunicação entre um único transmissor e vários receptores em uma rede. Esse é o tipo de conexão preferencial. Neste modo, vários usuários em vários locais podem receber a mesma transmissão de vídeo simultaneamente de uma mesma fonte, usando a largura de banda apenas uma vez. A maioria das unidades de vídeo são capazes de transmissões multicast.
  - **UDP:** Força o stream a ser enviado em UDP para o Archiver. O stream deve ser formatado usando o protocolo RTP.
  - **TCP:** Força o envio da transmissão em *TCP* para o Archiver. Aqui, TCP é considerado no sentido amplo. Para alguns tipos de câmeras, o Archiver estabelece uma conexão TCP com a unidade e recebe a transmissão em um protocolo exclusivo. Para outros, o stream é enviado sobre HTTP. Tipicamente, a transmissão não é formatada de acordo com o protocolo RTP pela unidade. O Archiver precisa converter o stream para o protocolo RTP para ser arquivada ou retransmitida ao sistema.

Ferragem

Na seção *Hardware*, você pode associar outros dispositivos de hardware (motor PTZ, alto-falante, microfone e assim por diante) a este monitor analógico. Quando o decodificador é adicionado ao sistema, todos os dispositivos de hardware pertencentes à mesma unidade são configurados por padrão. Você pode associar manualmente o monitor analógico a outros dispositivos, de acordo com a forma como eles estão fisicamente conectados.

Abas de configuração de área

Esta seção lista as configurações encontradas nas guias de configuração de Área, na tarefa *Exibição de área*.

Área - Aba Identidade

Na aba *Identidade*, você configura a finalidade da área (seja ou não usada para controle de acesso), além das informações de entidade padrão (nome, descrição, ID lógico etc.).

- **Controle de acesso:** Defina como **Ligado** para mostrar as abas de configuração *Propriedades* e *Avançado*.

  NOTA: Esta opção só é visível quando o Synergis™ está ativado como recurso.

Área - Aba Propriedades

Na aba *Propriedades*, você define quem tem acesso à área e através de suas portas perimetrais.

NOTA: Esta aba só está visível quando o Synergis™ está habilitado como recurso e *Controle de acesso* está definido como **Ligado** na aba *Identidade* da área.

- **Regras de acesso:** Define quem tem acesso à área e quando. Cada regra pode ser aplicada em um ou ambos os lados das portas.
  - **Regras de acesso:** Adiciona regras de acesso para conceder (ou negar) acesso (entrada, saída ou ambos) à área aos titulares de cartões e grupos de titulares de cartões com base em um cronograma.
  - **Titulares de cartão, grupos de titulares de cartão:** Adiciona titulares de cartões e grupos de titulares de cartões para definir quem tem acesso à área em todos os momentos.
    NOTA: Apenas conceda acesso diretamente aos titulares de cartões para situações temporárias ou exceções. Se um grupo de titulares de cartão deve ter acesso à área em todos os momentos enquanto configuração regular, defina uma regra de acesso com a agenda *Sempre*.
- **Portas:** Defina as portas de *Perímetro* e *Cativas* da área. As portas de perímetro são usadas para entrar e sair de uma área e ajudar a controlar o acesso. Portas cativas são portas dentro da área. Ao ajustar corretamente os lados das portas, as contagens de pessoas e anti-passback são devidamente rastreadas. Os lados de Entrada e Saída de uma porta são relativos à área sendo configurada.

  NOTA: As regras de acesso atribuídas à área se aplicam a todas as portas de perímetro da área. Se cada porta de perímetro dever ser governada por seu próprio conjunto de regras, configure as regras de acesso para cada porta.

Área - Aba Avançado

Na aba *Avançado*, você define os comportamentos avançados de controle de acesso para a área.

NOTA: Esta aba só está visível quando o Synergis™ está habilitado na sua licença e *Controle de acesso* está definido como **Ligado** na aba *Identidade* da área. Além disso, algumas dessas propriedades podem não ser visíveis, dependendo das opções de sua licença.

- **Anti-passback:** O anti-passback é a restrição de acesso colocada em uma área protegida que evita que um titular de cartão entre em uma área de onde ainda não saiu e vice-versa.
  - **Status:** Ativar ou desativar o recurso anti-passback.
  - **Cronograma:** Selecione *Sempre* se quiser que o anti-passback seja aplicado sempre.
  - **Tipo:** Tipo de antirretorno para aplicar.
    - **Virtual:** O antirretorno lógico apenas registra os eventos de antirretorno no banco de dados. Ele não impede a porta de ser desbloqueada devido a um evento de antirretorno.

    - **Física:** O antirretorno físico registra uma entrada no banco de dados e impede a porta de ser desbloqueada devido a um evento de antirretorno.
  - **Tempo limite de presença:** Configura por quantos minutos a presença de um titular de cartão na área é lembrada para fins de detecção de retorno (não é usado para contar pessoas). Depois desse período, um titular de cartão que nunca tenha deixado a área pode entrar novamente sem disparar um evento de retorno. O valor padrão de zero (0) minutos significa que a presença de um titular de cartão nunca tem o limite de tempo esgotado.
    NOTA: Quando o antirretorno global está ativado, a presença de um titular de cartão em uma área é esquecida após sete dias se nenhuma entrada ou saída dessa área é registrada para esse titular do cartão durante esse período. Isso significa que titulares de cartão podem entrar novamente em uma área da qual nunca saíram ou deixar uma área em que nunca entraram sem disparar um evento de retorno se nenhum movimento tiver sido registrado para esses titulares naquela área por sete dias. Isso se aplica mesmo que o **Tempo limite de presença** esteja definido como infinito (=0).
  - **Estrita:** Ative esta opção para gerar eventos de passback para ambos os tipos de violação de acesso: quando titulares de cartão tentarem entrar novamente em uma área da qual saíram e quando tentarem sai de uma área em que nunca entraram. Caso contrário, o padrão é definido como **Desligado** e a lógica de anti-passback é somente verificada em entradas de áreas, e os eventos de passback são somente gerados quando os titulares de cartão tentam entrar novamente em uma área da qual nunca saíram.
    MELHOR PRÁTICA: Se você optar por ativar o anti-passback *estrito* e *físico* em uma área que não seja controlada com catracas ou dispositivos similares que apenas permitam entrar uma pessoa por vez, conceda o privilégio *Perdoar violação de anti-passback* a operadores responsáveis por monitorar essa área.
    NOTA: Com o anti-passback estrito desligado, você pode ter portas de perímetro Card-In/REX-out, mas o parâmetro **Tempo limite de presença** precisa ser configurado (> 0). Com o anti-passbacl estrito ligado, todas as portas de perímetro precisam ser configuradas como Card-In/Card-Out, o **Tempo limite de presença** deve ser configurado como infinito (= 0) e nenhum REX pode ser configurado.
- **Ocupação máxima:** O recurso *Ocupação máxima* monitora o número de pessoas em uma área, até um limite configurado. Uma vez atingido o limite, a regra negará acesso a mais titulares de cartão (se definida para *Rígido*) ou acionará eventos embora permita outros acessos (*Leve*) .
  - **Status:** Definir para **ATIVO** para habilitar o recurso de ocupação máxima. Habilitar um limite de *Ocupação máxima* em uma área gera os seguintes eventos:
    - *Ocupação máxima alcançada* quando a área alcança o limite configurado. Esse evento coloca a área em estado de alerta.
    - *Ocupação máxima excedida* quando titulares de cartão adicionais entram na área
    - *Abaixo da capacidade máxima* quando o número de ocupantes fica abaixo do limite configurado.
  - **Tipo:** Selecione entre as seguintes opções:
    - *Pesado*: Quando a o limite de ocupação máxima é alcançado, irá negar solicitação de acesso na área porta do perímetro.
    - *Leve*: Não irá negar solicitações de acesso subsequentes.
  - **Limite de ocupação máxima:** Digite o número de pessoas que a área pode suportar antes de disparar o limite.
- **Intertravamento:** O Security Center suporta o bloqueio das portas perimetrais de uma área permitindo que apenas uma porta perimetral seja aberta ao mesmo tempo.
  - **Status:** Ativar ou desativar o recurso de intertravamento. Quando este recurso está ligado, somente uma porta de perímetro da área pode estar aberta a qualquer momento. Para abrir uma porta, todas as outras devem estar fechadas.

  - **Prioridade:** Quando ambas as entradas de *sobrescrita* e *travamento* estiverem configuradas, selecione qual tem a prioridade quando ambas as entradas estiverem ativas.
  - **Substituir:** Selecione a entrada que está ligada à tecla ou chave de acionamento de *sobrescrita*. Quando a chave está ligada, o recurso de intertravamento fica desativado.
  - **Trancamento:** Selecione a entrada que está ligada à tecla ou chave de acionamento de *travamento*. Quando a chave está ativada, todas as portas do perímetro permanecem trancadas até a chave voltar à sua posição normal.
- **Regra de primeira pessoa a entrar:** A regra de *primeira pessoa a entrar* é a restrição de acesso aplicada a uma área protegida que impede alguém de entrar na área, a não ser que um titular de cartão de supervisão esteja no local. A regra de primeira pessoa a entrar pode ser imposta em *agendas de desbloqueio* de portas, *regras de acesso* ou ambas.
  - **Impor agendamentos de destrancar portas:** Defina como **Ligado** para ignorar todas as agendas de desbloqueio de portas até que um supervisor tenha acesso à área. A regra de primeira pessoa não tem efeito nos horários de desbloqueio de elevador.
  - **Impor regras de acesso:** Defina como **Ligado** para ignorar regras de acesso até que um supervisor esteja presente na área. Você especifica quando a regra da primeira pessoa se aplica com um cronograma.
  - **Supervisores:** Lista de titulares de cartões que podem atuar como supervisores de área.
  - **Lista de isenções:** Lista de titulares de cartões que continuam a seguir as regras de acesso mesmo quando a regra da primeira pessoa está em vigor.
- **Regra de acompanhante de visitante:** Com o anti-passback estrito desligado, você pode ter portas de perímetro Card-In/REX-out, mas o Tempo limite de presença precisa ser configurado (> 0). Com o anti-passback estrito ligado, todas as portas de perímetro precisam ser configuradas como Card-In/Card-Out e nenhum REX ou tempo limite pode ser configurado.

  NOTA: Os hosts efetivos são configurados na tarefa *Gerenciamento de visitantes*. O atraso máximo concedido ao host para apresentar suas credenciais depois que o visitante apresentou a dele é configurado individualmente para cada porta.
  - **Fiscalizar regra de acompanhante de visitante:** Defina como **Ligado** para exigir que o host apresente sua credencial após o visitante, se o visitante tiver um host obrigatório atribuído.
- **PIN de dureza:** A função *PIN de coerção* permite que um titular de cartão que esteja sendo coagido a desbloquear uma porta acione um evento de *PIN de coerção digitado* sem alertar o intruso, ajudando assim a garantir a segurança do titular de cartão.

Área - Aba Ameaças

Na aba *Ameaças*, você configura ações específicas a serem executadas pelo sistema quando um nível de ameaça é ativado ou desativado para esta área.

NOTA: Esta aba só fica visível quando a opção de licença *Nível de ameaça* está ativada e pelo menos um nível de ameaça está configurado no seu sistema.

Modelo de crachá - Aba Designer de crachás

Esta seção lista as configurações encontradas na aba **Designer de crachás** do Modelo de crachá, na tarefa *Controle de acesso*.

Na aba *Designer de crachás*, você pode desenhar e modificar modelos de crachás. No Criador de crachá há diferentes ferramentas que você pode usar para editar um modelo.

- **Ferramentas:** Na seção *Ferramentas*, há seis ferramentas gráficas que você pode usar para editar o modelo:
  - **Ferramenta de seleção:** Use para clicar e selecionar um objeto no modelo.
  - **Ferramenta retângulo:** Use para desenhar um quadrado/retângulo no modelo.
  - **Ferramenta elipse:** Use para desenhar círculos/ovais no modelo.
  - **Ferramenta de texto:** Use para inserir texto no modelo.
  - **Ferramenta de imagem:** Use para inserir uma figura no modelo.
  - **Ferramenta de código de barras:** Use para inserir códigos de barras no modelo.
- **Imagem:** Neste widget, selecione se a Origem da imagem exibida no crachá usa uma imagem do titular do cartão ou uma imagem de um arquivo e se a imagem deve ser esticada ou não.
- **Texto:** Neste widget, você pode adicionar campos do titular do cartão, bem como editar o texto, a cor do texto e o alinhamento do texto.
- **Cor e borda:** Neste widget, as seguintes opções estão disponíveis:
  - **Preencher:** Use para modificar a cor de preenchimento de um objeto inserido, como um quadrado ou um oval.
  - **Opacidade:** Use para modificar a opacidade de um objeto inserido, como um quadrado ou um oval.
  - **Borda:** Use para modificar a cor da borda de um objeto inserido, como um quadrado ou um oval.
  - **Espessura da borda:** Use para modificar a espessura da borda do objeto inserido.
- **Tamanho e posição:** Neste widget, você pode selecionar onde o texto ou imagem estão localizados no crachá, e sua largura e altura.
- **Propriedades ( ):** Abre a caixa de diálogo *Formato*, onde você pode selecionar os seguintes tamanhos de cartão e orientações.
  - CR70
  - CR80
  - CR90
  - CR100
  - Tamanho personalizado de cartão
  - Orientação. Você pode escolher a orientação *Paisagem* ou *Retrato*.
- **Importar ( ):** Importa um design de crachá que foi exportado anteriormente do Config Tool como um modelo de crachá (somente formatos BDG).
- **Exportar ( ):** Salva o modelo de crachá atual em um arquivo BDG para que ele possa ser importado para outro sistema.
- **Recortar ( ):** Exclui o item selecionado no modelo de crachá.
- **Copiar ( ):** Copia o item selecionado do modelo de crachá.
- **Colar ( ) :** Cola o item selecionado no modelo de crachá.

- **Enviar para trás ( ):** Envie o item selecionado para o fundo do modelo de crachá. Esta opção é útil se desejar ter uma imagem de fundo no crachá.
- **Trazer para a frente ( ):** Leva o item selecionado para o primeiro plano do modelo de crachá.

Câmera - Aba vídeo

Esta seção lista as configurações encontradas na aba **Vídeo** da câmera, na tarefa *Vídeo*.

A aba *Vídeo* permite que você defina várias configurações de qualidade de vídeo (resolução, taxa de quadros e assim por diante) para cada *transmissão*de vídeo gerada pelo codificador de vídeo. Para cada fluxo, você também pode especificar seu uso (ou função) e configurações de rede específicas.

Qualidade do vídeo

Na seção *Qualidade do vídeo*, você pode definir configurações que afetam a qualidade do vídeo (resolução de imagem, taxa de bits, taxa de quadros e assim por diante). Várias configurações de qualidade de vídeo podem ser definidas para o mesmo fluxo em horários diferentes.

As configurações de qualidade de vídeo podem variar de um fabricante para outro. Nenhum fabricante suporta todas elas.

NOTA: Para qualquer configuração não coberta na lista abaixo, consulte a documentação do fabricante.

- **Resolução:** Formato de dados e resolução de imagem. As opções disponíveis dependem do tipo de unidade de vídeo que você possui.

  NOTA: Em certos modelos de unidades de vídeo que suportam um grande número de feeds de vídeo (4 a 12), alguns formatos de alta resolução podem ser desativados se você habilitar todos os fluxos de vídeo, pois a unidade não pode lidar com todos os fluxos em altas resoluções.
- **Qualidade:** A qualidade de vídeo depende de uma combinação de configurações. Config Tool propõe uma lista de configurações predefinidas para você escolher. Para ajustar cada uma delas individualmente, selecione *Personalizada* na lista suspensa *Qualidade*.
- **Taxa de transferência de bits:** Define a largura de banda máxima (kbps) permitida para este codificador.
- **Modo da taxa de transferência de bits:** Certos tipos de unidades de vídeo (como a Axis) permitem que você defina a taxa de bits máxima no nível da unidade. Neste caso, a lista suspensa *Modo de taxa de bits* fica disponível para suas configurações de taxa de bits.
  - **Variável:** A taxa de bits variável (VBR) ajusta a taxa de bits de acordo com a complexidade das imagens no vídeo. Isso usa muita largura de banda quando há muita atividade na imagem e menos largura de banda quando a área monitorada é tranquila.
  - **Constante:** A taxa de bits constante (CBR) permite que você defina uma taxa de bits alvo fixa que consumirá uma quantidade previsível de largura de banda que não irá mudar, seja o que for que ocorra na imagem. Isso requer que você defina outro parâmetro, a *Prioridade de taxa de bits*.
- **Prioridade de taxa de bits:** Se você optar por manter uma taxa de bits constante, o codificador pode não ser capaz de manter a taxa de quadros e a qualidade da imagem em seus valores definidos quando a atividade na imagem aumenta. A *Prioridade da taxa de bits* permite configurar o aspecto da qualidade de vídeo que deseja favorecer quando for forçado a fazer uma escolha.
  - **Taxa de quadros:** Mantém a taxa de quadros à custa da qualidade da imagem.
  - **Qualidade da imagem:** Mantém a qualidade da imagem à custa da taxa de quadros.
  - **Nenhuma:** Reduz a taxa de quadros e a qualidade da imagem para manter a taxa de bits.
- **Taxa de quadros:** Define o número de *quadros* por segundo (fps). Uma taxa de quadros alta (10 fps ou mais) produz vídeo fluido e é essencial para *detecção de movimentos* precisa. No entanto, aumentar a taxa de quadros também envia mais informações sobre a rede e, portanto, requer mais largura de banda.
- **Qualidade da imagem:** Define a qualidade da imagem (quanto maior o valor, melhor a qualidade). Uma qualidade de imagem maior requer mais largura de banda, o que pode comprometer a taxa de quadros.

  Quando a largura de banda é limitada, você deve considerar o seguinte:

- Para manter uma qualidade de imagem muito boa, restrinja o número de imagens por segundo (taxa de quadros mais baixa).

- Para transmitir mais imagens por segundo a uma taxa de quadros alta, reduza a qualidade da imagem.

O codificador tenta manter cada configuração de qualidade. No entanto, se a largura de banda for limitada, o codificador pode reduzir a taxa de quadros em favor da qualidade da imagem.

- **Configurações automáticas:** Alguns modelos de codificadores (como o Bosch) permitem selecionar esta opção em vez de definir seu próprio valor para a qualidade da imagem. Para definir a qualidade da imagem manualmente, você deve selecionar *Personalizado* na lista suspensa *Qualidade*.
- **Intervalo do quadro-chave:** Um *quadro-chave* é um quadro que contém uma imagem completa em si mesma ao contrário de um quadro usual que apenas possui informações que se alteraram em relação ao quadro anterior. Se a sua rede for menos confiável, você precisa de uma taxa de quadros mais alta para se recuperar mais rapidamente dos erros cumulativos no vídeo. Quadros-chave frequentes requerem maior largura de banda. Você pode especificar o intervalo de quadros-chave em segundos (1 a 20) ou por quadros (com base na taxa de quadros).
- **Velocidade de quadro de gravação:** Grava o vídeo em uma taxa de quadros inferior à da taxa usada para visualizar o vídeo. Essa configuração economiza espaço de armazenamento, mas não reduz o uso da largura de banda. Definir a *Taxa de quadros de gravação* para qualquer coisa diferente de *Todos os quadros* bloqueia o *Intervalo de quadros-chave*.
- **Perfil e nível:** Usado apenas para transmissões em *MPEG-4*, o perfil determina as ferramentas disponíveis ao gerar a transmissão (por exemplo, entrelaçamentos ou quadros B) e o nível limita o uso do recurso (por exemplo, taxa de bits máxima).
- **Tipo de objeto de vídeo:** O Tipo de Objeto de Vídeo (VOT) para usar para fluxos MPEG-4. As opções disponíveis são regidas pela escolha de *Perfil e nível*.
- **Estrutura do GOP:** Significa estrutura do *Grupo da Imagem*. É possível configurar até quatro tipos de estruturas do GOP:
  - **I:** Significa estrutura de quadros *Intra*. Significa que somente os quadros Intra (quadros-chave) são enviados. Isto serve principalmente para usar um multiplexador externo.
  - **IP:** Significa estrutura de quadros *Intra e Prevista*. Esta configuração resulta no menor atraso de vídeo possível.
  - **IPB:** Significa estrutura de quadros *Intra e Prevista e Bidirecional*. Esta configuração permite ao usuário ter uma qualidade superior e um atraso maior.
  - **IPBB:** Significa estrutura de quadros *Intra e Prevista e Bidirecional e Bidirecional*. Esta configuração permite ao usuário ter uma qualidade e um atraso ainda maiores.
- **Comprimento do GOP:** Significa comprimento do *Grupo da Imagem*. Com esse valor, é possível alterar a *distância* (número de quadros) entre os *quadros intra* na transmissão de vídeo em MPEG-2.
- **Tipo de fluxo:** Selecione entre VES (fluxo elementar de vídeo), que envia apenas informações de vídeo, ou PRG (fluxo de programa), que envia informações de vídeo e áudio.
- **Modo do filtro de entrada:** Permite selecionar um filtro de ruído para aplicar ao sinal de vídeo antes de ser codificado. Possui quatro configurações: *Nenhum*, *Baixo*, *Médio* e *Alto*.

  NOTA: A remoção de ruído do sinal de vídeo também reduz a nitidez da imagem. Se o sinal de vídeo estiver relativamente limpo, não aplique nenhum filtro (*Nenhum*). Quanto maior o nível de filtro, mais a imagem de vídeo fica desfocada. Manter uma imagem nítida cria mais pixels para codificar, o que usa mais largura de banda. É por isso que em algumas unidades de vídeo o padrão está configurado como *Médio*.
- **Controle da taxa de transferência de bits:** Permite que o codificador reduza automaticamente a *taxa de bits* quando um dos descodificadores está reportando erros de transmissão (pacotes descartados). Isso geralmente acontece quando há muito movimento na câmera. O codificador reduz a taxa de bits tão

baixo quanto necessário para permitir que todos os decodificadores recebam uma transmissão livre de erros. Quando o movimento diminui, o codificador aumenta gradualmente a taxa de bits até atingir o limite máximo configurado. A troca entre baixa taxa de bits e erros de transmissão é que com uma taxa de bits baixa, a imagem permanece nítida, mas o vídeo pode aparecer agitado, enquanto com erros de transmissão a imagem contém ruídos, mas o vídeo permanece fluido.

- **Modo de compressão:** Selecione entre SM4, a versão proprietária da compressão MPEG-4 da Verint ou ISO, a compressão MPEG-4 padrão.

Uso do stream

As opções de *Uso do stream* estão disponíveis somente para os decodificadores capazes de gerar várias transmissões de vídeo. Isso permite que você especifique o uso (ou função) de cada fluxo.

- **Ao vivo:** Transmissão padrão para ver vídeos ao vivo no Security Desk.
- **Gravando:** Stream gravado pelo Archiver para futura investigação.
- **Remoto:** Stream utilizado para ver vídeos quando a largura de banda de internet é limitada.
- **Baixa resolução:** Transmissão utilizada em vez da transmissão *Ao vivo* quando o ladrilho utilizado para visualizar a transmissão no Security Desk é pequeno.
- **Alta resolução:** Transmissão utilizada em vez da transmissão *Ao vivo* quando o ladrilho utilizado para visualizar a transmissão no Security Desk é grande.

Configurações de rede

As opções de *Configurações de rede* permitem configurar o tipo de conexão usada pelo codificador de vídeo.

- **Porta UDP:** Número da porta usada quando o tipo de conexão é *UDP* unicast. Se o codificador suportar múltiplos streams de vídeos, este parâmetro é diferente para cada stream.
- **Tipo de conexão:** Define como a comunicação é estabelecida entre o Archiver e a câmera para enviar ou receber fluxos de vídeo.
  - **Melhor disponível:** Permite que o Archiver selecione o melhor tipo de conexão disponível para o stream. Os melhores tipos disponíveis são classificados nesta ordem, de acordo com a disponibilidade: *Multicast*, *UDP*, *TCP*, *RTSP sobre HTTP* e *RTSP sobre TCP*.
  - **UDP Unicast:** Força o stream a ser enviado em UDP para o Archiver. O stream deve ser formatado usando o protocolo RTP.
  - **TCP Unicast:** Força o envio da transmissão em *TCP* para o Archiver. Aqui, TCP é considerado no sentido amplo. Para alguns tipos de câmeras, o Archiver estabelece uma conexão TCP com a unidade e recebe a transmissão em um protocolo exclusivo. Para outros, o stream é enviado sobre HTTP. Tipicamente, a transmissão não é formatada de acordo com o protocolo RTP pela unidade. O Archiver precisa converter o stream para o protocolo RTP para ser arquivada ou retransmitida ao sistema.
  - **Fluxo RTSP sobre HTTP:** Este é um caso especial de conexão TCP. O Archiver usa o protocolo RTSP para solicitar o stream por um túnel HTTP. O stream é enviado de volta por esse túnel usando o protocolo RTP. Este tipo de conexão é usado para minimizar o número de portas necessárias para se comunicar com uma unidade. Normalmente, esse é o melhor modo de solicitar o stream quando a unidade está por trás de um NAT ou firewall, pois as solicitações enviadas a portas HTTP são facilmente redirecionadas por eles.
  - **Fluxo RTSP sobre TCP:** Este é outro caso especial de conexão TCP. O Archiver usa o protocolo RTSP para solicitar o stream em TCP. A solicitação é enviada à porta RTSP da unidade.
  - **Igual ao da unidade:** Caso especial para unidades Panasonic. O tipo de conexão é o mesmo para todos os fluxos da unidade. Quando presente, é o único tipo de conexão suportado. O tipo de conexão real deve ser configurado na página de configuração específica da unidade.
- **Endereço multicast:** O endereço *multicast*e o *número da porta* são atribuídos automaticamente pelo sistema quando a unidade de vídeo é descoberta. Cada codificador de vídeo recebe um endereço

multicast diferente com um número de porta fixa. Se o codificador for capaz de gerar múltiplos fluxos de vídeo, um endereço multicast deve ser atribuído a cada fluxo. Esta é a configuração mais eficiente.

Melhorar a qualidade na gravação manual

Aumenta temporariamente a qualidade de vídeo quando a gravação é iniciada manualmente por um usuário do Security Desk ao clicar no botão *Gravar* (⚫) ou no botão *Adicionar marcador* (). Esta opção está disponível somente para o fluxo de gravação.

Melhorar a qualidade na gravação de evento

Aumenta temporariamente a qualidade do vídeo quando a gravação é disparada por um *evento do sistema* (a ação *Iniciar gravação* foi executada, um *alarme* foi disparado, ou por causa de um evento de movimentação). As configurações de *Aumentar qualidade na gravação de eventos* têm prioridade sobre as configurações de *Aumentar qualidade na gravação manual*. A duração do aumento da qualidade do vídeo depende do tipo de evento e das configurações de gravação das câmeras.

Câmera - Aba Gravação

Esta seção lista as configurações encontradas na aba **Gravação** da Câmera, na tarefa *Vídeo*.

Na aba *Gravação*, você pode personalizar as configurações de gravação em cada câmera individual em vez de usar as configurações da função de arquivamento.

Se a câmera estiver associada a funções Archiver auxiliar, existe um grupo de configurações para cada função de arquivamento à qual a câmera está associada.

- **Configurações de gravação:** Selecione se a câmera usa as configurações herdadas da função de arquivamento ou usa suas próprias configurações personalizadas.
  - **Herdar do Archiver:** Use as configurações de gravação da função de arquivamento.
  - **Definições personalizadas:** Defina as configurações de gravação para a câmera individual.

Você pode obter uma descrição de cada configuração de gravação na aba Gravação do Archiver.

Câmera - Aba Detecção de movimento

Esta seção lista as configurações encontradas na aba **Detecção de movimento** da Câmera, na tarefa *Vídeo*.

Na aba *Detecção de movimento*, você pode definir múltiplas configurações de detecção de movimento para sua câmera. Cada configuração é baseada em um cronograma diferente.

- **Detecção de movimento:** Ativa ou desativa a detecção de movimento pelos períodos de tempo abrangidos pela programação.
- **A detecção foi feita em:** Especifica se a detecção de movimento é realizada no Archiver (sempre disponível) ou na unidade de vídeo (nem todas as unidades suportam esse recurso).
- **Sensibilidade:** Controla o nível de diferença que deve ser detectado em um *bloco* entre dois quadros consecutivos antes de ele ser destacado como um *bloco de movimento*. Com a sensibilidade definida para o máximo (100%), a menor variação em um bloco de imagem é detectada como movimento. Reduzir a sensibilidade reduz o número de blocos de movimento detectados no vídeo. Você pode diminuir a sensibilidade quando seu equipamento for propenso a gerar ruído.
- **Autocalibrar:** Define automaticamente a sensibilidade para determinar o que constitui movimento positivo.
- **Detecções em quadros consecutivos:** Um quadro em que o número de *blocos de movimentos* atinja o *Limiar de movimento ativo* é chamado de *ocorrência*. Ajustar esse parâmetro com valor superior a 1 ajuda a evitar falhas de detecção de movimento falso, como o ruído de vídeo em um único quadro. Esta configuração garante que a detecção de movimento positivo seja relatada somente quando um alerta for observado em um certo número de quadros consecutivos. Quando foram alertas consecutivos suficientes, o primeiro alerta da série é marcado como o início do movimento.
- **Configurações avançadas:** Quando uma transmissão *H.264* é selecionada como a transmissão de gravação, o botão *Configurações avançadas* fica disponível. Clique no botão para abrir a caixa de diálogo *Configurações avançadas de detecção de movimento para H.264*, onde você pode refinar suas configurações de detecção de movimento para uma transmissão H.264.
- **Ênfase de vetor:** Configura a detecção de movimento com base na diferença de valores de vetor de movimentação (movimento) entre quadros consecutivos
- **Ênfase de luma:** Configura a detecção de movimento com base na diferença de valores de luma (brilho) entre quadros consecutivos
- **Personalizar:** Permite que você personalize suas configurações usando os controles deslizantes disponíveis, se as predefinições *Vetor* e *Ênfase de luma* não fornecerem resultados desejáveis (se você receber eventos de movimento em demasia ou insuficientes). Ajuste os valores dos seguintes controle deslizante entre 0 e 100, até obter resultados desejáveis. Quanto maior o valor, mais movimento é detectado.
  - *Ajuste de luma*. Configura a detecção de movimento com base na diferença de valores de luma (brilho) entre quadros consecutivos
  - *Ajuste de crominância*. Configura a detecção de movimento com base na diferença de valores de crominância (cor) entre quadros consecutivos.
  - *Ajuste de vetores*. Configura a detecção de movimento com base na diferença de valores de vetores (movimento) entre quadros consecutivos.
  - *Ajuste de macroblocos*. Define a detecção de movimento com base na presença de *intra-macroblocos* em seu quadro. Esta configuração é útil quando você observa indicadores de detecção de movimento em quadros fixos. Por exemplo, algumas unidades geram quadros completamente compostos de intra-macroblocos como um novo ponto de referência. Quando isso acontecer, você verá blocos de detecção de movimento cobrindo toda a imagem. Definir o *Ajuste de macroblocos* para 0 ajuda a evitar que isso aconteça.

- **Zonas de movimento:** Uma zona de movimento define *onde* deve ser detectado movimento na imagem de vídeo. Até seis zonas de movimento diferentes podem ser definidas por configuração. Para efeitos de detecção de movimento, a imagem de vídeo é dividida em um grande número de *blocos* (1320 para o padrão de codificação NTSC e 1584 para PAL). Cada um desses blocos pode ser ativado/desativado individualmente para detecção de movimento. Um bloco onde a detecção de movimento está ativada é representado por uma sobreposição quadrada azul semi-transparente na imagem de vídeo.
- **Limiar de movimento ativo:** Indica o número mínimo de *blocos de movimento* que devem ser detectados antes que o movimento seja significativo o suficiente para ser relatado. Juntamente com as *Ocorrências de quadros consecutivos*, uma detecção de movimento positivo é feita.
- **Limiar de desativação por movimento:** Da mesma maneira que o *Limiar de movimento ativo* detecta o início do movimento, o *Limiar de movimento inativo* detecta o fim do movimento. Considera-se que o movimento terminou quando o número de blocos de movimento cai abaixo do *Limiar de movimento inativo* por, pelo menos, 5 segundos.
- **Testar zona:** A zona de movimentação é exibida como sobreposições em azul. Os *blocos de movimentação* aparecem como sobreposições em verde. O número de blocos de movimentação é atualizado em tempo real. Quando o número de blocos de movimento alcança o *Limiar de movimento*, ele é exibido em vermelho.
- **Testar todas as zonas:** Neste modo, todas as *zonas de movimento* são exibidas ao mesmo tempo, com o número de blocos de movimento em cada uma exibido separadamente.
- **Visualizar todos os movimentos:** Testa toda a imagem de vídeo em busca de movimento. Todos os movimentos em qualquer lugar da imagem são exibidos como blocos de movimento (sobreposições verdes). O número total de blocos de movimentação é atualizado em tempo real. Utilize este modo para testar a definição de sensibilidade para esta câmara.
- **Eventos:** Seleciona os eventos relacionados à detecção de movimento gerados pelo sistema (eventos padrão ou personalizados).

Câmera - Aba Cor

Esta seção lista as configurações encontradas na aba **Cor** da Câmera, na tarefa *Vídeo*.

Na aba *Cor*, você pode ajustar os atributos de vídeo, como brilho, contraste, matiz e saturação, com base em agendas diferentes.

- **Brilho:** Ajusta o brilho da imagem de vídeo para a programação selecionada.
- **Contraste:** Ajusta o contraste da imagem de vídeo para a programação selecionada.
- **Matiz:** Ajusta o matiz da imagem de vídeo para a programação selecionada.
- **Saturação:** Ajusta a saturação da imagem de vídeo para a programação selecionada.
- **Carregar predefinidos:** Repor todos os parâmetros aos seus valores padrão para a programação selecionada.
- **Formato analógico:** Selecione o formato analógico NTSC (National Television System Committee) ou PAL (Phase Alternating Line) para o sinal de vídeo. O formato PAL geralmente transmite vídeo a uma velocidade de quadro mais baixa, mas com maior resolução.

Câmera - Aba Rastreamento visual

Esta seção lista as configurações encontradas na aba **Rastreamento visual**, na tarefa *Vídeo*.

Na aba *Rastreamento visual*, você pode configurar o recurso de rastreamento visual.

- **Selecionar:** Redimensione, reposicione e gire a sobreposição de vídeo selecionada usando o mouse.
- **Retângulo:** Desenhe um retângulo na imagem de vídeo.
- **Elipse:** Desenhe uma elipse na imagem de vídeo.
- **Entidades:** Apresente a exibição de área a partir da qual as câmeras vinculadas à sobreposição selecionada podem ser arrastadas.
- **Tamanho e posição:** Redimensione e reposicione a sobreposição de vídeo selecionada.
- **Preencher:** Selecione a cor de preenchimento da sobreposição selecionada.
- **Borda:** Selecione a cor da borda da sobreposição selecionada.
- **Opacidade:** Selecione a porcentagem de opacidade da sobreposição selecionada.
- **Espessura:** Selecione a espessura da borda da sobreposição selecionada.
- **Vínculos:** Lista de câmeras que foram arrastadas da exibição de área para a sobreposição selecionada e para as quais um usuário pode saltar a partir dessa câmera no Security Desk.

Câmera - Aba hardware

Esta seção lista as configurações encontradas na aba **Hardware** de Câmera, na tarefa *Vídeo*.

Na aba *Hardware*, você pode associar outros dispositivos de hardware (motores PTZ, alto-falantes, microfones e assim por diante) a esta câmera e definir configurações de hardware específicas. Quando a unidade é adicionada inicialmente ao sistema, todos os dispositivos de hardware pertencentes à mesma unidade são configurados por padrão. Você pode associar manualmente sua câmera a outros dispositivos, de acordo com a forma como eles estão fisicamente conectados.

Configuração de PTZ

Se o motor PTZ não estiver integrado na câmera, você precisará configurar o motor PTZ separadamente antes de poder controlá-lo no Security Desk. Quando você liga a PTZ, configurações adicionais aparecem.

- **Protocolo:** Protocolo usado pelo motor PTZ.
- **Porta serial:** Porta serial utilizada para controlar o motor PTZ. Clique em para definir os parâmetros de Retardo de inatividade, Comando de inativoe Atraso de bloqueio .
- **PTZ melhorado:** Ligue esta opção para ativar os comandos PTZ de caixa de zoom, centralizar no clique e zoom avançado.
- **Calibrar:** Clique para calibrar o PTZ.

  NOTA: Nem todas as câmeras exigem calibração PTZ.
- **Endereço de PTZ:** Número identificando o motor PTZ selecionado na porta serial. Esse número é importante porque é possível conectar mais de um motor PTZ na mesma porta serial. Este número deve corresponder às configurações de chaves dip no hardware PTZ.
- **Fator de zoom máximo:** O fator de zoom máximo permitido para esta câmera.

Se você observar problemas de posicionamento ou rotação ao controlar uma câmera PTZ, você pode clicar em **Especificar deslocamentos de rotação e direção** para as seguintes opções adicionais:

- **Deslocamento da panorâmica:** Digite o deslocamento da panorâmica (em graus) necessário para alinhar a câmera com a posição mostrada no Security Center.
- **Deslocamento dzo a inclinação:** Digite o deslocamento da inclinação (em graus) necessário para alinhar a câmera com a posição mostrada no Security Center.
- **Inverter direção da rotação:** Se a câmera não girar na mesma direção mostrada no Security Center, selecione esta opção para inverter a direção de rotação.

Retardo de inatividade

O Retardo de inatividade é a quantidade de tempo que um motor PTZ fica bloqueado quando um usuário faz um dos seguintes procedimentos:

- Move um PTZ inativo (o que gera o evento *PTZ ativado*). Após o período de retardo inativo, o evento *PTZ parado* é gerado. Se os usuários continuarem a mover o PTZ, o temporizador de contagem decrescente de tempo inativo reinicia continuamente.
- Aproxima o zoom do motor PTZ (o que gera o evento *Zoom de PTZ pelo usuário*). Após a última operação de zoom e depois de o período de retardo inativo terminar, o evento *Zoom de PTZ pelo usuário* parado é gerado.

Exemplo

O retardo inativo é de 120 segundos. Se um usuário der zoom várias vezes e cada ação de zoom tiver 120 segundos de separação, apenas um evento *Zoom de PTZ pelo usuário* é gerado. Se outro usuário efetuar um zoom no mesmo PTZ antes de o período de inatividade expirar, o evento *Zoom de PTZ pelo usuário* é gerado novamente, registrado para o segundo usuário, e o temporizador decrescente é reiniciado. O evento *Zoom de PTZ pelo usuário interrompido* só é gerado após o período de inatividade expirar e é registrado para o segundo usuário.

Comando de inativo

Quando o PTZ fica inativo (após o período de inatividade expirar e o evento *PTZ parado* ou *Zoom de PTZ pelo usuário interrompido* ser gerado), esta opção determina a próxima ação do PTZ.

- **Nenhuma:** O PTZ permanece inativo até que um usuário comece a controlá-lo.
- **Predefinição:** O PTZ move-se para uma posição predefinida quando fica inativo.
- **Padrão:** O motor PTZ inicia um padrão PTZ quando fica inativo.

Atraso de bloqueio

O *Atraso de bloqueio* é a quantidade de tempo que um motor PTZ fica bloqueado quando um usuário clica no botão Bloquear PTZ (🔒) no widget PTZ. Após o período de inatividade do bloqueio, o PTZ se desbloqueia automaticamente.

Alto-falante e microfone

Mesmo que a unidade à qual a sua câmera pertence não suporte áudio, você ainda pode ligar sua câmera a dispositivos de áudio (alto-falante e microfone) encontrados em outras unidades.

Modificação da câmera

Selecione esta opção para permitir que o Security Center processe eventos de *Adulteração de câmera* emitidos pela unidade. Esta configuração só está disponível se a unidade de vídeo for capaz de detectar a adulteração da câmera.

- **Duração mínima:** Normalmente, qualquer mau funcionamento que impeça a cena de ser vista corretamente (obstrução parcial ou completa da visão da câmera, mudança repentina do campo de visão ou perda de foco) pode ser vista como uma tentativa de adulteração da câmera. Você pode controlar a sensibilidade com que unidade reage a essas mudanças, especificando quanto tempo a disfunção deve durar antes de a unidade gerar um evento de *Adulteração de câmera*.
- **Alarme para imagens escuras:** Selecione esta opção para que as obstruções totais sejam consideradas como mau funcionamento.

Alarme de áudio

Selecione esta opção para permitir que o Security Center processe alarmes de áudio emitidos pela unidade como eventos de *Alarme de áudio*. Esta configuração só está disponível se a unidade de vídeo for capaz de disparar alarmes de áudio.

NOTA: O *Nível de alarme* define o valor usados para acionar alarmes de áudio na unidade. Uma unidade pode ser configurada para emitir alarmes de áudio quando o nível de som sobe acima ou cai abaixo do valor ajustado. O nível de alarme pode ser definido no intervalo 0-100%, onde 0% é o mais sensível e 100% menos sensível.

Rotação da imagem

Use esta configuração para corrigir a orientação da imagem quando a câmera estiver montada de cabeça para baixo ou com um ângulo de 90 graus. Este método utiliza a capacidade da câmera para rodar a imagem.

- Este recurso somente está disponível se ele for compatível com o hardware da câmera.
- As opções de rotação variam de acordo com o modelo da câmera.
- Rodar a imagem usando o recurso *Rotação de imagem* é preferível a usar o recurso *Rotação de vídeo*, contudo, se o recurso de rotação de imagem afetar adversamente a taxa de quadros de vídeo, experimente usar a rotação de vídeo.

Rotação do vídeo

Use esta configuração para corrigir a orientação da imagem quando a câmera estiver montada de cabeça para baixo ou com um ângulo de 90 graus. Este método utiliza Security Center para rodar o vídeo.

- Usar *Rotação de vídeo* adiciona carga extra nas estações de trabalho clientes. Por esse motivo, é preferível usar *Rotação de imagem*, se estiver disponível para a câmera.
- Este recurso não está disponível para câmeras PTZ ou câmeras que usem lentes panomórficas (olho de peixe).

Tipo de lente

Use esta configuração para selecionar o tipo de lente para câmeras com lentes intercambiáveis. Dependendo do tipo de lente selecionado, pode haver configurações adicionais a definir, como *dewarping* de uma lente olho de peixe.

Sequência de câmeras - Aba Câmeras

A aba **Câmeras** é onde você pode adicionar câmeras que compõem a sequência de câmeras.

A ordem das câmeras na lista é a ordem em que elas são exibidas no Security Desk. Cada câmera é definida pelas seguintes propriedades de exibição:

- **Tempo de permanência:** O período de tempo em que a câmera será exibida quando estiver circulando pela sequência.
- **Comando PTZ:** (Somente câmeras PTZ) A ação que a câmera PTZ realizará quando for exibida na sequência.
- **Comando PTZ:** (Somente câmeras PTZ) O número de comutador e o estado no qual definir o comutador quando a câmera é exibida na sequência.

Tópicos relacionados

Criar sequências de câmeras na página 510

Abas de configuração de titulares de cartão

Esta seção lista as configurações encontradas nas guias de configuração de titulares de cartão, na tarefa *Controle de acesso*.

Titular de cartão - Aba Propriedades

Na aba *Propriedades*, você pode ver as informações pessoais e o status do titular de cartão. Informações adicionais podem ser encontradas na aba *Campos personalizados*, se forem criados campos personalizados para entidades de titular de cartão.

- **Nome:** Primeiro nome do titular de cartão Se o idioma do software (escolhido na instalação) for de origem latina, o campo *Nome* é configurado como nome seguido pelo sobrenome. Esta ordem é invertida se estiver usando um idioma asiático, como japonês ou chinês.
- **Sobrenome:** Sobrenome do titular de cartão
- **Endereço de e-mail:** Endereço de e-mail do titular de cartão, usado para ações automatizadas associadas ao titular de cartão (enviar um e-mail).
- **Usar tempo de concessão estendido:** Concede ao titular de cartão mais tempo para passar pelas portas quando o parâmetro *Tempo de concessão estendido* estiver configurado para uma porta. Use esta opção para titulares de cartão com mobilidade reduzida.
- **Desconsiderar regras anti-passback:** Isenta o titular de cartão de todas as restrições de *anti-passback*.
- **Certificado de segurança :** (Visível apenas para usuários administrativos) Nível de certificado de segurança do titular de cartão. O nível de certificado de segurança determina o acesso a áreas onde há um nível de ameaça definido no Security Center. O nível 0 é o nível de certificado mais elevado, com mais privilégios.
  - **Herdado de grupos de titulares de cartão pais:** O nível de certificado de segurança do titular de cartão é herdado dos grupos de titulares de cartão pais. Se o titular de cartão fizer parte de vários grupos de titulares de cartão, ele herda o nível mais elevado de certificado de segurança dos grupos de titulares de cartão pais.
  - **Específico:** Defina um nível de certificado de segurança para o titular de cartão.
- **Status:** Define o status para *Ativo* ou *Inativo*. Para as credenciais funcionarem, e para ter acesso a qualquer área, o status deve estar *Ativo*.
- **Ativação:** Exibe a data em que o titular de cartão foi ativado.
- **Validade:** Defina uma data de vencimento para o perfil:
  - **Nunca:** Nunca vence.
  - **Data específica:** Vence em uma data e horário específicos.
  - **Definir vencimento no primeiro uso:** Vence após um número específico de dias depois do primeiro uso.
  - **Quando não é usado:** Vence quando não foi utilizado durante um número específico de dias.

Titular de cartão - Aba Imagem

Na aba *Imagem*, você pode atribuir uma imagem ao titular de cartão.

Grupo de titulares de cartão - Aba Propriedades

Esta seção lista as configurações encontradas na aba **Propriedades** de Grupo de titulares de cartão, na tarefa *Controle de acesso*.

Na aba **Propriedades** você pode visualizar e configurar os membros deste grupo de titulares de cartão e configurar suas propriedades comuns. Informações adicionais podem ser encontradas na aba **Campos personalizados**, se forem criados campos personalizados para grupos de titulares de cartão.

- **Grupo disponível para visitantes:** Defina como **Ligado** se este grupo for usado para visitantes.
- **Endereço de e-mail:** Endereço de e-mail para ações automatizadas associadas ao grupo (enviar um e-mail).
- **Certificado de segurança:** (Apenas visível para usuários administrativos) Nível de certificado de segurança para o grupo de titulares de cartão. O nível de certificado de segurança de um grupo de titulares de cartão determina o seu acesso a áreas quando um nível de certificado de segurança mínimo é exigido em zonas ao definir um nível de ameaça no Security Center. O nível 0 é o nível de certificado mais elevado, com mais privilégios.
  - **Herdado de grupos de titulares de cartão pais:** O nível de certificado de segurança é herdado dos grupos de titulares de cartão pais. Se existirem vários grupos de titulares de cartão pais, é herdado o certificado mais elevado.
  - **Específico:** Define um nível de certificado de segurança específico para o grupo de titulares de cartão.
- **Titulares do cartão:** Define os membros do grupo de titulares de cartão usando os botões  e  . Tanto os titulares de cartão individuais como outros grupos de titulares de cartão podem ser membros.

Abas de configuração de credencial

Esta seção lista as configurações encontradas nas guias de configuração de credenciais, na tarefa *Controle de acesso*.

Credencial - Aba Propriedades

Na aba *Propriedades*, você pode configurar as informações e o status da credencial. Informações adicionais podem ser encontradas na aba *Campos personalizados*.

- **Informações de credencial:** Esta seção identifica os detalhes da credencial em si. Se a credencial for um cartão de controle de acesso, o formato, o código da instalação e o número do cartão serão exibidos.
  - **Titular do cartão:** Exibe o titular do cartão com o qual esta credencial está associada. O titular do cartão pode ser alterado, se necessário.
- **Status:** Mostra se o status da credencial é *ativa* ou *Inativa/Perdida/Roubada/Expirada*.
- **Ativação:** Exibe a data e hora em que a credencial foi atribuída a este estado.
- **Validade:** Defina uma data de vencimento para a credencial:
  - **Nunca:** A credencial nunca vence.
  - **Data específica:** A credencial vence em uma data e horário específicos.
  - **Definir vencimento no primeiro uso:** A credencial vence depois de um número específico de dias após o primeiro uso.
  - **Quando não é usado:** A credencial vence quando não foi utilizada durante um valor específico de dias.

Credencial - aba Modelo de crachá

Na aba *Modelo de crachá*, você pode definir o modelo de crachá padrão associado a essa credencial. Você pode visualizar qual será a aparência da credencial quando impressa usando um modelo de crachá específico. Você também pode imprimir a credencial do cartão.

Abas Configuração de portas

Esta seção lista as configurações encontradas nas guias Configuração de portas, na tarefa *Exibição de área*.

Porta - aba Propriedades

Na aba *Propriedades*, você pode configurar o comportamento geral da porta. Alguns dos comportamentos não são suportados por todos os tipos de unidades de controle de acesso. Se o comportamento configurado não for suportado pela unidade de controle de acesso selecionada, um aviso amarelo aparece na página, explicando por que sua configuração não é válida.

- **Destrancada para manutenção:** Defina como *Ligado* se a porta estiver destrancada e possivelmente aberta para fins de manutenção. Enquanto a porta estiver em modo de manutenção ela permanece destrancada e não são gerados eventos, exceto o evento *Porta off-line O dispositivo está off-line*. O ícone de *modo de manutenção* () também é exibido no ícone de porta em mapas.
- **Tempo de concessão padrão:** Período de tempo em que a porta fica destrancada após um evento *Acesso concedido* ser gerado.
- **Tempo de concessão estendido:** Para os titulares de cartões com a propriedade "tempo de concessão estendido" ativada, a quantidade de tempo que a porta fica desbloqueada após o acesso ser concedido.
- **Tempo de entrada padrão:** Período de tempo que o titular de cartão tem para passar pelo sensor de entrada, para além do *Tempo de concessão padrão*. Se nenhuma entrada for detectada durante este tempo, um evento *Nenhuma entrada detectada* é gerado. Esta opção só é suportada quando sua porta está configurada com um sensor de entrada. Se nenhum sensor de entrada estiver configurado, a entrada é assumida quando a porta se abre. Se nenhum sensor de porta estiver configurado, a entrada é assumida quando o acesso é concedido.

  Por exemplo, se o *Tempo de concessão padrão* for 5 segundos e o Tempo de entrada for 3 segundos, o titular de cartão terá um total de 8 segundos para acionar o sensor de entrada da porta.
- **Tempo de entrada estendido:** Para titulares de cartões com a propriedade "tempo de concessão estendido" ativada, a quantidade de tempo que o titular de cartão tem para atravessar o sensor de entrada, além do tempo de concessão estendido. Se nenhuma entrada for detectada durante este tempo, um evento *Nenhuma entrada detectada* é gerado. Esta opção só é suportada quando sua porta está configurada com um sensor de entrada. Se nenhum sensor de entrada estiver configurado, a entrada é assumida quando a porta se abre. Se nenhum sensor de porta estiver configurado, a entrada é assumida quando o acesso é concedido.

  Por exemplo, se o *Tempo de concessão estendido* for 10 segundos e o *Tempo de entrada estendido* for 10 segundos, o titular de cartão terá um total de 20 segundos para acionar o sensor de entrada da porta.
- **Retravamento de porta:** Especifica quando rebloquear a porta depois que um acesso foi concedido.
  - **Ao fechar:** Rebloqueia quando a porta é fechada.
    NOTA: Esta opção não é suportada por unidades HID.
  - **Retardo após a abertura:** Rebloqueia após o retardo especificado depois que a porta foi aberta.
    NOTA: Para unidades HID, o retardo máximo é de 27 minutos.
- **Quando a porta é destrancada por agendamento:** Selecione os eventos que deseja suprimir quando a porta é desbloqueada por agendamento.
  - *Porta aberta por muito tempo* eventos
  - Eventos *Acesso concedido* e *Acesso negado*
- **Porta mantida aberta:** O que fazer quando a porta é mantida aberta.

- **Evento de disparo:** Defina como **Ligado** caso o evento *Porta aberta por muito tempo* deva ser gerado após a duração especificada.
- **Comportamento da campainha do leitor:** Defina como **Suprimida** para nunca soar a campainha ou como **Suprimida quando a porta fecha** para silenciar a campainha assim que a porta se fechar.

- **Porta forçada:** O que fazer quando a porta é forçada.
  - **Evento de disparo:** Defina como **Ligado** caso o evento *A porta forçada para abrir* deva ser gerado.
  - **Comportamento da campainha do leitor:** Defina como **Suprimida** para nunca soar a campainha, como **Suprimida quando a porta fecha** para interromper a campainha assim que a porta se fechar ou como **Suprimida quando o acesso é concedido** para que a campainha pare quando o acesso é concedido ou quando a porta é trancada manualmente.
- **Requisição de saída (REX):** As opções desta seção geralmente são usadas para diminuir o número de falsos eventos *Solicitação de saída* em uma porta.
  - **Tempo para ignorar "Requisição de saída" após acesso concedido:** Ignora quaisquer solicitações de saída para isto muito depois do acesso ter sido concedido.
  - **Destravar no REX:** Coloque em **Ligado** se um REX estiver sendo usado e você quiser conceder automaticamente acesso a todas as solicitações de saída.
    NOTA: O Security Center não recebe eventos REX se a unidade de controle de acesso estiver conectada ao Access Manager. No entanto, os eventos REX são recebidos quando a unidade está offline e depois é novamente conectada ao Access Manager.
  - **Ignorar eventos REX enquanto a porta estiver aberta:** Não gera eventos REX quando a porta estiver aberta.
  - **Tempo para ignorar REX após fechamento da porta:** Uma vez que a porta tenha fechado, espere este tempo antes de gerar mais eventos REX.
    NOTA: Os controladores HID não suportam este recurso.
- **Regra de acompanhante de visitante e regra de duas pessoas:** Configurações comuns a escolta de visitante e restrições de regras de duas pessoas.
  - **Fiscalizar regra de duas pessoas:** Defina como **Ligado** caso dois titulares de cartão devam apresentar as credenciais com um certo intervalo entre si para obter acesso. Esta regra pode ser aplicada apenas em um lado da porta ou em ambos.
  - **Atraso máximo entre apresentações de cartão:** Retardo máximo permitido entre as duas apresentações de cartão para satisfazer a regra de escolta de visitante e as restrições de regra de duas pessoas.

Porta - Aba hardware

Na aba *Hardware*, você pode configurar as relações de ligação física entre a unidade de controle de acesso e a porta e associar câmeras aos lados da porta.

- **Unidade preferencial:** Unidade de controle de acesso conectada à porta.
- **Interface preferida:** Módulo de interface conectado à porta.
- **Lado da porta:** Leitores, REX, sensores de entrada e câmeras associadas ao lado da porta, que correspondem à fiação física feita no controlador e na porta.

  As configurações disponíveis do leitor são:

  - **Tempo limite para digitação de PIN:** Isso configura apenas o tempo limite de digitação do PIN após o cartão ter sido lido. Por exemplo, por padrão (5 segundos), você tem 5 segundos para digitar todos os dígitos do PIN.

  - **Usar cartão e PIN:** Ajuste em **ATIVO** para alterar o modo do leitor para Cartão e PIN e selecione o **agendamento**ao qual esse modo se aplica. Quando não está em um período de tempo agendado, o leitor se comporta somente em modo de Cartão.
- **Conexões adicionais:** Outras conexões físicas associadas com o controlador e a porta.

Porta - aba Regras de acesso

Na aba *Regras de acesso*, você pode ver as regras de acesso aplicadas a esta porta.

- **O acesso da porta se aplica a:** A quais os lados da porta as regras de acesso se aplicam.
  - **Ambos os lados:** Aplica as mesmas regras de acesso para ambos os lados da porta.
  - **Lados individuais:** Aplica regras de acesso individuais para cada lado da porta.
- **Direitos de acesso para a porta (lado):** Define quem tem acesso a esta porta (ou lado da porta).
  - **Regras de acesso:** Adiciona regras de acesso para conceder (ou negar) acesso à porta aos titulares de cartões e grupos de titulares de cartões com base em um cronograma. Esta é a abordagem recomendada.
  - **Titulares de cartão, grupos de titulares de cartão:** Adiciona titulares de cartões e grupos de titulares de cartões para conceder acesso à área em todos os momentos. Use essa abordagem apenas para situações temporárias.
    NOTA: Se todas as portas do perímetro de uma área compartilharem as mesmas regras de acesso, defina essas regras no nível da área.

Porta - aba Agendamentos de desbloqueio

Na aba *Agendas de desbloqueio*, você pode configurar períodos agendados para quando a porta não esteja sendo usada para acesso protegido e nenhuma regra de acesso esteja em vigor.

- **Agendamentos de abertura (acesso livre):** Períodos em que a porta fica desbloqueada e nenhuma regra de acesso está em vigor.
- **Exceções aos agendamentos de abertura (acesso controlado):** Períodos em que a porta fica bloqueada e as regras de acesso estão em vigor.

Tópicos relacionados

Considerações sobre conexão de E/S do HID na página 1161

Abas de configuração de elevador

Esta seção lista as configurações encontradas nas guias de configuração de elevador, na tarefa *Visualização de área*.

Elevador - aba Andares

Na aba **Andares**, você pode configurar as relações de ligação física entre a unidade de controle de acesso e os andares do elevador e selecionar câmeras usadas para monitorar este elevador no Security Desk.

- **Unidade preferencial:** Unidade de controle de acesso que gerencia o painel da cabine do elevador.
- **Leitor de cabine do elevador:** *Interface de Leitor* que é usada dentro da cabine do elevador.

  As configurações disponíveis do leitor são:

  - **Tempo limite para digitação de PIN:** Isso configura apenas o tempo limite de digitação do PIN após o cartão ter sido lido. Por exemplo, por padrão (5 segundos), você tem 5 segundos para digitar todos os dígitos do PIN.
  - **Usar cartão e PIN:** Ajuste em **ATIVO** para alterar o modo do leitor para Cartão e PIN e selecione o **agendamento**ao qual esse modo se aplica. Quando não está em um período de tempo agendado, o leitor se comporta somente em modo de Cartão.
- **Câmera:** Câmera que monitora esse elevador no Security Desk.
- **Andares:** Relés e entradas de botões conectados aos botões de andares do elevador.
  - **Relé de botão:** Relés de saída atribuídos aos diferentes botões de andares do elevador. Os eventos de acesso concedido fazem com que um relé de saída feche, o que permite que o botão pressionado solicite um determinado andar.
  - **Rastreamento de andar:** Entradas atribuídas aos botões de andares do elevador. Quando você atribui entradas, o Security Center pode tomar nota de qual botão de andar foi pressionado.
  - **Câmeras:** Câmeras usadas para monitorar a porta do elevador em cada andar.

Elevador - aba Acesso

Na aba **Acesso**, você pode configurar as regras de acesso aplicadas a cada andar do elevador e determinar quando o acesso aos pisos do elevador é controlado e quando o *acesso livre* está disponível.

- **Regras de acesso:** Selecione as regras de acesso para determinar quais botões de andar estão habilitados, quando e para quais titulares de cartão. Diferentes regras de acesso podem ser aplicadas a diferentes andares ou aplicadas a todos os andares.
- **Exceções:** Determine se existem exceções à regra de acesso que você definiu.
  - **Cronograma:** Selecione um cronograma quando a exceção se aplica.
  - **Andar:** Selecione a quais andares se aplica a exceção.
  - **Modo:** Selecione se o acesso ao andar do elevador é *livre* ou *controlado* durante o cronograma da exceção.

Elevador - aba Avançado

Na aba **Avançado**, você pode configurar o comportamento avançado deste elevador.

- **Horário da concessão:** Quanto tempo o botão de andar do elevador fica ativado depois de um evento de acesso concedido ser gerado.
- **Acesso livre é quando o relé de saída está:**

- **Normal:** O acesso ao andar é concedido quando o relé de saída da unidade de controle de acesso é desenergizado. Significa que uma perda de energia resulta em acesso livre ao andar.
- **Ativo:** O acesso ao andar é concedido quando o relé de saída da unidade de controle de acesso é energizado. Significa que uma perda de energia resulta no acesso ao andar ser negado.

Abas de configuração de zonas de hardware

As zonas de hardware são controladas por uma única unidade de controle de acesso. Elas podem funcionar offline e podem ser armadas ou desarmadas usando um interruptor de chave ou segundo uma agenda.

Zona de hardware - Aba Propriedades

Clique na aba **Propriedades** para configurar as entradas que definem esta zona e defina como elas são avaliadas.

- **Unidade de controle de acesso:** Unidade de controle de acesso que controla a zona de hardware.
- **Módulo de interface:** Módulo de interface de onde as entradas são selecionadas.
- **Entradas:** Entradas combinadas para avaliar o estado de zona.
- **Operador:** Operador lógico usado para combinar os estados de entrada para avaliar o estado de zona.
- **Eventos associados:** Eventos representando os estados de zonas. Selecione *Nenhum* caso um estado de zona deva ser ignorado.
  - **Estado normal:** Quando a combinação de entradas resulta em zero (0).
  - **Estado ativo:** Quando a combinação de entradas resulta em um (1).
  - **Estado anormal:** Exige ter pelo menos uma entrada supervisionada. A zona fica no estado de *Problema* quando pelo menos uma das entradas está no estado *Problema*. O estado *Problema* supera todos os outros estados.
  - **Limite de reativação:** O período de tempo durante o qual o mesmo evento não deve ser acionado novamente.

Zona de hardware - Aba Armamento

Clique na aba **Armamento** para configurar a origem de armamento de sua zona e seu comportamento de armamento.

- **Origem de armamento:** Selecione se a zona de hardware é armada por um interruptor de chave ou segundo uma agenda.
  - **Agenda:** Selecione a agenda que corresponde ao período em que a zona fica armada.
  - **Ponto de entrada:** Selecione a entrada que está ligada ao interruptor de chave.
- **Atrasos:** Atrasos opcionais que dão tempo para que você abandone o local após armar a zona e tempo para desarmar a zona após o acionamento de um sensor.
  - **Atraso de armamento:** Duração (mm:ss) que você deseja entre o tempo em que a zona é armada e o tempo em que os disparos de evento se tornam ativos.
  - **Atraso na entrada:** Duração (mm:ss) que você deseja entre o tempo em que o sensor de entrada é disparado e o tempo em que os eventos são disparados. Esta opção permite desarmar a zona antes de disparar os relés de saída.
- **Sinal sonoro de contagem regressiva:** Você pode atribuir um relé de saída para ativar um sinal sonoro de contagem regressiva para coincidir com o atraso de armamento.
  - **Som de contagem regressiva:** Selecione o relé de saída.
  - **Comportamento de saída:** Selecione o comportamento de saída que define o padrão de sinal para o sinal sonoro.

Abas de configuração de lista de procurados

Esta seção lista as definições encontradas nas abas de configuração de listas de procurados, na tarefa *LPR*.

Lista de procurados - Aba Propriedades

Na aba *Propriedades*, você pode configurar as propriedades básicas da lista de procurados (prioridade, caminho, atributos etc.). Essas configurações indicam ao Security Center como analisar o arquivo da lista de procurados no formato exigido pelo *Patroller* e pelo *LPR Manager* para identificar placas lidas por *unidades Sharp*.

- **Prioridade. :** Prioridade da lista de procurados. Zero (0) é a configuração de mais alta prioridade e 100 é a configuração de prioridade mais baixa. Se uma leitura de placa corresponde a mais de uma lista de procurados, a lista de procurados com a maior prioridade é exibida em primeiro lugar entre as listas de procurados encontradas.
- **Caminho da lista de procurados:** Caminho para o arquivo de texto de origem da lista de procurados, que contém os dados da lista, como números da placa de licença e outras informações relacionadas ao veículo. O arquivo de texto de origem pode ser localizado na unidade local do computador do LPR Manager (por exemplo, a unidade C) ou em uma unidade de rede acessível a partir do computador LPR Manager.
- **Usar delimitadores:** Indica ao Security Center que os campos do arquivo da lista de procurados variam em comprimento e indica o caractere usado para separar cada campo no arquivo. Por padrão, *Usar delimitadores* está definido como *Ligado* e o delimitador especificado é *ponto e vírgula* (;). Se o seu arquivo de lista de procurados for feito de campos de comprimento fixo, configure *Usar delimitadores* como *Desligado*.
- **Visível no editor:** Permite que um usuário edite a lista de procurados ou lista de autorizações usando a tarefa do editor da lista de procurados ou da lista de autorizações.
- **Atributos:** Informa ao Security Center o nome e a ordem dos campos (atributos) no arquivo de texto de origem.

Lista de procurados - aba Avançado

Na aba *Avançado*, você pode configurar as propriedades avançadas da lista de procurados (cor, som, frequência de download etc.). Essas propriedades não são exigidas para todas as listas de procurados, mas permitem que você personalize certas listas para cenários específicos.

- **Cor. :** Atribui uma cor para uma lista de procurados: Ao escolher uma cor, o símbolo de mapa que marca a localização da ocorrência de lista de procurados no Security Desk e no Genetec Patroller™ aparecerá nessa cor, bem como nas telas Ocorrência de lista de procurados e Revisar ocorrências no Genetec Patroller™.
- **Usar caracteres curinga. :** Indica que a lista de procurados contém curingas (números de placa parciais). Você pode ter um máximo de dois caracteres curinga (asterisco *) em um campo PlateNumber. Os caracteres curinga são usados em situações em que testemunhas não viram ou não conseguem lembrar do número completo da placa de licença. Isso permite que o agente potencialmente intercepte veículos associados a um crime, que de outra maneira não teriam sido detectados usando listas de procurados padrão.
- **Oculta:** Defina a lista de procurados como uma *lista de prioridades ocultas*. Quando você escolhe esta configuração, os usuários do Genetec Patroller™ não são alertados quando acontece uma ocorrência. Somente usuários com privilégios suficientes podem ver *ocorrências ocultas* no Security Desk.
- **Endereço de e-mail:** Endereço de e-mail que recebe uma notificação quando a lista de procurados que está sendo configurada gera um alerta.

- **Arquivo de som:** O som que o Genetec Patroller™ reproduz quando acontece uma ocorrência de lista de procurados. Se você deixar este campo em branco, o Genetec Patroller™ reproduzirá seus sons padrão. O caminho (você deve incluir o nome do arquivo) indica a localização do arquivo no computador do Genetec Patroller™ a bordo do veículo.
- **Sobrepor privacidade para e-mails:** Ignorar as configurações de privacidade que você aplicou no nível do Directory e enviar um e-mail com dados LPR reais para o endereço de e-mail que você especificou para esta lista de procurados específica.
- **Desabilitar transferência periódica:** Desliga a transferência periódica de modificações em listas de procurados para o computador do Genetec Patroller™. Quando esta configuração está desativada, as alterações em listas de procurados são baixadas para o Genetec Patroller™ apenas quando o usuário faz logon no aplicativo. Esta opção exige uma conexão sem fio entre o Genetec Patroller™ e o Security Center.
- **Habilitar transferência na modificação:** Transfere modificações em listas de procurados para o Genetec Patroller™ assim que ocorrerem. Por exemplo, você pode usar essa opção em uma lista de procurados para forçar o Genetec Patroller™ a solicitar mudanças com mais frequência do que o período de transferência periódica (que se aplica a todas as listas de procurados). Isso pode ser útil para alertas AMBER, porque eles podem ser adicionados a uma lista de procurados específica e enviados para um Genetec Patroller™ quase que imediatamente. Esta opção exige uma conexão sem fio contínua entre o Genetec Patroller™ e o Security Center.

Zona de E/S - Aba Propriedades

Na aba **Propriedades** da zona de E/S, você pode configurar as entradas que definem a zona e os relés de saída que devem ser acionados, juntamente com o comportamento de saída desejado, quando o estado da zona estiver armado e ativo.

- **Manutenção:** Coloque em **Ligado** para deixar a zona em modo de manutenção. Enquanto estiver no modo de manutenção, a zona é desarmada e passa para o estado *Normal*. Nenhum evento é gerado e nenhum comportamento de saída é desencadeado durante este tempo, nem mesmo o evento *Problema*.
- **Agendamento de colocação em atenção:** Seleciona os agendamentos correspondentes aos períodos em que a zona fica armada.
- **Exceções:** Seleciona os agendamentos correspondentes aos períodos em que a zona não fica armada. Os horários de exceção têm precedência sobre os horários de armamento.
- **Unidade mestre:** Mostra a unidade Synergis™ que é selecionada na criação da zona para fazer ligação de E/S. A zona de E/S deixa de funcionar se a unidade mestre estiver desligada.
- **Entradas:** Selecione as entradas que devem ser combinadas para avaliar o estado da zona. As entradas podem pertencer a diferentes unidades Synergis™, mas todas as unidades devem estar no mesmo Access Manager.

  IMPORTANTE: Se as entradas não pertencerem à mesma unidade Synergis™, você deve selecionar a opção **Ativar ponto a ponto** no Access Manager.
- **Saídas:** Selecione os relés de saída para os quais deseja enviar o comportamento de saída configurado, quando a zona estiver armada e no estado *Ativo*. A zona também pode ser configurada para acionar as saídas quando a zona estiver no estado *Problema*, independentemente de a zona estar armada ou não. Os relés de saída podem pertencer a diferentes unidades Synergis™, mas todas as unidades devem estar no mesmo Access Manager.

  IMPORTANTE: Se os relés de saída não pertencerem à mesma unidade Synergis™, você deve selecionar a opção **Ativar ponto a ponto** no Access Manager.

  MELHOR PRÁTICA: O tanto quanto possível, use os relés de saída na unidade mestre. Isso permite que a zona E/S continue a funcionar quando uma ou mais unidades escravas estiverem desligadas.
- **Comportamento da saída:** Selecione o comportamento de saída para enviar para os relés de saída.
- **Ativar a saída com problema quando a zona estiver desarmada:** Selecione esta opção para sempre acionar os eventos e relés de saída quando a zona estiver no estado *Problema*, independentemente de a zona estar armada ou não.
- **Reverter para:** Selecione o comportamento de saída a ser enviado para os relés de saída quando a zona retornar ao estado *Normal*.
- **Eventos associados:** Eventos representando os estados de zonas. Selecione *Nenhum* caso um estado de zona deva ser ignorado.
  - **Estado normal:** Quando a combinação de entradas resulta em zero (0).
  - **Estado ativo:** Quando a combinação de entradas resulta em um (1).
  - **Estado anormal:** Exige ter pelo menos uma entrada supervisionada. A zona fica no estado de *Problema* quando pelo menos uma das entradas está no estado *Problema*. O estado *Problema* supera todos os outros estados.
  - **Limite de reativação:** O período de tempo durante o qual o mesmo evento não deve ser acionado novamente.

Área de detecção de intrusão - Aba Propriedades

Esta seção lista as configurações encontradas na aba **Propriedades** de Área de detecção de intrusão, na tarefa *Exibição de área*.

Na aba *Propriedades*, você pode visualizar as propriedades da área de detecção de intrusão conforme configuradas na *unidade de detecção de intrusão*.

NOTA: Esta página é somente leitura para áreas de detecção de intrusão (zonas) configuradas em unidades Bosch.

- **Nome físico:** Nome da área de detecção de intrusão (às vezes chamado de zona ou partição), como está configurado no painel de intrusão físico. Alterar o nome da entidade de área de detecção de intrusão não altera seu nome físico.
- **Unidade de detecção de intrusão:** Nome da entidade da unidade de detecção de intrusão (painel de intrusão) onde esta área está configurada.
- **Dispositivos:** Nome e descrição das entradas que definem esta área de detecção de intrusão.

Abas de configuração da unidade de detecção de intrusão

Esta seção lista as definições encontradas nas abas de configuração de Unidades de detecção de intrusão, na tarefa *Detecção de intrusão*.

Unidade de detecção de intrusão - Aba Propriedades

Na aba *Propriedades*, você pode configurar as opções específicas de hardware para esta unidade.

- **Limpar os registros após o download ser concluído:** Apague o registro do painel de intrusão assim que for baixado para o Security Center.
- **Tipo de interface:** O tipo de interface não pode ser alterado após a criação da entidade. Se você precisar alterar o tipo de interface, é necessário excluir a entidade e recriá-la.
  - **Host (somente interface IPv4):** Nome do host ou endereço IP do painel de intrusão.
  - **Porta:** Número da porta de conexão do painel de intrusão.
- **Sincronização automática:** Selecione essa opção para que o relógio no painel de intrusão seja sincronizado com o Security Center.
- **Sincronizar agora:** Sincronize o painel de intrusão com o Security Center agora.

Unidade de detecção de intrusão - Aba Periféricos

Na aba *Periféricos*, você pode visualizar os periféricos (pinos de entrada e relés de saída) conectados à unidade de detecção de intrusão.

- **Nome:** Nome dado ao dispositivo de E/S no Security Center.
- **Nome físico:** Nome físico do dispositivo.
- **ID lógico:** ID lógico dado ao dispositivo no Security Center.
- **Descrição:** Descrição dada ao dispositivo no Security Center.
- **Tipo de entrada (apenas entradas):** Tipo de entrada, conforme configurado no painel de intrusão.
  - **Indefinido:** A entrada não possui um tipo definido. Se você selecionar esta opção, a entrada é considerada como um tipo de entrada de *Perímetro*.
  - **Perímetro:** A entrada monitora o perímetro de uma área de detecção de intrusão.
  - **Interior:** A entrada monitora dentro da área de detecção de intrusão.
- **Tipo de contato (apenas entradas):** Estado padrão do contato.
  - **Opção normalmente:** O estado normal do contato de entrada é aberto.
  - **Normalmente fechado:** O estado normal do contato de entrada é fechado.

Unidade de LPR - Aba Propriedades

Esta seção lista as configurações encontradas na aba **Propriedades** da unidade de LPR, na tarefa *LPR*.

Na aba *Propriedades*, você pode visualizar informações de hardware e software sobre a unidade Sharp, como o endereço IP e a porta que está sendo usada. Você também pode associar uma lista de procurados específica ao Sharp, ou vincular a câmera LPR no Sharp a uma câmera *Omnicast*™, ou a própria câmera de contexto do Sharp.

- **Propriedades:** Exibe informações de hardware e software sobre a unidade Sharp:
  - **Endereço IP:** Endereço IP da unidade Sharp.
  - **Porta:** Porta usada pelo *LPR Manager* para comunicar com a unidade Sharp.
  - **Versão:** Versão do software AutoVu *PlateReaderServer* em execução na unidade.
  - **Tipo:** Versão do hardware da unidade.
  - **Número de série:** Número de série da unidade instalado de fábrica.
  - **Versão do Updater Service:** Exibe a versão do Updater Service em execução no Sharp.
  - **Versão do firmware:** Exibe a versão do firmware em execução no Sharp.
- **Configuração de rede (apenas Sharps fixos):**
  - **Endereço IP:** O endereço IP do Sharp fixo. O LPR Manager busca a unidade Sharp neste endereço IP.
  - **Atribuição:** Como a unidade Sharp foi registrada no Security Center:
    - **Passivo:** O LPR Manager descobriu a unidade Sharp na rede usando a porta de descoberta.
    - **Ativo:** O Sharp foi adicionado manualmente no Security Center Config Tool.
  - **Porta:** Porta usada pelo *LPR Manager* para comunicar com a unidade Sharp fixa.
- **Dispositivos:** Vincule a câmera LPR a uma câmera Omnicast™.
- **Associação de arquivos:** Selecione como o Sharp se comporta com listas de procurados:
  - **Herdar da função LPR Manager:** O Sharp usa as listas de procurados associadas ao seu LPR Manager pai. Esta é a configuração padrão.
  - **Específico:** Associe listas de procurados específicas à unidade Sharp. Isso permite que você crie Eventos causa-efeito no Security Desk acionados por essa lista de procurados específica. Por exemplo, se você estiver usando o Sharp para permitir o acesso a um estacionamento, você colocaria as placas de veículo em uma lista de procurados e depois associaria essa lista de procurados ao Sharp.

NOTA: Para reiniciar um Sharp fixo, clique no botão *Reiniciar* encontrado na barra de ferramentas da parte inferior do espaço de trabalho de Config Tool. Se o botão Reiniciar não estiver visível, faça logon na Página de configuração do Portal Sharp e selecione *Aceitar pedidos de reinício remotos*. Para obter mais informações, consulte o *Guia do Administrador Sharp*.

Abas de configuração de macro

Esta seção lista as configurações encontradas nas abas de configuração de macro, na tarefa *Sistema*.

Macro - Aba Propriedades

Na aba *Propriedades*, você pode escrever seu código C# usando um editor de texto básico.

- **Importar de arquivo:** Clique neste botão para importar o código-fonte de um arquivo.
- **Verificando a sintaxe:** Clique neste botão para validar o código C#. Se forem encontrados erros no código, eles serão listados em uma caixa de diálogo com os números de linha e coluna onde eles são encontrados.

Macro - aba Contexto de execução padrão

Na aba *Contexto de execução padrão* você pode visualizar as variáveis de contexto (parâmetros de entrada) definidas em sua macro.

Grupo de monitores - Aba Monitores

Esta seção lista as configurações encontradas na aba **Monitores** do grupo de monitores, na tarefa *Alarme*.

Na aba *Monitores*, você pode adicionar vários monitores analógicos ao grupo de monitores. Mais tarde, quando você cria alarmes, você pode adicionar um grupo de monitores e seus membros como destinatários do alarme.

Rede - Aba Propriedades

Esta seção lista as configurações encontradas na aba **Propriedades** de rede, na tarefa *Visualização de rede*.

Na aba **Propriedades**, você pode definir as características da rede e as informações de roteamento.

- **Capacidades:** Capacidades de transmissão de dados para o fluxo de vídeo ao vivo na rede.
  - **TCP Unicast:** Comunicação (individual) Unicast usando protocolo TCP é o modo de comunicação mais comum de comunicação. É suportado por todas as redes de IP, mas também é o método menos eficiente de transmitir vídeo.
  - **UDP Unicast:** Comunicação Unicast (individual) usando protocolo UDP. Devido ao fato de o UDP ser um protocolo sem conexão, funciona muito melhor para transmissão de vídeo ao vivo. Quando o tráfego de rede está ocupado, o UDP tem muito menos probabilidade de causar vídeos intermitentes do que o TCP. Uma rede que suporta UDP unicast necessariamente suporta TCP unicast.
  - **Multicast:** Multicast é o método de transmissão mais eficiente para vídeo ao vivo. Permite que a transmissão de vídeo seja transmitida uma vez pela rede para ser recebida por quantos destinos forem necessários. O ganho pode ser muito significativo se houverem muitos destinos. Uma rede que suporta multicast necessariamente suporta UDP unicast e TCP unicast.
    NOTA: Multicast necessita de roteadores e interruptores especializados. Certifique-se de confirmar isso com seu departamento de TI antes de definir as capacidades para multicast.
- **Prefixo de endereço IPv4:** *IPv4* tem dois modos de exibição. Clique em para selecionar o modo de exibição desejado.
  - **Exibição em subnet:** Esse modo exibe a máscara de subnet IPv4 como quatro bytes.
  - **Bloqueio de tela CIDR:** O modo Classless Inter-Domain Routing (CDIR) exibe a máscara de subnet IPv4 como número de bits.
- **Prefixo de endereço IPv6:** Prefixo de endereço de IP versão 6 para a rede. Sua rede deve suportar *IPv6* e você deve ativar a opção *Usar IPv6* em todos os seus servidores que usam o Server Admin.
- **Servidores públicos:** Você só precisa especificar o servidor proxy quando *Tradução de Endereço de Rede* (NAT) é usada entre as suas redes configuradas. O servidor de proxy deve ser um servidor conhecido ao seu sistema e deve ter uma porta pública e endereço configurado no seu firewall.
- **Rotas:** Lista as rotas entre cada duas redes no seu sistema e as capacidades de rota.

Tópicos relacionados

Servidor - Aba Propriedades na página 1029

Comportamento de saída - Aba Propriedades

Esta seção lista as configurações encontradas na aba **Propriedades** do comportamento de saída, na tarefa *Sistema*.

Na aba *Propriedades*, você pode configurar o padrão do sinal de saída.

- **Tipo de saída:** Escolha o tipo de saída.
  - **Estado:** Define o estado do circuito para abrir ou fechar.
  - **Pulso:** Define um pulso a ser gerado.
  - **Periódico:** Define uma saída cíclica a ser gerada.
- **Atraso:** O atraso antes da geração do pulso ou da saída periódica.
- **Duração:** A duração (em milissegundos) do pulso.
- **Infinita:** Selecione essa opção se o comportamento periódico continuar até que seja solicitado a parar por outro comportamento de saída.
- **Ciclo de trabalho:** O índice da largura do pulso do padrão de sinal de saída dividido pelo período.
- **Período:** O tempo para um ciclo completo do padrão de sinal de saída.

Abas de configuração de regra de horas extras

Esta seção lista as configurações encontradas nas abas de configuração de regras de horas extras, na tarefa *LPR*.

Regra de acesso - Aba Propriedades

Na aba *Propriedades*, você pode configurar as regras de estacionamento fiscalizadas por esta regra de horas extras.

- **Cor:** Atribui uma Cor para a regra de horas extras. Quando você seleciona a regra de tempo extra no Genetec Patroller™, as leituras de placas no mapa e a tela de ocorrências são exibidas nessa cor.
- **Posição de estacionamento do veículo:** Esta configuração diz ao Genetec Patroller™ o conjunto de parâmetros calibrados a serem usados para a leitura ótima das imagens das rodas, com base na posição de estacionamento dos veículos: paralela ou angulada (45 graus).
- **Hora extra ao longo prazo:** Use esta opção para estacionamento a longo prazo, quando os veículos podem estacionar no mesmo espaço por mais de 24 horas. Quando a hora extra ao longo prazo é selecionada, o limite de tempo de estacionamento é especificado em dias (2 a 5 dias).
- **Controle de estacionamento:** Tipo de área de estacionamento restrito que se aplica ao limite de tempo:
  - **Mesma posição.:** Um veículo está estacionado em horas extras se estacionar no mesmo local além do limite de tempo especificado.
  - **Distrito:** Um veículo está estacionado em horas extras se estiver estacionado em qualquer lugar dentro de um distrito da cidade (uma área geográfica) além do prazo especificado.
  - **Fachada (2 lados):** Um veículo está estacionado em horas extras se estiver estacionado em ambos os lados de uma estrada entre duas interseções além do limite de tempo especificado.
- **Regulamento:** Define parâmetros do limite de tempo de estacionamento:
  - **Limite de horário:** Digite quanto tempo em horas e minutos um veículo pode estacionar.
  - **Período de tolerância:** Adicione tempo extra além do *Limite de horário* antes de disparar uma ocorrência de horas extras. Por exemplo, se você definir um limite de tempo de 10 minutos e um período de tolerância de 5 minutos, o Genetec Patroller™ dará a ocorrência após 15 minutos.
  - **Dias aplicáveis:** Selecione em quais dias aplicar o *Limite de horário*.
  - **Horas aplicáveis:** Selecione em qual hora do dia aplicar o *Limite de horário*.

Regra de horas extras - Aba Zonas

Na aba *Zonas*, você pode configurar a área de estacionamento onde esta regra de hora extra deve ser fiscalizada. A aba Estacionamento exibe um mapa, no qual você pode adicionar um estacionamento, definir o número de espaços no estacionamento e então desenhar um polígono sobre o mapa para representar o estacionamento físico. O número de espaços no estacionamento é usado para calcular a porcentagem de ocupação de estacionamento naquela área.. Para obter mais informações sobre como essa informação está sendo usada no relatório de *Ocupação da zona*, consulte o *Guia do usuário Security Desk*.

NOTA: Você pode adicionar múltiplos estacionamentos a um mapa.

Instalação de estacionamento - Aba Propriedades

Esta seção lista as configurações encontradas na aba **Propriedades** do de estacionamento, na tarefa *LPR*.

Na aba *Propriedades*, você pode atribuir um LPR Manager à instalação de estacionamento e configurar seus setores e linhas para a rota de captura da placa de licença.

- **AutoVu™LPR Manager:** Selecione o LPR Manager responsável por criar e gerenciar o *inventário de placas de veículos* para este estacionamento. Somente descarregamentos de veículos de patrulha MLPI gerenciados pelo mesmo LPR Manager são usados para construir o inventário para esta instalação de estacionamento.
- **Configuração:** Lista de setores, linhas e contagem de espaço do estacionamento.
- **Rota:** Rota de coleta de placas de licença seguida pelas unidades MLPI responsáveis pela coleta de placas para o inventário. A rota é baixada pelos veículos de patrulha e dispositivos portáteis atribuídos a esta instalação de estacionamento.

Partição - Aba Propriedades

Esta seção lista as configurações encontradas na aba **Propriedades** da Partição, na tarefa *Gerenciamento de usuários*.

Na aba *Propriedades*, você pode visualizar e gerenciar o conteúdo da partição.

- **Membros:** Lista de membros que fazem parte da partição.
- **Mostrar:** Filtra a lista de membros por tipo de entidade.
- **Divisão global:** Ative esta opção para compartilhar a partição com outros sistemas independentes do Security Center (usando o Gerenciamento global de titulares de cartão).

  NOTA: Não é possível compartilhar a partição *raiz*.

Genetec Patroller™ - Aba Propriedades

Esta seção lista as configurações encontradas na aba **Propriedades** do Genetec Patroller™, na tarefa *LPR*.

Na aba *Propriedades*, você pode ver informações sobre o computador que hospeda a entidade Genetec Patroller™ (você não pode editar as propriedades do Genetec Patroller™). Você também pode definir o gerenciamento de som, configurações de buffer de confirmação e um retardo das ocorrências para a unidade Genetec Patroller™.

- **Propriedades:** Lista as propriedades do computador de bordo do Genetec Patroller™.
  - **Endereço de IP:** Endereço IP do computador do Genetec Patroller™.
  - **Versão:** Número de versão do aplicativo Genetec Patroller™.
  - **Tipo:** Tipo(s) de instalação do Genetec Patroller™.
  - **Número de série.:** Número de série do Genetec Patroller™.
  - **Nome da máquina:** Nome do computador do Genetec Patroller™.
  - **Versão do Updater Service:** Exibe a versão do serviço de atualização executado no computador do Genetec Patroller™.
- **Associação de arquivo:** Selecione como o Genetec Patroller™ se comporta com listas de procurados e/ou listas de autorização.
  - **Herdar da função LPR Manager:** O Genetec Patroller™ usa as listas de procurados e listas de autorizações associadas ao seu LPR Manager pai. Esta é a configuração padrão.
  - **Específico:** Associe listas de procurados ou listas de autorizações específicas à unidade Genetec Patroller™ em vez de ao LPR Manager. Se posteriormente você quiser mover a entidade Genetec Patroller™ para outro LPR Manager em seu sistema, a lista de procurados ou de autorizações acompanhará.
- **Gerenciamento de sons:** Configure o Genetec Patroller™ para reproduzir um som ao ler uma placa e/ou ao gerar uma ocorrência e selecione se sons devem ser tocados mesmo quando o Genetec Patroller™ está minimizado.
  - **Tocar som por alerta:** Toca um som quando o Genetec Patroller™ gera uma ocorrência.
  - **Tocar som por leitura:** Toca um som quando o Genetec Patroller™ lê uma placa.
  - **Tocar sons mesmo quando minimizado:** Permita a reprodução de sons mesmo quando a janela do Genetec Patroller™ está minimizada.
- **Buffer de confirmação:** Especifique uma restrição de buffer que limite a quantidade de ocorrências que podem ser ignoradas (não confirmadas ou rejeitadas) antes que o Genetec Patroller™ comece automaticamente a rejeitar *todas* as ocorrências subsequentes. Você também pode escolher (por prioridade) quais listas de procurados devem cumprir esta restrição
  - **Contagem de rejeição:** Quantos alertas não confirmados são permitidos.
  - **Prioridade de rejeição:** Quando você cria uma entidade de lista de procurados, você pode especificar uma prioridade para aquela lista de procurados. Esta definição diz ao Genetec Patroller™ quais listas de procurados devem atender a restrição do buffer.
- **Lista de procurados e autorizações:** Especifique o *Atraso de ocorrência duplicada* que informa o Genetec Patroller™ para ignorar múltiplas ocorrências da mesma placa durante o período de atraso. Por exemplo, se você definir um atraso de 10 minutos, não importa quantas vezes o Genetec Patroller™ leia a mesma placa durante esses 10 minutos, ele gerará apenas uma ocorrência.

Autorização - Aba Propriedades

Esta seção lista as configurações encontradas na aba **Propriedades** de Autorização, na tarefa *LPR*.

Na aba *Propriedades*, você pode configurar a análise do arquivo de dados de origem da autorização.

- **Caminho:** Caminho para o arquivo de texto de origem da autorização, que contém os dados da autorização, como números da placa de licença e outras informações relacionadas ao veículo. O arquivo de texto de origem pode ser localizado na unidade local do computador do LPR Manager (por exemplo, a unidade C) ou em uma unidade de rede acessível a partir do computador LPR Manager.
- **Usar delimitadores:** Indica ao Security Center que os campos do arquivo de lista de autorizações variam em comprimento e indica o caractere usado para separar cada campo no arquivo. Por padrão, *Usar delimitadores* está definido como *Ligado* e o delimitador especificado é *ponto e vírgula* (;). Se o seu arquivo de lista de autorizações for feito de campos de comprimento fixo, configure *Usar delimitadores* como *Desligado*.
- **Visível no editor:** Permite que um usuário edite a lista de procurados ou lista de autorizações usando a tarefa do editor da lista de procurados ou da lista de autorizações.
- **Atributos:** Informa ao Security Center o nome e a ordem dos campos (atributos) no arquivo de texto de origem.

Abas de configuração de restrição de autorização

Esta seção lista as configurações encontradas nas abas de configuração de restrição de autorização, na tarefa *LPR*.

Restrição de autorização - Aba Propriedades

Na aba *Propriedades*, você pode configurar as restrições para as permissões individuais que se aplicam à área de estacionamento representada pela regra.

- **Cor:** Cor usada para representar a restrição de autorização no Security Desk. No Genetec Patroller™, as restrições de autorização sempre são verdes para ocorrências de autorizações normais ou azuis para ocorrências de autorizações compartilhadas. Uma leitura é exibida como um ícone de forma triangular na cor selecionada no mapa, quando uma restrição de autorização está em vigor. Quando uma leitura viola uma das restrições, o ícone é circundado por um anel vermelho. Isso indica um alerta de autorização.
- **Autorizações:** As autorizações às quais a restrição de tempo se aplica.
  - *Todo mundo***:** O estacionamento fica disponível para todos, independentemente deles terem ou não uma autorização. Nenhuma restrição é fiscalizada durante o período especificado. Esta restrição é usada com outras restrições como uma substituição temporária. Por exemplo, se uma universidade estiver promovendo um jogo, o estacionamento poderá ser disponibilizado para todos durante o jogo em vez de titulares de autorizações específicas.
  - *Nenhuma autorização***:** Somente veículos sem autorizações podem estacionar. Por exemplo, você pode usar esse tipo de restrição para reservar uma zona para o estacionamento dos visitantes. Um leitura de placa que corresponda a qualquer uma das autorizações baixadas para o Genetec Patroller™ aciona uma ocorrência.
  - *Todas as autorizações***:** Somente veículos com autorização podem estacionar. Um leitura de placa que não corresponda a qualquer uma das autorizações baixadas para o Genetec Patroller™ aciona uma ocorrência.
  - *Autorizações específicas***:** Somente veículos que tenham uma ou mais das autorizações especificadas podem estacionar. Um leitura de placa que não corresponda a nenhuma das autorizações especificadas levanta um alerta.
- **Dias:** Dias da semana quando o estacionamento é permitido.
- **Horas:** Horários durante o dia quando o estacionamento é permitido.
- **Validade:** Datas quando o estacionamento é permitido.

Restrição de autorização - Aba Zonas

Na aba *Zonas*, você pode configurar a área de estacionamento onde esta regra de hora extra deve ser fiscalizada. A aba Estacionamento exibe um mapa, no qual você pode adicionar um estacionamento, definir o número de espaços no estacionamento e então desenhar um polígono sobre o mapa para representar o estacionamento físico. O número de espaços no estacionamento é usado para calcular a porcentagem de ocupação de estacionamento naquela área.. Para obter mais informações sobre como essa informação está sendo usada no relatório de *Ocupação da zona*, consulte o *Guia do usuário Security Desk*.

NOTA: Você pode adicionar múltiplos estacionamentos a um mapa.

Agendamento - Aba Propriedades

Esta seção lista as configurações encontradas na aba **Propriedades**do Agendamento, na tarefa *Sistema*.

A aba *Propriedades* permite configurar as restrições de tempo que definem o cronograma.

Datas cobertas

Na seção *Datas cobertas*, você pode definir um padrão de data ou datas específicas a serem cobertas pelo cronograma.

- **Diariamente:** Define um padrão que se repete diariamente.
- **Semanalmente:** Define um padrão que se repete semanalmente. Cada dia da semana pode ter uma cobertura de tempo diferente. Esta opção não está disponível para agendamentos de crepúsculo.
- **Ordinal:** Define uma série de padrões que se repetem mensalmente ou anualmente. Cada padrão de data pode ter uma cobertura de tempo diferente. Por exemplo, no dia 1º de julho de cada ano, no primeiro domingo de cada mês, ou na última sexta-feira de outubro de cada ano.
- **Específico:** Define uma lista de datas específicas no futuro. Cada data pode ter uma cobertura de tempo diferente. Esta opção é ideal para eventos especiais que ocorrem apenas uma vez.

Cobertura do tempo

Na seção *Cobertura do tempo*, você pode definir quais são os períodos de tempo aplicáveis durante um dia de 24 horas.

- **Todos os dias:** Cobre o dia inteiro. Esta opção não está disponível para agendamentos de crepúsculo.
- **Faixa:** Abrange um ou vários períodos discretos no decorrer do dia. Por exemplo, das 9 h a 12 h e de 13 h a 17 h. Esta opção não está disponível para agendamentos vespertinos.
- **Diurno:** Cobre do nascer do sol ao pôr do sol. Esta opção está disponível somente para agendamentos de crepúsculo.
- **Noturno:** Cobre do pôr do sol ao nascer do sol. Esta opção está disponível somente para agendamentos de crepúsculo.

Tarefa agendada - Aba Propriedades

Esta seção lista as configurações encontradas na aba **Propriedades** da Tarefa agendada, na tarefa *Sistema*.

Na aba *Propriedades*, você pode configurar o padrão da tarefa agendada.

- **Status:** Ativar ou desativar a tarefa agendada.
  - **Recorrência:** Especifica com que frequência a tarefa agendada ocorre.
  - **Uma vez:** Executado uma vez em uma data e horário específicos.
  - **A cada minuto:** Executado a cada minuto.
  - **A cada hora:** Executado em um minuto específico de cada hora.
  - **Diariamente:** Executado em uma hora específica a cada dia.
  - **Semanalmente:** Executado em um horário específico em dias selecionados na semana.
  - **Na inicialização:** Executado na inicialização do sistema.
  - **Intervalo:** Executado em intervalos regulares que podem ser dias, horas, minutos ou segundos.
- **Ação:** Ação a ser executada no agendamento.
- **Parâmetros adicionais:** Informações adicionais necessárias, dependendo do tipo de ação selecionado.

Servidor - Aba Propriedades

Na aba **Propriedades** do servidor, você pode visualizar as configurações de rede definidas para este servidor no Server Admin.

NOTA: Todas as configurações de rede são somente leitura no Config Tool. Elas devem ser configurados no Server Admin, exceto quando o servidor está sendo executado no modo de compatibilidade com versões anteriores (5.2 ou anteriores), caso em que as configurações de rede são definidas no Config Tool.

- **Endereço público:** Endereço público deste servidor. Esta configuração aparece apenas se um endereço público estiver configurado no Server Admin.
  - **Porta:** Porta usada pelo serviço Genetec™ Server para escuta de comandos recebidos de outros servidores do Security Center no endereço público.
  - **Proxy:** Esta opção é ativada se o servidor for usado como servidor proxy para uma rede privada protegida por um firewall.
- **Endereços privados:** Lista de *endereços IP privados* usados para a comunicação entre servidores do Security Center. Somente os endereços privados ativados no Server Admin aparecem nesta lista.
  - **Porta:** Porta usada pelo serviço Genetec™ Server para escuta de comandos recebidos de outros servidores do Security Center nos endereços públicos.

  IMPORTANTE: Se o servidor estiver sendo executado no modo de compatibilidade com versões anteriores (5.2 ou anteriores), o primeiro endereço na lista de endereços privados deve corresponder às propriedades IPv4 da entidade de rede à qual o servidor pertence na tarefa Exibição de rede.

- **Comunicação segura:** Use esta seção para visualizar a atual *certificado de identidade* usada pelo servidor para comunicar com outros servidores do Security Center.
  - **Emitido para:** Objeto do certificado atual. Um *certificado auto-assinado* criado na instalação do software aparece no formato *GenetecServer-{MachineName}*.
  - **Emitido por:** Nome da *autoridade de certificação (CA — certificate authority)* que emitiu o certificado. O emissor e o objeto são os mesmos para certificados autoassinados.
  - **Válido de/até:** Período de validade do certificado atual.

  Clique em **Vizualizar** para abrir a caixa de diálogo e ver mais informações.

Tópicos relacionados

O que é o protocolo Transport Layer Security? na página 372
Rede - Aba Propriedades na página 1019
Server Admin - Página de visão geral na página 101
Server Admin - Página do servidor principal na página 104
Server Admin - Página Servidor de expansão na página 107

Plug-in de Ladrilho - Aba Propriedades

Esta seção lista as configurações encontradas na aba **Propriedades** do plug-in de Ladrilho, na tarefa *Exibição de área*.

Na aba *Propriedades*, você pode vincular a entidade de plug-in de ladrilho a um site ou a um arquivo .dll.

- **Página da web:** Digite um endereço da Web para vincular o plug-in de ladrilho.
- **Modificar:** Selecione um arquivo .dll para vincular o plug-in de ladrilho.

Abas de configuração do usuário

Esta seção lista as configurações encontradas nas guias de configuração Usuário, na tarefa *Gerenciamento de usuários*.

Usuário - Aba Propriedades

Na aba *Propriedades*, você pode configurar as informações pessoais e a senha do usuário.

- **Status:** Ative ou desativa o perfil de usuário. Um usuário não pode iniciar sessão quando seu perfil estiver desativado. Desativar o perfil de um usuário enquanto ele estiver conectado efetuará imediatamente o seu logoff.
- **Informações pessoais:** As informações pessoais de um usuário podem ser importadas do serviço de diretório da sua empresa.
  - **Nome e sobrenome:** Nome e sobrenome do usuário.
  - **Endereço de e-mail:** O endereço de e-mail do usuário. Pode ser usado para enviar e-mails, relatórios ou mensagens para o usuário.
- **Configurações de senha:** Todos os usuários precisam de uma senha para fazer logon no Security Center. O usuário deve ter o privilégio *Alterar a própria senha* para que as opções de senha sejam ativadas.
  - **Expira em:** Ative esta opção para forçar o usuário a mudar sua senha após um determinado número de dias.
  - **Alterar no próximo logon:** Ative esta opção para o Genetec Patroller™ ou o Security Desk para forçar o usuário a alterar sua senha na próxima vez que fizer o logon.
  - **Alterar senha:** Para alterar a senha de outra pessoa, você precisa ter o privilégio *Modificar propriedades do usuário*.
- **Nível de usuário:** Definir o nível de usuário. É um valor numérico atribuído aos usuários para restringir sua capacidade de realizar certas operações, como controlar uma câmera PTZ, visualizar a alimentação de vídeo de uma câmera ou ficar registrado quando é definido um nível de ameaça. O nível 1 é o nível de usuário mais alto, com mais privilégios.
  - **Herdado do pai:** O nível de usuário pode ser herdado de um grupo pai. Se o usuário tiver vários pais, o nível de usuário mais alto será herdado. Se o usuário não tiver um grupo pai, o nível de usuário mais baixo (254) será herdado. Você deve configurar a opção *Herdar do pai* como *Sobrescrever* para alterar esta configuração.
  - **Configurar sobreposições de PTZ:** Definir valores diferentes de nível de usuário para as câmeras PTZ selecionadas. Os valores de substituição permitem que você dê a este usuário maior ou menor prioridade sobre determinadas câmeras PTZ.

Usuário - aba Regras de acesso

Na aba *Direitos de acesso*, você pode visualizar e configurar os direitos de acesso do usuário a *partições*. Esta aba aparece apenas quando existem criações criadas pelo usuário no sistema.

- **Lista de partições:** Selecione uma partição para conceder direitos de acesso a um usuário: Os direitos de acesso sobre partições pai e filho podem ser configurados de forma independente. Os direitos de acesso herdados de grupos de usuários pai não podem ser revogados.
- **Administrador:** Selecione esta opção para conceder direitos administrativos completos sobre todas as entidades contidas nessa partição ao usuário, incluindo os direitos de criar e excluir usuários, grupos de usuários e partições filho.
- **Exibir os itens marcados ( ):** Clique para alternar a exibição entre mostrar apenas as partições selecionadas e todas as partições.

Usuário - Aba Privilégios

Na aba *Privilégios*, você pode visualizar e configurar os privilégios do usuário. Os privilégios de um usuário podem ser herdados de grupos de usuários pai.

- **Permitir:** O privilégio é concedido ao usuário.
- **Negar:** O privilégio é recusado ao usuário.
- **Indefinido:** Este privilégio deve ser herdado de um grupo de usuários principal. Se o usuário não for membro de nenhum grupo ou se o privilégio também estiver indefinido no grupo de usuários pai, o privilégio será negado.
- **Exceções:** Os privilégios básicos podem ser substituídos no nível da partição se o usuário estiver autorizado a acessar múltiplas partições. Somente os privilégios *Administrativo* e *Ação*, mais os privilégios sobre *tarefas públicas*, podem ser sobrescritos no nível de partição.
- **Configurações adicionais ( ):** Clique para visualizar comandos adicionais para modelos de privilégios.
  - **Aplicar modelo:** Selecione um dos modelos de privilégios para aplicar.
  - **Definir configuração para apenas leitura:** Defina todas os privilégios de configuração de entidades encontrados no grupo de *Privilégios administrativos* como *Visualizar propriedades*.
  - **Definir configuração para leitura e gravação:** Permita a modificação de todas as configurações de entidades, inclusive *Adicionar* e *Excluir*.

Usuário - aba Avançado

Na aba *Avançado*, você pode definir as configurações avançadas do usuário.

- **Configurações de logon:** Define as configurações de logon do usuário.
  - **Agendamento de logon de usuário:** Restringe o logon do usuário de acordo com os agendamentos. Um agendamento pode ser usado para permitir o logon do usuário ou para bloqueá-lo.
  - **Supervisor de logon de:** Lista os usuários cujos logons são supervisionados pelo usuário atual. Quando um usuário nesta lista precisa fazer logon no sistema, o usuário atual também deve fornecer seu nome de usuário e senha para completar o logon. Um usuário pode ter mais de um supervisor de logon.
  - **Limitar os logons simultâneos:** Define o número máximo de estações de trabalho nas quais um usuário pode fazer logon ao mesmo tempo. Este limite somente se aplica ao Security Desk. O Config Tool não é restringido por esta configuração.
  - **Auto-travamento:** Defina esta opção como **Ligado** para bloquear o usuário fora da sua sessão do Security Desk após um período de inatividade. Para retomar a sua sessão atual, o usuário deve digitar novamente a senha. Essa exigência pode ser herdada de um grupo de usuários pai. Você deve configurar a opção **Herdar do pai** como **Sobrescrever** para alterar esta configuração.
    NOTA: Se o usuário for autenticado através de ADFS com autenticação passiva, o usuário será desconectado e a sua sessão atual fechada ao invés de ficar bloqueada.
- **Configurações do Security Desk:** Configure o espaço de trabalho Security Desk do usuário.
  - **Lista de tarefas ativas:** Exibe as tarefas encontradas na lista de tarefas ativas do usuário.
  - **Ações instantâneas:** Exibe as *ações instantâneas* mapeadas para as teclas de função do teclado do PC (Ctrl+F1 até Ctrl+F12) quando este usuário está conectado ao Security Center usando o Security Desk.
  - **Permitir controle remoto sobre:** Lista as estações de trabalho do Security Desk que este usuário pode controlar remotamente usando a tarefa *Remoto* no Security Desk ou um teclado de CCTV. Você pode especificar quais estações de trabalho podem ser controladas por usuário, grupo de usuários ou estação de trabalho específica.
  - **Iniciar circulação de tarefas no logon:** Ative esta opção para que, na próxima vez que o usuário faça login a partir do Security Desk, o *ciclo de tarefas* comece automaticamente.

- **Configurações de segurança:** Configure o que o usuário pode ver no sistema.
  - **Limitar visualização de arquivo:** Ative esta opção para restringir a capacidade do usuário em visualizar vídeos arquivados aos últimos *n* dias. Este privilégio deve ser herdado de um grupo de usuários pai. Se o usuário tiver vários pais, a limitação mais restritiva será herdada. Se o usuário não tiver nenhum grupo pai, nenhuma restrição será imposta. Você deve configurar a opção *Herdar do pai* como *Sobrescrever* para alterar esta configuração.
  - **Embaralhar os nomes de entidades:** (Apenas usuários não administrativos) Ative esta opção para exibir o GUID da entidade no Security Desk e no Config Tool, em todos os lugares em que o nome da entidade deva ser exibido para este usuário. Esta opção também impede o usuário de atualizar os campos de nome da entidade no Config Tool.
- **Mapa padrão:** O mapa carregado por padrão quando o usuário abre a tarefa *Mapas*. Se nenhum for definido, o mapa padrão global configurado no nível de função Map Manager é usado.

Abas de configuração Grupo de usuários

Esta seção lista as configurações encontradas nas abas de configuração Grupo de usuários, na tarefa *Gerenciamento de usuários*.

Grupo de usuários - Aba Propriedades

Na aba *Propriedades*, você pode visualizar e configurar os membros do grupo de usuários.

- **Endereço de e-mail:** Endereço de e-mail que é usado por todos os membros do grupo. As informações podem ser importadas do serviço de diretório da sua empresa. O endereço de e-mail pode ser usado para enviar e-mails, relatórios ou mensagens para os usuários.
- **Nível de usuário:** Definir o nível de usuário. É um valor numérico atribuído aos usuários para restringir sua capacidade de realizar certas operações, como controlar uma câmera PTZ, visualizar a alimentação de vídeo de uma câmera ou ficar registrado quando é definido um nível de ameaça. O nível 1 é o nível de usuário mais alto, com mais privilégios.
  - **Herdado do pai:** O nível de usuário pode ser herdado de um grupo pai. Se o usuário tiver vários pais, o nível de usuário mais alto será herdado. Se o grupo de usuários não tiver um grupo pai, o nível de usuário mais baixo (254) será herdado. Você deve configurar a opção *Herdar do pai* como *Sobrescrever* para alterar esta configuração.
  - **Configurar sobreposições de PTZ:** Definir valores diferentes de nível de usuário para as câmeras PTZ selecionadas. Os valores de substituição permitem que você dê a este grupo de usuários maior ou menor prioridade sobre determinadas câmeras PTZ.
- **Membros:** Lista de membros do grupo de usuários. Por padrão, os membros herdam os privilégios e os direitos de partições do grupo de usuários.

Grupo de usuários - aba Direitos de acesso

Na aba *Direitos de acesso*, você pode visualizar e configurar os direitos de acesso compartilhados pelos membros do grupo de usuários. Esta aba aparece apenas quando existem criações criadas pelo usuário no sistema.

- **Lista de partições:** Selecione uma partição para conceder direitos de acesso a um grupo de usuários: Os direitos de acesso sobre partições pai e filho podem ser configurados de forma independente. Os direitos de acesso herdados de grupos de usuários pai não podem ser revogados.
- **Administrador:** Selecione esta opção para conceder direitos administrativos completos sobre todas as entidades contidas nessa partição ao grupo de usuários, incluindo os direitos de criar e excluir usuários, grupos de usuários e partições filho.
- **Exibir os itens marcados ( ):** Clique para alternar a exibição entre mostrar apenas as partições selecionadas e todas as partições.

Grupo de usuários - Aba Privilégios

Na aba *Privilégios*, você pode visualizar e configurar os privilégios do grupo de usuários. Os privilégios de um grupo de usuários podem ser herdados pelos membros do grupo ou podem ser herdados de outros grupos de usuários.

- **Permitir:** O privilégio é concedido ao grupo de usuários.
- **Negar:** O privilégio é negado ao grupo de usuários.
- **Indefinido:** Este privilégio deve ser herdado de um grupo de usuários principal. Se o grupo de usuários não for membro de nenhum outro grupo ou se o privilégio também estiver indefinido no grupo de usuários pai, o privilégio será negado.

- **Exceções:** Os privilégios básicos podem ser substituídos no nível da partição se o grupo de usuários estiver autorizado a acessar múltiplas partições. Somente os privilégios *Administrativo* e *Ação*, mais os privilégios sobre *tarefas públicas*, podem ser sobrescritos no nível de partição.
- **Configurações adicionais ( ):** Clique para visualizar comandos adicionais para modelos de privilégios.
  - **Aplicar modelo:** Selecione um dos modelos de privilégios para aplicar.
  - **Definir configuração para apenas leitura:** Defina todas os privilégios de configuração de entidades encontrados no grupo de *Privilégios administrativos* como *Visualizar propriedades*.
  - **Definir configuração para leitura e gravação:** Permita a modificação de todas as configurações de entidades, inclusive *Adicionar* e *Excluir*.

Grupo de usuários - aba Avançado

Na aba *Avançado*, você pode definir as configurações avançadas comuns para os membros do grupo.

- **Configurações de logon:** Define as configurações de logon comuns para os membros do grupo.
  - **Supervisor de logon de:** Lista os usuários cujos logons são supervisionados pelos membros do grupo de usuários atual. Quando os usuários desta lista precisam fazer logon no sistema, qualquer membro desse grupo de usuários pode ajudá-los a completar seu logon.
  - **Auto-travamento:** Defina esta opção como **Ligado** para bloquear membros do grupo de usuários fora da sua sessão do Security Desk após um período de inatividade. Para retomar a sua sessão atual, o usuário deve digitar novamente a senha. Essa exigência pode ser herdada de um grupo de usuários pai. Você deve configurar a opção **Herdar do pai** como **Sobrescrever** para alterar esta configuração. **NOTA:** Se o usuário for autenticado através de ADFS com autenticação passiva, o usuário será desconectado e a sua sessão atual fechada ao invés de ficar bloqueada.
- **Configurações do Security Desk:** Defina as configurações comuns do Security Desk para os membros do grupo.
  - **Permitir controle remoto sobre:** Lista as estações de trabalho do Security Desk que os membros deste grupo de usuários podem controlar remotamente usando a tarefa *Remoto* no Security Desk ou um teclado de CCTV. Você pode especificar quais estações de trabalho podem ser controladas por usuário, grupo de usuários ou estação de trabalho específica.
- **Limitar visualização de arquivo:** Ative esta opção para restringir a capacidade do grupo de usuários em visualizar vídeos arquivados aos últimos *n* dias. Este privilégio deve ser herdado de um grupo de usuários pai. Se o grupo de usuários tiver vários pais, a limitação mais restritiva será herdada. Se o grupo de usuários não tiver nenhum grupo pai, nenhuma restrição será imposta. Você deve configurar a opção *Herdar do pai* como *Sobrescrever* para alterar esta configuração.

Unidade de vídeo - Aba Identidade

Esta seção lista as configurações encontradas na aba **Identidade** de Unidade de vídeo, na tarefa *Vídeo*.

Na aba *Identidade*, é possível visualizar informações específicas do hardware, além das informações de entidade padrão (nome, descrição, ID lógico etc.).

- **Fabricante:** Fabricante da unidade de vídeo.
- **Tipo de produto:** Modelo da unidade de vídeo.
- **Versão do firmware:** Versão de firmware atual instalada na unidade de vídeo.
- **Proposta:** Exibe a versão de firmware recomendada. Se a versão de firmware for a mesma que a versão proposta, exibirá *Atualizado*.
- **Atualizar (☢):** Atualiza o firmware na unidade de vídeo.
- **Áudio:** Indica se a unidade de vídeo suporta áudio.
- **SSL:** Indica se a unidade de vídeo é compatível com o protocolo *SSL* (Secure Socket Layer).

Unidade de vídeo - Aba Propriedades

Esta seção lista as configurações encontradas na aba **Propriedades** de Unidade de vídeo, na tarefa *Vídeo*.

Na aba *Propriedades*, você pode configurar as informações exigidas pelo Archiver para se conectar a esta unidade e outras propriedades de transmissão de dados. Essas configurações variam de um fabricante para outro. Opções adicionais podem estar disponíveis, dependendo do tipo de unidade.

- **Endereço de IP:** Define o endereço IP da unidade de vídeo.
- **Obter configurações de rede dinamicamente (DHCP):** Selecione esta opção para que o endereço IP seja atribuído dinamicamente pelo servidor DHCP (protocolo de configuração de host dinâmico).

  NOTA: Não use esta opção, a menos que seu servidor DHCP esteja configurado para sempre atribuir o mesmo endereço IP ao mesmo dispositivo.
- **Configurações específicas:** Selecione esta opção para inserir um valor fixo. Este é o endereço IP que você digitou quando criou inicialmente a entidade da unidade de vídeo. É necessário preencher os seguintes campos:
  - *IP local*. Endereço IP fixo.
  - *Máscara de sub-rede*. A máscara de sub-rede informa a unidade com a qual os periféricos podem se comunicar diretamente. Qualquer coisa que não pertença à mesma sub-rede deve passar pelo Gateway.
  - *Gateway*. Endereço IP do gateway. Deve estar na mesma sub-rede da unidade.
- **Porta de comando:** A porta usada pelo Archiver para se conectar à unidade de vídeo. A porta de comando às vezes é chamada de porta HTTP por alguns fabricantes.
- **Porta de descoberta:** A porta usada para descoberta automática. Nem todos os fabricantes suportam esse recurso.
- **porta VSIP:** (Somente para unidades Verint) Em unidades Verint, tanto a porta de comando como a porta de descoberta são substituídas pela *Porta VSIP*.
- **Autenticação:** Credenciais usadas pelo Archiver para se conectar à unidade de vídeo.
  - **Login inicial:** Selecione esta opção para que o Archiver use as credenciais definidas na extensão do fabricante da unidade.
  - **Específico:** Selecione esta opção para que o Archiver use credenciais específicas para se conectar a esta unidade. Os campos que você precisa preencher dependem do fabricante da unidade.
  - **Usar comunicação segura:** Selecione esta opção para usar comunicação *HTTPS* em vez de HTTP (padrão).
- **Taxa de transferência de bits:** Use esta opção para limitar a taxa de bits máxima permitida para esta unidade. Definir um limite para a taxa de bits ajuda a evitar que uma unidade use toda a largura de banda disponível na rede.
- **Habilitar UPnP:** Selecione esta opção para ativar o protocolo UPnP (Universal Plug and Play). Desative o UPnP se você não quiser que a unidade seja descoberta por outros aplicativos do Windows.
- **Habilitar Bonjour:** Selecione esta opção para ativar o protocolo Bonjour. Desative o Bonjour se você não estiver usando rede de configuração zero.
- **Habilitar endereço link-local:** Selecione esta opção para ativar o uso de endereço link-local.
- **Tipo de conexão do fluxo de evento:** Selecione o tipo de conexão (HTTP ou TCP) usado para enviar eventos. O uso de TCP é obrigatório. Selecione HTTP se houver um firewall entre o Archiver e a unidade.
- **Eventos de aplicativos:** (Somente Axis) Lista de aplicativos ACAP instalados na unidade. Selecione os aplicativos que deseja ativar.

NOTA: Para habilitar o aplicativo AXIS Video Motion Detection (VMD), você deve selecionar a opção **Usar detecção de movimento do aplicativo da câmera** na aba *Detecção de movimento* da câmera.

Unidade de vídeo - Aba Periféricos

Esta seção lista as configurações encontradas na aba **Periféricos** da unidade de vídeo, na tarefa *Vídeo*.

Na aba *Periféricos*, você pode visualizar todos os dispositivos periféricos (entradas/saídas, codificadores/decodificadores de áudio) encontrados na unidade que não são explicitamente mostrados como entidades, como *codificadores de vídeo* ou *decodificadores de vídeo*.

- **Estado do Periférico (LED):**
  - Verde ( ): Periférico ativo.
  - Vermelho ( ): Periférico desativado pelo usuário.
  - Amarelo ( ): Ativação do periférico em progresso.
    NOTA: Se o LED permanecer amarelo, isso indica que o periférico não é suportado ou está com problemas, caso em que é recomendado desativá-lo.
- **Nome:** Nome lógico. É o mesmo que o nome físico por padrão.
- **ID lógico:** Identificador lógico.
- **Descrição:** Descrição do serviço:

Você também pode modificar os dispositivos periféricos selecionados.

- **Editar o item ( ):** Altera as configurações do dispositivo periférico selecionado.
- **Ativar/Desativar itens selecionados (/):** Ativar ou desativar os dispositivos periféricos selecionados.

Configurações do relé de saída

A configuração específica para relés de saída é a seguinte:

- **Modo padrão:** Estado padrão do relé de saída.
  - **Opção normalmente:** O estado normal do contato de saída é aberto.
  - **Normalmente fechado:** O estado normal do contato de saída é fechado.

Configurações de alto-falantes

As configurações específicas para alto-falantes (dispositivos *decodificadores de áudio*) são as seguintes:

- **Volume:** Nível de volume desejado (0 para mudo, 100 equivale ao volume máximo).
- **Porta UDP:** Número da porta usada quando o tipo de conexão é unicast UDP.
- **Tipo de conexão:** Tipo de conexão usado entre a unidade e o Archiver para este decodificador de áudio.

Configurações de microfone

As configurações específicas para microfones (dispositivos *codificadores de áudio*) são as seguintes:

- **Formato de dados:** Formato de compressão de áudio.
- **Tipo de entrada:** Tipo de origem de entrada.
  - **Entrada de linha:** Usado para origem pré-amplificada.
  - **Entrada de Microfone:** Use isso se o microfone estiver diretamente conectado à unidade. Nesse caso, o sinal é amplificado pelo hardware.
  - **Interno:** Usa microfones integrados à unidade.

- **Sensibilidade:** Nível de amplificação desejado (padrão = 68). Quanto menor o nível, menos sensível é o microfone ao ruído ambiente, mas o nível da gravação também será menor.
- **Porta UDP:** Número da porta usada quando o tipo de conexão é unicast UDP.
- **Tipo de conexão:** Tipo de conexão usado entre a unidade e o Archiver para este codificador de áudio.
- **Endereço multicast:** O endereço *multicast* e o *número da porta* são atribuídos automaticamente pelo sistema quando a unidade de vídeo é descoberta. Cada codificador de áudio recebe um endereço multicast diferente com um número de porta fixa. Esta é a configuração mais eficiente.

Abas de configuração de zona virtual

As zonas virtuais são controladas pela função Zone Manager. As zonas virtuais são usadas para combinar entradas e disparar saídas que pertencem a diferentes unidades de diferentes tipos. As zonas virtuais podem ser armadas e desarmadas no Security Desk ou usando as ações *Armar zona* e *Desarmar zona*.

Zona virtual - aba Propriedades

Clique na aba **Propriedades** para configurar as entradas que definem esta zona e defina como elas são avaliadas.

- **Gerenciador de Zona:** Função Zone Manager que controla a zona virtual.
- **Entradas:** Entradas combinadas para avaliar o estado de zona.
- **Operador:** Operador lógico usado para combinar os estados de entrada para avaliar o estado de zona.
- **Eventos associados:** Eventos representando os estados de zonas. Selecione *Nenhum* caso um estado de zona deva ser ignorado.
  - **Estado normal:** Quando a combinação de entradas resulta em zero (0).
  - **Estado ativo:** Quando a combinação de entradas resulta em um (1).
  - **Estado anormal:** Exige ter pelo menos uma entrada supervisionada. A zona fica no estado de *Problema* quando pelo menos uma das entradas está no estado *Problema*. O estado *Problema* supera todos os outros estados.
  - **Limite de reativação:** O período de tempo durante o qual o mesmo evento não deve ser acionado novamente.

Zona virtual - aba Armamento

Clique na aba **Armamento** para configurar a origem de armamento de sua zona e seu comportamento de armamento.

- **Colocando origem em atenção:** Seleciona os agendamentos correspondentes aos períodos em que a zona fica armada.
- **Atrasos:** Atrasos opcionais que dão tempo para que você abandone o local após armar a zona e tempo para desarmar a zona após o acionamento de um sensor.
  - **Atraso de armamento:** Duração (mm:ss) que você deseja entre o tempo em que a zona é armada e o tempo em que os disparos de evento se tornam ativos.
  - **Atraso na entrada:** Duração (mm:ss) que você deseja entre o tempo em que o sensor de entrada é disparado e o tempo em que os eventos são disparados. Esta opção permite desarmar a zona antes de disparar os relés de saída.

52

Tipos de função

Esta seção inclui os seguintes tópicos:

- "Abas de configuração do Access Manager" na página 1043
- "Abas de configuração do Active Directory" na página 1045
- "Active Directory Federation Services - Aba Propriedades" na página 1047
- "Archiver - Aba Configurações padrão de câmera" na página 1048
- "Archiver - Aba Extensões" na página 1050
- "Archiver - Aba Recursos" na página 1053
- "Archiver auxiliar - Aba Gravação da câmera" na página 1056
- "Archiver auxiliar - Aba Câmeras" na página 1057
- "Archiver auxiliar - Aba Recursos" na página 1058
- "Abas de configuração do Directory Manager" na página 1061
- "Abas de configuração do Global Cardholder Synchronizer" na página 1063
- "Abas de configuração do Health Monitor" na página 1064
- "Abas de configuração do Intrusion Manager" na página 1065
- "LPR Manager - Aba Propriedades" na página 1066
- "LPR Manager - Aba Recursos" na página 1074
- "Abas de configuração do Map Manager" na página 1075
- "Abas de configuração do Media Gateway" na página 1076
- "Abas de configuração do Media Router" na página 1077
- "Abas de configurações Omnicast Federation" na página 1079
- "Abas de configuração do Gerenciador de relatórios" na página 1080
- "Abas de configuração do Security Center Federation" na página 1081
- "Abas de configuração Web-based SDK" na página 1082
- "Abas de configuração do Web Client Server" na página 1083
- "Abas de configuração do Zone Manager" na página 1084

Abas de configuração do Access Manager

Você define as configurações da função Access Manager a partir da visualização **Funções e unidades** da tarefa *Controle de acesso* na Security Center do Config Tool.

Access Manager - Aba Propriedades

Clique na aba **Propriedades** para definir as configurações gerais do Access Manager.

- **Manutenção de eventos:** Especifique quanto tempo você deseja manter os eventos no banco de dados do Access Manager antes de serem excluídos. O evento de controle de acesso é usado para relatórios e fins de manutenção (inclui eventos relacionados a portas, elevadores, áreas e outras entidades do controle de acesso).
  - **Indefinidamente:** Manter os eventos até que sejam excluídos manualmente.
  - **Por:** Selecione o número de dias para o período de retenção.

  CUIDADO: Se estiver usando o mecanismo de banco de dados *SQL Server 2014 Express* (incluído com os arquivos de instalação do Security Center), o tamanho do banco de dados será limitado a 10 GB. Um evento de porta usa (em média) 200 bytes na base de dados. Se você configurar o Access Manager para manter eventos de porta indefinidamente, o banco de dados uma hora atingirá o limite de 10 GB e o mecanismo parará.
- **Ativar ponto a ponto:** Selecione esta opção para ativar a comunicação entre as unidades Synergis™ gerenciadas por este Access Manager.

  MELHOR PRÁTICA: Somente ative a comunicação ponto a ponto se você planejar criar zonas de E/S que envolvam várias unidades Synergis™ ou aplicar antirretorno a áreas controladas por múltiplas unidades Synergis™. Deixe essa opção desmarcada para melhor segurança e desempenho do sistema.
- **Ativar antirretorno global:** Selecione esta opção se precisar aplicar o antirretorno a áreas controladas por várias unidades Synergis™. Para ativar esta opção, primeiro você deve ativar o ponto a ponto.

  MELHOR PRÁTICA: Se todas as áreas antirretorno são controladas por uma única unidade, não habilite o antirretorno global. Habilitar o antirretorno global aumenta a comunicação entre as unidades Synergis™.

Access Manager - aba Extensões

Clique na aba **Extensões** para configurar os parâmetros de conexão específicos do fabricante compartilhados por unidades de controle de acesso controladas por este Access Manager.

- **Genetec™Synergis™:** Extensão para todas a unidades Synergis™. Esta extensão requer pelo menos uma porta de descoberta. Para mais informações, consulte o *Guia de Configuração de Aparelhos Synergis™*.
- **HID VertX:** Extensão para todas as unidades HID, incluindo os modelos legais VertX (V1000 e V2000), o VertX EVO e os controladores Edge EVO. Para uma lista completa das unidades de controladores e firmwares suportados, consulte *Notas de Lançamento do Security Center*.

Access Manager - Aba Recursos

Clique na aba **Recursos** para configurar os servidores e o banco de dados atribuídos a esta função.

- **Servidores:** Servidores que hospedam esta função.
- **Status do banco de dados:** Status atual do banco de dados.
- **Servidor de banco de dados:** Nome do serviço SQL Server (padrão=`(local)\SQLEXPRESS`).
- **Banco de dados:** Nome da instância do banco de dados.
- **Ações:** Funções de manutenção que você pode realizar no banco de dados da função:

- **Criar um banco de dados ():** Crie um novo banco de dados..
- **Excluir o banco de dados ():** Exclua o banco de dados..
- **Informações do banco de dados ():** Mostrar informações do banco de dados.
- **Notificações ():** Definir notificações para quando o espaço do banco de dados estiver se esgotando.
- **Backup/restauração ():** Faça backup de ou restaure o banco de dados.

Abas de configuração do Active Directory

Você define as configurações da função Active Directory a partir da visualização **Funções** da tarefa *Sistema* no Security Center do Config Tool.

Active Directory - aba Propriedades

Clique na aba **Propriedades** para definir os parâmetros de como a função Active Directory funciona.

- **Status da conexão:** Status da conexão entre a função e o AD corporativo.
- **Status:** Mostra o que a função está fazendo. *Inativo* é o status normal. Se houver um problema, uma mensagem de erro é exibida.
- **Diretório ativo:** Nome de Domínio Totalmente Qualificado (FQDN) do AD, nome do host ou endereço IP do servidor de AD corporativo.
  - **Usar as credenciais do Windows:** Você pode usar as credenciais do Windows usadas para executar o serviço *Genetec Server*, ou especificar um conjunto diferente de nomes de usuários e senhas do Windows. Em ambos os casos, as credenciais que você especifica devem ter acesso de leitura e gravação ao AD corporativo especificado.
  - **Usar conexão SSL:** Selecione esta opção para criptografar o tráfego de rede LDAP (Lightweight Directory Access Protocol). LDAP é o protocolo usado para comunicação entre a função Active Directory e o AD. A porta padrão usada para comunicação criptografada é 636. Se você usar uma porta diferente, é necessário especificá-la explicitamente adicionando o número da porta após o nome do servidor AD, separado por dois pontos (':').
  - **Usar um controlador de domínio específico:** Selecione esta opção e especifique o nome do seu controlador de domínio se você tiver um dedicado ao Security Center.
- **Partição:** *Partição* padrão onde as entidades sincronizadas com o AD corporativo são criadas se a partição não for mapeada para um atributo AD.
- **Grupos sincronizados:** Lista de todos os grupos de segurança AD importados como grupos de usuários, grupos de titulares de cartão ou ambos.
- **Não existe nenhuma tarefa agendada para sincronizar esta função. :** Esta mensagem de aviso aparece se você não configurou uma tarefa agendada para gerenciar automaticamente a sincronização com o AD corporativo.
- **Sincronizar agora. :** Sincronizar com o Active Directory agora. Você sempre deve sincronizar depois de fazer alterações nos grupos sincronizados.

Active Directory - aba Links

Clique na aba **Links** para mapear atributos AD para campos do Security Center.

- **Titular do cartão:** Mapear os atributos do AD para os campos de titular do cartão Security Center:
- **Fazer upload de imagens para o Active Directory:** Selecione esta opção se desejar que as fotos que você atribuir aos titulares de cartão importados do Security Center sejam carregadas para o AD.
- **Tamanho máximo do arquivo da imagem carregado:** Este parâmetro só aparece se *Carregar imagens no Active Directory* for selecionado. Ele serve para limitar o tamanho do arquivo das fotos que você carrega do Security Center para o AD.
- **Formato do cartão:** Selecione o formato de cartão padrão a ser usado para as credenciais de titular de cartão importado quando a propriedade de formato de cartão não estiver mapeada para um atributo de AD ou quando o atributo mapeado estiver vazio.
- **Modelo do crachá:** Selecione o modelo de crachá padrão para usar para as credenciais de titular de cartão importadas.

- **Campos personalizados:** Mapeia AD adicionais em campos personalizados do Security Center.

Active Directory - aba Recursos

Clique na aba **Recursos** para configurar os servidores atribuídos a esta função. A função Active Directory não exige um banco de dados.

- **Servidores:** Servidores que hospedam esta função.

Active Directory Federation Services - Aba Propriedades

Na aba **Propriedades**, você pode configurar sua cadeia de confiança e todos os grupos de ADFS que você aceita como grupos de usuários do Security Center.

- **Cadeia de confiança (domínios):** A cadeia de confiança define o domínio de seu *ADFS raiz*, o servidor ADFS com o qual a função está diretamente falando e os domínios dos servidores ADFS remotos dos quais o Security Center está recebendo declarações (*Grupo* e *UPN*) através do ADFS raiz.
- **Grupos de usuários aceitos:** Grupos de usuários correspondentes aos grupos ADFS que o Security Center aceita. Esses nomes de grupos de usuários devem corresponder ao nome definido pelos servidores ADFS remotos, seguido pelo nome de domínio ADFS. Por exemplo: *operators@companyXYZ.com*.

Archiver - Aba Configurações padrão de câmera

Você pode usar a aba **Configurações padrão de câmera** para definir as configurações padrão de gravação aplicadas a todas as câmeras controladas pela função Archiver.

A aba **Configurações padrão de câmera** inclui as seguintes configurações:

- **Qualidade do vídeo:** Selecione uma **Resolução**.
  - **Alta:** 1270x720 e superior.
  - **Padrão:** Entre 320x240 e 1280x720.
  - **Baixa:** 320x240 e inferior.
  - **Padrão:** Configurações padrão do fabricante.
  - **Taxa de quadros:** Você pode selecionar um valor entre 1 e 30 fps. Não se aplica às configurações padrão.
- **Gravando:** Na lista suspensa **Modos de gravação**, selecione um dos seguintes modos de gravação:
  - **Contínuo:** Grava continuamente. A gravação não pode ser interrompida pelo usuário ().
  - **Em movimento/Manual:** A gravação é desencadeada por uma ação (como *Iniciar gravação*, *Adicionar favorito* ou *Disparar alarme*) por meio de detecção de movimento ou manualmente por um usuário. Neste modo, o botão **Gravar** no Security Desk aparece de uma das seguintes maneiras:
    - Cinza () quando o Archiver não está gravando
    - Vermelho () quando está gravando mas pode ser interrompido pelo usuário
    - Vermelho com um cadeado () quando está gravando mas não pode ser interrompida pelo usuário (gravação com movimento ou alarme).
  - **Manual:** Grava quando disparado manualmente por um usuário. Neste modo, o botão **Gravar** no Security Desk aparece de uma das seguintes maneiras:
    - Cinza () quando o Archiver não está gravando
    - Vermelho () quando está gravando mas pode ser interrompido pelo usuário
    - Vermelho com um cadeado () quando está gravando mas não pode ser interrompida pelo usuário (gravação com movimento ou alarme).
  - **Personalizar:** A gravação é especificada por um agendamento personalizado. Para obter mais informações sobre como criar agendas usando a tarefa *Sistema*, consulte Criando agendamentos na página 199.
    CUIDADO: Agendamentos de gravação do mesmo tipo (por exemplo, dois agendamentos diários) não podem ser sobrepostos, independentemente do modo de gravação configurado para cada um. Quando ocorre um conflito de agendamento o Archiver e as unidades de vídeo são exibidas em amarelo no navegador de entidades e emitem mensagens de alerta de entidades.
  - **Desligado:** A gravação fica desligada (), mesmo quando um alarme é disparado.
  - **(Opcional) Exibir configurações avançadas:** Clique para definir configurações avançadas de gravação.
  - **Gravar áudio:** Ajuste em **Ligado** para gravar áudio com o seu vídeo. Uma entidade de microfone deve estar conectada às suas câmeras. Para mais informações, consulte Definição das configurações de câmera na página 475.
  - **Gravar metadados:** Ajuste em **Ligado** para gravar metadados com o seu vídeo.

- **Arquivamento redundante:** Ajuste em **Ligado** para permitir que servidores primários, secundários e terciários arquivem vídeo ao mesmo tempo. Esta configuração só é efetiva se o failover estiver configurado. Para mais informações, consulte Configurar failover do Archiver na página 188.
- **Limpeza automática:** Especifique um período de retenção para o vídeo gravado (em dias). Arquivos de vídeo mais antigos do que esse período são excluídos.
- **Tempo de gravação anterior a um evento:** Use o controle deslizante para definir a duração (em segundos) da gravação antes de um evento. Esse buffer é salvo sempre que começa a gravação, garantindo que o que quer que tenha iniciado a gravação também seja capturado no vídeo.
- **Tempo para gravar após um movimento:** Use o controle deslizante para definir a duração (em segundos) da gravação após um evento de movimento. Durante esse período, o usuário não pode interromper a gravação.
- **Duração inicial de gravação manual:** Use o controle deslizante para selecionar a duração (em minutos) da gravação quando for iniciada manualmente por um usuário ou quando a ação *Iniciar gravação* for desencadeada.

- **Codificação:** Defina como **Ligado** para ativar *criptografia de fluxo de fusão* para todas as câmeras gerenciadas pelo Archiver selecionado. Somente usuários que tenham um ou mais dos **Certificados** listados instalados em suas estações de trabalho podem visualizar vídeo.

  NOTA: Para ativar a **Criptografia**, você deve adicionar pelo menos um *certificado de criptografia* à função Archiver. Para mais informações, consulte O que é a criptografia de transmissão de fusão? na página 417.

NOTA:

- As definições de gravação configuradas no assistente de instalação do Security Center são transferidas para a aba **Configurações padrão de câmera**.
- As configurações de gravação definidas na aba **Gravação** de uma câmera individual sobrescrevem as configurações definidas na aba **Configurações padrão de câmera**.

Archiver - Aba Extensões

Na aba **Extensões**, você pode configurar os parâmetros de conexão comuns compartilhados pelas unidades de vídeo que são controladas pelo Archiver selecionado. As extensões são criadas automaticamente quando você adiciona uma unidade ao Archiver.

A aba *Extensões* inclui as seguintes configurações:

- **Tempo limite da transação:** Tempo gasto na espera de uma resposta antes de enviar novamente um comando para a unidade.
- **Porta de comando:** (Somente Bosch) Porta usada pelo Archiver para enviar comandos para as unidades Bosch. Este campo tem valores padrão que são redefinidos sempre que o campo **Protocolo** for modificado.
- **Protocolo:** (Somente Bosch) Protocolo de transporte usado pelo Archiver para enviar comandos para as unidades Bosch.

  Os resultados aceitos são:

  - **RCP:** Usa RCP+ sobre TCP (padrão). A porta de comando deve ser definida como 1756.
  - **HTTP:** Usa HTTP ou HTTPS (RCP+ sobre CGI).
    IMPORTANTE: Para registrar uma unidade Bosch usando HTTP ou HTTPS, você deve criar manualmente a extensão Bosch ou modificar uma existente.
    - Para usar HTTP, configure **Porta de comando** para corresponder ao valor de **Porta HTTP de navegador** configurado na unidade Bosch.
    - Para usar HTTPS, defina **Usar HTTPS** como **Ligado** no grupo *Logon padrão* e defina **Porta** para corresponder ao valor de **Porta HTTPS de navegador** configurado na unidade Bosch.

    NOTA: As portas de comando configuradas na extensão Bosch são valores padrão. Os valores configurados nas unidades Bosch podem ser diferentes. A **Porta de descoberta** deve corresponder aos valores configurados nas unidades Bosch.
- **Porta RSTP:** RTSP (Real Time Streaming Protocol) usado pelo Archiver para solicitar o vídeo das unidades que suportam este protocolo.

  A porta RTSP é usada para ouvir os pedidos RTSP (Real Time Streaming Protocol). Quando várias funções de arquivamento estão hospedadas no mesmo servidor, esse valor deve ser exclusivo para cada uma. O valor configurado não pode ser o mesmo que qualquer valor usado para a função Media Router, seu agente redirecionador ou qualquer Auxiliary Archiver hospedado no mesmo servidor.
- **porta VSIP:** (Somente Verint) Porta usada para *descoberta automática*. Todas as unidades que são controladas através da mesma extensão Verint devem ser configuradas com a mesma *Porta VSIP*. Todas as extensões Verint configuradas para o mesmo Archiver devem ter diferentes portas de descoberta.
- **Recusar autenticação básica:** Use esta opção para ativar ou desativar a autenticação básica para uma extensão. Isso é útil se você tiver desativado a autenticação básica do Security Center InstallShield, mas você precisará ativá-la novamente para usar uma câmera que suporte somente a autenticação básica. Para ativar novamente a autenticação básica, você deve colocar a opção **Recusar autenticação básica** em **Desligado**.
- **Porta de descoberta:** Porta de descoberta automática. Se várias instâncias do mesmo tipo de extensão estiverem configuradas para o mesmo Archiver, todas elas devem usar uma porta de descoberta diferente.

  - (ACTi) Corresponde a *Porta do servidor de pesquisa 1* nas configurações do servidor de vídeo ACTi.
  - (Bosch) Todas as unidades que são controladas através da mesma extensão Bosch devem ser configuradas com a mesma porta de descoberta.

NOTA: Se você decidir alterar a *Porta de descoberta* depois que as unidades forem descobertas, você deve criar uma nova extensão com a nova porta de descoberta e excluir a antiga. Se as unidades não forem descobertas automaticamente, você deve adicioná-las manualmente.

- **Porta de resposta de detecção:** (ACTi e Interlogix) Corresponde a *Porta do servidor de pesquisa 2* nas configurações do servidor de vídeo ACTi.
- **Período de unicast:** Período de tempo em que a extensão repete os testes de conexão usando unicast para determinar se cada unidade ainda está ativa no sistema.
- **Período de multicast:** Período de tempo em que a extensão tenta descobrir novas unidades usando multicast. Esta opção pode ser desativada. O endereço IP que se segue é o endereço IP multicast padrão usado pelo *Omnicast™*. Altere o endereço IP multicast padrão somente se ele já for usado para outra coisa.
- **Período de difusão:** Período de tempo em que a extensão tenta descobrir novas unidades usando a transmissão. Esta opção pode ser desativada.
- **Logon padrão:** Certos tipos de unidades podem ser protegidos por um nome de usuário e uma senha contra acesso ilegal. As credenciais de logon podem ser definidas individualmente para cada unidade ou para todas as unidades usando a mesma extensão.
  - **Nome do usuário:** Certos tipos de unidades (como a Axis) requerem um nome de usuário.
  - **Senha:** Certos tipos de unidades (como a Bosch) requerem uma senha.
  - **Usar HTTPS:** Selecione esta opção para usar o *Secure Hypertext Transfer Protocol* para segurança adicional.
    NOTA: Para unidades Bosch, esta definição só aparece quando **Protocolo** é definido como **HTTP**. Quando **Usar HTTPS** está definido como **Ligado**, a **Porta** definida aqui tem prioridade sobre a **Porta de comando**.
- **Porta de notificação TCP:** (Panasonic e Interlogix) utilizados pela função Archiver para receber notificações das unidades. Quando ocorre um evento, como *Perda de Sinal* ou *Sinal recuperado*, a unidade inicia uma conexão *TCP* com o Archiver e envia a notificação através desta porta.
- **Canal de notificação:** (Somente para o Interlogix) Quando você configura várias funções Archiver para ouvir as mesmas unidades, como em uma lista de failover, cada Archiver deve ser identificado com um canal de notificação diferente (1 a 8). Você pode ignorar esse parâmetro se você estiver usando apenas um Archiver. Para várias funções Archiver, você deve seguir estas regras:
  - Todas as funções Archiver que controlam as mesmas unidades devem ser configuradas com a mesma porta de notificação TCP.
  - Todas as funções Archiver devem usar um canal de notificação diferente.
- **Configurações do Bosch VRM:** As configurações VRM são exclusivas do Bosch VRM (Video Recording Manager). Essas configurações permitem que você consulte e reproduza vídeos das câmeras Bosch gerenciadas por um Bosch VRM. Várias extensões Bosch podem usar o mesmo VRM. Se você adicionar mais de um VRM à lista, você pode usar os botões mover para cima () e mover para baixo () para mover um VRM para cima ou para baixo na lista. Por padrão, o Archiver usa o primeiro VRM na lista para consultas e vídeo arquivado. Se o primeiro VRM não estiver disponível, o Archiver usa o próximo VRM na lista.
- **Configurações específicas do Verint:** As configurações a seguir são encontradas apenas nas unidades Verint.
  - **Exibir todos os fluxos de vídeo disponíveis como câmeras separadas:** (Somente Verint) O Omnicast™ suporta codificadores que geram múltiplas transmissões de vídeo da mesma fonte de vídeo. Quando esses codificadores são descobertos, o Archiver cria um *codificador de vídeo* com múltiplas alternativas de transmissão. Selecione esta opção para representar cada fluxo de vídeo como uma câmera separada.
    NOTA: Esta opção requer uma licença de conexão de câmera para cada fluxo.

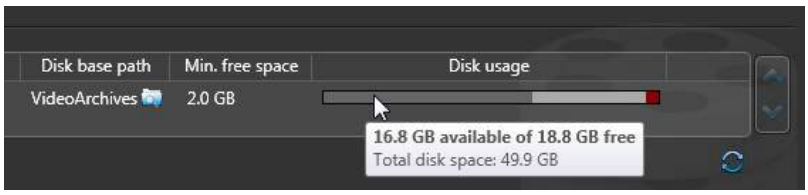
    - **Configurações SSL:** SSL (Secure Sockets Layer) é um protocolo usado para proteger aplicativos que precisam se comunicar através de uma rede. O Security Center suporta SSL em todas as transmissões de mensagens entre o Archiver e as unidades, exceto para transmissões de vídeo, porque o volume de dados é muito alto. O objetivo do uso de SSL no Security Center é evitar ataques, não é evitar a interceptação. Selecione *Impor SSL* somente se for necessário impor SSL em todas as unidades controladas por este Archiver. Se esta opção for apagada, o Archiver usará SSL somente para se comunicar com as unidades nas quais o SSL está habilitado.
- **Configurações avançadas:** As configurações avançadas estão reservadas para uso do Centro de Assistência Técnica Genetec™.
- **Configurações de NTP:** Sincroniza o tempo entre as unidades que suportam NTP (Network Time Protocol) e o servidor NTP. Manter o tempo de sincronização das unidades é particularmente importante para as unidades que manipulam o arquivamento de vídeo. Você deve definir os seguintes parâmetros:
    - **Servidor NTP:** Especifique o nome do servidor NTP.
    - **Porta NTP:** Especifique o número da porta do servidor NTP.
    - **Tempo limite de consulta:** Especifique a frequência com que deseja que o tempo nas unidades seja verificado para garantir que elas estejam corretamente sincronizadas com o servidor NTP. Por exemplo, se 60 segundos for inserido, o tempo será verificado a cada 60 segundos.

Archiver - Aba Recursos

Esta seção lista as configurações encontradas na aba **Recursos** da função Archiver, na tarefa Vídeo.

Clique na aba **Recursos** para atribuir servidores, bancos de dados e armazenamento em disco para esta função Archiver.

- **Servidor ( ):** Um dos servidores que hospeda esta função Archiver. Você pode atribuir um máximo de dois servidores a uma função Archiver para fins de failover usando as abas na parte inferior da página.
  - **Placa de rede:** Placa de rede usada para comunicação com todas as unidades de vídeo.
  - **Porta RTSP:** Portas usadas para ouvir os pedidos RTSP (Real Time Streaming Protocol). Quando várias funções de arquivamento estão hospedadas no mesmo servidor, esses valores devem ser exclusivos para cada uma. Os valores padrão são 555 e 605 para o Archiver e 558 para o Auxiliary Archiver. Os valores configurados não devem duplicar quaisquer valores usados para a função Media Router ou seu agente redirecionador hospedados no mesmo servidor.
  - **Porta Telnet:** Porta usada para escutar solicitações de conexão do *console Telnet* para fins de depuração. Quando você altera esse valor, você precisa desativar e reativar a função Archiver para que a alteração entre em vigor.
  - **Portas UDP de recepção de transmissão ao vivo:** Para cada agente Archiver, você pode atribuir manualmente portas UDP de transmissão ao vivo, que são usadas para receber as transmissões das câmeras. Cada câmera pode necessitar de várias portas (1 porta por periférico). Por isso, a gama de portas deve ser vasta o suficiente para acomodar todos os periféricos de todos os dispositivos. Se a sua configuração exceder o limite máximo de portas (65535), você pode alterar a porta inicial padrão (15000) e as portas alocadas por agente Archiver (5000).
- **Status do banco de dados:** Status atual do banco de dados.
- **Servidor de banco de dados:** Nome do serviço SQL Server (padrão=`(local)\SQLEXPRESS`).
- **Banco de dados:** Nome da instância do banco de dados.
- **Ações:** Funções de manutenção que você pode realizar no banco de dados da função:
  - **Criar um banco de dados ( ):** Crie um novo banco de dados..
  - **Excluir o banco de dados ( ):** Exclua o banco de dados..
  - **Informações do banco de dados ( ):** Mostrar informações do banco de dados.
  - **Notificações ( ):** Definir notificações para quando o espaço do banco de dados estiver se esgotando.
  - **Backup/restauração ( ):** Faça backup de ou restaure o banco de dados.
- **Gravando:** Exibe informações sobre unidades locais e unidades de rede que podem ser usadas para armazenar vídeo. Todas as unidades locais encontradas no servidor host estão listadas por padrão e agrupadas em *Grupo de discos padrão*.
  - **Caminho básico do disco:** Pasta raiz no disco em que todos os arquivos de vídeo estão localizados. O valor padrão é *VideoArchives*.
  - **Espaço livre mínimo:** Espaço livre mínimo que o Archiver nunca deve usar no disco. O valor padrão é 1% da capacidade total do espaço em disco.
  - **Espaço livre:** Espaço livre real restante no disco.
  - **Uso do disco:** Gráfico que mostra a capacidade total do disco (gráfico completo), o espaço livre mínimo (vermelho), o espaço ocupado do disco (cinza escuro) e o espaço livre restante para arquivos de vídeo (cinza claro). Passe o mouse sobre a tabela para esses valores serem exibidos em um balão.



- **Adicionar local de rede ( ):** Somente é possível adicionar unidades de rede ao seu armazenamento em arquivo. Todas as unidades locais no servidor host são listadas por padrão. Você pode excluí-las de ser usadas pelo Archiver, desmarcando a caixa de seleção na frente de cada disco.
- **Adicionar grupo:** Um grupo de discos é uma unidade de armazenamento lógica usada pelo Archiver para melhorar a produtividade geral dos discos. Clique nas setas **Para cima** e **Para baixo** para mover o disco selecionado de um grupo para outro.
- **Excluir ( ):** Exclui o disco ou grupo de discos selecionado. Cada grupo de discos deve ter ao menos um disco associado a ele.
- **Distribuição de câmeras ( ):** Divide as câmeras entre os grupos de discos. Este botão aparece apenas se você tiver mais de um grupo de discos definido.
- **Atualizar informações da unidade ( ):** Atualiza as informações da unidade.

- **Transferência de arquivos:** Este botão aparece apenas se você tiver mais de um grupo de discos definido.
  - **Pasta de backup:** Local onde os arquivos de backup são salvos como um arquivo G64x.
  - **Apagar arquivos mais antigos quando os discos estiverem cheios:** Ative esta opção para eliminar os arquivos de vídeo mais antigos quando o disco estiver cheio.
  - **Limpeza automática:** Ligue esta opção para especificar um período de retenção para os arquivos de vídeo em backup (em dias). Se você não ativar essa opção, os arquivos de vídeo em backup não serão excluídos pelo sistema e você deverá excluí-los manualmente.

Estatística do Archiver

A caixa de diálogo Estatísticas aparecerá ao clicar no botão *Estatísticas* ( ). Ela oferece informações relacionadas ao armazenamento do arquivo e a taxa na qual ela está sendo ocupada.

- **Atualizar ( ):** Atualiza as estatísticas.
- **Lista de discos atribuídos:** Instantâneo das estatísticas de disco feitas desde a última vez que uma atualização ocorreu.
- **Estatísticas do arquivo de vídeo protegido ( ):** Visualiza a porcentagem dos arquivos de vídeo protegidos do disco selecionado.
- **Uso médio de disco:** O espaço médio usado por dia (primeira linha) e espaço médio usado por câmera por dia (segunda linha).
- **Tempo de gravação restante estimado:** Número de dias, horas e minutos de tempo de gravação restantes com base na média de utilização de disco e a carga atual.
- **Câmeras ativas:** Número de câmeras ativas no momento.
- **Arquivando câmeras:** Número de câmeras que têm o arquivamento ativo.
- *Ver detalhes*: Visualize o *estado de gravação* e as estatísticas de cada câmera individual na caixa de diálogo *Detalhes da câmera de arquivamento*. As estatísticas são obtidas da última atualização da caixa de diálogo *Estatísticas*. Este relatório permite verificar se cada codificador atualmente está transmitindo vídeo (e áudio) e se o Archiver atualmente está gravando os dados.
- **Período de arquivamento:** Intervalo de tempo no qual os arquivos de vídeo podem ser encontrados.

- **Pior caso de largura de banda:** Número que indica a pior hipótese na exigência total de largura de banda se todas as câmeras estiverem no pico de suas demandas de arquivamento.

Configurações avançadas

As configurações avançadas são independentes do servidor que hospeda a função Archiver.

- **Marca d'água de vídeo:** Ligue esta opção para proteger seu arquivo de vídeo contra adulteração.
- **Apagar arquivos mais antigos quando os discos estiverem cheios:** Ligue esta opção para reciclar o armazenamento do arquivo (o modo padrão). Os arquivos mais antigos são excluídos para abrir espaço para novos arquivos quando todos os discos dentro de um grupo estão cheios.
- **Habilitar solicitações de reprodução na unidade:** Ligue esta opção somente se o Archiver controlar unidades configuradas para *gravação avançada*. Como padrão, esta opção fica desligada para evitar o envio de solicitações de reprodução para unidades que não estejam gravando.
- **Habilitar solicitações de miniaturas:** Ligue esta opção para mostrar miniaturas de vídeos para o Archiver (por exemplo, em relatórios). Esta opção também deve ser ligada para enviar instantâneos usando a ação *Enviar uma foto por e-mail*.
- **Ativar consolidação de arquivo:** Ative esta opção para duplicar arquivos de vídeos do servidor de Archiver secundário ou terciário para o servidor de Archiver primário após failover de um Archiver. O servidor de Archiver primário verifica a cada hora se existem arquivos de vídeos que possam ser consolidados dos servidores secundário e terciário para o período em que esteve offline.
- **Habilitar console Telnet:** Ligue esta opção para ativar o console de depuração Telnet para este Archiver.
- **Limiar de vídeo protegido:** Este é um limiar de segurança que limita a quantidade de espaço que arquivos de vídeo protegidos podem ocupar em discos. A porcentagem que você configurar é a proporção de vídeos protegidos que você pode ter do tamanho total de vídeos gravados no disco. Os arquivos de vídeo protegidos são arquivos que não serão excluídos por procedimentos normais de limpeza de arquivos. Se esse limiar for excedido, o Archiver gera o evento *Limiar de vídeos protegidos excedido* a cada 15 minutos enquanto a condição for verdadeira, mas não excluirá nenhum arquivo de vídeo que esteja protegido.
- **Limiar de advertência de carga de disco:** A porcentagem de espaço em disco que deve estar ocupada antes do evento *Limiar de carga de disco excedido* ser gerado. O valor padrão é 90%. O Archiver gera este evento uma vez por hora enquanto a condição for verdadeira. A carga de disco é calculada como segue:

  ```
  Carga de disco = Espaço ocupado em disco / (Capacidade total do disco - Espaço livre mín.)
  ```

- **Capacidade máxima de processamento de transferência de arquivo:** A largura de banda máxima disponível para o Archiver para transferência de arquivos.
- **Arquivos de vídeo:** Essas duas configurações são usadas para controlar o tamanho dos arquivos de vídeo criados pelo Archiver:
  - **Duração máxima:** Limita o comprimento da sequência de vídeo contida em cada arquivo. A duração do vídeo é faixa de tempo entre o primeiro quadro de vídeo e o último quadro de vídeo armazenados em um arquivo. O valor padrão é 20 minutos.
  - **Tamanho máximo:**
    Limita o tamanho do arquivo de vídeo. O valor padrão é 500 MB.
    O Archiver começa a salvar o vídeo em um novo arquivo de vídeo quando uma dessas condições é cumprida.
- **Configurações adicionais:** Essas configurações adicionais são reservadas para uso pelo nosso pessoal de Assistência Técnica.

Tópicos relacionados

Portas usadas por aplicativos Omnicast no Security Center na página 1141

Archiver auxiliar - Aba Gravação da câmera

Você pode usar a aba **Gravação da câmera** para definir as configurações de gravação padrão aplicadas a todas as câmeras associadas a um Archiver auxiliar. As configurações de gravação definidas na aba **Gravação** de uma câmera individual sobrescrevem as configurações definidas na aba **Gravação da câmera** do Archiver auxiliar.

A aba **Gravação da câmera** inclui as seguintes configurações:

- **Fluxo de vídeo:** Selecione o fluxo de vídeo padrão que o Auxiliary Archiver deve gravar para cada câmera. Os streams de vídeo são configurados para cada câmera individual.
- **Modos de gravação:** Aplique modos de gravação diferentes em horários diferentes.
  - **Contínuo:** Grava continuamente. A gravação não pode ser interrompida pelo usuário ( ).
  - **Manual:** Grava quando disparado manualmente por um usuário. Neste modo, o botão *Gravar* do Archiver auxiliar no menu de contexto de ladrilho do Security Desk aparece de uma das seguintes maneiras:
    - Cinza ( ) quando o Auxiliary Archiver não está gravando
    - Vermelho ( ) quando o Auxiliary Archiver está gravando
  - **Personalizar:** A gravação é especificada por um agendamento personalizado. Você pode usar a agenda personalizado que você criou com o assistente de instalação ou clicar em para adicionar uma nova agenda de gravação personalizada que você criou usando a tarefa *Sistema*. Para obter mais informações sobre como criar agendas usando a tarefa *Sistema*, consulte Criando agendamentos na página 199.
    CUIDADO: Agendamentos de gravação do mesmo tipo (por exemplo, dois agendamentos diários) não podem ser sobrepostos, independentemente do modo de gravação configurado para cada um. Quando há um conflito de agendamento o Archiver e as unidades de vídeo são exibidas em amarelo no navegador de entidades e emitem mensagens de alerta de entidades.
  - **Desligado:** A gravação fica desligada ( ), mesmo quando um alarme é disparado.
- **Gravar áudio:** Ajuste em **Ligado** para gravar áudio com o seu vídeo. Uma entidade de microfone deve estar conectada às suas câmeras para que esta opção funcione. Para mais informações, consulte Definição das configurações de câmera na página 475.

  NOTA: Não é necessário que os dispositivos anexos pertençam à mesma unidade do codificador de vídeo. No entanto, para que a gravação de áudio funcione, garanta que o microfone pertence a uma unidade gerenciada pelo mesmo Archiver, com a mesma extensão Archiver, que o codificador de vídeo.
- **Gravar metadados:** Ajuste em **Ligado** para gravar metadados (como sobreposições) com o seu vídeo.
- **Limpeza automática:** Especifique um período de retenção para o vídeo gravado (em dias). Arquivos de vídeo mais antigos do que esse período são excluídos.

Archiver auxiliar - Aba Câmeras

Esta seção lista as configurações encontradas na aba *Câmeras* da função Archiver auxiliar, na tarefa Vídeo.

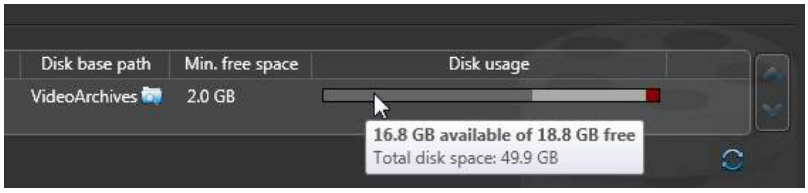
Na aba *Câmeras*, você pode selecionar as *câmeras* arquivadas por esta função. O Archiver auxiliar pode gravar qualquer câmera em seu sistema, exceto aquelas que são federadas de um sistema Omnicast™ 4.x.

Archiver auxiliar - Aba Recursos

Esta seção lista as configurações encontradas na aba *Recursos* da função Archiver auxiliar, na tarefa Vídeo.

Clique na aba **Recursos** para atribuir servidores, bancos de dados e armazenamento em disco para esta função Archiver auxiliar.

- **Servidor ( ):** Servidor que hospeda esta função. O failover não é suportado para a função Auxiliary Archiver. Você só pode selecionar um servidor.
  - **Placa de rede:** Placa de rede usada para comunicação com todas as unidades de vídeo.
  - **Porta RTSP:** Porta usada para ouvir os pedidos RTSP (Real Time Streaming Protocol). Quando várias funções de arquivamento estão hospedadas no mesmo servidor, esse valor deve ser exclusivo para cada uma. O valor padrão é 555 para o Archiver e 558 para o Auxiliary Archiver. Além disso, os valores configurados não devem duplicar quaisquer valores usados para a função *Media Router* ou seu *agente redirecionador* hospedados no mesmo servidor.
- **Status do banco de dados:** Status atual do banco de dados.
- **Servidor de banco de dados:** Nome do serviço SQL Server (padrão=`(local)\SQLEXPRESS`).
- **Banco de dados:** Nome da instância do banco de dados.
- **Ações:** Funções de manutenção que você pode realizar no banco de dados da função:
  - **Criar um banco de dados ( ):** Crie um novo banco de dados..
  - **Excluir o banco de dados ( ):** Exclua o banco de dados..
  - **Informações do banco de dados ( ):** Mostrar informações do banco de dados.
  - **Notificações ( ):** Definir notificações para quando o espaço do banco de dados estiver se esgotando.
  - **Backup/restauração ( ):** Faça backup de ou restaure o banco de dados.
- **Informações do disco:** Exibe informações sobre unidades locais e unidades de rede que podem ser usadas para armazenar vídeo. Todas as unidades locais encontradas no servidor host estão listadas por padrão e agrupadas em *Grupo de discos padrão*.
  - **Caminho básico do disco:** Pasta raiz no disco em que todos os arquivos de vídeo estão localizados. O valor padrão é *AuxiliaryArchives*.
  - **Espaço livre mínimo:** Espaço livre mínimo que o Auxiliary Archiver nunca deve usar no disco.
  - **Uso do disco:** Gráfico que mostra a capacidade total do disco (gráfico completo), o espaço livre mínimo (vermelho), o espaço ocupado do disco (cinza escuro) e o espaço livre restante para arquivos de vídeos (cinza claro). Passe o mouse sobre a tabela para esses valores serem exibidos em um balão.



- **Adicionar local de rede ( ):** Somente é possível adicionar unidades de rede ao seu armazenamento em arquivo. Todas as unidades locais no servidor host são listadas por padrão. Você pode excluí-las de ser usadas desmarcando a caixa de seleção na frente de cada disco.
- **Adicionar grupo ( ):** Um grupo de discos é uma unidade de armazenamento lógica usada pelo Archiver para melhorar a produtividade geral dos discos. Clique nas setas *Para cima* e *Para baixo* para mover o disco selecionado de um grupo para outro.

- **Excluir ( ):** Exclui o disco ou grupo de discos selecionado. Você não pode deixar um grupo de discos sem nenhum disco associado a ele.
- **Distribuição de câmeras ( ):** Divide as câmeras entre os grupos de discos. Este botão aparece apenas se você tiver mais de um grupo de discos definido.
- **Atualizar informações da unidade ( ):** Atualiza as informações da unidade.

Estatística do Archiver

A caixa de diálogo Estatísticas aparecerá ao clicar no botão *Estatísticas* ( ). Ela oferece informações relacionadas ao armazenamento do arquivo e a taxa na qual ela está sendo ocupada.

- **Atualizar ( ):** Atualiza as estatísticas.
- **Lista de discos atribuídos:** Instantâneo das estatísticas de disco feitas desde a última vez que uma atualização ocorreu.
- **Estatísticas do arquivo de vídeo protegido ( ):** Visualiza a porcentagem dos arquivos de vídeo protegidos do disco selecionado.
- **Uso médio de disco:** O espaço médio usado por dia (primeira linha) e espaço médio usado por câmera por dia (segunda linha).
- **Tempo de gravação restante estimado:** Número de dias, horas e minutos de tempo de gravação restantes com base na média de utilização de disco e a carga atual.
- **Câmeras ativas:** Número de câmeras ativas no momento.
- **Arquivando câmeras:** Número de câmeras que têm o arquivamento ativo.
- *Ver detalhes***:** Visualize o *estado de gravação* e as estatísticas de cada câmera individual na caixa de diálogo *Detalhes da câmera de arquivamento*. As estatísticas são obtidas da última atualização da caixa de diálogo *Estatísticas*. Este relatório permite verificar se cada codificador atualmente está transmitindo vídeo (e áudio) e se o Archiver atualmente está gravando os dados.
- **Período de arquivamento:** Intervalo de tempo no qual os arquivos de vídeo podem ser encontrados.
- **Pior caso de largura de banda:** Número que indica a pior hipótese na exigência total de largura de banda se todas as câmeras estiverem no pico de suas demandas de arquivamento.

Configurações avançadas

As configurações avançadas são independentes do servidor que hospeda a função Archiver.

- **Marca d'água de vídeo:** Ligue esta opção para proteger seu arquivo de vídeo contra adulteração.
- **Apagar arquivos mais antigos quando os discos estiverem cheios:** Ligue esta opção para reciclar o armazenamento do arquivo (o modo padrão). Os arquivos mais antigos são excluídos para abrir espaço para novos arquivos quando todos os discos dentro de um grupo estão cheios.
- **Habilitar solicitações de reprodução na unidade:** Ligue esta opção somente se o Archiver controlar unidades configuradas para *gravação avançada*. Como padrão, esta opção fica desligada para evitar o envio de solicitações de reprodução para unidades que não estejam gravando.
- **Habilitar solicitações de miniaturas:** Ligue esta opção para mostrar miniaturas de vídeos para o Archiver (por exemplo, em relatórios). Esta opção também deve ser ligada para enviar instantâneos usando a ação *Enviar uma foto por e-mail*.
- **Ativar consolidação de arquivo:** Ative esta opção para duplicar arquivos de vídeos do servidor de Archiver secundário ou terciário para o servidor de Archiver primário após failover de um Archiver. O servidor de Archiver primário verifica a cada hora se existem arquivos de vídeos que possam ser consolidados dos servidores secundário e terciário para o período em que esteve offline.
- **Habilitar console Telnet:** Ligue esta opção para ativar o console de depuração Telnet para este Archiver.

- **Limiar de vídeo protegido:** Este é um limiar de segurança que limita a quantidade de espaço que arquivos de vídeo protegidos podem ocupar em discos. A porcentagem que você configurar é a proporção de vídeos protegidos que você pode ter do tamanho total de vídeos gravados no disco. Os arquivos de vídeo protegidos são arquivos que não serão excluídos por procedimentos normais de limpeza de arquivos. Se esse limiar for excedido, o Archiver gera o evento *Limiar de vídeos protegidos excedido* a cada 15 minutos enquanto a condição for verdadeira, mas não excluirá nenhum arquivo de vídeo que esteja protegido.
- **Limiar de advertência de carga de disco:** A porcentagem de espaço em disco que deve estar ocupada antes do evento *Limiar de carga de disco excedido* ser gerado. O valor padrão é 90%. O Archiver gera este evento uma vez por hora enquanto a condição for verdadeira. A carga de disco é calculada como segue:

  `Carga de disco = Espaço ocupado em disco / (Capacidade total do disco - Espaço livre mín.)`
- **Capacidade máxima de processamento de transferência de arquivo:** A largura de banda máxima disponível para o Archiver para transferência de arquivos.
- **Arquivos de vídeo:** Essas duas configurações são usadas para controlar o tamanho dos arquivos de vídeo criados pelo Archiver:
  - **Duração máxima:** Limita o comprimento da sequência de vídeo contida em cada arquivo. A duração do vídeo é faixa de tempo entre o primeiro quadro de vídeo e o último quadro de vídeo armazenados em um arquivo. O valor padrão é 20 minutos.
  - **Tamanho máximo:**
    Limita o tamanho do arquivo de vídeo. O valor padrão é 500 MB.
    O Archiver começa a salvar o vídeo em um novo arquivo de vídeo quando uma dessas condições é cumprida.
- **Configurações adicionais:** Essas configurações adicionais são reservadas para uso pelo nosso pessoal de Assistência Técnica.

Abas de configuração do Directory Manager

Você define as configurações da função Directory Manager a partir da visualização **Funções** da tarefa *Sistema* no Security Center do Config Tool.

Directory Manager - aba Servidores de Directory

Na aba **Servidores do Directory** você pode configurar os servidores atribuídos a *failover* e *balanceamento de carga* do Directory.

- **Lista de servidores de Directory (para failover e balanceamento de carga):** Lista de servidores atribuídos a failover e balanceamento de carga do Directory, chamada de *Lista de failover do Directory*. O servidor identificado com um ícone diferente ( ) dos outros ( ) é o *servidor principal*. O servidor principal é o único servidor do Directory que pode gravar no banco de dados do Directory. O resto só pode ler a partir desse banco de dados.
- **Avançado ( ):** Configure o servidor como um servidor de recuperação de desastre ou gateway.
- **Modificar a licença para todos os servidores...:** Modifica sua licença do Security Center sempre que você fizer uma alteração na lista de servidores atribuídos para hospedar a função Directory.

Directory Manager - aba Failover de banco de dados

Na aba **Failover de banco de dados**, você pode configurar o failover de bancos de dados do Directory.

- **Usar failover de banco de dados:** Ativar failover de banco de dados do Directory.
- **Modo de failover:** Seleciona qual modo de failover do banco de dados usar.
- **Backup e restauração:** O Directory Manager protege o banco de dados do Directory fazendo backup regular da instância principal do banco de dados mestre (cópia de origem). Durante um failover, os backups mais recentes são restaurados para o banco de dados de reserva que for o próximo da fila.
  - **LED ( ):** Indica o servidor de banco de dados que está ativo.
  - **Servidor:** *Servidor* do Security Center que hospeda a instância do banco de dados. O servidor que gerencia a instância do banco de dados mestre é sinalizado como *(Mestre)*.
  - **Servidor de banco de dados:** Nome do servidor de Banco de dados. O nome deve ser acessível por todos os computadores. Nomes relativos, como `(local)\SQLSEXPRESS` não podem ser usados. Sempre escreva explicitamente o nome DNS do servidor (por exemplo `TW-WIN7-SC-5`) em vez de `(local)`.
  - **Nome do banco de dados:** Nome da instância de banco de dados.
  - **Estado:** Estado do banco de dados. Se houver um problema, uma mensagem de erro é exibida.
  - **Horário do último Backup/Restauração:** Hora do último backup no banco de dados mestre ou a última restauração no banco de dados de backup.
  - **Pasta:** Pasta local no servidor especificado onde os arquivos de backup são copiados.
  - **Reconectar automaticamente ao banco de dados mestre:** Selecione esta opção para forçar todos os servidores do Directory a se reconectarem ao banco de dados mestre assim que ele voltar a ficar online após um failover. Isso causará uma breve interrupção do serviço, e todas as alterações feitas à configuração do sistema enquanto o banco de dados mestre estava offline serão perdidas.
  - **Gerar backup completo a cada:** Especifique com que frequência (em dias) é gerado um backup completo e em que hora.
  - **Gerar backup diferencial a cada:** Especifique com que frequência (em minutos) um backup diferencial deve ser gerado. Um backup diferencial contém as transações de banco de dados feitas

após o backup anterior (completo ou diferencial). Os backups diferenciais são excluídos após o próximo backup completo ser feito.
NOTA: Todas as atividades de backup são interrompidas quando o banco de dados ativo não é o banco de dados mestre.

- **Espelhando:** O failover de banco de dados é tratado pelo Microsoft SQL Server e é transparente para o Security Center. As instâncias *Principal* e *Espelho* do banco de dados do Directory são sempre mantidos em sincronia. Não há perda de dados durante o failover.
  - **Servidor de banco de dados:** Nome do servidor de Banco de dados. O nome deve ser acessível por todos os computadores. Nomes relativos, como `(local)\SQLSEXPRESS` não podem ser usados. Sempre escreva explicitamente o nome DNS do servidor (por exemplo `TW-WIN7-SC-5`) em vez de `(local)`.
  - **Nome do banco de dados:** Nome da instância de banco de dados.
- **SQL AlwaysOn:** Selecione esta opção de você estiver usando o recurso *SQL AlwaysOn* do Windows como solução de failover de banco de dados do Directory.

Abas de configuração do Global Cardholder Synchronizer

Você define as configurações da função do Global Cardholder Synchronizer a partir da aba **Funções e unidades** da tarefa *Controle de acesso* em Security Center do Config Tool.

Global Cardholder Synchronizer - aba Propriedades

Clique na aba **Propriedades** para configurar os parâmetros de conexão ao *host de compartilhamento*, as *partições globais* que deseja compartilhar e como você deseja sincronizar.

- **Status da conexão:** Indica o estado atual da conexão entre a função Global Cardholder Synchronizer (GSC) e o host de compartilhamento. A segunda linha mostra as atividades de conexão ou quando a última sincronização foi realizada.
- **Directory:** Nome do *servidor do Directory* no host de compartilhamento. Se qualquer outra porta diferente da porta de conexão padrão (5500) for usada, você deve indicar explicitamente o número da porta após o nome do Directory, separado por dois pontos. Por exemplo: `HostServer:5888`.
- **Nome de usuário e senha:** Credenciais usadas pela função GCS para conectar ao host compartilhado. Os direitos e privilégios deste usuário determinam o que seu sistema local é capaz de ver e compartilhar com o sistema host.
- **Partições globais:** Lista de partições globais encontradas no host de compartilhamento. Selecione as que deseja compartilhar.
- **Atualizar:** Clique neste botão para ver a lista de partições globais encontradas no host de compartilhamento.
- **Sincronizar:** Clique neste botão para receber as atualizações mais recentes do host de compartilhamento. Você também pode sincronizar o sistema local segundo uma agenda configurando uma tarefa agendada.

Global Cardholder Synchronizer - aba Recursos

Clique na aba **Recursos** para configurar os servidores atribuídos a esta função. A função GCS não exige um banco de dados.

- **Servidores:** Servidores que hospedam esta função.

Abas de configuração do Health Monitor

Você define as configurações da função Health Monitor a partir da visualização **Funções** da tarefa *Sistema* em Security Center do Config Tool.

Health Monitor - Aba Propriedades

Clique na aba **Propriedades** para configurar os eventos de saúde do sistema a serem monitorados.

- **Modo de manutenção de aplic. cliente:** Ative esta opção para colocar os aplicativos clientes no modo de manutenção.
- **Eventos a monitorar:** Selecione os eventos que você deseja que a função Health Monitor controle.

Health Monitor - Aba Recursos

Clique na aba **Recursos** para configurar os servidores e o banco de dados atribuídos a esta função.

- **Servidores:** Servidores que hospedam esta função.
- **Status do banco de dados:** Status atual do banco de dados.
- **Servidor de banco de dados:** Nome do serviço SQL Server (padrão=`(local)\SQLEXPRESS`).
- **Banco de dados:** Nome da instância do banco de dados.
- **Ações:** Funções de manutenção que você pode realizar no banco de dados da função:
  - **Criar um banco de dados ( ):** Crie um novo banco de dados..
  - **Excluir o banco de dados ( ):** Exclua o banco de dados..
  - **Informações do banco de dados ( ):** Mostrar informações do banco de dados.
  - **Notificações ( ):** Definir notificações para quando o espaço do banco de dados estiver se esgotando.
  - **Backup/restauração ( ):** Faça backup de ou restaure o banco de dados.

Abas de configuração do Intrusion Manager

Você define as configurações da função Intrusion Manager a partir da tarefa *Detecção de intrusão* no Security Center do Config Tool.

Intrusion Manager - Aba Propriedades

Clique na aba **Propriedades** para configurar o período de retenção dos eventos de intrusão no banco de dados do Intrusion Manager.

- **Manter eventos:** Especifique quanto tempo manter os eventos de intrusão registrados pelo Intrusion Manager no banco de dados antes de serem excluídos.
- **Atraso de reconexão:** Especifique quanto tempo o *Intrusion Manager* espera antes de tentar se reconectar a uma unidade que ficou offline.

Intrusion Manager - Aba Extensões

Clique na aba **Extensões** para visualizar os modelos de unidades de intrusão controlados por esta função Intrusion Manager.

Todas as *extensões* suportadas são criadas por padrão quando a função é criada.

Intrusion Manager - Aba Recursos

Clique na aba **Recursos** para configurar os servidores e o banco de dados atribuídos a esta função.

- **Servidores:** Servidores que hospedam esta função.
- **Status do banco de dados:** Status atual do banco de dados.
- **Servidor de banco de dados:** Nome do serviço SQL Server (padrão=`(local)\SQLEXPRESS`).
- **Banco de dados:** Nome da instância do banco de dados.
- **Ações:** Funções de manutenção que você pode realizar no banco de dados da função:
  - **Criar um banco de dados ( ):** Crie um novo banco de dados..
  - **Excluir o banco de dados ( ):** Exclua o banco de dados..
  - **Informações do banco de dados ( ):** Mostrar informações do banco de dados.
  - **Notificações ( ):** Definir notificações para quando o espaço do banco de dados estiver se esgotando.
  - **Backup/restauração ( ):** Faça backup de ou restaure o banco de dados.

LPR Manager - Aba Propriedades

Na tarefa LPR, na aba *Propriedades*, você pode definir as configurações gerais da função LPR Manager e recursos opcionais do AutoVu™. A disponibilidade de determinados recursos depende da sua licença do Security Center.

Configurações gerais

Use as *Configurações gerais* para configurar a *Pasta raiz* para o LPR Manager, o grupo de usuários para instalações do Genetec Patroller™ e quanto tempo os dados do LPR Manager são mantidos no banco de dados.

- **Pasta raiz:** A pasta principal no computador que hospeda o LPR Manager, onde todos os arquivos de configuração são criados, salvos e trocados entre o LPR Manager e as unidades Genetec Patroller™ que ele administra.
- **Otimizar o espaço em disco da pasta Raiz:** Ativa o uso de links simbólicos para reduzir a utilização do disco quando o mesmo arquivo é replicado em várias pastas, como, por exemplo, quando você possui grandes listas de procurados ou listas de autorizações associadas a unidades Genetec Patroller™ individuais. Isso reduz o espaço em disco total da pasta raiz e otimiza o desempenho da transferência de arquivos para o computador de bordo do Genetec Patroller™.

  IMPORTANTE: Se a sua pasta raiz estiver em uma unidade de rede, o serviço Genetec™ Server deve ser configurado para ser executado com um usuário de domínio e não um usuário local.
- **Grupo de usuários para Patrollers:** Lista de usuários (e suas senhas) que podem fazer logon nos veículos de patrulha gerenciados pelo LPR Manager. Essa lista é baixada para os veículos de patrulha.
- **Período de retenção:** Especifica quantos dias de dados relacionados ao LPR o Security Center pode consultar. O padrão é 90 dias e o máximo é 4000 dias. A data de LPR que for mais antiga do que os valores especificados não aparece nas consultas e relatórios do Security Center (relatórios de ocorrências, relatórios de leituras e assim por diante).
  - **Genetec Patroller™ período de retenção de rota:** Número de dias em que os dados de Genetec Patroller™ *rota* (coordenadas GPS) são mantidos no banco de dados.
  - **Período de retenção de alerta:** Número de dias durante os quais os dados do alerta são mantidos na base de dados do Gerenciador LPR.
  - **Período de retenção de imagem de alerta:** Número de dias durante os quais a imagem do alerta é mantida pela função do Archiver conectado. The *Período de retenção de imagem de ocorrência* não pode exceder o *Período de retenção de ocorrência* uma vez que uma imagem de ocorrência está sempre associada a uma ocorrência.
  - **Período de retenção de leitura:** Número de dias durante os quais as *leituras de placa de licença* são mantidos na base de dados do Gerenciador LPR. O *período de retenção de leitura* não pode ultrapassar o *período de retenção de alerta*. Se a retenção de leitura for menor do que a retenção de alerta, apenas as leituras associadas aos alertas são mantidas.
  - **Período de retenção de imagem de leitura:** Número de dias em que os dados de leitura da imagem são mantidos pela função de Archiver ligado. O *período de retenção de leitura de imagem* não pode exceder o *período de retenção de leitura*, uma vez que uma leitura de imagem está sempre associada a uma leitura.
  - **Período de retenção de evento:** Número de dias durante os quais os eventos do Genetec Patroller™ (usuário conectado, desconectado e posições do veículo de patrulha) são mantidos na base de dados do LPR Manager.
  - **Período de retenção da ocupação de estacionamento:** Número de dias em que os dados da ocupação do estacionamento são mantidos na base de dados do LPR Manager.

- **Período de retenção de dados de zona de estacionamento:** Número de dias em que os dados da zona de estacionamento são mantidos na base de dados do LPR Manager. Esses dados incluem informações de sessão de estacionamento, por exemplo, os horários de início da sessão de estacionamento e transições de estado, assim como informações de eventos que ocorreram dentro da zona de estacionamento. O *período de retenção de dados da zona de estacionamento* não pode ultrapassar o *período de retenção de leitura*.

Ao vivo

As configurações *Dinâmicas* são usadas para definir como os dados são transferidos entre o Security Center e o Genetec Patroller™.

- **Porta de escuta:** Porta usada para escutar pedidos de conexão provenientes de câmeras Sharp fixas e veículos de patrulha. Depois que a conexão seja estabelecida, o LPR Manager pode receber atualizações dinâmicas das *unidades LPR* que gerencia.

  NOTA: Se você estiver usando vários LPR Managers, cada LPR Manager deve usar uma porta de escuta diferente.
- **Porta de descoberta de Sharp Sharp:** Porta usada pelo LPR Manager para encontrar unidades Sharp fixas na rede. O mesmo número de porta deve ser usado na configuração de *Porta de descoberta* no Sharp.

  NOTA: Ao configurar a porta de descoberta, não use a porta 5050, pois ela é reservada para o serviço do registrador.
- **Enviar na leitura (somente Sharp fixas):** As imagens do Sharp que são enviadas para o Security Center de cada leitura de placa. Essas imagens são exibidas no Security Desk ao monitorar eventos de LPR.
  - **Imagem da placa de licença:** Inclui a imagem de alta resolução da placa de licença junto com os dados de leitura da placa.
  - **Imagem do contexto:** Inclui a imagem de contexto de ângulo amplo junto com os dados de leitura da placa.
- **Segurança de canal:** Criptografa a comunicação entre o Security Center e o Genetec Patroller™.

  IMPORTANTE: Se você selecionar esta opção, a criptografia também deve ser ativada no Genetec Patroller™ do Config Tool.
  - **Criptografar o canal de comunicação:** Criptografa a comunicação entre o Genetec Patroller™ e o Security Center.
  - **Aceitar mensagens não criptografadas:** O Security Center aceitará as conexões recebidas de veículos de patrulha que não possuam a opção de criptografia ativada.

Associação de arquivos

As configurações de *Associação de arquivos* especificam quais listas de procurados e de autorização estão ativas e são gerenciadas pelo LPR Manager.

- **Listas de procurados:** Uma lista de todas as *listas de procurados* no Security Center. Selecione quais listas você deseja que o LPR Manager gerencie.
- **Autorizações:** Uma lista de todas as *autorizações* no Security Center. Selecione quais autorizações você deseja que o LPR Manager gerencie.

Correspondência

As configurações de *Correspondência* são usadas para ativar a correspondência entre listas de procurados e unidades Sharp fixas. Quando a correspondência está ativada, você pode configurar eventos causa-efeito no Security Desk que são acionados em eventos de *Correspondência* e *Não combina*.

- **Correspondência:** Quando a correspondência está ativada, você pode configurar eventos causa-efeito no Security Desk que são acionados quando o Sharp lê uma placa que está em uma lista de procurados que você ativou na Associação de arquivos.
- **Gerar eventos de Não combina:** O Security Center gera eventos de *Não combina* quando uma placa não é encontrada em uma lista de procurados específica. Você pode então configurar eventos causa-efeito Security Desk com base em eventos de *Não combina*.
- **Correspondência de leitura passada:** Quando a correspondência de leitura passada está ativada, o sistema compara listas novas ou atualizadas contra as leituras da placa de licença capturadas anteriormente.

  NOTE:

  - O período de retenção do banco de dados é configurável. Todos as ocorrências posteriores ao período de retenção configurado são excluídas do banco de dados.
  - Se um alerta de lista de procurados já tiver sido gerado para uma placa, a realização de correspondências de leitura passada não gera um alerta duplicado para a placa.
  - Listas de procurados federadas não podem ser usadas para a correspondência de leitura passada.
  - Se uma ocorrência for gerada com base em uma correspondência de leitura passada, ela é indicada na coluna **Correspondência passada** no relatório *Ocorrências* do Security Desk.
  - **Listas de procurados:** Selecione uma ou mais listas de procurados para serem usadas para a correspondência de leitura passada.
    NOTE: Para que uma lista de procurados seja usada com correspondência de leituras passadas, primeiro a lista deve ser associada à função ou câmera Sharp fixa para a qual a correspondência de leituras passadas foi ativada.
  - **Pesquisar hora para trás:** Define o limite de quão longe no passado o sistema procura leituras de placas quando a correspondência de leitura passada é acionada.

Geocodificação

O recurso de *Geocodificação* converte dados GPS brutos (longitude, latitude) de veículos de patrulha em endereços de rua. Os endereços de ruas são então salvos juntamente com as leituras no banco de dados do LPR Manager.

NOTA: Você precisa de geocodificação se seus veículos de patrulha estiverem equipados com GPS, mas sem mapas.

- **Tipo de mapa:** Exibe o tipo de mapa definido na licença do Security Center.
- **Pasta de mapas e dados:** Pasta onde os arquivos Benomad são encontrados. Esta pasta deve estar no mesmo computador onde o LPR Manager está instalado.

Filtrando placa de licença

As configurações de *Filtragem de placas* determinam o que fazer quando uma lista de procurados ou de autorização é modificada e o LPR Manager detecta que há entradas com caracteres inválidos (caracteres não alfanuméricos).

- **Caracteres válidos para placa de licença:** Os tipos de caracteres a serem filtrados (latino, árabe ou japonês).
- **Número de placa de licença inválido:** Como o LPR Manager lida com registros inválidos.
  - **Modificar registro:** (Configuração padrão). Exclui quaisquer caracteres não alfanuméricos do número da placa. Por exemplo, o número de placa "ABC #% 3" torna-se "ABC3".
  - **Remover registro:** Exclui toda a entrada da lista.

- **Registrar filtragem:** Selecione para registrar o processo de filtragem. Os registros de filtragem de placas de veículo são salvos na pasta raiz do AutoVu™: *C:\Genetec\AutoVu\RootFolder*.

Notificação de e-mail

A configuração de *Notificação por e-mail* ativa notificações por e-mail para ocorrências de listas de procurados e permite que você personalize a aparência e o conteúdo da mensagem de e-mail.

- **Nome de atributo de e-mail:** Usado para notificação de e-mail no nível da placa de licença individual. Digite o nome do atributo da lista de procurados relacionado à notificação por e-mail. Por exemplo, se você adicionou um atributo "Email" na aba Propriedades da entidade da lista de procurados, digite exatamente o mesmo nome aqui. Os nomes devem corresponder exatamente.
- **Anexos de e-mail:** Os dados LPR que são anexados ao e-mail de notificação e se devem ocultar os números da placa no corpo da mensagem.
  - **Imagem da placa de licença:** Imagens em close-up de alta resolução da placa de licença.
  - **Imagem do contexto:** Uma imagem colorida em ângulo maior do veículo.
  - **Imagem da roda:** Substitui a leitura de número de placa e o número da placa correspondente no e-mail com asteriscos (*).
- **Registrar e-mails:** Selecione esta opção para registrar a lista de procurados e receber e-mails de notificação. Os registros de e-mail são salvos na pasta raiz do AutoVu™: *C:\Genetec\AutoVu\RootFolder*.
- **Modelo:** Personaliza o e-mail. Faça um dos seguintes:
  - Edite a linha de assunto do e-mail ou o corpo da mensagem.
  - Alterne entre texto simples e HTML.
  - Adicione formatação (negrito, itálico, etc.).
  - Clique com o botão direito do mouse no corpo da mensagem para um menu de tags rápidas que você pode usar para adicionar mais informações ao e-mail.
  - Restaure o modelo de e-mail padrão a qualquer momento.

Importar XML

As configurações de *Importação XML* são usadas para importar dados de aplicativos de terceiros para o banco de dados do LPR Manager. Ao acionar esta configuração, o Security Center cria uma entidade de *Importação XML* e associa os dados importados a esta entidade. No Security Desk, será então possível filtrar por entidade de *Importação XML* ao executar relatórios de ocorrências ou de leituras.

NOTA: Esta opção requer uma licença. Entre em contato com o representante da Genetec Inc. para obter mais informações.

- **Arquivo de modelo XML lido:** Especifica onde o arquivo de modelo de leitura XML está localizado. Você encontrará um modelo padrão no pacote de instalação do Security Center em *Tools\LPR \XMLTemplatesSamples\XMLImport*.

  NOTA: Na maioria dos casos, o modelo padrão pode ser usado.
- **Pasta de dados XML:** Especifica a pasta que contém os arquivos de dados XML para o Security Center importar.

  NOTA: Os arquivos são excluídos desta pasta uma vez que foram processados.
- **Hashtags de importação XML suportadas:** São suportadas as seguintes hashtags de importação XML. Cada hashtag deve ter uma tag XML de abertura e encerramento (por exemplo, para usar a tag *#CONTEXT_IMAGE#*, você deve escrever <*ContextImage*>*#CONTEXT_IMAGE#*</*ContextImage*> no XML).
  - **#PLATE_READ#:** Placa de veículo conforme lida pelo Sharp.
  - **#PLATE_STATE#:** O estado emissor da placa, se lido.

- **#DATE_LOCAL#:** Data local do evento LPR.
- **#DATE_UTC#:** Data UTC do evento LPR.
- **#TIME_UTC#:** Hora UTC do evento LPR.
- **#TIME_ZONE#:** Fuso horário local para o evento LPR.
- **#CONTEXT_IMAGE#:** Imagem de contexto (JPEG com codificação em base 64).
- **#PLATE_IMAGE#:** Imagem da placa de licença (JPEG com codificação em base 64).
- **#LONGITUDE#:** Longitude do evento LPR (em graus decimais ou DMS).
- **#LATITUDE#:** Latitude do evento LPR (em graus decimais ou DMS).
- **#GUID#:** Identificador único do evento LPR.
- **#CUSTOM_FIELDS#:** Você pode importar outros campos com esta hashtag usando o formato de chave = valor. Formate a chave como #CUSTOM_FIELDS#{CHAVE}.
  NOTA: Você deve especificar um formato para as hashtag DATE e TIME. Por exemplo, #DATE_LOCAL#{aaaa/ MM/dd}). Clique aqui para obter mais informações sobre quais formatos usar. Se estas hashtags não estiverem incluídas, as datas e horários UTC são usados como base para calcular a hora local. Se ocorrer um erro, a hora em que a função LPR Manager importou os dados é usada

Exportar XML

As configurações de *Importação XML* são usadas para enviar leituras e alertas do LPR Manager para aplicativos de terceiros. As leituras e alertas são enviadas ao vivo à medida que ocorrem.

- **Pasta de modelos XML:** Especifica onde o arquivo de modelos XML está localizado. Você encontrará modelos padrão em *Program Files (x86)\Genetec Security Center X.X\Add-On\LPR\XMLTemplatesSamples \XMLExport*. Existem modelos XML para cada tipo de evento LPR (leituras de placas, alertas da lista de procurados, alertas de horas extras, alertas de autorizações e alertas de autorizações compartilhadas).

  NOTA: Na maioria dos casos, o modelo padrão pode ser usado.
- **Pasta de exportação XML:** Especifica a pasta que contém os arquivos XML exportados pelo LPR Manager.
- **Formato do horário:** Digite o formato de hora usado nos arquivos exportados. À medida que você configura o formato de hora, o campo de informações exibe qual será a aparência do formato de hora no arquivo XML.

  Para identificar as unidades de tempo use a seguinte notação:

Notação	Descrição
h	Hora
m	Minuto
s	Segundo
:	Deve-se usar dois pontos (:) entre as unidades de hora, minuto e segundo.
hh,mm,ss	Exibe a hora com o zero à esquerda. Por exemplo: 03:06:03 representa 3 horas, 6 minutos e 3 segundos.
h,m,s	Exibe sem o zero à esquerda. Por exemplo: 3:6:3 representa 3 horas, 6 minutos e 3 segundos.

tt	Inclui A.M. ou P.M. Se estiver usando um relógio de 12 horas, você pode querer usar a notação A.M. ou P.M. A unidade pode ser precedida por um espaço ou não. Por exemplo, HH:mm:ss tt exibe 17:38:42 PM.
h minúsculo	Relógio de 12 horas.
H maiúsculo	Relógio de 24 horas.

- **Formato de data:** Selecione um formato de data para usar nos arquivos exportados. Você pode escolher entre **MM/dd/aaaa** ou **aaaa-MM-dd**. Por exemplo, aaaa-MM-dd exibe 2016-06-21.
- **Hashtags XML suportadas:** São suportadas as seguintes hashtags de exportação XML. Cada hashtag deve ter uma tag XML de abertura e encerramento (por exemplo, para usar a tag *#CONTEXT_IMAGE#*, você deve escrever <*ContextImage*>*#CONTEXT_IMAGE#*</*ContextImage*> no XML).
  - **#ACCEPT_REASON#:** Motivo pelo qual o alerta foi aceito.
  - **#ATTRIBUTES#:** Gera os atributos de todas as Leituras e Alertas.
  - **#CAMERA_NAME#:** Nome da câmera.
  - **#CONTEXT_IMAGE#:** Imagem de contexto (JPEG com codificação em base 64).
  - **#DATE_LOCAL#:** Data local do evento LPR.
  - **#ELAPSED_TIME#:** Para uma alerta de horas extras, esta tag indica a diferença de horário entre as duas leituras de placas (a exibição do número de dias é opcional).
  - **#FIRST_VEHICLE#:** Para uma ocorrência de autorização compartilhada, esta tag gera o conteúdo especificado em *ReadTemplate.xml* para o primeiro veículo visto.
  - **#FIRST_VEHICLE_FROM_STREET#:** Para uma ocorrência de tempo extra, esta tag recupera o atributo *Da rua* na primeira leitura de placa.
  - **#FIRST_VEHICLE_TO_STREET#:** Para uma ocorrência de tempo extra, esta tag recupera o atributo *Para a rua* na primeira leitura de placa.
  - **#HOTLIST_CATEGORY#:** Campo de categoria da lista de procurados que gerou o alerta.
  - **#GUID#:** Identificador único do evento LPR.
  - **#INVENTORY_LOCATION#:** Para instalações MLPI, a localização do inventário do veículo.
  - **#ISHIT#:** Esta tag indica se o evento LPR é um alerta.
  - **#LATITUDE#:** Latitude do evento LPR (em graus decimais).
  - **#LATITUDE#{dms}:** Latitude do evento LPR (em graus, minutos e segundos).
  - **#LATITUDE#{dec}:** Latitude do evento LPR (em graus decimais).
  - **#LATITUDE_DEGREE#:** Latitude do evento LPR (graus).
  - **#LATITUDE_DMS#:** Latitude do evento LPR (em graus, minutos e segundos).
  - **#LATITUDE_MINUTE#:** Latitude do evento LPR (minutos).
  - **#LATITUDE_SECOND#:** Latitude do evento LPR (segundos).
  - **#LONGITUDE#:** Longitude do evento LPR (em graus decimais).
  - **#LONGITUDE#{dec}:** Longitude do evento LPR (em graus decimais).
  - **#LONGITUDE#{dms}:** Latitude do evento LPR (em graus, minutos e segundos).
  - **#LONGITUDE_DEGREE#:** Longitude do evento LPR (graus).
  - **#LONGITUDE_DMS#:** Longitude do evento LPR (em graus, minutos e segundos).
  - **#LONGITUDE_MINUTE#:** Longitude do evento LPR (minutos).
  - **#LONGITUDE_SECOND#:** Longitude do evento LPR (segundos).

- **#MATCHED_PLATE#:** Placa de licença contra a qual o alerta foi gerado.
- **#ORIGINAL#:** Para uma ocorrência de tempo extra, esta tag gera o conteúdo especificado em *ReadTemplate.xml* para a primeira leitura de determinada placa.
- **#OVERVIEW_IMAGE#:** Imagem de visão geral (JPEG com codificação em base 64).
- **#PATROLLER_ID#:** ID da unidade Patroller.
- **#PATROLLER_NAME#:** Nome da unidade de veículo de patrulha.
- **#PERMIT_NAME#:** Nome da autorização que gerou o evento LPR.
- **#PLATE_IMAGE#:** Imagem da placa de licença (JPEG com codificação em base 64).
- **#PLATE_READ#:** Placa de veículo conforme lida pelo Sharp.
- **#PLATE_STATE#:** O estado emissor da placa, se lido.
- **#REJECT_REASON#:** Motivo pelo qual o alerta foi rejeitado.
- **#READ#:** Incorpora o conteúdo de *ReadTemplate.xml* dentro de outro modelo XML (útil para ocorrências).
- **#RULE_COLOR#:** Cor da regra associada ao evento LPR.
- **#RULE_ID#:** ID da regra associada ao evento LPR.
- **#RULE_NAME#:** Nome da regra associada ao evento de LPR (lista de procurados, tempo extra, autorização ou restrição da autorização).
- **#SECOND_VEHICLE#:** Para uma ocorrência de autorização compartilhada, esta tag gera o conteúdo especificado em *ReadTemplate.xml* para o segundo veículo visto.
- **#SECOND_VEHICLE_FROM_STREET#:** Para uma ocorrência de tempo extra, esta tag recupera o atributo *Da rua* na segunda leitura de placa.
- **#SECOND_VEHICLE_TO_STREET#:** Para uma ocorrência de tempo extra, esta tag recupera o atributo *Para a rua* na segunda leitura de placa.
- **#SHARP_NAME#:** Nome do Sharp que leu a placa.
- **#STATE#:** O estado emissor da placa, se lido.
- **#TIME_LOCAL#:** Horário local.
- **#USER_ACTION#:** Ação do usuário relacionada ao evento LPR.
- **#USER_ID#:** ID do usuário.
- **#USER_NAME#:** Nome do usuário.
- **#VEHICLE#:** O mesmo que #READ#.

Provedor de atualização

Ative o *Provedor de atualizações* para criar a subpasta necessária na pasta raiz de LPR que receberá os arquivos de atualização. Além disso, é necessário especificar a *Porta de escuta* usada para atualizações do Genetec Patroller™ e do Sharp. O LPR Manager usa esta porta para atualizar veículos de patrulha e Sharp com novos hot fixes, sons de alerta de ocorrência, listas de procurados, firmware e assim por diante.

- **Porta de escuta:** Porta que o Security Center usa para enviar atualizações para veículos de patrulha e unidades Sharp conectadas, bem como para Sharps fixas na rede. Certifique-se de usar o mesmo número de porta no Genetec Patroller™ do Config Tool (consulte o *Guia de Administrador do Genetec Patroller™*) e no Sharp Portal (consulte o *Guia de Administrador do Sharp*).

AutoVu™ Free-Flow

Ative *AutoVu™ Free-Flow* para configurar a exportação XML de eventos de estacionamento para provedores terceiros de autorização de estacionamento que usam o plug-in Pay-by-Plate Sync.

- **Correspondência:**
  - **Limite de tolerância de correspondência:** Este valor indica o número de diferenças de caractere simples entre leituras de placa de entrada e saída que serão ainda consideradas uma correspondência. Definir o valor para 0 é equivalente a uma correspondência exata.
    IMPORTANTE: Definir para um valor demasiado elevado faz com que leituras de placa sejam associadas ao veículo errado. O valor padrão é 1.
- **Pay-by-Plate:**
  - **Servidor:** Digite o endereço IP da máquina onde o Pay-by-Plate Sync está instalado.
  - **Porta:** Digite o número de porta para a conexão do Pay-by-Plate Sync (padrão: 8787).
- **Exportar XML:**
  - **Pasta de exportação XML:** Especifique a pasta de exportação para dados XML do AutoVu™ Free-Flow.
  - **Incluir imagens do veículo na exportação:** Por padrão, as imagens de veículos não são incluídas no arquivo XML exportado. Para incluir imagens de veículos, selecione **Incluir imagens de veículos no relatório**.
    NOTA: Incluir imagens de veículos aumenta o tamanho do arquivo de exportação XML.
  - **Exportar ocupação:**
    Exporta dados de ocupação de zona de estacionamento para um arquivo XML separado.
  - **Exportar violações:** Quando um veículo está em violação, as informações do veículo são exportadas como um arquivo XML separado.
  - **Exportar sessões concluídas:** Quando um veículo sai do parque de estacionamento, as informações da sessão de estacionamento são exportadas como um arquivo XML separado.
- **Eventos:**
  - **Limite de capacidade:** Especifica o limite de capacidade da zona de estacionamento quando um evento de *limite de capacidade atingido* é gerado.

LPR Manager - Aba Recursos

Clique na aba **Recursos** para configurar os servidores e o banco de dados atribuídos a esta função.

- **Servidores:** Servidores que hospedam esta função.
- **Status do banco de dados:** Status atual do banco de dados.
- **Servidor de banco de dados:** Nome do serviço SQL Server (padrão=`(local)\SQLEXPRESS`).
- **Banco de dados:** Nome da instância do banco de dados.
- **Ações:** Funções de manutenção que você pode realizar no banco de dados da função:
  - **Criar um banco de dados ( ):** Crie um novo banco de dados..
  - **Excluir o banco de dados ( ):** Exclua o banco de dados..
  - **Informações do banco de dados ( ):** Mostrar informações do banco de dados.
  - **Notificações ( ):** Definir notificações para quando o espaço do banco de dados estiver se esgotando.
  - **Backup/restauração ( ):** Faça backup de ou restaure o banco de dados.
- **Imagens salvas na:** função Archiver responsável por gerir as imagens (imagens de placas de veículo, contextuais e WMS) que são associadas a leituras e ocorrências.

  MELHOR PRÁTICA: Selecione um Archiver que não esteja gerindo também unidades de vídeo. Se todas as funções Archiver atuais estiverem gerindo unidades de vídeo, crie uma nova.

NOTA: Ao usar o banco de dados Azure baseado em nuvem, as opções *Notificações* e *Backup/restauração* estão desativadas.

Abas de configuração do Map Manager

Você define as configurações da função Map Manager a partir da visualização **Funções** da tarefa *Sistema* no Security Center do Config Tool.

Map Manager - Aba Propriedades

Clique na aba **Propriedades** para alterar as configurações padrão para essa função e configurar os recursos externos gerenciados por essa função, como os provedores de mapas e os objetos KML.

- **Provedores de mapas:** Lista de provedores de mapas de terceiros (*GIS*) que você tem licença para usar.
- **Camadas do mapa:** Lista de objetos KML importados que podem ser exibidos em qualquer mapa georeferenciado. Cada objeto KML corresponde a uma camada de mapa distinta que os usuários do Security Desk podem escolher mostrar ou ocultar.
- **Local do cache:** O cache é uma pasta onde os ladrilhos de mapas são salvos. Quando você cria mapas a partir de arquivos de imagens, a função gera um conjunto de pequenas imagens, chamadas de *ladrilhos do mapa*, para cada nível de zoom no qual você precisa visualizar o mapa. Quanto maior a escala do mapa, mais ladrilhos de mapa precisam ser gerados pela função. A pasta padrão é *C:\ProgramData\Security Center\Maps.*.
- **Porta:** Porta HTTP usada pelo Map Manager para se comunicar com aplicativos do cliente. (Default=8012).
- **Mapa padrão:** O mapa padrão do sistema, também conhecido como *mapa padrão global*, é usado quando um usuário não tem um mapa padrão personalizado configurado. Você só pode definir o mapa padrão global depois de ter criado seu primeiro mapa.

Map Manager - Aba Recursos

Clique na aba **Recursos** para configurar os servidores atribuídos a esta função. A função Map Manager não exige um banco de dados.

- **Servidores:** Servidores que hospedam esta função.

Tópicos relacionados

Criar mapas na página 244

Abas de configuração do Media Gateway

Você configura a função Media Gateway a partir da tarefa *Vídeo* no Security Center do Config Tool.

Media Gateway - aba Propriedades

Clique na aba **Propriedades** para configurar o endereço de multicast de início e a porta RTSP para o Media Gateway, e você pode habilitar a comunicação segura entre a função e os aplicativos do cliente RTSP.

- **Endereço inicial de multicast:** Endereço multicast de início e número da porta. No multicast, todas as fontes de vídeo são transmitidas para diferentes endereços multicast enquanto usam o mesmo número de porta, porque os switches e roteadores multicast usam o endereço IP de destino para fazer suas decisões de roteamento. De igual forma, o Media Gateway atribui o mesmo número de porta a todas as câmeras de transmissão, começando com o endereço IP especificado e adicionando 1 para cada nova câmera encontrada.
- **Porta de escuta:** Porta de comando TCP recebida usada pelo Media Gateway.
- **Autenticação do usuário:** Permite a autenticação entre os aplicativos de cliente Media Gateway e RTSP.

  IMPORTANTE: As câmeras que um aplicativo cliente RTSP pode exibir no sistema dependem da conta de usuário que o cliente usa para fazer logon no Security Center. Atribua uma senha a cada conta de usuário adicionada à lista, de preferência uma senha diferente da usada no Security Center.
- **Usar as portas Web padrão do servidor:** Por padrão, o Media Gateway se comunica com dispositivos e o Web Client com a porta HTTPS 443 e a porta HTTP 80. Essas portas são definidas no servidor que hospeda a função Web Client Server. Se a sua política de TI requer portas diferentes, ou existe algum tipo de conflito, você pode alterar as portas. Defina **Usar as portas da web padrão do servidor** como **Desligado**, em seguida, altere a porta HTTP e as configurações de porta HTTP seguras.

  IMPORTANTE: Se você tiver um certificado SSL sem assinatura (inválido) e os usuários finais forem monitorar vídeo no Web Client usando navegadores Mozilla Firefox ou Microsoft Edge, certifique-se de que as portas configuradas no Gateway de Mídia correspondem às portas no Web Client Server.
- **Endereço da Web:** Defina o sufixo da URL usada pela função Web Client Server para se conectar ao Media Gateway. O padrão é *mídia*. O formato da URL é *host:port/web address*; onde *host* é o endereço IP ou nome do host do computador do servidor que hospeda o Media Gateway, *port* é a porta HTTP 80 (padrão) ou a porta HTTPS 443 (padrão) e o endereço da web é *mídia* (padrão).

Media Gateway - aba Recursos

Clique na aba **Recursos** para configurar os servidores atribuídos a esta função. A função Media Gateway não exige um banco de dados.

- **Servidores:** Servidores que hospedam esta função.

Abas de configuração do Media Router

Você define as configurações da função Media Router a partir da tarefa *Vídeo* no Security Center do Config Tool.

Media Router - aba Propriedades

Clique na aba **Propriedades** para configurar os redirecionadores de stream, a extremidade inicial de *multicast* e a porta RTSP para o Media Router.

- **Redirecionadores:** Servidores atribuídos para hospedar *agentes redirecionadores*, módulos de software lançados pelo Media Router para redirecionar fluxos de dados de uma extremidade IP para outra.
  - **Servidor:** Servidor selecionado para hospedar o agente redirecionador.
  - **Intervalo de portas UDP de entrada:** Intervalo de portas usadas pelo agente redirecionador para enviar vídeo usando *UDP*. Se o agente redirecionador estiver executando por trás de um firewall, certifique-se de que essas portas estejam desbloqueadas para pacotes de entrada para conexões UDP.
  - **Capacidade de vídeo ao vivo:** Limita o número máximo de streams ao vivo que podem ser redirecionadas por este servidor (redirecionador). Este recurso impede a sobrecarga do servidor com excesso de usuários que tentam visualizar simultaneamente o vídeo que precisa de redirecionamento. Quando o limite é alcançado, uma mensagem de erro é exibida no aplicativo cliente quando os usuários solicitam o vídeo ao vivo, afirmando que a capacidade de stream foi ultrapassada.
  - **Capacidade de reprodução:** Limita o número máximo de reproduções de streams que podem ser redirecionadas por este servidor (redirecionador). Este recurso impede a sobrecarga do servidor com excesso de usuários que tentam visualizar simultaneamente o vídeo que precisa de redirecionamento. Quando o limite é alcançado, uma mensagem de erro é exibida no aplicativo cliente quando os usuários tentam solicitar reprodução do vídeo, afirmando que a capacidade de stream foi ultrapassada.
  - **Controle de largura de banda:** Limita a largura de banda máxima para streams de vídeo que podem ser redirecionados por este servidor (redirecionador). Você também pode configurar um novo limite de largura de banda para vídeo ao vivo e de reprodução. Este recurso impede a sobrecarga da rede com excesso de streams de vídeo vindos de um local remoto que tenha largura de banda limitada. Quando o limite é alcançado e os usuários solicitam uma nova transmissão de vídeo, uma mensagem é exibida afirmando que o limite de largura de banda foi ultrapassado. Se o limite de largura de banda for alcançado e um usuário com um alto *nível de usuário* solicitar um stream, o usuário com o nível de usuário mais baixo que estiver visualizando o vídeo que está sendo redirecionado desse redirecionador perde sua conexão de stream de vídeo. Se vários usuários com o mesmo nível de usuário estiverem exibindo streams de vídeo redirecionados, o usuário que solicitou o stream de vídeo por último perde a conexão do stream.
  - **Estratégia de redirecionamento:** Se você tiver múltiplas placas de rede, você poderá especificar as ações realizadas em cada placa de rede. Por exemplo, você pode querer especificar que a exportação de vídeo e a transferência de vídeo somente possam ser realizadas por sua placa de rede sem fio. Para mais informações, consulte Configurar o uso de placas de rede para um redirecionador on page 465.
    NOTE: Por padrão, todas as ações são realizadas em todas as placas de rede disponíveis.
  - **Interface de multicast:** Adaptador de rede a usar para streaming de dados no modo multicast.
  - **Porta RTSP:** Porta usada pelo agente redirecionador para receber comandos TCP.
    NOTE: Se você configurar o agente redirecionador no servidor que hospeda o Media Router, a porta RTSP não pode ser a mesma usada pelo Media Router.
  - **Porta RTP:** Porta usada pelo agente redirecionador para stream de dados de vídeo ao vivo usando TCP.

- **Iniciar multicast do ponto de vigilância:** Endereço multicast de início e número da porta. No multicast, todas as fontes de áudio e vídeo são transmitidas para diferentes endereços multicast enquanto usam o mesmo número de porta, porque os switches e roteadores multicast usam o endereço IP de destino para fazer suas decisões de roteamento. Da mesma forma, o Media Router atribui o mesmo número de porta a todos os dispositivos de streaming (microfones e câmeras), começando com o endereço IP especificado e adicionando 1 para cada novo dispositivo encontrado.

  NOTA: Se você estiver usando o Windows Server 2008 ou anterior, poderá melhorar consideravelmente o desempenho do sistema atribuindo manualmente um número de porta diferente para cada dispositivo de streaming.
- **Porta RTSP:** Porta de comando TCP recebida usada pelo Media Router.
- **Usar comunicação segura:** Criptografa todas as solicitações de vídeo RTSP. Quando a comunicação segura está ativada, todas as comunicações de vídeo usam RTSP sobre TLS. Se sua rede estiver configurada para Multicast ou Unicast UDP, somente o canal de controle RTSP será criptografado. Se sua rede estiver configurada para Unicast TCP, somente o canal de controle RTSP será criptografado para redirecionamento de vídeo ao vivo. A reprodução de vídeo e exportação de vídeo sempre usa RTSP sobre TCP, portanto, o canal de controle RTSP e o canal de dados de vídeo são ambos criptografados.

  IMPORTANTE: A comunicação segura é ativada como padrão em novas instalações, mas desativada se você atualizar de uma versão anterior à 5.5. Quando a comunicação segura está ativada, os sistemas Security Center mais antigos que o 5.5 não podem federar o seu sistema Security Center.

Media Router - aba Recursos

Clique na aba **Recursos** para configurar os servidores e o banco de dados atribuídos a esta função.

- **Servidores:** Servidores que hospedam esta função.
- **Status do banco de dados:** Status atual do banco de dados.
- **Servidor de banco de dados:** Nome do serviço SQL Server (padrão=`(local)\SQLEXPRESS`).
- **Banco de dados:** Nome da instância do banco de dados.
- **Ações:** Funções de manutenção que você pode realizar no banco de dados da função:
  - **Criar um banco de dados ( ):** Crie um novo banco de dados..
  - **Excluir o banco de dados ( ):** Exclua o banco de dados..
  - **Informações do banco de dados ( ):** Mostrar informações do banco de dados.
  - **Notificações ( ):** Definir notificações para quando o espaço do banco de dados estiver se esgotando.
  - **Backup/restauração ( ):** Faça backup de ou restaure o banco de dados.

Abas de configurações Omnicast™ Federation™

Você define as configurações da função Omnicast™ Federation™ a partir da visualização *Funções* da tarefa *Sistema* em Security Center do Config Tool.

Omnicast™ Federation™ - Aba Identidade

Clique na aba **Identidade** para visualizar informações descritivas sobre esta função e pular para a página de configuração de entidades relacionadas.

- **Grupo de funções:** Uma configuração avançada que só é necessária se você planeja hospedar mais de 40 funções do Omnicast™ Federation™ no mesmo servidor.

Omnicast™ Federation™ - Aba Propriedades

Clique na aba **Propriedades** para configurar os parâmetros de conexão ao sistema Omnicast™ remoto e os eventos e transmissões de vídeo padrão que deseja receber dele.

- **Status da conexão:** Mostra o status de conexão da função Federation™ para o sistema Omnicast™ remoto.
- **Diretório:** Nome do Gateway Omnicast™ que conecta você ao sistema Omnicast™ remoto.
- **Nome de usuário e senha:** Credenciais utilizadas pela função Federation™ para fazer logon no sistema Omnicast™ remoto. Os direitos e privilégios daquele usuário determinam o que seus usuários locais podem ver e fazer no sistema federado remoto.
- **Versão:** Versão do sistema Omnicast™ federado. Esta lista contém apenas versões Omnicast™ para as quais você instalou um pacote de compatibilidade.
- **Fluxo de vídeo ao vivo padrão:** Transmissão de vídeo padrão usada para visualizar vídeos ao vivo em câmeras Omnicast™ federadas.
- **Eventos federados:** Selecione os eventos que deseja receber do sistema Omnicast™ federado. Os eventos são necessários se você planeja monitorar as entidades federadas no Security Desk ou configurar eventos causa-efeito para as *entidades federadas*.
- **Reiniciar a conexão:** Force a função Federation™ a se reconectar ao sistema remoto.

Omnicast™ Federation™ - Aba Recursos

Clique na aba **Recursos** para configurar os servidores e o banco de dados atribuídos a esta função. A função Omnicast™ Federation™ não exige um banco de dados.

- **Servidores:** Servidores que hospedam esta função.

Abas de configuração do Gerenciador de relatórios

Você define as configurações da função Gerenciador de relatórios a partir da visualização **Funções** da tarefa *Sistema* no Security Center do Config Tool.

Gerenciador de relatórios - Aba Propriedades

Clique na aba **Propriedades** para configurar o comportamento padrão desta função.

- **Número máximo de resultados para relatórios em lote:** Define o número máximo de resultados que podem ser devolvidos pelas ações *Enviar relatório por e-mail* ou *Exportar relatório*.
- **Pasta de destino:** A pasta de destino para os relatórios que são salvos usando a ação *Exportar relatório*. Você pode selecionar uma unidade local ou uma unidade de rede.

Report Manager - Aba Recursos

Clique na aba **Recursos** para configurar os servidores atribuídos a esta função. A função Report Manager não exige um banco de dados.

- **Servidores:** Servidores que hospedam esta função.

Abas de configuração do Security Center Federation™

Você define as configurações da função Security Center Federation™ a partir da visualização *Funções* da tarefa *Sistema* em Security Center do Config Tool.

Security Center Federation™ - Aba Identidade

Clique na aba **Identidade** para visualizar informações descritivas sobre esta função e saltar para a página de configuração de entidades relacionadas além das opções gerais.

- **Grupo de funções:** Uma configuração avançada que só é necessária se você planeja hospedar mais de 100 funções do Security Center Federation™ no mesmo servidor.

Security Center Federation™ - Aba Propriedades

Clique na aba **Propriedades** para configurar os parâmetros de conexão ao sistema Security Center remoto e os eventos e transmissões de vídeo padrão que deseja receber dele.

- **Status da conexão:** Mostra o status de conexão da função Federation™ para o sistema Security Center remoto.
- **Diretório:** Nome do servidor principal para o sistema Security Center remoto.
- **Nome de usuário e senha:** Credenciais utilizadas pela função Federation™ para fazer logon no sistema Security Center remoto. Os direitos e privilégios daquele usuário determinam o que seus usuários locais podem ver e fazer no sistema federado remoto.
- **Conexão resiliente:** Quando essa opção é ativada, se a conexão entre a função Federation™ e o servidor do Security Center Directory federado for temporariamente interrompida, a função Federation™ tentará reconectar-se ao Directory por um período de tempo definido antes que a conexão seja considerada perdida e a função entre em um estado de aviso.
- **Tempo limite de reconexão expirado:** Especifique o número de segundos durante os quais a função Federation™ tenta se reconectar ao Directory antes de a conexão ser considerada perdida.
- **Fluxo de vídeo ao vivo padrão:** Transmissão de vídeo padrão usada para visualizar vídeos ao vivo em câmeras Security Center federadas.
- **Habilitar solicitações de reprodução:** Quando esta opção está ativada, os usuários podem visualizar vídeo de reprodução de câmeras Security Center federadas.
- **Federar alarmes:** Quando esta opção está ativada, são recebidos alarmes do sistema Security Center federado.
- **Eventos federados:** Selecione os eventos que deseja receber do sistema Security Center federado. Os eventos são necessários se você planeja monitorar as entidades federadas no Security Desk ou configurar eventos causa-efeito para as *entidades federadas*.

Security Center Federation™ - Aba Recursos

Clique na aba **Recursos** para configurar os servidores atribuídos a esta função.A função Security Center Federation™ não exige um banco de dados.

- **Servidores:** Servidores que hospedam esta função.

Abas de configuração Web-based SDK

Você define as configurações da função Web-based SDK a partir da visualização **Funções** da tarefa *Sistema* no Security Center do Config Tool.

SDK com base na Web - aba Propriedades

Clique na aba **Propriedades** para configurar o que os desenvolvedores externos precisam saber para usar os serviços Web.

- **Porta + URI de Base:** Esses dois parâmetros são usados para determinar o endereço do serviço da Web.

  Por exemplo, com Port=4590 e Base URI=WebSdk, o endereço do serviço Web seria “http://<computer>:4590/WebSdk/”, onde <computer> é o nome DNS ou o endereço IP público do servidor que hospeda a função Web-based SDK.
- **Porta de fluxo:** Porta usada para transmitir os eventos. Você pode configurar quais eventos escutar.
- **Usar conexão SSL:** Ative esta opção (padrão = desligado) para usar criptografia *SSL* para comunicações com o serviço Web. Se você estiver usando criptografia SSL, o endereço do serviço Web usa *https* em vez de *http*.
- **Configurações SSL:** Configurações necessárias quando você estiver usando criptografia SSL.
  - **Certificado:** Nome do certificado para usar. Use o formato: “CN=NameOfTheCertificate”. O certificado deve estar registrado no Windows. Você pode encontrar procedimentos na web sobre como fazer isso.
  - **Associar certificado à porta:** Ative esta opção (padrão = desligado) para vincular o certificado à porta. Esta operação faz o mesmo que você faria normalmente com o Windows.

SDK com base na Web - aba Recursos

Clique na aba **Recursos** para configurar os servidores atribuídos a esta função. A função SDK com base na Web não exige um banco de dados.

- **Servidores:** Servidores que hospedam esta função.

Abas de configuração do Web Client Server

Você define as configurações do Web Client Server a partir da visualização **Funções** da tarefa *Sistema* no Security Center do Config Tool.

Servidor de Cliente Web - aba Propriedades

Clique na aba **Propriedades** para configurar o tempo de sessão do usuário, estatísticas de uso, a URL, configurações de porta e o certificado SSL.

- **Tempo de sessão ilimitado:** Ativa ou desativa a duração de uma sessão de usuário. Defina **Tempo de sessão ilimitado** para **Ligado** para que os usuários permaneçam conectados ao Web Client enquanto mantiverem sua janela do navegador aberta. Defina **Tempo de sessão ilimitado** para **Desligado** para que os usuários terminem sessão no Web Client automaticamente após 12 horas de inatividade.
- **Endereço da Web:** Defina o sufixo da URL que os usuários digitam para se conectar ao Web Client. O padrão é *SecurityCenter*. O formato da URL completa do Web Client é *https://host:port/web address*, onde *host* é o endereço IP ou nome de host de computadores do servidor que hospeda o Web Client Server, *porta* é a porta HTTP (padrão) ou a porta HTTPS 443 (padrão) e o *endereço Web* é *SecurityCenter* (padrão). A URL de cada função Web Client deve ser exclusiva.
- **Local do cofre:** Quando você baixa vídeos, os arquivos são compactados e temporariamente armazenados no cofre do Web Client. Esses arquivos temporários são excluídos quando o download está completo. A localização padrão é *ProgramData\Security Center\WebClientExports*.
- **Usar as portas Web padrão do servidor:** Como padrão, o Web Client se comunica pela porta HTTPS 443 e a porta HTTP 80. Essas portas são definidas no servidor que hospeda a função Web Client Server. Se a sua política de TI exigir portas diferentes, ou se existir algum tipo de conflito, você pode alterar as portas usadas pelo Web Client. Para alterar as portas padrão, defina **Usar as portas Web padrão do servidor** como **Desligado** e, em seguida, altere a porta HTTP e a porta HTTP segura.

  IMPORTANTE: Se você tiver um certificado SSL sem assinatura (inválido) e os usuários finais forem monitorar vídeo no Web Client usando navegadores Mozilla Firefox ou Microsoft Edge, certifique-se de que as portas configuradas no Gateway de Mídia correspondem às portas no Web Client Server.
- **Configurações de comunicação:** Visualiza a URL e o certificado SSL em uso.
  - Clique na URL para abrir o Web Client do Security Center no seu navegador da Web padrão.
  - Clique em **Visualizar** para ver informações detalhadas sobre o certificado e para instalar o certificado.

  O certificado SSL fornece uma conexão HTTP segura ao Web Client. Você pode continuar usando o certificado SSL auto-assinado que está instalado com a função Web Client Server ou instalar um certificado assinado de uma Autoridade de Certificação, como a VeriSign. Em ambos os casos, as comunicações são criptografadas e seguras. No entanto, os usuários do Web Client são notificados pelo navegador da Internet de que o certificado autoassinado não é válido até que o certificado esteja instalado em cada computador que execute uma sessão do Web Client.

Web Client Server - Aba Recursos

Clique na aba **Recursos** para configurar os servidores atribuídos a esta função. A função Web Client Server não exige um banco de dados. Idealmente, cada função é atribuída a um único servidor. Você pode adicionar mais de um servidor para failover e balanceamento de carga.

- **Servidores:** Servidores que hospedam esta função.

Abas de configuração do Zone Manager

Você define as configurações da função Zone Manager a partir da visualização **Funções** da tarefa *Sistema* no Security Center do Config Tool.

Zone Manager - Aba Propriedades

Clique na aba **Propriedades** para configurar o período de retenção dos eventos de zona no banco de dados.

- **Manter eventos:** Especifique quanto tempo manter os eventos de zona registrados pelo Zone Manager no banco de dados antes de serem excluídos.

Zone Manager - Aba Recursos

Clique na aba **Recursos** para configurar os servidores e o banco de dados atribuídos a esta função.

- **Servidores:** Servidores que hospedam esta função.
- **Status do banco de dados:** Status atual do banco de dados.
- **Servidor de banco de dados:** Nome do serviço SQL Server (padrão=`(local)\SQLEXPRESS`).
- **Banco de dados:** Nome da instância do banco de dados.
- **Ações:** Funções de manutenção que você pode realizar no banco de dados da função:
  - **Criar um banco de dados ( ):** Crie um novo banco de dados..
  - **Excluir o banco de dados ( ):** Exclua o banco de dados..
  - **Informações do banco de dados ( ):** Mostrar informações do banco de dados.
  - **Notificações ( ):** Definir notificações para quando o espaço do banco de dados estiver se esgotando.
  - **Backup/restauração ( ):** Faça backup de ou restaure o banco de dados.

53

Tarefas de administração

Esta seção lista as opções nas tarefas de administração do Security Center que possuem uma visualização de configurações gerais, onde você pode definir configurações gerais ou específicas da solução para o seu sistema.

Esta seção inclui os seguintes tópicos:

- "Tarefa LPR - Visualização de configurações gerais" na página 1086
- "Tarefa do sistema - Configurações gerais - Página Campos personalizados" na página 1089
- "Tarefa do sistema - Configurações gerais - Página Eventos" na página 1090
- "Tarefa do sistema - Configurações gerais - Página de ações" na página 1091
- "Tarefa do sistema - Configurações gerais - Página de ID lógico" na página 1092
- "Tarefa do sistema - Configurações gerais - Página de configurações de senha do usuário" na página 1093
- "Tarefa do sistema - Configurações gerais - Página de trilhas de atividades" na página 1094
- "Tarefa do sistema - Configurações gerais - Página de áudio" na página 1095
- "Tarefa do sistema - Configurações gerais - Página de níveis de ameaça" na página 1096
- "Tarefa do sistema - Configurações gerais - Página de categorias de incidentes" na página 1097
- "Tarefa do sistema - Configurações gerais - Página Recursos" na página 1098
- "Tarefa de controle de acesso - Visualização de configurações gerais" na página 1099

Tarefa LPR - Visualização de configurações gerais

Esta seção lista as configurações encontradas na visualização *Configurações gerais* da tarefa LPR.

Configurações gerais - Página aplicativos

A página *Aplicativos* permite configurar a forma como o Security Desk exibe mapas nas tarefas *Monitoramento* e *Reprodução da rota*. Você também pode limitar o número de tentativas de logon no Genetec Patroller™, impor configurações de privacidade no Genetec Patroller™ e definir os atributos que um usuário do Genetec Patroller™ deve inserir ao fiscalizar uma ocorrência.

- **Tipo de mapa:** Exibe o tipo de sistema de mapa suportado pela licença do Security Center.
- **Cor para leituras:** Clique para selecionar a cor usada para exibir *leituras de placas de veículo* nos mapas.
- **Requer motivo ao gerar relatório do LPR:** Quando definido como **Ligado**, uma caixa de diálogo *Motivo necessário* é exibida ao gerar qualquer relatório que contenha dados de LPR. Isso garante que o motivo para a pesquisa de LPR seja registrado e incluído em registro de auditoria de trilha de atividade (relatório gerado) para cumprir as leis estaduais.
- **Longitude/latitude inicial:** Defina a localização inicial padrão para exibição de mapas no Security Desk. Você pode digitar as coordenadas nos campos ou clicar em Selecionar e ampliar em um local e clicar em Selecionar. Um alfinete vermelho parece indicar a posição selecionada.
- **Tentativas de logon antes de bloquear:** Você pode especificar o número de tentativas de login sem sucesso que um Genetec Patroller™ pode fazer antes que a conta seja bloqueada. Por exemplo, se o limite for definido como 3, os usuários do Genetec Patroller™ têm três tentativas para fazer logon no Genetec Patroller™ com seu nome de usuário e senha. Na quarta tentativa, suas contas serão bloqueadas e não poderão fazer logon. Os usuários com contas bloqueadas devem entrar em contato com seus administradores para que a senha seja redefinida. O Genetec Patroller™ deve ser conectado ao servidor do Security Center para que a senha seja redefinida.
- **Privacidade:** Configure o Genetec Patroller™ para obscurecer os números de placas de veículo ou para excluir as imagens de placa, contexto ou de roda das leituras e ocorrências, de modo que as informações não sejam armazenadas no banco de dados do LPR Manager.
  - **Imagens de placa de licença, contexto ou volante:** Quando definido como *Ligado*, as imagens não são enviadas para o Security Center nem incluídas em dados descarregados.
  - **Placa de licença:** Quando definido como *Ligado*, a sequência de texto do número da placa é substituída por asteriscos (*) quando é enviada para o Security Center ou nos dados descarregados.
- **Atributos de alerta autuado:** Crie campos de entrada de texto onde os usuários do Genetec Patroller™ devem inserir texto quando *impõem* uma ocorrência. As informações dos campos de texto da ocorrência fiscalizada podem ser consultadas no relatório de ocorrências do Security Desk.

Configurações gerais - Página de lista de procurados

A página *Lista de procurados* permite definir os atributos, motivos e categorias personalizados que aparecerão no Genetec Patroller™ quando o usuário adiciona uma entrada de *Novo procurado* ou rejeita ou aceita uma ocorrência. As configurações são baixadas para o Genetec Patroller™ juntamente com as listas de procurados selecionadas quando o Genetec Patroller™ se conecta ao Security Center. Essas configurações também estão disponíveis como opções de filtragem para relatórios de ocorrências no Security Desk.

- **Novos atributos de pesquisa:** Um novo procurado é um item de lista de procurados que é inserido manualmente pelo usuário do Genetec Patroller™. Os atributos do novo procurado são atributos diferentes dos padrões (número de placa, estado de emissão da placa, categoria) que um usuário do Genetec Patroller™ deve especificar ao inserir um item de novo procurado no Genetec Patroller™.

- **Novas categorias de pesquisa:** Lista de categorias que um usuário do Genetec Patroller™ pode escolher ao inserir um item de novo procurado. A categoria é o atributo que diz por que um número de placa de licença está em uma lista de procurados.
- **Motivos para rejeição de alerta:** Lista de motivos para rejeitar alertas da lista de procurados. Esses valores também ficam disponíveis como opções de filtragem de motivos de Rejeição para gerar relatórios de ocorrências no Security Desk.
- **Motivos para aceitação de alerta:** Um formulário que contém informações que os usuários do Genetec Patroller™ devem fornecer quando aceitam uma ocorrência. As informações do formulário de ocorrências podem ser consultadas no relatório de Ocorrências do Security Desk.
- **Habilitar o botão "Nenhuma infração":** Selecionar esta opção para ativar o botão *Nenhuma infração* na pesquisas de ocorrências do Genetec Patroller™. Este botão permite que o usuário do Genetec Patroller™ ignore a pesquisa de ocorrências depois de fiscalizar uma ocorrência.

Configurações gerais - Página de regra de horas extras

A página *Regra de tempo extra* permite definir os motivos de rejeição personalizados para ocorrências de tempo extra. Os valores definidos aqui são baixados para os Patrollers e ficam disponíveis como opções de filtragem para motivos de Rejeição para gerar relatórios de ocorrências no Security Desk.

Uma categoria é pré-configurada para você quando você instala o Security Center.

Configurações gerais - Página Autorização

A página *Autorização* permite que você defina os motivos de rejeição personalizados para ocorrências de autorização e selecione o tempo mínimo decorrido para violações de autorização compartilhada (Fiscalização de estacionamento na universidade e Fiscalização de estacionamento da cidade). Os valores definidos aqui são baixados para os veículos de patrulha e ficam disponíveis como opções de filtragem para motivos de Rejeição para gerar relatórios de ocorrências no Security Desk.

Uma categoria é pré-configurada para você quando você instala o Security Center.

- **Motivos para rejeição de alerta:** Lista de motivos para rejeitar alertas de autorização ou alertas de permissões compartilhadas. Esses valores também ficam disponíveis como opções de filtragem de motivos de Rejeição para gerar relatórios de ocorrências no Security Desk.
- **Máximo tempo decorrido para violação de autorização compartilhada:** Este parâmetro define o período de tempo usado por veículos de patrulha de Fiscalização de estacionamento na universidade para gerar ocorrências de autorização compartilhada. Uma ocorrência de autorização compartilhada é gerada quando dois veículos que compartilham o mesmo ID de autorização estão estacionados na mesma área de estacionamento dentro do período especificado.

  Por exemplo, digamos que você está usando os 120 minutos (duas horas) padrão, e as placas de licença ABC123 e XYZ456 estão compartilhando a mesma licença de estacionamento. Se o Genetec Patroller™ ler a placa ABC123 às 9:00 e depois ler a placa XYZ456 às 11:01, o Genetec Patroller™ **não** aciona uma ocorrência porque o tempo excede os 120 minutos.

Configurações gerais - Página campos de anotações

A página *Campos de anotação* permite definir seletores adicionais que aparecem nos relatórios *Leituras* ou *Ocorrências* do Security Desk. Para ser válido, o seletor deve se relacionar exatamente com as informações contidas na leitura ou alerta real.

Por exemplo, se você configurar *CarModel* e *CarColor* como um atributo de ocorrência Fiscalizada, o usuário do Genetec Patroller™ será solicitado a inserir o modelo e a cor do carro ao fiscalizar uma ocorrência e as informações serão armazenadas com a ocorrência. Especificar *CarColor* como um campo de *Anotação* permitirá que os valores inseridos pelo usuário sejam exibidos em um relatório *Ocorrências*. Para obter mais informações sobre o atributo de ocorrência Fiscalizada, consulte os *Guias de Implementação do AutoVu™*.

Você também pode adicionar campos personalizados do usuário aos campos de anotação para associar os metadados de um usuário a leituras e alertas individuais. Isso permite consultar e filtrar os campos personalizados do usuário nos relatórios *Leituras* e *Ocorrências* do Security Desk.

Configurações gerais - Página Atualizações

A página *Atualizações* permite atualizar veículos de patrulha e unidades Sharp com hotfixes ou novos arquivos de som para alertas de ocorrências. Você também pode atualizar serviços em unidades Sharp e atualizar firmware Sharp. Antes de poder enviar atualizações, você precisa receber as atualizações da Genetec Inc. e copiar as atualizações para a pasta *Upgrade*. Por exemplo, *C:\Genetec\AutoVu\RootFolder2\Updates\SharpOS\Upgrade*.

- **Recolher todos:** Recolhe todos os itens no campo *Entidade*.
- **Expandir todos:** Expande todos os itens no campo *Entidade*.
- **Atualizar todos:** Atualiza todas as unidades que são controladas pelo LPR Manager atualmente selecionado. Este botão atualiza apenas as unidades na aba atual. Por exemplo, se você estiver na aba *Unidades Genetec Patroller™ e Sharp*, você atualizará todos os veículos de patrulha e unidades Sharp na lista.
  - **Status:** Mostra o status da atualização. Os possíveis status:
  - **Não disponível:** O serviço de atualização não é suportado (por exemplo, Sharp versões 1.5 e 2.0 com menos de 512 MB de RAM).
  - **Qualificado:** A máquina cliente pode receber a atualização.
  - **Sincronizando:** A máquina cliente começou a sincronizar com o servidor.
  - **Sincronizado:** Todos os arquivos de atualização foram baixados com êxito para a máquina cliente. A máquina cliente está aguardando a atualização da atualização.
  - **Instalando:** A máquina cliente aceitou a atualização e começou a substituir arquivos desatualizados por novos arquivos.
  - **Instalado:** As novas atualizações foram aplicadas com sucesso na máquina cliente.
  - **Desinstalando:** A atualização está sendo removida da máquina cliente.
  - **Desinstalado:** A atualização foi removida com sucesso da máquina cliente.
  - **Erro:** Ocorreu um erro durante o processo de atualização.
- **Pasta de entrada:** Abre a pasta necessária para você copiar o arquivo de atualização. Por exemplo, clicar no ícone de pasta de destino de uma entidade Genetec Patroller™ abre *C:\Genetec\AutoVu\RootFolder\Updates\Patroller* (localização padrão).

  NOTA: Se o Config Tool não estiver sendo executado na mesma máquina que o LPR Manager, clicar na pasta de destino abre a pasta *Meus Documentos* na máquina local.
- **Instalações Genetec Patroller™ e unidades Sharp:** Exibe as instalações Genetec Patroller™ e unidades Sharp (fixas e móveis) que são elegíveis para uma atualização.
- **Atualizar os serviços:** Exibe os serviços Sharp que são elegíveis para uma atualização.
- **Atualização da versão do firmware:** Exibe as unidades Sharp que são elegíveis para uma atualização de firmware.

Tópicos relacionados

Gerar relatórios na página 53

Tarefa do sistema - Configurações gerais - Página Campos personalizados

(Visível apenas para usuários administrativos) A página *Campos personalizados* na visualização *Geral* é onde você define campos personalizados e tipos de dados personalizados para entidades do seu sistema.

Aba campos personalizados

A aba *Campos personalizados* lista todos os campos personalizados definidos no seu sistema e permite que você adicione novos.

Cada campo personalizado é caracterizado pelas seguintes propriedades:

- **Ícone da entidade/Nome do campo:** Nome do campo personalizado e o tipo de entidade que o usa.
- **Tipo de dados:** Tipo de dado do campo personalizado. Os tipos de dados padrão são:
  - **Texto:** Texto alfanumérico.
  - **Numérico:** Números inteiros no intervalo de -2147483648 a 2147483647.
  - **Decimal:** Números reais de -1E28 a 1E28.
  - **Data:** Data do calendário gregoriano.
  - **Data/Hora:** Data e hora do calendário gregoriano.
  - **Booleanos:** Dados booleanos, representados por uma caixa de seleção.
  - **Imagem:** Arquivo de imagem. Os formatos compatíveis são: bmp, jpg, gif e png.
  - **Entidade:** Entidade Security Center.
- **Valor padrão:** Valores padrão predefinidos são fornecidos para certos tipos de dados. Esta coluna exibe o valor padrão que foi selecionado ao definir o campo personalizado. O valor selecionado aparece quando o campo é exibido na entidade específica.
- **Obrigatório:** Um valor deve ser fornecido com este tipo de campo, caso contrário o sistema não aceitará suas alterações.
- **O valor deve ser único:** Indica um campo de chave. Esta opção não se aplica aos campos que utilizam tipos de dados personalizados.
- **Nome do grupo/Prioridade:** Nome sob o qual o campo personalizado é agrupado e a ordem de aparição do campo dentro do grupo. *Nenhum grupo (1)* é o valor padrão. Os campos personalizados que não pertencem a nenhum grupo aparecem primeiro na página de campo personalizado da entidade.
- **Proprietário:** Nome da função Global Cardholder Synchronizer quando o campo personalizado é parte de uma definição de *entidade global* compartilhada.

Aba tipos de dados personalizados

A aba *Tipos de dados personalizados* lista todos os tipos de dados personalizados definidos no seu sistema e permite que você adicione novos.

Cada tipo de dado personalizado é caracterizado pelas seguintes propriedades:

- **Tipo de dados:** Nome do tipo de dado personalizado.
- **Descrição:** Descrição opcional do tipo de dado.
- **Valores:** Enumeração de valores aceitáveis (sequências de texto) para este tipo de dados.
- **Proprietário:** Nome da função Global Cardholder Synchronizer quando o tipo de dado personalizado é parte de uma definição de *entidade global* compartilhada.

Tarefa do sistema - Configurações gerais - Página Eventos

(Visível apenas para usuários administrativos) A página *Eventos* permite definir eventos e cores de eventos personalizados.

Aba cores de eventos

A aba *Cores de eventos* permite atribuir cores diferentes a diferentes *eventos do sistema*.

- **Evento:** Evento ao qual atribuir uma cor.
- **Cor:** Cor atribuída para esse evento no Security Desk.

Aba eventos personalizados

A aba *Eventos personalizados* permite visualizar e adicionar eventos personalizados ao seu sistema.

- **Evento personalizado:** Nome do evento personalizado.
- **VALOR:** Número exclusivo para diferenciar o evento personalizado de outros eventos personalizados.

Tarefa do sistema - Configurações gerais - Página de ações

A página *Ações* permite criar eventos causa-efeito para o seu sistema e procurar aqueles que já foram definidos pela entidade de origem (nome e tipo), tipo de evento e tipo de ação.

- **Entidade:** Entidade de origem, ou aquela à qual o evento está anexado.
- **Evento:** Nome do evento que dispara o ação.
- **Ação:** Nome da ação disparada pelo evento.
- **Argumentos:** Informações adicionais necessárias para a ação. Por exemplo, se a ação for *Disparar alarme*, o argumento é o tipo de alarme que é acionado. Ou, se a ação for *Enviar uma mensagem*, o argumento é o destinatário de e-mail.
- **Detalhes:** Detalhes adicionais sobre a ação.
- **Cronograma:** Agenda quando este evento para ação se aplica. O evento que ocorre fora do intervalo de tempo coberto pelo agendamento não desencadeia nenhuma ação.

Tarefa do sistema - Configurações gerais - Página de ID lógico

A página *ID Lógico* permite visualizar e atribuir IDs lógicos a todas as entidades definidas no seu sistema.

- **Exibir o ID lógico para:** Diferentes grupos de tipos de entidades. IDs lógicas devem ser únicas em todas as entidades de um mesmo grupo. Os grupos são relacionados na lista suspensa.
- **Ocultar IDs lógicos não atribuídos:** Selecione esta opção para mostrar apenas entidades com uma ID lógica atribuída.
- **Nome:** Nome da entidade, tarefa pública ou estação de trabalho.
- **ID:** ID lógica atribuída à entidade, tarefa pública ou estação de trabalho.
- **Monitoramento do alarme:** Atribua um ID lógico à tarefa *Monitoramento de alarmes* no Security Desk. Isso permite que o usuário do Security Desk abra a tarefa de Monitoramento de alarmes usando um atalho de teclado.

Tarefa do sistema - Configurações gerais - Página de configurações de senha do usuário

(Visível apenas para usuários administrativos) A página *Configurações de senha de usuário* é onde você pode impor uma complexidade mínima em todas as senhas de usuário e configurar o período avançado de notificação de expiração de senha.

- **Garanta um número mínimo de:** Adiciona requisitos mínimos às senhas de usuário.
  - **Caracteres:** Número mínimo de caracteres.
  - **Letras maiúsculas:** Número mínimo de letras maiúsculas.
  - **Letras minúsculas:** Número mínimo de letras minúsculas.
  - **Caracteres numéricos:** Quantidade mínima de números.
  - **Caracteres especiais:** Número mínimo de caracteres especiais.
- **Período de notificação de expiração:** Seleciona em quantos dias antes da senha expirado o usuário será notificado (0-30 dias).

Tarefa do sistema - Configurações gerais - Página de trilhas de atividades

(Visível apenas para usuários administrativos) A página *Trilhas de atividade* permite selecionar quais tipos de atividades relacionadas ao usuário (eventos disparados por usuários) são gravados no banco de dados e estão disponíveis para relatórios na tarefa Trilhas de atividade.

Tarefa do sistema - Configurações gerais - Página de áudio

(Visível apenas para usuários administrativos) A página *Áudio* mostra todos os trechos de som (arquivos .wav) disponíveis para o seu sistema que podem alertá-lo quando você receber um novo alarme ou que pode usar com a ação *Reproduzir um som*.

- **Reproduzir:** Reproduz o trecho de som.
- **Término:** Interrompe a reprodução do trecho de som.

Tarefa do sistema - Configurações gerais - Página de níveis de ameaça

(Visível somente para usuários administrativos) A página *Níveis de ameaça* lista todos os níveis de ameaças configurados no seu sistema, permite que você adicione novos e permite modificar e excluir os existentes.

- **Nível de ameaça:** Nome do nível de ameaça.
- **Descrição:** Descrição do nível de ameaça.
- **Cor:** Cor que identificar este nível de ameaça. A cor de fundo do Security Desk muda para esta cor quando o nível de ameaça está definido no nível do sistema.
- **Ações de ativação:** Número de ações na lista de ativação do nível de ameaça. Essas ações são executadas pelo sistema quando o nível de ameaça é definido.
- **Ações de desativação:** Número de ações na lista de desativação do nível de ameaça. Essas ações são executadas pelo sistema quando o nível de ameaça é liberado.

Tarefa do sistema - Configurações gerais - Página de categorias de incidentes

(Visível apenas para usuários administrativos) A página *Categorias de incidentes* permite que você defina categorias que podem ser selecionadas ao relatar incidentes no Security Desk.

- **Adicionar categoria:** O sinal mais em verde permite digitar categorias que podem servir como um agrupamento lógico de seus incidentes, como roubo, assuntos internos, atividades suspeitas etc. Elas serão usadas no Security Desk quando o incidente for criado.
- **Remover categoria:** O X vermelho permite que você exclua a categoria selecionada.
- **Editar categoria:** O lápis permite que você modifique o nome da categoria selecionada.

Tarefa do sistema - Configurações gerais - Página Recursos

(Apenas visível para usuários administrativos) Para simplificar a interface do usuário, a página *Recursos* permite que você desligue recursos que você não está usando no seu sistema, embora eles sejam compatíveis com sua licença. Você somente pode selecionar entre recursos que sejam suportados por sua licença. Os recursos não suportados não são listados.

Tarefa de controle de acesso - Visualização de configurações gerais

Esta seção lista as configurações encontradas na visualização *Configurações gerais* da tarefa Controle de acesso.

A visualização *Controle de acesso – Configurações gerais* permite definir as configurações gerais relativas ao controle de acesso e instalar e configurar formatos de cartões personalizados.

- **Disparar evento 'Entidade está vencendo em breve':** Ative esta opção (padrão = desligado) para que o Security Center gere o evento *A entidade expirará em breve* em *n* dias antes de um titular de cartão ou uma credencial expirar, o que pode desencadear uma ação para avisar alguém sobre a expiração próxima.
- **Criar incidente antes de sobreposição de estado da porta:** Ativar esta opção (padrão = desligado) para solicitar ao usuário do Security Desk que informe um incidente toda vez que ele bloquear ou desbloquear uma porta manualmente ou substituir o cronograma de desbloqueio atribuído à porta.
- **Motivos de solicitação de cartão:** Adicione motivos que usuários podem escolher para explicar porque estão solicitando um cartão de credencial para ser impresso (por exemplo, não há impressora no local).
- **Tamanho máximo do arquivo da imagem:** Defina o tamanho máximo de arquivo (padrão=20KB) para imagens (como imagem de titular d cartão) armazenado na base de dados do Directory para salvar espaço em disco.
- **Formatos de cartão personalizados:** Lista os formatos de cartão personalizados definidos no seu sistema e permite que os adicione, exclua ou modifique.
- **Provedores de credenciais móveis:** Lista os provedores de credenciais móveis e perfis no seu sistema e permite que os adicione, exclua ou modifique.

Tópicos relacionados

Receber notificações quando os portadores de cartão estiverem para expirar na página 671
Adicionar motivos para solicitações de cartão de credencial na página 686
Definir o tamanho máximo de arquivos de imagem na página 656
Criar formatos de cartão personalizados na página 691
Configurar perfis de credencial móvel na página 665

54

Eventos e ações

Esta seção inclui os seguintes tópicos:

- "Tipos de evento" na página 1101
- "Tipos de ação" na página 1120

Tipos de evento

Todos os eventos no Security Center estão associados a uma *entidade de origem*, que é o foco principal do evento.

O Security Center suporta os seguintes tipos de evento:

Evento	Entidade de origem	Descrição
A capacidade de gravar em um disco foi restaurada	Função Archiver ou Archiver auxiliar	A capacidade de gravar em um disco foi restaurada.
Acesso negado: Violação antirretorno	porta	Um titular de cartão solicitou o acesso a uma área em que já entrou, ou solicitou acesso para deixar uma área na qual nunca esteve.
Acesso negado: É preciso um segundo titular de cartão	porta	Dois titulares de cartão devem apresentar suas credenciais com um certo intervalo entre si e o intervalo expirou. Este evento se aplica somente a portas controladas por unidades Synergis™.
Acesso negado: Negado por regra de acesso	porta ou elevador	O acesso do titular de cartão é negado de acordo com a regra de acesso.
Acesso negado: Capacidade máxima	porta	O acesso do titular de cartão é negado porque a área atingiu o limite de ocupação.
Acesso negado: Este modelo de unidade não oferece suporte a acompanhante	porta	A regra de acompanhamento de visitante é aplicada em uma área, mas a unidade que controla suas portas não suporta este recurso.
Acesso negado: Credencial expirada	titular de cartão, credencial, porta ou elevador	Uma credencial expirada foi usada.
Acesso negado: Supervisor de regra de primeira pessoa a entrar ausente	porta	A regra de primeira pessoa a entrar foi aplicada na área, e nenhum supervisor ainda chegou.
Acesso negado: Titular de cartão inativo	titular de cartão, porta ou elevador	Um titular de cartão com um perfil inativo tentou acessar uma porta ou elevador.
Acesso negado: Credencial inativa	titular de cartão, credencial, porta ou elevador	Uma credencial com um perfil inativo foi usada.
Acesso negado: Permissão insuficiente	porta ou elevador	O acesso do titular de cartão é negado porque não possui a autorização de segurança necessária. Este evento se aplica somente a portas controladas por unidades Synergis™.
Acesso negado: Intertravamento	porta	O acesso é negado devido a uma restrição de intertravamento.

Evento	Entidade de origem	Descrição
Acesso negado: PIN inválido	porta ou elevador	O titular de cartão inseriu um PIN inválido.
Acesso negado: Credencial perdida	titular de cartão, credencial, porta ou elevador	Uma credencial que foi declarada como perdida foi usada.
Acesso negado: Nenhuma regra de acesso atribuída	porta ou elevador	O acesso do titular de cartão é negado porque não tem regras de acesso atribuídas.
Acesso negado: Fora de agendamento	porta ou elevador	A regra de acesso associada a este titular de cartão não se aplica durante a data ou hora especificada na agenda.
Acesso negado: Credencial furtada	titular de cartão, credencial, porta ou elevador	Uma credencial que foi declarada como furtada foi usada.
Acesso negado: Credencial não atribuída	credencial, porta ou elevador	Uma credencial que não foi atribuída a um titular de cartão foi usada.
Acesso negado: Credencial desconhecida	porta ou elevador	Uma credencial desconhecida no sistema do Security Center foi usada.
Acesso negado: Cartão válido, PIN inválido	porta ou elevador	É necessário um cartão e um PIN para entrar em uma área e o titular de cartão introduziu um PIN inválido.
Acesso negado: Negado ao acompanhante do visitante	porta	Em um cenário de acompanhamento de visitante, o acesso de um dos visitantes ou seu acompanhante foi negado.
Acesso concedido	titular de cartão, porta ou elevador	Foi concedido acesso através de uma porta a um titular de cartão de acordo com as regras de acesso que regem a porta, elevador ou área. Para uma porta perimetral de um intertravamento: quando um titular de cartão autorizado acessa uma porta de um intertravamento, o Security Center pode gerar um evento *Acesso concedido* para a porta mesmo que a porta não desbloqueie (devido a outra porta perimetral já estar aberta).
Falha de CA	unidade de controle de acesso ou unidade de detecção de intrusão	CA (corrente alternada) falhou.
Uma porta de um intertravamento tem um agendamento de destravamento configurado	área	Uma porta que é parte de uma configuração de intertravamento tem uma agenda de desbloqueio configurada. Isso invalida o intertravamento.
Uma porta de um intertravamento está em modo de manutenção	área	Uma porta que é parte de uma configuração de intertravamento está em modo de manutenção. Isso desativa o intertravamento.

Evento	Entidade de origem	Descrição
Movimento adaptativo disparado	câmera (análise de vídeo)	Foi detectado movimento em uma câmera equipada com recursos de análise de vídeo.
Alarme confirmado	alarme	Um alarme foi confirmado por um usuário ou confirmado automaticamente pelo sistema.
Alarme confirmado (Alternativo)	alarme	Um alarme foi confirmado por um usuário usando o modo alternativo.
Alarme sob investigação	alarme	Um alarme com uma condição de confirmação ainda ativa entrou no estado *sob investigação*.
Condição de alarme apagada	alarme	A condição de confirmação de um alarme foi liberada.
Alarme confirmado forçadamente	alarme	A confirmação de um alarme foi forçada por um usuário com privilégios especiais.
Alarme disparado	alarme	Um alarme foi acionado.
Um intertravamento não pode estar em modo de antirretorno por hardware	área	Um intertravamento não pode estar em modo de anti-passback forçado. Esta é uma configuração ilegal.
Um intertravamento não pode ter uma porta de perímetro sem nenhum sensor de porta configurado	área	O intertravamento não pode ser imposto se o sistema não puder determinar se uma porta está aberta ou não.
Um intertravamento não pode ter apenas uma porta de perímetro	área	Você precisa de pelo menos duas portas perimétricas para o intertravamento ser aplicado.
Antirretorno desabilitado: Definições inválidas	área	Anti-passback desabilitado: definições inválidas.
Antirretorno desabilitado: Não suportado quando a unidade está em modo servidor.	área	As unidades não foram configuradas no modo de servidor. O anti-passback está disponível de acordo com o modo operacional da unidade. Para obter mais informações sobre limitações de unidades, consulte as *Notas de Versão do Security Center.*
Antirretorno desabilitado: A unidade está off-line	área	Pelo menos uma unidade está no modo offline, impedindo o anti-passback. O anti-passback está disponível de acordo com o modo operacional da unidade. Consulte as *Notas de Versão do Security Center* para obter mais informações sobre limitações das unidades.

Evento	Entidade de origem	Descrição
Violação antirretorno	área ou titular de cartão	Uma solicitação de acesso foi feita para entrar em uma área com uma credencial que já está dentro da área, ou para sair de uma área com uma credencial que nunca esteve na área.
Violação de antirretorno perdoada	titular de cartão	Um operador de segurança concedeu acesso a um titular de cartão responsável por uma violação de passback.
Aplicativo conectado	aplicativo ou função	Um aplicativo ou uma função se conectou ao Directory.
Aplicativo perdido	aplicativo ou função	Um aplicativo ou uma função perdeu sua conexão ao Directory.
O caminho da pasta de repositório é longo demais	Função Archiver ou Archiver auxiliar	O caminho básico no disco para arquivos de vídeos excedeu o comprimento máximo permitido pelo sistema operacional.
Substituído o disco do repositório	Função Archiver ou Archiver auxiliar	O **Espaço alocado** em um dos discos atribuído para armazenamento de arquivos para este Archiver foi esgotado, e o Archiver mudou para o disco seguinte na linha. Os nomes do disco anterior e do disco atual são indicados no campo **Descrição**.
Fila de arquivamento cheia	câmera	Uma câmera (codificador de vídeo) transmite vídeos mais rapidamente do que o Archiver pode gravar os pacotes de vídeo no disco. Um problema com o banco de dados do Archiver também desencadeia esse evento. O nome da câmera cujos pacotes são perdidos é indicado no campo **Descrição**.
Arquivamento interrompido	Função Archiver ou Archiver auxiliar	O arquivamento parou porque os discos atribuídos para arquivamento estão cheios. Este evento sempre acompanha um evento *Disco cheio*.
O ativo foi movido	ativo	Um ativo foi movido.
O ativo está off-line	ativo	A etiqueta RFID de um ativo ficou offline.
O ativo está on-line	ativo	A etiqueta RFID de um ativo ficou online.
Alarme de áudio	câmera	Um som foi captado por um microfone associado a uma câmera.
Evento de análise de áudio	câmera (análise de vídeo)	Foi detectado um evento de análise de áudio em uma câmera equipada com recursos de análise de áudio.
Tarefa de impressão de crachás cancelada	usuário	Um usuário cancelou uma tarefa de impressão de crachás.

Evento	Entidade de origem	Descrição
Tarefa de impressão de crachás concluída	usuário	Um usuário concluiu uma tarefa de impressão de crachás.
Tarefa de impressão de crachás colocada em fila	usuário	Um usuário colocou na fila uma tarefa de impressão de crachás.
Falha de bateria	unidade de controle de acesso ou unidade de detecção de intrusão	A bateria da unidade falhou.
Bloquear câmera iniciado	câmera	Um usuário bloqueou uma transmissão de vídeo de outros usuários no sistema.
Bloquear câmera interrompido	câmera	Um usuário desbloqueou uma transmissão de vídeo de outros usuários no sistema.
Câmera sem arquivamento	câmera	A câmera está sob uma agenda de arquivamento ativa, mas o Archiver não está recebendo a transmissão de vídeo.
Adulteração de câmera	câmera (análise de vídeo)	Ocorreu uma disfunção, potencialmente devido à adulteração da câmera, resultando em obstrução parcial ou total da visão da câmera, uma alteração repentina do campo de visão ou uma perda de foco.
Não foi possível gravar no local especificado	Função Archiver ou Archiver auxiliar	O Archiver não pode gravar em uma unidade específica. O caminho para a unidade é indicado no campo **Descrição**.
Não é possível gravar em nenhum disco	Função Archiver ou Archiver auxiliar	O Archiver não consegue gravar em nenhuma das unidades de disco. A situação pode surgir pelos seguintes motivos: Quando acessos de escrita a unidades compartilhadas são revogados. Quando as unidades compartilhadas estão inacessíveis. Quando unidades compartilhadas não existem mais. Quando isso acontece, o arquivamento é interrompido. O Archiver reavalia o estado do disco a cada 30 segundos.
Limite de capacidade alcançado	zona de estacionamento	A capacidade da zona de estacionamento alcançou o limiar de capacidade definido no LPR Manager.
Tempo de gratuidade iniciado	regra de estacionamento	A porção de tempo de conveniência da sessão de estacionamento começou.
A credencial expirou	credencial	Uma credencial expirou
Detecção de multidão	câmera (análise de vídeo)	Uma multidão ou fila foi detectada em uma câmera equipada com recursos de análise de vídeo.

Evento	Entidade de origem	Descrição
Evento personalizado	em todo o sistema	É um evento adicionado depois da instalação do sistema inicial. Os eventos definidos na instalação do sistema são chamados de eventos do sistema. Os eventos personalizados podem ser definidos pelo usuário ou adicionados automaticamente pelas instalações do plugin. Diferente dos eventos do sistema, os eventos personalizados podem ser renomeados e excluídos.
Perda do banco de dados	Função Archiver ou Archiver auxiliar	A conexão com o banco de dados de funções foi perdida. Se este evento estiver relacionado a um banco de dados de funções, pode ser porque o servidor de dados está desativado ou não pode ser alcançado pelo servidor de funções. Se o evento estiver relacionado ao banco de dados do Directory, a única ação que você pode usar é *Enviar um e-mail* porque todas as outras ações exigem uma conexão ativa com o banco de dados do Directory.
Banco de dados recuperado	Função Archiver ou Archiver auxiliar	A conexão com o banco de dados de funções foi recuperada.
Fechadura trancada	zona	O ferrolho de uma porta foi bloqueado.
Fechadura destrancada	zona	O ferrolho de uma porta foi desbloqueado.
Alarme de direção	câmera (análise de vídeo)	Um alarme de direção foi acionado em uma câmera equipada com recursos de análise de vídeo.
Limiar de carga de disco excedido	Função Archiver ou Archiver auxiliar	O espaço em disco alocado para arquivamento excedeu seu limiar de carga (padrão = 80%). Isso é causado por uma avaliação subestimada do espaço em disco requerido, ou por outro aplicativo que está ocupando mais espaço em disco do que deveria. Se 100% do espaço em disco atribuído é usado, o Archiver começa a excluir arquivos antigos prematuramente para liberar espaço em disco para novos arquivos, começando com os arquivos mais antigos.
Discos cheios	Função Archiver ou Archiver auxiliar	Todos os discos atribuídos para arquivamento estão cheios e o Archiver não consegue liberar espaço em disco excluindo arquivos de vídeos existentes. Esse evento pode ocorrer quando outro aplicativo usou todo o espaço em disco reservado para o Security Center, ou quando a opção **Excluir arquivos mais antigos quando os discos estiverem cheios** não estiver selecionada no Server Admin. Quando isso acontece, o arquivamento é interrompido. O Archiver reavalia o espaço em disco a cada 30 segundos.

Evento	Entidade de origem	Descrição
Porta fechada	porta	A porta fechou. Para que este evento seja gerado, a porta deve estar equipada com um sensor de porta.
A porta forçada para abrir	porta	A porta está bloqueada, mas o sensor da porta indica que a porta está aberta.
Maçaneta em posição	zona	A maçaneta está posicionada e a porta está fechada.
Maçaneta girada	zona	A maçaneta foi girada.
Porta trancada	porta	A porta foi bloqueada.
Manutenção da porta concluída	porta	A porta foi tirada do modo de manutenção.
Manutenção da porta iniciada	porta	A porta foi colocada no modo de manutenção.
Porta destrancada manualmente	porta	No Security Desk, um usuário desbloqueou manualmente uma porta.
Porta off-line O dispositivo está off-line	porta	Um ou mais dispositivos associados a esta porta ficaram offline.
Porta aberta	porta	A porta foi aberta. Para que este evento seja gerado, a porta deve estar equipada com um sensor de porta.
Porta aberta por muito tempo	porta	A porta foi mantida aberta por muito tempo. Para ativar este evento, você deve definir a propriedade "Disparar um evento 'porta aberta por muito tempo'" na aba *Propriedades* de uma entidade de Porta no Config Tool.
Porta destrancada	porta	A porta foi desbloqueada.
Falha na mídia de armazenamento edge	câmera	Após uma unidade ter sido reiniciada, o vídeo que foi gravado na unidade não pôde ser acessado.
Elevador offline: O dispositivo está off-line	elevador	Um ou mais dispositivos associados a este elevador ficaram offline.
Fim da adulteração de câmera	câmera (análise de vídeo)	Um mau funcionamento causado pela adulteração da câmera foi resolvido.
A entidade expirou	credencial	Uma credencial ou o titular de cartão associado expirou (seu status agora é *Expirado*).
A entidade expirará em breve	titular de cartão ou credencial	O Security Center gera esse evento para avisar que a data de expiração de uma entidade está se aproximando. O número de dias de aviso prévio permitido por este evento deve ser definido.

Evento	Entidade de origem	Descrição
Alerta de entidade	qualquer entidade	Um aviso de saúde do sistema foi emitido para esta entidade.
Entrada assumida	titular de cartão ou porta	Um titular de cartão recebeu acesso a uma porta ou área, e supõe-se que ele entrou, porque nenhum sensor de porta está configurado.
Entrada detectada	titular de cartão ou porta	Um titular de cartão recebeu acesso a uma porta ou área e sua entrada foi detectada. Para que esse evento seja gerado, você deve configurar um sensor de entrada no lado da porta onde você deseja que a entrada seja detectada. Se não houver sensores de entrada configurados na porta, o evento será gerado com base na entrada dada pelo sensor de porta.
Face detectada	câmera (análise de vídeo)	Um rosto foi detectado em uma câmera equipada com recursos de análise de vídeo.
Face reconhecida	câmera (análise de vídeo)	Um rosto em uma *lista de procurados* foi reconhecido em uma câmera equipada com recursos de análise de vídeo.
Arquivo excluído	câmera	Um arquivo de vídeo associado a uma câmera foi excluído porque o período de retenção terminou ou o disco de armazenamento de arquivos estava cheio.
Falha na atualização de firmware	unidade de controle de acesso	Uma atualização de firmware em uma unidade de controle de acesso falhou.
Atualização de firmware iniciada	unidade de controle de acesso	Uma atualização de firmware em uma unidade de controle de acesso foi iniciada.
Atualização de firmware bem sucedida	unidade de controle de acesso	Uma atualização de firmware em uma unidade de controle de acesso foi concluída com sucesso.
Primeira pessoa a entrar	área	Um titular de cartão entrou em uma área vazia.
Andar acessado	elevador	Um botão de andar do elevador foi pressionado.
Quebra de vidro	zona	O vidro se quebrou.
Violação de hardware	unidade de controle de acesso, porta, elevador ou zona	A entrada de adulteração em uma unidade foi acionada.
Evento de saúde	Função Health Monitor	Um evento de saúde do sistema ocorreu.
Mapa de calor alterado	câmera (análise de vídeo)	Uma alteração foi detectada em uma área de mapa térmico em uma câmera equipada com recursos de análise de vídeo.

Evento	Entidade de origem	Descrição
Entrada de alarme ativada	entrada em unidade de detecção de intrusão	A entrada entrou em um estado de *alarme*.
Entrada de alarme restaurada	entrada em unidade de detecção de intrusão	A entrada saiu de um estado de *alarme*.
Derivação de entrada	entrada em unidade de detecção de intrusão	A entrada entrou em um estado *derivado*.
Derivação de entrada restaurada	entrada em unidade de detecção de intrusão	A entrada saiu de um estado *derivado*.
Estado de entrada alterado: Entrada ativa	entrada em câmera, unidade de controle de acesso ou unidade de detecção de intrusão	A entrada entrou em um estado *ativo*.
Estado de entrada alterado: Entrada normal	entrada em câmera, unidade de controle de acesso ou unidade de detecção de intrusão	A entrada entrou em um estado *normal*.
Estado de entrada alterado: Problema na entrada	entrada em unidade de controle de acesso ou unidade de detecção de intrusão	A entrada entrou em um estado de *problema*.
O intertravamento não é suportado pela unidade	área	O intertravamento está ativado em uma área, mas a unidade de controle de acesso que controla as portas não suporta este recurso.
Entrada ativa de trancamento de intertravamento	área	O trancamento de intertravamento foi ativado.
Entrada normal de trancamento de intertravamento	área	O trancamento de intertravamento foi desativado.
Entrada ativa de cancelamento de intertravamento	área	O cancelamento de intertravamento está ativo.
Entrada normal de cancelamento de intertravamento	área	O cancelamento de intertravamento está inativo.
Alarme da área de detecção de intrusão ativado	área de detecção de intrusão	Alarme de área de detecção de intrusão ativado.
Colocação da área de detecção de intrusão em atenção	área de detecção de intrusão	A área de detecção de intrusão está sendo armada.

Evento	Entidade de origem	Descrição
Colocação da área de detecção de intrusão em atenção postergada	área de detecção de intrusão	O armamento da área de detecção de intrusão foi postergado.
Alarme cancelado da área de detecção de intrusão	área de detecção de intrusão	O alarme da área de detecção de intrusão foi cancelado.
Solicitação postergada cancelada da área de detecção de intrusão	área de detecção de intrusão	A solicitação de postergação da área de detecção de intrusão foi cancelada.
Área de detecção de intrusão colocada fora de atenção	área de detecção de intrusão	A área de detecção de intrusão foi desarmada.
Solicitação de colocação da área de detecção de intrusão fora de atenção	área de detecção de intrusão	A solicitação de postergação da área de detecção de intrusão foi cancelada.
Alarme de coação da área de detecção de intrusão	área de detecção de intrusão	A área de detecção de intrusão foi desarmada com coação.
Atraso de entrada na área de detecção de intrusão ativado	área de detecção de intrusão	Atraso de entrada na área de detecção de intrusão ativado.
Colocação forçada da área de detecção de intrusão em atenção	área de detecção de intrusão	A área de detecção de intrusão foi armada à força.
Desvio de entrada da área de detecção de intrusão ativado	área de detecção de intrusão	A desconsideração da entrada de área de detecção de intrusão foi ativada.
Desvio de entrada da área de detecção de intrusão desativado	área de detecção de intrusão	A desconsideração da entrada de área de detecção de intrusão foi desativada.
Problema de entrada da área de detecção de intrusão	área de detecção de intrusão	Problema com a entrada da área de detecção de intrusão.
Master da área de detecção de intrusão colocado em atenção	área de detecção de intrusão	A área de detecção de intrusão foi armada pelo mestre.
Solicitação de colocação do master da área de detecção de intrusão em atenção	área de detecção de intrusão	A solicitação de armamento do mestre da área de detecção de intrusão foi emitida.
Perímetro da área de detecção de intrusão colocado em atenção	área de detecção de intrusão	A área de detecção de intrusão está com o perímetro armado.

Evento	Entidade de origem	Descrição
Solicitação de colocação do perímetro da área de detecção de intrusão em atenção	área de detecção de intrusão	A solicitação de armamento do perímetro de detecção de intrusão foi emitida.
Solicitação postergada de armamento da área de detecção de intrusão	área de detecção de intrusão	A solicitação de armamento da área de detecção de intrusão foi postergado.
Desvio de entrada da unidade de detecção de intrusão ativado	unidade de detecção de intrusão	A desconsideração da entrada de unidade de detecção de intrusão foi ativada.
Desvio de entrada da unidade de detecção de intrusão desativado	unidade de detecção de intrusão	A desconsideração da entrada de unidade de detecção de intrusão foi desativada.
Problema de entrada da unidade de detecção de intrusão	unidade de detecção de intrusão	Problema com a entrada da unidade de detecção de intrusão.
Violação de unidade de detecção de intrusão	unidade de detecção de intrusão	A unidade de detecção de intrusão foi adulterada.
Configuração inválida na unidade	unidade de vídeo	A configuração da unidade é inválida.
Valores personalizados de criptografia inválidos	Função Archiver ou Archiver auxiliar	Este aviso é emitido pelo Archiver na inicialização e a cada 5 minutos se um dos valores de criptografia personalizados (impressão digital inicial ou chave de criptografia) especificado no Server Admin for inválido.
Redefinição de inventário	zona de estacionamento	O inventário da zona de estacionamento foi zerado para que a ocupação da zona de estacionamento relatada possa ser reinicializada.
Última pessoa a sair	área	O último titular de cartão saiu de uma área.
Alerta de placa de licença	Qualquer regra de ocorrências	Uma leitura de placa de licença de veículo foi correspondida com uma lista de procurados, uma regra de tempo extra ou uma restrição de autorização.
Leitura da placa de licença	Unidade de LPR ou Genetec Patroller™	Uma placa de licença de veículo foi lida.
Marcador de vídeo ao vivo acrescentado	câmera	Um usuário adicionou um marcador a um vídeo ao vivo.
Fechadura destrancada	zona	Evento relacionado a uma entidade de zona.
Fechadura trancada	zona	Evento relacionado a uma entidade de zona.

Evento	Entidade de origem	Descrição
Vagando	câmera (análise de vídeo)	Foi detectada atividade demorada na filmagem da câmera.
Bateria fraca	ativo	A bateria na etiqueta RFID de um recurso está prestes a esgotar.
Macro abortada	macro	A execução de uma macro falhou.
Macro iniciada	macro	A execução de uma macro foi iniciada.
Estação manual ativada	porta	Alguém puxou a liberação de emergência da porta (estação de alavanca manual).
Estação manual revertida para o estado normal	porta	A liberação de emergência da porta (estação de alavanca manual) foi restaurada para a posição de operação normal.
Macro completado	macro	A execução de uma macro foi concluída normalmente.
Anfitrião de acompanhamento perdido	porta	O host final de uma delegação com dois hosts não passou o crachá.
Movimento	câmera	Há movimento detectado.
Movimento inativo	câmera	Este evento é emitido após um evento de *Movimento ativo* quando o movimento (medido em termos de número de blocos de movimento) fica abaixo do "limiar de movimento inativo" por pelo menos 5 segundos.
Movimento ativo	câmera	Este evento é emitido quando ocorre detecção de movimento positiva.
Múltiplas unidades estão configuradas para o intertravamento	área	Todas as portas que fazem parte de uma configuração de intertravamento devem ser controladas pela mesma unidade.
Nenhuma entrada detectada	titular de cartão ou porta	Um titular de cartão recebeu acesso a uma porta ou área, mas nenhuma entrada foi detectada. Para que esse evento seja gerado, você deve configurar um sensor de porta no lado da porta onde você deseja que a entrada seja detectada.
Não combina	lista de procurados	Um veículo não foi correspondido à lista de procurados associada à unidade Sharp.
Nenhum pacote RTP perdido no último minuto	câmera	O Archiver recebeu todos os pacotes RTP no último minuto.
Condição do objeto alterada	câmera (análise de vídeo)	Um objeto subitamente mudou de direção ou velocidade, como quando uma pessoa começa a correr ou escorrega.

Evento	Entidade de origem	Descrição
Contagem de objeto alterada	câmera (análise de vídeo)	Uma alteração foi detectada na contagem de objetos em uma câmera equipada com recursos de análise de vídeo.
Contagem de objeto alcançada	câmera (análise de vídeo)	Um limite de contagem de objetos foi atingido para a contagem de objetos em uma câmera equipada com recursos de análise de vídeo.
Objeto cruzou a linha	câmera (análise de vídeo)	Um objeto atravessou um fio de tropeço predefinido.
Objeto detectado	câmera (análise de vídeo)	Um objeto está no campo de visão da câmera.
Objeto detectado no campo	câmera (análise de vídeo)	Uma objeto foi detectado em uma zona que está sendo monitorada contra intrusão em uma câmera equipada com recursos de análise de vídeo.
Direção do objeto alterada	câmera (análise de vídeo)	Um objeto foi detectado mudando de direção em uma câmera equipada com recursos de análise de vídeo.
Objeto entrou	câmera (análise de vídeo)	Um objeto entrou no campo de visão da câmera.
Objeto saiu	câmera (análise de vídeo)	Um objeto saiu do campo de visão da câmera.
Objeto seguindo a rota	câmera (análise de vídeo)	Um objeto segue uma rota predeterminada, em uma direção específica.
Objeto abandonado	câmera (análise de vídeo)	Um objeto entrou e saiu do campo de visão da câmera.
Objeto juntou-se	câmera (análise de vídeo)	Dois objetos distintos no campo de visão da câmera foram mesclados.
Objeto removido	câmera (análise de vídeo)	Um objeto foi removido do campo de visão da câmera.
Objeto separado	câmera (análise de vídeo)	Um objeto no campo de visão da câmera se separou em dois objetos.
Objeto parado	câmera (análise de vídeo)	Um objeto em movimento parou.
Velocidade do objeto alterada	câmera (análise de vídeo)	Um objeto foi detectado mudando de velocidade em uma câmera equipada com recursos de análise de vídeo.
A descarga falhou	Genetec Patroller™	Um descarregamento de Genetec Patroller™ para Security Center falhou.

Evento	Entidade de origem	Descrição
Descarga bem sucedida	Genetec Patroller™	Um descarregamento de Genetec Patroller™ para Security Center foi bem-sucedido.
Tempo pago iniciado	regra de estacionamento	Foi comprado tempo de estacionamento através de estações de pagamento conectadas ou aplicativos móveis.
Contagem de pessoas desabilitada: A unidade está off-line	área	Uma unidade ficou offline, impossibilitando assim a contagem de pessoas.
Contagem de pessoas reiniciada	área	O número de pessoas contadas em uma área foi redefinido para *0*.
Pessoa caindo	câmera (análise de vídeo)	Uma pessoa caindo foi detectada na câmera.
Pessoa correndo	câmera (análise de vídeo)	Uma pessoa correndo foi detectada na câmera.
Pessoa escorregando	câmera (análise de vídeo)	Uma pessoa escorregando foi detectada na câmera.
Marcador de reprodução acrescentado	câmera	Um usuário adicionou um marcador a um vídeo gravado.
O limiar de proteção foi excedido	Função Archiver ou Archiver auxiliar	O *Limiar de vídeos protegidos* configurado do Archiver foi excedido. Você pode monitorar a porcentagem de espaço em disco ocupada por arquivos de vídeo protegidos na página Estatísticas, na aba Recursos do Archiver no Config Tool.
PTZ ativado	câmera (PTZ)	Um usuário começou a usar o PTZ depois dele ter estado inativo. O campo *Descrição* indica o usuário que ativou o PTZ. Este evento é regenerado sempre que um usuário diferente assume o controlo do PTZ, mesmo quando o PTZ ainda está ativo.
PTZ bloqueado	câmera (PTZ)	Um usuário tentou mover o PTZ enquanto ele está sendo bloqueado por outro usuário com maior prioridade de PTZ. O campo *Descrição* indica a máquina, o tipo do aplicativo e o usuário que atualmente mantém o bloqueio.
PTZ parado	câmera (PTZ)	O PTZ não foi manipulado por nenhum usuário após um período de tempo predeterminado. O campo *Descrição* indica o usuário que usou o PTZ por último.

Evento	Entidade de origem	Descrição
Zoom de PTZ pelo usuário	câmera (PTZ)	Um usuário iniciou o zoom do PTZ. O campo Descrição indica o usuário que realizou o zoom. Eventos de *Zoom de PTZ pelo usuário* posteriores são gerados se outro usuário acionar o zoom do PTZ, ou se o usuário original acionar o zoom após o *Intervalo de inatividade* ter expirado.
Zoom de PTZ pelo usuário interrompido	câmera (PTZ)	O zoom do PTZ não foi acionado por nenhum usuário após um período de tempo predeterminado. O campo *Descrição* indica o usuário que acionou o zoom do PTZ por último.
Recebendo pacotes de RTP de múltiplas origens	câmera	O Archiver está recebendo mais de uma transmissão de vídeo da mesma câmera. **IMPORTANTE:** Quando esta situação rara ocorre, o Archiver não consegue identificar qual transmissão é a correta simplesmente pelo endereço IP da origem devido a NAT (Network Address Translation), então uma escolha arbitrária é feita. Isso pode resultar no arquivamento da transmissão de vídeo incorreta. No entanto, o endereço IP da origem e o número da porta de ambas as transmissões são indicados no campo *Descrição* e as duas origens são identificadas como *Arquivada* e *Rejeitada*. Você pode identificar a unidade defeituosa que está causando esse conflito.
Problema de gravação	câmera	Existe um problema ao gravar a câmera. O problema pode ser devido a um erro ao salvar no disco, um erro ao salvar no banco de dados do Archiver ou o fato de que a câmera não está transmitindo o vídeo quando deveria.
Gravação iniciada (alarme)	câmera	A gravação em uma câmera foi iniciada como resultado do acionamento de um alarme.
Gravação iniciada (contínua)	câmera	A gravação em uma câmera foi iniciada por uma agenda de arquivamento contínua.
Gravação iniciada (externa)	câmera	A gravação em uma câmera foi iniciada pela ação *Iniciar gravação*. Esta ação pode ter sido desencadeada por outro evento ou executada a partir de uma macro.
Gravação iniciada (movimento)	câmera	A gravação em uma câmera foi iniciada por detecção de movimento.
Gravação iniciada (usuário)	câmera	A gravação em uma câmera foi iniciada manualmente por um usuário.
Gravação interrompida (alarme)	câmera	A gravação em uma câmera parou porque o tempo de gravação do alarme se esgotou.

Evento	Entidade de origem	Descrição
Gravação interrompida (contínua)	câmera	A gravação em uma câmera parou porque ela não é mais coberta por uma agenda de arquivamento contínua.
Gravação interrompida (externa)	câmera	A gravação em uma câmera foi interrompida pela ação Interromper gravação. Esta ação pode ter sido desencadeada por outro evento ou executada a partir de uma macro.
Gravação interrompida (movimento)	câmera	A gravação em uma câmera parou porque o movimento cessou.
Gravação interrompida (usuário)	câmera	A gravação em uma câmera foi interrompida manualmente por um usuário.
Solicitação de saída	porta	Alguém apertou o botão de liberação da porta ou acionou um detector de movimento de solicitação de saída. O evento *Solicitação de saída* tem filtragem especial para tornar este recurso compatível com hardware de detecção de movimento de solicitação de saída. Defina essas propriedades na aba **Porta** > **Propriedades** > **Config Tool**.
Requisição normal de saída	porta	Nenhuma solicitação de saída está sendo feita.
Perda de pacotes RTP	câmera	Existem pacotes RTP que o Archiver nunca recebeu. Isso pode acontecer se os pacotes forem perdidos na rede ou se o Archiver não tiver CPU suficiente para processar todos os pacotes recebidos na placa de rede. O campo *Descrição* indica o número de pacotes perdidos desde a última vez que esse evento foi emitido (não mais de uma vez a cada minuto).
Acesso controlado agendado	elevador	Atualmente, o cronograma de acesso controlado ao andares do elevador é válido.
Acesso livre agendado	elevador	A agenda de acesso livre a andares de elevador é agora aplicada.
Trancamento agendado	porta	A agenda de desbloqueio de portas expirou, a trava está agora redefinida (a porta está trancada).
Abertura agendada	porta	A tranca da porta está destrancada devido a uma agenda de desbloqueio programado.
Agendamento de destravamento ignorado: supervisor de regra de primeira pessoa a entrar ausente	porta	A agenda de desbloqueio de portas é ignorado porque a restrição imposta pela regra de primeira pessoa a entrar ainda não foi satisfeita.

Evento	Entidade de origem	Descrição
Sessão concluída	regra de estacionamento	O veículo saiu da zona de estacionamento.
Sessão iniciada	regra de estacionamento	O veículo entrou na zona de estacionamento.
Perda de Sinal	câmera	O sinal da câmera foi perdido.
Sinal recuperado	câmera	O sinal da câmera foi recuperado.
A sincronização foi concluída: Sistema externo	Função do Active Directory	A sincronização de um sistema externo foi concluída.
Erro de sincronização: Sistema externo	Função do Active Directory	A sincronização de um sistema externo resultou em erro.
A sincronização foi iniciada: Sistema externo	Função do Active Directory	A sincronização de um sistema externo foi iniciada.
Carona	câmera (análise de vídeo)	Duas pessoas entraram em uma área protegida se seguindo muito de perto.
Alarme de temperatura	unidade de vídeo	A temperatura da unidade de vídeo aumentou acima do nível de segurança.
Nível de ameaça apagado	nível da ameaça	Um nível de ameaça foi apagado.
Nível da ameaça definido	nível da ameaça	Um nível de ameaça foi definido.
Transmissão interrompida	câmera	O Archiver ainda está conectado à câmera, mas não recebeu nenhum pacote de vídeo por mais de 5 segundos.
Transmissão recuperada	câmera	O Archiver começou a receber pacotes de vídeo da câmera de novo.
Evento de análise de vídeo indefinido	câmera (análise de vídeo)	Um evento genérico de análise de vídeo foi emitido, mas ainda não foi mapeado para um evento do Security Center. **DICA:** Você pode procurar informações de subtipo adicionais nos metadados de análise.
Unidade conectada	unidade	A conexão a uma unidade foi estabelecida ou restaurada.
A unidade deixou de responder à solicitação de vídeo de unidade	câmera	Evento relacionado a uma câmera que está gravando diretamente na unidade.
Perda de unidade	unidade	A conexão a uma unidade foi perdida.
A sincronização da unidade falhou	unidade de controle de acesso	A sincronização da unidade com o Access Manager falhou.

Evento	Entidade de origem	Descrição
Iniciada sincronização da unidade	unidade de controle de acesso	A sincronização da unidade com o Access Manager iniciou.
Sincronização da unidade bem sucedida	unidade de controle de acesso	A sincronização da unidade com o Access Manager foi concluída com sucesso.
Atualização publicada	Genetec Patroller™, Mobile Sharp	Uma atualização foi processada e está pronta para ser implantada no Genetec Patroller™.
A atualização falhou	Genetec Patroller™, Mobile Sharp	Uma atualização no Genetec Patroller™ ou em uma unidade Mobile Sharp falhou, ou um arquivo não pôde ser sincronizado em um computador Genetec Patroller™.
Concluída a instalação de atualização	Genetec Patroller™, Mobile Sharp	Uma atualização foi concluída no Genetec Patroller™ ou em uma unidade Mobile Sharp, e nenhuma reinicialização é necessária.
Iniciada a instalação de atualização	Genetec Patroller™, Mobile Sharp	Um usuário iniciou uma atualização no Genetec Patroller™ clicando no ícone "Atualizar".
Concluída a desinstalação de atualização	Genetec Patroller™, Mobile Sharp	Uma reversão para uma versão anterior do Genetec Patroller™ ou de uma unidade Mobile Sharp foi concluída.
Iniciada a desinstalação de atualização	Genetec Patroller™, Mobile Sharp	Um usuário iniciou uma reversão para uma versão anterior no Genetec Patroller™ clicando no ícone "Reverter".
Usuário desconectado	usuário	Um usuário se desconectou de um aplicativo do Security Center.
Usuário conectado	usuário	Um usuário se conectou a um aplicativo do Security Center.
Validando tempo pago	Regra de estacionamento	O tempo de conveniência ou o tempo pago da sessão de estacionamento expirou.
Violação detectada	regra de estacionamento	O tempo de conveniência, o período de cortesia ou o tempo pago da sessão de estacionamento expirou.
Violação imposta	regra de estacionamento	O veículo em violação foi multado.
Visitante perdido	porta	Um visitante não apresentou o crachá dentro do tempo alocado após o host da delegação ou um visitante anterior.
Tentativa de conexão VRM	Função Archiver	O Archiver tentou se conectar a uma unidade VRM.
Falha de conexão VRM	Função Archiver	O Archiver não conseguiu se conectar a uma unidade VRM.

Evento	Entidade de origem	Descrição
Janela fechada	zona	Uma janela física foi fechada.
Janela aberta	zona	Uma janela física foi aberta.
Zona colocada em atenção	zona	Uma zona foi armada.
Zona colocada fora de atenção	zona	Uma zona foi desarmada.
Manutenção da zona concluída.	Zona de E/S	Uma zona de E/S foi tirada do modo de manutenção.
Manutenção da zona iniciada	Zona de E/S	Uma zona de E/S foi colocada no modo de manutenção.
Zona off-line	Zona de E/S	Uma zona de E/S está offline.

Tópicos relacionados

Tipos de eventos que podem exigir condições de confirmação na página 924

Tipos de ação

Todas as ações no Security Center estão associadas a uma entidade de destino, que é a entidade principal afetada por essa ação. Parâmetros adicionais são indicados na coluna *Descrição*. Todos os parâmetros devem ser configurados para que a ação seja válida.

Ação	Descrição
Adicionar favorito	Adiciona um *favorito* a uma *câmera*. • **Câmera:** Selecione a câmera • **Mensagem:** Texto do favorito

Armar uma área de detecção de intrusão	Arma uma *área de detecção de intrusão*.
	• **Área de detecção de intrusão:** Selecione uma área de detecção de intrusão.
	• **Mestre:** Arma todos os sensores na área de detecção de intrusão selecionada. Todos os sensores podem disparar o alarme quando ativados.
	• **Perímetro:** Arma somente os sensores designados para estarem no perímetro. A atividade de sensores dentro da área, como detectores de movimento, é ignorada.
	• **Instantâneo:** Arma a área imediatamente.
	• **Atraso:** Arma a área após um intervalo. Se você não especificar uma duração, o painel padrão é utilizado.
	• **Modo de armação:**
	  • **Normal:** Arma a área de detecção de intrusão normalmente. Áreas com sensores ativos ou com problemas permanecem desarmadas.
	  • **Forçar:** Se a área não estiver pronta para a armação normal, essa opção força a armação da área. Forçar ignora temporariamente sensores ativos ou com problemas durante a sequência de armação. Se um servidor ignorado voltar ao estado normal enquanto armado, atividades futuras podem disparar o alarme.
	  • **Desvio:** Se a área não estiver pronta para a armação normal, essa opção ignora automaticamente sensores ativos ou com problemas antes de armar a área. Os sensores permanecem ignorados enquanto a área estiver armada. Desarmar a área remove o desvio.

Armar zona	Arma uma *zona virtual*. • **Zona:** Selecione uma zona virtual.

Ação	Descrição

Bloquear e desbloquear vídeo	Bloqueia ou desbloqueia uma câmera de outros usuários do sistema.
	• **Bloquear/Desbloquear:** Selecione se a ação bloqueará ou desbloqueará a câmera.
	• **Câmera:** Selecione a câmera
	• **Final:** Selecione por quanto tempo bloquear o vídeo:
	  • **Por:** O vídeo está bloqueado para os usuários durante o período selecionado.
	  • **Indefinidamente:** O vídeo está bloqueado para os usuários até que você o desbloqueie manualmente.
	• **Nível de usuário:** Selecione um nível de usuário mínimo. Todos os usuários com um nível inferior ao selecionado serão bloqueados e não poderão exibir o vídeo.

Cancelar postergar a colocação da área de detecção de intrusão em atenção	Cancela a armação adiada de uma *área de detecção de intrusão*. • **Área de detecção de intrusão:** Selecione a área de detecção de intrusão.

Limpar tarefas	Limpa a lista de tarefas nos monitores especificados do Security Desk.
	• **Destino:** Selecione um dos seguintes:
	  • **Usuário:** Todos os monitores de todos os aplicativos do Security Desk conectados com o nome de usuário especificado.
	  • **Monitoramento:** Monitor Security Desk específico identificado por um nome de máquina e por um ID de monitor.

Desarmar a área de detecção de intrusão	Desarma uma *área de detecção de intrusão*. • **Área de detecção de intrusão:** Selecione a área de detecção de intrusão.
Desarmar zona	Desarma uma *zona virtual*. • **Zona:** Selecione uma zona virtual.
Exibir uma câmera em um monitor analógico	Exibe uma câmera em um monitor analógico em uma tela lado a lado. • **Câmera:** Selecione qual câmera deverá ser exibida no monitor analógico. A Câmera deverá ser suportada pelo monitor analógico e usar o mesmo formato de vídeo. • **Monitor analógico:** Selecione um monitor analógico no qual exibir a câmera.

Ação	Descrição

Exibir uma entidade no Security Desk	Exibe uma lista de entidades na Security Desk *tela* de *usuários* selecionados, em termos de uma entidade por tela. Essa ação será ignorada, se um usuário não tiver uma tarefa *Monitoramento* aberta no Security Desk.
	• **Destinatários:** Selecione os usuários.
	• **Entidades:** Lista de entidades a serem exibidas. Cada entidade é exibida em uma tela separada.
	• **Opções de exibição:** Selecione um dos seguintes:
	  • **Exibir em uma tela livre:** Use apenas telas livres.
	  • **Forçar a exibição em telas:** Exiba em telas livres primeiro. Quando não houver mais nenhuma tela livre, use as telas ocupadas, seguindo a sequência de IDs de telas.

Enviar relatório por e-mail	Envia um relatório (com base em uma tarefa de geração de relatório salva) como um anexo de e-mail a uma lista de *usuários*. • **Relatório:** Selecione uma tarefa pública salva. • **Destinatários:** Selecione os usuários para os quais enviar o relatório. • **Formato para exportação:** Formato de relatório, *PDF* ou *Excel*.
Enviar uma foto por e-mail	Envia uma série de instantâneos de um vídeo como um anexo de e-mail a uma lista de usuários. • **Câmera:** Selecione a câmera • **Instantâneos:** Selecione quantos segundos antes (máximo -300 segundos) ou depois (máximo 5 segundos) do *Tempo de recorrência* definido para enviar o instantâneo por e-mail. • **Destinatários:** Seleciona os usuários que receberão o instantâneo. Um endereço de e-mail deve ser definido nas configurações do usuário. • **Formato para exportação:** Formatos de imagem disponíveis: *PNG*, *GIF*, *JPEG* ou *Bitmap*. **NOTA:** Para enviar instantâneos, a opção **Habilitar solicitações de miniaturas** deve estar ligada na aba *Recursos* do Archiver ou do Archiver auxiliar gerenciando a câmera.

Exportar relatório	Gera e salva um relatório especificado por uma tarefa pública.
	• **Relatório:** Selecione uma tarefa pública.
	• **O que exportar:**
	  • **Dados:** Exporte os dados e selecione o formato de exportação (Excel, CSV, PDF).
	  • **Gráficos:** Exporte quaisquer gráficos associados e selecione o formato de exportação (PNG, JPEG).
	• **Orientação:** (Somente PDF) Selecione se o arquivo PDF deve estar no modo retrato ou paisagem.
	• **Sobrescrever arquivo existente:** Selecione se deverá substituir um relatório anteriormente salvo em uma pasta de destino. A pasta de destino é uma propriedade da função Gerenciador de relatórios.

Ação	Descrição
Perdoar violação de antirretorno	Perdoa uma violação de *antipassback* para um *portador de cartão* ou *grupo de portadores de cartão*. • **Entidade:** Selecione um titular de cartão de cartão ou um grupo de titulares de cartão.
Ir para posição inicial	Comanda a câmera PTZ para ir para sua posição inicial. Nem todas as câmeras PTZ oferecem suporte a esse recurso. • **Câmera:** Selecione uma câmera PTZ.
Vai para predefinição	Comanda a câmera PTZ para ir para a posição de predefinição especificada. • **Câmera:** Selecione uma câmera PTZ. • **Predefinição:** Predefinir uma posição (número) para a qual ir.
Importar do arquivo	Importa um arquivo e envia os resultados da importação para um *usuário*. • **Destinatário:** Selecione um usuário. • **Nome do arquivo:** Abre a janela da ferramenta de importação, onde você pode selecionar o arquivo que é usado para importar os dados.
Sobrepor com a qualidade de gravação do evento	Define *Melhorar a qualidade da gravação do evento* como *LIGADO* para a câmera de seleção e aplica as configurações personalizadas de melhoria da qualidade da gravação. Selecionar essa opção substitui as configurações gerais da gravação do evento. O efeito dessa ação dura, enquanto ela não for modificada por outra ação, como o *Qualidade da gravação como configuração padrão*, ou até o Arquivador ser reiniciado. • **Câmera:** Selecione uma câmera.
Substituir com qualidade de gravação manual	Define *Melhorar a qualidade da gravação manual* como *LIGADO* para a câmera de seleção e aplica as configurações personalizadas de melhoria da qualidade da gravação. Selecionar essa opção substitui as configurações gerais da gravação do evento. O efeito dessa ação dura, enquanto ela não for modificada por outra ação, como o *Qualidade da gravação como configuração padrão*, ou até o Arquivador ser reiniciado. • **Câmera:** Selecione uma câmera.
Reproduzir um som	Reproduz um som no Security Desk de um usuário ou de um grupo de usuários. Essa ação será ignorada se o usuário não estiver executando o Security Desk. • **Usuário, grupo de usuários:** Selecione um usuário ou um grupo de usuários. • **Som a ser reproduzido:** Arquivo de som (.wav) a ser reproduzido. Para o usuário ouvir o som, o mesmo arquivo de som deverá ser instalado no PC em que o Security Desk está sendo executado. Os arquivos de som de alerta padrão que vêm com a instalação estão localizados em *C:\Program files\Genetec Security Center 5.7\Audio*.

Ação	Descrição
Postergar o armamento da área de detecção de intrusão	Adia a armação da área de detecção de intrusão. • **Modo de armação:** A armação *Mestre ou* a armação *Perímetro*. • **Área de detecção de intrusão:** Selecione a área de detecção de intrusão. • **Adiar para:** Define por quanto tempo adiar a armação, em segundos. • **Atraso de armamento:** Define o atraso da armação, em segundos.
Reiniciar unidade	Reinicia uma unidade • **Entidade:** Selecione uma unidade de vídeo ou uma unidade de controle de acesso a ser reiniciada.
Qualidade da gravação como configuração padrão	Cancela o efeito do *Substituir com qualidade de gravação manual* e das ações do *Sobrepor com a qualidade de gravação do evento* e restaura a configuração de gravação padrão. • **Câmera:** Selecione uma câmera.
Redefinir a contagem de pessoas na área	Redefine o contador de pessoas em uma *área*. • **Área:** Selecione uma área.
Redefinir o sistema externo	Força a função Omnicast™ Federation™ a se reconectar ao sistema Omnicast™ remoto. • **Função:** Selecionar função Omnicast™ Federation™
Redefinir inventário da zona de estacionamento	Redefine o inventário da zona de estacionamento para zero para que a ocupação da zona de estacionamento relatada possa ser reinicializada.
Executar uma macro	Inicia a execução de uma *macro*. • **Macro:** Selecione uma macro. • **Contexto:** Especifique configurações de valor para as variáveis de contexto.
Executar um padrão	Comanda a câmera PTZ para executar o padrão especificado. • **Câmera:** Selecione uma câmera PTZ. • **Padrão:** Número de padrão a ser executado.
Enviar uma mensagem	Envia uma mensagem pop up para o Security Desk de um usuário. Essa ação será ignorada se o usuário não estiver executando o Security Desk. • **Destinatários:** Selecione um usuário ou um grupo de usuários. • **Mensagem:** Texto a ser exibido na mensagem pop up. • **Tempo limite de execução expirado:** Selecione por quanto tempo a mensagem será exibida.

Ação	Descrição
Enviar um e-mail	Envia um e-mail para usuários ou portadores de cartão. O usuário selecionado deverá ter um endereço de e-mail configurado e o servidor de e-mail deverá estar adequadamente configurado para o Security Center ou a ação será ignorada. • **Destinatários:** Selecione um usuário, um grupo de usuários, titular ou grupo de titulares de cartão. • **Mensagem:** O texto de e-mail a ser enviado para o destinatário.

Enviar tarefa	Envia e adiciona uma tarefa pública a um aplicativo do Security Desk.
	• **Tarefa:** Selecione uma tarefa pública salva a ser enviada.
	• **Destino:** Selecione um dos seguintes:
	  • **Usuário:** Todos os Security Desk conectados a esse usuário
	  • **Monitoramento:** Monitor Security Desk específico identificado por um nome de máquina e por um ID de monitor.

Definir modo do leitor	Define o modo do leitor para acesso às portas. • **Localização:** Seleciona uma área, porta ou elevador. • **Modo do leitor:** Seleciona se o acesso é concedido usando *Cartão e PIN* ou *Cartão ou PIN* para as áreas selecionadas. Esta ação funciona somente com os controladores de portas e os leitores que suportam este recurso.
Definir modo de manutenção da porta	Define o status *Desbloqueado para manutenção* de uma *porta* como Ligado ou Desligado. • **Porta:** Selecione uma porta. • **Manutenção:** Modo de manutenção desejado (Ligado ou Desligado).
Definir o nível de ameaça	Define um nível de ameaça no seu sistema do Security Center ou em áreas específicas. • **Área:** Selecione em quais áreas definir o nível de ameaça. Pode ser todo o seu sistema ou áreas específicas. • **Nível de ameaça:** Selecione qual nível de ameaça deverá ser definido.
Silenciar alarme	Reconfigura a saída de alarme definida para uma porta. Essa ação define a opção *Alarme* como *Nenhuma*na guia *Hardware* de uma porta no Config Tool. • **Porta:** Selecione uma porta.
Alarme de som	Configura a saída de alarme definida para uma porta. O som do alarme é especificado na opção *Alarme* na guia *Hardware* de uma porta no Config Tool. • **Porta:** Selecione uma porta.

Ação	Descrição

Iniciar a aplicação da proteção do vídeo	Inicia a proteção das próximas gravações de vídeo contra exclusão. A proteção é aplicada em todos os *arquivos de vídeo* necessários para armazenar a *sequência de vídeos protegidos*. Como nenhum arquivo de vídeo pode ser parcialmente protegido, o tamanho real da sequência de vídeos protegida depende da granularidade dos arquivos de vídeo.
	Quando as várias ações do *Iniciar a aplicação da proteção do vídeo* são aplicadas no mesmo arquivo de vídeo, o maior período de proteção é mantido.
	• **Câmera:** Selecione uma câmera.
	• **Manter protegido para:** Duração da proteção do vídeo.
	  • **Específico:** Define o período de proteção em número de dias.
	  • **Infinita:** A proteção só pode ser removida manualmente da tarefa *Arquivar detalhes do armazenamento*.
	• **Proteger vídeo durante os próximos:** Duração do vídeo a ser protegido.
	  • **Específico:** Define a duração em minutos e em horas.
	  • **Infinita:** Todas as gravações futuras estarão protegidas, até que a ação do *Parar aplicação de proteção de vídeo* seja executada.

Iniciar gravação	Inicia a gravação na câmera especificada. Essa ação será ignorada, se a câmera não estiver em uma programação de gravação ativa. As gravações iniciadas por essa ação não poderão ser interrompidas manualmente por um usuário.
	• **Câmera:** Selecione uma câmera.
	• **Duração da gravação:** Define a duração da gravação do vídeo.
	  • **Padrão:** Define a duração para seguir o valor definido em *Tamanho padrão da gravação manual* configurado para a câmera.
	  • **Infinita:** A gravação só poe ser interrompida pela ação do *Interromper gravação*.
	  • **Específico:** Define a duração da gravação em segundos, em minutos e em horas.

Iniciar transferência	Inicia uma transferência de arquivo. • **Grupo de transferência:** Selecione um grupo de transferência para o qual começar a transferência. A transferência pode consistir na recuperação das gravações de vídeo a partir de unidades, duplicando os arquivos de vídeo de um arquivador para outro arquivador ou fazendo back-up de arquivos em um local especificado.
Parar aplicação de proteção de vídeo	Interrompe a proteção das próximas gravações de vídeo contra exclusão. Essa ação não afeta os *arquivos de vídeo* que já estão protegidos. • **Câmera:** Selecione uma câmera. • **Interromper em:** Define a proteção do vídeo para ser interrompida *Agora* ou em um *Determinado* período em minutos e em horas.

Ação	Descrição
Interromper gravação	Interrompe a gravação na câmera especificada. Essa ação funciona apenas se a gravação tiver sido iniciada pela ação do *Iniciar gravação*. • **Câmera:** Selecione uma câmera. • **Interromper em:** Define a gravação para ser interrompida *Agora* ou em um *Determinado* período em segundos, em minutos e em horas.
Interromper transferência	Interrompe uma transferência de arquivo. • **Grupo de transferência:** Selecione um grupo de transferência para o qual interromper a transferência.
Sincronizar função	Inicia um processo de sincronização na função especificada (*Active Directory* ou *Sincronizador Global de Portadores de Cartão*). • **Função:** Selecione uma função que precisa de sincronização. • **Obter imagem:** (Função Active Directory apenas) Ative essa opção se os atributos da imagem não tiverem que ser sincronizados também.

Substituir temporariamente as programações de desbloqueio	Bloqueia ou desbloqueia temporariamente uma porta por um determinado período.
	• **Porta:** Selecione uma porta.
	• **Modo de bloqueio:** Selecione *Desbloqueado* ou *Bloqueado*.
	  • **Por:** Quantidade de tempo em minutos ou em horas
	  • **De/Para:** Intervalo de data e de hora para desbloquear a porta.

Disparar alarme	Aciona um alarme. Esta ação pode gerar eventos adicionais, dependendo da configuração do alarme. • **Alarme:** Selecione um alarme. • **Condição de confirmação:** Tipo de evento que deve ser acionado, antes de o alarme poder ser confirmado. • **Confirmação do usuário necessária:** Selecione se o alarme deverá ser confirmado manualmente ou se ele será confirmado automaticamente pelo sistema depois da condição de confirmação ter sido limpa.
Aciona um alarme de intrusão	Aciona um alarme físico em uma área de detecção de intrusão. • **Tipo de destinatário:** Tipo de acionamento de alarme, de detecção de área de intrusão ou uma entrada de alarme específica. • **Área de detecção de intrusão:** Selecione uma área de detecção de intrusão.
Disparar saída	Aciona um *comportamento de saída* em um pino de saída de uma *unidade*. Por exemplo, uma ação pode ser configurada para acionar o pino de saída de uma unidade (controlador ou módulo de entrada/saída). • **Relé de saída:** Selecione um pino de saída (unidade). • **Comportamento da saída:** Selecione o comportamento de saída a ser acionado.

Ação	Descrição
Acionar correspondência de leituras passadas	Dispara a função LPR Manager para comparar lista de procurados novas ou atualizadas contra reconhecimentos de placas de veículos previamente capturados.
Desbloquear a porta explicitamente	Desbloqueia, temporariamente, uma porta por cinco segundos, ou pelo *Tempo de concessão padrão* configurado para essa porta. • **Porta:** Selecione uma porta.

Apêndices

Apêndices

Esta seção inclui os seguintes tópicos:

- "Opções de licença" na página 1130
- "Portas padrão do Security Center" na página 1136
- "Referência do HID" na página 1146
- "Recurso de múltiplas leituras" na página 1173

A

Opções de licença

Esta seção inclui os seguintes tópicos:

- "Ver informações da licença" na página 1131
- "Opções de licença no Security Center" na página 1132

Ver informações da licença

Você pode ver informações sobre sua licença comprada, como seu número SMA, recursos suportados, data de validade da licença e assim por diante, a partir da página Sobre no Config Tool ou no Server Admin.

Para visualizar informações da licença no Config Tool:

1 Na página inicial, clique em **Sobre.**

Caso você não consiga visualizar suas opções de licença, maximize a janela do Config Tool ou clique na lista suspensa **Licença**.

Para visualizar informações da licença no Server Admin:

1 Faça login no seu servidor principal usando o Server Admin.

2 Clique na aba **Directory**, vá para a seção **Licença** e clique em **Informações da licença**.

Opções de licença no Security Center

Esta seção descreve o significado de todas as opções de licença do Security Center.

Opções de licença Security Center

As opções de licença genéricas do Security Center são as seguintes:

- **Gerenciamento de ativos:** Permite usar a funcionalidade de gerenciamento de ativos no Security Center em combinação com o plug-in *Código RF*, que permitem que você defina ativos que você pode acompanhar e denunciar no Security Desk.
- **Notificação automática por e-mail:** Permite configurar um servidor de e-mail para notificações por e-mail, incluindo:
  - Receber notificações por e-mail do *Watchdog*.
  - Usando as ações *Enviar um e-mail* e *Enviar relatório por e-mail*.
- **Gráficos:** Permite gerar relatórios visuais.
- **Detecção de intrusão:** Permite usar a funcionalidade de detecção de intrusão no Security Center, como adicionar funções de Intrusion Manager e unidades de detecção de intrusão no Config Tool e receber alarmes de intrusão no Security Desk.
- **Macros:** Permite criar macros no seu sistema.
- **SDK de mídia:** Permite criar funções de SDK Media.
- **Número de Active Directories:** Número máximo de domínios do Active Directory que podem ser sincronizados com o sistema.
- **Número de servidores adicionais de Directory:** O número máximo de servidores de Directory que você pode ter além do seu servidor principal para configurar um sistema de alta disponibilidade.
- **Número de integrações do ADFS:** Número máximo de conexões *Active Directory Federation Service* permitidos no seu sistema.
- **Número de caixas registradoras:** Número máximo de caixas registradoras de que você pode importar de um sistema de *ponto de venda* externo.
- **Número de campos personalizados:** Número máximo de campos personalizados que você pode definir.
- **Número de sistemas federados:** Número máximo de sistemas federados permitidos, contando os sistemas 4.x Omnicast™ e Security Center.
- **Número de pontos de entrada:** Número máximo de entradas que podem ser configuradas para *portas*, *elevadores* e *zonas*. Somente são contadas as entradas encontradas em subpanéis dedicados de E/S, como o HID V200 ou o Mercury MR16IN. As entradas integradas encontradas nas placas controladoras não são contadas.
- **Número de unidades de detecção de intrusão:** Número máximo de painéis de intrusão suportados no seu sistema.
- **Número de relés de saída:** Número máximo de saídas que podem ser configuradas para *portas*, *elevadores* e *zonas*. Somente são contadas as saídas encontradas em subpanéis dedicados de E/S, como o HID V200 ou o Mercury MR16OUT. As saídas integradas encontradas nas placas controladoras não são contadas.
- **Número de conexões Security Desk:** Número máximo de conexões simultâneas de Security Desk permitidos no seu sistema.
- **SDK de plugin:** Permite criar funções de plug-in.
- **Remoto Security Desk:** Permite que você monitore e controle remotamente outros monitores e estações de trabalho Security Desk, usando a tarefa *Remoto* em seu Security Desk local.

- **Nível de ameaça:** Permite que você crie níveis de ameaça no Config Tool e configure níveis de ameaça no Security Desk.
- **Web SDK:** Permite criar funções SDK baseadas na Web.

Opções de licença Synergis™

As opções de controle de acesso *Synergis™* são as seguintes:

- **Antirretorno:** Permite configurar áreas com restrições *anti-passback*.
- **Modelo do crachá:** Permite definir *modelos de crachá* no seu sistema.
- **Solicitações de cartão:** Permite que os usuários solicitem credenciais de cartão para serem impressas por outros usuários no sistema. Também permite que você crie motivos para a solicitação no Config Tool.
- **Ferramenta de importação:** Permite importar titulares de cartões e credenciais a partir de um arquivo simples.
- **Número de Access Managers:** Número máximo de funções *Access Manager* que podem ser criadas no seu sistema.
- **Número de titulares de cartão e visitantes:** Número máximo de titulares de cartões e visitantes permitidos em seu sistema, incluindo os importados de Active Directories.
- **Número de Global Cardholder Synchronizers:** Número máximo de funções *Global Cardholder Synchronizer* sendo executadas em sistemas *compartilhando visitante* convidados de compartilhamento que têm permissão para se conectar ao *host de compartilhamento* simultaneamente. Essa opção de licença é usada pelo *host de compartilhamento* para limitar o número de conexões.
- **Número de leitores:** Número máximo de *leitores* que podem ser configurados para *portas* e *elevadores* em seu sistema.
- **Contagem de pessoas:** Permite usar a tarefa *Contagem de pessoas* no Security Desk.
- **Codificação de cartão inteligente:** Permite criptografar cartões inteligentes.
- **Leitor de inscrição USB:** Permite detectar e usar leitores USB no seu sistema.
- **Visitantes:** Permite usar a tarefa *Gerenciamento de visitantes* no Security Desk.

Opções de licença Genetec Mission Control™

Para obter as opções de licença do *Genetec Mission Control™*, consulte o *Genetec Mission Control™Guia do usuário*.

Opções de licença Omnicast™

As opções de licença do *Omnicast™* são as seguintes:

- **Criptografia do Archiver:** Permite criptografar fluxos de vídeo.
- **Áudio:** Permite que seu sistema transmita áudio e ative todos os recursos de áudio em seu sistema.
- **Bloqueio de câmera:** Permite bloquear o vídeo de outros usuários no sistema.
- **Gravação de borda:** Permite a capacidade de transferir dados das unidades de gravação da unidade para o Archiver.
- **Pesquisa forense:** Ativa a tarefa *Pesquisa forense* no Security Desk.
- **Aceleração de hardware:** Permite que você use o recurso de aceleração de hardware para decodificação de vídeo.
- **Número de Auxiliary Archivers:** Número de funções *Archiver auxiliar* permitidas no seu sistema.
- **Número de câmeras e monitores analógicos:** Número máximo de *câmeras* e *monitores* analógicos permitidos em seu sistema. Câmeras e monitores analógicos gerenciados localmente pelo seu sistema

e os federados de sistemas remotos são contados. Câmeras e monitores analógicos também são cumulativos. Por exemplo, se você usar 5 câmeras e 5 monitores analógicos simultaneamente, eles contam como 10 entidades na licença.

- **Número de teclados CCTV:** Número de teclados CCTV permitidos no seu sistema.
- **Número de entradas de DVR:** Número de entradas de vídeo de DVRs (gravadores de vídeo digitais) permitidos em seu sistema.
- **Número de câmeras OVReady:** Número máximo de câmeras OVReady (com recursos de *análise de vídeo*) permitido em seu sistema.
- **Número de câmeras panorâmicas:** Número de câmeras panorâmicas permitidas no seu sistema.
- **Número de streams protegidos por privacidade:** Número de transmissões de vídeo com proteção de privacidade permitidos no seu sistema.
- **Número de câmeras promocionais:** Número de canais de vídeo permitidos no seu sistema de acordo com uma promoção comercial disponível no momento da compra. As unidades de vídeo elegíveis para tal promoção usam estas licenças promocionais primeiro. Por exemplo, se você comprar conexões de câmera quando uma promoção aplica-se, as próximas câmeras elegíveis que você adicionar ao seu sistema usarão as licenças da câmera promocional até o limite de *Número de câmeras promocionais*. Quando este limite for atingido, as próximas câmeras elegíveis adicionadas usarão conexões regulares da câmera. Isso se aplica à atual *Promoção de Câmera Analógica*.
- **Número de câmeras restritas:** Número de *câmeras restritas* permitidas no seu sistema. Câmeras restritas também exigem uma licença de câmera regular. Para exibir uma lista de fabricantes que exigem uma licença restrita, use o filtro **Tipo de licença** *Restrito* na Lista de Dispositivos Suportados.
- **Número de fluxos RTSP:** Número máximo de fluxos de vídeo que podem ser solicitados simultaneamente a partir da função Media Gateway.
- **Número de servidores do Archiver em standby:** Número total de servidores secundários atribuídos a funções de Archiver no sistema.
- **Número de servidores do Archiver em standby por Archiver:** Número de servidores em standby permitidos por função Archiver. Esta licença é necessária para atribuir um servidor terciário para o failover da função Archiver.

Opções de licença AutoVu™

As opções de licença do *AutoVu™* LPR são as seguintes:

- **Geocodificador:** Tipo de mecanismo de mapa usado pelo LPR Manager para geocodificação: *Bing* ou *BeNomad*.
- **Número de fluxos de análise de Sharp fixas:** Número máximo de unidades Sharp fixas permitidas no seu sistema.
- **Número de LPR Managers:** Número máximo de funções *LPRManager* permitidas no seu sistema.
- **Número de Patrollers - Fiscalização de estacionamento municipal:** Número máximo de *Patrollers* configurados para *Fiscalização de estacionamento da cidade* permitidos em seu sistema.
- **Número de Patrollers - Fiscalização da lei:** Número máximo de *Patrollers* configurados para *Aplicação da lei* permitidos em seu sistema.
- **Número de Patrollers - MLPI:** Número máximo de *Patrollers* configurados para *Inventário de placas de veículos móvel* permitidos em seu sistema.
- **Número de Patrollers - Fiscalização de estacionamento universitário:** Número máximo de *Patrollers* configurados para *Fiscalização de estacionamento na universidade* permitidos em seu sistema.
- **Número de Patrollers equipados com mapas:** Número máximo de *Patrollers* equipados com mapas permitidos em seu sistema.
- **Security Deskmapa:** Tipo de mecanismo de mapa suportado em Security Desk: *Bing* ou *BeNomad*.

- **Importar XML:** Permite importar dados de aplicativos de terceiros.
- **Data de expiração da licença do Microsoft Bing:** Data de expiração da licença do Bing.

Opções Plan Manager

As opções de licença do *Gestor de planos* são as seguintes:

- **Plan Manager Avançado:** Permite que você use o Plan Manager no Modo avançado.
- **ArcGIS Plan Manager:** Permite usar mapas ArcGIS.
- **Plan Manager Básico:** Permite que você use o Plan Manager no modo Básico.
- **Plan Manager Padrão:** Permite que você use o Plan Manager no modo Padrão.

Opções de licença móveis

As opções de licença do *Security Center Mobile* são as seguintes:

- **Número de servidores de dispositivos móveis:** Número máximo de *Mobile Servers* permitidos no seu sistema.
- **Número de dispositivos móveis:** Número máximo de conexões simultâneas de *Aplicativos móveis* permitidos no seu sistema.
- **Número de Web Clients:** Número máximo de conexões simultâneas de *Web Clients* permitidos no seu sistema.

Opções de licença do certificado

As opções de licença do *certificado*. Cada certificado é identificado por um nome de aplicativo/plugin e o nome do editor. A opção especifica o número máximo de conexões simultâneas de cada tipo de aplicativo permitido em seu sistema.

B

Portas padrão do Security Center

Esta seção inclui os seguintes tópicos:

- "Portas usadas por aplicativos principais no Security Center" na página 1137
- "Portas usadas por aplicativos AutoVu no Security Center" na página 1139
- "Portas usadas por aplicativos Omnicast no Security Center" na página 1141
- "Portas usadas por aplicativos Synergis no Security Center" na página 1144

Portas usadas por aplicativos principais no Security Center

Para que o Security Center funcione corretamente, precisa criar regras de firewall para permitir uma comunicação adequada entre os vários serviços.

IMPORTANTE: Expor o Security Center à Internet é altamente desaconselhado sem que o sistema seja reforçado primeiro. Antes de expor o seu sistema, implemente o nível de segurança avançado descrito no *Guia de Reforço do Security Center* para ajudar a proteger o seu sistema contra ameaças da Internet. Em alternativa, use uma VPN confiável para conexões remotas.

A tabela a seguir lista as portas de rede padrão usadas por aplicativos principais no Security Center. Para visualizar o diagrama de rede, clique aqui.

Aplicativo	Integrado	Externo	Utilização da porta
Diretório	TCP 5500		Conexões do cliente
Aplicativos clientes (Security Desk, Config Tool, SDK)		TCP 5500	Comunicação Genetec™ Server/Directory
		TCP 8012	Solicitações de download de mapas para o Map Manager (HTTPS)
Aplicativos clientes (Config Tool)		TCP 443	Comunicação com a GTAP para validação do Genetec™ Advantage e feedback (HTTPS)
Todas as funções (nova instalação)	TCP 5500	TCP 5500	Comunicação Genetec™ Server/Directory
	TCP 4502	TCP 4502	Comunicação com o Genetec™ Server (compatibilidade com o Security Center 5.3 e versões anteriores)
	TCP 80	TCP 80	Comunicação REST/Server Admin (HTTP)
	TCP 443	TCP 443	Comunicação segura REST/Server Admin (HTTPS)
Todas as funções (atualizado do 5.3 e versões anteriores)	TCP 4502	TCP 4502	Se 4502 era a porta do servidor antes da atualização, então 4502 permanece como a porta após a atualização, e 4503 será usada para compatibilidade com versões anteriores. Se outra porta foi usada como porta do servidor antes da atualização, então essa mesma porta é mantida como porta do servidor após a atualização. 4502 será então usada para compatibilidade com versões anteriores e 4503 não será necessária.
	TCP 4503	TCP 4503	
Gerenciador de invasão	TCP 3001	TCP 3001	Comunicação com painéis de intrusão Bosch
Gerenciador de mapas	TCP 8012		Solicitações de download de mapa do aplicativo cliente (HTTPS)

Aplicativo	Integrado	Externo	Utilização da porta
Genetec™ Update Service (GUS)	TCP 4595	TCP 4595	Comunicação com outros servidores GUS
	TCP 443	TCP 443	Comunicação com o sistema Azure e Genetec Inc. (HTTPS)
Agente do monitor de disponibilidade do sistema (SAMA, System Availability Monitor)	TCP 4592		Conexão dos servidores do Security Center
		TCP 443	Conexão ao Health Service na Nuvem (HTTPS)

Portas usadas por aplicativos AutoVu™ no Security Center

Quando o AutoVu™ está ativado em seu sistema, precisa criar regras de firewall adicionais para permitir uma comunicação adequada entre o Security Center e componentes AutoVu™ externos.

IMPORTANTE: Expor o Security Center à Internet é altamente desaconselhado sem que o sistema seja reforçado primeiro. Antes de expor o seu sistema, implemente o nível de segurança avançado descrito no *Guia de Reforço do Security Center* para ajudar a proteger o seu sistema contra ameaças da Internet. Em alternativa, use uma VPN confiável para conexões remotas.

A tabela a seguir lista as portas de rede padrão usadas por aplicativos AutoVu™ no Security Center. Para visualizar o diagrama de rede, clique aqui.

Aplicativo	Integrado	Externo	Utilização da porta
LPR Manager		UDP 5000	Descoberta de unidades Sharp fixas
	TCP 8731		Unidades Sharp fixas e instalações Genetec Patroller™
	TCP 8787		Pay-by-Plate (plug-in instalado separadamente)
	TCP 8832		Serviço de atualização
		TCP 8001	Porta de controle Sharp
		TCP 2323	Configuração de unidades Sharp (HTTP)
Flexreader™ (unidade Sharp)	TCP 80		Porta de vídeo (extensão Security Center HTTP)
	TCP 443		Porta de vídeo (extensão Security Center HTTPS)
	TCP 2323		Extensão do serviço de configuração (HTTP)
	TCP 4502–4534		Portas Silverlight e serviço de alimentação de imagens (para modelos Sharp anteriores a SharpV)
	TCP 4545		Porta de controle (instalação Mobile)
	UDP 5000		Porta de descoberta
	TCP 8001		Porta de controle (instalação Fixa)
		TCP 21	Carregamento de arquivo FTP
		TCP 8666	Comunicação com o serviço de atualização
Servidor do Portal (Unidade Sharp)	TCP 80		Porta de comunicação (HTTP)
	TCP 443		Porta de comunicação segura (HTTPS)

Aplicativo	Integrado	Externo	Utilização da porta
Serviço de atualização (unidade Sharp e computador no veículo)	TCP 8666		Comunicação com Flexreader™ (somente saudações)
	TCP 8889	TCP 8899	Comunicação com o serviço de atualização Genetec Patroller™
		TCP 8832	Comunicação com o LPR Manager
Genetec Patroller™ (computador de bordo)	TCP 4546		Comunicação com o servidor de Hora
	TCP 8001		Comunicação com o host Simples
		UDP 5000	Descoberta de câmera Sharp
		TCP 8666	Comunicação com o Serviço de Atualização (somente saudações)
		TCP 8731	Conexão do LPR Manager

Portas usadas por aplicativos Omnicast™ no Security Center

Quando o Omnicast™ está ativado em seu sistema, precisa criar regras de firewall adicionais para permitir uma comunicação adequada entre o Security Center e dispositivos de vídeo IP externos.

IMPORTANTE: Expor o Security Center à Internet é altamente desaconselhado sem que o sistema seja reforçado primeiro. Antes de expor o seu sistema, implemente o nível de segurança avançado descrito no *Guia de Reforço do Security Center* para ajudar a proteger o seu sistema contra ameaças da Internet. Em alternativa, use uma VPN confiável para conexões remotas.

A tabela a seguir lista as portas de rede padrão usadas por aplicativos Omnicast™ no Security Center. Para visualizar o diagrama de rede, clique aqui.

Aplicativo	Integrado	Externo	Utilização da porta
Archiver	TCP 555		Solicitações de stream ao vivo e de reprodução
	TCP 605		Solicitações de stream de reprodução Edge
	TCP 5602		Solicitações de conexão a console Telnet
	UDP 6000–6500		Áudio de aplicativos cliente
	UDP 15000–19999[1]		Transmissão unicast ao vivo de câmeras de IP
	UDP 47806, 47807	UDP 47806, 47807	Transmissão de vídeo e áudio multicast ao vivo
	TCP e UDP		Portas específicas de vendedores para eventos e detecção de câmera de IP
		TCP 80	Porta HTTP
		TCP 443	Porta HTTPS
		TCP 554	Porta RTSP
Redirecionador	TCP 560, 5004[2]		Solicitações de stream ao vivo e de reprodução
		TCP 554	Comunicação com o Media Router (Security Center Federation™)
		TCP 555	Comunicação com o Archiver
		TCP 558	Comunicação com o Archiver Auxiliar
		TCP 560, 5004	Solicitações de stream para outros redirecionadores

Aplicativo	Integrado	Externo	Utilização da porta
		UDP 6000–6500	Transmissão de mídia a aplicações de clientes
	UDP 8000–12000	UDP 8000–12000	Transmissão de mídia a outros redirecionadores
	UDP 47806, 47807	UDP 47806, 47807	Transmissão de vídeo e áudio multicast ao vivo
Archiver Auxiliar	TCP 558		Solicitações de stream ao vivo e de reprodução
	UDP 15000–19999[1]		Transmissão unicast ao vivo (câmeras de IP)
	UDP 47806, 47807	UDP 47806, 47807	Transmissão de vídeo e áudio multicast ao vivo
		TCP 554, 560	Solicitações de stream ao vivo e de reprodução
Roteador de mídia	TCP 554		Solicitações de stream ao vivo e de reprodução
		TCP 554	Solicitações de stream de Media Router Federado
Gateway de mídia	TCP 654		Solicitações de stream ao vivo e de reprodução
	UDP 6000–6500		Stream de vídeo unicast
	UDP 47806	UDP 51914	Transmissão de vídeo multicast ao vivo
Omnicast™ Federation™		TCP 5001–5002	Conexão a sistemas remotos Omnicast™ 4.x.
Aplicativos clientes (Security Desk e Config Tool)	UDP 6000–6200		Streams de mídia unicast
	UDP 47806, 47807		Streams de vídeo e áudio multicast ao vivo
		TCP 554, 560	Solicitações de vídeo e áudio de reprodução e ao vivo
Aplicativo cliente (Config Tool)		Portas TCP e UDP específicas do fornecedor	Detecção de unidade com a ferramenta de Inscrição de unidade

[1] Você pode ter vários agentes Archiver no mesmo servidor. Cada agente Archiver atribui uma porta UDP exclusiva para cada unidade de vídeo que controla. Para garantir que a atribuição de portas UDP em um servidor seja exclusiva, cada agente Archiver adicional no mesmo servidor adiciona 5000 ao seu número de porta UDP inicial. Por exemplo, o primeiro agente Archiver usa portas 15000–19999, o segundo usa portas 20000–24999, o terceiro usa portas 25000–29999 e assim por diante.

NOTA: Você pode atribuir manualmente portas UDP de recepção de transmissões ao vivo na aba **Recursos** da função Archiver.

[2] As portas TCP 560 e 5004 são aplicáveis a sistemas que usem apenas um redirecionador. Se estiver usando vários redirecionadores, estes números de porta aumentam um valor para cada redirecionador. Por exemplo, os números de porta para o seu segundo redirecionador serão TCP 561 e TCP 5005 e assim por diante para cada redirecionador que estiver usando.

Tópicos relacionados

Archiver - Aba Recursos na página 1053

Portas usadas por aplicativos Synergis™ no Security Center

Quando o Synergis™ está ativado em seu sistema, precisa criar regras de firewall adicionais para permitir uma comunicação adequada entre o Security Center e dispositivos de controle de acesso IP externos.

IMPORTANTE: Expor o Security Center à Internet é altamente desaconselhado sem que o sistema seja reforçado primeiro. Antes de expor o seu sistema, implemente o nível de segurança avançado descrito no *Guia de Reforço do Security Center* para ajudar a proteger o seu sistema contra ameaças da Internet. Em alternativa, use uma VPN confiável para conexões remotas.

A tabela a seguir lista as portas de rede padrão usadas por aplicativos Synergis™ no Security Center. Para visualizar o diagrama de rede, clique aqui.

Aplicativo	Integrado	Externo	Utilização de portas
Access Manager		UDP 2000	Extensão Synergis™ - descoberta
		TCP 443	Comunicação protegida com unidades Synergis™ e unidades HID (HTTPS)
	TCP 20	TCP 21	Extensão HID - dados e comandos FTP[1]
		TCP 22	Extensão HID - SSH[1]
		TCP 23	Extensão HID - Telnet[1]
		TCP 80	Extensão HID - comunicação HTTP
		TCP 4050	Extensão HID - protocolo VertX OPIN
	TCP/UDP 4070	TCP/UDP 4070	Extensão HID - descoberta VertX[2]
	TCP/UDP		Portas específicas de fornecedores para eventos e descoberta de dispositivo de controle de acesso IP
Synergis™ Softwire (unidade Synergis™)	TCP 80	TCP 80	Porta de comunicação (HTTP)
	TCP 443	TCP 443	Porta de comunicação segura (HTTPS)
			Integração do AutoVu™ SharpV (HTTPS)
	UDP 2000	UDP 2000	Descoberta e comunicação P2P
	TCP 3389		Conexão RDP (desativada por padrão)
	TCP 2571	TCP 2571	Travas de IP Assa Abloy (protocolo R3)
		UDP 5353	Descoberta de controlador Axis (mDNS)
	TCP 3001	TCP 3001	Comunicação Mercury ou Honeywell
	TCP 1234	TCP 1234	Comunicação de trava Salto Sallis

Aplicativo	Integrado	Externo	Utilização de portas
Controladores HID VertX/Edge Legacy e EVO	TCP 21		Comando FTP[1]
	TCP 22		Porta SSH (somente EVO)[1]
	TCP 23		Telnet[1]
	TCP 4050		Protocolo VertX OPIN
	UDP 4070	UDP 4070	Descoberta VertX

[1] Não necessário se as unidades HID estiverem configuradas no **Modo seguro**.

[2] A porta de descoberta de uma unidade HID está configurada em 4070. Após ser descoberta, a unidade é atribuída a um Access Manager que utiliza as portas exibidas na tabela anterior para controlá-la.

Para mais informações sobre a configuração inicial do hardware HID, baixe a documentação em http://www.HIDglobal.com

C

Referência do HID

Esta seção inclui os seguintes tópicos:

- "Hardware HID suportado" na página 1147
- "Download de documentação de HID" na página 1148
- "Controladores HID VertX suportados" na página 1149
- "Subpainéis HID VertX suportados" na página 1151
- "Controladores HID Edge suportados" na página 1153
- "Módulos de interface Edge suportados" na página 1155
- "Versões de firmware de HID suportadas" na página 1156
- "O que pode ser feito ou não instalação do hardware HID" na página 1157
- "Conexões do HID VertX V1000 RS-485" na página 1159
- "Comportamento de E/S do HID VertX V1000" na página 1160
- "Considerações sobre conexão de E/S do HID" na página 1161
- "LEDs de Alimentação e Com. do HID" na página 1162
- "Recursos e modelos de HID suportados pelo Security Center" na página 1163
- "Habilitar suporte a PIN longos em unidades HID" na página 1166
- "Configurações suportadas da unidade HID" na página 1167
- "Recursos do Security Center suportados por unidades HID" na página 1168

Hardware HID suportado

HID Global tem duas linhas de produtos. A linha de produtos mais recente é chamada EVO, e a mais antiga é chamada Legacy. Existem duas famílias de produtos em cada linha de produtos: VertX e Edge. Os produtos de diferentes famílias não podem se misturar. O Security Center oferece suporte para todos eles.

Sobre controladores HID

O Gestor de Acesso comunica diretamente com controladores HID através de uma rede IP. Portanto, todos os controladores HID são chamados de *unidades de controle de acesso* no Security Center.

Diferenças de plataformas entre EVO e Legacy

Características	EVO	Legado
Processador/Velocidade	ARM9/200 Mips	ETRAX/100 Mips
RAM	64 MB	32 MB
Sistema operacional	Linux 2.6	Linux 2.4
Shell seguro e protocolo	Sim	Não
Buffer máximo de eventos	99,999	5,000

Limitações

Em uma porta *Cartão e PIN* controlada por uma unidade HID Edge EVO, se uma pesquisa de host for necessária (uma credencial desconhecida é inserida e a unidade deve consultar o Access Manager antes de tomar uma decisão), o titular de cartão deve aguardar alguns segundos depois de apresentar seu cartão antes de inserir o PIN. Digitar o PIN muito rapidamente pode resultar em acesso negado porque os primeiros dígitos do PIN podem não ter sido registrados pela unidade.

Download de documentação de HID

Você pode encontrar toda a documentação de produtos HID online.

Clique nos links abaixo para baixar o documento desejado.

Linha de produtos	Nome do produto	Links para documentos
EVO	VertX EVO V1000	Folha de Dados do Controlador de Rede VertX EVO V1000 Exemplo de Fiação do VertX EVO V1000
	VertX EVO V2000	Folha de Dados da Interface de Leitor/Controlador em Rede VertX EVO V2000 Exemplo de Fiação do VertX EVO V2000
	Edge EVO EH400-K	Folha de Dados do Edge EVO EH400-K
	Edge EVO EHR40-K	Folha de Dados do Controlador/Leitor e Módulo Edge EVO EHR40-K
	Edge EVO EHRP40-K	Folha de Dados do Controlador/Leitor e Módulo Edge EVO EHRP40-K
Descontinuados	VertX V1000	Folha de Dados do Controlador de Rede VertX V1000
	VertX V2000	Folha de Dados da Interface de Leitor/Controlador em Rede VertX V2000
	EdgePlus E400	Folha de Dados do EdgePlus E400
	EdgeReader ER40	Folha de Dados do EdgeReader ER40
	EdgeReader ERP40	Folha de Dados do EdgeReader ERP40

Controladores HID VertX suportados

O HID tem duas linhas ce controladores VertX: EVO (mais recente) e Legacy. A mais nova linha de controladores tem significativamente mais poder de processamento e memória do que a linha mais antiga. Ambas as linhas de controladores usam os mesmos módulos de interface (V100, V200, V300) que permanecem inalterados.

Nas tabelas a seguir, comparamos as características dos controladores EVO com as suas contrapartes Legacy.

Diferenças de plataformas VertX entre EVO e Legacy

Características	EVO	Legado
Memória flash	256 MB	8 MB
Capacidade máxima de titulares de cartão	250.000	44.000
Capacidade offline de titulares de cartão com o Security Center[1]	65.000[2]	22.000[2, 3]
Fonte de alimentação	12–24 VCC	12–18 VCC
Faixa de temperatura operacional	0–49 °C (32–120 °F)	0–50 °C (32–122 °F)
Tolerância à umidade	5% a 85% sem condensação	5% a 95% sem condensação

[1] No Security Center, um titular de cartão pode ter várias credenciais. Um titular de cartão com duas credenciais é contado como dois pelo HID.

[2] Com o Security Center, a capacidade de titulares de cartão da unidade é inferior à sua capacidade máxima de titulares de cartão. Em parte isso é devido à memória extra ser usada como cache para permitir que a sincronização de unidades seja realizada sem afetar a operação normal.

[3] Até 125.000 credenciais com atualização de memória total.

Diferenças de VertX V1000 entre EVO e Legacy

Características	EVO	Legado
Corrente máxima a 12 – 24 VCC por unidade	1 A	1 A
Corrente operacional média a 12 VCC	210 mA	140 mA
Capacidade de dispositivos a jusante[4]	Até 32 módulos de interface (ou 64 leitores)	Até 32 módulos de interface (ou 64 leitores)
Compatibilidade de dispositivos seguintes	VertX V100, V200, V300	VertX V100, V200, V300
Backup RTC	Bateria tipo moeda	Bateria tipo moeda
Portas RS-232	1	2
Portas USB	1 (reservada para uso futuro)	0

[4] O HID indica que um controlador V1000 pode suportar um máximo de 32 módulos de interface a jusante (16 em cada bus serial RS-485) No entanto, os testes de desempenho executados pela Genetec Inc. indicam que, como "prática recomendada", não devem ser excedidos os 20 módulos de interface a jusante (10 por bus serial).

Diferenças de VertX V2000 entre EVO e Legacy

Características	EVO	Legado
Corrente máxima a 12 – 24 VCC por unidade	1 A	1 A
Corrente operacional média a 12 VCC (0 leitores)	125 mA	160 mA
Corrente operacional média a 12 VCC (2 leitores)	625 mA	660 mA
Relés de saída	30 VCC, 2 A	30 VCC, 2 A

Subpainéis HID VertX suportados

Os subpainéis HID VertX (também conhecidos como *painéis de interface*) pode ser usado com controladores de rede HID VertX V1000 ou dispositivos de controle de acesso Genetec™ (Synergis™ Master Controller e Synergis™ Cloud Link).

VertX V100

Características	Especificações
Fonte de alimentação	9–18 VCC
Corrente operacional média a 12 VCC (0 leitores)	60 mA
Corrente operacional média a 12 VCC (2 leitores)	600 mA
Faixa de temperatura operacional	0–50 °C (32–122 °F)
Umidade	5% a 95% sem condensação

VertX V200

Características	Especificações
Fonte de alimentação	9–18 VCC
Corrente operacional média a 12 VCC	50 mA
Resistores para supervisão de entrada	1–10 kohm
Faixa de temperatura operacional	0–50 °C (32–122 °F)
Umidade	5% a 95% sem condensação

VertX V300

Características	Especificações
Fonte de alimentação	9–18 VCC
Corrente operacional média a 12 VCC	60 mA
Classificação do relé	2 A @ 30 VCC (carga máxima)
Faixa de temperatura operacional	0–50 °C (32–122 °F)
Umidade	5% a 95% sem condensação

Especificações de cabo

Ao conectar os módulos de interface aos seus controladores, certifique-se de não exceder os comprimentos de cabo recomendados.

Tipo de cabo	Duração máxima	Descrição
Wiegand	500 ft. (152 m) até o leitor	ALPHA 1299C, 22AWG, 9-condutores, trançado, proteção geral. Menos condutores são necessários se todas as linhas de controle não forem usadas.
RS-485	4000 ft. (1220 m) até o controlador	Cabo Belden 3105A, par trançado 22AWG, com proteção 100 Ω ou equivalente.
Ethernet	328 ft. (100 m)	Cat5, Cat5E e Cat6.
Bus Hi-O CAN	100 ft. (30 m)	Bitola 22AWG. Máximo entre quedas de 30 ft. (10 m).

Controladores HID Edge suportados

O HID tem duas linhas de controladores Edge: EVO (mais recente) e Legacy. A linha mais recente de controladores pode ter um segundo leitor opcional e ter maior eficiência de energia (12 a 24 VDC), portanto, pode suportar fechaduras de 12 V ou 24 V.

Nas tabelas a seguir, comparamos as características dos controladores EVO com as suas contrapartes Legacy.

Diferenças de plataformas Edge entre EVO e Legacy

Características	EVO	Legado
Memória flash	128 MB	8 MB
Capacidade máxima de titulares de cartão	125,000	44,000
Capacidade offline de titulares de cartão com o Security Center[1]	65,000[2]	22,000[2]
Padrão de alimentação sobre Ethernet (PoE)	802.3af	802.3af
Backup RTC	Super-cap (2-5 dias) Não é necessária substituição	Bateria (3-5 dias) Exige substituição
Violação	Chave óptica e externa	Chave mecânica e externa
Comunicação da porta	E/S discreta, Wiegand, Hi-O	E/S discreta, Wiegand
Furos de montagem e terminação da fiação	US Single-Gang, EU/ASIA 60 mm	US Single-Gang
Corrente em condição de espera	85 – 180 mA	1 A
Corrente máxima	1.5 A	1.5 A
Classificação máxima de saída combinada	1.2 A	700 mA
Faixa de temperatura operacional	0–49 °C (32–120 °F)	0–49 °C (32–120 °F)
Umidade	5% a 85% sem condensação	5% a 85% sem condensação

[1] No Security Center, um titular de cartão pode ter várias credenciais. Um titular de cartão com duas credenciais é contado como dois pelo HID.

[2] Com o Security Center, a capacidade de titulares de cartão da unidade é inferior à sua capacidade máxima de titulares de cartão. Em parte isso é devido à memória extra ser usada como cache para permitir que a sincronização de unidades seja realizada sem afetar a operação normal.

Diferenças de Edge entre EVO e Legacy

Características	EVO (EH400-K)	Legacy (E400)
Potência de bloqueio fornecida pelo controlador	12 V ou 24 V	12 V
Potência do leitor fornecida pelo controlador	12 V	12 V
Potência de entrada	PoE, 12 V, 24 V	PoE, 12 V
Potência de dispositivo periférico usando PoE	340 mA @ 24 V	700 mA @ 12 V
Leitura de E/S (2 Leitores)	Sim	Não
Entradas/Saídas	5 entradas & 2 saídas	5 entradas & 2 saídas

Diferenças de leitor/controlador Edge entre EVO e Legacy

Características	EVO (EHR40-K, EHRP40-K)	Legacy (ER40, ERP40)
Potência de entrada	PoE, 12 V, 24 V	PoE, 12 V
Potência de dispositivo periférico usando PoE	310 mA @ 24 V	600 mA @ 12 V
Compatibilidade com credencial "Smart card" 13.56 MHz	iCLASS	iCLASS
Compatibilidade com credencial "Prox" 125 kHz	HID Prox, Indala, EM4102, AWID	HID Prox
Entradas/Saídas	5 entradas & 2 saídas	5 entradas & 2 saídas
Embalagem: número de peças a instalar	2	1
Apenas acesso lateral seguro para bloquear a saída	Sim	Não

Módulos de interface Edge suportados

Os módulos de interface HID Edge (também conhecidos como *painéis de interface* e *subpainéis*) somente podem ser usados com controladores HID Edge EVO.

Clique no link para baixar o guia de instalação do produto.

- Módulo EDWM-M Door & Wiegand (Guia de Instalação)
- Módulo EDWM-M Door (Guia de Instalação)
- Módulo EDWM-M Wiegand (Guia de Instalação)
- Módulo de Entrada EIM-M (Guia de Instalação)
- Módulo de Trava ELM (Guia de Instalação)

Versões de firmware de HID suportadas

A Genetec Inc. recomenda uma versão de firmware específica para cada geração de controladores HID, antigos (legado) e novos (EVO). O uso de versões anteriores de firmware pode causar problemas com o sistema.

O Security Center funciona melhor quando os controladores HID executam as versões de firmware certificadas recomendadas.

Firmware suportado	Controladores Legacy	Controladores EVO
Firmware certificado recomendado	2.2.7.568	3.7.0.108
Firmware mínimo suportado	2.2.7.568	3.5.x

Versões anteriormente suportadas de firmware

Para saber mais sobre problemas com as versões de firmware previamente suportadas, consulte as *Notas de Versão do Security Center*.

Atualizar firmware HID EVO

Para atualizar as unidades HID EVO de uma versão de firmware anterior (2.3.1.603 ou 2.3.1.605 para Edge EVO e 2.3.1.542 ou 2.3.1.673 para VertX EVO) para a versão de firmware recomendada, os procedimentos de atualização específicos devem ser seguidos.

Tópicos relacionados

Atualizar firmware de unidade de controle de acesso na página 747

O que pode ser feito ou não instalação do hardware HID

Para sua segurança e para obter o melhor desempenho do seu equipamento, siga as instruções recomendadas de montagem e fiação.

Recomendações de montagem

- Os controladores e módulos de interface devem sempre ser montados em uma área protegida.
- Monte usando os quatro parafusos de montagem (fornecidos) ou outros parafusos apropriados. Coloque os parafusos nos orifícios de canto da base.
- Os dispositivos VertX podem ser empilhados com ou sem a tampa. Não remova a base de plástico. Certifique-se de posicionar os dispositivos VerteX de forma a proporcionar espaço para fiação, fluxo de ar e corrida de cabos.

Recomendações de fiação

CUIDADO: Os controladores VertX e os módulos de interface são sensíveis às descargas eletrostáticas (ESD). Tenha cuidado ao manusear o conjunto da placa de circuito usando correias de aterramento adequadas o tempo todo.

- Conexões de entrada de energia e alarme (todos os dispositivos VertX): conecte a energia fornecendo 12 VDC ao conector P7. +12 VDC vai para o Pino 1 e o aterramento para o Pino 2. Conecte as entradas *Falha de Bateria* e *Falha de AC* para os contatos de bateria fraca/falha e falha de AC. Conecte a entrada *Violação* a um interruptor de violação no gabinete.

  NOTA: Conecte a linha de retorno de dados ao mesmo aterramento que a alimentação do leitor se o leitor não for alimentado pelo 12 VDC do controlador VertX.
- O controlador VertX deve ter uma fonte de alimentação separada daquela do bloqueio mag e outros dispositivos, como o PIR (Sensor infravermelho passivo).
- A saída do relé deve ser protegida com um diodo. Em um controlador Edge com PoE, um relé não protegido pode fazer com que a unidade seja reiniciada ou entrar no modo somente leitura.
- Se a corrente de entrada com mag lock exceder as especificações, um circuito de amortecedor deve ser adicionado na saída do relé.
- Configure a entrada de violação em seu estado apropriado (NO/NC), mesmo que seja desabilitado.
- Para configurações com o mecanismo REX incorporado na alça da porta, recomenda-se aumentar o tempo de desbloqueio para o sensor da porta para evitar falsos eventos *A porta forçada para abrir*.
- O sensor da porta é, por padrão, configurado para NC e sem supervisão, enquanto todas as outras entradas são, por padrão, definidas como NO e sem supervisão (sem resistências EOL). Qualquer entrada pode ser configurada como NO ou NC, bem como supervisionada ou sem supervisão. Eles podem ser configurados para resistores de supervisão de 1 a 6 kΩ. As entradas supervisionadas devem ser configuradas no Security Center pelo Config Tool e enviadas para os módulos da interface VertX pelo Access Manager. A configuração de entrada supervisionada padrão é feita usando dois resistores EOL 2 kΩ.
- Por padrão, as portas se fecham novamente ao serem abertas. Para portas duplas, recomenda-se definir um tempo de ação mínimo no relé para mantê-lo ativo durante toda a duração do tempo de concessão.
- Um módulo de interface V300 dedicado ao controle do elevador só deve ser usado para o controle do elevador e não deve ser usado para disparar saídas não relacionadas ao elevador.

Recomendações de rede

- Recomenda-se configurar um endereço IP estático no controlador HID. O processo de descoberta é diferente para os controladores que possuem um endereço IP atribuído pelo DHCP. A descoberta para o endereço DHCP através de várias VLAN não é suportada. Se o Access Manager estiver em uma VLAN diferente do controlador HID, o endereço IP do controlador não pode ser atribuído pelo DCHP.
- Recomenda-se isolar o controlador de porta do tráfego broadcast ou multicast não tratado na rede.
- O número máximo de caracteres para o controlador deve ser 15 caracteres, sem espaços nem caracteres especiais.
- Todos os controladores HID têm o mesmo endereço IP 169.254.242.121 atribuído na fábrica. Você sempre pode fazer logon em uma unidade HID do seu computador usando um cabo de rede. O nome de usuário e senha de logon padrão para unidades Legacy são `root/pass`. O nome de usuário de logon padrão para unidades EVO é `admin` e a senha fica em branco, a menos que já esteja configurada.

Conexões do HID VertX V1000 RS-485

O controlador VertX V1000 possui dois barramentos seriais RS-485 com duas portas cada.

Os dois barramentos em série RS-485 são rotulados **P3** e **P4**. Cada barramento serial possui um conector de 10 pinos dividido em duas portas, rotuladas **Porta 1** e **Porta 2** no barramento **P3** e **Porta 3** e **Porta 4** no barramento **P4**. Ter duas portas em cada barramento oferece a opção de dividir cada barramento RS-485 em duas conexões físicas, permitindo um total de quatro conexões físicas.

Segue o que e o que não pode ser feito.

- Os módulos de interface devem ser conectados aos barramentos seriais RS-485 usando a topologia em cascata, e não a topologia em estrela.
- Use somente as portas de "entrada" nos módulos de interface. Isso elimina a possibilidade de muitos módulos de interface ficarem off-line, caso um módulo de interface tenha morrido ou perdido a potência.
- Finaliza de modo apropriado. O barramento serial RS485 precisa de um resistor de 120 Ω para "finalizar" as extremidades do loop de comunicação. Todos os dispositivos (incluindo o controlador V1000) possuem jumpers para isso.
- Os jumpers de terminação no V1000 devem estar na posição "Saída" se não houver módulos de interface conectados à porta. Se houver módulos de interface anexos, o jumper de terminação deve estar na posição "Entrada".
- Todos os módulos de interface, exceto as extremidades das cadeias seriais, devem ter seus jumpers de terminação na posição "Saída".
- O mostrador no módulo de interface indica seu endereço físico (padrão de fábrica = 0) ao controlador ao qual ele está anexado. Não duplique endereços no mesmo barramento serial.
- Recomenda-se ligar o RS-485 à posição do bloco de terminal **P9** do módulo de interface da série Vx00. Isto é especialmente importante quando a comunicação RS-485 está em uma configuração "em cascata". Se o RS-485 for ligado e desligado, e a energia for perdida, ou o bloco de terminais **P9** estiver desconectado em um módulo de interface da série Vx00, as comunicações RS-485 serão perdidas para os módulos de interface da série Vx00 seguintes.

Comportamento de E/S do HID VertX V1000

O seguinte se aplica às entradas e saídas do controlador HID VertX V1000:

- Por padrão, a entrada do monitor da porta está configurada como normalmente fechada (NC) e não supervisionada (sem resistores EOL). Como resultado, se nada estiver conectado à entrada do monitor da porta, a unidade emite sinais sonoros para indicar que a porta está aberta. Para corrigir isso, conecte a entrada do monitor da porta a um monitor de porta real ou reconfigure a entrada para normalmente aberta (NO).
- Todas as outras entradas são configuradas como normalmente abertas (NO), sem supervisão (sem resistências EOL).
- Não é recomendado usar as entradas e saídas do controlador HID VertX V1000 para requisitos especiais, tais como:
  - Uma porta: REX, sensor de porta, fechadura
  - Cancelar ou desativar intertravamento
  - Rastreamento de andar de elevador
  - Campainha da porta
  - vinculação de E/S (*zona de hardware*)

  Em vez disso, você deve usar as entradas e saídas dos subpainéis do V1000 (V200, V300) para esses fins.
- Todas as entradas não utilizadas (incluindo falha CA, falha da bateria e REX) podem ser usadas para outros fins, exceto as entradas *Adulteração* e *Monitor de porta*. Esses dois tipos de entradas só podem ser usados para o propósito especificado.
- Os estados dos relés de saída HID não podem ser mostrados na tarefa *Status do sistema*.

Considerações sobre conexão de E/S do HID

Sempre que uma alteração for feita na *vinculação de E/S* em uma unidade HID, uma tarefa interna (chamada IOLinker) deve ser reiniciada para levar em consideração a nova configuração. Quando isso acontece, todos os relés de saída controlados pela unidade estão configurados para o estado *Normal* por meio segundo antes de retornarem ao estado esperado. Esse comportamento pode causar interrupções temporárias na operação do seu sistema.

As seguintes ações aplicadas a entidades controladas por unidades HID podem fazer com que os relés de saída sejam redefinidos:

- Substituir os horários de desbloqueio de uma porta do Security Desk.
- Alterar os horários de desbloqueio atribuídos a uma porta.
- Alterar as exceções de programação de desbloqueio em uma porta.
- Configurar leitores em uma porta com horários de desbloqueio atribuídos.
- Alterar a opção de *Porta mantida aberta*de uma porta.
- Alterar a opção de *Porta forçada* de uma porta.
- Alterar as restrições de *Intertravamento* em uma área usando portas controladas por HID no seu perímetro.
- Configurando exceções aos horários operacionais de um andar de elevador.
- Configurando um evento para ação para acionar uma saída com base nas entradas de uma *zona de hardware* controlada pela mesma unidade HID.

Tópicos relacionados

Abas Configuração de portas na página 1005
Selecionar quem tem acesso a portas na página 619
Selecionar quem tem acesso a elevadores na página 628
Definição de configurações de área de hardware na página 945

LEDs de Alimentação e Com. do HID

As unidades HID são equipadas com 2 LEDs de status; uma é rotulada *Alimentação* e a outra é rotulada *Comu*. Você pode encontrar esses LEDs na placa dianteira para V1000 e V2000. Para dispositivos Edge e Edge Plus, os LEDs são encontrados na parte de baixo da unidade.

LEDs de alimentação e comunicação de V1000, V2000 e Leitor Edge

Indicador de LED	Estado	Descrição
Potência	Desligado	Verifique a tensão de entrada na unidade
	Vermelho contínuo	Sem atividade da rede
	Piscando (Vermelho/desligado)	Atividade da rede
Comu	Verde contínuo	Todas as interfaces encontradas (por ex. V100, V200, V300)
	Vermelho contínuo	Nenhuma interface encontrada
	Piscando (Vermelho/verde)	Algumas interfaces foram encontradas (o ciclo de trabalho muda de acordo com o número de interfaces encontradas).
	Piscando (Âmbar/verde)	A unidade está em modo "*Me localize*" (alguém clicou no botão *Identidade*).

Para unidades VertX V1000: se o indicador LED *Comu* estiver desativado, atualize o firmware para a interface (V100) parte da unidade.

Placas de interface VertX (subpainéis) V100, V200, V300

Indicador de LED	Estado	Descrição
Potência	Vermelho contínuo	OK
	Qualquer coisa diferente de vermelho sólido	Verificar tensão de entrada
Comu	Piscando (Vermelho/verde)	Atividade do barramento RS-485
	Alaranjado	Download do firmware em progresso

Se o indicador do LED *Comu* para um painel de interface estiver desligado, verifique a fiação do barramento RS-485. Em seguida, tente atualizar o firmware.

Recursos e modelos de HID suportados pelo Security Center

Esta seção lista os recursos de controle de acesso do Security Center que são suportados por cada modelo de unidade HID.

Opções do leitor de teclado compatível

A operação do cartão e do PIN depende do tipo de unidade e do leitor do teclado instalado.

Para leitores HID iCLASS e Prox, a opção *Definição de configuração do teclado* é selecionada no ato da compra. As opções suportadas incluem as seguintes:

- Opção 00: ""Opção de definição da configuração do teclado" de 00 = Buffer de uma tecla, sem paridade, mensagem de 4 bits.
- Opção 14: "Opção de definição da configuração do teclado" de 14 = Buffer de uma a cinco teclas (saída de 26 bits padrão). Essa opção de leitor também é conhecida como “Modo Galaxy”.

Tipo de unidade	Opção de leitor de teclado HID	Operação online	Operação offline	Observação
V1000 com V100 V2000 EdgePlus E400	Opção 14	Cartão ou PIN.	Cartão ou PIN.	Os leitores do teclado podem ser usados para registrar PINs.
	Opção 00	Cartão ou PIN. Cartão e PIN com agendamento. Quando fora de programação, a operação reverte para apenas cartão.		O leitor não pode ser usado para inscrever PINs para criação de credencial.
EdgeReader ER40 EdgeReader ERP40 EdgeReader ERW400	Essas unidades não podem ser encomendadas com um teclado.	Somente cartão.	Somente cartão.	—

Para os leitores de teclado HID SmartID (SK10), a seguinte opção é necessária para suportar a funcionalidade de cartão e PIN:

- Opção 02PIN-0000: "Código PIN Wiegand de 4 bits por tecla sem paridade".

Comprimento suportado do PIN

Como padrão, controladores HID somente aceitam números de PIN com até 5 dígitos de extensão. Você pode aumentar esse limite para 8 dígitos para leitores que usem o modo *Cartão e PIN* e para 15 dígitos para leitores que usem o modo *Cartão* ou *PIN*.

Leitores suportados

As unidades HID suportam a maioria dos leitores de cartões padrão da indústria que produzem dados de cartão usando o protocolo Wiegand (formatos de cartão até 128 bits).

Leitores HID SmartID (MIFARE e DESFire) também são suportados.

Leitores de inscrição USB RF Ideas suportados

Os leitores RF Ideas somente suportam formatos de dados de cartão até 64 bits. Os seguintes leitores de inscrição USB são suportados:

- Leitor pcProx HID USB para registrar cartões de proximidade
- Leitor AIR ID Enroll iCLASS ID # USB para inscrição de cartões HID iCLASS
- Leitor AIR ID Enroll 14443/15693 CSN USB para inscrição de um cartão MIFARE usando o CSN (número de série do cartão)

Suporte a Power over Ethernet (PoE)

As seguintes unidades Legacy e EVO suportam PoE (15.4W):

Tipo de unidade	Assistência
HID Legacy/EVO V1000	Não suportado
HID Legacy/EVO V2000	Não suportado
HID Legacy EdgeReader/EdgePlus	Suportado
HID EVO Edge	Suportado

Capacidade de titular de cartão e leitor suportados

O número de *titulares de cartão* (ou *credenciais*) que uma unidade pode suportar enquanto estiver offline é como segue:

Tipo de unidade	Número suportado de titulares de cartão
HID Legacy V1000 com V100	22.000, até 125.000 credenciais com atualização total de memória.
HID EVO V1000 com V100	65,000. Nenhuma atualização de memória é possível.
HID Legacy V2000	22.000, até 125.000 credenciais com atualização total de memória.
HID EVO V2000	65,000. Nenhuma atualização de memória é possível.
HID Legacy EdgeReader/EdgePlus	22.000 titulares (máximo). Nenhuma atualização de memória é possível.
HID EVO Edge	65,000. Nenhuma atualização de memória é possível.

O número de leitores que uma unidade pode suportar é como segue:

Tipo de unidade	Número suportado de leitores
HID Legacy/EVO V1000 com V100	64 leitores com 32 módulos de interface de leitor V100[1] 32 portas configuradas como card in/REX out 64 portas configuradas como card in/REX out
HID Legacy/EVO V2000	2 leitores 1 porta configurada como card in/REX out 2 portas configuradas como card in/REX out
HID Legacy EdgeReader/EdgePlus	1 leitores 1 porta configurada como card in/REX out
HID EVO Edge	2 leitores 1 porta configurada como card in/REX ou como card in/card out

[1] O HID indica que um controlador V1000 pode suportar um máximo de 32 módulos de interface a jusante (16 em cada bus serial RS-485) No entanto, os testes de desempenho executados pela Genetec Inc. indicam que, como "prática recomendada", não devem ser excedidos os 20 módulos de interface a jusante (10 por bus serial).

Habilitar suporte a PIN longos em unidades HID

Você pode habilitar o suporte de PIN longo (mais de 5 dígitos) em controladores HID (legacy e EVO) ao alterar um arquivo de configuração (gconfig) nos servidores que hospedam a função Access Manager.

O que você deve saber

Como padrão, controladores HID somente aceitam números de PIN com até 5 dígitos de extensão. Você pode aumentar esse limite para 8 dígitos para os leitores usando o modo Cartão e PIN e para 15 dígitos para leituras usando o modo Cartão ou PIN.

Para habilitar suporte a PIN longos em controladores HID:

1 Crie o arquivo *VertXConfig.gconfig* com o conteúdo a seguir:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <Vertx MaximumPinLength="nn"/>
</configuration>
```

onde nn o comprimento máximo do PIN em dígitos.

Se esse arquivo já existir, basta adicionar a tag `MaximumPinLength="nn"`.

2 Copie este arquivo para a pasta de instalação do Security Center em todos os servidores que hospedam a função Access Manager.

O padrão é *C:\Program Files (x86)\Genetec Security Center 5.x\ConfigurationFiles* em uma máquina de 64 bits.

Na próxima vez que você sincronizar uma unidade (controlador HID) com o Access Manager, a unidade aceitará números PIN até o comprimento máximo do PIN. Para cada credencial de PIN que seja maior do que o máximo especificado, uma mensagem de aviso será emitida durante a sincronização e o PIN não será sincronizado com a unidade.

Para sincronizar uma unidade:

1 Conecte ao Security Center com o Config Tool.

2 Abra a tarefa **Controle de acesso** e selecione a página **Funções e unidades**.

3 Selecione uma unidade (controlador HID), selecione **Sincronização** e, em seguida, clique em **Sincronizar agora**.

Configurações suportadas da unidade HID

Esta seção descreve as configurações da unidade de controle de acesso HID suportadas no Security Center.

Entradas gerais vs. dedicadas

Quando um controlador é usado para controlar uma porta, algumas entradas devem ser usadas apenas para o propósito pretendido (entradas dedicadas). Por exemplo, se uma porta tiver um sensor REX ou um sensor de porta, as entradas do controlador destinadas a esses sensores devem ser usadas.

Entrada	Quando usado como	Configuração exigida
Solicitação de saída	Sinal de entrada de solicitação de saída.	• Definir **desbloquear no REX** para Ligado na aba **Porta > Propriedades**para gerar eventos *Solicitação de saída* quando a entrada é acionada. Os eventos são registrados e podem ser usados para eventos para ações. • Atribua a entrada REX ao lado da porta na aba **Porta > Hardware** para programar o controlador para reagir à entrada REX soltando o bloqueio.
	Entrada de uso geral (para monitoramento de zona, por exemplo)	• Definir **desbloquear no REX** para Desligado na aba **Porta > Propriedades**. • Configure a entrada para uma zona, intertravamento etc.
Monitor da porta	Entrada de sensor de posição da porta (porta aberta ou porta fechada)	• Atribua esta entrada para **Sensor de porta** na aba **Porta > Hardware**. **NOTA:** Esta entrada não pode ser usada para nenhum outro fim.

Configuração da porta HID com leitores

Uma porta com um leitor atribuído a um dispositivo V2000, V100 ou Edge deve ter todas as entradas (por exemplo, contato da porta, REX) e saídas (por exemplo, bloqueio da porta) associadas a esse mesmo dispositivo. Entradas e saídas não devem ser distribuídas em vários dispositivos.

Configuração da porta HID com dois sensores de porta

Não é recomendado configurar uma porta com dois sensores de porta (ou contatos de porta) sem fiação física dos sensores em série. No Security Center, apenas um único sensor de porta deve ser configurado por porta.

Recursos do Security Center suportados por unidades HID

Esta seção lista os recursos padrão de controle de acesso do Security Center que as unidades HID suportam.

Porta sem leitor

Portas sem leitor (portas que usam um módulo de E/S para REX, estado da porta e bloqueio da porta somente) são suportadas quando a unidade está operando tanto online quanto offline.

Para que as portas sem leitura funcionem, é necessário o seguinte:

- As entradas de um HID VertX V1000 não devem ser usadas para este recurso.
- Todas as entradas e saídas devem pertencer ao mesmo controlador HID (um V2000 ou um Edge).

NOTA: Uma porta sem leitura não suporta o recurso de campainha.

Controle de porta

- **Cartão e PIN:** O modo de leitor de cartão e PIN é suportado se o leitor instalado o suportar.

  Para que o modo de leitor de cartão e PIN funcione, todas as interfaces/entradas/saídas do leitor para uma porta devem ser controladas pela mesma unidade HID (módulo de interface HID Edge, VertX V2000 ou VertX V100).
- **Tempo limite para digitação de PIN:** Suportado de acordo com a configuração por porta.
- **Tempo de concessão estendido:** Suportado de acordo com a configuração por porta.
- **Tempo de entrada (padrão e estendido):** Suportado de acordo com a configuração por porta.
- **Retravamento de porta:** A opção de rebloqueio na porta fechada não é suportada. Somente o bloqueio atrasado após a abertura da porta é suportado, e o atraso máximo é de 27 minutos.
- **Evento de porta mantida aberta e campainha:** Tanto o evento *Porta aberta por muito tempo* quanto a campainha do leitor são suportados conforme a configuração da porta.
- **Evento de porta forçada e campainha:** Tanto o evento *A porta forçada para abrir* quanto a campainha do leitor são suportados conforme a configuração da porta.
- **Requisição de saída (REX):** Todos os comportamentos de tratamento REX são suportados conforme a configuração da porta.
- **Desabilitação:** A desabilitação do leitor não é suportada. Somente entradas podem ser desabilitadas.

Contagem de pessoas

A contagem de pessoas é suportada apenas quando todas as unidades usadas para esse recurso estão conectadas ao mesmo Access Manager. No momento em que uma unidade atribuída a uma das portas perimetrais de uma área está desconectada, o recurso é desativado para toda a área.

Folga de segurança

O conceito de segurança não é suportado para áreas controladas por unidades HID.

Controle do elevador

Para que o controle do elevador funcione, é necessário o seguinte:

- Todos os módulos de interface utilizados para controle de elevador (HID VertX V100, V200 e V300) devem ser atribuídos ao mesmo VertX V1000. Leitor, entradas e saídas devem ser atribuídos ao mesmo V2000 (máximo de 4 andares) ou Edge (máximo de 2 andares).
- Todas as unidades usadas para este recurso devem ser atribuídas ao mesmo Access Manager.
- A interface do leitor, as entradas e as saídas devem estar conectadas ao mesmo controlador HID (VertX V1000, V2000 ou Edge). Um máximo de 1 leitor de cabine de elevador pode ser atribuído por controlador HID (VertX V1000, V2000 ou Edge).

NOTA: Se você planeja oferecer períodos de acesso controlado e acesso livre aos seus elevadores, entre em contato com seu representante da Genetec Inc. para obter um firmware personalizado para usar com as unidades que controlam os elevadores.

O uso de controladores HID VertX (V1000 e V2000) para controle de elevador está sujeito às seguintes limitações:

- Um controlador VertX deve ser dedicado ao controle de uma única cabine de elevador.
- Uma vez que um controlador VertX tenha sido designado para executar controle de elevador, ele só deve ser usado para esse propósito. O controle de porta e zona não deve ser misturado com controle de elevador, mesmo quando a unidade possui leitores, entradas e saídas não utilizados.
- Quando os andares de *elevador* funcionam no modo de acesso controlado, as agendas de diferentes *regras de acesso* aplicadas a diferentes andares são mescladas quando as regras são aplicadas ao mesmo titular de cartão.

  Exemplo: Bob tem acesso ao Andar-1 das 9:00 às 10:00 mediante a regra de acesso 1 e ao Andar-2 das 10:00 às 11:00 mediante a regra de acesso 2. Quando Bob apresenta o seu cartão no elevador, na realidade, o controlador VertX concede a Bob acesso a ambos os andares das 9:00 às 11:00.
- Os horários de desbloqueio não podem ser usados em elevadores controlados por unidades HID.

Rastreamento do andar do elevador

O rastreamento de andares é suportado apenas quando a unidade está online e quando todas as unidades usadas para esse recurso estão atribuídas ao mesmo Access Manager.

NOTA: O rastreamento de andar de elevador não é suportado quando a unidade está offline porque o relatório de eventos não está disponível. Os eventos não são regenerados quando a unidade se reconecta ao Security Center.

Recurso de antirretorno

O recurso de *anti-passback* é suportado quando a unidade está operando tanto online quanto offline.

Para que o antirretorno funcione, é necessário o seguinte:

- Use os controladores VertX V1000 (múltiplas áreas e portas múltiplas por área) ou VertX V2000 (área com uma porta única). Os produtos HID Edge não são suportados.
- Todas as unidades usadas para o antirretorno devem ser atribuídas ao mesmo Access Manager.
- O recurso de intertravamento deve estar desativado. Intertravamento (incluindo as funções de bloqueio e substituição) e antirretorno são mutuamente exclusivos; ambos os recursos não podem ser ativados para uma área ao mesmo tempo.

O antirretorno funciona melhor quando o sistema de controle de acesso foi configurado e o sistema está operacional e relativamente estático. Recomenda-se habilitar o anti-passback uma vez que as seguintes entidades tenham sido configuradas corretamente no Security Center e não sejam esperadas mudanças em uma base diária:

- Fusos horários de unidades
- Portas e leitores associados

- Áreas (grupos de portas)
- Elevadores e andares associados (inclusive agendamentos de desbloqueio)
- Grupos de titulares
- Agendamentos (incluindo agendamentos de cartão e PIN)
- Regras de acesso

A seção a seguir fornece diretrizes para configurar, habilitar e gerenciar antirretorno com controladores HID VertX (unidades):

- Você deve usar o V1000 ou V2000 para antirretorno.
  - V2000: O anti-passback é somente suportado para uma área com uma única porta com leitores de entrada e saída.
  - V1000: O anti-passback é suportado para várias áreas, com cada área suportando várias portas com leitores de entrada e saída. A limitação no número de portas é baseada no número de módulos V100 instalados.
- O antirretorno não é recomendado com a linha de produtos Edge pelos seguintes motivos:
  - Apenas um único leitor pode ser especificado para entrada ou saída (não em ambos), enquanto o antirretorno normalmente requer tanto leitores de entrada como de saída.
  - A comunicação ponto a ponto entre os dispositivos Edge não é suportada pelo Security Center.
- Uma área com antirretorno deve ser configurada para os leitores conectados e as portas gerenciadas pela mesma unidade (V1000 ou V2000) porque:
  - As funções antirretorno são tratadas pela unidade (V1000 ou V2000).
  - O Security Center não suporta comunicação ponto a ponto entre dispositivos VertX V1000 ou V2000.
- O antirretorno pode ser reiniciado usando os seguintes métodos:
  - Uma operação de sincronização de unidade
  - Uma ação (manualmente ou com um evento para ação)
- O seguinte comportamento do sistema irá redefinir o estado do antirretorno de uma unidade:
  - Sincronização inicial da unidade quando os serviços do Security Center são iniciados ou reiniciados.
  - Sincronização da unidade após a perda e recuperação de uma conexão com a unidade (V1000 ou V2000).
  - Sincronização da unidade após determinadas alterações de configuração (veja abaixo para mais detalhes).
  - Sincronização manual da unidade pela página do Config Tool.

Opções de antirretorno

As seguintes opções de antirretorno são suportadas:

- O antirretorno suave (evento de violação de retorno gerado e acesso concedido) só é suportado quando a unidade está online. O antirretorno suave não é suportado quando a unidade está offline porque o relatório de eventos não está disponível. Os eventos não são regenerados quando a unidade se reconecta ao Security Center.
- O antirretorno rígido (evento de violação de retorno gerado e acesso negado) é suportado quando a unidade está operando online ou offline.
- Antirretorno estrito (evento de violação de retorno quando um titular de cartão tenta sair de uma área à qual nunca recebeu acesso). Com unidades HID, antirretorno rígido e estrito são a mesma coisa. Não há distinção entre os dois.

- O antirretorno com agendamento é suportado quando a unidade está operando tanto online quanto offline.
- O antirretorno com agendamento não é suportado com o antirretorno rígido.

NOTA: A opção de antirretorno com tempo não é suportada:

Recurso de intertravamento

O recurso de intertravamento é suportado quando a unidade está operando tanto online quanto offline.

Para que o intertravamento funcione, é necessário o seguinte:

- O recurso de antirretorno deve estar desativado. O *intertravamento* (incluindo as funções de bloqueio e substituição) e o *anti-passback* são mutuamente exclusivos; ambos os recursos não podem ser ativados para uma área ao mesmo tempo.
- As entradas de um HID VertX V1000 não devem ser usadas para este recurso.
- Todas as portas perimetrais de uma área interligada devem ser atribuídas ao mesmo controlador HID (um VertX V1000 ou um V2000).

NOTA: Se uma porta perimetral de um intertravamento estiver aberta, quando um titular de cartão autorizado acessa uma segunda porta perimetral do mesmo intertravamento, um evento *Acesso concedido* para a segunda porta pode ser gerado, mesmo que a segunda porta não seja destravada.

Opções de intertravamento

As seguintes opções de intertravamento são suportadas quando a unidade está operando tanto online quanto offline:

- Trancamento
- Substituir

Regra de primeira pessoa a entrar

A regra de primeira pessoa a entrar não é suportada pelas unidades HID.

Regra de duas pessoas

A regra de duas pessoas não é suportada pelas unidades HID.

Regra de acompanhante de visitante

A regra de acompanhamento de visitante não é suportada pelas unidades HID.

Eventos para ação

O evento para ação é suportado quando a unidade está operando online e offline, com limitações.

- **Eventos causa-efeito com a ação Disparar saída:** O tipo de ação *Disparar saída* pode ser usado em eventos causa-efeito quando a unidade está online e é parcialmente suportado quando a unidade está offline. Para que o tipo de ação *Disparar saída* funcione, todas as unidades usadas para esse recurso devem ser atribuídas ao mesmo Access Manager.
- **Eventos causa-efeito com ações Silenciar alarme ou Alarme de som:** Os tipos de ações *Silenciar alarme* e *Alarme de som* podem ser usados em eventos causa-efeito quando a unidade está operando tanto online quanto offline. Para que essas ações funcionem, todas as entradas e saídas devem pertencer ao mesmo controlador HID (VertX V1000, um V2000 ou um Edge).

  NOTA: O recurso *Ação* não está disponível em portas sem leitor.

- **Os eventos de Acesso concedido não são suportados quando a unidade está offline.:** Eventos causa-efeito baseados no evento *Acesso concedido* não funcionam quando a unidade é desconectada do Gestor de Acesso.

Ligação de E/S

O recurso de Ligação de E/S é suportado quando a unidade está operando tanto online quanto offline, com as seguintes limitações.

- As entradas de um HID VertX V1000 não devem ser usadas para este recurso.
- Todas as entradas e saídas devem ser controladas pelo mesmo controlador HID.
- Apenas a ação *Disparar saída* é suportada quando a unidade está operando offline.

Tópicos relacionados

Recursos e modelos de HID suportados pelo Security Center na página 1163

D

Recurso de múltiplas leituras

Esta seção inclui os seguintes tópicos:

- "Sobre o recurso de múltiplas leituras" na página 1174
- "Implementando o recurso de múltiplas leituras" na página 1175

Sobre o recurso de múltiplas leituras

O recurso de múltiplas leituras permite que os titulares de cartão apresentem suas credenciais várias vezes em uma porta para gerar um evento personalizado. Este evento pode então ser usado para desencadear uma ação por meio de um *evento de causa-efeito*.

A macro MultiSwipe

A macro MultiSwipe permite que um grupo específico de titulares de cartão gere dois eventos personalizados distintos ao apresentar suas credenciais um determinado número de vezes na porta, dentro do intervalo prescrito. N leituras geram o primeiro evento personalizado, e N+1 leituras geram o segundo evento personalizado. Todos os titulares de cartão no grupo designado devem ter acesso à porta.

A macro MultiSwipe é fornecida com o software do Security Center para ajudá-lo a implementar este recurso.

Implementando o recurso de múltiplas leituras

Você pode implementar o recurso de leituras múltiplas usando a macro fornecida com o software do Security Center.

Antes de iniciar

Você precisa criar as seguintes entidades para implementar o recurso de leituras múltiplas:

- Uma porta equipada com um leitor, para ser usada para o recurso de leituras múltiplas.
- Um grupo de titulares de cartões autorizado para usar o recurso de leituras múltiplas. Todos os membros deste grupo devem ter acesso à porta designada.
- Dois eventos personalizados: um primeiro a ser gerado quando um titular de cartão autorizado passa N vezes na porta, e um segundo para ser gerado quando o titular do cartão passa N + 1 vezes.
- Um agendamento que define quando o recurso de múltiplas leituras está disponível.

O que você deve saber

Todas as macros fornecidas com o software Security Center são encontradas na pasta *Add-On\Macros* na pasta de instalação do Security Center(padrão=*C:\Program Files (x86)\Genetec Security Center 5.7*).

Para implementar o recurso de múltiplas leituras em uma porta:

1 Crie uma macro e nomeie-a como *Múltiplas leituras em* <*Porta*>, em que <*Porta*> é o nome da porta onde o recurso de múltiplas leituras está ativado.

Em vez de uma porta, você também pode selecionar uma área. Neste caso, o recurso de múltiplas leituras é habilitado em todas as portas da área.

2 Selecione a aba **Propriedades**, clique em **Importar do arquivo**, selecione *MultiSwipe.cs* e clique em **Abrir**.

3 Clique em **Verificar sintaxe**, em seguida clique em **Fechar** e então clique em **Aplicar**.

4 Selecione a aba **Contexto de execução padrão** e ajuste as seguintes propriedades.

- **CardholderGroup:** Grupo de titulares de cartões autorizado para usar o recurso de leituras múltiplas.
- **DoorOrArea:** Porta ou área para a qual o recurso de múltiplas leituras está sendo ativado.
- **DelayInSecondsBetweenEachSwipe:** O atraso máximo em segundos entre duas leituras consecutivas do mesmo titular de cartão autorizado para que a leitura seja considerada como parte da ação de múltiplas leituras.
- **NumberOfSwipes:** Número de leituras (N) para gerar o primeiro evento personalizado.
- **NSwipesCustomEventId:** Valor atribuído ao primeiro evento personalizado. Observe que o primeiro evento personalizado só é gerado *n* segundos após a última leitura, *n* sendo o atraso máximo em segundos entre duas leituras consecutivas.
- **Np1SwipesCustomEventId:** Valor atribuído ao segundo evento personalizado. Observe que o segundo evento personalizado é gerado imediatamente após N+1 leituras.
- **Cronograma:** Agendamento durante o qual o recurso de múltiplas leituras está em vigor.

5 Clique em **Aplicar**.

6 Crie uma tarefa agendada e nomeie-a como *RunMultiSwipe-OnStartup*.

7 Selecione a aba **Propriedades**, e configure suas propriedades como segue.

- **Status:** Configure o status como ON.
- **Recorrência:** Defina a recorrência como **Na inicialização**.
- **Ação:** Selecione **Executar uma macro** e defina **Macro** para a macro que acabou de criar.

8 Clique em **Aplicar**.

Isso garante que a macro de múltiplas leituras esteja sempre em execução, mesmo após o reinício do sistema.

9 Crie um evento causa-efeito para vincular o primeiro evento personalizado à ação desejada.

Exemplo: Substitua temporariamente a programação de desbloqueio, arme uma zona e assim por diante.

10 Crie um evento causa-efeito para vincular o segundo evento personalizado à ação desejada.

Exemplo: Cancelar temporariamente a substituição de agendamento de desbloqueio, desarmar uma zona e assim por diante.

Glossário

A

ação
É uma função programável pelo usuário que pode ser disparada como uma resposta automática a um evento, como porta aberta por muito tempo ou objeto desacompanhado ou que pode ser executada de acordo com um cronograma específico.

alarme ativo
Um alarme ativo é aquele que ainda não foi reconhecido.

autenticação ativa
Autenticação ativa é quando o aplicativo cliente captura as credenciais do usuário e as envia através de um canal seguro para um provedor de identidade confiável para autenticação.

add-on
Um add-on é um pacote de software que adiciona tarefas, ferramentas ou definições específicas de configurações para os sistemas Security Center.

Active Directory Federation Service
Serviços de Federação do Active directory (ADFS) é um componente do sistema operacional Microsoft® Windows® que emite e transforma reclamações, e implementa entidades federadas. É também um tipo de função que permite que o Security Center receba reclamações de um servidor externo do ADFS.

Advanced Systems Format - Formato de Sistemas Avançados
O Advanced Systems Format (ASF) é um formato de stream de vídeo da Microsoft. O formato ASF pode apenas ser reproduzido em reprodutores de mídia que suportam este formato, como o Windows Media Player.

agente
É um subprocesso criado por uma função do Centro de Segurança para executar simultaneamente vários servidores para compartilhar sua carga.

alarme
Um alarme é um tipo de entidade que descreve uma situação de problema particular que requer atenção imediata e como pode ser tratada no Security Center. Por exemplo, um alarme pode indicar quais entidades (geralmente câmeras e portas) melhor descrevem, quem deve ser notificado, como deve ser exibido para o usuário, etc.

Alarmes
A tarefa *Alarmes* é uma tarefas de administração que o permite configurar grupos de monitoramento de alarmes.

anti-retorno
O antirretorno é uma restrição de acesso colocada em uma área protegida que evita que um titular de cartão entre em uma área de onde ainda não saiu e vice-versa.

Archiver	A função Archiver é responsável pelo descobrimento, escolha de status e controle das unidades de vídeo. O Archiver também gerencia o arquivo de vídeo e realiza detecção de movimento quando não for feito na própria unidade.
Arquivos	É um tipo de tarefa de investigação que permite encontrar e visualizar arquivos de vídeo disponíveis por câmera e período.
Atividades da área	É um tipo de tarefa de investigação que relata os eventos do controle de acesso pertinentes às áreas selecionadas.
ativo	É um tipo de entidade que representa qualquer objeto de valor com uma etiqueta RFID, permitindo assim ser rastreada por um software de gestão de bens.
autenticação	O processo de verificação de que uma entidade é o que afirma ser. A entidade pode ser um usuário, um servidor ou um aplicativo cliente.
autorização	O processo de estabelecimento dos direitos que uma entidade tem sobre as características e os recursos de um sistema.
AutoVu™	Security Center AutoVu™ é o sistema de reconhecimento automático de placas de veículo (ALPR) que automatiza a leitura e a identificação de placas de veículo. Implantado em instalações fixas e móveis, permite estender a sua segurança física aos seus estacionamentos e perímetros, para que você esteja sempre ciente dos veículos que entram e saem das suas instalações.
Archiver auxiliar	A função Archiver auxiliar complementa o arquivo de vídeo produzido pela função Archiver. Ao contrário da função Archiver, a função Archiver auxiliar não está vinculada a nenhuma *porta de descoberta* particular, portanto, ela pode arquivar qualquer câmera no sistema, incluindo câmeras federadas de outros sistemas do Security Center. A função Archiver auxiliar não pode operar de forma independente; ela necessita da função Archiver para comunicar com unidades de vídeo.
Atividades do titular de cartão	É um tipo de tarefa de investigação que reporta as atividades do titular do cartão, como acesso negado, primeira pessoa a entrar, última pessoa a sair, violação antipassback, etc.
autoridade de certificação	Uma autoridade de certificação ou autoridade de certificado (AC) é uma entidade ou organização que assina certificados de identidade e atesta a validade do seu conteúdo.
Autenticação com base em reivindicações	A autenticação baseada em reivindicações é o processo de autenticação de um usuário com base em um conjunto de reivindicações sobre sua identidade contidas em um token confiável. Esse token é freqüentemente emitido e assinado por uma entidade que é capaz de autenticar o usuário por outros

	meios e que é confiável pela entidade que faz a autenticação baseada em reivindicações.
Atividades da credencial	É um tipo de tarefa de investigação que reporta as atividades relacionadas à credencial, como acesso negado por credencial vencida, inativa, perdida ou roubada, etc.
atraso padrão da expiração	O atraso padrão da expiração é usado para autorizações fornecidas pelo Pay-by-Plate Sync que não incluem uma expiração. Neste caso, o AutoVu™ Free-Flow verifica junto do provedor de autorização de estacionamento se a autorização permanece válida. Aumentar este valor reduz a frequência das verificações de autorização. Por exemplo, se o estacionamento for cobrado em incrementos de 15 minutos e você também definir o atraso padrão da expiração para 15 minutos, o sistema valida a autorização junto do provedor de estacionamento a cada 15 minutos.
Autenticação do Directory	A autenticação do Directory é uma opção do Security Center que força todas as aplicações do cliente e do servidor em determinada máquina a validar o certificado de identidade do Directory antes de se conectar a ele. Esta medida impede ataques man-in-the-middle.
Atividades da porta	É um tipo de tarefa de investigação que reporta as atividades relacionadas à porta, como acesso negado, abertura forçada, porta aberta por muito tempo, falsificação de hardware, etc.
Atividades de elevador	É um tipo de tarefa de investigação que reporta as atividades relacionadas ao elevador, como acesso negado, andar acessado, a unidade está desligada, falsificação de hardware, etc.
acesso livre	É um estado de ponto de acesso onde não é necessário apresentar as credenciais para entrar de uma área segura. A porta não é bloqueada. Normalmente, é usado durante as horas comerciais normais, como medida temporária durante manutenção ou quando o sistema de controle de acesso é ligado pela primeira vez e ainda precisa ser configurado.
anti-passback global	Anti-passback global é um recurso que estende as restrições de anti-passback a áreas controladas por várias unidades Synergis™.
Alta disponibilidade	A alta disponibilidade é uma abordagem que permite que um sistema funcione em um nível operacional mais alto que o normal. Muitas vezes, isso envolve failover e balanceamento de carga.
alerta	Uma ocorrência é uma leitura de placa de veículo que corresponde a uma regra de ocorrências, como uma lista de procurados, autorização ou restrição de autorização. Um usuário do Genetec Patroller™ pode rejeitar ou aceitar uma

	ocorrência. Um ocorrência aceita pode ser posteriormente imposta.
ação instantânea	É uma ação mapeada a uma tecla de função do teclado do PC (Ctrl+F1 até Ctrl+F12) no Security Desk para acesso rápido.
Atividades de área de detecção de intrusão	*Atividades de área de detecção* de intrusão é um tipo de tarefa de investigação que relata as atividades (armação principal, armação do período, pressão, etc.) nas áreas de detecção de invasão selecionadas.
Aplicação da lei	Aplicação da lei é uma instalação de software do Genetec Patroller™ que está configurada para fiscalizar a lei: a correspondência entre leituras de placas de veículo e listas de placas de veículo procuradas (listas de procurados). O uso de mapas é opcional.
armamento mestre	O armamento mestre é armar uma área de detecção de intrusão de modo que todos os sensores atribuídos à área disparem o alarme se um deles for disparado.
arquivo ausente	Um arquivo ausente é um arquivo de vídeo que ainda é referenciado por um banco de dados designado do Archiver, mas que não pode mais ser acessado. Esta situação ocorre se os ficheiros de vídeo forem apagados manualmente sem usar a tarefa *Detalhes de armazenamento de arquivos*, criando uma incompatibilidade entre o número de arquivo de vídeo referenciados no banco de dados e o número real de arquivos de vídeo no disco.
Admin Móvel	É uma ferramenta de administração na Web usada para configurar o servidor móvel.
Aplicativo móvel	É o componente do cliente do Centro de Segurança Móvel instalado nos dispositivos móveis. Os usuários do aplicativo móvel se conectam ao Servidor Móvel para receber alarmes, visualizar streams vídeo ao vivo, visualizar o status das portas e, muito mais, do Centro de Segurança.
autenticação multifator	A autenticação multifator (MFA) é um sistema de segurança que exige mais de um método de autenticação por categorias independentes de credenciais para verificar a identidade do usuário no login ou em outra transação.
arquivo órfão	Um arquivo órfão é um arquivo de vídeo que não é mais referenciado por qualquer banco de dados de arquivos. Os arquivos órfãos permanecem no disco até serem manualmente excluídos. Essa situação ocorre quando o banco de dados de arquivos é alterado inadvertidamente, criando uma incompatibilidade entre o número de arquivos de vídeo referenciado no banco de dados e o número real de arquivos de vídeo armazenados no disco.

Atividades da zona de estacionamento	A tarefa *Atividades da zona de estacionamento* é um tipo de tarefa de investigação que permite controlar os eventos relacionados à zona de estacionamento que ocorrem entre os momentos em que a placa do veículo é lida na entrada e na saída da zona de estacionamento.
administrador de partição	(Obsoleto) A partir do Security Center 5.7 GA, os privilégios que costumavam ser exclusivos de administradores podem agora ser concedidos individualmente, tornando obsoleto o conceito de *administrador de partição*.
autenticação passiva	Autenticação passiva (também chamada autenticação baseada na Web) é quando o aplicativo cliente redireciona o usuário para um formulário Web gerido por um provedor de identidade confiável. O provedor de identidade pode solicitar qualquer número de credenciais (senhas, tokens de segurança, verificações biométricas e assim por diante) para criar uma defesa multicamada contra acesso não autorizado. Isto também é conhecido como autenticação multifator.
armamento do perímetro	Ela arma uma área de detecção de invasão de um modo que somente os sensores atribuídos compensariam o alarme se um deles fosse disparado. Outros sensores, como o de movimento dentro da área, são ignorados.
autorização	Uma autorização é um tipo de entidade que define uma lista única de detentores de autorização de estacionamento. Cada detentor de autorização é caracterizado por uma categoria (zona de autorização), um número de placa de licença, um estado emissor da licença e, opcionalmente, um período de validade da autorização (data de entrada em vigor e data de expiração). As autorizações são usadas na fiscalização de estacionamento tanto municipal quanto universitário.
agente redirecionador	É um agente criado pela função de Roteador de Mídia para redirecionar os streams de dados de um ponto final de IP para outro.
arquivamento redundante	É uma opção que permite uma cópia de todos os streams de vídeo da função de um Archiver para ser arquivado simultaneamente no servidor de reserva como uma proteção contra perda de dados.
agenda	Uma agenda é um tipo de entidade que define um conjunto de restrições de tempo que pode ser aplicado a várias situações no sistema. Cada restrição de tempo é definida por uma cobertura de datas (diária, semanal, ordinal ou específica) e uma cobertura de horário (todo o dia, intervalo fixo, durante o dia e durante a noite).
antipassback estrito	É uma opção de antipassback. Quando habilitado, um evento de passagem de volta (passback) é gerado quando um titular de cartão tenta sair de uma área onde ele nunca teve acesso

	concedido. Quando desabilitado, o Centro de Segurança gera somente eventos de passback para titulares de cartão que entram em uma área de onde nunca saíram.
anti-passback programado	Anti-passback programado é uma opção de anti-passback. Quando o Security Center considera que um titular de cartão já está em uma área, é gerado um evento de passback quando o titular de cartão tenta acessar novamente a mesma área durante o retardo de tempo definido pelo *Tempo limite de presença*. Quando o retardo de tempo tiver expirado, o titular de cartão pode passar novamente para a área sem gerar um evento de passback.
agendamento vespertino	É um tipo de entidade de agendamento que suporta coberturas durante o dia e a noite. Esse cronograma não pode ser usado em todas as situações. Sua utilidade principal é controlar comportamentos relacionados a vídeo.
análise de vídeo	É uma tecnologia por software usada para analisar o vídeo quanto a informações específicas sobre seu conteúdo. Exemplos de análise de vídeo incluem contar o número de pessoas que cruzam uma linha, detecção de objetos abandonados ou o a direção na qual as pessoas andam ou correm.
arquivo de vídeo	Um arquivo de vídeo é uma coleção de transmissões de vídeo, áudio e metadados gerida por uma tarefa de Archiver ou Archiver auxiliar. Estas coleções são catalogadas no banco de dados de arquivos, que inclui eventos de câmera vinculados às gravações.
arquivo de vídeo	É um arquivo criado por uma função de arquivamento (Archiver ou Auxiliary Archiver) para guardar vídeos arquivados. A extensão do arquivo é G64 ou G64x. É preciso ter o Security Desk ou o Genetec Video Player para visualizar os arquivos de vídeo.
Atividades do visitante	É um tipo de tarefa de investigação que reporta as atividades do visitante, como acesso negado, primeira pessoa a entrar, última pessoa a sair, violação antipassback, etc.
Atividades da zona	É um tipo de tarefa de investigação que relata as atividades relacionadas à zona (zona em que está armado, zona desarmada, trava liberada, trava protegida, etc.).

B

bloqueio de câmera	Bloqueio de câmera é um recurso do Omnicast™ que permite restringir a visualização do vídeo (ao vivo ou de reprodução) de certas câmeras a usuários com um nível mínimo de usuário.
bairro	Um bairro é um tipo de regulamentação de estacionamento que caracteriza uma regra de tempo extra. Um bairro é uma

	área geográfica dentro de uma cidade. Um veículo está em violação se for visto dentro dos limites do bairro por um período específico de tempo.
balanceamento de carga	É a distribuição da carga de trabalho em vários computadores.
bandeja de notificação	A bandeja contém ícones que permitem o rápido acesso a certos recursos do sistema e também exibe indicadores para eventos do sistema e informação de status. As configurações de exibição são salvas como parte do seu perfil de usuário e se aplicam ao Security Desk e à Config Tool.
barra de tarefas	É um elemento da interface do usuário da janela do aplicativo do cliente do Centro de Segurança, composto pela guia Inicial e pela lista de tarefas ativas. A barra de ferramentas pode ser configurada para aparecer em qualquer borda da janela do aplicativo.
Body-Worn Camera Manager	Body-Worn Camera Manager é a função usada para configurar e gerenciar câmeras usadas junto ao corpo no Security Center. Isto inclui configurar câmeras ou estações de câmeras, adicionar usuários, carregar conteúdo para um Archiver e definir o período de retenção de evidências carregadas.

C

Controle de acesso	A tarefa *Controle de acesso* é uma tarefa de administração que permite configurar funções, unidades, titulares de cartão, credenciais de controle de acesso e entidades e configurações relacionadas.
Configuração de regra de acesso	É um tipo de tarefa de manutenção que reporta as entidades e os pontos de acesso afetados por determinada regra de acesso.
câmera usada junto ao corpo	Uma câmera usada junto ao corpo (BWC), também conhecida como câmera corporal, é um sistema de gravação de vídeo tipicamente usado por agentes da lei para gravar suas interações com o público ou coletar evidências em vídeo de cenários de crime.
Caixa de derivação	A caixa de derivação é uma caixa de conexão patenteada da Genetec Inc. para soluções móveis AutoVu™ que usem câmeras Sharp. A caixa de derivação fornece energia e ligação de rede às unidades Sharp e ao computador de bordo.
câmera	Uma entidade de câmera representa uma única fonte de vídeo no sistema. Essa fonte pode ser uma câmera IP ou uma câmera analógica que esteja conectada ao decodificador de vídeo de uma unidade de vídeo. Vários streams de vídeo podem ser gerados a partir da mesma fonte de vídeo.

Configuração de câmera	É um tipo de tarefa de manutenção que relata as propriedades e as configurações das câmeras locais no seu sistema (fabricante, resolução, taxa de quadro, uso de fluxo, etc.)
Cartão e PIN	É um modo de ponto de acesso que exige que o titular apresente seu cartão e digite o número de identificação pessoal (PIN).
Configuração do titular do cartão	É um tipo de tarefa de manutenção que reporta as propriedades do titular do cartão, como nome, sobrenome foto, status, propriedades personalizadas, etc.
certificado	Designa uma das seguintes opções: (1) *certificado digital*; (2) *certificado SDK*.
Cloud Archives	Cloud Archives é um serviço da Genetec Inc. que permite às organizações manter gravações de vídeo na nuvem enquanto continuam a potencializar o seu sistema Security Center existente.
Config Tool	Config Tool é um aplicativo administrativo do Security Center usado para gerenciar todos os usuários do Security Center e configurar todas as entidades do Security Center, como áreas, câmeras, portas, agendas, titulares de cartão, veículos de patrulha/unidades de LPR e dispositivos de hardware.
câmera de contexto	Uma câmera de contexto é uma câmera ligada a uma Unidade de LPR que produz uma imagem colorida com ângulo mais amplo do veículo cuja placa foi lida por uma Câmera de LPR.
credencial	É um tipo de entidade que representa um cartão de proximidade, um modelo biométrico ou um PIN necessário para obter acesso a uma área protegida. Uma credencial pode ser atribuída a apenas um titular de cartão de cada vez.
código da credencial	É uma representação textual da credencial, normalmente indicando o código da Instalação e o número do Cartão. Para credenciais usando os formatos de cartão personalizados, o usuário pode escolher o que incluir no código.
Configuração da credencial	É um tipo de tarefa de manutenção que reporta as propriedades de credencial, como status, titular atribuído, formato do cartão, código da credencial, propriedades personalizadas, etc.
campo personalizado	É uma propriedade definida pelo usuário que está associada a um tipo de entidade e é usada para armazenar informações adicionais que são úteis para sua organização.
certificado digital	Um certificado digital, também chamado de *certificado de identidade* ou *certificado de criptografia*, é um "passaporte" eletrônico que permite que uma pessoa, computador ou organização troquem informações de modo seguro na Internet usando uma infraestrutura de chave pública (PKI).

contato da porta Um contato da porta monitora o estado de uma porta, se está aberta ou fechada. Também pode ser usada para detectar um estado impróprio, como porta aberta por muito tempo.

curso da porta elétrica É um dispositivo elétrico que libera a trava da porta quando a corrente é aplicada.

certificado de criptografia Um certificado de criptografia, também chamado de *certificado digital* ou *certificado de chave pública*, é um documento eletrônico que contém um par de chaves pública e privada usadas no Security Center para *criptografia de transmissão de fusão*. Informações criptografadas com a *chave pública* somente podem ser decodificadas com a *chave privada* correspondente.

criptografia de fluxo de fusão A criptografia de fluxo de fusão é uma tecnologia proprietária da Genetec Inc. usada para proteger a privacidade de seus arquivos de vídeo. O Archiver usa uma estratégia de criptografia de dois níveis para garantir que somente as máquinas cliente autorizadas possam acessar seus dados privados.

câmera fantasma Um câmera fantasma é uma entidade usada como câmera substituta. Esta entidade é criada automaticamente pelo Archiver quando arquivos de vídeos são detectados para uma câmera cuja definição tenha sido excluída do Directory, seja por acidente ou porque o dispositivo físico não existe mais. As câmeras fantasmas não podem ser configuradas e existem somente para que os usuários possam consultar o arquivo de vídeos que, de outro modo, não estaria associadas a nenhuma câmera.

certificado de identidade Um certificado de identidade, também conhecido como *certificado digital* ou *certificado de chave pública*, é um documento digitalmente assinado que permite que um computador ou organização troquem informações de modo seguro em uma rede pública. O certificado inclui informações sobre a identidade do proprietário, a *chave pública* usada para criptografar futuras mensagens enviadas ao proprietário e a assinatura digital da autoridade de certificação (CA).

categoria do incidente Uma categoria de incidente é um tipo de entidade que representa um agrupamento de tipos de incidentes com características similares.

Configuração de incidente A tarefa *Configuração de incidente* é a tarefa administrativa que pode ser usada para configurar tipos de incidentes, categorias de incidentes e os documentos de apoio para o Mission Control. É possível também usar essa tarefa para gerar relatórios sobre as alterações feitas nos tipos de incidentes.

Configuração de I/O	É um tipo de tarefa de manutenção que relata as configurações de E/S (pontos de acesso controlados, portas e elevadores) das unidades de controle de acesso.
Câmera IP	Uma câmera IP é uma unidade de codificação de vídeo que incorpora uma câmera.
chave de licença	É a chave do software usada para desbloquear o software do Centro de Segurança. A chave é gerada especificamente para cada computador onde a função de Diretório está instalada. Para obter sua chave de licença, é preciso ter o *ID do sistema* (que identifica seu sistema) e a *Chave de validação* (que identifica seu computador).
Câmera de LPR	Uma câmera de Reconhecimento de placas de veículos (LPR) é uma câmera conectada a uma unidade de LPR que produz imagens ampliadas em alta resolução de placas de veículo.
Contexto de LPR	Um contexto de LPR é uma otimização do LPR que aprimora o desempenho do reconhecimento de placas de veículos para placas de veículos de uma região específica (por exemplo, Nova York) ou de um grupo de regiões (por exemplo, estados do Nordeste).
captura manual	A captura manual ocorre quando informações de placas de veículo são introduzidas no sistema por um usuário e não pelo LPR.
credencial móvel	É uma credencial em um smartphone que utiliza tecnologia Bluetooth ou de Leitor de Comunicação de Campo Próximo (NFC) para acessar áreas protegidas.
Computador de dados portátil	Computador de dados portátil é um Tablet PC ou um laptop reforçado usado em veículos de patrulha para executar o aplicativo Genetec Patroller™. O computador de dados portátil geralmente possui uma tela sensível ao toque com uma resolução mínima de 800x600 pixels e recurso de rede sem fio.
comportamento de saída	É um tipo de entidade que define um formato de sinal de saída personalizado, como um pulso com atraso e duração.
capacidade da zona de estacionamento	A capacidade da zona de estacionamento é o número máximo de veículos que podem ser estacionados em uma zona de estacionamento.
Contagem de pessoas	É um tipo de tarefa de operação que permite contar em tempo real o número de titulares do cartão em todas as áreas protegidas do seu sistema.
chave privada	Em criptografia, uma chave privada ou secreta é uma chave de encriptação/decodificação da qual se conhece apenas uma das partes para trocar mensagens secretas.

chave pública
Na criptografia, uma chave pública é um valor fornecido por uma autoridade designada como uma chave de criptografia que, combinada com uma chave privada gerada ao mesmo tempo, pode ser usada para criptografar mensagens e verificar as assinaturas digitais de modo eficaz.

criptografia por chave pública
A criptografia por chave pública, conhecida como *criptografia assimétrica*, é um tipo de criptografia em que duas chaves diferentes são usadas para criptografar e descriptografar informações. A chave privada é uma chave que é conhecida apenas para seu proprietário, enquanto a chave pública pode ser disponibilizada a entidades conhecidas e outros na rede. O que é criptografado com uma chave só pode ser descriptografado com a outra chave.

câmera restrita
Câmeras restritas são câmeras que o Genetec Inc. identificou como perigos de segurança cibernética.

Certificado SDK
Um certificado SDK permite que um aplicativo (ou plug-in) SDK se conecte ao Security Center. O certificado deve estar incluso na chave de licença do Security Center para que a aplicação SDK funcione.

certificado de segurança
Um certificado de segurança é um valor numérico usado para restringir o acesso a uma área quando um nível de ameaça está em vigor. Os titulares de cartão somente podem entrar em uma área se o certificado de segurança deles for igual ou superior ao certificado de segurança mínimo estabelecido para a área.

certificado auto-assinado
Um certificado auto-assinado é um certificado de identidade assinado pela mesma entidade cuja identidade certifica.

compartilhando visitante
Um convidado de compartilhamento é um sistema do Security Center que possui os direitos para visualizar e modificar entidades pertencentes a outro sistema do Security System, chamado anfitrião de compartilhamento. O compartilhamento é realizado ao colocar as entidades em uma partição global.

cronograma padrão
É um tipo de entidade de cronograma que pode ser usado em todas as situações. Sua única limitação é que não suporta cobertura durante o dia ou durante a noite.

criptografia simétrica
A criptografia simétrica de um tipo de criptografia onde a mesma chave é usada para criptografar e descriptografar.

carona
Ato de entrar em uma área protegida sem apresentar uma credencial, ao seguir outra pessoa que apresentou a sua.

ciclo de tarefas
É um recurso do Security Desk que faz o ciclo automaticamente de todas as tarefas na lista de tarefas ativas, seguindo um tempo de permanência fixo.

cronograma desbloqueado Cronograma que define os períodos em quando o acesso livre é cedido por um ponto de acesso (lateral da porta ou andar do elevador).

chave de validação É um número de série exclusivo que identifica um computador que deve ser dado para obter a chave da licença.

Cofre Cofre é uma ferramenta que exibe seus instantâneos salvos e arquivos de vídeo G64, G64x e GEK (criptografado) exportados. No Cofre, você pode visualizar os arquivos de vídeo, criptografar ou decodificar arquivos, converter arquivos para ASF ou compactar arquivos com o Genetec Video Player.

codificador de vídeo É um dispositivo que converte uma fonte de vídeo analógico para digital, usando um algoritmo de compressão padrão, como H.264, MPEG-4, MPEG-2, ou M-JPEG. O decodificador é um dos vários dispositivos encontrados em uma unidade de decodificação de vídeo.

certificado X.509 A verificação de identidade, a criptografia assimétrica e a segurança dos dados em trânsito são todas habilitadas por certificados X.509, que são compostos pela identidade de um usuário ou computador e por uma chave pública. Os certificados X.509 são a base do protocolo HTTPS.

D

direito de acesso É um direito básico que os usuários devem ter sobre qualquer parte do sistema antes de poder fazer algo. Outros direitos, como visualização e modificação de configuração da entidade, são cedidos pelos privilégios.No contexto de um sistema Synergis™, um direito de acesso é aquele cedido a um titular de cartão para passar por um ponto de acesso em determinada data e hora.

Diretório ativo É um diretório de serviço criado pela Microsoft e um tipo de função que importa usuários e titulares de cartão de um Directory Ativo e os matém sincronizados.

Detalhes de armazenagem de repositório É um tipo d tarefa de manutenção que relata os arquivos de vídeo (nome do arquivo, hora de início e final, tamanho do arquivo, status de proteção, etc.) usados para armazenar o arquivo de vídeo e que permite alterar os status de proteção desses arquivos, entre outras coisas.

decodificador de áudio É um dispositivo ou software que decodifica os streams de áudio comprimidos para reprodução. Sinônimo de *alto-falante*.

decodificador de áudio É um dispositivo ou software que decodifica os streams de áudio usando um algoritmo de compressão. Sinônimo de *microfone*.

Desenho de crachá	É uma ferramenta que permite desenhar e modificar os modelos de crachá.
difusão	É a comunicação entre um único remetente e todos os destinatários em uma rede.
Direitos de acesso do titular do cartão	É um tipo de tarefa de manutenção que relata quis titulares ou grupos de titulares têm acesso concedido ou negado para áreas selecionadas, portas e elevadores.
declaração	Uma *declaração* é uma afirmação que um sujeito faz sobre ele próprio ou outro sujeito. A afirmação pode ser sobre um nome, identidade, chave, grupo, privilégio ou capacidade, por exemplo. As declarações são emitidas por um provedor, recebem um ou mais valores e, em seguida, são empacotadas em tokens de segurança emitidos por um *emitente*, geralmente conhecido como *serviço de token de segurança* (STS).
dewarping	Dewarping é a transformação usada para corrigir uma imagem digital tirada com lente olho de peixe.
Directory	A função Directory identifica um sistema Security Center. Ela gerencia as configurações de todas as entidades e de todo o sistema no . O seu sistema pode ter apenas uma instância dessa função. O servidor que hospeda a função do Diretório é chamado de *servidor principal* e deve ser configurado primeiro. Todos os outros servidores adicionados ao Security Center são chamados *servidores de expansão* e devem ser conectados ao servidor principal para fazerem parte do mesmo sistema.
Directory Manager	A função Directory Manager gerencia o failover e o balanceamento de carga do Directory para produzir as características de alta disponibilidade no Security Center.
dureza	É um código especial usado para desarmar um sistema de alarme. Este código alerta, calmamente, a estação de monitoramento que o sistema de alarme foi desarmado sob ameaça.
destinatário do incidente	O destinatário do incidente é o usuário para o qual o incidente foi despachado. Esse usuário pode ver o incidente na tarefa *Monitoramento de incidentes*.
desencadeador de incidente	Um desencadeador de incidente é uma sequência de regras que são aplicadas pelo Mecanismo de regras Genetec Mission Control™ para detectar e desencadear incidentes automaticamente. O Mecanismo de regras procura combinações específicas de eventos (tipo, tempo, correlação e frequência) no sistema para determinar se um incidente deve ser desencadeado.

Detecção de intrusão
A tarefa *Detecção de intrusão* é uma tarefa de administração que permite configurar funções e unidades de detecção de instrusão.

Detector de Intrusões KiwiVision™
(obsoleto) Na análise de vídeo do KiwiVision™, o Detector de Intrusões KiwiVision™ é o módulo que adiciona a capacidade de análise de detecção de intrusão ao Security Center.

detecção de movimento
A detecção de movimento é o recurso que busca mudanças em uma série de imagens de vídeo. A definição do que constitui um movimento em um vídeo pode ser baseada em critérios altamente sofisticados.

decodificador de vídeo
É um dispositivo que converte um stream de vídeo digital em sinais analógicos (NTCS ou PAL) para exibir em um monitor analógico. O decodificador é um dos vários dispositivos encontrados em uma unidade de decodificação de vídeo.

Detalhes da visita
É um tipo de tarefa de investigação que reporta a estadia (horário de check-in e check-out) dos visitantes atuais e anteriores.

E

eventos de unidade de controle de acesso
É um tipo de tarefa de manutenção que reporta os eventos que pertencem às unidades de controle de acesso selecionadas.

Eventos do arquivador
É um tipo de tarefa de manutenção que relata os eventos que pertencem a funções selecionadas.

Exibição de área
A tarefa *Exibição de área* é uma tarefa de administração que permite configurar áreas, portas, câmeras, plug-ins de ladrilho, áreas de detecção de intrusão, zonas e outras entidades encontradas na exibição de área.

Eventos da câmera
É um tipo de tarefa de investigação que reporta eventos que pertencem às câmeras selecionadas em um intervalo especificado.

estacionamento autorizado contratual
Estacionamento autorizado contratual é um cenário de estacionamento em que somente os motoristas com autorizações mensais podem estacionar em uma zona de estacionamento. Uma lista de permissões é usada para conceder aos titulares de autorização acesso à zona de estacionamento.

evento personalizado
É um evento adicionado depois da instalação do sistema inicial. Os eventos definidos na instalação do sistema são chamados de eventos do sistema. Os eventos personalizados podem ser definidos pelo usuário ou adicionados automaticamente pelas instalações do plugin. Diferente dos eventos do sistema, os eventos personalizados podem ser renomeados e excluídos.

elevador	É um tipo de entidade que oferece propriedades de controle de acesso aos elevadores. Para um elevador, cada andar é considerado um ponto de acesso.
entidade	Entidades são os blocos de construção básicos do Security Center. Tudo o que precisa de configuração é representado por uma entidade. Uma entidade pode representar um dispositivo físico, como uma câmera ou porta, ou um conceito abstrato, como um alarme, um cronograma, um usuário, uma função, um plugin ou add-on.
estrutura de entidades	É uma representação gráfica das entidades do Centro de Segurança em uma estrutura de árvore, que ilustra a natureza hierárquica de suas relações.
evento	Um evento indica a ocorrência de uma atividade ou um incidente, como acesso negado a um titular de cartão ou movimento detectado em uma câmera. Os eventos são automaticamente registrados no Centro de Segurança e podem ser programados para disparar ações. Todo evento foca, principalmente, em uma entidade, chamada origem do evento.
evento causa-efeito	Um evento causa-efeito vincula uma ação a um evento. Por exemplo, é possível configurar o Security Center para acionar um alarme quando uma porta é forçada.
extensão	Um extensão se refere a um grupo de configurações específicas de um fabricante na página de configuração *Extensões* de uma função como o Archiver, o Access Manager ou o Intrusion Manager. A maioria das extensões vem integrada no Security Center, mas algumas requerem a instalação de um suplemento; nessas situações, a extensão também refere esse suplemente.
entidade federada	Uma entidade federada é qualquer entidade que seja importada de um sistema independente por meio de uma das funções Federation™.
entidade global	Uma entidade global é uma entidade compartilhada por vários sistemas independentes do Security Center em virtude de sua associação a uma partição global. Somente titulares de cartão, grupos de titulares de cartão, credenciais e modelos de crachá são elegíveis para compartilhamento
Estatísticas de saúde do sistema	Estatísticas de saúde do sistema é um tipo de tarefa de manutenção que dá uma visão geral da saúde do seu sistema.
Editor de lista de procurados e autorizações	O Editor de lista de procurados e autorizações é um tipo de tarefa de operação usada para editar uma lista de procurados ou uma lista de autorizações. Um nova lista não pode ser criada com esta tarefa, mas após uma lista existente ser adicionada ao Security Center, os usuários podem editar, adicionar ou excluir itens da lista, e o arquivo de texto original é atualizado com as alterações.

entidade inativa	entidade que é sombreada em vermelho no navegador. Indica que a entidade do mundo real que representa é não funciona, offline ou configurado incorretamente.
Eventos de unidade de detecção de intrusão	*Eventos da unidade de detecção de intrusão* são um tipo de tarefa de investigação que relata os eventos (falha de CA, falha da bateria, unidade perdida, problema de entrada etc.) relacionados a unidades de detecção de intrusão selecionadas.
Exibição de rede	A tarefa *Exibição de rede* é uma tarefa de administração que permite configurar suas redes e seus servidores.
equivalência de OCR	A equivalência de OCR é a interpretação de caracteres com equivalência OCR (Reconhecimento ótico de caracteres) realizada durante o reconhecimento de placas de veículos. Os caracteres com equivalência OCR são visualmente semelhantes, dependendo da fonte da placa. Por exemplo, a letra “O” e o número “0” ou o número “5” e a letra “S”. Existem vários caracteres com equivalência OCR predefinidos para diferentes idiomas.
estacionamento	Um estacionamento é um polígono que define a localização e a forma de uma área de estacionamento em um mapa. Ao definir o número de espaços de estacionamento dentro de um estacionamento, o Security Center pode calcular a sua percentagem de ocupação durante um determinado período de tempo.
estados da sessão de estacionamento	A sessão de estacionamento de um veículo é dividida em quatro estados: *Válido* (incluindo tempo de conveniência, tempo pago e período de cortesia), *Violação*, *Fiscalizado* e *Concluído*. Quando um veículo estaciona em uma zona de estacionamento, a sua sessão de estacionamento progride pelos estados da sessão de estacionamento com base no tempo configurado para a regra de estacionamento, a validade do tempo pago e se a sessão de estacionamento do veículo incorre em violação.
Endereço de IP privado	É um endereço de IP escolhido em uma série de endereços que é válido somente para uso em uma LAN. Os intervalos para um endereço de IP privados são: 10.0.0.0 a 10.255.255.255, 172.16.0.0 a 172.16.255.255 e 192.168.0.0 a 192.168.255.255. Os roteadores na Internet normalmente são configurados para eliminar todo tráfego que usar endereços de IP privados.
estado da gravação	É o estado de gravação atual de determinada câmera. Há quatro estados possíveis de gravação> *Habilitado*, *Desabilitado*, *Gravação atual (desbloqueada)*e *Gravação atual (bloqueada)*.
exibição de funções e unidades	A exibição de funções e unidades é uma exibição de navegador que lista as funções no seu sistema com as unidades que elas controlam como entidades secundárias.

Equipamento SV Um equipamento SV é um dispositivo completo que vem com um sistema operacional embutido e o Security Center pré-instalado. Você pode usar equipamentos SV para implementar rapidamente um sistema de vigilância por vídeo e controle de acesso unificado ou autônomo.

Equipamento Synergis™ Um aparelho Synergis ™ é um aparelho de segurança preparado para IP fabricado pela Genetec Inc., que é dedicado a funções de controle de acesso. Todos os aparelhos Synergis™ são fornecidos pré-instalados com Synergis™ Softwire e podem ser inscritos como unidades de controle de acesso no Security Center.

evento do sistema É um evento pré-definido que indica a ocorrência de uma atividade ou incidente. Os eventos de sistema são definidos pelo sistema e não podem ser renomeados nem excluídos.

espaço de trabalho da tarefa Um espaço de trabalho da tarefa é uma área na janela do aplicativo do cliente do Centro de Segurança reservado para a tarefa atual. O espaço de trabalho é normalmente dividido nos seguintes painéis: tela, painel de relatório, painel e visualização lógica.

estacionamento temporário Estacionamento temporário é um cenário de estacionamento em que o motorista deve comprar tempo de estacionamento assim que o veículo entra no estacionamento.

F

fachada (2 lados) Uma fachada (2 lados) é um tipo de regulamentação de estacionamento que caracteriza uma regra de tempo extra. Uma fachada é a extensão de uma rua entre duas interseções. Um veículo está em violação se for visto estacionado dentro da mesma fachada por um período específico de tempo. Mover o veículo de um lado da rua para o outro não faz diferença.

Fiscalização de estacionamento da cidade Fiscalização de estacionamento da cidade é uma instalação de software do Genetec Patroller™ configurada para a fiscalização de autorizações de estacionamento e restrições de tempo extra.

Fiscalização de estacionamento da cidade com imagens das rodas Fiscalização de estacionamento da cidade com imagens das rodas é uma instalação de *Fiscalização de estacionamento da cidade* de um aplicativo do Genetec Patroller™ que também inclui imagens de rodas. O uso de mapas e do Navegador é obrigatório.

Ferramenta copiar configuração Esta ferramenta ajuda a economizar tempo de configuração ao copiar as definições de uma entidade para várias outras que compartilham parcialmente as mesmas configurações.

filtragem de variação A filtragem de variação é o tempo que uma entrada pode estar em um estado alterado (por exemplo, alterado de ativo

	para inativo) antes que a alteração do estado seja relatada. Frequentemente, interruptores elétricos causam sinais instáveis temporários ao trocar de estados, possivelmente confundindo o circuito lógico. A filtragem de variação é usada para filtrar sinais instáveis, ao ignorar todas as mudanças de estado que são mais curtas do que um determinado período (em milissegundos).
forçar	Para forçar uma ação a ser tomada, seguindo um acerto confirmado. Por exemplo, um funcionário do estacionamento pode forçar uma violação de identificação de pessoas que ignoram a lei (tíquete de estacionamento sem pagar) ao colocar travas nas rodas.
failover	Failover é um modo operacional de backup em que uma função (do sistema) é automaticamente transferida do seu servidor primário para um secundário que está em espera. Esta transferência entre servidores ocorre somente quando o primeiro servidor está indisponível, seja por falha ou por inatividade programada.
Federal Information Processing Standard	Os Federal Information Processing Standards (FIPS) são padrões do conhecimento público desenvolvidos pelo governo federal dos Estados Unidos para uso em sistemas informáticos por agências governamentais não militares e prestadores de serviços a governos.
Federation™	O recurso Federation™ associa múltiplos sistemas de segurança IP Genetec™ independentes em um único sistema virtual. Com essa função, os usuários do Security Center podem controlar entidades que pertencem a sistemas remotos diretamente pelo sistema local do Security Center.
função hash	Em criptografia, uma função hash usa um algoritmo matemático para obter dados de entrada e devolver uma cadeia alfanumérica de tamanho fixo. Uma função hash está concebida para ser uma função unidirecional, ou seja, uma função impossível de reverter.
Ferramenta de importação	É uma ferramenta que permite importar titulares de cartão, grupos de titulares e credenciais de um arquivo CSV (Comma Separated Values - Valores separados por vírgula).
fluxo de trabalho de incidente	Um fluxo de trabalho de incidente é uma série de atividades associadas a um tipo de incidente. Essas atividades são realizadas pelo sistema durante o ciclo de vida de um incidente. Essas atividades podem mudar o estado e as propriedades do incidente, afetar outras entidades no sistema ou simplesmente esperar para que uma condição se tone verdadeira. Os fluxos de trabalho ajudam a automatizar as tarefas simples, tais como a exportação do incidente quando ele é resolvido para que operadores possam concentrar-se nos mais complexos.

Fiscalização de estacionamento Light
Fiscalização de estacionamento Light é uma configuração de instalação de software Genetec Patroller™ que é semelhante à configuração da Fiscalização de estacionamento da cidade, mas exclui recursos como autorizações compartilhadas, seleção automática de zonas, Conexão de placa e WMS. Você pode configurar o sistema para fiscalização de tempo extra ou fiscalização de autorização, mas não pode configurar os dois tipos de fiscalização.

função de plug-in
Uma função de plug-in adiciona recursos opcionais ao Security Center. Uma função de plug-in é criada usando o modelo de função *Plug-in*. Por padrão, é representada por uma peça de quebra-cabeça laranja na visualização *Funções* da tarefa *Sistema*. Antes de você poder criar uma função de plug-in, o pacote de software específico para essa função deve ser instalado no seu sistema.

função
Uma função é um componente de software que realiza um trabalho específico no Security Center. Para executar uma função, você deve atribuir um ou mais servidores para hospedá-la.

Ferramenta de detecção de unidade
Começando com um Security Center 5.4 GA, a ferramenta de detecção de unidade foi substituída pela ferramenta de inscrição de unidade.

Ferramenta de registro de unidades:
A Ferramenta de registro de unidades permite descobrir unidades IP (controle de acesso e vídeo) conectadas à sua rede, com base no fabricante e propriedades de rede (porta de descoberta, intervalo de endereços IP, senha e assim por diante). Uma vez detectadas, as unidades podem ser adicionadas ao seu sistema.

Fiscalização de estacionamento na universidade
Fiscalização de estacionamento na universidade é uma instalação de software do Genetec Patroller™ configurada para a fiscalização de estacionamento na universidade: a fiscalização de autorizações de estacionamento agendadas ou restrições de tempo extra. O uso de mapas é obrigatório. O recurso da lista de procurados não está incluído.

G

Gestor de Acesso
A função Gestor de Aceso gerencia e monitora as unidades de controle de acesso no sistema.

grupo de titulares de cartão
É um tipo de entidade que configura os direitos de acesso comum de um grupo de titulares de cartão.

Gerenciamento de titulares de cartão
É um tipo de tarefa de operação que permite criar, modificar e excluir os titulares de cartão. Nesta tarefa, também é possível gerenciar as credenciais de um titular de cartão de crédito, incluindo cartões de substituição temporária.

Gerenciamento de credenciais	É um tipo de tarefa de operação que permite criar, modificar e excluir os credenciais. Permite também imprimir crachás e inscrever grandes números de credenciais de cartão no sistema, seja por scanner em um leitor de cartão designado ou ao inserir um intervalo de valores.
Gateway do Directory	Os gateways do Directory permitem que aplicações do Security Center localizadas em uma rede não segura se conectem a um servidor principal protegido por um firewall. Um gateway de Directory é um servidor do Security Center que age como proxy para o servidor principal. Um servidor não pode ser um servidor de Directory e um gateway de Directory; o primeiro deve se conectar ao banco de dados do Directory, enquanto o outro não deve, por motivos de segurança.
gravação avançada	Gravação avançada é o processo de gravação e armazenamento local de vídeos gravados, removendo assim a necessidade de uma unidade ou servidor de gravação centralizado. Com a gravação avançada, é possível armazenar vídeo diretamente no dispositivo de armazenamento interno da câmera (cartão SD) ou em um volume de armazenamento conectado à rede (volume NAS).
G64	G64 é um formato do Security Center usado por funções de arquivamento (Archiver e Archiver auxiliar) para armazenar sequências de vídeos exportadas de uma única câmera. Este formato de dados suporta áudio, marcadores, sobreposição de metadados, marcas temporais, marcadores de movimento e evento e taxa de quadro e resolução variáveis.
G64x	G64x é um formato do Security Center usado para armazenar sequências de vídeos de várias câmeras cuja exportação e backup são feitos simultaneamente. Este formato de dados suporta áudio, marcadores, sobreposição de metadados, marcas temporais, marcadores de movimento e evento, taxa de quadro e resolução variáveis e marca d'água.
Genetec Clearance™ Uploader	Genetec Clearance™ Uploader é um aplicativo usado para carregar automaticamente uma mídia de uma câmera usada junto ao corpo ou pasta de sincronização, ou outro dispositivo para o Genetec Clearance™ ou um arquivo de vídeo Security Center dependendo do arquivo de configuração *.json* que seja usado.
Genetec Mission Control™	Genetec Mission Control™ é um sistema colaborativo de gerenciamento de decisões que oferece novos níveis de inteligência situacional, visualização e capacidades completas de gerenciamento de incidentes para empresas. Ele permite o pessoal de segurança tome a decisão certa ao enfrentar tarefas rotineiras ou situações não antecipadas, assegurando um fluxo atempado de informação. O Genetec Mission Control™ capacita organizações a saírem da simples gestão de

	eventos e alarmes através da coleta e qualificação de dados de milhares de dispositivos de sensor e segurança, observando as situações e incidentes mais complexos e guiando as equipes de segurança na sua resposta seguindo processos e requisitos de conformidade específicos da organização. Para aprender mais sobre o Genetec Mission Control™, consulte o hub de recursos Genetec.com.
Genetec™ Protocol	Genetec™ Protocol é um protocolo padrão desenvolvido pela Genetec Inc. que fabricantes terceirizados de codificadores de vídeo e câmeras IP podem usar para integrar os seus produtos ao Security Center Omnicast™.
Genetec™ Update Service	O Genetec™ Update Service (GUS) é automaticamente instalado com a maioria dos produtos Genetec™ e permite atualizar produtos quando uma nova versão fica disponível.
Genetec™ Video Player	Genetec™ Video Player é um reprodutor de mídia usado para visualizar arquivos de vídeo G64 e G64x exportados do Security Desk ou em um computador que não tenha o Security Center instalado.
geocodificação	Geocodificação é o processo de determinar coordenadas geográficas associadas (latitude e longitude) a partir do endereço de uma rua.
georreferenciamento	Georreferenciamento é o processo de utilização das coordenadas geográficas (latitude e longitude) de um objeto para determinar a sua posição em um mapa.
Global Cardholder Synchronizer	A função Global Cardholder Synchronizer garante a sincronização bilateral de titulares de cartão compartilhados e suas entidades relacionadas entre o sistema local (convidado de compartilhamento) onde ela reside e o sistema central (host de compartilhamento).
Gerenciador de incidentes	O Gerenciador de incidentes é a função central que reconhece padrões situacionais e ativa incidentes em um sistema Genetec Mission Control™. Essa função grencia o fluxo de trabalho de incidente e rastreia todas as atividades de usuários que estejam relacionadas a incidentes.
Gerenciador de invasão	A função Gerenciador de intrusão monitora e controla as unidades de detecção de intrusão. Ele ouve os eventos relatados pelas unidades, oferece relatórios ao vivo para o Security Center e registra os eventos em um banco de dados para relatório futuro.
Gerenciamento de inventários	Gerenciamento de inventário é um tipo de tarefa operacional que o permite adicionar e reconciliar reconhecimentos de placas de veículos ao inventário de um estacionamento.

Gerador de Mapa	É um módulo do Servidor de Mapas que importar os dados raster e os mapas de vetor para o banco de dados Gerenciador de Planos.
Gateway de mídia	O Media Gateway é uma função usada pelo Web Client do Security Center e aplicações externas para solicitar vídeo ao vivo e reprodução usando o Real Time Streaming Protocol (RTSP), e receber transmissões de vídeo puras a partir de câmeras gerenciadas por sistemas do Security Center.
grupo de monitor	É um tipo de entidade usado para designar monitores analógicos para exibir o alarme. Além dos grupos de monitor, a outra maneira de exibir alarmes em tempo real é usar a tarefa de monitoramento de alarme no Security Desk.
Gestor de planos	O Plan Manager é um módulo do Security Center que fornece funcionalidade de mapeamento interativo para visualizar melhor o seu ambiente de segurança.
Gerenciador de relatórios	O Gerenciador de relatórios é um tipo de função que automatiza o envio por e-mail e a impressão de relatórios com base em agendas.
geocodificação reversa	A geocodificação reversa é um recurso do AutoVu™ que converte um par de latitude e longitude em um endereço de rua legível.
grupo de transferência	Um grupo de transferência é um cenário de transferência de arquivos persistente que permite executar uma transferência de vídeo sem redefinir as configurações de transferência. Estas transferências podem ser agendadas ou executadas sob demanda. Os grupos de transferência definem quais câmeras ou funções de arquivamento estão inclusas na transferência, quando os arquivos são transferidos, quais dados são transferidos e assim por diante.
grupo de usuários	É um tipo de entidade que define um grupo de usuários que compartilham as propriedades e privilégios comuns. Ao se tornar membro de um grupo, um usuário automaticamente herda todas as propriedades do grupo. Um usuário pode ser membro de vários grupos. Os grupos de usuários também podem ser aninhados.
Gerenciamento de usuários	A *tarefa Gerenciamento de usuários* é um tipo de tarefa de administração que permite configurar usuários, grupos de usuários e partições.
Gerenciamento de visitantes	É um tipo de tarefa de operação que permite fazer check-in, check-out e modificar os visitantes e também gerenciar as credenciais, incluindo os cartões de troca temporários.
Gerenciador de Zona	É um tipo de função que gerencia as zonas virtuais e dispara eventos ou relés de saída com base nas entradas configuradas

	por cada zona. Também registra os eventos de zona em um banco de dados para relatórios de atividades de zona.

H

Histórico de saúde do controle de acesso	É um tipo de tarefa de manutenção que reporta os eventos de defeito para as unidades de controle de acesso.
Histórico de solicitação de credencial	É um tipo de tarefa de investigação que reporta quais usuários solicitaram, cancelaram ou imprimiram credenciais do titular do cartão.
Host de Federation™	O Host de Federation™ é o sistema do Security Center que executa funções Federation™. Os usuários no Host de Federation™ podem visualizar e controlar entidades que pertencem a sistemas federados diretamente do seu sistema local.
Histórico de saúde do sistema	Histórico de saúde do sistema é um tipo de tarefa de manutenção que relata problemas de saúde do sistema.
Health Monitor	A função Health Monitor monitora entidades do sistema como servidores, funções, unidades e aplicativos cliente em busca de problemas de saúde do sistema.
host de compartilhamento	Host de compartilhamento é um sistema do Security Center que confere a outros sistemas do Security Center o direito de visualizar e modificar suas entidades ao colocá-las para compartilhamento em uma partição global.

I

incidente colaborativo	Um incidente colaborativo é um tipo de incidente que requer a colaboração de várias equipes para ser resolvido. Cada equipe tem tarefas específicas a seguir, que são apresentadas como incidentes secundários. O incidente colaborativo fica resolvido quando todos os incidentes secundários ficam resolvidos.
identidade federada	Uma identidade federada é um token de segurança gerado fora do seu próprio realm que você aceita. Uma identidade federada habilita o logon único, permitindo que os usuários iniciem sessão em aplicativos em vários realms sem terem de digitar credenciais específicas do realm.
Inventário de hardware	Inventário de hardware e um tipo de tarefa de manutenção que relata as características (modelo da unidade, versão do firmware, endereço IP, fuso horário etc.) de unidades de controle de acesso, vídeo, detecção de invasão e LPR no seu sistema.

iluminador Um iluminador é uma luz na unidade Sharp que ilumina a placa, melhorando, assim, a precisão das imagens produzidas pela câmera de LPR.

incidente Um incidente é qualquer evento inesperado reportado por um usuário do Security Desk. Os relatórios de incidente podem usar texto formatado e incluir eventos e entidades como material de apoio.

incidente (Mission Control) Um incidente Genetec Mission Control™ é uma situação incomum ou indesejável que exige ação para ser resolvida.

Incidentes É um tipo de tarefa de investigação que permite fazer buscas, revisar e modificar os relatórios de incidentes.

intertravamento Um intertravamento (também conhecido como portão duplo ou câmara de vácuo) é uma restrição de acesso colocada em uma área protegida que permite que somente uma porta seja aberta em determinado momento.

IPv4 IPv4 é o protocolo de internet de primeira geração que usa um espaço de endereço de 32 bits.

IPv6 IPv6 é um protocolo de internet de 128-bit que usa oito grupos de quatro dígitos hexadecimais para o espaço do endereço.

Inventário de placas É uma lista de números de placas de veículos encontrados em um estacionamento em determinado período, mostrando onde cada um está estacionado (setor e fila).

ID lógico É um ID exclusivo atribuído a cada entidade no sistema para facilitar a referência. Os IDs lógicos são exclusivos apenas em um tipo de entidade particular.

Inventário de placas de veículos móvel O Inventário de placas de veículos móvel (MLPI) é a instalação do software Genetec Patroller™ que está configurado para coletar placas de veículo e outras informações do veículo para criar e manter um inventário de placas de veículo para uma área de estacionamento ou garagem grande.

ID do monitor É um ID usado para identificar unicamente a tela de uma estação de trabalho controlada pela Secretaria de Segurança.

instalação de estacionamento É um tipo de entidade que define uma grande área de estacionamento como um número de setores e filas para fins de rastreamento de inventário.

infraestrutura de chave pública Uma infraestrutura de chave pública (PKI) é um conjunto de hardware, software, pessoas, políticas e procedimentos necessários para suportar a distribuição e identificação de chaves de encriptação públicas. Isso permite aos usuários e computadores trocar dados com segurança nas redes como a Internet e verificar a identidade da outra pessoa.

ID do ladrilho — É o número exibido no canto superior esquerdo do ladrilho. Este número identifica exclusivamente cada ladrilho na tela.

inha do tempo — É uma ilustração gráfica de uma sequência de vídeo, mostrando onde estão em tempo, movimento e marcadores. As miniaturas também podem ser adicionadas à linha do tempo para ajudar o usuário a selecionar o segmento de interesse.

imagem da roda — É uma tecnologia virtual de calço do pneu que tira fotos das rodas do veículo para provar se eles se movimentou entre duas leituras de placa.

K

Kit de Desenvolvimento da Unidade — É um SDK para criação de unidades.

Keyhole Markup Language — Keyhole Markup Language (KML) é um formato de arquivo usado para exibir dados geográficos em um navegador da Terra, como Google Earth e o Google Maps.

KiwiVision™ Privacy Protector™ — KiwiVision™ Privacy Protector™ é um módulo da plataforma Security Center que assegura a privacidade dos indivíduos gravados por câmeras de vigilância por vídeo enquanto salvaguarda potenciais evidências.

Kit de desenvolvimento de software — O Kit de desenvolvimento de software (SDK — Software Development Kit) permite que os usuários finais desenvolvam aplicativos personalizados ou extensões de aplicativos personalizados para o Security Center.

L

ladrilho armado — Um ladrilho armado é um ladrilho no Security Desk que exibe novos alarmes que são acionados. Na tarefa *Monitoramento de alarmes*, todos os ladrilhos estão armados, enquanto na tarefa *Monitoramento* os ladrilhos devem ser armados por um usuário.

lista de procurados secreta — Listas de procurados secretas permitem garantir a discrição de uma investigação ou operação especial em andamento. Quando uma ocorrência é identificada, somente o responsável autorizado na estação do Security Center é notificado, enquanto o responsável no veículo de patrulha não é alertado. Isto permite que os responsáveis de fiscalização atribuam múltiplos objetivos ao veículo e aos sistemas back-end sem interromper as prioridades dos responsáveis em serviço.

lado da porta — Toda porta tem dois lados, chamados de *entrada* e *saída* por padrão. Cada lado é um ponto de acesso de uma área. Por exemplo, ao passar por um lado ocorre a entrada em uma área e ao passar pelo outro lado se sai dessa área. Para fins de gestão de acesso, as credenciais que são

	necessárias para passar por uma porta em uma direção não são necessariamente as mesmas para passar para a direção oposta.
leitura falso-positiva	Podem ocorrer leituras falso-positivas quando um sistema de reconhecimento de placas de veículos confunde outros objetos na imagem com placas de veículos. Por exemplo, inscrições em um veículo ou placas de rua podem criar leituras de placas de veículo falso-positivas.
lista de procurados	Uma lista de prioridades é uma lista de veículos procurados, na qual cada veículo é identificado por um número de placa, com o estado de emissão e com o motivo pelo qual o veículo é procurado (roubado, criminoso procurado, alerta âmbar, VIP, etc). As informações opcionais do veículo podem incluir o modelo, a cor e o número de identificação do veículo (VIN).
layout	No Security Desk, um layout é uma entidade que representa um instantâneo do que é exibido em uma tarefa de *Monitoramento*. Somente o padrão de ladrilho e o conteúdo do ladrilho são salvos, não o estado do ladrilho.
leitura de placa de veículo	Uma leitura de placa de veículo é um número de placa de veículo capturado de uma imagem de vídeo usando tecnologia LPR.
leitura de placa de veículo	Leitura de placa de veículo (LPR) é uma tecnologia de processamento de imagem usada para ler números de placas de veículo. A LPR converte números de placas de veículo recortados de imagens de câmeras em um formato pesquisável em bancos de dados.
leitura dinâmica	Uma leitura dinâmica é uma placa de veículo capturada pelo veículo de patrulha e imediatamente enviada para o Security Center através de uma rede sem fio.
Logons por Patroller	Logons é um tipo de tarefa de investigação que relata os registros de logon de um veículo de patrulha selecionado.
longo prazo	Longo prazo é um tipo de regulamentação de estacionamento que caracteriza uma regra de tempo extra. A regulamentação de *longo prazo* usa o mesmo princípio da regulamentação de *mesma posição*, mas o período de estacionamento é superior a 24 horas. A regulamentação de longo prazo não pode ser usada por mais de uma regra de tempo extra no sistema inteiro.
LPR	A tarefa *LPR* é uma tarefa administrativa que permite configurar funções, unidades, listas de procurados, autorizações e regras de tempo extra para LPR, bem como entidades e configurações relacionadas.
LPR Manager	A função LPR Manager gerencia e controla o software do veículo de patrulha (Genetec Patroller™), câmeras Sharp e zonas de estacionamento. O LPR Manager armazena os dados de LPR

	(leituras, ocorrências, carimbos de data e hora, coordenadas GPS e assim por diante) coletados pelos dispositivos.
link de mapa	Um link de mapa é um objeto que leva você a outro mapa com um simples clique.
limite de capacidade da zona de estacionamento	A definição de limite de capacidade da zona de estacionamento determina em que ponto um evento de *limite de capacidade atingido* é gerado. Por exemplo, se diminuir o limite para 90%, o sistema gera um evento quando a zona de estacionamento atinge a capacidade de 90%.
leitor	É um sensor que lê a credencial para um sistema de controle de acesso. Por exemplo, pode ser um leitor de cartão ou scanner biométrico.
Leituras	Leituras é um tipo de tarefa de investigação que relata as leituras de placas de veículo verificadas em um intervalo de tempo e área geográfica selecionados.
Leituras/ocorrências por dia	Leituras/ocorrências por dia é um tipo de tarefa de investigação que relata as leituras de placas de veículo verificadas em um intervalo de tempo e área geográfica selecionados.
Leituras/ocorrências por zona	Leituras/ocorrências por zona é um tipo de tarefa de investigação que relata o número de leituras e ocorrências por zona de estacionamento em um intervalo de datas selecionado.
logon único	Logon único (SSO) é o uso de uma autenticação de usuário única em vários sistemas de TI ou até mesmo organizações.
ladrilho	É uma janela individual na tela, usado para exibir uma única entidade. A entidade exibida é normalmente o vídeo de uma câmera, um mapa ou algo de natureza gráfica. A aparência e a impressão do ladrilho depende da entidade exibida.
leitura não reconciliada	É uma leitura de placa MLPI que não está vinculada a um estoque.
lista de permissões	Uma lista de permissões é uma lista de procurados que é criada com o objetivo de conceder a um grupo de placas de veículo acesso a um estacionamento. Uma lista de permissões pode ser comparada a uma regra de acesso em que a área protegida é o estacionamento. Ao invés de listar os titulares de cartão, a lista de permissões é aplicada a credenciais de placa de veículo.

M

Monitoramento do alarme	Tipo de tarefa de operação que permite monitorar e responder a alarmes (reconhecimento, encaminhamento, soneca, etc.) em tempo real e também revisar os alarmes anteriores.

monitor analógico É um tipo de entidade que representa um monitor que exibe vídeos a partir de uma fonte analógica, como um decodificador ou câmera analógica. Este termo é usado no Security Center para se referir aos monitores que não são controlados por um computador.

Modelo de crachá É um tipo de entidade usada para configurar um modelo impresso para crachás.

marcador É um indicador de evento ou incidente usado para marcar um momento específico em uma sequência de vídeo gravada. Um marcador também contém uma breve descrição de texto que pode ser usada para pesquisar e analisar as sequências de vídeo em um momento posterior.

marcadores É um tipo de tarefa de investigação que busca marcadores relacionados às câmeras selecionadas em um intervalo especificado.

módulo de controlador O módulo de controlador é o componente de processamento do Synergis™ Master Controller com capacidade de IP. Este módulo vem pré-carregado com o firmware do controlador e a ferramenta de administração baseada na Web, o Synergis™ Applicance Portal.

modo degradado É um modo de operação offline do módulo da interface quando a conexão à unidade Synergis™ é perdida. O módulo da interface concede acesso a todas as credenciais correspondentes a um código de uma instalação específica. Somente os módulos de interface Mercury e HID VertX podem operar no modo degradado.

modo dependente É um modo de operação online do módulo da interface em que a unidade Synergis™ toma todas as decisões de controle de acesso. Nem todos os módulos da interface podem operar em modo dependente.

módulo RS-485 de quatro portas Um módulo RS-485 de quatro entradas é um componente de comunicação do Synergis™ Master Controller com quatro portas (ou canais) chamados A, B, C e D. O número de módulos de interface que pode ser conectado a cada canal depende do tipo de hardware que você tem.

Monitoramento de incidente A tarefa *Monitoramento de incidentes* é um tipo de tarefa operacional que você pode usar para monitorar e responder a incidentes. Desta tarefa, você pode ver os incidentes exibidos em um mapa, melhorando a sua atenção situacional.

módulo de interface Um módulo da interface é um dispositivo de segurança que se comunica com uma unidade de controle de acesso por IP ou RS-485 e oferece conexões de entrada, saída e leitor à unidade.

macro	É um tipo de entidade que envolve um programa C# que adiciona funcionalidades personalizadas ao Security Center.
man-in-the-middle	Na segurança de informática, man-in-the-middle (MITM) é um modo de ataque onde o atacante inclui e provavelmente altera secretamente a comunicação entre duas partes que acreditam estar em contato direto entre si.
mapa	Um mapa no Security Center é um diagrama bidimensional que o ajuda a visualizar as localizações físicas de seu equipamento de segurança em uma área geográfica ou em um espaço de construção.
Map designer	A tarefa *Map designer* é uma tarefa administrativa que permite criar e editar mapas que representam as localizações físicas do seu equipamento para usuários do Security Desk.
Map Manager	O Map Manager é a função central que gerencia todos os recursos de mapeamento no Security Center, inclusive arquivos de mapas importados, provedores externos de mapas e objetos KML. Ele funciona como o servidor de mapas para todos os aplicativos clientes que exigem mapas.
modo de mapa	É um modo operacional da tela do Security Desk onde a área principal da tela é usada para exibir um mapa geográfico, com todos os eventos ativos georreferenciados no seu sistema.
Mapas	Mapas é um tipo de tarefa de investigação que amplia a sua consciência situacional fornecendo o contexto de um mapa às suas atividades de controle e monitoramento da segurança.
Media Router	O Media Router é a função central que comanda todas as solicitações de transmissão (áudio e vídeo) no Security Center. Estabelece sessões de transmissão entre a fonte de fluxo (câmera ou Archiver) e seus solicitantes (aplicativos cliente). As decisões de roteamento são baseadas no local (endereço de IP) e nas capacidades de transmissão de todas as partes envolvidas (origem, destinos, redes e servidores).
Mobile Server	Mobile Server é o componente de servidor do Security Center Mobile que conecta aplicativos móveis e Web Clients ao Security Center e sincroniza os dados e vídeo entre o Security Center e os componentes de clientes móveis suportados.
Monitoramento	A tarefa *Monitoramento* é um tipo de tarefa operacional que você pode usar para monitorar e responder a eventos em tempo real relacionados a entidades selecionadas. Usando a tarefa *Monitoramento*, você também pode monitorar e responder a alarmes.
Mover unidade	Ferramenta usada para mover as unidades de uma função do gerenciador para outra. O movimento preserva todas as configurações e dados da unidade. Depois do movimento, o

	novo gerenciador imediatamente assume o comando e da função de controle da unidade, enquanto que o gerenciador antigo continua a gerenciar os dados da unidade coletados antes do movimento.
modo de gravação	Modo de gravação é o critério pelo qual o Archiver agenda a gravação de transmissões de vídeo. Existem quatro modos possíveis de gravação: • Desligado (nenhuma gravação permitida) • Manual (gravar somente quando o usuário solicitar) • Contínuo (gravar sempre) • Em movimento/manual (gravar de acordo com as configurações de detecção de movimento ou quando o usuário solicitar)
Mecanismo de regras	O Mecanismo de regras é o componente do sistema Genetec Mission Control™ que analisa e correlaciona os eventos coletados pelo Security Center com base em regras predefinidas. O Mecanismo de regras usa esses eventos para detectar e acionar incidentes no sistema Genetec Mission Control™.
mesma posição	Mesma posição é um tipo de regulamentação de estacionamento que caracteriza uma regra de tempo extra. Um veículo está em violação se for visto estacionado no mesmo lugar exato por um período de tempo específico. O Genetec Patroller™ deve estar equipado com capacidade GPS para impor este tipo de regulamentação.
modo de servidor	O modo de servidor é um modo de operação especial restrito a unidades Synergis™, onde a unidade permite o acesso ao Access Manager (o servidor) para tomar todas as decisões de controle de acesso. A unidade deve permanecer conectada ao Access Manager a todo momento para operar nesse modo.
modo autônomo	É um modo operacional offline do módulo de interface onde este opera de forma independente, tomando decisões com base nas configurações de controle de acesso descarregadas anteriormente da unidade do Synergis™. A comunicação da atividade ocorre dentro da agenda, ou quando a conexão com a unidade estiver disponível. Nem todos os módulos da interface podem operar em modo autônomo.
modo supervisionado	É um modo operacional online do módulo de interface onde este toma decisões com base nas configurações de controle de acesso descarregadas anteriormente da unidade do Synergis™. O módulo da interface relata as suas atividades em tempo real à unidade e permite que a unidade substitua uma decisão, caso contradiga as configurações atuais da unidade. Nem todos os módulos da interface podem operar em modo supervisionado.

Monitor de disponibilidade do sistema System Availability Monitor (SAM) o permite coletar informações de integridade e visualizar o status da integridade dos seus sistemas Security Center para que você possa evitar e resolver proativamente problemas técnicos.

modo do ladrilho É o modo operacional da tela do Security Desk onde a área principal é usada para exibir os ladrilhos e o painel.

marca d'água de vídeo A marca d'água de vídeo adiciona uma assinatura digital (marca d'água) a cada quadro do vídeo gravado para garantir sua autenticidade. Se o vídeo for posteriormente alterado através da adição, exclusão ou modificação de um quadro, as assinaturas do conteúdo modificado não corresponderão mais, mostrando que o vídeo foi adulterado.

N

novo procurado Um novo procurado é um item de lista de procurados inserido manualmente no Genetec Patroller™. Ao procurar uma placa de veículo que não apareça nas listas de procurados carregadas no Genetec Patroller™, você pode introduzir a placa para acionar uma ocorrência se a placa for capturada.

nível da ameaça É um procedimento de tratamento de emergência que o operador do Security Desk pode representar em uma área ou em todo o sistema para lidar prontamente com uma situação potencialmente perigosa, como incêndio ou disparos.

nível de usuário É um valor numérico atribuído aos usuários para restringir sua capacidade de realizar certas operações, como controlar uma câmera PTZ, visualizar a alimentação de vídeo de uma câmera ou ficar registrado quando é definido um nível de ameaça. O nível 1 é o nível de usuário mais alto, com mais privilégios.

número de identificação do veículo Um número de identificação do veículo (VIN) é um número de identificação que um fabricante atribui a veículos. Normalmente, é visível do exterior do veículo como uma pequena placa no painel de instrumentos. É possível incluir um VIN como informação adicional em entradas de placa de veículo em uma lista de procurados ou de autorizações para melhor validar uma ocorrência e garantir que se trata do veículo correto.

O

ocorrência oculta Uma ocorrência oculta é uma leitura (placa de licença capturada) com correspondente em uma lista de procurados secreta. As ocorrências ocultas não são exibidas na tela do Genetec Patroller™, mas podem ser exibidas no Security Desk por um usuário com os privilégios corretos.

Ocorrências Alertas é um tipo de tarefa de investigação que relata sobre as ocorrências reportadas em um intervalo de tempo e área geográfica selecionados.

ocorrência dinâmica Uma ocorrência dinâmica é uma ocorrência correspondida pelo Genetec Patroller™ e imediatamente enviada para o Security Center através de uma rede sem fio.

objeto de mapa Os objetos de mapa são representações gráficas de entidades do Security Center ou qualquer característica geográfica (cidades, estradas, rios e assim por diante) nos seus mapas. Com objetos de mapa, você pode interagir com seu sistema sem sair do mapa.

Ocupação máxima O recurso *Ocupação máxima* monitora o número de pessoas em uma área, até um limite configurado. Uma vez atingido o limite, a regra negará acesso a mais titulares de cartão (se definida para *Rígido*) ou acionará eventos embora permita outros acessos (*Leve*) .

Omnicast™ Security Center Omnicast™ é o sistema de gerenciamento de vídeo (VMS) IP que oferece a organizações de todos os tamanhos a habilidade de implementar um sistema de vigilância adaptado às suas necessidades. Com uma ampla gama de câmeras IP, atende à crescente demanda por vídeos HD e análises, o tempo todo protegendo a privacidade individual.

Omnicast™ Federation™ A função Omnicast™ Federation™ conecta um sistema Omnicast™ 4.x ao Security Center. Desse modo, as entidades e eventos do Omnicast™ podem ser usados no seu sistema do Security Center.

ocorrência de autorização Uma ocorrência de autorização é uma ocorrência que é gerada quando uma leitura (número de placa de veículo) não corresponde a nenhuma entrada em uma autorização ou quando corresponde a uma autorização inválida.

ocupação da zona É um tipo de tarefa de investigação que informa o número de veículos estacionados em uma área selecionada e a porcentagem de ocupação.

P

ponto de acesso Qualquer entrada (ou saída) a uma área física onde o acesso pode ser monitorado e governado pelas regras de acesso. Um ponto de acesso é normalmente uma lateral da porta.

Presença na área É um tipo de tarefa de investigação que oferece uma foto instantânea de todos os titulares de cartão e visitantes atualmente em uma área selecionada.

provedor de reivindicações Um componente de software ou serviço que gera tokens de segurança mediante solicitação. Também conhecido como o emissor de reivindicações.

plataforma na nuvem Uma plataforma na nuvem fornece serviços de armazenamento e computação remotos através de data centers que são acessíveis pela Internet.

painel de controle É um dos três painéis que pertencem à tela no Security Desk. Contém comandos gráficos (ou widgets) que pertencem à entidade exibida no ladrilho atual.

porta de descoberta É uma porta usada por certas funções do Centro de Segurança (Gestor de acesso, Archiver, Gestor de LPR) para encontrar as unidades que são responsáveis na LAN. Não pode haver duas portas de descoberta iguais em um sistema.

porta Uma entidade de porta representa uma barreira física. Frequentemente, é uma porta, mas também pode ser um portão, uma catraca ou qualquer outra barreira controlável. Toda porta tem dois lados, chamados de *Entrada* e *Saída* por padrão. Cada lado é um ponto de acesso (entrada ou saída) de uma área protegida.

Pesquisa forense É um tipo de tarefa de investigação que busca sequências de vídeo com base nos eventos analíticos.

Patroller fantasma Um Patroller fantasma é uma entidade criada automaticamente pelo LPR Manager quando a licença do AutoVu™ inclui o módulo XML Import. No Security Center, todos os dados de LPR devem ser associados a uma entidade Genetec Patroller™ ou a uma unidade LPR que corresponda a uma câmera Sharp fixa. Ao importar dados de LPR de uma fonte externa através de um LPR Manager específico usando o módulo XML Import, o sistema usa a entidade fantasma para representar a fonte de dados LPR. Você pode formular consultas usando a entidade fantasma do mesmo modo que faria com uma entidade normal.

partição global Partição global é uma partição que é compartilhada em vários sistemas independentes do Security Center pelo proprietário da partição, o chamado anfitrião de compartilhamento.

período de cortesia Você pode adicionar um período de cortesia a uma sessão de estacionamento para fins de fiscalização leniente. Após o término do tempo pago ou do tempo de conveniência do veículo, o período de cortesia é o tempo extra dado antes de uma sessão de estacionamento ser identificada como uma *Violação*.

pacote de integração de hardware Um pacote de integração de hardware, ou HIP, é uma atualização que pode ser aplicada ao Security Center. Ele permite a gestão de novas funcionalidades (por exemplo, novos

	tipos de unidade de vídeo), sem precisar de uma atualização para a versão seguinte do Security Center.
ponto crucial	É um tipo de objeto de mapa que representa uma área no mapa que precisa de atenção especial. Clicar em um hotspot exibe as câmeras PTZ e fixas associadas.
provedor de identidade	Um site de internet que administra as contas de usuários e é responsável por gerar e manter a autenticação do usuário e as informações de identidade. Por exemplo, o Google administra contas do Gmail para os seus usuários, o que permite acessos únicos a outros sites usando uma conta.
proprietário do incidente	O proprietário do incidente é o destinatário do incidente que tomou posse do incidente. Somente o proprietário do incidente pode tomar ações para resolver o incidente. Um incidente só pode ter um proprietário do incidente de cada vez.
painel de intrusão	Um painel de intrusão (também conhecido como painel de alarme) é uma unidade montada na parede onde os sensores de alarme (sensores de movimento, detectores de fumaça, sensores de porta etc.) e os fios dos alarmes de intrusão estão conectados e são gerenciados.
predefinição de mapa	Uma predefinição de mapa é uma exibição de mapa salva. Cada mapa tem pelo menos uma predefinição, chamada *exibição padrão*. É a predefinição que é exibida por padrão quando um usuário abre o mapa.
Pesquisa de movimentos	É o tipo de tarefa de investigação que busca o movimento detectado em áreas específicas do campo de visão da câmera.
Pacote de compatibilidade do Omnicast™	É o componente de software necessário para tornar o Security Center compatível com um sistema Omnicast™ 4.x.
partição	É um tipo de entidade que define um conjunto de entidades que são visíveis apenas para um grupo específico de usuários. Por exemplo, uma divisão poderia incluir todas as áreas, portas, câmeras e zonas em um edifício.
Patroller	1 Genetec Patroller™ é o aplicativo de software AutoVu™ instalado em um computador de bordo. O Genetec Patroller™ conecta ao Security Center e é controlado pelo LPR Manager. O Genetec Patroller™ compara as placas de veículo lidas por câmeras de LPR com listas de veículos de interesse (listas de procurados) e de veículos autorizados (listas de autorização). Também coleta dados para fiscalização de estacionamento limitado por tempo. O Genetec Patroller™ alerta acerca de ocorrências de listas de procurados ou autorização para que seja possível tomar ações imediatas. 2 Tipo de entidade que representa um veículo de patrulha equipado com um computador de bordo executando o software Genetec Patroller™.

Patroller Config Tool Patroller Config Tool é o aplicativo administrativo do Genetec Patroller™ usado para configurar definições específicas do Patroller, como adicionar câmeras Sharp à LAN interna do veículo, habilitar recursos como Captura Manual ou Novo Procurado; e especificar a necessidade de um nome de usuário e senha para fazer logon no Genetec Patroller™.

Plate Reader Plate Reader é o componente de software da unidade Sharp que processa as imagens capturadas pela câmera de LPR para produzir leituras de placa de veículo, e associa cada leitura de placa de veículo a uma imagem de contexto capturada pela câmera de contexto. O Plate Reader também trata das comunicações com o Genetec Patroller™ e o LPR Manager. Se uma câmera WMS externa estiver conectada à unidade Sharp, o Plate Reader também captura imagens WMS dessa câmera.

plug-in Um plug-in (com letra minúscula) é um componente de software que adiciona um recurso específico a um programa existente. Dependendo do contexto, plug-in pode ser o próprio componente de software ou o pacote de software usado para instalar o componente de software.

Plug-in Plug-in (com uma maiúscula, no singular) é o modelo de função que serve para criar funções de plug-in específicas.

Plug-ins A tarefa *Plug-ins* é uma tarefa de administração que permite configurar funções específicas de plug-ins e entidades relacionadas.

proteção de privacidade No Security Center, proteção de privacidade é a tecnologia de software usada para desfocar ou mascarar partes de uma transmissão de vídeo. Tudo o que esteja se movendo e seja analisado como não fazendo parte do plano de fundo na cena é desfocado e mascarado para proteger a identidade de pessoas ou objetos em movimento sem obscurecer movimentos ou ações, para que possa continuar havendo monitoramento.

Privacy Protector™ A função Privacy Protector™ é responsável pela realização de operações de análise em transmissões. É uma função de processamento de mídia que solicita os vídeos originais do Archiver e modifica a transmissão para aplicar anonimização de vídeo confidencial. A transmissão de vídeo protegida por privacidade (anonimizada) é então enviada de volta para o Archiver para gravação.

privilégio Os privilégios definem o que os usuários podem fazer, como as zonas de armamento, bloqueio de câmeras e desbloqueio de portas, em parte do sistema que têm direito de acesso.

painel de relatórios O painel de relatórios é um dos painéis encontrados no espaço de trabalho de tarefas do Security Desk. Ele exibe resultados de consulta ou eventos em tempo real em um formato de tabela.

Portal de Dispositivos Synergis™ — O Portal de Dispositivos Synergis™ é uma ferramenta de administração baseada na web usada para configurar e administrar o dispositivo Synergis™, assim como atualizar o firmware.

padrão do azulejo — O padrão do azulejo é a distribuição nas telas.

plug-in de ladrilho — Um plug-in de ladrilho é um componente de software que é executado dentro de um ladrilho do Security Desk. Por padrão, é representado por uma peça de quebra-cabeça verde na exibição de área.

Pesquisador de arquivo de vídeo — É um tipo de tarefa de investigação que procura no seu sistema de arquivos por vídeos (G64 e G64x) e permite executá-los, converter para ASF e verificar a autenticidade desses arquivos.

proteção de vídeo — É possível proteger os vídeos contra exclusão. A proteção é aplicada em todos os arquivos de vídeo necessários para armazenar a sequência de vídeos protegida. Como nenhum arquivo de vídeo pode ser parcialmente protegido, o tamanho real da sequência de vídeos protegida depende da granularidade dos arquivos de vídeo.

porta VSIP — É o nome dado à porta de descoberta das unidades de Verint. Um determinado Archiver pode ser configurado para escutar várias portas VSIP.

R

regra de acesso — É um tipo de entidade que define uma lista de titulares de cartão a quem o acesso é dado ou negado com base em um cronograma. Uma regra de acesso pode ser aplicada a uma área protegida ou a um ponto de acesso.

reconhecimento de alarme — É uma resposta do usuário para um alarme. No Centro de Segurança, o reconhecimento padrão e o alternativo são as duas variações de reconhecimento de alarme. Cada variante está associada a um evento diferente, para que ações específicas possam ser programadas com base na resposta do alarme selecionada pelo usuário.

Relatório de alarme — É um tipo de tarefa de investigação que permite buscar e visualizar os alarmes atuais e anteriores.

Rastreamento de auditoria — É um tipo de tarefa de manutenção que relate as alterações de configuração das entidades selecionadas no sistema e também indica o usuário que fez tais alterações.

registro automático — O registro automático acontece quando novas unidades IP em uma rede são descobertas automaticamente e adicionadas ao Security Center. A função que é responsável pelas unidades *transmite* uma solicitação de descoberta em uma porta específica e as unidades que escutam nessa porta respondem

	com uma mensagem que contém suas próprias informações de conexão. Em seguida, a função usa a informação para configurar a conexão à unidade e habilitar a comunicação.
reconhecimento automático de placas de veículo	Reconhecimento automático de placas de veículo (ALPR) é o termo usado para *Reconhecimento de placas de veículo (LPR)* na Europa.
regra de primeira pessoa a entrar	A regra de primeira pessoa a entrar é a restrição de acesso adicional feita a uma área protegida que impede alguém de entrar na área até que um supervisor esteja no local. A restrição pode ser aplicada quando existe acesso livre (mediante agendas de desbloqueio de portas) e quando existe acesso controlado (mediante regras de acesso).
regra de ocorrências	Regra de ocorrências é um tipo de regra de LPR usada para identificar veículos de interesse (chamados de "ocorrências") usando leituras de placa de licença. Outras regras de ocorrências incluem lista de prioridades, regra de tempo extra, autorização e restrição de autorização.
Relatório do incidente	A tarefa *Relatório de incidentes* é um tipo de tarefa de investigação que você pode usar para pesquisar, revisar e analisar incidentes do Mission Control.
Relatório de inventário	Relatório de inventários é um tipo de tarefa de investigação que o permite visualizar um inventário específico (localização do veículo, duração da estadia do veículo e assim por diante) ou compare dois inventários de um estacionamento selecionado (veículos adicionados, veículos removidos e assim por diante).
Regra de LPR	Regra de LPR é um método usado pelo Security Center e pelo AutoVu™ para processar uma leitura de placa de veículo. Uma Regra de LPR pode ser uma regra de ocorrências ou um estacionamento.
rede	A entidade de rede é usada para captar as características das redes usadas pelo seu sistema, para que possam ser tomadas as decisões adequadas de roteamento de stream.
regra de tempo extra	Uma regra de tempo extra é um tipo de entidade que define um limite de tempo estacionado e o número máximo de violações a fiscalizar em um único dia. As regras de tempo extra são usadas na fiscalização de estacionamentos municipais e universitários. Para estacionamentos universitários, uma regra de tempo extra também define a zona de estacionamento em que essas restrições se aplicam.
regra de estacionamento	Uma regra de estacionamento define como e quando uma sessão de estacionamento é considerada como sendo válida ou uma violação.

Rastreamento do Patroller	Rastreamento do Patroller é um tipo de tarefa de investigação que permite reproduzir a rota seguida por um veículo de patrulha em determinada data em um mapa, ou visualizar a localização atual de veículos de patrulha em um mapa.
restrição de autorização	Uma restrição de autorização é um tipo de entidade que aplica restrições de tempo a uma série de autorizações de estacionamento para uma dada zona de estacionamento. As restrições de autorização são apenas usadas por veículos de patrulha configurados para Fiscalização de estacionamento na universidade.
realm	Em termos de identidade, um realm é o conjunto de aplicativos, URLs, domínios ou sites para o qual um token é válido. Geralmente, um realm é definido usando um domínio de Internet como genetec.com, ou um caminho dentro desse domínio, como genetec.com/support/GTAC. Um realm é por vezes descrito como um domínio de segurança, pois abrange todos os aplicativos dentro de uma fronteira de segurança especificada.
redirecionamento	É um servidor atribuído para hospedar um agente de redirecionamento criado pela função do Roteador de Mídia.
Remoto	Remoto é um tipo de tarefa de operação que permite monitorar remotamente e controlar outras Security Desks que fazem parte do seu sistema, usando a tarefa Monitoramento e a tarefa Monitoramento de alarmes.
rota	Rota é uma configuração que define as capacidades de transmissão entre dois pontos de extremidade em uma rede para fins de roteamento de transmissões de vídeo.
regra de acesso temporário	É uma regra de acesso que tem uma hora de ativação e término. Regras de acesso temporário são adequadas para situações em que titulares de cartão permanentes precisam de acesso temporário ou sazonal a áreas restritas. Essas regras de acesso são automaticamente excluídas sete dias após o término para evitar que o sistema fique sobrecarregado.
regra de duas pessoas	A regra de duas pessoas é a restrição de acesso aplicada a uma porta que exige que dois titulares de cartão (inclusive visitantes) apresentem as credenciais com um certo intervalo entre si para ganhar acesso.
regra de acompanhante de visitante	A regra de acompanhante de visitante é a restrição de acesso adicional aplicada a uma área protegida que exige que os visitantes sejam acompanhados por um titular de cartão durante a estadia. Os visitantes que tenham um host não podem passar por pontos de acesso até que eles e seu host (titular de cartão) apresentem as credenciais com um intervalo de tempo entre uma apresentação e outra.

relatório visual São diagramas ou gráficos dinâmicos do Security Desk que apresentam dados a partir dos quais você pode agir. É possível realizar buscas e investigar situações usando esses relatórios visuais e fáceis de usar. Os dados do relatório visual podem ser analisados para ajudar a identificar padrões de atividade e melhorar a sua compreensão.

rastreamento visual Rastreamento visual é um recurso do Security Desk que permite seguir um indivíduo por diferentes áreas da empresa sem perdê-lo de vista, desde que os lugares por onde esta pessoa passar estejam monitorados por câmeras. Este recurso exibe sobreposições transparentes no vídeo para exibir onde é possível clicar para passar para as câmeras adjacentes.

S

Solução de problemas de acesso É uma ferramenta que ajuda a detectar e diagnosticar os problemas de configuração de acesso. Com essa ferramenta, é possível saber:

- Quem tem permissão para passar por um ponto de acesso em uma determinada data e hora
- Quais pontos de acesso um titular de cartão tem permissão para usar em uma determinada data e hora
- Por que um determinado titular de cartão pode ou não usar um ponto de acesso em uma determinada data e hora

sequência da câmera É um tipo de entidade que define uma lista de câmeras que são exibidas, uma depois da outra, de modo giratório, em um único ladrilho no Security Desk.

saída controlada Uma saída é controlada quando é necessário apresentar as credenciais para sair de uma área segura.

servidor do banco de dados É um aplicativo que gerencial os bancos de dados e as solicitações de dados feitas pelos aplicativos do cliente. O Security Center usa o Microsoft SQL Server como servidor de banco de dados.

Servidor de dados É o módulo do Gerenciador de Plano que administrar o banco de dados onde a configuração do mapa é armazenada.

servidor do Directory Qualquer dos vários servidores que executam simultaneamente a função do Directory em uma configuração de alta disponibilidade.

Solução de problemas da porta É um tipo de tarefa de manutenção que lista todos os titulares de cartão que têm acesso a um lado da porta particular ou andar do elevador em determinada data e hora.

servidor de expansão Um servidor de expansão é qualquer servidor em um sistema Security Center que não hospede a função de Directory. A

	finalidade do servidor de expansão é aumentar o poder de processamento do sistema.
sistema federado	Um sistema federado é um sistema independente (Omnicast™ ou Security Center) que é unificado no seu Security Center local por uma função Federation™, para que os usuários locais possam visualizar e controlar suas entidades, como se pertencessem ao sistema local.
saída livre	É um estado de ponto de acesso onde não é necessário apresentar as credenciais para sair de uma área segura. A pessoa libera a porta ao girar a maçaneta ou ao pressionar o botão REX e sai. Um sistema de fechamento automático fecha a porta, para que possa ser trancada depois de aberta.
Servidor Genetec™	Genetec™ Server é um serviço do Windows que está no núcleo da arquitetura do Centro de Segurança e que deve ser instalado em todo computador que faça parte do conjunto de servidores do Security Center. Cada um desses servidores é um recurso computacional genérico capaz de assumir qualquer conjunto de funções que você atribua a ele.
Sistema de informação geográfica	O Sistema de informação geográfica (GIS) é um sistema que captura dados geográficos espaciais. O Map Manager pode se conectar a fornecedores terceirizados que prestam serviços de GIS a fim de integrar mapas e todos os tipos de dados geograficamente referenciados no Security Center.
supervisor do incidente	Um supervisor do incidente é um usuário que vê um incidente na tarefa *Monitoramento de incidentes* pois eles supervisionam os destinatários do incidente. Os supervisores do incidente não são eles mesmos destinatários do incidente. Um usuário não pode ser ao mesmo tempo supervisor e recipiente do mesmo incidente.
servidor principal	O servidor principal é o único servidor no sistema Security Center que hospeda a função do Directory. Todos os outros servidores no sistema devem se conectar ao servidor principal para fazer parte do mesmo sistema. Em uma configuração de alta disponibilidade, onde vários servidores hospedam a função de Directory, é o único servidor que pode gravar no banco de dados do Directory.
sessão de estacionamento	O recurso AutoVu™ Free-Flow no Security Center usa sessões de estacionamento para controlar a permanência de cada veículo em uma zona de estacionamento. Uma sessão de estacionamento é dividida em quatro estados: *Válido* (incluindo tempo de conveniência, tempo pago e período de cortesia), *Violação*, *Fiscalizado* e *Concluído*.
Sessões de estacionamento	A tarefa *Sessões de estacionamento* é um tipo de tarefa de investigação que permite gerar uma lista de veículos que estão atualmente em violação. Você pode criar um relatório

	de inventário de veículos para a ocupação da zona de estacionamento atual ou para um período específico no passado com base no filtro de tempo selecionado.
servidor primário	É o servidor padrão escolhido para realizar uma função específica no sistema. Para aumentar a tolerância de falha do sistema, o servidor primário pode ser protegido por um servidor secundário em espera. Quando o servidor primário ficar indisponível, o secundário automaticamente começa a funcionar.
solicitação de saída	Solicitação de saída (REX) é um botão de liberação de portas normalmente localizado dentro de uma área protegida que, quando pressionado, permite que uma pessoa saia da área protegida sem ter que mostrar nenhuma credencial. Também pode ser o sinal de um detector de movimento. Também é o sinal recebido pelo controlador para uma solicitação de saída.
servidor secundário	Um servidor secundário é qualquer servidor alternativo em espera para substituir o servidor primário no caso de este vir a ficar indisponível.
Secure Socket Layer	Secure Socket Layer (SSL) é um protocolo de rede informático que gerencia a autenticação de servidores, a autenticação de clientes e a comunicação criptografada entre servidores e clientes.
Security Center	O Security Center é uma plataforma verdadeiramente unificada que combina vigilância por vídeo IP, controle de acesso, reconhecimento de placas de veículo, detecção de intrusão e comunicação em uma única solução modular intuitiva. Tirando partido de uma abordagem unificada à segurança, a sua organização ganha eficiência, toma melhores decisões e responde a situações e ameaças com maior confiança.
Security Center Federation™	A função Security Center Federation™ conecta um sistema Security Center remoto e independente ao seu Security Center local. Desse modo, as entidades e eventos do sistema remoto podem ser usados no seu sistema local.
Security Center Mobile	Security Center Mobile é um recurso que você pode usar para se conectar remotamente ao seu sistema Security Center através de uma rede IP sem fio utilizando um smartphone.
Security Center Edição SaaS	O Security Center Edição SaaS é Security Center oferecido mediante assinatura. A propriedade baseada em assinatura simplifica a transição para serviços em nuvem e fornece uma maneira alternativa de comprar, implantar e manter a plataforma unificada Genetec™ Security Center.
Security Desk	Security Desk é a interface de usuário unificada do Security Center. Oferece um fluxo de operador consistente entre todos os principais sistemas do Security Center, Omnicast™, Synergis™

	e AutoVu™. O exclusivo design baseado em tarefas do Security Desk permite que os operadores controlem e monitorem, de modo eficiente, vários aplicativos de segurança e de segurança pública.
Serviço de token de segurança	O Serviço de Token de Segurança (STS) é um provedor de declarações implementado como serviço web que emite tokens de segurança. Os Serviços de Federação do Active Directory (ADFS) são um exemplo do serviço de tokens de segurança. Também conhecido como emissor.
servidor	Um servidor é um tipo de entidade que representa uma máquina de servidor em que o serviço Servidor Genetec™ está instalado.
Server Admin	É um aplicativo web que executa em toda máquina do servidor em Centro de Segurança que permite configurar o Servidor Genetec. O Server Admin também permite configurar a função do Diretório no servidor principal.
Sharp EX	Sharp EX é a unidade Sharp que inclui um processador de imagens integrado e suporta duas entradas NTSC ou PAL de definição padrão para câmeras externas (Câmeras de contexto e de LPR).
Sharp Portal	Sharp Portal é uma ferramenta com base na Web usada para configurar câmeras Sharp cameras para sistemas AutoVu™ fixos ou móveis. A partir de um navegador Web, você faz login em um endereço IP específico (ou o nome Sharp em certos casos) que corresponde ao Sharp que deseja configurar. Ao fazer login, você pode configurar opções, tais como selecionar o contexto LPR (por ex., Alabama, Oregon, Quebec etc.), selecionar a estratégia de leitura (por ex., veículos rápidos ou lentos), visualizar feeds de vídeo ao vivo do Sharp e muito mais.
Sharp VGA	Sharp VGA é uma unidade Sharp que integra os seguintes componentes: um iluminador infravermelho; uma câmera de LPR de definição padrão (640 x 480) para captura de placas; um processador de imagens integrado; uma câmera de contexto colorida NTSC ou PAL com capacidades de transmissão de vídeo.
Sharp XGA	Sharp XGA é uma unidade Sharp que integra os seguintes componentes: um iluminador infravermelho, uma câmera de LPR de alta definição (1024 x 768) para captura de placas; um processador de imagens integrado, uma câmera de contexto colorida NTSC ou PAL com capacidades de transmissão de vídeo e GPS interno opcional.
SharpOS	SharpOS é um componente de software de um Sharp ou uma unidade Sharp. O SharpOS é responsável por tudo relacionado à captura, à coleta, ao processamento e à análise de placas. Por exemplo, uma atualização do SharpOS pode incluir novos

	contextos LPR, novo firmware, atualizações do Sharp Portal e atualizações aos serviços do Windows do Sharp (Plate Reader, HAL, serviço de atualização e assim por diante).
SharpV	SharpV é uma unidade Sharp especializada para instalações fixas e destina-se idealmente a diversos aplicativos, desde o gerenciamento de estacionamentos fora da rua e instalações, até a cobertura de pontos de acesso de grandes cidades para detectar veículos procurados. SharpV combina duas câmeras de alta definição (1.2MP) com processamento integrado e iluminação em uma unidade robusta e ambientalmente selada. Ambas as lentes são varifocais para facilitar a instalação e a câmera é alimentada através de PoE+.
SharpX	SharpX é o componente de câmera do sistema SharpX. A unidade de câmera SharpX integra um iluminador de LED pulsado que funciona na escuridão total (0 lux), uma Câmera de LPR monocromática (1024 x 946 @ 30 fps) e uma câmera de contexto de cores (640 x 480 @ 30 fps). Os dados de LPR capturados pela unidade de câmera SharpX são processados em um componente de hardware separado chamado Unidade de processamento AutoVu™ LPR.
SharpX VGA	SharpX VGA é o componente de câmera do sistema SharpX. A unidade de câmera SharpX VGA integra um iluminador de LED pulsado que funciona na escuridão total (0 lux), uma Câmera de LPR monocromática (640 x 480 @ 30 fps) e uma câmera de contexto de cores (640 x 480 @ 30 fps). Os dados de LPR capturados pela unidade de câmera SharpX VGA são processados em um componente de hardware separado chamado Unidade de processamento AutoVu™ LPR.
SV-16	SV-16 é um dispositivo tudo em um subcompacto que vem com Microsoft Windows, Security Center e SV Control Panel pré-instalado. SV-16 é para instalações de pequena escala, com um único servidor e oferece suporte tanto a câmeras quanto a leitores de controle.
SV-32	SV-32 é um dispositivo tudo em um que vem com Microsoft Windows, Security Center e SV Control Panel pré-instalado. Com placas de captura com codificação analógica, SV-32 é um dispositivo completo que o permite implantar rapidamente um sistema autônomo (vigilância de vídeo ou controle de acesso) ou um sistema unificado (vigilância de vídeo e controle de acesso).
SV Control Panel	SV Control Panel é um aplicativo de interface do usuário que você pode usar para configurar o seu dispositivo SV para funcionar com controle de acesso Security Center e vigilância por vídeo.

SV-PRO	SV-PRO é um dispositivo montado em bastidor que vem com Microsoft Windows, Security Center e SV Control Panel pré-instalados. SV-PRO é para instalações de pequena a média escala, com instalações de servidor únicas ou múltiplas e oferece suporte tanto a câmeras quanto a leitores de controle.
Synergis™	Security Center Synergis™ é o sistema de controle de acesso IP (ACS) que aumenta a segurança física da sua organização e a prontidão para responder a ameaças. Com um crescente portfólio de hardware de controle de portas e travas eletrônicas de terceiros, permite que você aproveite o seu investimento existente em rede e equipamentos de segurança.
Synergis™ Cloud Link	Synergis™ Cloud Link é um dispositivo inteligente e habilitado para Power-over-Ethernet (PoE) de controle de acesso da Genetec Inc. que suporta vários módulos de interfaces de terceiros por IP e RS-485. O Synergis™ Cloud Link é integrado ao Centro de Segurança, de modo contínuo e é capaz de tomar decisões de controle de acesso independentemente do Gestor de Acesso.
Synergis™ Master Controller	Synergis™ Master Controller (SMC) é um dispositivo de controle de acesso da Genetec Inc. que suporta vários módulos de interfaces de terceiros por IP e RS-485. O SMC é integrado ao Centro de Segurança, de modo contínuo e é capaz de tomar decisões de controle de acesso independentemente do Gestor de Acesso.
Synergis™ Softwire	Synergis™ Softwire é o software de controle de acesso desenvolvido pela Genetec Inc. para executar uma variedade de aparelhos de segurança preparados para IP. Synergis™ Softwire permite que esses aparelhos se comuniquem com módulos de interface de terceiros. Um dispositivo de segurança executando o Synergis™ Softwire pode ser inscrito como uma unidade de controle de acesso no Security Center.
System Availability Monitor Agent	O System Availability Monitor Agent (SAMA) é componente do SAM, instalado em todos os servidores principais Security Center. SAMA coleta informações de saúde do Security Center e envia para o serviço de Health Monitor na nuvem.
Sistema	A tarefa *Sistema* é uma tarefa de administração que permite configurar funções, macros, agendas e outras entidades e configurações do sistema.
Status do sistema	É um tipo de tarefa de manutenção que monitora o status de todas as entidades de um determinado tipo em tempo real e permite interagir com elas.
Substituição da unidade	É uma ferramenta usada para substituir um dispositivo de hardware com problema por outro compatível, enquanto garante que os dados associados à unidade antiga sejam transferidos para a nova. Para uma unidade de controle

	de acesso, a configuração da unidade antiga é copiada na nova unidade. Para uma unidade de vídeo, o arquivo associado à unidade antiga agora está associado à nova, mas a configuração da unidade não é copiada.
sincronização de unidades	A sincronização de unidades é o processo de baixar as configurações mais recentes do Security Center para uma unidade de controle de acesso. Essas configurações, como regras de acesso, titulares de cartão, credenciais, agendamentos de desbloqueio, etc. são necessárias para que a unidade possa tomar decisões autônomas e precisas na ausência do Access Manager.
sequência de vídeo	Qualquer stream de vídeo de certa duração.
stream de vídeo	É uma entidade que representa uma configuração de qualidade de vídeo específica (formato de dados, resolução de imagem, taxa de bits, taxa de quadros, etc.) em uma câmera.
SDK baseado na web	Esta função expõe os métodos SDK do Security Center e os objetos como serviços Web para dar suporte ao desenvolvimento da plataforma cruzada.
Servidor Web Client	O Web Client Server é a função usada para configurar o Security Center Web Client, um aplicativo da Web que oferece aos usuários acesso remoto ao Security Center. Cada função criada define um endereço da Web exclusivo (URL) que os usuários inserem no navegador da Web da Internet para fazer logon no Web Client e acessar informações do Security Center.

T

Trilhas de atividade	É um tipo de tarefa de manutenção que reporta a atividade do usuário relacionada ao vídeo, controle de acesso e funcionalidade LPR. Essa tarefa pode fornecer informações como quem reproduziu quais gravações de vídeo, quem usou o editor da lista de procurados e autorizações, quem habilitou a filtragem da lista de procurados e muito mais.
Transferência de arquivo	A tarefa transferência de arquivo é um tipo de tarefa de administração que o permite definir as configurações para recuperar gravações de uma unidade de vídeo, duplicar arquivos de um Archiver para o outro Archiver ou fazer back-up de arquivos em um local específico.
transferência de arquivo	Transferência de arquivo é o processo de transferência de dados de vídeo de um local para outro. O vídeo é gravado e armazenado na própria unidade de vídeo ou em um disco de armazenamento do Archiver e, em seguida, as gravações são transferidas para outro local.

tela
É um dos painéis encontrados no espaço de trabalho da tarefa do Security Desk. A tela é usada para exibir informações multimídia, como vídeos, mapas e fotos. É dividido em três painéis: os ladrilhos, o painel e as propriedades.

taxa de captura
A taxa de captura mede a velocidade à qual um sistema de leitura de placa de veículo consegue tirar uma foto de um veículo passando e detectar a placa de veículo na imagem.

titular de cartão
É um tipo de entidade que representa uma pessoa que pode entrar e sair das áreas protegidas por ter suas credenciais (normalmente cartões de acesso) e cujas atividades podem ser rastreadas.

transmissão de chave específica do cliente
A transmissão de chave específica do cliente é a forma criptografada da *transmissão de chave principal*. A transmissão de chave principal é criptografada com a *chave pública* contida em um *certificado de criptografia*, emitido especificamente para uma ou mais máquinas clientes. Somente as máquinas clientes que possuem o certificado de criptografia instalado possuem a *chave privada* necessária para descriptografar a transmissão de chave criptografada.

tempo de conveniência
O tempo de conveniência é um tempo de leniência configurável que é aplicável antes de um veículo começar a ser cobrado após entrar na zona de estacionamento. Por exemplo, se você precisar configurar um período de estacionamento grátis de 2 horas que é aplicável antes de o tempo pago ou a fiscalização de estacionamento entrar em vigor, você deverá definir do tempo de conveniência para 2 horas. Para estacionamentos onde a fiscalização de estacionamento começa imediatamente, você precisaria definir um breve tempo de conveniência para dar tempo aos proprietários dos veículos encontrarem um lugar de estacionamento e adquirirem tempo de estacionamento antes que a fiscalização de estacionamento comece.

texto criptografado
Na criptografia, texto criptografado são os dados criptografados.

transmissão de fusão
Um fluxo de fusão é uma estrutura de dados de propriedade de Genetec Inc. para transmissão de fluxo de multimídia. Cada fluxo de fusão é um conjunto de fluxos de dados (vídeo, áudio e metadados) e fluxos chave relacionados com uma única câmera. As transmissões de fusão são criadas em resposta a solicitações específicas de cliente. As transmissões de chaves estão inclusas somente se as transmissões de dados estiverem criptografadas.

tipo de incidente
Um tipo de incidente é uma entidade que representa uma situação que exige ações específicas para ser resolvida. A entidade tipo de incidente pode ser usada também para automatizar a detecção de incidente no Controle de Missão e

	impor os procedimentos operacionais padrão que a sua equipe de segurança deve seguir.
transmissão de chave principal	Em criptografia de *transmissão de fusão*, a transmissão de chave principal é a sequência de chaves simétricas geradas pelo Archiver para criptografar uma transmissão de dados. As chaves simétricas são geradas aleatoriamente e mudam a cada minuto. Por motivos de segurança, o stream de chave mestra nunca é transmitido ou armazenado em qualquer lugar como texto.
tempo máximo da sessão	Definir um tempo máximo da sessão ajuda a melhorar as estatísticas de ocupação de estacionamentos. Quando um veículo excede o tempo máximo da sessão, presume-se que a placa do veículo não foi lida à saída e que o veículo já não se encontra na zona de estacionamento. A sessão de estacionamento aparece em relatórios gerados a partir da tarefa *Sessões de estacionamento* com o *Motivo do estado: tempo máximo da sessão excedido*.
tradução do endereço de rede	É o processo de modificação da informação de endereço de rede em cabeçalhos do pacote (IP) do conjunto de dados, enquanto em trânsito por um dispositivo de roteamento de tráfego, para fins de remapeamento de um espaço de endereço de IP para outro.
tempo pago	A etapa de tempo pago de uma sessão de estacionamento começa quando o *tempo de conveniência* expira. Os proprietários de veículos podem adquirir tempo de estacionamento através de uma estação de pagamento ou um aplicativo móvel e o sistema de pagamento pode ser fornecido por provedores terceiros de autorização de estacionamento integrados.
texto simples	Na criptografia, os dados de texto simples são dados não criptografados.
tarefa privada	Uma tarefa privada é uma tarefa somente visível para o usuário que a criou.
tarefa pública	Uma tarefa pública é uma tarefa salva que pode ser compartilhada e reutilizada entre vários usuários do Security Center.
taxa de leitura	A taxa de leitura mede a velocidade à qual o sistema de reconhecimento de placas de veículo consegue detectar e ler corretamente todos os caracteres em uma imagem de uma placa de veículo.
taxa de renderização	Taxa de renderização é a comparação entre a velocidade com que a estação de trabalho renderiza um vídeo e a velocidade com que a estação de trabalho recebe esse vídeo da rede.

tarefa agendada	Uma tarefa agendada é um tipo de entidade que define uma ação que é executada automaticamente em data e hora específicas ou de acordo com uma agenda recorrente.
token de segurança	Uma representação física das declarações assinada criptograficamente pelo emissor, fornecendo prova às partes necessárias em relação à integridade das declarações e à identidade do emissor.
tarefa	Uma tarefa é o conceito central em que toda a interface do usuário do Centro de Segurança está construída. Cada tarefa corresponde a um aspecto do seu trabalho como profissional de segurança. Por exemplo, use uma tarefa de monitoramento para monitorar os eventos do sistema em tempo real, use uma tarefa de investigação para descobrir padrões de atividade suspeita ou use uma tarefa de administração para configurar seu sistema. Todas as tarefas podem ser personalizadas e várias tarefas podem ser executadas ao mesmo tempo.
Tempo e comparecimento	É um tipo de tarefa de investigação que relata quem estava dentro de uma área selecionada e a duração total de sua estadia em determinado intervalo de tempo.
Transmission Control Protocol	Um conjunto de regras (protocolo) focado em conexões que, juntamente com o IP (Internet Protocol), é usado para enviar dados através de uma rede IP. O protocolo TCP/IP define como os dados podem ser transmitidos de forma segura entre redes. TCP/IP é o padrão de comunicação mais largamente usado e é a base da Internet.
Transport Layer Security	Transport Layer Security (TLS) é um protocolo que fornece privacidade de comunicações e integridade de dados entre dois aplicativos que se comunicam através de uma rede. Quando um servidor e um cliente se comunicam, o TLS garante que nenhum terceiro possa interceptar ou modificar nenhuma mensagem. TLS é o sucessor do Secure Sockets Layer (SSL).

U

unidade de controle de acesso	É um tipo de entidade que representa um dispositivo de controle de acesso inteligente, como um aparelho Synergis™ ou um controlador de rede HID, que se comunica diretamente com o Access Manager por uma rede IP. Uma unidade de controle de acesso opera de modo autônomo quando está desconectada do Access Manager.
usuário autorizado	É um usuário que pode ver (tem o direito de acessar) as entidades em uma divisão. Os usuários podem apenas exercer seus privilégios nas unidades que podem ver.
Unidade de processamento AutoVu™ LPR	A Unidade de processamento AutoVu™ LPR é o componente de processamento do sistema SharpX. A Unidade de

	processamento LPR é disponibilizada com duas ou quatro portas de câmera, com um processador dedicado por câmera (usando SharpX) ou por duas câmeras (usando SharpX VGA). Isto garante o máximo desempenho de processamento por câmera. A Unidade de processamento LPR é por vezes apelidada de *unidade de porta-malas*, porque é normalmente instalada no porta-malas de um veículo.
Utilitário de resolução de conflito	É uma ferramenta que ajuda a resolver os conflitos causados ao importar usuários e titulares de cartão de um Diretório Ativo.
Uso diário por Patroller	Uso diário por Patroller é um tipo de tarefa de investigação que relata as estatísticas de uso diário de um veículo de patrulha selecionado (tempo de operação, paragem mais longa, número total de paragens, desligamento mais longo e assim por diante) em um determinado intervalo de datas.
unidade de detecção de invasão	Uma unidade de detecção de intrusão é uma entidade que representa um dispositivo de intrusão (painel de intrusão, painel de controle, receptor e assim por diante) que é monitorado e controlado pela função Gerenciador de intrusão.
Unidade de LPR	Uma Unidade de LPR é um dispositivo que captura números de placas de veículo. Uma Unidade de LPR inclui normalmente uma câmera de LPR e uma câmera de contexto. Essas câmeras podem ser incorporadas à unidade ser externas a ela.
unidade Sharp	A unidade Sharp é uma unidade de LPR proprietária da Genetec Inc. que integra componentes de captura e processamento de placa de veículo, bem como funções de processamento de vídeo digital, envolvidas em um estojo robusto.
Unidade Synergis™	A unidade Synergis™ é um dispositivo Synergis™ inscrito como uma unidade de controle de acesso no Security Center.
unidade	É um dispositivo de hardware que se comunica por uma rede IP que pode ser diretamente controlada por uma função do Centro de Segurança. Distinguimos quatro tipos de unidades no Centro de Segurança: • Unidades de controle de acesso, gerenciadas pela função de Gerenciador de Acesso • Unidades de vídeo, gerenciada pela função do Archiver • Unidades LPR, gerenciadas pela função de Gerenciador de LPR • Unidades de detecção de invasão, gerenciadas pela função de Gerenciador de Invasão
usuário	É um tipo de entidade que identifica uma pessoa usa os aplicativos do Security Center e define os direitos e os privilégios que a pessoa tem no sistema. Os usuários podem ser criados manualmente ou importados de um Active Directory.

unidade de vídeo

Uma unidade de vídeo é um tipo de dispositivo de codificação e decodificação de vídeo capaz de comunicar-se por uma rede IP e pode incorporar um ou mais decodificadores de vídeo. Os modelos de codificação de ponta também incluem suas próprias capacidades analíticas de vídeo e gravação. Câmeras (com IP ou analógicas), codificadores e decodificadores de vídeo são exemplos de unidades de vídeo. No Security Center, uma unidade de vídeo se refere a um tipo de entidade que representa um dispositivo de codificação ou decodificação de vídeo.

V

visualização da área

É uma visualização que organiza as entidades usadas normalmente, como porta, câmeras, plugin de ladrinho, áreas de detecção de invasão, zonas, etc, por áreas. Esta visualização é criada basicamente para o trabalho diário dos operadores de segurança.

vídeo não sincronizado

É um tipo de entidade que representa qualquer objeto de valor com uma etiquet RFID, permitindo assim er rastreada por um software de gestão de bens.

Vinculação de I/O

A vinculação de entrada e saída controla o relé de saída com base no estado combinado (normal, ativo ou com problema) de um grupo de entradas monitoradas. Uma aplicação padrão é tocar uma buzina (por um relé de saída) quando qualquer janela no andar térreo de um edifício seja rompida (supondo que cada janela seja monitorada por um sensor de "quebra de vidro" conectado a uma entrada).

visualização de mapa

Uma visualização de mapa é uma seção definida de um mapa.

visualização de rede

A visualização de rede é um navegador que ilustra seu ambiente de rede ao mostrar cada servidor na rede a que pertence.

veículo de patrulha

Um veículo de patrulha monitora estacionamentos e ruas urbanas em busca de violações de estacionamento e viaturas procuradas. Um veículo de patrulha inclui uma ou mais câmeras de reconhecimento automático de placas de veículos (ALPR) Sharp e um computador de bordo executando software Genetec Patroller™.

vídeo sincronizado

é um vídeo ao vivo ou de reprodução simultâneo de mais de uma câmera que está sincronizada.

Vídeo

A tarefa *Vídeo* é uma tarefa administrativa que permite configurar funções de gerenciamento, unidades, monitores analógicos e câmeras de vídeo.

vigilante

é um serviço do Centro de Segurança instalado no serviço do Genetec Server em todo computador servidor. O vigilante

	monitora o serviço Genetec Server e reinicia-o, caso condições anormais sejam detectadas.

W

Web Client	Você pode fazer logon no Security Center Web Client pelo seu navegador da Internet para monitorar vídeo, investigar eventos relacionados à atividade de portas, procurar e investigar alarmes atuais e passados, visualizar e gerenciar titulares de cartão, visitantes, grupos de titulares de cartão e credenciais. Seu administrador de sistema deve criar uma função de Web Client Server no Security Center, que define o endereço do Web Client (URL).
Web Map Service	Web Map Service (WMS) é um protocolo padrão de distribuição de imagens de mapas georreferenciados pela Internet, que são geradas por um servidor de mapas usando dados de um banco de dados GIS.
widget	Componente da interface gráfica do usuário (GUI) com o qual o usuário interage.
Windows Communication Foundation	Windows Communication Foundation (WCF) é uma arquitetura de comunicação usada para habilitar aplicativos, em uma máquina ou em várias máquinas conectadas por uma rede, a se comunicar. O Genetec Patroller™ usa WCF para comunicação sem fio com o Security Center.

Z

zona de hardware	Uma zona de hardware é um tipo de zona onde o vínculo de E/S é feito por uma única unidade de controle de acesso. Uma zona de hardware funciona independentemente do Access Manager e, consequentemente, não pode ser ativada ou desativada pelo Security Desk.
Zona de E/S	Uma zona de E/S é uma entidade de zona na qual a ligação E/S pode ser distribuída a várias unidades Synergis™, enquanto uma unidade age como a unidade principal. Todas as unidades Synergis™ envolvidas em uma zona de E/S devem ser gerenciadas pelo mesmo Access Manager. A zona I/O trabalha independentemente do Access Manager, mas para de funcionar se a unidade mestra está desativada. Uma zona de E/S pode ser ativada e desativada pelo , desde que a unidade mestre esteja online.
zona de movimento	É uma área definida pelo usuário em uma imagem de vídeo onde o movimento deve ser detectado.

zona de estacionamento	As zonas de estacionamento que você define no Security Center representam estacionamentos fora da rua cujas entradas e saídas são monitoradas por câmeras Sharp.
zona virtual	Uma zona virtual é um tipo de zona onde o vínculo de E/S é feito pelo software. Os dispositivos de entrada e saída podem pertencer a diferentes unidades de diferentes tipos. Uma zona virtual é controlada pelo Zone Manager e somente funciona quando todas as unidades estão online. Ela pode ser armada e desarmada pelo Security Desk.
zona	É um tipo de entidade que monitora um conjunto de entradas e dispara eventos com base nos estados combinados. Esses eventos podem ser usados para controlar relés de saída.

Onde encontrar informações do produto

É possível encontrar a documentação do nosso produto nos seguintes locais:

- **Hub TechDoc da Genetec™:** Os documentos atualizados estão disponíveis no TechDoc Hub. Para acessar o TechDoc Hub, acesse o Genetec™ Portal e clique em TechDoc Hub. Não conseguiu achar o que estava procurando? Entre em contato pelo e-mail documentation@genetec.com.
- **Pacote de instalação:** O guia de instalação e as notas da versão estão disponíveis na pasta "Documentação" do pacote de instalação. Alguns dos documentos também têm um link de download direto para a última versão do documento.
- **Ajuda:** Security Center as aplicações com base na Web e clientes incluem ajuda, que explica como o produto funciona e dá instruções sobre como usar os recursos do produto. Para acessar a ajuda, clique em **Ajuda**, pressione F1, ou toque o **?** (ponto de interrogação) nos diferentes aplicativos clientes.

Suporte técnico

A Central de Assistência Técnica Genetec™ (GTAC) está comprometida em fornecer à sua clientela mundial os melhores serviços de assistência técnica disponíveis. Como cliente da Genetec Inc., você tem acesso ao TechDoc Hub, onde é possível encontrar informações e procurar por respostas às suas dúvidas sobre produtos.

- **Hub TechDoc da Genetec™:** Encontre artigos, manuais e vídeos que respondam às suas perguntas ou ajudem você a resolver problemas técnicos.

  Antes de contatar a GTAC ou abrir um chamado de assistência, é recomendável procurar no TechDoc Hub por possíveis correções, soluções alternativas ou problemas conhecidos.

  Para acessar o TechDoc Hub, acesse o Genetec™ Portal e clique em TechDoc Hub. Não conseguiu achar o que estava procurando? Entre em contato pelo e-mail documentation@genetec.com.

- **Centro de Assistência Técnica Genetec™ (GTAC):** Os modos de contatar a GTAC estão descritos nos documentos de gestão do ciclo de vida Genetec™: Genetec™ Assurance Description e Genetec™ Advantage Description.

Recursos adicionais

Se você precisar de recursos adicionais além da Central de Assistência Técnica Genetec™, os seguintes estão disponíveis:

- **Fórum:** O fórum é um aplicativo de mensagens fácil de usar que permite aos clientes e funcionários da Genetec Inc. se comunicarem e discutirem uma variedade de tópicos, desde questões técnicas a dicas de tecnologia. É possível se registrar ou entrar em https://gtapforum.genetec.com.
- **Treinamento técnico:** Em um ambiente de sala de aula profissional ou na conveniência de seu próprio escritório, nossos treinadores qualificados podem orientá-lo sobre o projeto do sistema, instalação, operação e solução de problemas. Os serviços de treinamento técnico são oferecidos para todos os produtos e para clientes com nível variado de experiência técnica, podendo ser personalizado para atender suas necessidades e objetivos específicos. Para mais informações, vá para http://www.genetec.com/support/training/training-calendar.

Licença

- Para ativação ou redefinição da licença, entre em contato com o GTAC em https://gtap.genetec.com.
- Para questões de conteúdo de licença ou números de peça ou problemas com um pedido, entre em contato com o atendimento ao cliente Genetec™ em customerservice@genetec.com, ou ligue para 1-866-684-8006 (opção 3 - nos EUA).
- Se você precisar de uma licença de demonstração ou tiver perguntas sobre preços, entre em contato com o departamento de vendas Genetec™ em sales@genetec.com ou ligue para 1-866-684-8006 (opção 2 - nos EUA).

Problemas e defeitos com produtos de hardware

Entre em contato com a GTAC em https://gtap.genetec.com para resolver qualquer problema relacionado aos aparelhos Genetec™ ou qualquer hardware adquirido por intermédio da Genetec Inc..