Manual do usuário

DEFENSE IA 3.2

Defense IA 3.2

Sistema de operação

Parabéns, você acaba de adquirir um produto com a qualidade e segurança Intelbras.

Este manual do usuário apresenta as funções e operações do centro de gerenciamento de vigilância geral do Defense IA e operações do cliente.

O manual é atualizado regularmente, caso não encontre algum conteúdo específico, verifique se possui a última versão disponível.

Cuidados e segurança

Os seguintes símbolos abaixo com significados definidos na tabela podem aparecer durante o manual.

Símbolo	Significado
	Indica um perigo de alto potencial que, se não for evitado, resultará em problemas graves no sistema.
	Indica um perigo de médio ou baixo potencial que, se não for evitado, pode resultar em problemas moderados.
	Indica um potencial risco que, se não for evitado, pode resultar em danos à máquina, perda de dados, queda de desempenho ou resultado imprevisível.
	Fornece métodos para ajudá-lo a resolver um problema ou economizar seu tempo.
	Fornece informações adicionais como ênfase e/ou suplemento ao texto.

Aviso de proteção de privacidade

» Como usuário do dispositivo ou controlador de dados, você pode coletar dados pessoais de terceiros, como rosto, impressões digitais, número da placa do carro, endereço de e-mail, número de telefone, GPS e assim por diante. Você precisa estar em conformidade com as leis e regulamentos locais de proteção de privacidade para proteger os direitos e interesses legítimos de outras pessoas implementando medidas que incluem, mas não se limitam a: fornecer identificação clara e visível para informar o titular dos dados sobre a existência de área de vigilância e fornecer informações relacionadas de contato com a empresa.

» LGPD – Tratamento de dados pela Intelbras: este produto faz tratamento de dados pessoais, porém a Intelbras não possui acesso aos dados a partir deste produto.

» LGPD - Segurança do produto no tratamento de dados: este produto possui criptografia no armazenamento dos dados pessoais.

Sobre o manual

» O manual é apenas para referência. Se houver inconsistência entre o manual e o produto real, o produto real prevalecerá. Não nos responsabilizamos por quaisquer perdas causadas por operações que não estejam de acordo com o manual.

» O manual será atualizado de acordo com as leis e regulamentações mais recentes das regiões relacionadas. Para obter informações detalhadas, consulte o manual no nosso site: *www.intelbras.com.br.* Se houver inconsistência entre manuais em papel e a versão eletrônica, a versão eletrônica prevalecerá.

» Todo o software está sujeito a alterações sem aviso prévio por escrito. As atualizações do produto podem causar algumas diferenças entre o produto real e o manual. Contate o serviço de apoio ao cliente para obter informações referentes as versões mais recentes e documentações complementares.

» Ainda pode haver desvio nos dados técnicos, descrição de funções e operações ou erros na impressão. Se houver qualquer dúvida ou disputa, consulte nossa explicação final.

» Atualize o software do leitor de PDF ou tente outro software do leitor de PDF se o manual (em formato PDF) não puder ser aberto.

» Todas marcas comerciais, marcas registradas e os nomes das empresas no manual são de propriedade dos respectivos proprietários.

» Visite nosso site, entre em contato com o fornecedor ou atendimento ao cliente se houver algum problema ocorrido ao usar o software.

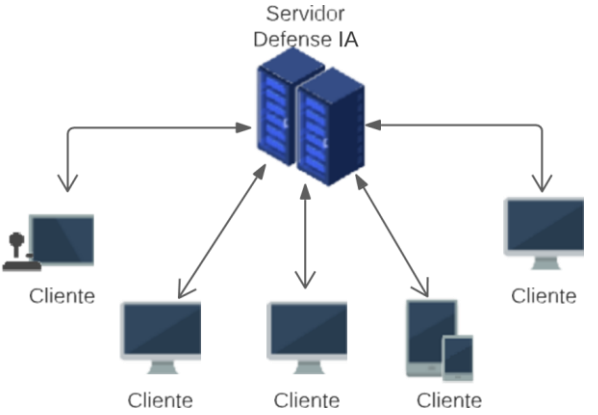
» Se houver alguma incerteza ou controvérsia, consulte nossa explicação final.

Índice

1. Produto

Defense IA é o software Intelbras de gerenciamento centralizado de segurança; o sistema dispõe interfaces de controle para monitoramento de vídeo, controle de acesso, eventos e alarmes, administração de dispositivos, recursos de Inteligência Artificial, entre outras funcionalidades que compõem o ecossistema de segurança.

Baseado em uma estrutura cliente-servidor, o Defense IA apresenta uma arquitetura de rede descentralizada, ou seja, múltiplos clientes podem se conectar ao servidor central, acessando seus serviços e recursos.



Isso torna a estrutura de informação escalável e eficiente, permitindo a distribuição da execução de tarefas entre múltiplos dispositivos enquanto apresenta a centralização da utilização de recursos para gerenciamento e processamento de serviços.

O Defense IA é projetado com uma grande capacidade de expansão, portanto, uma de suas prin- cipais características é o crescimento horizontal, permitindo a implantação de sistemas com até
20.000 canais de monitoramento e capacidade de armazenamento de até 4 PB. Além de todas suas funcionalidades, você também pode solicitar customizações que atendam às suas necessidades, construindo assim um ambiente só seu.

2. Instalação e implantação

A plataforma do Defense IA permite tipos diferentes de implantação durante sua instalação, são essas, implantação de servidor único, distribuída, de estrutura N+M, de alta disponibilidade e mapeamento LAN para WAN.

2.1. Requisitos do servidor

Parâmetros	Requisitos de Hardware	Sistema Operacional
Configuração	CPU: Intel® Xeon® Silver 4310T @ 2.3 GHz 10 núcleos	
Recomendada	RAM: 16 GB	Windows Server 2016
	Interface de Rede: 4x portas Ethernet @ 1000 Mbps	Windows Server 2019
	Armazenamento: SSD/HDD Classe Enterprise 1 TB @ 7200 RPM	Windows Server 2022
	Espaço Livre: 500 GB	
Configuração Mínima	CPU: Intel® Xeon® E-2224 @ 3.4 GHz 4 núcleos RAM: 8 GB disponível Interface de Rede: 2× portas Ethernet @ 1000 Mbps Armazenamento: HDD Classe Enterprise 1 TB @ 7200 RPM Espaço Livre: 500 GB	Windows 10 - 64 bit

Imagens de reconhecimento facial, vídeos, e arquivos não podem ser armazenados no disco do sistema e no diretório de instalação do Defense IA. É recomendado o uso de discos de rede para isso.

Para melhor performance, é recomendado adicionar discos extras para armazenamento de imagens.

2.2. Requisitos do cliente

Parâmetros	Requisitos de Hardware	Sistema Operacional
Configuração recomendada	CPU: Intel® Core™ i7 7700 4 Core™ RAM: 16 GB GPU: NVIDIA GTX 1660 @ 6Gb RAM Armazenamento: SSD para pasta de instalação do Defense IA Espaço Livre: 200 GB	Windows 10 - 64 bit

Verifique a ficha técnica do Defense IA para maiores informações sobre especificações do cliente.
Encontre-a em nosso site: *www.intelbras.com.br*

2.3. Implantação de servidor único

Essa estrutura é recomendada para projetos envolvendo um menor números de dispositivos, dessa forma, apenas um servidor Defense IA é necessário.

Instalação de servidor único

» Execute o instalador do Defense IA

O nome do instalador inclui a versão e data, confirme-os antes da instalação.

» Clique em Termos de aceite do DEFENSE IA para ler os termos de contrato e selecione a checkbox para aceitá-los, e então clique em *Avançar.*

» Selecione Principal como tipo de servidor e clique em *Avançar* (caso opte por utilizar o algorítmo InSearch, selecione a checkbox abaixo para instalá-lo).

» Selecione o diretório de instalação clicando em *Navegar,* deixe habilitada a checkbox para gerar um atalho na área de trabalho e clique em *Instalar.*

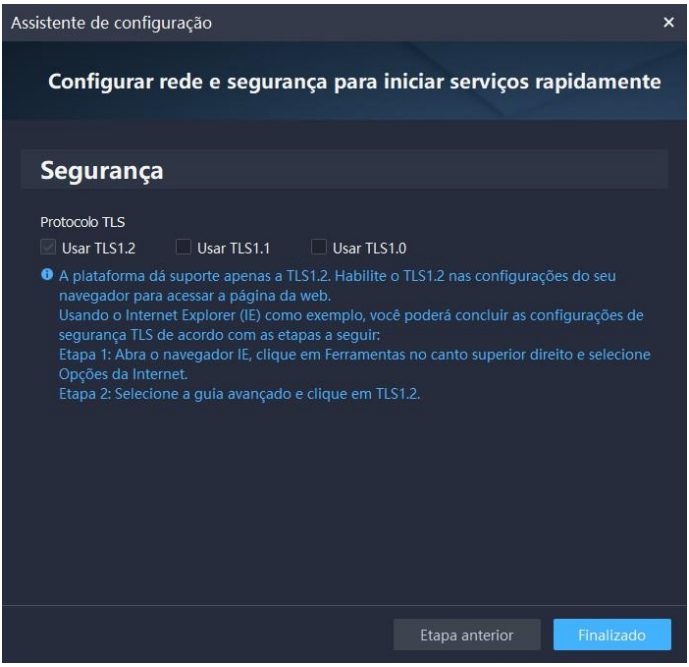
Verifique se o local de instalação cumpre os requisitos de espaço disponível.

O processo de instalação deve demorar de 4 a 8 minutos. Não feche o programa ou desligue o computador.

» Após a instalação, clique em *Executar* para continuar para a etapa de configuração.

» Selecione uma interface de rede para o servidor do Defense IA, e clique em *Próxima etapa.*

Caso o servidor possua mais de uma interface de rede, você pode configurar ambas interfaces clicando em *Modo NIC duplo.* Desta forma, você pode acessar dispositivos em 2 segmentos de rede diferentes



» Durante etapa final, ative ou desative o TLS 1.0 ou 1.1 se necessário. Clique em *Finalizado* para finalizar o processo de instalação e executar os serviços.

TLS 1.0 possui vulnerabilidades conhecidas, é recomendável desativá-lo, porém isso torna a página web inacessível pelo navegador. Você deve habilitar TLS 1.1 e 1.2 nas configurações do navegador para acessar a página web.

Se a memória RAM disponível for inferior a 8 GB, apenas serviços básicos de vídeo serão iniciados. Caso seja inferior a 6 GB, nenhum serviço será iniciado.

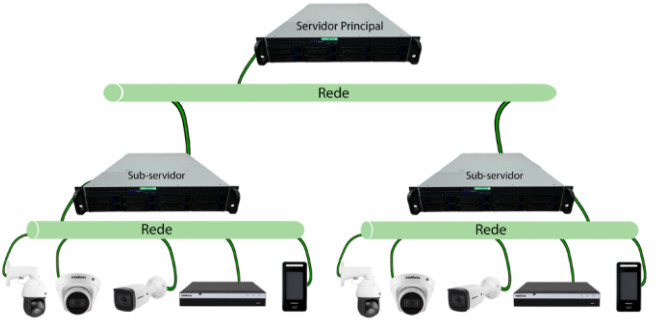
Atualizar e desinstalar

» Para atualizar o sistema, instale normalmente a nova versão. A plataforma automaticamente cobrirá a versão anterior.

» Para desinstalar a plataforma, acesse o diretório de instalação e siga para *"..\Defense IA\Defense IA Server\uninstall\uninst.exe".* Siga as instruções do executável para desinstalar.

2.4. Implantação distribuída

Essa estrutura é recomendada para projetos médios e grandes. Sub-servidores são utilizados para compartilhar a carga do sistema, para que assim mais dispositivos possam ser acessados. Os sub-servidores se conectam ao servidor principal, e este, centralizado, administra-os. Até 10 sub-servidores podem se conectar a um servidor principal.



Instalação do servidor principal

Para instalação do servidor principal, veja o capítulo *Instalação de servidor único.* Após a instalação do servidor principal, os sub-servidores podem ser instalados e seus status visualizados pelo cliente.

A arquitetura do Defense recomenda que os servidores estejam na mesma rede e que não possua nenhum interferencia ou oscilação.

Instalação de servidor auxiliar

» Execute o instalador do Defense IA

O nome do instalador inclui a versão e data, confirme-os antes da instalação.

» Clique em Termos de aceite do DEFENSE IA para ler os termos de contrato e selecione a checkbox para aceitá-los, e então clique em *Avançar.*

» Selecione Sub Servidor como tipo do servidor e clique em *Avançar.*

» Selecione o diretório de instalação clicando em *Navegar,* deixe habilitada a checkbox para gerar um atalho na área de trabalho e clique em Instalar.

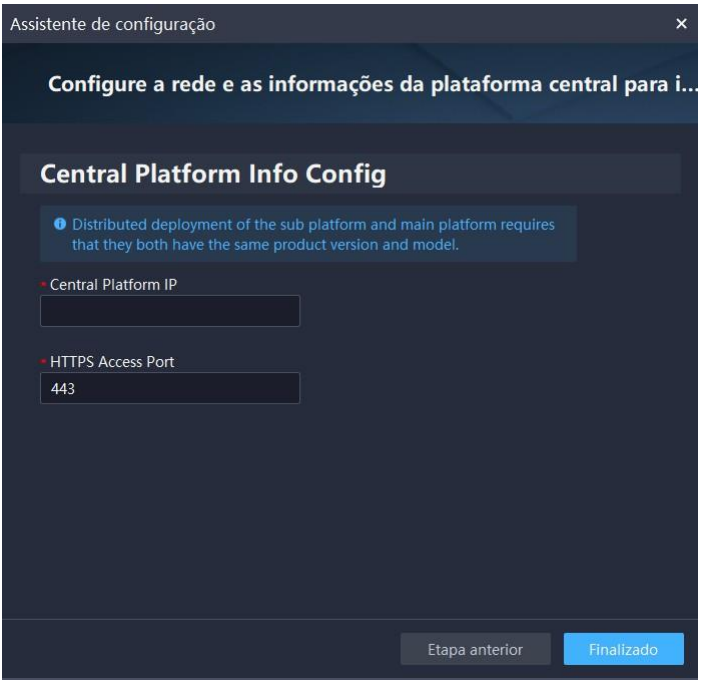
Verifique se o local de instalação cumpre os requisitos de espaço disponível.

O processo de instalação deve demorar de 4 a 8 minutos. Não feche o programa ou desligue o computador.

» Após a instalação, clique em *Executar* para continuar para a etapa de configuração.

» Selecione uma interface de rede para o servidor do Defense IA, e clique em *Próxima etapa.*

Caso o servidor possua mais de uma interface de rede, você pode configurar ambas interfaces clicando em *Modo NIC duplo.* Desta forma, você pode acessar dispositivos em 2 segmentos de rede diferentes



» Configure o endereço IP e porta do servidor principal a se conectar, e então clique em *Finalizado* para finalizar a instalação.

Depois de instalar o servidor auxiliar, você deve habilitá-lo acessando o cliente pelo servidor principal para que funcione corretamente. Veja como configurá-lo em *Configurações Iniciais de Aplicativos >Implantação.*

Implantação de estrutura M+N

Utilizando essa estrutura, é possível configurar um servidor standby para cada servidor auxiliar a fim de mais estabilidade.

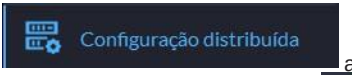
Quando um servidor auxiliar apresenta uma falha de funcionamento, o sistema o substitui por um em espera; assim que o servidor auxiliar originalmente ativo normalizar, é possível manualmente retorná-lo como ativo. A configuração da estrutura é feita pelo cliente após pelo menos 2 servidores auxiliares configurados.

Veja o capítulo *Instalação e configuração do cliente* para instalar o cliente e ter acesso às configurações do sistema.

» No cliente, clique em  , em seguida em Implantação 

.

»

» Na aba configuração distribuída 

ative os servidores auxiliares e acesse as configurações de um deles clicando na engrenagem 
.

» Selecione o tipo de servidor como servidor auxiliar, clique em *OK* no fim da página.

» Realize a mesma operação para o segundo servidor, desta vez selecione o tipo de servidor como servidor standby.

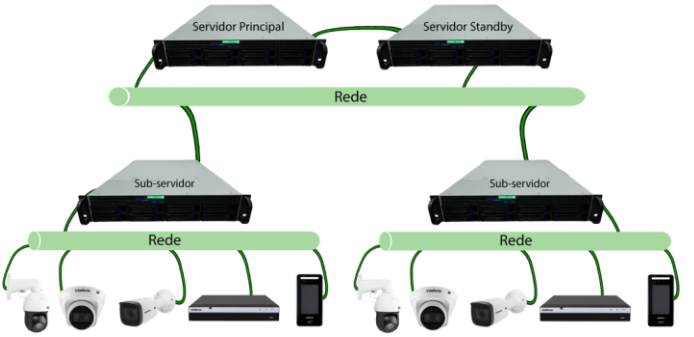
» Ao selecionar o tipo de servidor como standby, a lista de servidores auxiliares será atualizada, selecione o servidor o qual deseja acompanhar.

Esta operação pode ser realizada múltiplas vezes, baseando-se no número recomendado de 10 servidores auxiliares ativos.

Verifique a ficha técnica do Defense IA para maiores informações sobre especificações de servidor. Encontre-a em nosso site: *www.intelbras.com.br*

2.5. Implantação de alta disponibilidade

Essa estrutura é recomendada para projetos que necessitam de alta disponibilidade dos serviços. O servidor secundário assume o gerenciamento quando o principal apresenta uma falha de funciona- mento. É possível retornar o gerenciamento ao servidor originalmente ativo após sua recuperação.

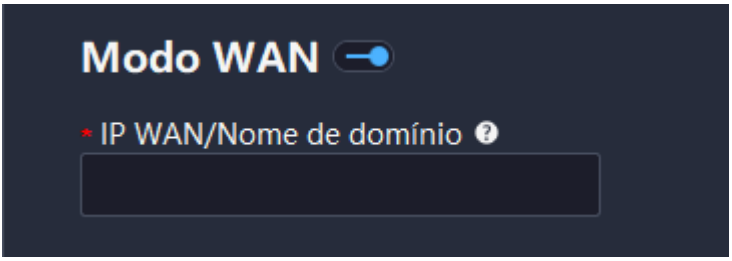


2.6. Implantação de mapeamento LAN para WAN

Caso queira acessar os serviços via uma rede WAN, o roteador deve ser configurado, mapeando as portas de acordo. A lista de portas pode ser encontrada em nosso site.

Se a plataforma está configurada numa rede LAN, é possível mapear o endereço IP para uma rede WAN ou um nome de domínio, e assim, acessar a plataforma.

» Durante a instalação ou acessando a interface do Defense IA Server pelo aplicativo e então, as configurações de rede clicando na engrenagem no canto superior direito.



» Insira um endereço de IP WAN fixo ou nome de domínio no campo vazio e clique em *OK*. Os serviços reiniciarão.

3. Configurações básicas

Antes de utilizar o sistema, configure as funções básicas, incluindo a instalação do cliente, ativação do sistema, organização e gerenciamento de dispositivos, usuários e armazenamento.

3.1. Instalação e configuração do cliente

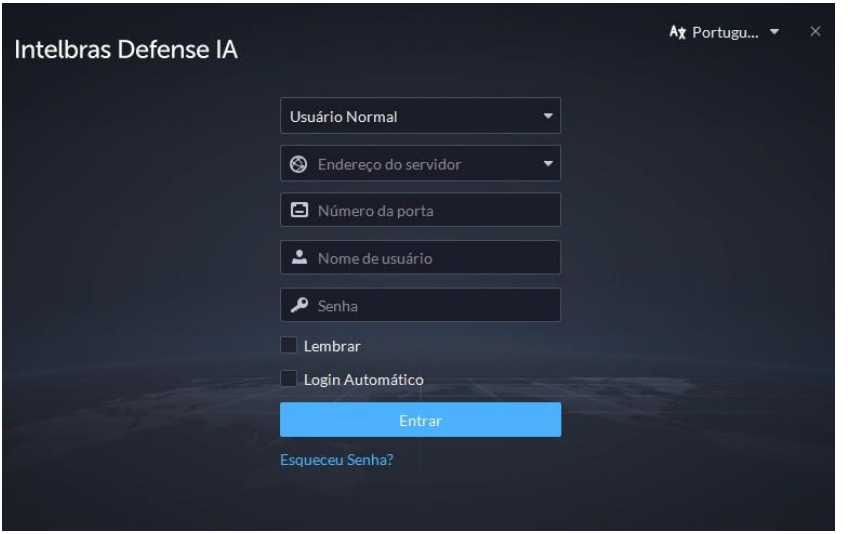
Para baixar o instalador do cliente, acesse a página web do servidor pelo navegador utilizando o endereço IP configurado, ou nome de domínio. Clique no ícone do Windows em PC para iniciar o download.

Após baixado, execute o instalador e siga as instruções para instalar e configurar o Cliente.

Caso não seja possível acessar a página web, verifique se está utilizando *https://* junto ao endereço de acesso.

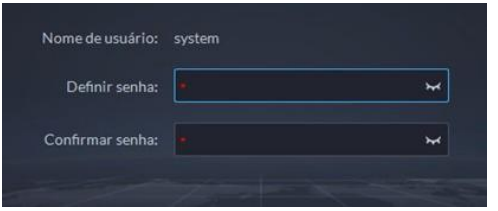
Primeiro acesso à plataforma

Para o primeiro acesso à plataforma, você deve cadastrar uma senha para o usuário system, usu- ário padrão do sistema. Este apresenta permissões de configuração de super administrador do sistema.



O idioma padrão do Defense IA é inglês e pode ser alterado pela lista suspensa presente na direita superior da interface. Suporta Português (BR) e Espanhol.

Para cadastrar a senha, insira o endereço e porta do servidor em seus respectivos campos, ou selecione o servidor a partir da lista suspensa, caso este apareça. Após isso você será diretamente encaminhado para o cadastro da senha.

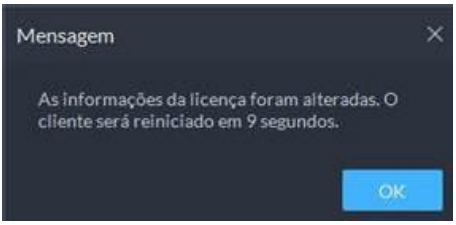


Siga as recomendações e cadastre uma senha complexa para maior segurança. Uma senha forte é composta por caracteres maiúsculos e minúsculos, numerais e caracteres especiais.

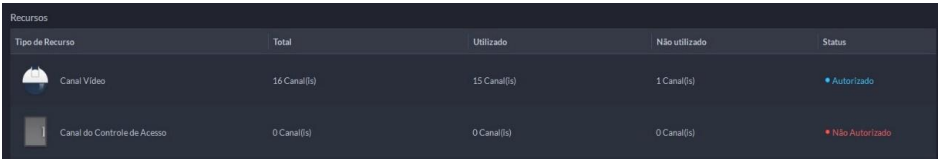
3.2. Licenciamento

Após primeiro acesso ao cliente, suas funções devem estar indisponíveis, uma vez que este ainda não foi licenciado. Para realizar o licenciamento, acesse o menu de configurações à esquerda da tela, e então, o menu de configurações da licença.

Acessando o menu, escolha a opção de ativação desejada (on-line ou off-line) e siga as instruções apresentadas para ativação da licença. Após ativação, o cliente reiniciará automaticamente, e ao realizar o login novamente, as funções licenciadas serão habilitadas.



Você pode verificar as informações da licença no menu de configurações da licença, onde é apresentado o recurso total disponibilizado pela licença ativada, o total já consumido e o total disponível para uso. Além disso, também é possível verificar se um módulo está ou não Autorizado para uso.

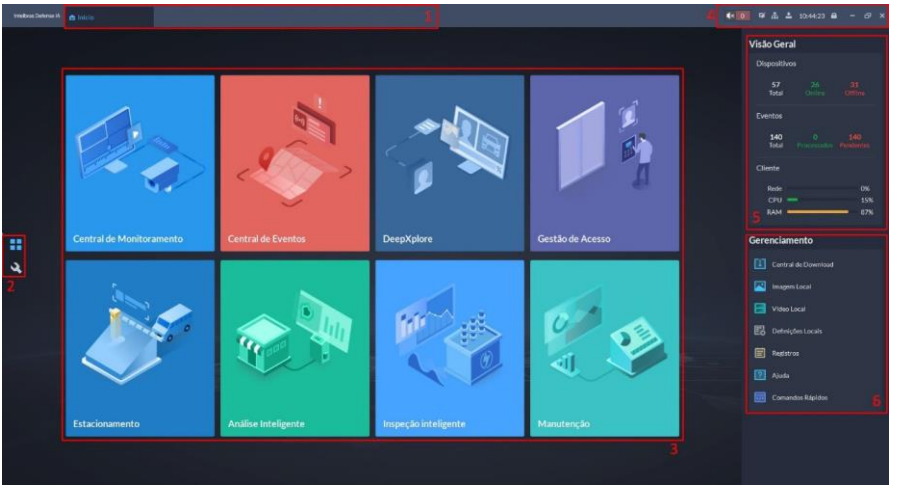


Importante:

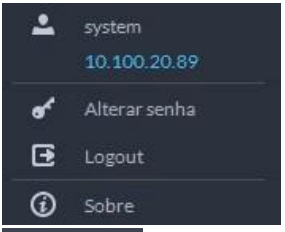
Vale ressaltar que os dispositivos de controle de acesso ou portaria que possuem streaming de vídeo, irão consumir licenças de canal de video dentro da plataforma. Somatizando com dispositivos de CFTV como câmeras Ips, gravadores, etc.

3.3. Menu principal

A interface inicial do Defense IA pode ser dividida em 6 partes para interação com o usuário. A imagem e tabela abaixo apresentam detalhes.



Alguns módulos necessitam de licenças e permissões específicas para visualização. Verifique se o usuário de utilização possui as permissões necessárias e as devidas licenças estão ativadas.

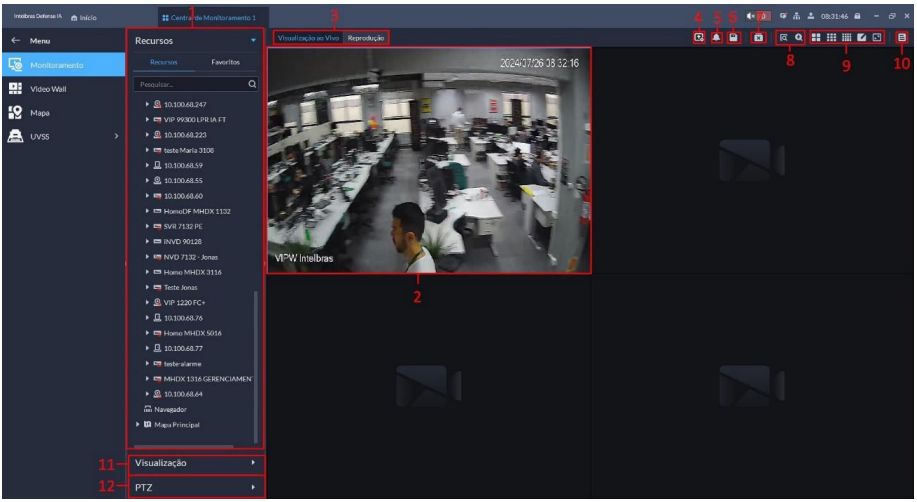
Índice	Definição	Detalhes
1	Aba de navegação	Aba em que as guias de navegação entre aplicativos abertos podem ser acessadas.
2	Alteração entre menus	Botões para alternar entre menus de aplicativos  e configurações  destes.
3	Aplicativos	Janelas de aplicativos de monitoramento, suas respectivas configurações são feitas no menu de configurações.
4	Ícones de gerenciamento	 Botão para ativar/desativar sons do sistema.  Apresenta o número de eventos não tratados.  Atalho para a central de notificações.  Botão para adicionar outro servidor (multi-site).  Botão para acessar atalhos de gerenciamento do sistema, como:   Horário do sistema do cliente.  Botão para bloquear o cliente.  Configurações gerais da janela.
5	Visão geral do sistema	Informações sobre a carga e capacidade do sistema, apresentando dados sobre o número de dispositivos integrados ao sistema, eventos gerados, e processamento computacional do cliente.
6	Gerenciamento do sistema	Botões de acesso a pastas, gerenciamento, configurações do sistema e links externos.

3.4. Central de Monitoramento

A Central de monitoramento fornece aplicativos integrados de monitoramento em tempo real para cenários como o centro de CFTV. A plataforma suporta vídeo ao vivo, reconhecimento de placas, detecção de alvos, controle de acesso, e-map, instantâneos, eventos, reprodução de vídeo, Video Wall e muito mais.

3.4.1 Página principal

Fornece funções usadas com frequência, como vídeo, evento e alarme. Faça login no cliente Intel- bras Defense IA. Na página inicial, clique em e selecione Central de Monitoramento.

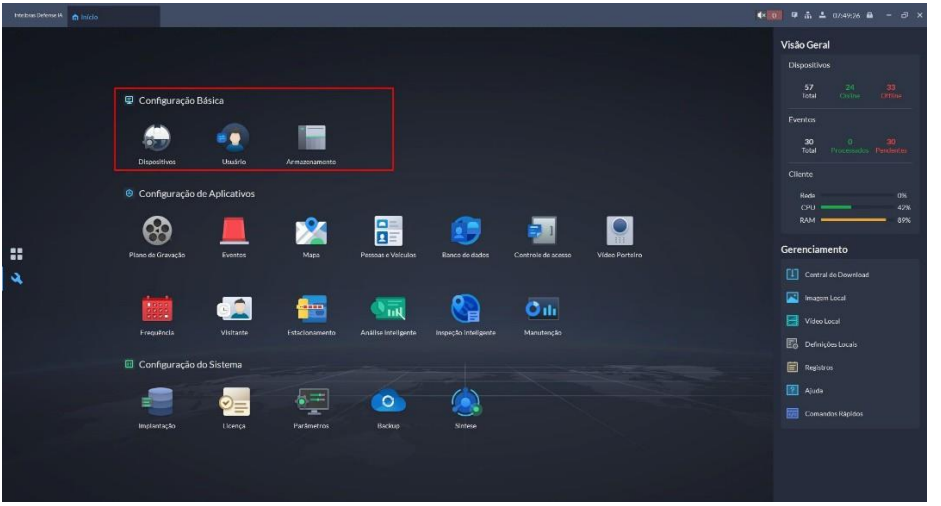


Índice	Parâmetro	Descrição
1	Favorito e árvore de dispositivo	Lista de Recursos, incluindo dispositivos, navegador e mapas Você pode procurar um dispositivo ou canal de no campo de pesquisa. A pesquisa difusa é suportada para qe você possa simplesmente inserir parte do nome e selecionar o nome exato na lista de nomes fornecida. Adicione, exclua ou renomeie os favoritos. Você também pode visitar os canais nos favoritos
2	Visualização ao Vivo	Arraste um canal para as janelas e veja seu vídeo em tempo real.
3	Visualização e Reprodção ao vivo	Visualização ao vivo: visualize vídeos em tempo real. Reprodução: visualize vídeos gravados.
4	Enviar videos para o Video Wall	Os vídeos vídeos em tempo real que estão abertos no momento podem ser exibidos rapidamente em um Video Wall. Você deve configurar um Vídeo Wall antes de usar esta função
5	Defina janleas de alarmes em lotes	Defina todas as janelas como janelas de alarme. Depois de selecionar “Abrir vídeo de ligação de alarmes em visualização ao vivo” em Configurações locais > Alarme, os vídeos de alarme serão exibidos nas janelas de alarme . Se o número de alarmes for menor que o de vídeos de ligação, o vídeo vinculado ao alarme acionado mais cedo será aberto.
6	Salvar visualização	Salve todos os canais o sites abertos em uma visualização para que você possa abri-los rapidamente mais tarde.
7	Fechar todas as janelas	Fecha todas as janelas em visualização ao vivo.
8	Pesquisar por alvos no vídeo	A plataforma suporta a seleção manual de alvos e o reconhecimento automático de alvos no vídeo e em seguida, a busca rápida no DeepXplore. Para obter detalhes, consulte Selecionando e pesquisando o Alvo manualmte e InSearch.

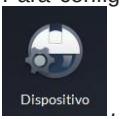
9	Modo de divisão de janela e tela cheia	Defina um mode de divisão de janela. Suporta 1, 4, 6, 8, 9, 13, 16, 20, 25, 36 ou 64 divisões ou clique para definir um modo de divisão personalizado. Se o número do canal de visualização ao vivo for maior que o número de janelas atuais, você poderá virar a(s) página(s) clicando na parte inferior da página. Mude a janela de víde para o modo Tela Cheia. Para sair da Tela cheia, você pode pressionar a tecla Esc ou clicar com o botão direito no vídeo e selecionar Sair da Tela inteira.
10	Botão Painel de evento	Exiba ou Oculte o Painel de eventos.
11	Visualização	Salve a visualização atual da divisão da janela e dos canis de vídeo na seção de visualização ao vivo e dê um nome à visualização . Você pode selecionar diretamente a visualização na guia exibi-la rapidamente na próxima vez. Os canais em uma visualização ou grupo de visualização podem ser exibidos passeio (por sua vez). Você pode definir o intervalo do tour como 10 s, 30 s, 1 min, 2 min, 5 min ou 10 min. Podem ser criadas no máximo 100 visualizações.
12	PTZ	Se o canal do qual você está visualizando o vídeo ao vivo for de uma câmera PTZ, você poderá controlá-lo através do painel de controle.

3.4.2 Menu de configurações

Acessando o menu de configurações  , apresentado pelo índice 2 na imagem do menu prin- cipal, é possível acessar a página apresentada a seguir; é a partir desta interface que as configura- ções gerais, e inicialmente as básicas, são feitas.



3.4.3 Configuração de dispositivos

Para configurar dispositivos no sistema, na aba de configurações básicas, acesse *Dispositivo* 

.

Nesse menu é possível adicionar, excluir, editar e administrar os dispositivos do sistema.

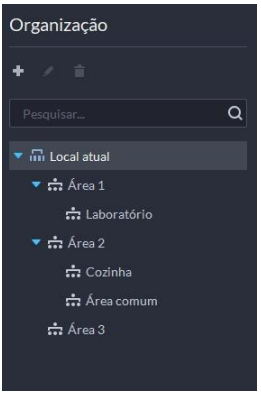
3.5. Adicionar dispositivos

O menu *Adicionar Dispositivo* é dividido em duas janelas principais, uma aba lateral (Organização) e uma janela (Local atual) com duas listas:

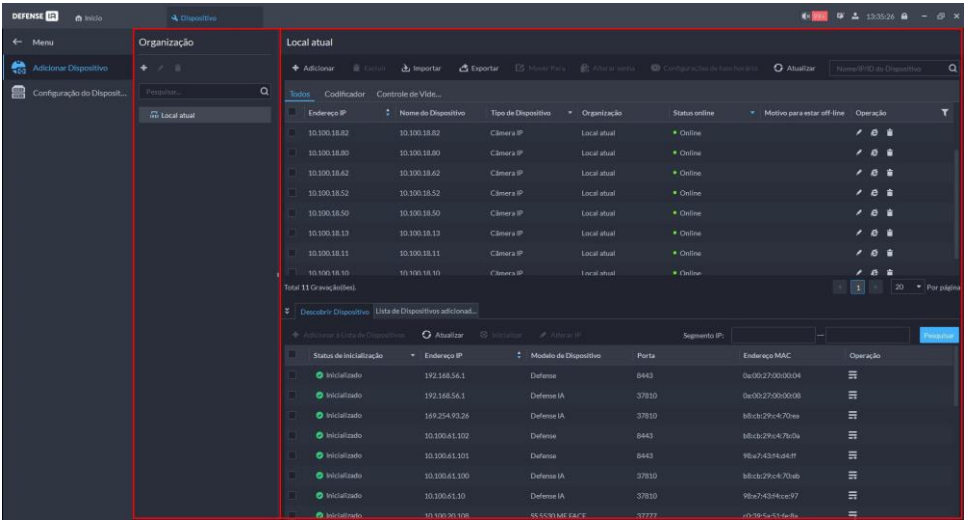
3.5.1 Organização

Na plataforma, Organização é onde as árvores de dispositivos são estruturadas. Por padrão, a Organização principal na hierarquia é o *Local atual.* É possível adicionar, renomear e excluir organizações nesta janela.

Um local representa um servidor principal. É possível acessar mais de um local (servidor) pelo cliente, como apresentado no próximo tópico *Local.*



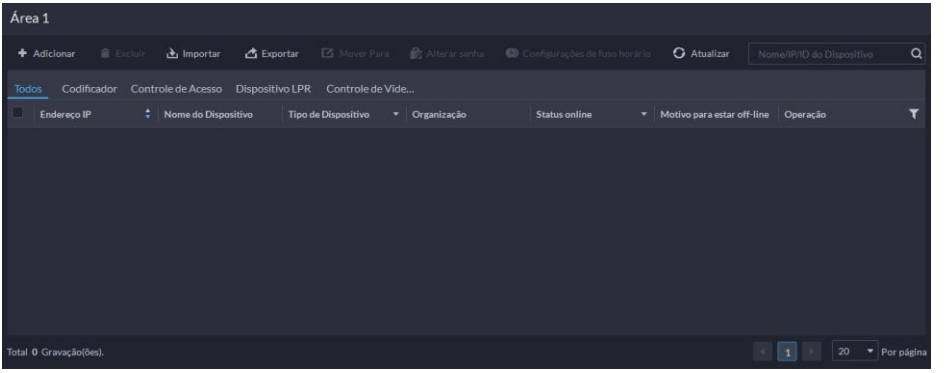
Recomenda-se dividir os dispositivos adicionados no sistema entre diferentes organizações para melhor gerenciamento destes, como por exemplo, caso tenha-se um local dividido entre três áreas (área 1, 2 e 3), e cada área apresenta seus próprios cômodos, com seus respectivos dispositivos, estes podem ser configurados como à seguir:



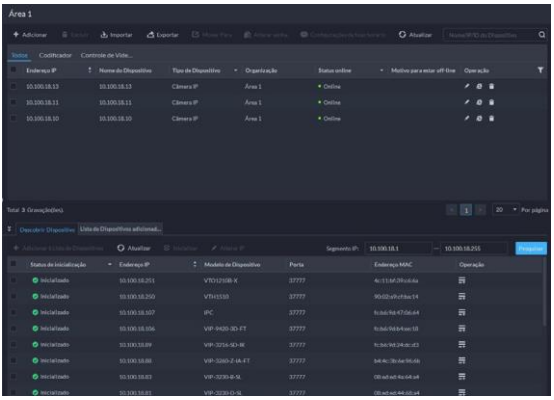
Na janela ao lado, apresentada no próximo tópico, é possível realizar o gerenciamento de dispositivos da organização selecionada.

3.5.2 Local

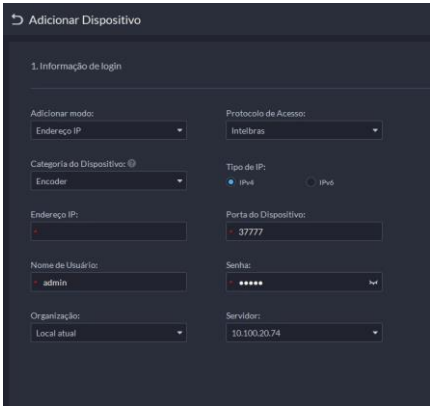
É nessa janela onde é possível gerenciar a conexão de dispositivos. É possível adicionar/excluir dis- positivos um a um, ou em lotes. Neste módulo também é possível exportar, mover, alterar senhas e configurar fuso-horário de dispositivos. No topo, identifica-se a organização selecionada, e logo abaixo atalhos para as operações. Também é possível filtrar os dispositivos apresentados.



Abaixo da lista de dispositivos da organização, há a janela de descoberta de dispositivos, em que apresenta dispositivos compatíveis presentes na rede. Estes podem ser adicionados rapidamente em lote ou individualmente.



Para adicionar manualmente um dispositivo que está, ou não presente na lista, clique em *Adicionar* na janela acima. A seguinte tela será aberta:



Nessa janela, as informações de login devem ser preenchidas de acordo. O Defense IA suporta 4 modos de adição de dispositivos, endereço único de IP, seção de endereço IP, nome de domínio e cadastro automático.

Caso os dados sejam preenchidos corretamente, as informações do dispositivo aparecerão nos campos, restando apenas nomeá-lo de acordo.

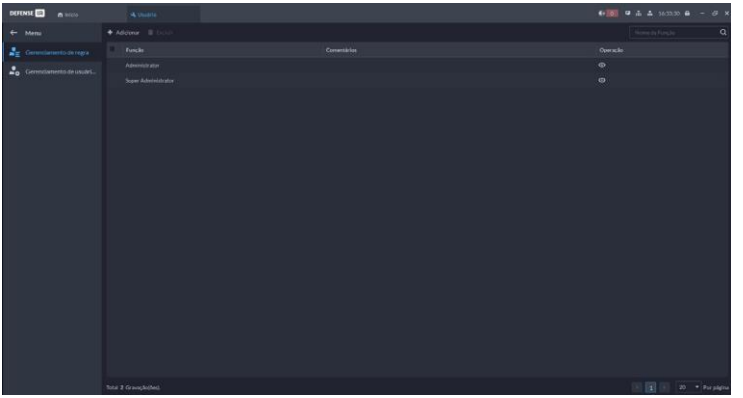
Com os dispositivos adicionados, você pode gerenciá-los a partir das funções dessa página. Mais informações sobre gerenciamento de dispositivos e métodos de adicioná-los são apresentadas no capítulo *Gerenciamento de Dispositivos.*

3.6. Usuários e permissões

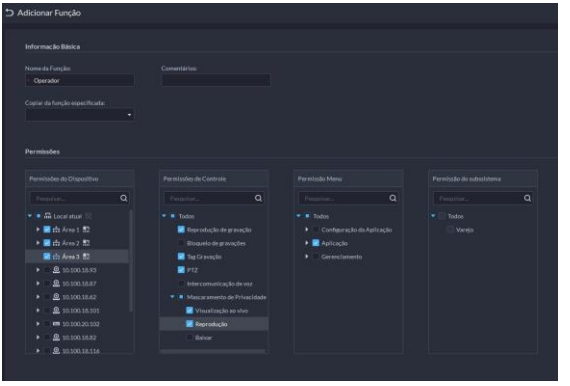
Como usuário padrão, o usuário system possui função de super administrador, permitindo a criação e manutenção de usuários e funções pelo módulo Usuário, 

em configurações.

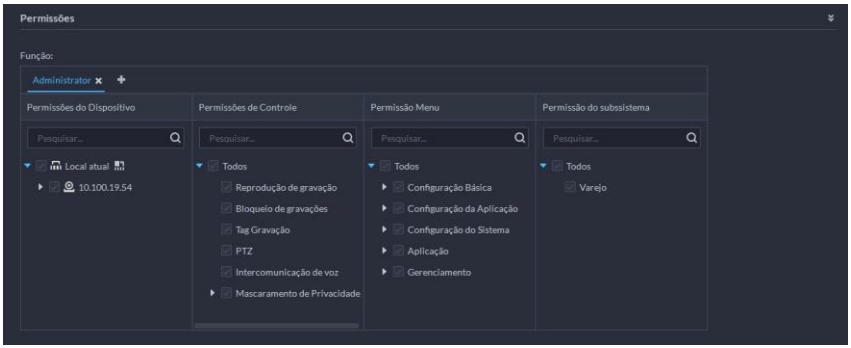
No Defense IA, existem duas funções de usuário padrão, Super Administrador, limitado a 3 usuários, e Administrador, limitado a 10 usuários. Mais funções e usuários personalizados podem ser adicionados pelo módulo.



» **Adicionar função:** para adicionar uma função específica, acesse a aba *Gerenciamento de regra* e clique em *Adicionar no topo.* Uma tela para preenchimento será aberta:

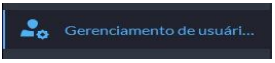


É possível selecionar dispositivos específicos, organizações e interface gráfica que o usuário com essa função terá acesso, também é possível selecionar quais permissões essa função concederá ao usuário, tanto para gerenciamento de dispositivos, quanto para gerenciamento do sistema.

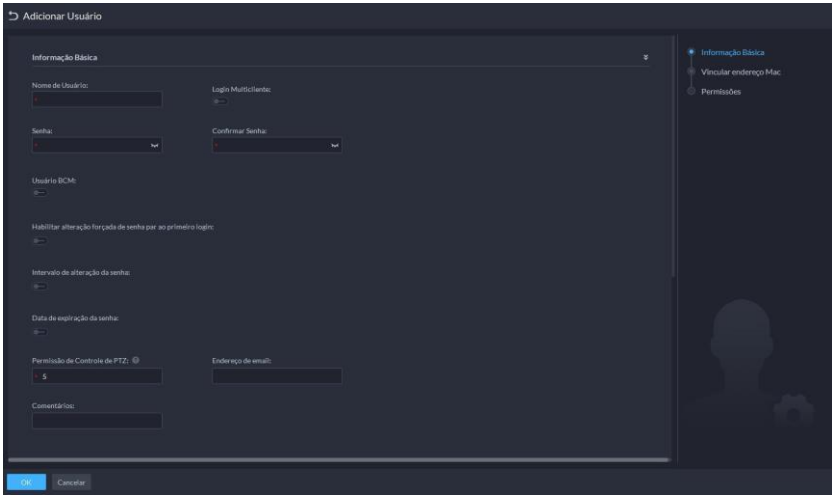


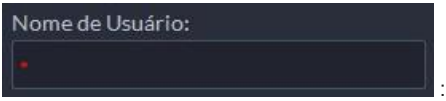
» **Adicionar usuários:** a plataforma apresenta dois modos de adição de usuários diferentes, é possí- vel adicionar manualmente um usuário por vez e/ou sincronizar e importar usuários de um servi- dor AD previamente configurado.

Adicionar um usuário

Na aba *Gerenciamento de usuários* 

, no menu de configuração de usuá- rios, clique em Adicionar no topo. Uma tela para preenchimento será aberta. Preencha as informa- ções necessárias para o usuário, como nome, senha e autoridade para controle de PTZ; também é possível habilitar opções relacionadas a proteção de senha do usuário. Por fim, deve-se selecionar as permissões de sistema para o usuário atribuindo funções a este. Até 32 funções podem ser atribuídas a um usuário, outras informações sobre limitações de configurações podem ser encon- tradas em nosso Datasheet.

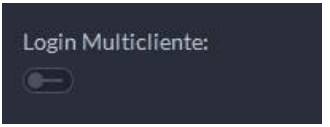


» 

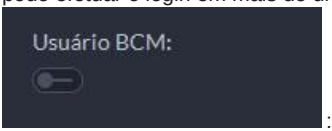
: identificador do usuário, não pode existir mais de um usuário com o mesmo nome.

» 

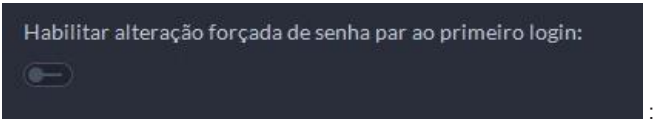
: senha do usuário, recomenda-se utilizar uma senha forte.

» 

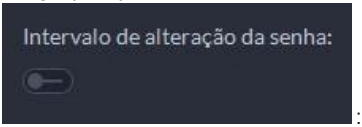
: botão Multicliente, caso selecionado, indica que o usuário pode efetuar o login em mais de um cliente simultaneamente.

» 

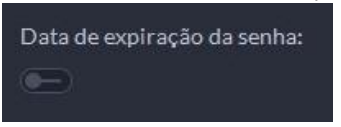
: botão de usuário BCM, caso selecionado, indica que o usuário pode participar de chamadas de grupo. Um usuário BCM não pode ser um usuário Multicliente.

» 

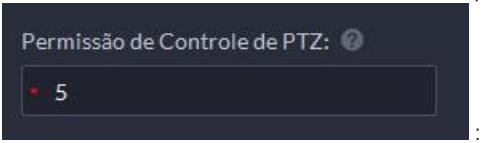
: botão de forçar troca de senha após primeiro login, caso selecionado, o usuário deverá trocar a senha registrada ao efetuar o login pela primeira vez.

» 

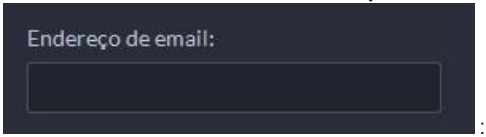
: botão de Intervalo de alteração de senha, caso selecionado, o usuário deverá trocar a senha após um período contínuo definido entre 1 e 365 dias.

» 

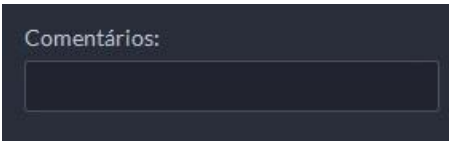
: botão de expiração de senha, caso selecionado, data e horá- rio deveram ser definidos para expiração da senha do usuário, após a data escolhida, o usuário não terá mais acesso ao sistema. A data pode ser alterada por um Super-Administrador.

» 

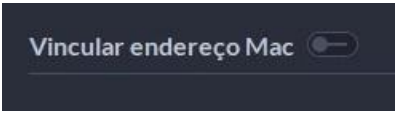
: define autoridade sobre controle de dispositivos PTZ caso mais de um usuário esteja acessando-o simultaneamente.

» 

: vincula um endereço de e-mail ao usuário.

» 

: texto auxiliar vinculado ao usuário.

» 

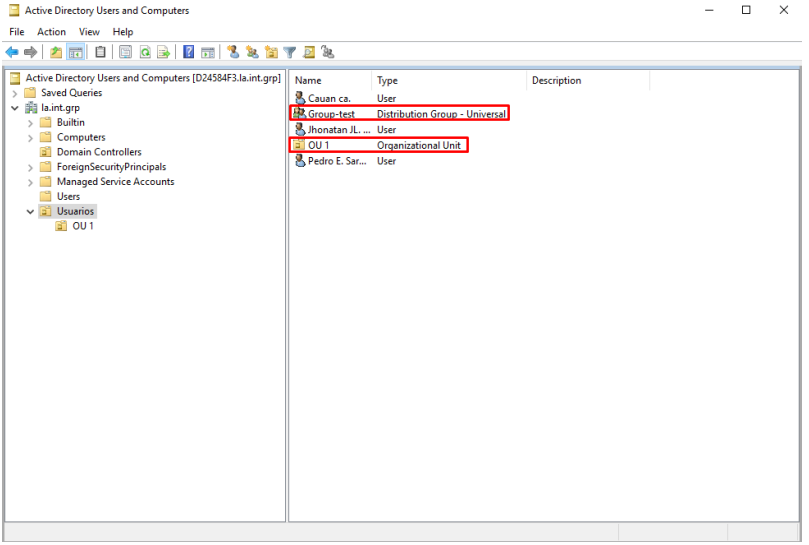
: botão para vincular endereços MAC ao usuário.

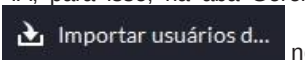
Vincula uma função existente ao usuário, apresentando as permissões definidas.

Sincronizar com servidor AD

Antes de sincronizar a plataforma com usuários de um servidor AD, deve-se configurá-lo previamente. Veja o capítulo *Active Directory* para configurá-lo.

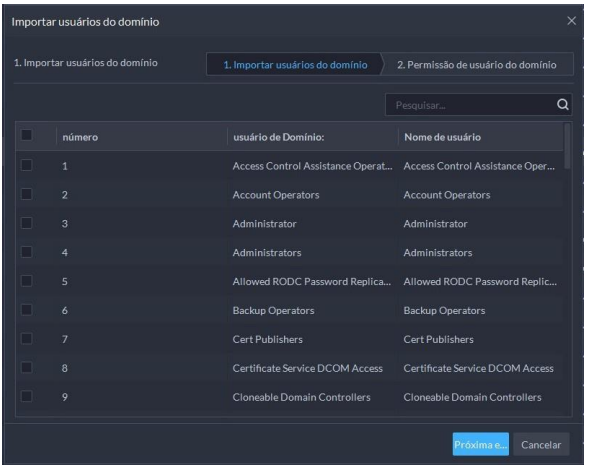
Com o AD configurado o Defense entende que usuários que estão adicionados no tipo *Organiza- tional Unit* como um grupo de domínio, (Usuarios adicionados do tipo *Security/Distribution Group -Universal/Global* serão reconhecidos como usuarios no Defense e não como um grupo).



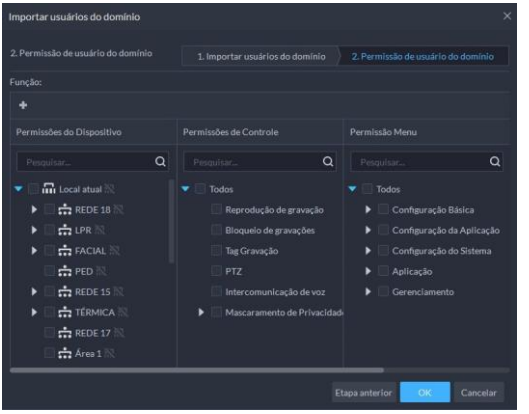
Após um servidor AD configurado na plataforma, você pode importar usuários do domínio para o Defense IA, para isso, na aba *Gerenciamento de usuários* clique em *Importar usuários do domínio* 

no topo. Um pop-up deve aparecer com a lista de usuários do domí- nio. Selecione o(s) usuário(s) que deseja adicionar e em seguida, atribua funções a estes(s).

As funções selecionadas serão atribuídas a todos os usuários selecionados. Para atribuir funções diferentes para usuários de domínio, o processo terá que ser repetido para cada função.



Selecione os usuários que deseja importar e clique em *Próxima etapa.*



Selecione as funções necessárias para o(s) usuário(s) selecionado(s) no ícone  e clique em *OK* para finalizar o processo.

3.7. Armazenamento

O Defense IA permite diferentes configurações de discos em seu ambiente (tanto em volume local, quanto em volume de rede), apresentando 3 configurações de disco: disco de vídeo, disco de ima- gens e arquivos e disco de arquivos de incidente.

Acesse 

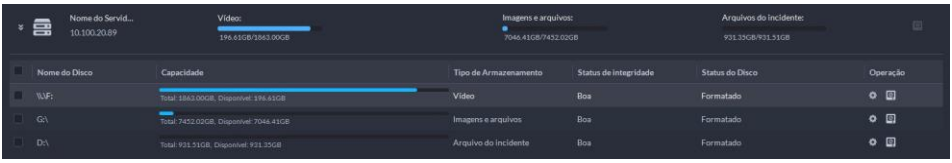
Armazenamento em configurações para gerenciar os discos e armazenamento de vídeo do sistema.

3.7.1 Disco do servidor

Nessa página configura-se os discos locais. Os discos disponíveis para configuração aparecerão ao expandir a janela do servidor, clicando no ícone 

.

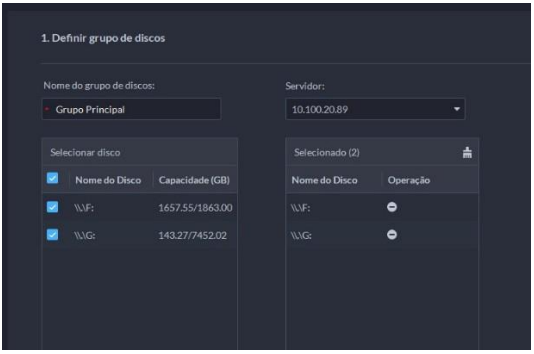
Na janela expandida é possível ver a capacidade, integridade, status e realizar operações de disco. Clicando na engrenagem é possível selecionar o tipo de disco que deseja configurar; o botão ao lado formata o disco apagando todos os dados nele.



Ao configurar um novo tipo de disco, este será formatado automaticamente, excluindo todos os dados armazenados.

3.7.2 Grupo de discos

Quando há um disco na plataforma configurado como disco de vídeo, é possível configurar também um grupo de discos, vinculando volumes à canais de gravação, assim tornando possível um melhor gerenciamento do armazenamento. Para isso, em *Grupo de Discos* clique em *Adicionar Grupo de Discos.* Selecione os discos que deseja vincular e nomeie o grupo.



Clique em *Próxima etapa* na parte inferior da tela para vincular os canais de vídeo ao grupo de discos. Clique em *OK* para finalizar o processo.

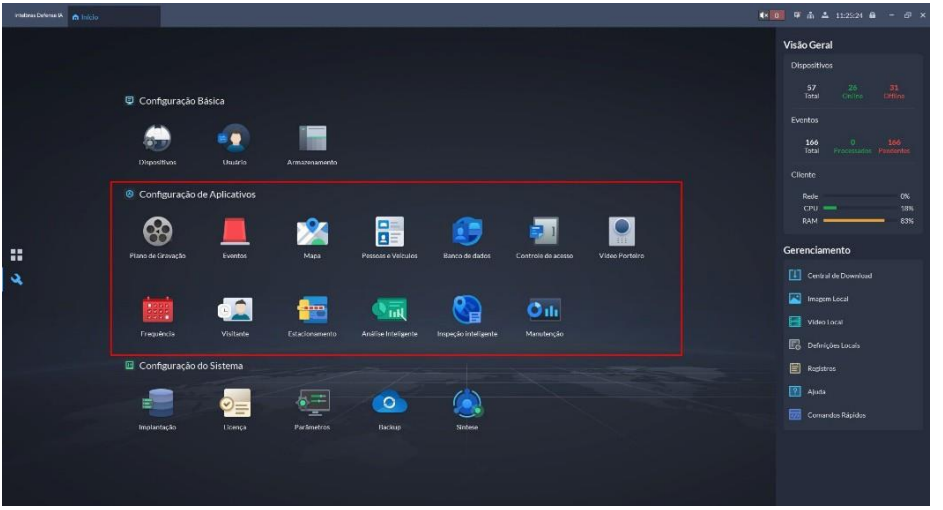
Este processo não configura um plano de gravação para os canais selecionados, apenas os vincula a um volume de armazenamento. Para configurar um plano de gravação, veja *Plano de gravação.*

Caso tenha servidores auxiliares configurados, também é possível gerenciar seus discos pela interface.

Para informações sobre capacidades e armazenamento, verifique a ficha técnica do produto em nosso site.

4. Configurações iniciais de aplicativos

Após concluir as configurações básicas, você pode avançar na preparação de alguns módulos es- senciais para sua aplicação. Nesta página, você encontrará informações sobre a criação de planos de gravação, eventos, mapas e bancos de dados. Vale ressaltar que a configuração detalhada, des- tas e de outras funções, é abordada em capítulos posteriores.



4.1. Configuração de gravações

O menu para configurar as gravações de dispositivos encontra-se no menu de configuração de aplicativos, esse menu apresenta atalhos para configurar os módulos de uso que são encontrados no menu inicial. Também permite gerenciar dados e informações do sistema, como cadastros em seu banco de dados.

4.2. Gerenciador de Serviços

Se você não conseguir fazer login no cliente porque o banco de dados está anormal, você pode repara-lo manualmente. Clique no serviço MySQL e siga as instruções. Com base nos itens verifica- dos, a plataforma determinará se é necessário reparo ou restauração. Se o reparo falhar, você pode tentar restaurar o banco de dados usando um dos arquivos de backup. Durante a restauração, a pla- taforma também fará backup do banco de dados. Certifque-se de que há espaço o suficiente, caso contrário, a restauração falhará. A plataforma fará backup automaticamente do banco de dados de acordo com as configurações de backup e restauração.

» Esta operação não pode ser executada em espera ativa.

» Para restaurar o banco de dados , a plataforma precisa usar a porta 3306. Se um processo estiver usando a porta, será necessário encerrá-lo primeiro.

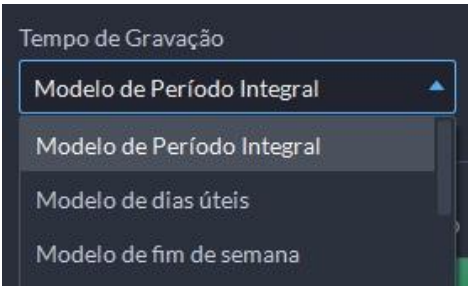
4.3. Plano de Gravação

Acessando a página de Plano de Gravação 

, é possível navegar entre duas janelas, Plano e Recuperação de gravação.

4.3.1 Criar plano de gravação

É nesta janela em que adiciona-se os planos de gravação dos dispositivos adicionados no servidor, podendo optar pelo plano geral de gravação, ou plano de gravação por detecção de movimento. Assim como na página de *Configuração de dispositivos,* os dispositivos aparecem na aba de Orga- nização. Para adicionar um plano de gravação para um ou mais dispositivos, clique em Adicionar plano de gravação no canto superior.

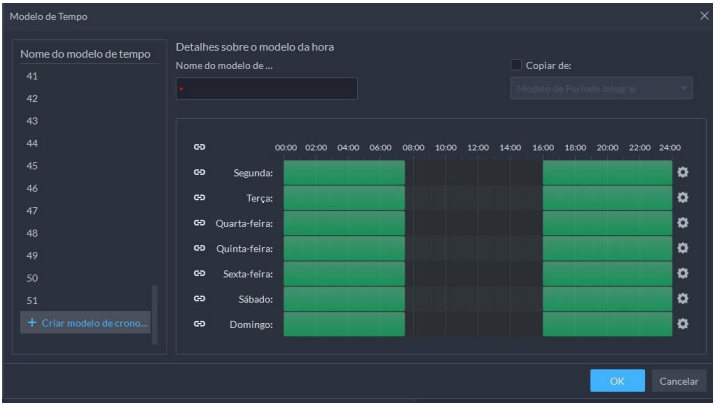


O plano geral de gravação definirá um cronograma para que a gravação de canais de vídeo seja realizada quando o dispositivo estiver disponível, enquanto o plano de gravação por detecção de movimento funciona da mesma maneira, porém a gravação de canais de vídeo será realizada quan- do houver movimentação detectada.

Na aba aberta é possível configurar parâmetros como o tipo de transmissão (Principal, secundário 1 ou 2) que deseja gravar e o período de gravação. O Defense IA apresenta 3 modelos de período pré-configurados, Modelo de período integral, de dias úteis e de fim de semana.

Além desses, também é possível criar um período de gravação personalizado clicando em *criar modelo de cronograma* 

.



Apague ou crie blocos em verde para definir os horários em que a gravação deve ser feita. Também é possível copiar um modelo já existente como referência.

Por fim, selecione os canais de vídeo que deseja vincular a este plano de gravação; é possível selecioná-los na árvore de dispositivos abaixo.

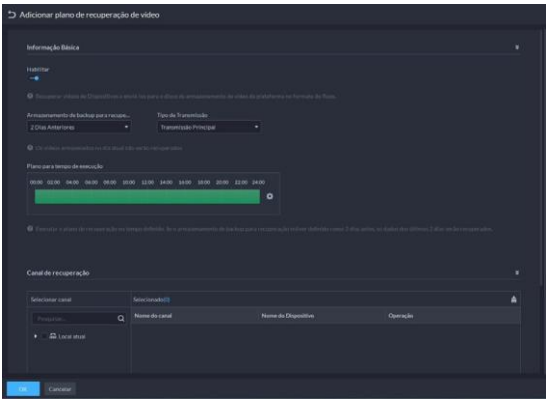
Todos os dispositivos selecionados serão vinculados ao mesmo plano de gravação, mas é possível gerenciá-los de forma separada.

4.3.2 Recuperação de Gravação

Na janela de recuperação de gravação, assim como na anterior, há duas opções, recuperação de vídeo e recuperação de arquivo; ambas apresentam o mesmo funcionamento, diferenciando-se apenas pela compatibilidade de dispositivos.

A recuperação de gravação tem como objetivo agendar um cronograma para que vídeos e/ou arquivos sejam copiados do armazenamento do dispositivo para o armazenamento do servidor. Possuindo prazo máximo de 7 dias e mínimo de 1 dia (dia anterior), o plano pra recuperação de vídeos e arquivos pode ser configurado para ocorrer durante as 24 horas do dia.

Para adicionar um plano de recuperação para um ou mais dispositivos, clique em Adicionar plano de recuperação no canto superior.



Na aba aberta é possível configurar parâmetros como a quantidade de dias que deseja recuperar (1- 7), o tipo de transmissão (Principal, secundário 1 ou 2) e os horários para realizar a recuperação. Por fim, selecione os canais de vídeo que deseja vincular ao plano de gravação; é possível selecioná-los na árvore de dispositivos abaixo.

4.4. Configuração de Eventos

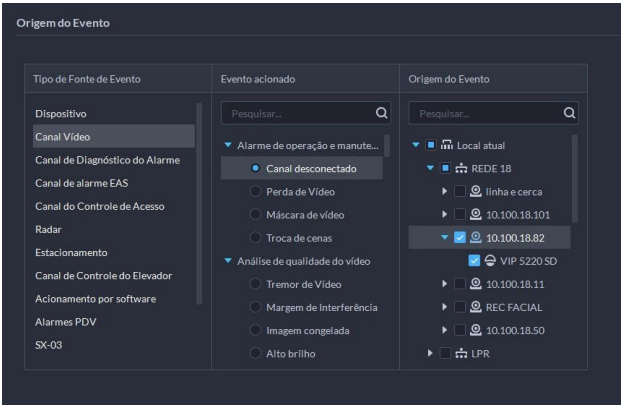
Acessando a configuração de eventos é possível adicionar, editar, excluir, habilitar e desativar eventos. Todos os eventos cadastrados aparecem nessa interface, é possível gerenciá-los na aba acima e navegar por eles na aba de navegação abaixo.

4.4.1 Adicionar Eventos

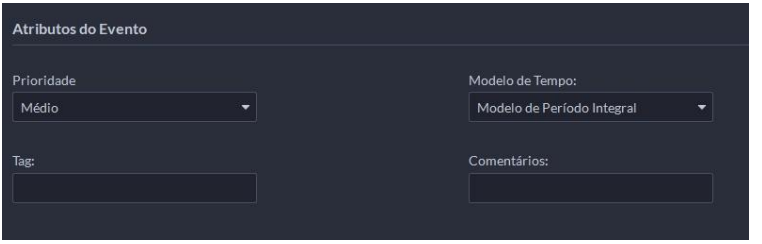
Para adicionar um evento, clique em *Adicionar,* a interface de criação de evento será aberta. Nessa interface deve-se selecionar parâmetros do sistema e de dispositivos, vinculando-os ao evento desejado, este processo é realizado em 5 etapas.

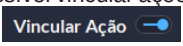
Primeiramente, deve-se indicar o tipo e origem do evento, selecionando um dos eventos disponíveis na lista e o dispositivo que será responsável pelo gatilho do evento.

Note que os dispositivos disponíveis para seleção dependem do tipo de evento selecionado. Se algum dispositivo não aparece na lista, verifique se este é compatível com o tipo de evento selecionado.



Em seguida, em atributos do evento, indique o nível de prioridade do evento (baixo, médio ou alto) e o modelo de tempo que esse evento deve ficar ativo (para configurar um modelo de tempo persona- lizado, veja aqui). Também é possível definir uma Tag e adicionar comentários ao evento.

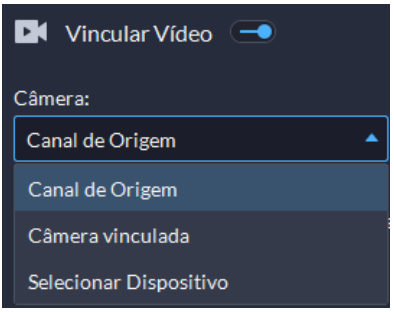


É possível vincular ações a partir do acionamento do evento, para isso, ative o botão Vincular ação 

novas opções aparecerão. Selecione as ações que deseja vincular ao evento,
são elas:

Vincular vídeo

Para vincular câmeras, canais de vídeo ou executar gravações do evento de até 300 segundos. Você pode optar por vincular e/ou gravar o próprio canal de origem do evento ou selecionar outros canais/dispositivos.



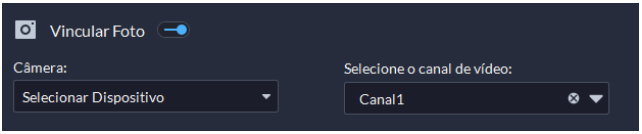
» **Canal de Origem:** vincula ao evento o próprio canal de vídeo que o gerou.

» **Câmera vinculada:** caso o canal que gerou o evento esteja vinculado a algum outro canal de vídeo, este será vinculado (recomenda-se utilizar esta opção quando a origem do evento for um canal de alarme).

» **Selecionar Dispositivo:** vincula ao evento outros dispositivos disponíveis na árvore de dispositivos. Ao selecionar esta ação vinculada, também é possível optar por fazer o pop-up do canal de vídeo ao acionamento do evento configurado. Para isso, marque a caixa correspondente.

Além disso, também é possível realizar a gravação de até 5 minutos do canal vinculado, a partir do acionamento do evento (é possível configurar um tempo de pré-gravação de até 10 segundos). Para isso, ative a função clicando no botão *Gravações de Evento,* e configure de acordo.

Vincular Foto

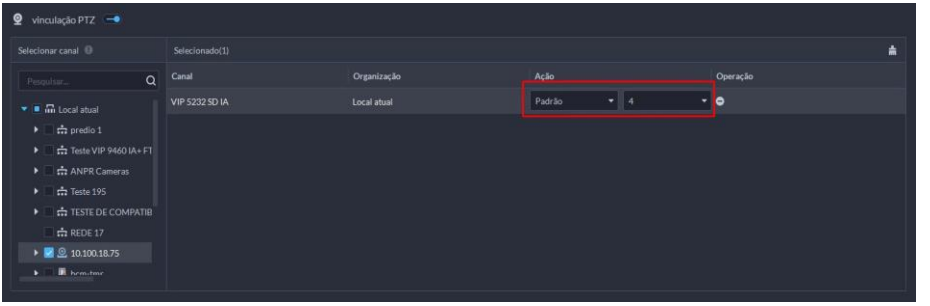


Assim como a anterior, esta ação vincula um canal de vídeo ao evento e um snapshot é realizado, capturando a imagem durante o acionamento do evento.

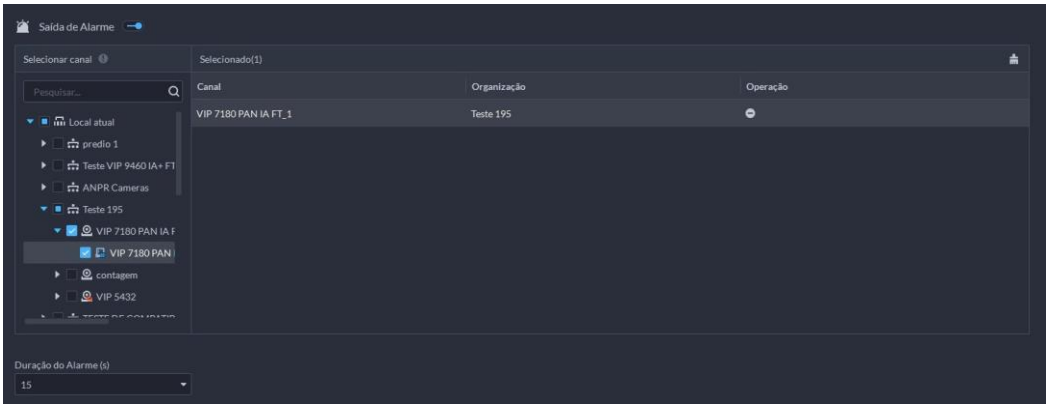
É possível selecionar o próprio canal de origem do evento (se este for de vídeo), ou selecionar um outro canal na árvore de dispositivos.

Vincular PTZ

É possível vincular uma rontina PTZ ao acionamento do evento. Para isso, selecione o dispositivo compatível e configure de acordo.



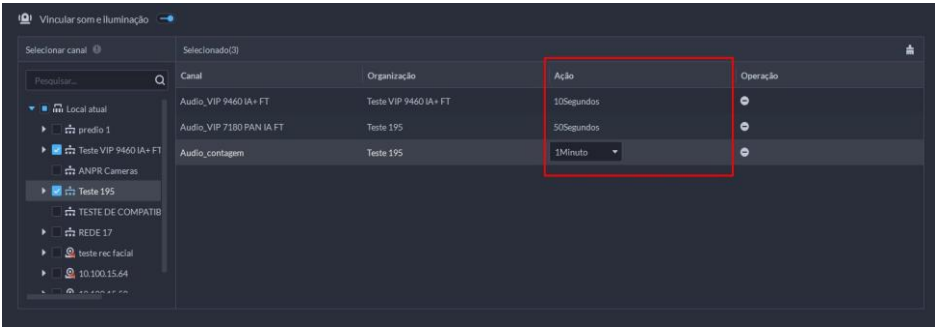
Na coluna *Ação* é possível escolher entre as rotinas PTZ pré-configuradas no dispositivo.



Saída de Alarme

Esta ação vincula saídas de alarme de dispositivos na plataforma a partir do acionamento do evento. Para configurar, selecione o canal de alarme na árvore de dispositivos e a duração da ativação (5 a 600 segundos). Caso a duração *sempre* seja selecionada, o alarme deverá ser desligado manualmente após sua ativação.

Som e iluminação

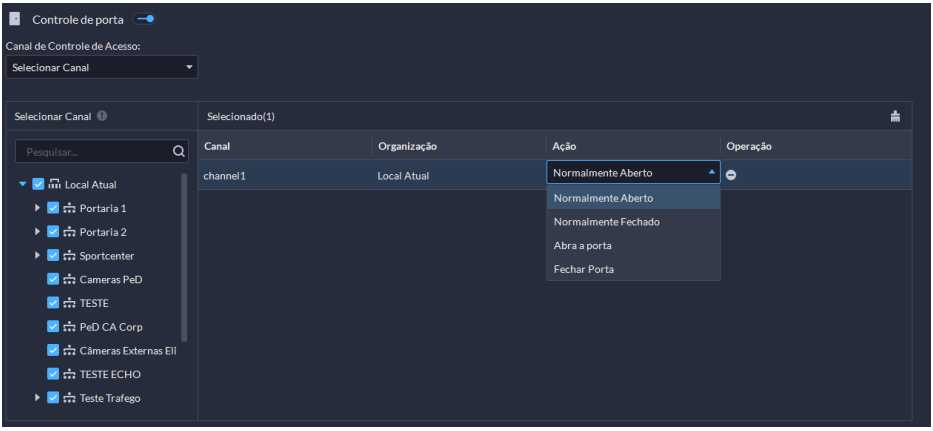


Assim como a anterior, esta ação vincula saídas de dispositivos a partir do acionamento do evento. Saídas sonoras e luminosas são vinculadas, e sua duração pode ser selecionada na coluna *Ação.*

Controle de Porta

Esta ação vincula canais de controle de acesso (portas) ao acionamento do evento. É possível optar por ações como tornar as portas normalmente abertas ou fechadas, ou apenas abrí-las ou fechá-las.

É possível aplicar a regra a todos os canais de controle de acesso da plataforma, ou selecionar os canais desejados e aplicar caso a caso.

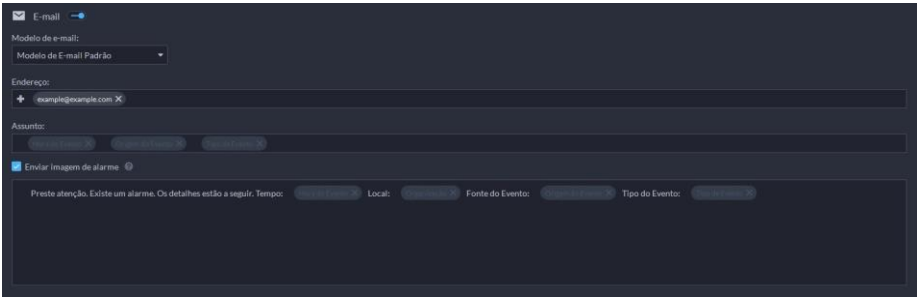


Comando URL HTTP

É possível vincular comandos HTTP a partir do acionamento do evento. Para isso, clique em *Adicio- nar* 

e escolha o método de solicitação entre comandos Get, Post, Put e Delete. Na segunda coluna é onde insere-se o endereço do comando. Também é possível adicionar comentá- rios e testar o comando configurado.

E-mail

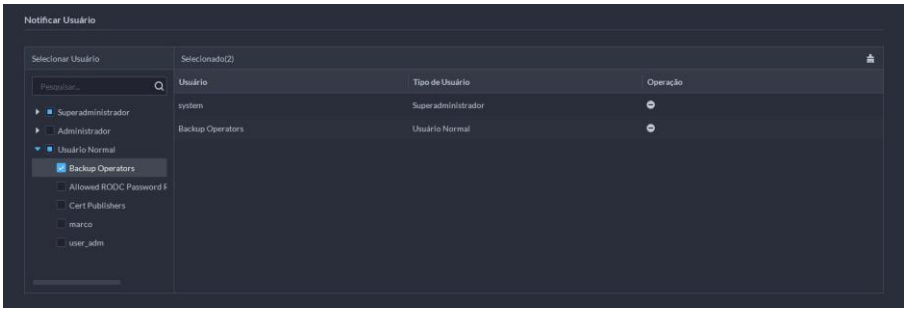


Esta ação envia um e-mail aos destinatários configurados. É possível escolher entre um template padrão, ou personalizar um modelo próprio. Para esta ação funcionar corretamente, um servidor de e-mail deve estar devidamente configurado na plataforma. Veja *Parâmetros* em Configurações do sistema.

Protocolo de Alarme

Também é opcional ativar o Protocolo de Alarme ativando o botão *Protocolo de Alarme.*

O Protocolo de alarme é uma instrução disponível ao operador quando este reconhece o alarme.



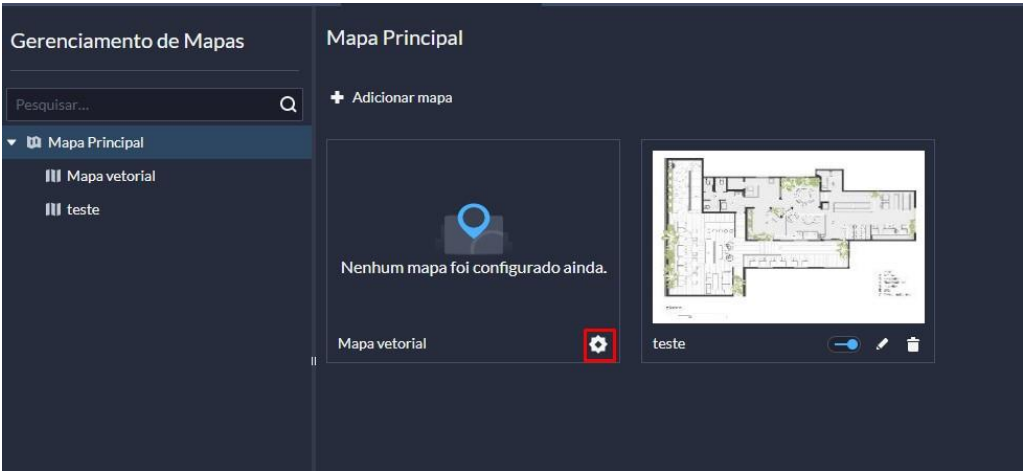
Por fim, selecione o(s) usuário(s) que deve(m) ser notificado(s) a partir do acionamento do evento. Clique em *OK* para finalizar a criação do evento. Caso posteriormente queira modificar alguma informação, clique no ícone de edição 

4.5. Configuração de Mapa

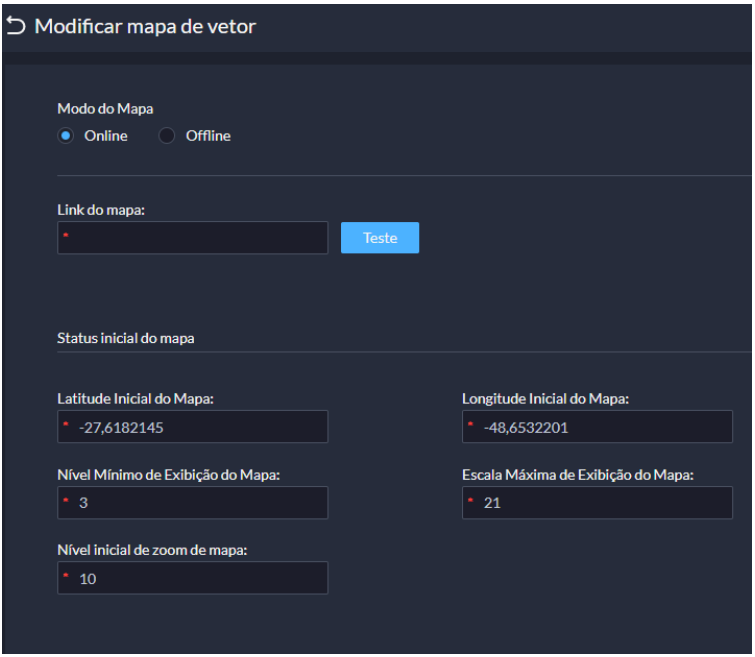
O **mapa vetorial** pode ser utilizado de maneira mais ampla junto ao Google Maps contendo longitude e Altitude,já o **mapa principal** é utilizado comumente como uma planta baixa do local desejado.

1. Na página **Inicial**, clique em  e então em **configurações de aplicativos** selecione **Mapa**  .

2. Na lista de mapas, selecione o mapa vetorial e clique  .



3. Configure os parâmetros.



- **Mapa Online**

1. Selecione **Online**
2. Configure a informação do mapa e então clique **OK**.

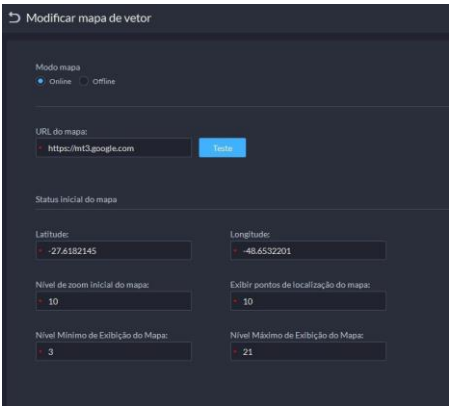
- **Mapa Offline**
- Selecione **Offline**.

1. Clique **Importar** e importe um mapa offline
2. Configure a informação do mapa e clique **OK**.

Deve ser inserido a URL do Google Maps para que o mapa funcione .

4.5.1 Mapa principal

Preencha as informações necessárias de acordo com a personalização desejada.



Modo mapa

Neste campo seleciona-se o modo do mapa, dois modos podem ser configurados, Online e Offline.

URL do mapa/Importar

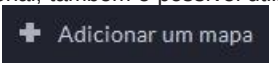
Caso selecione o modo online, insira neste campo a URL do mapa vetorial, o endereço no qual a plataforma se conectará ao mapa.

Caso utilize o modo offline, importe o arquivo de mapa.

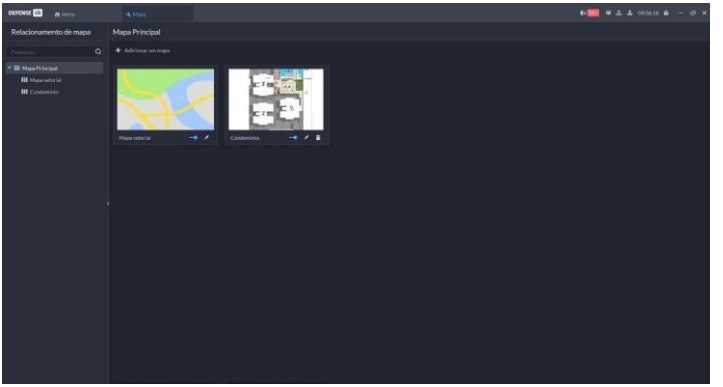
Status inicial do mapa

Dentre esses campos são inseridos os parâmetros iniciais do mapa, configurando Latitude e Longitude iniciais do mapa, além de zoom máximo, mínimo e inicial.

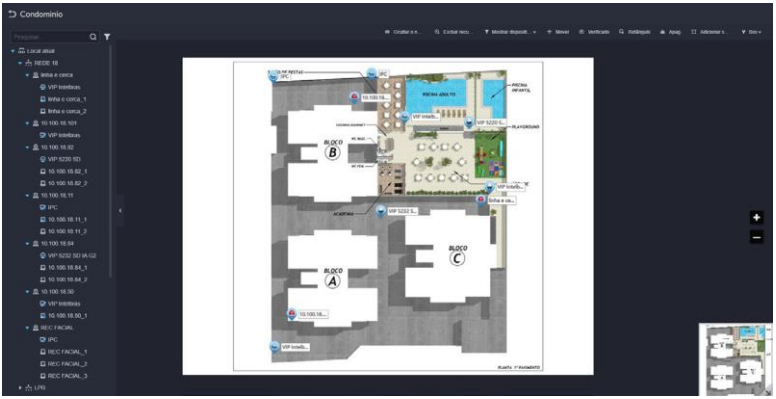
Mapas personalizados

Além do mapa vetorial, também é possível utilizar um mapa raster próprio. Para isso, clique em *Adicionar um mapa* 

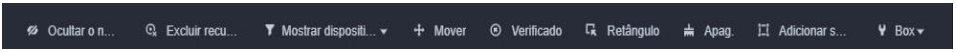
para enviar a imagem (suporta formatos de imagem JPEG/JPG e PNG). O mapa adicionado aparecerá como um mapa principal.



Clique duas vezes no mapa desejado para acessá-lo e visualizar a lista de dispositivos, você pode **arrastá-los** sob o mapa para **adicioná-los** a ele.



Acima, há uma barra de ferramentas que permite o gerenciamento dos dispositivos no mapa.



» Ocultar/Mostrar o nome dos elementos inseridos no mapa.

» Excluir elementos selecionados no mapa.

» Filtrar elementos presentes no mapa.

» Mover elementos inseridos no mapa.

» Selecionar elementos no mapa. Seleção pelo clique.

» Selecionar elementos no mapa. Cria uma área retangular para seleção.

» Apaga todas as marcações presentes no mapa.

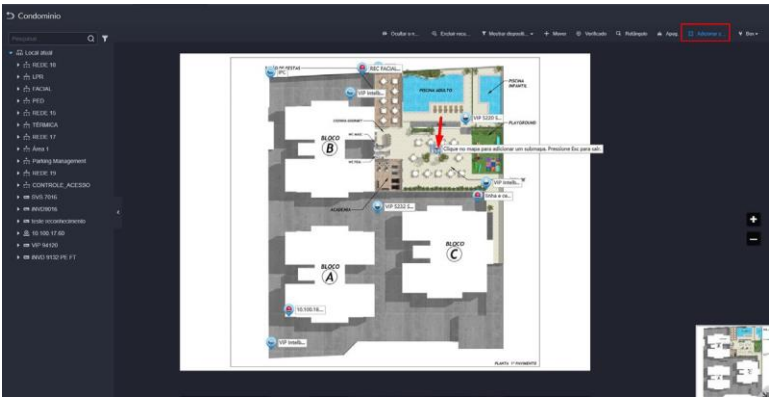
» Adiciona um submapa como elemento no mapa.

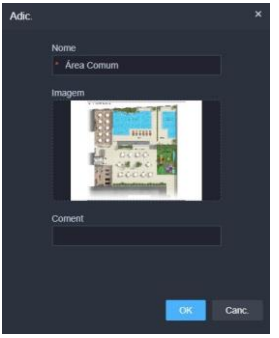
» Adiciona uma marcação no mapa como um elemento no mapa.

» Redefine a visualização do mapa para encaixar na tela.

4.5.2 Submapas

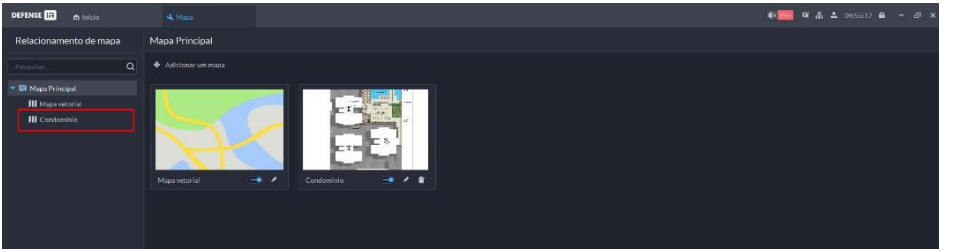
Como visto pela ferramenta *Adicionar submapa,* a plataforma também permite a hierarquização de mapas em camadas, ou seja, é possível adicionar camadas inferiores a mapas, como por exemplo, é possível adicionar um submapa *Área comum* ao mapa *Condomínio.* Para isso, selecione a ferramenta *Adicionar submapa* e selecione um local no mapa. Insira o nome e imagem desejados.

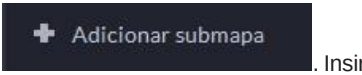




Você pode acessar e gerenciar o submapa clicando duas vezes no elemento adicionado. É possível acessá-lo pela árvore de mapas no menu inicial também.

Também é possível adicionar um submapa a partir da tela inicial da configuração de mapas. Para isso, selecione o mapa principal desejado na árvore de relacionamento de mapa.



Clique em *Adicionar submapa* 

. Insira o nome, imagem e posição no mapa principal.

É possível inserir até 8 camadas de mapas, com até 32 mapas por hierarquia.

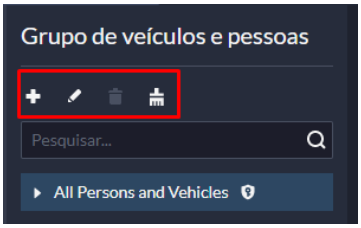
4.6. Configuração de Pessoas e Veículos

No Defense IA, você pode registrar pessoas e veículos para integração de inteligências a um ban- co de dados próprio. A plataforma permite a criação de grupos e subgrupos personalizados para classificar e organizar as informações de cadastro, além de associar diferentes autenticações e permissões de acesso a cada entidade registrada.

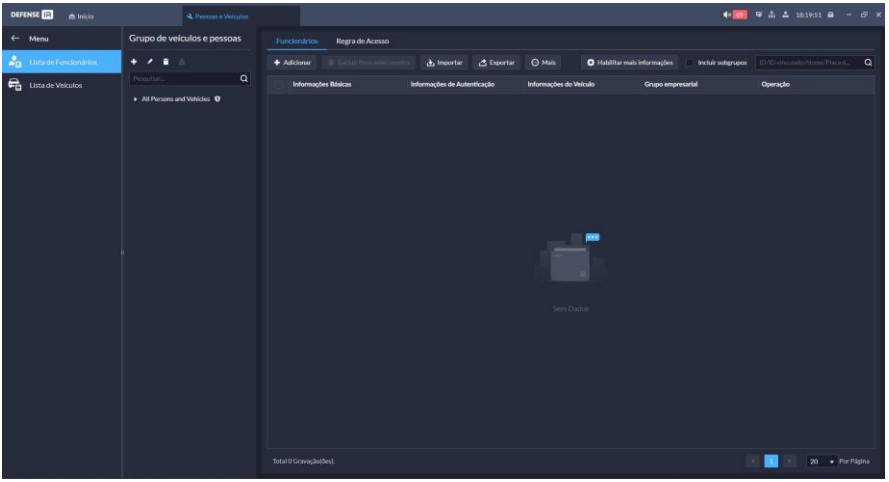
Essas funcionalidades podem ser encontradas no menu de configurações de Pessoas e Veículos.

4.6.1 Cadastrar pessoas

A estrutura da página divide-se entre a árvore de grupo de pessoas e a lista de pessoas, é possível adicionar, editar e excluir grupos pelas ferramentas mostradas abaixo. Assim como em outros mó- dulos do programa, é possível criar hierarquias entre os grupos criados.

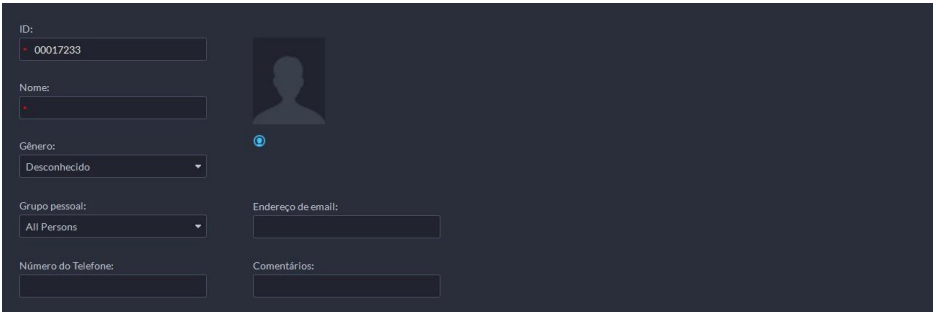


Existem dois métodos gerais para cadastrar pessoas na plataforma. Diretamente pelo módulo, preenchendo informações manualmente, ou a partir da importação de dados, seja de dispositivos compatíveis, ou uma planilha modelo preenchida. No capítulo *Gerenciamento de dados* a importação de dados para plataforma é abordada com mais detalhes.



Para cadastrar uma pessoa na plataforma diretamente pelo módulo, clique em *Adicionar* na guia de ferramentas acima.

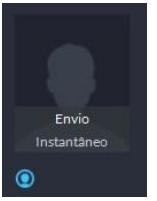
Informações Básicas



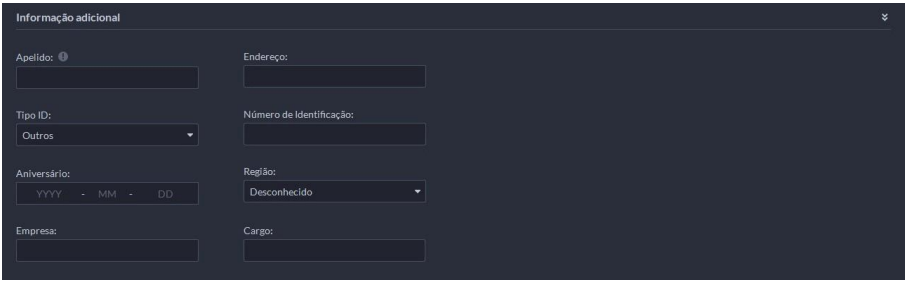
Nesta etapa preenche-se informações básicas sobre a pessoa cadastrada. ID, nome e foto da pes- soa são informações obrigatórias.

O ID é um Código único identificador da pessoa no sistema. O Defense IA gera um ID aleatório não existente. É possível alterar este campo.

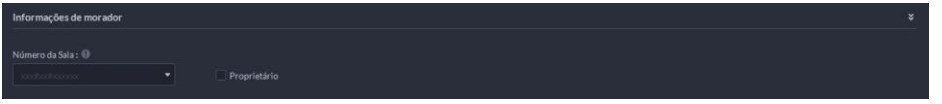
Há duas opções para inserir uma foto da pessoa, por upload de arquivo de imagem (Envio), ou fotografia pela web-cam (Instantâneo).



Informações Adicionais

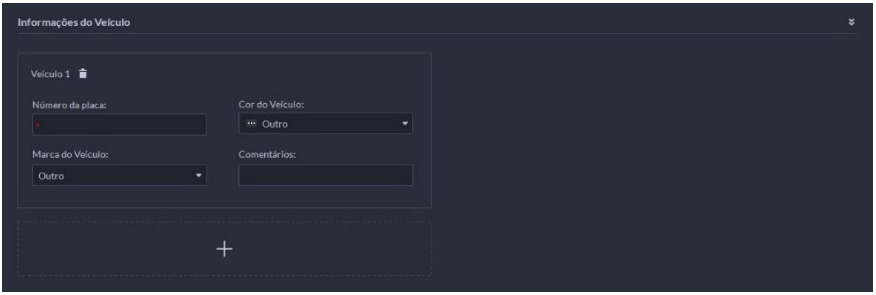


É possível adicionar informações adicionais ao cadastro. Expandindo a aba de informações adi- cionais, campos extras para preenchimento aparecem, como Apelido, Endereço, Documento de identificação, data de nascimento, naturalidade, empresa e cargo. Outras informações adicionais podem ser configuradas na plataforma.



Caso utilize portaria remota no sistema, e queira vincular a pessoa cadastrada a um número de sala, é possível selecionar um existente a partir da lista suspensa ou inserir um manualmente no campo. Também é possível indicar pela checkbox se a pessoa cadastrada é responsável ou não pela sala.

Informações do Veículo



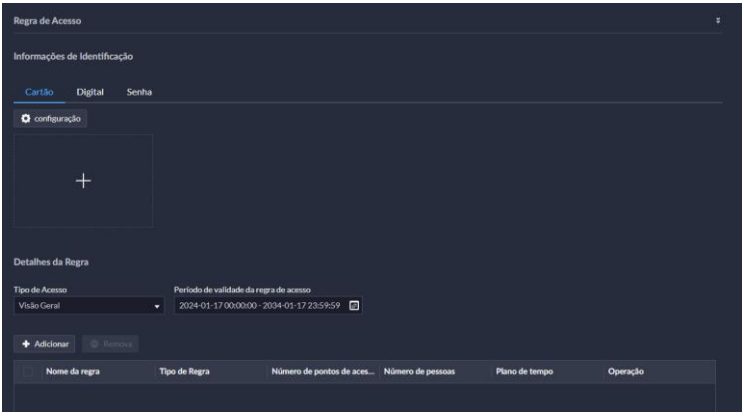
Para vincular um veículo à pessoa cadastrada, clique em “+” na aba Informações do Veículo. Pre- encha as informações como:

- **Placa do veículo:** a placa é o identificador do veículo, ela será vinculada à pessoa cadastrada.
- **Cor do veículo:** selecione a cor do veículo na lista suspensa.
- **Marca do veículo:** selecione a marca do veículo na lista suspensa.
- **Comentários:** adicione comentários sobre o veículo no campo.

Veja mais informações sobre em *Cadastrar veículos.*

Regra de Acesso

O uso da regra de intertravamento (clausura) não é recomendado quando regras de antipassback estão habilitadas e ativas dentro do mesmo cenário ou contexto.



Em Regra de Acesso, você pode inserir métodos de autenticação da pessoa cadastrada, tais mé- todos poderão ser usados para acesso a dispositivos de controle de acesso presentes no sistema (veja em Controle de acesso mais detalhes de como cadastrar regras de acesso).

Os métodos de autenticação são:

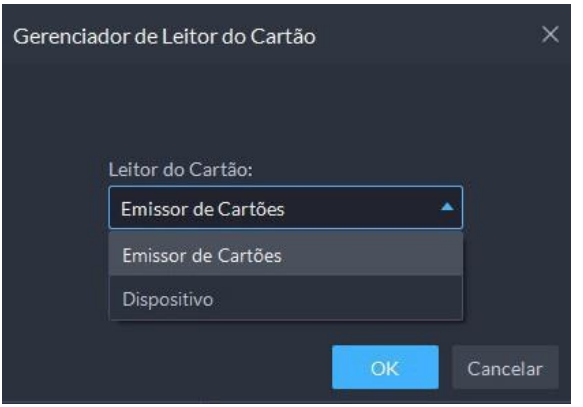
Cartão

Uma pessoa cadastrada pode possuir até 5 cartões, um deles deve ser o principal. O cartão deve apresentar um código hexadecimal de 8 à 16 dígitos.

Existem dois métodos para registrar um cartão, digitando manualmente, caso o código do cartão seja conhecido, ou adicioná-lo via leitora. Para registrar um cartão via leitora, clique no botão configuração.

É possível escolher entre uma leitora de cartão que pode ser conectada via USB com o computador, ou algum dispositivo de controle de acesso já conectado à plataforma. Ao selecionar a opção de- sejada, clique em *OK* e passe o cartão no sensor de leitura.

O código do cartão deve aparecer no campo, confirme para registrar o cartão. O mesmo passo pode ser repetido para emitir outros cartões.



Existem 3 funções de gerenciamento do cartão:

» **Cartão de coação:** selecione este ícone para definir o cartão como cartão de coação. Cartão de coação emite um evento de coação quando passado numa leitora conectada ao Defense IA (o evento deve ser devidamente configurado para notificar a plataforma, veja em Eventos como configurar um evento).

» **Alterar número do cartão:** selecione este ícone para alterar o número do cartão.

» **Excluir cartão:** selecione este ícone para excluir o cartão da plataforma.

Digital

Até 3 digitais podem ser cadastradas por pessoa. Para cadastrar um digital, o sistema deve estar conectado à uma leitora de digitais, seja um leitor via USB ou dispositivo conectado à plataforma.

Para registrar uma digital, clique no botão configuração.

Selecione o dispositivo desejado para leitura e clique em *OK.* Em seguida, clique em *Adicionar* Adicionar.

Posicione o dedo no leitor, clique em Adicionar digitais e realize a coleta da impressão digital 3 vezes.

Existem 3 funções de gerenciamento da impressão digital:

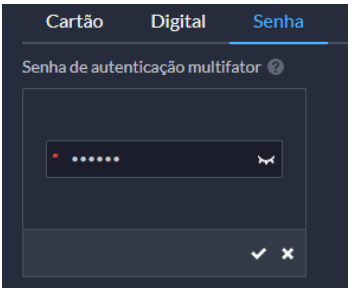
» **Digital de coação:** selecione este ícone para definir a impressão digital como digital de coação. Digital de coação emite um evento de coação quando passada numa leitora conectada ao Defense IA (o evento deve ser devidamente configurado para notificar a plataforma, veja em Even- tos como configurar um evento).

» **Alterar nome da impressão digital:** selecione este ícone para alterar o nome da impressão digital.

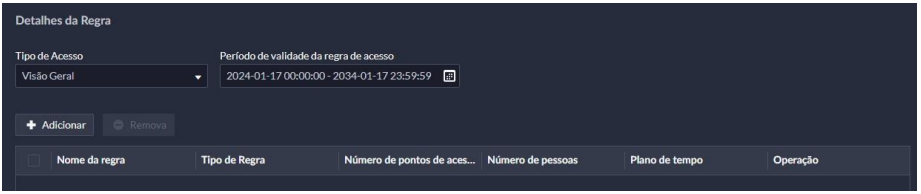
» **Excluir impressão digital:** selecione este ícone para excluir a digital da plataforma.

Senha de autenticação multifator

Senha numérica de 6 dígitos para uma segunda camada de segurança no acesso.



Detalhes da regra



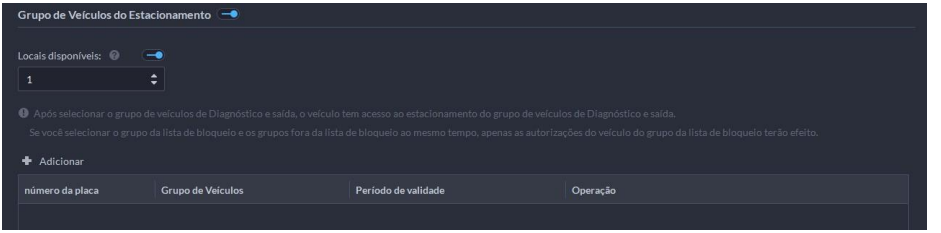
Também é possível vincular um tipo de acesso e um período de validade, que indica o nível de permissão e prazo para vencimento dos métodos de autenticação da pessoa.

Em *Adicionar,* é possível vincular uma regra de acesso à pessoa cadastrada. Veja *Controle de Acesso* para mais informações sobre criação e gerenciamento de regras de acesso.

Comparação de Rosto

Vincula a pessoa cadastrada a um grupo de comparação de rostos. Veja Banco de dados para ver como cadastrar um grupo de comparação de rostos.

Grupo de Veículos do Estacionamento



» **Locais disponíveis:** define à pessoa cadastrada a quantidade de vagas de estacionamento que esta pode ocupar.

Clicando em *Adicionar* 

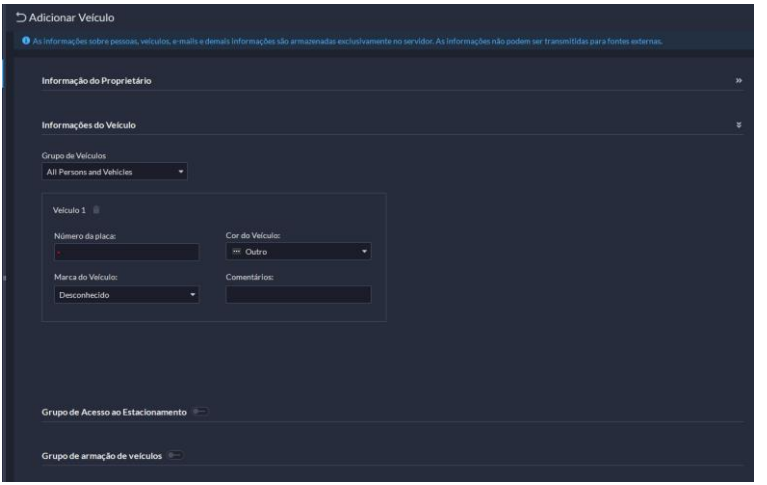
, vincula a pessoa cadastrada e seus veículos a grupos de veículos. Veja Estacionamento para mais informações sobre como gerenciar grupos de veículos.

Ao fim do cadastro, a pessoa aparecerá na lista juntamente com algumas informações cadastradas. Você pode editar informações clicando no ícone de edição  , ou excluí-la clicando no ícone de exclusão 

É possível visualizar detalhes do cadastro clicando duas vezes sob o mesmo. Também é possível visualizar o QR-code vinculado à pessoa clicando no ícone  na coluna *Informações de Autenticação.* Este QR-code pode ser utilizado para liberar acesso baseado nas permissões concedidas.

4.6.2 Cadastrar veículos

Na janela Lista de Veículos, clique em *Adicionar* para registrar um veículo na lista.



Informação do Proprietário

Caso o veículo que será cadastrado possua um proprietário cadastrado na plataforma, é possível selecioná-lo em *Selecione da lista de pessoas.* Suas informações aparecerão nas caixas abaixo.

Informações do Veículo

» **Placa do veículo:** a placa é o identificador do veículo, ela será vinculada à pessoa cadastrada.

» **Cor do veículo:** selecione a cor do veículo na lista suspensa.

» **Marca do veículo:** selecione a marca do veículo na lista suspensa.

» **Comentários:** adicione comentários sobre o veículo no campo.

Grupo de Acesso ao Estacionamento

» **Locais disponíveis:** caso um proprietário esteja vinculado ao veículo, este campo aparece. Define ao proprietário a quantidade de vagas de estacionamento que esta pode ocupar. Veja *Estaciona- mento* para mais informações.

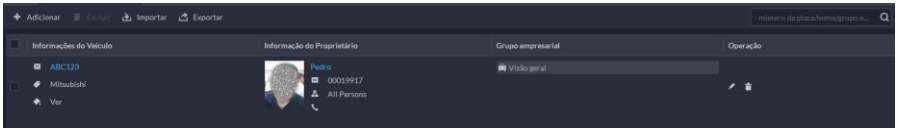
Clicando em *Adicionar* 

, vincula veículos a grupos de veículos e um período de validade. Veja *Estacionamento* para mais informações sobre como gerenciar grupos de veículos.

Grupo de armação de veículos

Clicando em *Adicionar* 

, vincula veículos a grupos de armação de veículos e um período de validade. Veja Banco de dados para mais informações sobre como gerenciar grupos de armação de veículos.



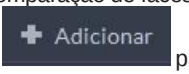
Ao fim do cadastro, o veículo aparecerá na lista juntamente com algumas informações cadastradas. Você pode editar informações clicando no ícone de edição  , ou excluí-lo clicando no ícone de exclusão 

É possível visualizar detalhes do cadastro e editá-lo clicando duas vezes sob o mesmo.

4.7. Banco de dados

O banco de dados é uma interface do Defense IA para criação e gerenciamento de grupos de armação de pessoas e veículos. Ou seja, é um ambiente para organizar as pessoas e veículos registrados na plataforma a fim de administrar inteligências de reconhecimento sob estes, permitindo identificá- los para notificação de alarmes e eventos. Veja *Eventos* para mais informações.

Banco de dados facial

No banco de dados facial é possível criar grupos de comparação de faces e cadastrar pessoas e/ou adicionar da Lista de pessoas. Clique em *Adicionar* 

para criar o grupo.

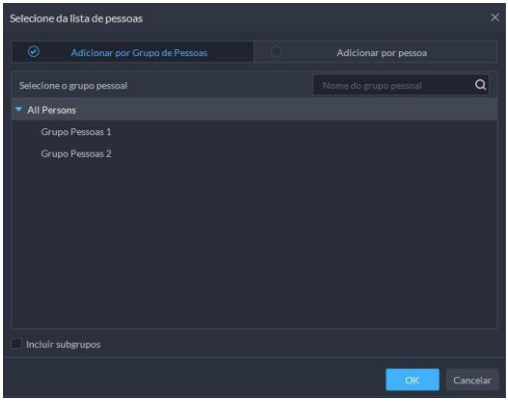
Insira um nome para o grupo e selecione uma cor para identificá-lo. O módulo permite também a inserção de comentários.

Clique em *Adicionar* para criar o grupo, *Salvar grupo e Adicionar pessoas* para registrar uma nova pessoa no grupo e, automaticamente, na lista de pessoas.

»  : botão para registrar pessoas ao grupo. Veja *Cadastro de Pessoas* para mais instruções de registro de pessoas.

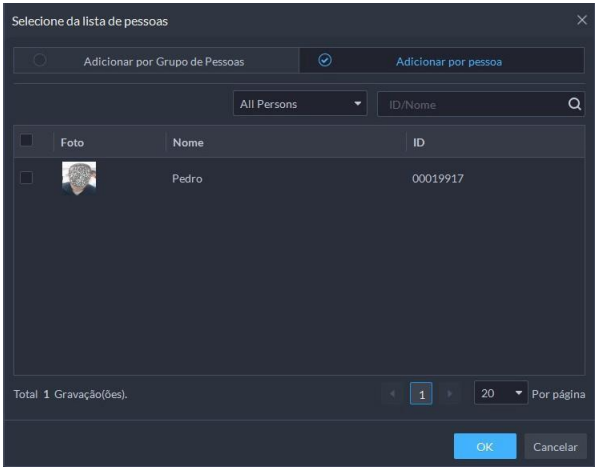
»  : botão para adicionar pessoas ao grupo a partir da lista de pessoas. Existem duas opções.

Adicionar por Grupo de Pessoas



Indique o grupo e/ou subgrupos que deseja incluir no banco de dados facial, clique em *OK*, os integrantes do grupo de pessoas selecionado serão inseridos no grupo facial.

Adicionar por Lista de Pessoas



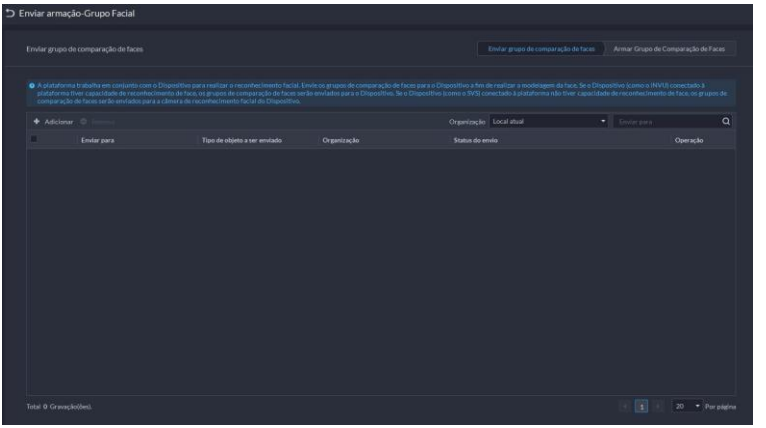
Selecione o grupo de pessoas no qual deseja buscar as pessoas na lista suspensa mostrada abaixo.

Selecione as pessoas que deseja incluir no banco de dados facial, clique em *OK,* os integrantes selecionados serão inseridos no grupo facial.

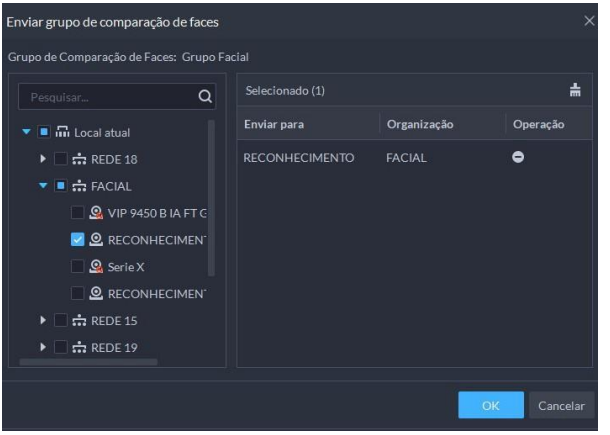
»  : botão para enviar e armar o grupo facial para dispositivos compatíveis com reconhecimento facial, como câmeras e gravadores.

Enviar grupo de comparação e faces

A armação do grupo facial em dispositivos resume-se em duas etapas. Primeiramente, deve-se enviar o grupo de faces em questão para o dispositivo.



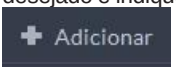
Para enviar o grupo, clique em em *Adicionar*  e selecione os dispositivos que deseja enviar o grupo



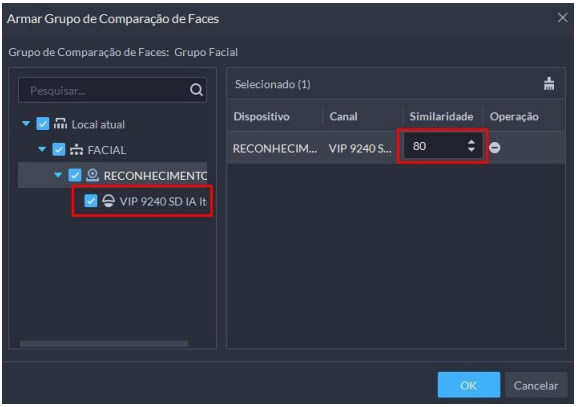
Ao clicar em *OK,* o(s) dispositivo(s) aparecerão na lista, assim como o status do envio do grupo facial para este(s). Clique em *Próxima etapa* no final da página.

Armar grupo de comparação e faces

Para iniciar a comparação de faces obtidas pelo dispositivo com o grupo adicionado, ative o canal desejado e indique o valor de similaridade para identificação da face. Para isso, clique em *Adicionar*



.



Ao clicar em *OK,* o canal selecionado é ativado para comparação de faces com o grupo configurado.

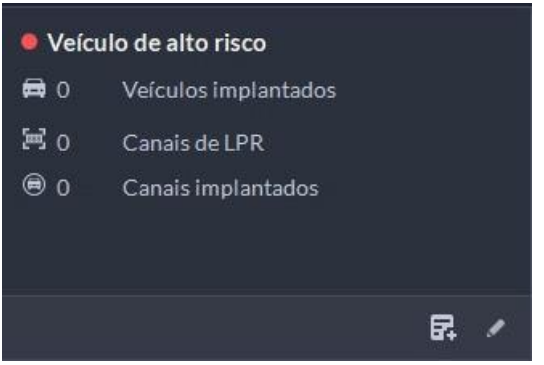
É possível adicionar mais pessoas ao grupo facial após armação e configuração dos canais, o sistema atualiza o envio ao dispositivo automaticamente. Caso o dispositivo esteja indisponível, o ícone  aparecerá, indicando a falha no envio.

»  : botão para editar o grupo facial. É possível alterar nome, cor e comentários.

»  : botão para excluir o grupo facial.

Banco de dados de veículos

Assim como o banco de dados facial, no banco de dados de veículos é possível criar grupos de comparação de veículos e adicionar da Lista de veículos. Por padrão, um grupo que indica veículos de alto risco já vem configurado, é possível incluir veículos a este grupo e editar sua cor de identifi- cação, mas não é possível renomeá-lo.

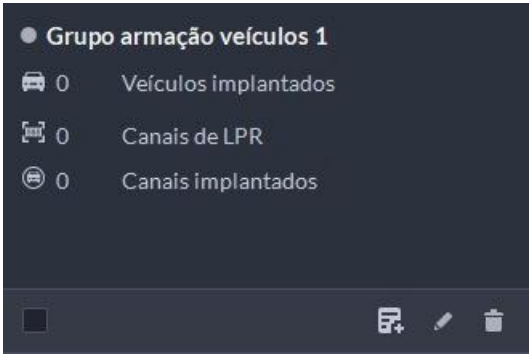


Ao contrário do banco de dados facial, não é necessário enviar o grupo a dispositivos de inteligência, uma vez que estes já identificam e vinculam-se automaticamente a dispositivos LPR cadastrados no sistema.

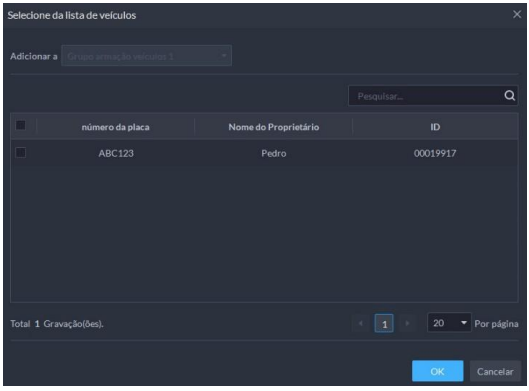
Clique em *Adicionar* 

na aba de ferramentas acima na tela para criar um novo grupo de armação de veículos.

Insira um nome para o grupo e selecione uma cor para identificá-lo. O módulo permite também a inserção de comentários. Clique em *Adicionar* para criar o grupo.



»  : botão para inserir veículos ao grupo. Veja *Cadastro de Veículos* para mais instruções de registro de veículos.



Selecione os veículos que deseja incluir no grupo de armação, clique em *OK,* os veículos selecionados serão adicionados ao grupo e os canais de LPR vinculados automaticamente.

»  : botão para editar o grupo de armação de veículos. É possível alterar nome, cor e comentários.

»  : botão para excluir o grupo de armação de veículos.

4.8. Controle de acesso

» **Controle de Acesso:** emita cartões, colete impressões digitais e dados faciais, e aplique permissões, para que as pessoas autorizadas possam abrir portas usando cartões, reconhecimento facial ou impressões digitais.

» **Funções Avançadas:** configure regras avançadas de controle de acesso, como Desbloqueio com Primeiro Cartão, Desbloqueio com Múltiplos Cartões, Anti-retorno e Interbloqueio, para aumentar a segurança.

» **Preparações:** certifique-se de que as seguintes preparações foram feitas:

- » Os dispositivos de controle de acesso estão corretamente implantados. Para detalhes, consulte o manual do dispositivo correspondente.
- » As configurações básicas da plataforma foram concluídas
- » Ao adicionar dispositivos de controle de acesso, selecione Controle de Acesso como categoria do dispositivo.
- » (Opcional) Na página de Vinculação de Recursos, vincule canais de vídeo aos canais de controle de acesso.
- » As informações do pessoal estão corretamente adicionadas.

» **Configurando Ambientes:** um ambiente é uma coleção de permissões de acesso a portas e eleva- dores. Crie ambientes para definir rapidamente áreas de controle de segurança com permissões diferentes. Apenas o administrador pode adicionar, editar e excluir ambientes.

» **Adicionando um Ambiente:**

Procedimento:

1. Faça login no Cliente Defense IA. Na página inicial, clique em e, em seguida, na seção *Configura- ção de Aplicativo,* selecione *Controle de Acesso* > *Gerenciamento de Ambientes.*
2. Clique em  .
3. Configure as informações e clique em *OK.*

Parâmetros	Descrição
Ambiente Pai	Selecione um ambiente pai para gerenciamento de permissões. Por exemplo, se um usuário tem permissões para o ambiente A, o usuário também terá permissões para todas as subzonas sob o ambiente A por padrão. Permissões adicionais podem ser configuradas para as subzonas.
Nome do Ambiente	Insira um nome para o ambiente
Ícone	Selecione um ícone para o ambiente. Os ícones são usados para que os usuários identifiquem rapidamente diferentes ambientes.
Funções Permitidas	Apenas as funções selecionadas e seus usuários podem acessar este ambiente. Clique para ver  os usuários atribuídos às funções.

» **Adicionando Ambientes em Lote**

Procedimento:

1. Faça login no Cliente Defense IA. Na página inicial, clique em e, em seguida, na seção *Confi- guração de Aplicativo,* selecione *Controle de Acesso > Gerenciamento de Ambientes.*
2. Clique em um ambiente e, em seguida, clique em . Todos os ambientes serão adicionados como sub-ambientes do que você selecionou.
3. Clique em *Adicionar* para adicionar mais níveis. Há apenas 1 nível por padrão. Pode haver até 8 níveis de ambientes. Por exemplo, se o ambiente que você seleciona é um ambiente de nível 3, você pode adicionar apenas 5 níveis de ambientes abaixo dele.
4. Configure os parâmetros para cada nível e clique em *OK*. Você pode verificar os resultados para suas configurações atuais.

Parâmetro	Descrição
Nível	O número indica o nível do ambiente. A região com um número maior é um subambiente da região com o número menor. Por exemplo, o ambiente de nível 2 é um subambiente do ambiente de nível 1.
Nome do Ambiente	Insira um nome para o ambiente.
Número Inicial	Insira um número inicial e todos os ambientes desse nível serão numerados automaticamente. Por exemplo, se o número inicial é 1 e a quantidade de ambientes é 3, então os ambientes serão numerados como ambiente 1, ambiente 2 e ambiente 3.
Quantidade	Insira um número para cada ambiente. O número de ambientes de cada nível = níveis superiores × o nível atual. Por exemplo, os números dos níveis 1, 2 e 3 são 1, 2 e 3. Então, o número de ambientes de nível 3 = 1×2×3 = 6.
Selecionar Ícone	Selecione um ícone para o ambiente. Os ícones são usados para que os usuários identifiquem rapidamente diferentes ambientes.

5. Clique em *OK*. As funções que têm permissão para acessar o ambiente pai serão automaticamente aplicadas aos subambientes.

» **Edição e Exclusão de Ambientes:** apenas administradores podem editar e excluir ambientes.

Faça login no Cliente Defense IA. Na página inicial, clique em e, em seguida, na seção *Configuração de Aplicativo,* selecione *Controle de Acesso > Gerenciamento de Ambientes.*

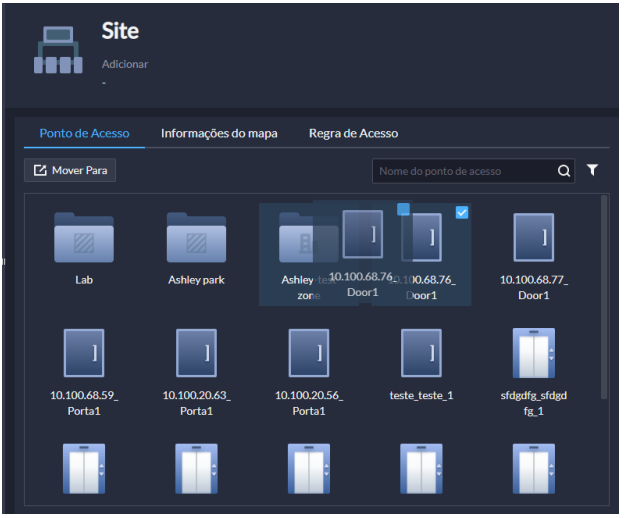
» Clique em um ambiente e , em seguida, clique em para editar as informações do ambiente, incluindo o nome, ícone e funções permitidas de acesso.

» Clique em um ambiente e , em seguida, clique em para excluí-lo. Após a exclusão do ambien- te, todas as informações relacionadas ao ambiente também serão excluídas, incluindo subam- bientes, regras de acesso e mapas. Pontos de acesso nesse ambiente e seus subambientes serão movidos para o ambiente raiz.

» **Movendo Pontos de Acesso:** pontos de acesso incluem canais de controle de portas e elevadores. Os pontos de acesso em um ambiente podem ser movidos para outros ambientes. Após adicionar dispositivos de controle de acesso, dispositivos de intercomunicador de vídeo com funções de controle de acesso e dispositivos de controle de elevadores à plataforma, os pontos de acesso dos canais de controle de portas e elevadores serão gerados e adicionados ao ambiente raiz por padrão. Você precisa alocá-los a outros ambientes.

Procedimento:

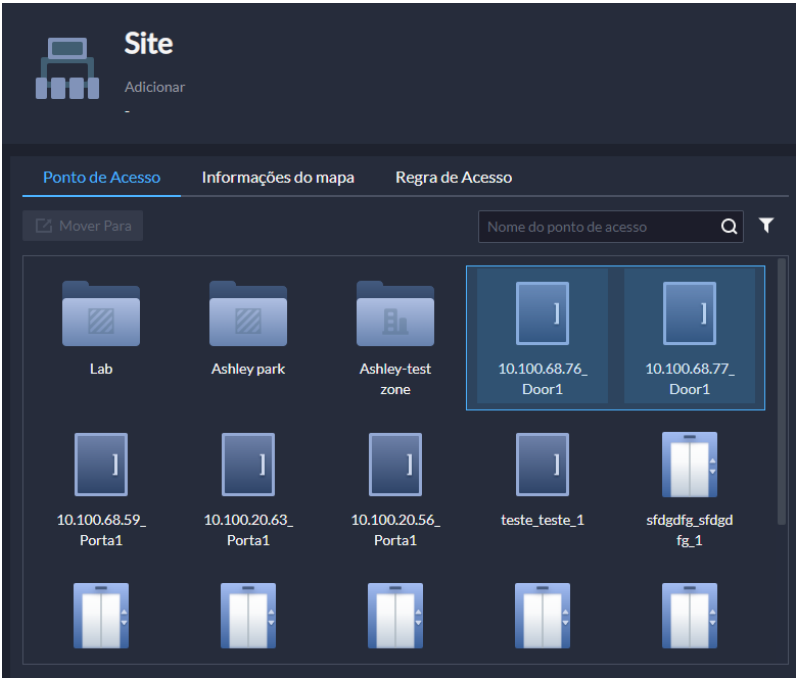
1. Faça login no Cliente Defense IA. Na página inicial, clique em e, em seguida, na seção Configuração de Aplicativo, selecione Controle de Acesso > Gerenciamento de Ambientes.
2. Clique em um ambiente e, em seguida, clique em Ponto de Acesso. Todos os pontos de acesso e subambientes serão exibidos.
3. Mova os pontos de acesso. Após mover os pontos de acesso, as regras de acesso dos ambientes atuais não serão aplicadas a eles, e suas informações no mapa também serão excluídas. As regras de acesso do ambiente alvo serão aplicadas a eles. Pontos de acesso que foram configurados com regras de acesso não podem ser movidos.
   » Mover um ponto de acesso. Arraste um ponto de acesso para um subambiente.



Clique com o botão direito em um ponto de acesso, selecione Mover Para e, em seguida, sele- cione um ambiente.

» Mover vários pontos de acesso.

1. Arraste para selecionar vários pontos de acesso. Ou passe o mouse sobre um ponto de acesso, clique na caixa de seleção para selecioná-lo e, em seguida, repita as operações para selecionar vários pontos de acesso.



2. Arraste os pontos de acesso para um subambiente. Ou clique em Mover Para e selecione um ambiente. Ou clique com o botão direito em qualquer ponto de acesso selecionado, clique em Mover Para e selecione um ambiente. Você também pode arrastar para selecionar pontos de acesso nos resultados da busca.

» **Configurando Pontos de Acesso**

» **Visualizando Detalhes do Ponto de Acesso:** visualize as informações de um ponto de acesso, incluindo o nome, tipo, ambiente ao qual pertence, recursos vinculados e regras de acesso.

Procedimento:

1. Faça login no Cliente Defense IA. Na página inicial, clique em e, em seguida, na seção *Configuração de Aplicativo,* selecione *Controle de Acesso* > *Gerenciamento de Ambientes.*
2. Clique em um ambiente e, em seguida, clique em *Ponto de Acesso.*
3. Clique duas vezes em um ponto de acesso para visualizar seus detalhes.
   - » **Nome do Ponto de Acesso:** o nome do ponto de acesso que pode ser alterado.
   - » **Tipo de Ponto de Acesso:** exibe o tipo do ponto de acesso, porta ou elevador.
   - » **Nome do Ambiente:** exibe o nome do ambiente ao qual o ponto de acesso pertence.
   - » **Recursos Vinculados:** exibe o nome e tipo do canal do ponto de acesso, o nome e tipo do dispositivo de intercomunicador ao qual pertence, e os canais de vídeo vinculados a ele. Se você deseja vincular recursos a este ponto de acesso, você pode clicar em Vinculação de Canais para ir rapidamente à página.

» **Regra de Acesso:**

O uso da regra de intertravamento (clausura) não é recomendado quando regras de antipassback estão habilitadas e ativas dentro do mesmo cenário ou contexto.

exibe as regras de acesso aplicadas a este ponto de acesso em si e ao ambiente ao qual pertence. Clique duas vezes em uma regra para visualizar seus detalhes. Você pode adicionar ou excluir regras, mas as regras do ambiente não podem ser excluídas.

» **Definindo Limites:** defina pontos de acesso como limites para contar pessoas que entraram, saíram ou entraram, mas não saíram.

Procedimento:

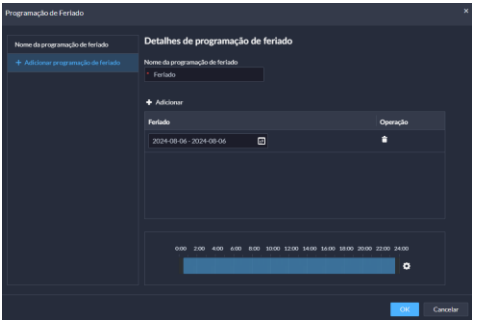
1. Faça login no Cliente Defense IA. Na página inicial, clique em e, em seguida, na seção Configuração de Aplicativo, selecione Controle de Acesso > Gerenciamento de Ambientes.
2. Clique em um ambiente e, em seguida, clique em Ponto de Acesso.
3. Clique com o botão direito em um ponto de acesso e selecione Definir como Limite. Um ícone será exibido no canto inferior direito do ícone do ponto de acesso.

» **Configurando Regras de Acesso para um Ambiente:**

uma regra de acesso define a permissão e o horário efetivo dessa permissão para canais de elevadores ou portas. Configure uma regra de acesso para um ambiente e ela será aplicada a todos os pontos de acesso dentro dele. Apenas administradores podem configurar regras de acesso.

Procedimento:

1. Faça login no Cliente Defense IA. Na página inicial, clique em e, em seguida, na seção *Configuração de Aplicativo,* selecione *Controle de Acesso > Gerenciamento de Ambientes.*
2. Clique em um ambiente e, em seguida, clique em Regra de Acesso.
3. Clique em *Citar.* Esta página exibe regras que foram adicionadas. Você pode selecionar e usar qualquer uma delas diretamente.
4. Clique em *Adicionar* e configure os parâmetros da nova regra de acesso. Ao configurar uma regra de acesso para um ambiente, você pode apenas configurar regras de verificação geral para portas.

Parâmetro	Descrição
Nome da Regra	Digite um nome para a regra.
Tipo de Ponto de Acesso	Apenas Porta está disponível.
Tipo de Regra	Apenas Verificação Geral está disponível. Para este tipo de regra, as portas podem ser desbloqueadas por cartões, impressões digitais e senhas.
Modelo de Tempo	Selecione quando esta regra será efetiva.
Programação de Feriado	Selecione quando esta regra não será efetiva. Você pode adicionar até 4 planos de férias. Siga os passos abaixo para criar um novo plano de férias: 1. Selecione Adicionar programação de Feriado na lista suspensa. 2. Digite um nome para a programação de feriado. 3. Clique em Adicionar para adicionar e configurar um feriado. Você pode adicionar até 16 feriados. 4. Configure os períodos efetivos para cada dia no feriado. Você pode arrastar na linha do tempo ou clique para configurar os períodos com mais precisão. É possível configurar até 4 períodos. 5. Clique em *OK.* 
Selecionar por Grupo de Pessoas	Selecione um ou mais grupos de pessoas, e então todas as pessoas nos grupos terão permissões para acessar todos os canais de porta no ambiente. Selecione Vincular Sub-nó e então você pode selecionar um ambiente e todos os seus subambientes ao mesmo tempo.

5. Selecione as regras de acesso e, em seguida, clique em OK.

» **Configurando o Mapa:** no mapa de um ambiente, você pode marcar pontos de acesso e subam- bientes para gerenciar melhor e localizar rapidamente eventos. Você pode configurar um mapa para cada ambiente. Além dos administradores, qualquer usuário pode configurar mapas para ambientes se tiver permissões para acessar os ambientes. No entanto, se um usuário não tiver acesso à função de mapa, não conseguirá configurar o mapa para nenhum ambiente.

» **Adicionando Mapa:**

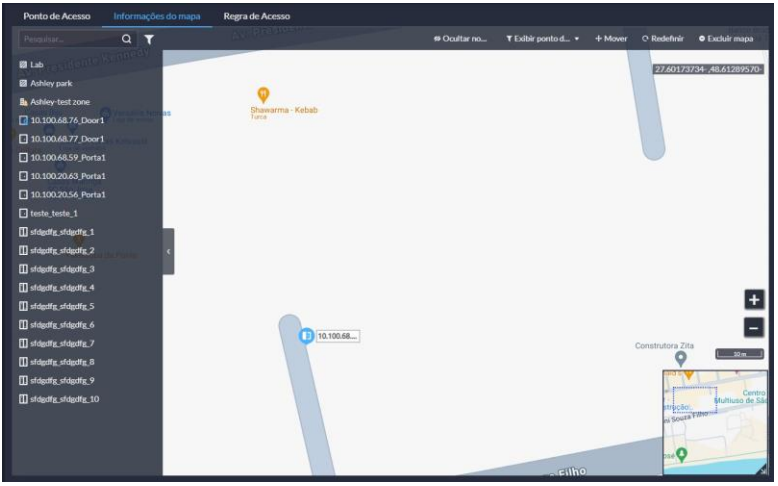
Procedimento:

1. Faça login no Cliente Defense IA. Na página inicial, clique em e, em seguida, na seção *Configuração de Aplicativo,* selecione *Controle de Acesso > Gerenciamento de Ambientes.*
2. Clique em um ambiente e, em seguida, clique em Informações do Mapa.
3. Clique em *Configurar Mapa* para adicionar um mapa para o ambiente.
   - » Selecione um mapa que tenha sido adicionado à plataforma.
   - » Faça upload de uma imagem como o mapa. Após adicionado, o mapa será incorporado à plataforma como um mapa principal.
4. Clique em *OK.*

» **Marcando Ponto de Acesso e Subambiente:**

Procedimento:

1. Faça login no Cliente Defense IA. Na página inicial, clique em e, em seguida, na seção *Configuração de Aplicativo,* selecione *Controle de Acesso > Gerenciamento de Ambientes.*
2. Clique em um ambiente e, em seguida, clique em *Informações do Mapa.*
3. Arraste um subambiente ou ponto de acesso para o mapa.



» **Marcando Subambiente:** ao marcar um subambiente, é necessário configurar um mapa para ele.

- » Se um mapa foi adicionado como submapa do mapa atual, você pode selecioná-lo diretamente como o mapa para o subambiente.
- » Se nenhum mapa foi adicionado para o subambiente, você pode adicionar um novo mapa para ele. O novo mapa será adicionado como submapa do mapa atual.
- » Se você adicionou um mapa para o subambiente, mas ele não é um submapa do mapa atual, você não conseguirá marcar o subambiente no mapa.

» **Operações Relacionadas:**

» **Ocultar Nome do Ponto de Acesso:** exibe apenas o ícone dos pontos de acesso.

» **Mostrar Ponto de Acesso:** selecione quais tipos de pontos de acesso devem ser exibidos no mapa.

» **Mover:** clique em *Mover* e, em seguida, ajuste as localizações dos subambientes e pontos de acesso no mapa.

» **Redefinir:** restaura o mapa para sua posição inicial e nível de zoom.

» **Remover Mapa:** remove o mapa deste ambiente. Esta operação não excluirá o mapa da plataforma.

» **Configurando Regras de Acesso:**

O uso da regra de intertravamento (clausura) não é recomendado quando regras de antipassback estão habilitadas e ativas dentro do mesmo cenário ou contexto.

uma regra de acesso define a permissão e o tempo efetivo dessa permissão para canais de elevadores ou portas. Apenas administradores podem configurar regras de acesso.

» **Visualizando Detalhes da Regra de Acesso:** esta página exibe todas as regras de acesso na pla- taforma, incluindo aquelas configuradas para uma pessoa, grupo de pessoas, ambiente e ponto de acesso.

1. Faça login no Cliente Defense IA. Na página inicial, clique em  , e então, na seção *Configura- ção de Aplicativo,* selecione *Controle de Acesso > Regra de Acesso > Todas as Regras.*
2. Clique duas vezes em uma regra para visualizar seus detalhes.
3. Clique  em uma regra para visualizar o progresso de autorização. Se ocorrerem exceções, clique  para ver os detalhes. Siga o motivo e as instruções para lidar com a exceção e, em seguida, clique em Enviar Novamente para reenviar a regra. Note que isso só se aplica a regras de Verificação Geral. Para outros tipos de regras, você só pode reenviá-las manualmente.

» **Configurando Verificação Geral:** conceda permissões às pessoas para que possam verificar suas identificações e acessar portas ou elevadores dentro dos períodos efetivos.

Procedimento:

1. Faça login no Cliente Defense IA. Na página inicial, clique em  , e então, na seção *Configura- ção de Aplicativo,* selecione *Controle de Acesso > Regra de Acesso > Todas as Regras.*
2. Clique em *Adicionar.*
3. Configure os parâmetros e, em seguida, clique em *OK.*

Parâmetro	Descrição
Nome da Regra	Insira um nome para a regra.
Tipo de Ponto de Acesso	Selecione Porta ou Elevador, e a plataforma exibirá apenas os canais correspondentes.
Tipo de Regra	Selecione Verificação Geral.
Modelo de Tempo	Selecione quando esta regra é efetiva.
Programação de Feriado	Selecione quando esta regra não é efetiva. Você pode adicionar até 4 planos de férias. Siga os passos abaixo para criar um novo plano de férias: 1. Selecione Programação de Feriado na lista suspensa. 2. Insira um nome para a Programação de Feriado. 3. Clique em Adicionar para adicionar e configurar um feriado. Você pode adicionar até 16 feriados. 4. Configure os períodos efetivos para cada dia no feriado. Você pode arrastar na linha do tempo ou clicar  para configurar os períodos de forma mais precisa. Você pode configurar até 4 períodos. 5. Clique em *OK.*

Selecionar por Ambiente	Selecione um ou mais ambientes, e então esta regra será aplicada a todos os pontos de acesso nos ambientes selecionados. Selecione Vincular Subnó, e você pode selecionar um ambiente e todos os seus subambientes ao mesmo tempo.
Selecionar por Ponto de Acesso	Selecione um ou mais pontos de acesso. Selecione Incluir Subambiente para exibir todos os pontos de acesso no ambiente selecionado e seus subambientes.
Selecionar por Grupo de Pessoas	Selecione um ou mais grupos de pessoas, e então todas as pessoas nos grupos terão permissões para acessar os pontos de acesso selecionados. Selecione Vincular Subnó, e você pode selecionar um ambiente e todos os seus subambientes ao mesmo tempo.
Selecionar por Pessoa	Selecione uma ou mais pessoas, e então elas terão permissões para acessar os pontos de acesso selecionados. Selecione Incluir Subgrupos para exibir todas as pessoas no grupo selecionado e seus subgrupos.

» **Configuração de Desbloqueio por Primeiro Pessoa:** qualquer pessoa pode acessar portas apenas depois que as pessoas que você especificou passarem. Quando você especifica várias pessoas, outras pessoas podem acessar portas após qualquer uma das pessoas especificadas passar.

Pré-requisitos: as pessoas só podem ser configuradas como primeiros desbloqueadores quando tiverem permissões para acessar portas.

Procedimento:

1. Faça login no Defense IA Client. Na página inicial, clique em  , e então, na seção *Configura- ção do aplicativo,* selecione *Controle de Acesso* > *Regra de Acesso* > *Todas as Regras.*
2. Clique em *Adicionar.*
3. Configure os parâmetros e clique em *OK.*

Parâmetros	Descrições
Nome da Regra	Insira um nome para a regra.
Tipo de Ponto de Acesso	Apenas Porta está disponível.
Tipo de Regra	Selecione Desbloqueio por Primeiro Pessoa.
Tipo de Regra após Desbloqueio pelo Primeiro Pessoa	» Normal: outras pessoas devem verificar suas identidades para passar. » Normalmente Aberto: Ttodas as pessoas podem passar sem verificar suas identidades.
Modelo de Tempo	Selecione quando esta regra é efetiva.
Ponto de Acesso	Selecione uma ou mais portas. Selecione Incluir Subambiente para exibir todos os pontos de acesso no ambiente selecionado e seus subambientes.
Pessoa	Selecione uma ou mais pessoas, e então elas terão permissões para acessar as portas. Selecione Incluir Subgrupos para exibir todas as pessoas no grupo selecionado e seus subgrupos. Tipos de acesso que afetarão a regra estão listados abaixo: » As regras de desbloqueio por primeira pessoa suportam apenas o tipo de acesso Geral. » Pessoas cujo tipo de acesso é Patrulha não serão restritas pela regra. Quando ninguém na regra de desbloqueio por primeira pessoa desbloquear a porta, pessoas cujo tipo de acesso é Patrulha ainda poderão desbloqueá-la.

» **Configurando Desbloqueio por Várias Pessoas:** vários grupos de desbloqueio devem usar seus cartões nas portas na ordem especificada para desbloqueá-las.

Procedimento:

1. Faça login no Defense IA Client. Na página inicial, clique em  , e então, na seção *Configuração*

de Aplicativos, selecione *Controle de Acesso > Regra de Acesso > Todas as Regras.*

2. Clique em *Adicionar* e configure os parâmetros.

» **Configuração do Anti-Passback:** as pessoas só podem passar na ordem definida. Por exemplo, se desejam ir para o edifício D, devem passar pelos edifícios A, B e C nesta ordem. Não é permitido entrar diretamente no edifício D.

Procedimento:

1. Faça login no Defense IA Client. Na página inicial, clique em  , e depois na seção *Configura- ção de aplicativos,* selecione *Controle de Acesso > Regra de Acesso > Todas as Regras.*
2. Clique em *Adicionar.*
3. Configure os parâmetros e clique em *OK.*

Parâmetro	Descrição
Nome da Regra	Insira um nome para a regra
Tipo de Ponto de Acesso	Apenas Portão está disponível.
Tipo de Regra	Selecione Anti-passback.
Tipo de Anti-passback	Você pode selecionar apenas os canais de porta de um dispositivo de controle de acesso para o Anti-passback Local.
Tempo de Redefinição	Se as pessoas não passarem na ordem definida, não serão autorizadas a passar por nenhuma porta dentro do tempo de redefinição. Após o tempo de redefinição, elas devem seguir a ordem desde o início. O tempo de redefinição pode variar entre 5 minutos e 24 horas.
Modelo de Tempo	Selecione quando esta regra será efetiva.
Plano de Feriado	Selecione quando esta regra não será efetiva. Você pode adicionar até 4 planos de feriado. O Anti-passback Local não suporta plano de feriado. Siga os passos abaixo para criar um novo plano de feriado: 1. Selecione Adicionar Plano de Feriado na lista suspensa. 2. Insira um nome para o plano de feriado. 3. Clique em Adicionar para adicionar e configurar um feriado.Você pode adicionar até 16 feriados. 4. Configure os períodos de efetividade para cada dia do feriado.Você pode arrastar na linha do tempo ou clicar para configurar os períodos de forma mais precisa. Você pode configurar até 4 períodos. 5. Clique em *OK.*
Ponto de Acesso	Adicione portas a diferentes grupos e, em seguida, as pessoas devem passar na ordem dos grupos para acessar as portas no último grupo.

» **Configuração de Senhas Públicas:** para uma porta, qualquer pessoa com a senha pública pode desbloqueá-la. Você pode configurar até 1.500 senhas.

Procedimento:

1. Faça login no Cliente Defense IA. Na página inicial, clique em  *Configuração de Aplicativos* e, em seguida, selecione *Controle de Acesso > Senha Pública.*
2. Clique em *Adicionar.*
3. Insira um nome para a senha, configure a senha e, em seguida, selecione os canais de porta dos dispositivos de controle de acesso e intercomunicadores de vídeo aos quais a senha será aplicada.
4. Clique em *Salvar.*
5. (Opcional) Se ocorrerem exceções, clique  para visualizar os detalhes. Resolva as exceções de acordo com os motivos fornecidos pela plataforma e, em seguida, clique em *Enviar Novamente.*

4.9. Vídeo Porteiro

Preparações:

Certifique-se de que as seguintes preparações foram feitas:

» Os dispositivos de controle de acesso estão corretamente implantados. Para detalhes, consulte os manuais de usuário correspondentes.

» As configurações básicas da plataforma foram concluídas.

Ao adicionar dispositivos de vídeo porteiro na página de Dispositivos, selecione Vídeo Porteiro como a categoria do dispositivo.

Ao adicionar dispositivos de controle de acesso que suportam vídeo porteiro, selecione Categoria do Dispositivo como Controle de Acesso nas Informações de Login e, em seguida, selecione *Termi- nal de Reconhecimento de Controle de Acesso.*

» A plataforma cria automaticamente uma sala após adicionar um TVIP.

» Qualquer modificação de configuração no dispositivo não será reportada para a plataforma. Você precisa ir à página de modificação de dispositivos do Web Manager para sincronizar manualmente a modificação.

4.9.1 Gerenciamento de Chamadas

Crie grupos de chamadas, grupos de gerenciamento e grupos de relação, e defina as relações de chamada restritas. Esta função está disponível apenas para administradores.

Clique na página do grupo de chamadas, grupo de gerenciamento ou grupo de relação, e o sistema restaurará o grupo de gerenciamento e o grupo de relação ao seu status original.

4.9.2 Configurando Grupo de Chamadas

Apenas dispositivos no mesmo grupo de chamadas podem se chamar mutuamente.

» Um grupo de chamadas será gerado automaticamente após você adicionar à plataforma um PVIP ou um dispositivo de controle de acesso que suporte vídeo porteiro. Todos os TVIPs na mesma unidade também serão automaticamente adicionados ao grupo. 2 TVIPs ou um TVIP e um PVIP no grupo podem se chamar mutuamente.

» Um grupo de chamadas será gerado automaticamente após você adicionar uma estação de confirmação secundária à plataforma. Adicione os TVIPs na mesma casa ao grupo; então a estação de confirmação secundária e os TVIPs poderão se chamar mutuamente.

» Um grupo de chamadas será gerado automaticamente após você adicionar uma estação de cerca à plataforma. Todos os TVIPs na plataforma serão automaticamente adicionados ao grupo por padrão; então a estação de cerca e os TVIPs poderão se chamar mutuamente. Você também pode clicar para editar os TVIPs no grupo, de forma que a estação de cerca possa chamar apenas certos TVIPs.

» Após serem adicionados à plataforma, os TVIPs serão automaticamente adicionados aos grupos correspondentes se estiverem associados a PVIPs, estações de confirmação secundária ou estações de cerca, para que possam se chamar mutuamente.

4.9.3 Adicionando Grupo de Gerenciamento

Divida os administradores em diferentes grupos e vincule-os a grupos de chamadas em diferentes combinações. Isso é útil quando certos administradores só podem atender chamadas de determinados dispositivos. Administradores incluem VTS e usuários com permissões para usar a função de vídeo porteiro e operar os dispositivos. O VTS será automaticamente adicionado ao grupo de gerenciamento padrão após ser adicionado.

Procedimento:

1. Faça login no Cliente Defense IA. Na página inicial, clique em *Configuração de Aplicativos* e, em seguida, selecione *Vídeo Porteiro.*
2. Clique em .
3. Clique em *Configuração de Grupo de Gerenciamento.*
4. Clique em *Adicionar Grupo.*
5. Insira o nome do grupo, selecione a conta de administrador ou VTS, e clique em *OK.*

O grupo de gerenciamento adicionado será exibido na lista.

» Para transferir membros, clique em transferir e mova o membro para outros grupos.

» Para gerenciar os membros do grupo, clique em para adicionar ou excluir membros do grupo.

4.9.6 Configurando Grupo de Relação

Vincule grupos de chamadas e grupos de gerenciamento, e os PVIPs ou TVIPs em um grupo de chamadas só poderão chamar administradores ou VTSs de um grupo de gerenciamento vinculado. Existem 2 tipos de relações:

» **Um grupo de chamadas vinculado a 1 grupo de gerenciamento:** todos os administradores online no grupo de gerenciamento receberão a chamada quando qualquer dispositivo estiver chamando. Se um administrador atender, a chamada parará de tocar para os outros administradores. A cha- mada será rejeitada apenas se todos os administradores a rejeitarem.

» **Um grupo de chamadas vinculado a vários grupos de gerenciamento:** as prioridades variam para diferentes grupos de gerenciamento. Quando qualquer dispositivo estiver chamando, todos os ad- ministradores online no grupo de gerenciamento com a maior prioridade receberão a chamada primeiro. Se ninguém atender em 30 segundos, a chamada será encaminhada para o grupo de gerenciamento com a segunda maior prioridade. Se ainda assim ninguém atender, o dispositivo indicará que não houve resposta à chamada.

Procedimento:

1. Faça login no Cliente Defense IA. Na página inicial, clique em *Configuração de Aplicativos* e, em seguida, selecione *Vídeo Porteiro.*
2. Clique em .
3. Clique em *Configuração de Grupo de Relação.*
4. Clique em *Adicionar.*
5. Insira o nome do grupo e selecione um ou mais grupos de chamadas e grupos de gerenciamento. Como apenas até 2 grupos de gerenciamento receberão uma chamada, recomendamos que você selecione no máximo 2 grupos de gerenciamento.
6. Clique em ou para ajustar a Prioridade para ajustar as prioridades dos grupos de gerenciamento e, em seguida, clique em *OK.*

O grupo de gerenciamento superior tem maior prioridade.

4.9.7 Configurando Edifício/Unidade e Modo de Chamada

Certifique-se de que o status do edifício e da unidade no Cliente Defense IA seja o mesmo do PVIP. Se o edifício e a unidade estiverem habilitados na plataforma, eles também devem estar habilitados no dispositivo e vice-versa; caso contrário, o PVIP ficará offline após ser adicionado. Isso também afeta a regra de discagem. Tome o exemplo do quarto 1001, unidade 2, edifício 1. A regra de disca- gem é a seguinte:

- » Se o edifício estiver habilitado e a unidade não, o número do quarto é “1#1001”.
- » Se o edifício estiver habilitado e a unidade também, o número do quarto é “1#2#1001”.
- » Se o edifício não estiver habilitado e a unidade também não, o número do quarto é “1001”.

Selecione um modo de chamada para especificar a ordem de chamada do TVIP e do App.

Procedimento:

1. Faça login no Cliente Defense IA. Na página inicial, clique em *Configuração de Aplicativos* e, em seguida, selecione *Vídeo Porteiro.*
2. Clique em .
3. Habilite ou desabilite o edifício e a unidade conforme necessário e, em seguida, clique em *OK.* Essa configuração deve ser a mesma das configurações do dispositivo. Caso contrário, as informações dos dispositivos podem estar incorretas. Por exemplo, se apenas o Edifício estiver habilitado em um PVIP, você deve habilitar apenas o Edifício na plataforma.
4. Configure o modo de chamada:
   - » **Chamada Simultânea:** quando um quarto está sendo chamado, todos os TVIPs e usuários do App nele receberão a chamada. Se houver apenas usuários do App no quarto, então todos os usuários do App receberão a chamada.
   - » **Chamada em Grupo:** ao chamar um quarto, apenas os TVIPs nele receberão a chamada. Se o encaminhamento de chamadas estiver habilitado nos TVIPs, então todos os usuários do App receberão a chamada.
5. Clique em *Salvar.*

4.9.6 Configurando a Sala

Adicione uma sala para incluir os TVIPs e usuários do aplicativo nele.

4.9.7 Informações de Contexto

Quando você adiciona um TVIP à plataforma, a plataforma criará automaticamente um quarto. Você também pode criar uma sala e adicionar o TVIP posteriormente. O TVIP se juntará automa- ticamente ao quarto correspondente. As salas que são criados automaticamente não podem ser excluídos. Você só pode excluir aqueles que são criados manualmente.

Procedimento:

1. Faça login no Cliente Defense IA. Na página inicial, clique em *Configuração de Aplicativos* e, em seguida, selecione *Vídeo Porteiro > Configuração da sala.*
2. Clique em *Adicionar.*
3. Selecione uma organização, insira um nome para a sala e o número da sala, e depois clique em *Adicionar.*

Se o TVIP com o mesmo número da sala já foi adicionado à plataforma, ou se o proprietário da casa com o mesmo número da sala se registrou, o TVIP ou o usuário do aplicativo se juntará automaticamente a sala.

Operações Relacionadas

Operações nos usuários do aplicativo:

» **Definir como Proprietário**: defina um usuário do aplicativo como proprietário após vinculá-lo a uma pessoa.

» **Redefinir Senha**: redefina a senha de um usuário do aplicativo. O usuário precisará fazer login no aplicativo com a nova senha.

» **Vincular Pessoa**: vincule um usuário do aplicativo a uma pessoa.

» **Excluir Usuário**: exclua um usuário do aplicativo. O usuário não poderá mais fazer login no aplicativo. Se o usuário também for um proprietário, todas as contas do aplicativo no quarto correspondente serão excluídas, e todas as pessoas nesta sala não poderão mais fazer login no aplicativo.

4.9.4 Sincronizando Contatos

Envie as informações do quarto para um PVIP e, em seguida, você poderá visualizá-las no PVIP ou em sua página da web.

Procedimento:

1. Faça login no Cliente Defense IA. Na página inicial, clique em *Configuração de Aplicativos* e, em seguida, selecione *Vídeo Porteiro.*
2. Clique em .
3. Envie as informações do quarto:

» Selecione um PVIP e clique em uma Sala.

» Selecione um PVIP e clique em **Enviar Contatos** para enviar todos ou os quartos selecionados. Agora você pode visualizar as informações do quarto no PVIP ou em sua página da web. Se algum quarto não puder ser enviado, a razão será fornecida.

Operações Relacionadas

Após enviar as informações da sala com sucesso, você pode excluí-las do PVIP; elas não serão mais exibidas no PVIP ou em sua página da web.

» Clique em *Excluir* para excluir uma sala por vez.

» Clique em *Excluir Contatos* para excluir todas ou as salas selecionadas.

4.9.4 Configurando Senha Privada

Defina senhas para a porta da sala para que a porta possa ser aberta inserindo a senha no PVIP (estação externa).

Certifique-se de que os contatos sejam enviados ao PVIP; caso contrário, você não poderá definir a senha privada.

Procedimento:

1. Faça login no Cliente Defense IA. Na página inicial, clique em *Configuração de Aplicativos* e, em seguida, selecione *Vídeo Porteiro.*
2. Clique em .
3. Selecione um PVIP e, em seguida, você poderá ver todos os TVIPs vinculados a este PVIP.
4. Selecione um TVIP e clique em , ou selecione vários TVIPs e clique em *Alterar Senha.*
5. Insira a senha e clique em *OK.*

Você pode usar a nova senha para desbloquear no PVIP.

O formato deve ser *número da sala + senha privada,* e o número da sala deve consistir em 6 dígi- tos. Por exemplo, uma pessoa que mora em 1001 com a senha privada do PVIP no edifício sendo 123456 pode inserir 001001123456 para desbloquear a porta.

4.9.6 Códigos QR

Configure as informações dos códigos QR que são usados pelos proprietários para baixar o aplicativo e registrar uma conta.

Procedimento:

1. Faça login no Cliente Defense IA. Na página inicial, clique em *Configuração de Aplicativos* e, em seguida, selecione *Vídeo Porteiro > Códigos QR.*
2. Insira um nome e algumas notas para sua comunidade e, em seguida, clique em *Salvar.*

Os proprietários podem escanear o Código QR para Download do Aplicativo para baixar e instalar o aplicativo no telefone e, em seguida, escanear o Código QR para Registro do Aplicativo para se registrar.

4.9.3 Usuário do Aplicativo

Você pode visualizar informações dos usuários do aplicativo, congelar usuários, modificar a senha de login e excluir usuários.

Pré-requisitos:

Os usuários do aplicativo devem ter se registrado escaneando o código QR na plataforma ou no TVIP. Para mais detalhes, consulte o manual do usuário do aplicativo.

Procedimento:

4. Faça login no Cliente Defense IA. Na página inicial, clique em *Configuração de Aplicativos* e, em seguida, selecione *Vídeo Porteiro.*
5. Clique em .

Operação	Descrição
Congelar Usuário do aplicativo	O usuário do aplicativo não poderá fazer login por 600 segundos após ser congelado. A conta será congelada quando o número de tentativas de senha inválida exceder 5 por um usuário do aplicativo.
Alterar Senha de Login do aplicativo	Clique em e insira uma nova senha na página de Redefinição de Senha, e depois clique em *OK.* A senha deve ter de 8 a 16 caracteres e incluir números e letras. Clique em *Mostrar Senha* para exibir a senha ou em *Ocultar Senha* para ocultá-la.
Atualizar Lista de Usuários do aplicativo	Clique em *Atualizar* para exibir os usuários do aplicativo que se registraram recentemente.
Excluir Usuário do aplicativo	Clique em *Excluir* para remover usuários do aplicativo um por vez ou selecione vários usuários e clique em *Excluir* e siga as instruções para excluí-los. Os usuários não poderão mais fazer login no aplicativo. Se um usuário for um proprietário, todas as contas do aplicativo no quarto correspondente serão excluídas, e todas as pessoas neste quarto não poderão mais fazer login no aplicativo.

4.9.6 Gerenciamento de Visitantes

Após o agendamento na plataforma e o registro das informações do visitante, o visitante pode obter permissão de acesso. A permissão de acesso é desativada após a saída do visitante.

Preparações:

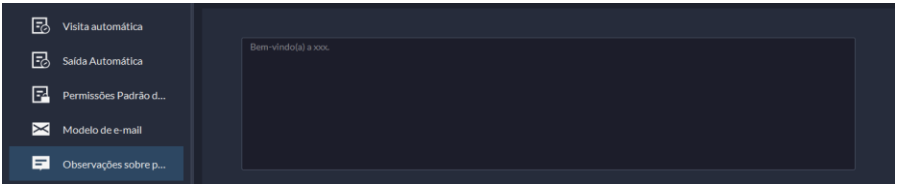
» Dispositivos de controle de acesso foram adicionados à plataforma.

» As configurações básicas da plataforma foram concluídas. Para configurar, consulte *Configurações Básicas.*

4.9.7 Configurando Configurações de Visitas

Procedimento:

1. Faça login no Cliente Defense IA. Na página inicial, clique em *Configuração de Aplicativos* e, em seguida, selecione *Visitante.*
2. Configure os parâmetros.
   - » **Visita automática**: habilite a função e selecione os canais conforme necessário. Visitantes com agendamento podem verificar suas identidades nos canais selecionados sem precisar se registrar.
   - » **Saída automática**: habilite a função e selecione os canais conforme necessário. Visitantes que estão em visita podem verificar suas identidades nos canais selecionados para encerrar suas visitas automaticamente.
     - » **Desconectar regularmente:** visitas expiradas serão automaticamente encerradas no horário definido.
     - » **Horário de desconexão diário:** para visitantes que não chegarem à sua visita antes do horário de desconexão diário, o agendamento será cancelado.
     - » **Desconectar agora:** para visitantes que perderam o agendamento ao clicar neste botão, o agendamento será cancelado.
   - » **Permissões padrão para visitantes**: defina as permissões de acesso padrão para os visitantes.
   - » **Modelo de e-mail**: você pode configurar um modelo de e-mail e enviar automaticamente e-mails quando os visitantes fizerem um agendamento, chegarem para sua visita e encerrarem sua visi- ta. Você pode personalizar o assunto e o conteúdo do e-mail com as informações do visitante, como nome e número de identificação.
   - » **Observações no passe do visitante**: personalize o conteúdo das observações no passe do visitante.



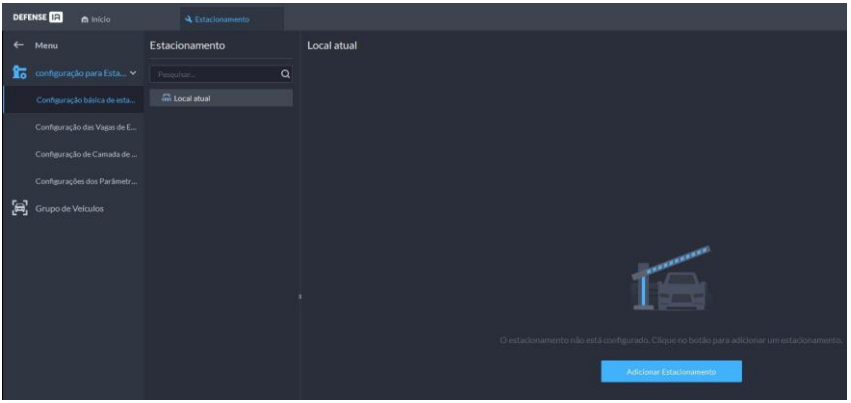
3. Clique em *Salvar.*

4.10. Estacionamento

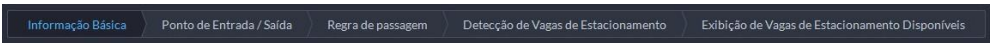
As configurações de estacionamento e grupo de veículos podem ser feitas pelo módulo de configuração de estacionamento.

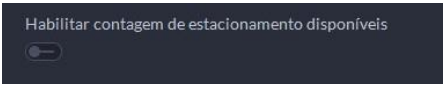
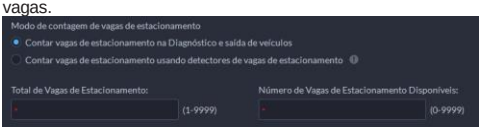
4.10.1 Configuração básica de estacionamento

Para adicionar, editar, organizar e/ou excluir um estacionamento, acesse *Configuração básica de estacionamento.* Para adicionar, clique em *Adicionar* ou *Adicionar Estacionamento.*

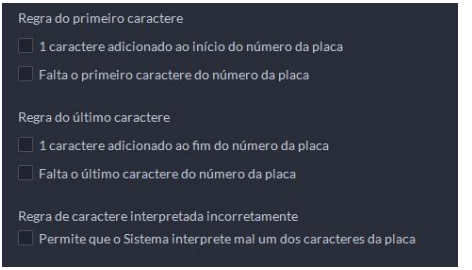


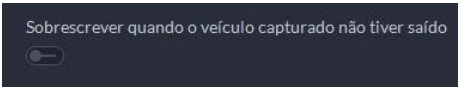
Preencha as infromações básicas do Estacionamento



Campo	Descrição
	Insira na caixa o nome que deseja chamar o estacionamento. O asterísco indica campo obrigatório.
	Botão para habilitar contagem de vagas. Quando habilitado apresenta novas opções. Selecione a opção que deseja para contagem de vagas entre Contagem por entrada e saída ou Contagem por detector de vagas.  Insira nas caixas o total de vagas que o estacionamento comporta e a quantidade de vagas disponíveis para uso (esse número não pode ser maior que o número total de vagas.).

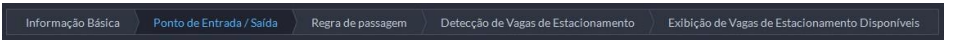
Botão para habilitar e editar regra de autopreenchimento de placas no caso de leitura incompleta. Quando habilitado apresenta novas opções.



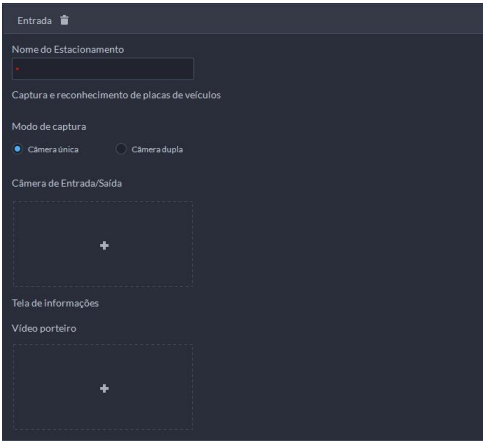


Botão para habilitar opção de sobrescrição de veículo nos registros de entrada caso o mesmo passe pela entrada mais de uma vez antes de passar em uma saída.

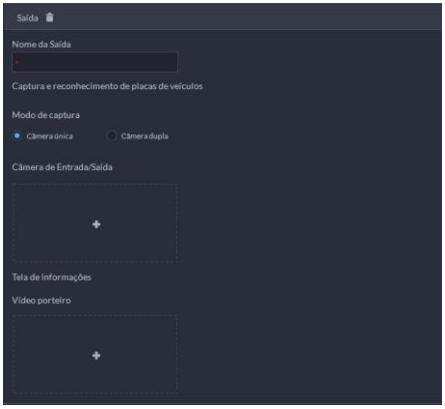
Na próxima etapa, em Ponto de Entrada/Saída, adiciona-se os pontos de acesso e dispositivos LPR de acesso do estacionamento.



Clique em *Adicionar Ponto de Entrada e Saída* para adicionar um ponto de acesso do estacionamen- to. Ao nomeá-lo, as entradas e saídas do estacionamento poderão ser adicionadas.



Campo	Descrição
Nome do Estacionamento	Insira na caixa o nome que deseja chamar a entrada do estacionamento. O asterísco indica campo obrigatório.
Modo de captura	Selecione o modo de captura entre câmera única ou câmera dupla. Caso o modo *câmera* dupla seja selecionado, aparecerá espaço para inserir um tempo de até 5s de coordenação entre as câmeras. O tempo definido é o período em que o veículo pode passar por ambas as câmeras sem haver registro duplo.
Câmera de Entrada/Saída	Clique em "+" para adicionar as câmeras que serão reposnáveis por realizar os registros de entrada. Para uma câmera realizar registros de entrada/saída ela deve estar cadastrada como um dispositivo "LPR de acesso", veja Gerenciamento de dispositivos para mais informações.
Vídeo Porteiro	Clique em "+" para adicionar dispositivos compatíveis com controle (controladoras de acesso ou vídeo porteiros) para vinculá-lo à entrada.



Campo	Descrição
Nome do Estacionamento	Insira na caixa o nome que deseja chamar a saída do estacionamento. O asterísco indica campo obrigatório.
Modo de captura	Selecione o modo de captura entre câmera única ou câmera dupla. Caso o modo *câmera dupla* seja selecionado, aparecerá espaço para inserir um tempo de até 5s de coordenação entre as câmeras. O tempo definido é o período em que o veículo pode passar por ambas as câmeras sem haver registro duplo.
Câmera de Entrada/Saída	Clique em "+" para adicionar as câmeras que serão reposnáveis por realizar os registros de saída. Para uma câmera realizar registros de entrada/saída ela deve estar cadastrada como um dispositivo *LPR de acesso,* veja *Gerenciamento de dispositivos* para mais informações.
Vídeo Porteiro	Clique em "+" para adicionar dispositivos de vídeo portaria para vinculá-lo à saída.

A plataforma suporta até 60 entradas e saídas.

Na terceira etapa, Regra de passagem, devem ser definidas as regras para entrada e saída dos veículos.

As regras de acesso podem ser definidas entre 3 opções, para veículos registrados, para todos os veículos, ou de forma personalizada.

Veículos registrados

Caso a regra de acesso seja definida para veículos registrados, clique em *Adicionar* 

e selecione se a regra deverá valer para o estacionamento todo, ou apenas para pontos de acesso escolhidos.

Selecione os grupos de veículos desejados para terem permissão de acesso e clique em *OK*. Os veículos registrados em tais grupos agora possuem permissão de acesso nos pontos de acesso do estacionamento especificados.

Veja em *Grupo de Veículos* como configurar grupos de veículos.

Permitir passagem quando o espaço disponível for 0

Ao ativar esta regra, deve-se selecionar para quais grupos permitidos essa regra valerá. Essa regra ativada habilita o acesso de veículos com permissão mesmo quando todas as vagas do estaciona- mento estiverem ocupadas.

Todos os veículos

Permitir a entrada de veículos na lista de bloqueio

Ao ativar esta regra, todos os veículos, inclusive os registrados como veículos de risco, ou na lsita de bloqueio, terão acesso liberado.

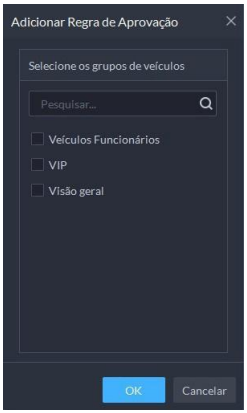
Permitir passagem quando o espaço disponível for 0

Ao ativar esta regra, deve-se selecionar para quais grupos permitidos essa regra valerá. Essa regra ativada habilita o acesso de veículos com permissão mesmo quando todas as vagas do estaciona- mento estiverem ocupadas.

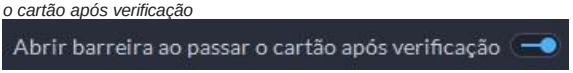
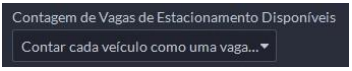
Personalizado

Caso a regra de acesso seja definida para personalizado, clique em *Adicionar* 

e selecione se a regra deverá valer para o estacionamento todo, ou apenas para pontos de acesso escolhidos.



Selecione os grupos de veículos desejados para terem permissão de acesso e clique em *OK*. Também é possível definir um período o qual a regra será válida. Os veículos registrados em tais grupos agora possuem permissão de acesso nos pontos de acesso do estacionamento e durante o período especificado.

Regra	Descrição
	Quando habilitada, permite acesso de todos os veículos. Permite a seleção de um período para a regra ser válida, assim como filtrar ou não veículos na lista de bloqueio.
	Ao ativar esta regra, deve-se selecionar para quais grupos permitidos essa regra valerá. Essa regra ativada habilita o acesso de veículos com permissão mesmo quando todas as vagas do estacionamento estiverem ocupadas.
	Quando habilitada, esta regra não permite o acesso automático ao estacionamento a veículos com permissão. O veículo é identificado, mas a entrada não é liberada. A entrada deve ser habilitada manualmente. Há duas opções: Habilitar entrada por cartão, para isso, a sub-regra *Abrir barreira ao passar o cartão após verificação*  deve ser habilitada. Ou, caso a sub-regra não seja habilitada, a entrada só será liberada por acionamento manual pelo Defense.
	Quando habilitada, esta regra permite o acesso ao estacionamento ao passar um cartão válido.
	Há três opções para realizar a contagem de vagas no estacionamento: A primeira opção contabiliza cada veículo que entra no estacionamento como uma vaga ocupada. A segunda opção contabiliza apenas veículos não registrados como vaga ocupada. Na terceira opção, 'personalizado', deve-se selecionar os grupos de veículos que não serão contabilizados como vaga ocupada.

Enviar lista negra e lista branca para o dispositivo

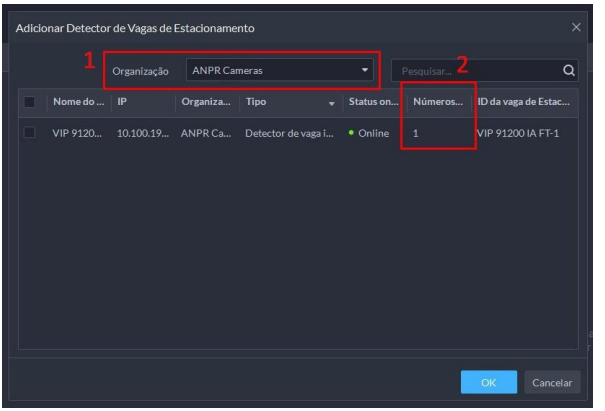
Esta regra habilita o envio de listas de permissão e bloqueio de veículos ao dispositivo de acesso LPR. Caso a plataforma esteja desconectada, o dispositivo fará a gestão de acesso com base em tais listas.

Em Detecção de vagas de estacionamento, na quarta etapa de configuração, dispositivos de detec- ção de vagas podem ser escolhidos caso o estacionamento seja configurado para realizar a gestão de vagas via sensores.

Para o funcionamento correto, o dispositivo deve estar devidamente configurado como detector de vagas. Veja em Gerenciamento de dispositivos como configurar um dispositivo compatível na plataforma.

Clique em *Adicionar* 

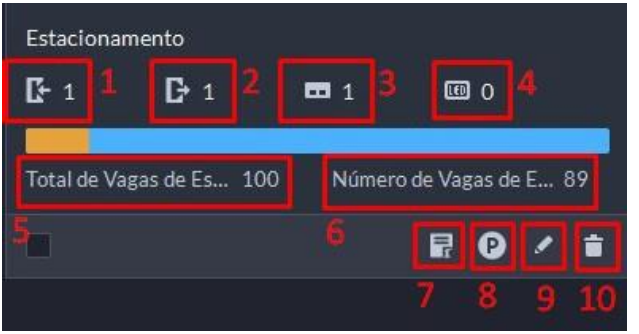
para selecionar da lista de dispositivos os sensores de vagas.



1. Filtre por organização para obter o(s) dispositivo(s) desejado(s).
2. O número de vagas configurado no dispositivo aparece na coluna indicada, este número fará parte da quantidade de vagas do estacionamento.

Na quinta etapa, caso desejado, também é possível adicionar painés LED compatíveis com a plata- forma para apresentar o número de vagas ainda disponíveis no estacionamento.

Ao fim da configuração, é possível visualizar e gerenciar o estacionamento criado.



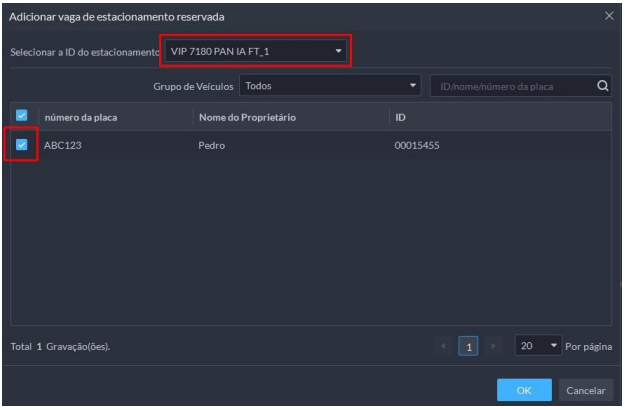
Índice	Descrição
1	Número de entradas no estacionamento
2	Número de saídas no estacionamento
3	Número de sensores de vagas no estacionamento
4	Número de painéis LED de contagem de vagas no estacionamento
5	Tota de vagas existentes no estacionamento
6	Total de vagas disponíveis no estacionamento
7	Edição rápida de regra de passagem
8	Edição rápida de vagas disponíveis
9	Edição de parâmetros do estacionamento
10	Excluir estacionamento

Configuração de vagas reservadas

Uma vaga de estacionamento reservada, vincula uma veículo registrado na plataforma (Lista de ve- ículos) a uma vaga monitorada no estacionamento. Vagas reservadas só poderão ser configuradas em estacionamentos que possuem detectores de vagas configurados.

Para reservar uma vaga, selecione o estacionamento desejado na árvore de estacionamentos à es- querda e então clique em *Adicionar* 

. Selecione a vaga e o veículo com permissão para esta vaga.



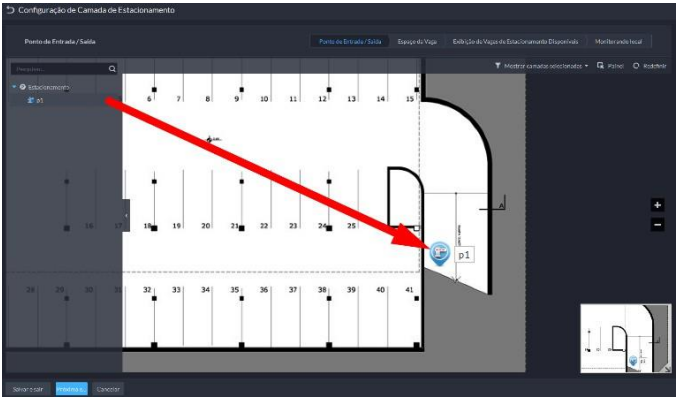
É possível selecionar mais de um veículo por vaga, desta forma, é possível cadastrar um evento para identificar quando veículos sem permissão ocuparem a vaga.

Configuração de camada de estacionamento

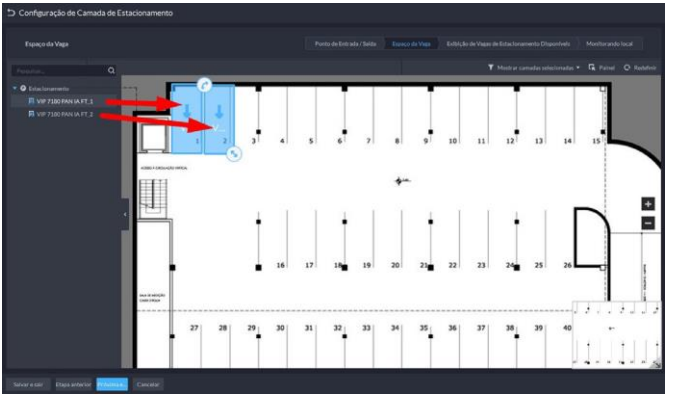
Uma camada de estacionamento é uma imagem que representa o estacionamento, para cadastrar uma, selecione o estacionamento desejado na árvore de estacionamentos à esquerda e então cli- que em A*dicionar* 

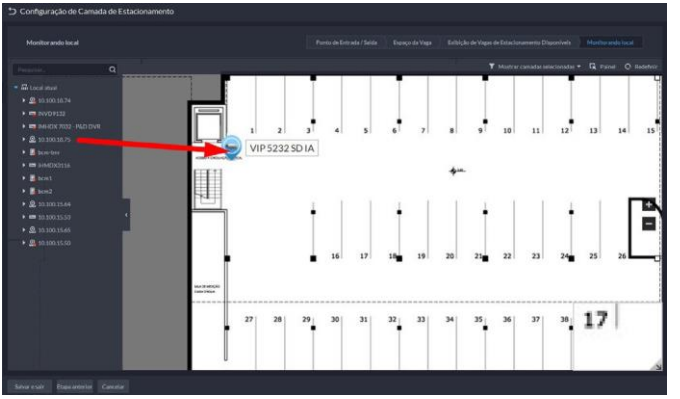
.

Nomeie e selecione a imagem desejada para prosseguir para configuração. Na primeira etapa, arraste para o mapa as entradas e saídas.



Durante a segunda e terceira etapa, arraste as vagas com detectores e os pontos de exibição de va- gas configurados. Caso o estacionamento não possua detectores ou pontos de exibição de vagas, estas etapas podem ser ignoradas.



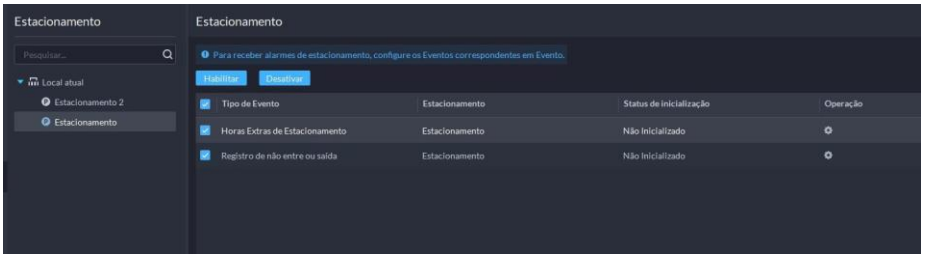


Na última etapa, arraste canais de vídeos das câmeras do estacionamento.

A camada configurada pode ser visualizada no módulo Estacionamento.

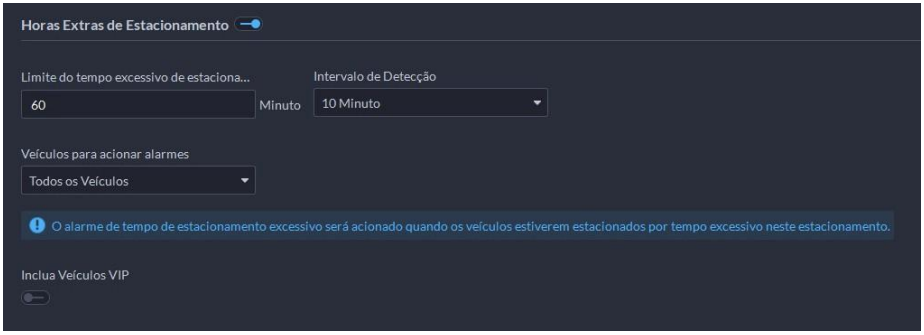
Configuração de parâmetros de eventos

Existem 2 tipos de eventos passíveis de configuração em um estacionamento na plataforma: Horas extras de estacionamento e Registro de não entrada/saída.



Para configurar as regras de cada tipo de evento, clique na engrenagem  na coluna *Operação.*

Horas extras de estacionamento



Insira parâmetros como Limite de tempo e Intervalo de detecção. O evento será acionado na cadência do intervalo de detecção sempre que um veículo ultrapassar o limite de tempo no estacionamento.

É possível configurar a regra para Todos os veículos, para apenas veículos não registrados ou na lista de bloqueio, ou de maneira personalizada, selecionando os grupos de veículos.

Registro de não entrada/saída

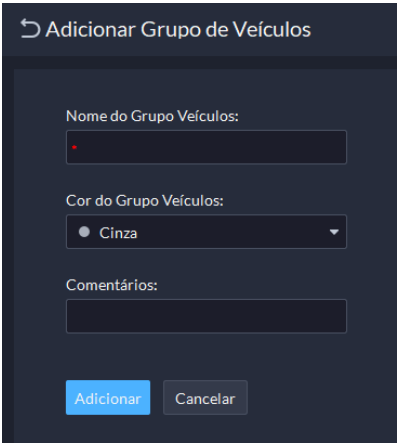
Insira parâmetros como Duração do registro e ponto de tempo estatístico. Caso algum veículo do grupo focalizado não entre ou saia do estacionamento no período definido (quando a duração do registro, em dias, for excedida), o evento será acionado. A plataforma utiliza o ponto de tempo estatístico para finalizar o período de contagem de 1 registro.

É possível utilizar tais eventos para gerar alarmes na plataforma, veja Central de Eventos para mais informações.

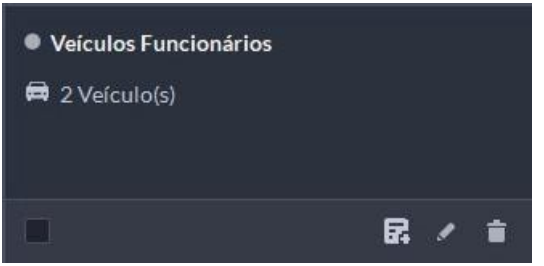
Grupo de veículos

Em grupo de veículos é possível criar e administrar grupos de veículos para a organização e gerenciamento de veículos registrados na platforma.

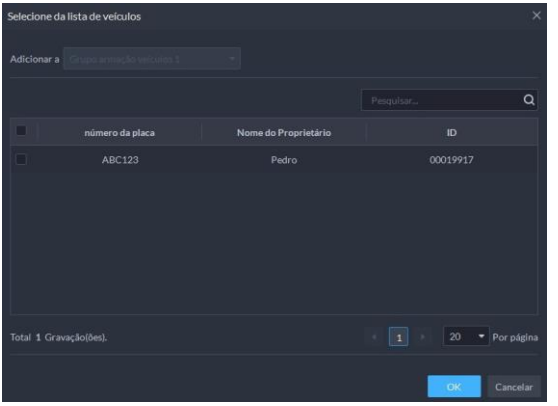
Por padrão, 3 grupos já vêm configurados: Visão geral, VIP e Lista negra. É possível adicionar veícu- los à tais grupos da Lista de veículos. Para criar um novo grupo, clique em *Adicionar.*



Insira um nome para o grupo e selecione uma cor para identificá-lo. O módulo permite também a inserção de comentários. Clique em *Adicionar* para criar o grupo.



»  **:** botão para inserir veículos ao grupo. Veja Cadastro de Veículos para mais instruções de registro de veículos.



Selecione os veículos que deseja incluir no grupo, clique em *OK,* os veículos selecionados serão adicionados ao grupo.

»  : botão para editar o grupo de armação de veículos. É possível alterar nome, cor e comentários.

»  : botão para excluir o grupo de armação de veículos.

4.11. Análise Inteligente

Antes de usar as funções de contagem de pessoas e relatórios agendados, é necessário configurá-las primeiro:

» **Contagem de Pessoas:** crie um grupo de contagem de pessoas e adicione várias regras de con- tagem de pessoas de um ou mais dispositivos a ele. Depois, você pode visualizar o número em tempo real e histórico de pessoas do grupo.

» **Relatório Agendado:** configure quando enviar um relatório com dados históricos de contagem de pessoas, o endereço de e-mail para o qual enviar o relatório e o conteúdo do e-mail.

4.11.1 Grupo de Contagem de Pessoas

Crie um grupo de contagem de pessoas e adicione várias regras de contagem de pessoas de um ou mais dispositivos. Na Análise Inteligente, você pode visualizar o número em tempo real e histórico de pessoas do grupo.

Procedimento:

1. Faça login no Cliente Defense IA. Na página inicial, clique em *Configuração de Aplicativos* e, em seguida, selecione *Análise Inteligente > Configuração de Grupo de Contagem de Pessoas.*
2. Clique em *Adicionar* no canto superior esquerdo.
3. Configure os parâmetros e clique em *Adicionar.*

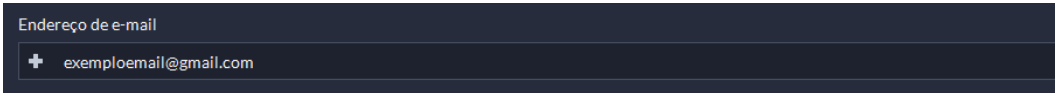
Parâmetro	Descrição
Nome do Grupo de Contagem de Pessoas	Quando ativado, você pode configurar os limites de multidão e excesso de pessoas para o grupo. Se um alarme estiver configurado ao mesmo tempo, os alarmes serão acionados quando o número de pessoas atingir os limites estabelecidos. Limite de Multidão: Quando o número de pessoas no grupo atinge o limite de multidão definido, mas é menor que o limite de excesso, a luz ficará amarela. Limite de Excesso: Quando o número de pessoas no grupo atinge o limite de excesso definido, a luz ficará vermelha.
Limite de multidão	
Limite acima do limite	
Regra	Selecione os dispositivos cujas regras de contagem de pessoas você deseja incluir no grupo, e então seus dados serão combinados.

4.11.4 Relatório Agendado

Dados históricos serão enviados regularmente para um ou mais endereços de e-mail que você definir no horário agendado.

Procedimento:

1. Faça login no Cliente Defense IA. Na página inicial, clique em *Configuração de Aplicativos* e, em seguida, selecione *Análise Inteligente* > *Configuração de Relatório Agendado.*
2. Configure um ou mais tipos de relatório.
   - » **Relatório Diário:** dados do dia anterior serão enviados para seu e-mail em um horário definido. Se definido para 03:00:00, os dados do dia anterior (00:00:00–23:59:59) serão enviados para seu e-mail às 03:00:00 todos os dias.
   - » **Relatório Semanal:** dados da semana passada serão enviados para seu e-mail em um horário definido. Se definido para 03:00:00 na quarta-feira, os dados de quarta-feira a terça-feira de cada semana serão enviados para seu e-mail às 03:00:00 todas as quartas-feiras.
   - » **Relatório Mensal:** dados do mês passado serão enviados para seu e-mail em um horário definido. Se definido para 03:00:00 no dia 3, os dados do dia 3 do mês passado até o dia 2 do mês atual serão enviados para seu e-mail às 03:00:00 do dia 3 de cada mês.
3. Configure um ou mais endereços de e-mail para enviar o relatório e o conteúdo do e-mail.
   - » Clique para selecionar os usuários que possuem endereços de e-mail configurados, ou insira um endereço de e-mail e pressione *Enter.*



4. Configure o conteúdo do e-mail.
5. Envie o relatório.
   - » Clique em *Enviar Agora* para enviar imediatamente o relatório que você configurou.

4.12. Inspeção Inteligente

Configure objetos e planos de inspeção para que a plataforma possa inspecionar regularmente dispositivos, como equipamentos elétricos, ou uma área, e coletar imagens e dados durante o processo.

Antes de usar esta função, você deve:

1. Adquirir uma licença com a função de inspeção inteligente e ativar a licença.
2. Obter e instalar o plugin de inspeção inteligente.
3. Configurar discos de imagem e vídeo, para armazenar instantâneos e vídeos gravados durante as inspeções.
4. Adicionar dispositivos utilizados para inspeção à plataforma e configurar seus períodos de retenção de vídeo.

4.12.5 Configurando o Modelo de Objeto

Configure tipos de objetos e pontos de inspeção frequentemente usados. Ao configurar um ponto de inspeção real, você pode selecioná-los para preencher automaticamente a maioria das informações.

4.12.6 Adicionando um Tipo de Objeto

Personalize o nome de um tipo de objeto, como *disjuntor.*

Procedimento:

» **Passo 1:** faça login no **Cliente Defense IA**. Na página inicial, clique em , e então na seção de *Configuração de aplicativo,* selecione *Inspeção Inteligente > Modelo de Objeto.*

» **Passo 2:** clique em .

» **Passo 3:** digite um nome para o tipo de objeto e, em seguida, clique em *OK.*

Operações Relacionadas

» **Alterar o nome de um tipo de objeto:** selecione um tipo de objeto e, em seguida, clique em para alterar seu nome.

» **Excluir um tipo de objeto:** selecione um tipo de objeto e, em seguida, clique em para excluí-lo.

4.12.7 Adicionando Ponto de Inspeção

Configure as informações do ponto de inspeção de um tipo de objeto. Por exemplo, a área no disjuntor a ser inspecionada, itens a serem inspecionados e tecnologias a serem usadas.

Procedimento:

» **Passo 1:** faça login no **Cliente Defense IA**. Na página inicial, clique em , e então na seção de *Configuração de Aplicativo,* selecione *Inspeção Inteligente > Modelo de Objeto.*

» **Passo 2:** clique em um tipo de objeto e, em seguida, clique em Adicionar.

Parâmetro	Descrição
Área de Inspeção	Clique na caixa de entrada para inserir um nome manualmente. Se houver pontos de inspeção que já foram adicionados, você pode selecionar uma área de inspeção na lista suspensa.
Tipo de Ponto	Insira um nome para o tipo de ponto.
Item de Inspeção	Insira os itens a serem inspecionados.
Tecnologia de Inspeção	Instantâneo Visível: A plataforma tirará apenas instantâneos. Monitoramento de Temperatura Térmica: Use tecnologia térmica para monitorar a temperatura. Você pode configurar o limite de alerta de temperatura e o limite de diferença de temperatura, mas eles são parâmetros opcionais.
Limite de Alerta de Temperatura	Configure os limites para baixo, médio e alto. Quando a temperatura for maior que qualquer um deles, um alarme será acionado.
Limite de Alerta de Diferença de Temperatura	Configure os limites para baixo, médio e alto. Quando a diferença de temperatura for maior que qualquer um deles, um alarme será acionado. A diferença é calculada por 2 pontos de inspeção. Ao configurar um ponto de inspeção real, você deve selecionar outro ponto para que a plataforma possa calcular a diferença.

» **Passo 3:** configure os parâmetros e, em seguida, clique em OK. Ou clique em Salvar e Continuar para adicionar mais pontos de inspeção.

4.12.8 Importando Tipos de Objetos e Pontos de Inspeção

Se precisar adicionar muitos tipos de objetos e pontos de inspeção, você pode importá-los para a plataforma.

Procedimento:

» **Passo 1:** faça login no **Cliente Defense IA**. Na página inicial, clique em , e então na seção de *Configuração de Aplicativos,* selecione Inspeção *Inteligente > Modelo de Objeto.*

» **Passo 2:** clique em .

» **Passo 3:** clique em *Baixar Modelo* e salve o modelo no seu computador.

» **Passo 4:** preencha as informações e salve as alterações. Clique em para baixar um modelo com tipos de objetos comuns e pontos de inspeção relacionados a subestações para referência.

» **Passo 5:** clique em *Importar Arquivo* e abra o modelo.

As informações são importadas para a plataforma. Se houver pontos de inspeção que já estejam na plataforma, suas informações serão atualizadas.

Configurando Objeto de Inspeção

Adicione objetos de inspeção para que a plataforma possa inspecionar um ou mais pontos. Os objetos de inspeção são geridos por organizações de inspeção. Apenas papéis e usuários específicos podem acessar determinadas organizações.

Adicionando Organização de Inspeção

Organizações de inspeção são usadas para gerenciar objetos e pontos de inspeção. Apenas admi- nistradores podem configurá-las e especificar quais papéis e seus usuários podem acessar deter- minadas organizações.

Procedimento:

» **Passo 1:** faça login no **Cliente Defense IA**. Na página inicial, clique em  , e então na seção de *Configuração de Aplicativos*, selecione *Inspeção Inteligente > Objeto de Inspeção.*

» **Passo 2:** clique em  .

» **Passo 3:** configure os parâmetros e, em seguida, clique em *OK*. Ou clique em *OK* e *Adicionar Objeto* para adicionar objetos a esta organização.

Parâmetro	Descrição
Organização Pai	Isso é para controle de permissão. Por exemplo, se um usuário não pode acessar A, então o usuário não poderá acessar todas as organizações sob A.
Nome da Organização	Insira um nome para a organização.
Papéis Permitidos para Acesso	Apenas os papéis selecionados e seus usuários podem acessar esta organização. Clique  para ver os usuários atribuídos aos papéis.

Adicionando Objeto de Inspeção

Procedimento:

» **Passo 1:** faça login no Cliente Defense IA. Na página inicial, clique em  , e então na seção de *Configuração de Aplicativos,* selecione *Inspeção Inteligente > Objeto de Inspeção.*

» **Passo 2:** selecione uma organização e, em seguida, clique em *Adicionar.*

Parâmetro	Descrição
Nome do Objeto de Inspeção	Insira um nome para o objeto de inspeção.
Organização	Exibe o nome da organização que você selecionou na etapa anterior. Você pode selecionar outra.
Tipo de Objeto a Ser Enviado	Selecione um tipo de objeto que foi adicionado. Isto é opcional.

» **Passo 3:** configure as informações básicas e clique em *Avançar.*

» **Passo 4:** clique em *Adicionar Ponto.* Se você selecionar um tipo de objeto da etapa anterior, todos os pontos de inspeção nesse tipo de objeto serão adicionados automaticamente.

» **Passo 5:** configure as informações do ponto e clique em *OK.*

Adicionando Objeto de Inspeção

Procedimento:

» **Passo 1:** faça login no **Cliente Defense IA**. Na página inicial, clique em , e então na seção de *Configuração de Aplicativos,* selecione *Inspeção Inteligente* > *Objeto de Inspeção.*

» **Passo 2:** selecione uma organização e, em seguida, clique em *Adicionar.*

» **Passo 3:** configure as informações básicas e clique em *Avançar.*

Parâmetro	Descrição
Nome do Ponto	Insira um nome para o ponto.
Área de Inspeção	Clique na caixa de entrada para inserir um nome manualmente. Se houver pontos de inspeção que já foram adicionados, você pode selecionar uma área de inspeção na lista suspensa.
Tipo de Ponto	Insira um nome para o tipo de ponto.
Item de Inspeção	Insira os itens a serem inspecionados.
Tecnologia de Inspeção	» Instantâneo Visível: A plataforma tirará apenas instantâneos. » Monitoramento de Temperatura Térmica: Use tecnologia térmica para monitorar a temperatura. Você pode configurar o limite de alerta de temperatura e o limite de diferença de temperatura, mas eles são parâmetros opcionais. » Limite de Alerta de Temperatura: Configure os limites para baixo, médio e alto. Quando a temperatura for maior que qualquer um deles, um alarme será acionado. » Limite de Alerta de Diferença de Temperatura: Configure os limites para baixo, médio e alto. Quando a diferença de temperatura for maior que qualquer um deles, um alarme será acionado. » A diferença é calculada por 2 pontos de inspeção. Ao configurar um ponto de inspeção real, você deve selecionar outro ponto para que a plataforma possa calcular a diferença.

» **Passo 6:** clique em *Vincular Câmera.*

» **Passo 7:** configure os parâmetros e, em seguida, clique em *OK* para vincular o ponto a um canal.

Parâmetro	Descrição
Selecionar Canal	Dê um duplo clique em um canal para ser vinculado. Seu vídeo ao vivo e informações serão exibidos à direita.
PTZ	Se você estiver vinculando a um canal PTZ, você pode operá-lo usando o painel de controle PTZ. Também, você deve vincular a um preset do canal PTZ. Clique em , e então clique em de um preset para vinculá-lo ao ponto.
Parâmetros de monitoramento de temperatura	» Após vincular a um canal térmico, você deve adicionar uma regra de monitoramento de temperatura no vídeo ao vivo. As regras incluem ponto, linha, retângulo e polígono. O dispositivo pegará a maior temperatura na área incluída pela regra que você definir. Por exemplo, se você adicionar um retângulo no vídeo ao vivo, o dispositivo pegará a maior temperatura nesse retângulo. » Limite de Alerta de Temperatura: Configure os limites para baixo, médio e alto. Quando a temperatura for maior que qualquer um deles, um alarme será acionado. » Limite de Alerta de Diferença de Temperatura: Configure os limites para baixo, médio e alto. Quando a diferença de temperatura for maior que qualquer um deles, um alarme será acionado. A diferença é calculada por 2 pontos de inspeção. Ao configurar um ponto de inspeção real, você deve selecionar outro ponto para que a plataforma possa calcular a diferença.

» **Passo 8:** clique em *Salvar e Sair.*

Configurando Plano de Inspeção

Durante os períodos definidos, a plataforma irá inspecionar os objetos e pontos que você selecionou e salvar os dados relacionados na plataforma.

Procedimento:

» **Passo 1:** faça login no **Cliente Defense IA**. Na página inicial, clique em , e então na seção de *Configuração de Aplicativos,* selecione *Inspeção Inteligente > Plano de Inspeção.*

» **Passo 2:** selecione uma organização de inspeção e clique em *Adicionar.*

» **Passo 3:** configure as informações básicas e clique em *Avançar.*

Parâmetro	Descrição
Nome do Plano	Insira um nome para o plano.
ID do Plano	Este é gerado automaticamente. Você pode editá-lo conforme necessário.
Organização de Inspeção	Exibe o nome da organização que você selecionou na etapa anterior. Você pode selecionar outra.
Tipo de Inspeção	Selecione um tipo para o plano. É usado para buscar determinados planos de inspeção.
Tempo de Processamento	O tempo de processamento funciona das seguintes 2 maneiras: » Para referência dos revisores quando revisam os resultados da inspeção. » Quando restam 5 minutos e o plano de inspeção ainda está sem processamento, todos os usuários que têm permissão para acessar a organização à qual este plano pertence são notificados.
Ativar	Após ativado, este plano é eficaz após adicionado.

» **Passo 4:** configure os objetos e pontos de inspeção.

1. Clique em *Adicionar.* Somente a organização que você selecionou, suas sub-organizações e seus objetos e pontos serão exibidos.
2. Selecione um ou mais objetos e clique em *OK.*
3. Clique nas setas para cima e para baixo para ajustar a ordem dos objetos e pontos.
4. Clique em *Avançar.*

» **Passo 5:** configure o horário de execução e clique em *OK.*

Parâmetro	Descrição
Modo de Execução	» Por Período: O plano é executado automaticamente dentro dos períodos especificados.
Estratégia de Execução	» Uma Vez Por Dia: O plano será executado no horário definido todos os dias. » Você pode usar para configurar vários dias ao mesmo tempo. » Repetição: Configure o intervalo de repetição e, em seguida, o plano será executado dentro dos períodos eficazes a cada intervalo que você configurar. Para saber como criar um modelo de tempo, veja *Adicionando Modelo de Tempo.* » Apenas Uma Vez: O plano será executado apenas uma vez após adicionado ou no horário definido.
Modo de Luz	Selecione se deseja acender a luz nos dispositivos durante a inspeção. Como pode levar tempo para os dispositivos acenderem a luz, você pode configurar um período de aquecimento para garantir que a luz possa ser normalmente acesa antes do início da inspeção.

Configurando Evento de Monitoramento de Temperatura

Se você configurou limiares de alerta em inspeções, pode configurar eventos para realizar ações de vinculação quando os limites forem alcançados. Por exemplo, se um ponto de inspeção monitorar uma temperatura maior que o limite, uma câmera gravará um vídeo da área que está monitorando. Para detalhes, veja *4.1 Configurando Eventos.*

4.13. Manutenção

Configure regras de alerta para monitorar servidores e dispositivos, para que você possa lidar com eles em tempo hábil e garantir que o sistema esteja funcionando corretamente. Você também pode configurar a detecção de armazenamento de vídeo. Você será avisado se a duração ou integridade da gravação estiver anormal.

4.13.1 Configurando Regra de Alerta

Configure regras de alerta para monitorar servidores e dispositivos, para que você possa lidar com eles em tempo hábil.

Procedimento:

» **Passo 1:** faça login no **Cliente Defense IA**. Na página inicial, clique em , e então na seção de *Configuração de Aplicativos,* selecione *Centro de Manutenção > Configuração de Regra de Alerta.*

» **Passo 2:** clique em *Adicionar Regra.*

» **Passo 3:** configure os parâmetros e clique em *OK.*

Parâmetro	Descrição
Nome da Regra	Insira um nome para a regra. Pode ter até 50 caracteres.
Nível de Alerta	Selecione um nível para o alerta. Isso é usado para saber rapidamente a urgência do alerta quando ele é acionado.
Tempo de Execução da Regra	O alerta será acionado apenas dentro do período definido.
Alvos de Monitoramento	Os alvos incluem servidores e dispositivos. Você pode selecionar diferentes fontes de alerta para cada um deles.
Condições da Regra	Defina o limite para cada condição. Quando o valor for maior ou igual ao limite, o alerta será acionado.
Notificação Push	Após ativado, você pode selecionar os usuários que receberão notificações quando o alerta for acionado.
Notificação por Email	Após ativado, você pode personalizar o conteúdo a ser enviado para endereços de email especificados. Você pode configurar os endereços de email das seguintes maneiras: Clique para selecionar os endereços de email dos usuários. Insira manualmente um endereço de email e pressione a tecla *Enter.*

4.13.2 Configurando Detecção de Armazenamento de Vídeo

A plataforma continuará a verificar a duração e a integridade dos vídeos. Você será avisado se algum deles estiver anormal. Por exemplo, 30 dias de duração e integridade do vídeo foram configurados para o canal A. Se houver apenas 24 dias de vídeo, ou se o vídeo não durar 24 horas em algum dia, a plataforma fornecerá avisos correspondentes.

Pré-requisitos:

Planos de gravação foram configurados para canais e vídeos foram gravados.

Procedimento:

» **Passo 1:** faça login no **Cliente Defense IA**. Na página inicial, clique em , e então na seção de *Configuração de Aplicativos,* selecione *Centro de Manutenção > Configuração de Integridade do Vídeo.*

» **Passo 2:** clique em *Adicionar.*

» **Passo 3:** configure os dias de armazenamento consecutivos e, em seguida, selecione os canais para detecção.

» **Passo 4:** clique em *OK.*

Operações Relacionadas

Você pode visualizar os resultados da detecção ao visualizar as informações detalhadas de um dispositivo no *Centro de Manutenção.* Se a duração do vídeo não for suficiente, o número de dias será exibido em vermelho. Se a duração do vídeo para um dia for inferior a 24 horas, o status de integridade será anormal e exibido em vermelho.

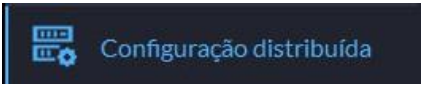
5. Configurações do sistema

As configurações do sistema desempenham um papel essencial na personalização e gerenciamento do ambiente. Esses módulos são responsáveis por administrar diversos elementos que permitem uma customização precisa. Entre suas funcionalidades, incluem-se a configuração de servidores auxiliares, o gerenciamento de informações de licença, a definição de parâmetros do sistema, a disponibilização de opções de backup e a integração da plataforma por meio do módulo de síntese com ambientes externos.

5.1. Implantação

A página de implantação apresenta duas opções para arquitetura do software e disposição dos dispositivos no sistema: Configuração distribuída e Configuração em cascata, ambas são apresentadas a seguir.

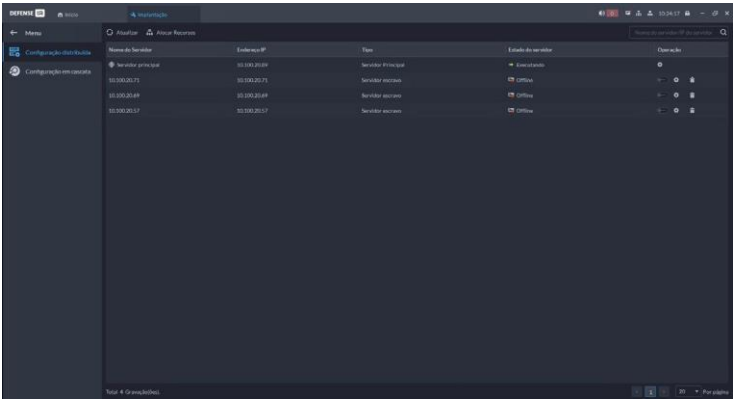
5.2. Configuração distribuída



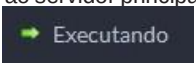
Nesta página, você pode configurar servidores auxiliares e administrar recursos (alocar dispositivos por servidores) a fim de aumentar e balancear o consumo de recursos computacionais do sistema.

Um servidor auxiliar escravo funciona como uma extensão de serviços do Defense IA, cedendo pro- cessamento computacional para aumentar a capacidade do sistema. Veja o Datasheet para mais informações sobre a capacidade do sistema.

Caso servidores auxiliares tenham sido instalados (Instalação de servidor auxiliar), estes aparecerão na lista, sendo possível configurá-los de acordo com o projeto.



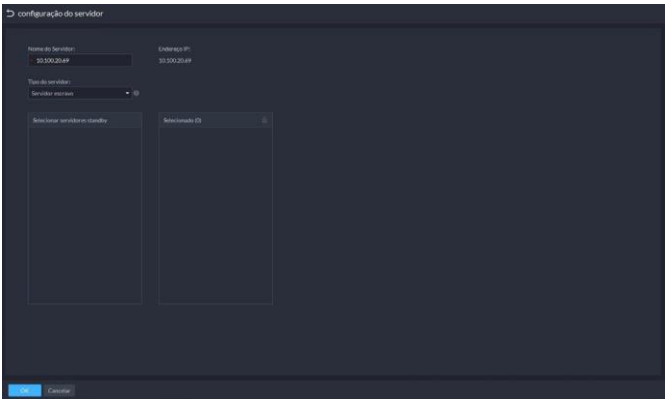
Nesta página a configuração do Servidor principal limita-se a alteração de seu nome. Ative os servidores auxiliares clicando no botão *Ativar*  .

Ao ativar os servidores, aguarde alguns segundos até estes conectarem-se ao servidor principal e clique em *Atualizar* para visualizar o estado do servidor como *Executando* 

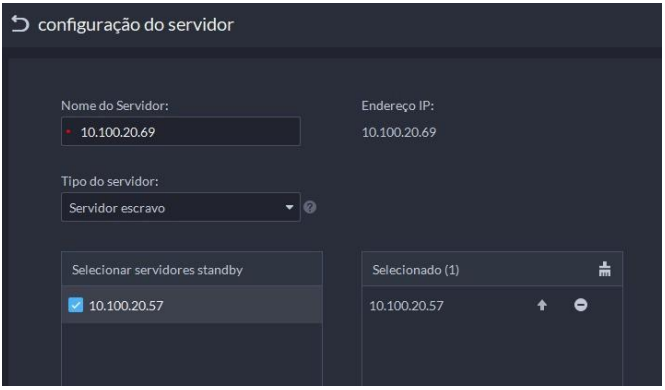
Os servidores auxiliares (ou slave servers) suportam dois modos de configuração. Para configurá-los, clique na engrenagem  .

Servidor auxiliar escravo

Modo padrão. Ao ativá-lo, o servidor auxiliar já está configurado neste modo. Servidor auxiliar em modo escravo dispõe de seus recursos para o servidor principal, de tal forma, não é possível aces- sá-lo diretamente pelo Cliente já que ele funciona como uma extensão do servidor principal.

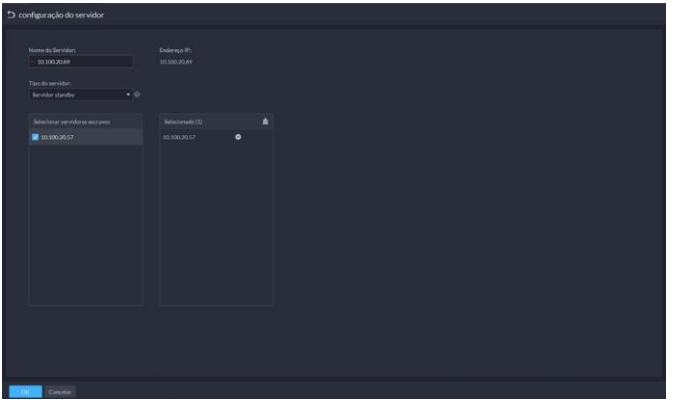


Caso haja um servidor auxiliar standby configurado, este aparecerá disponível para vinculação:



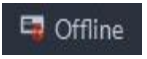
Servidor auxiliar standby

Um servidor auxiliar standby funciona como uma redundância ao servidor auxiliar escravo, assumindo como ativo em casos de indisponibilidade do servidor assistido. Utilizado em cenários de Implantação de estrutura M+N.



Para utilizar um servidor auxiliar standby, deve-se vinculá-lo a um servidor auxiliar escravo para realizar a redundância de disponibilidade.

Ao configurar os servidores auxiliares, é possível verificá-los na tabela.

» 

: servidor desconectado, não funcional.

» 

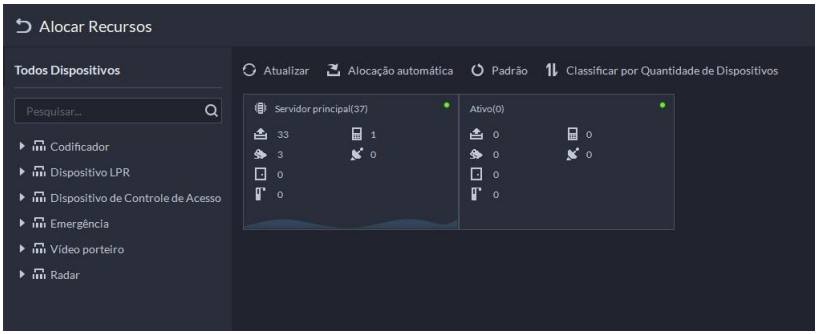
: servidor conectado e funcional.

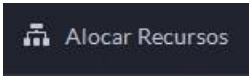
» 

: servidor auxiliar standby, em espera. Assumirá como servidor auxiliar escravo caso o servidor vinculado desconecte-se.

5.3. Alocar Recursos

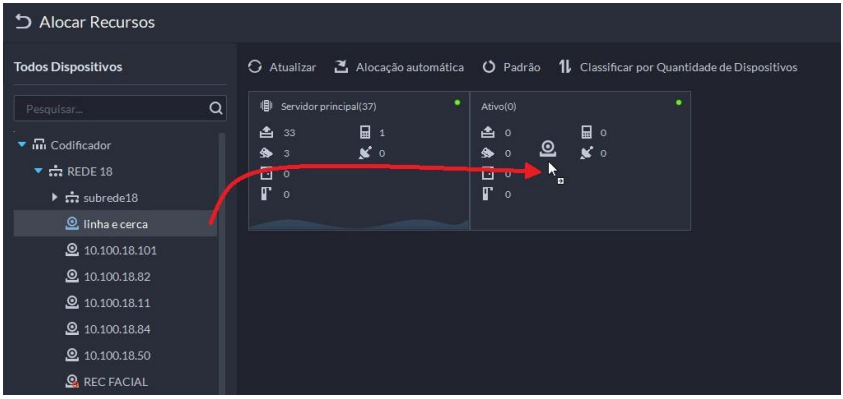
Para balancear carga do sistema, é possível alocar recursos do sistema entre os servidores (principal e auxiliares), vinculando cada dispositivo com um servidor que será responsável por seu gerenciamento.



Para isso clique em *Alocar Recursos*  na parte superior da tela. Existem duas opções para a alocação de recursos.

Alocação manual

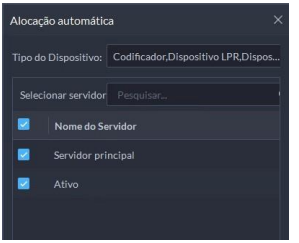
Aloca-se um dispositivo por vez, isso pode ser feito ao arrastar o dispositivo da árvore de dispositivos para o bloco do servidor



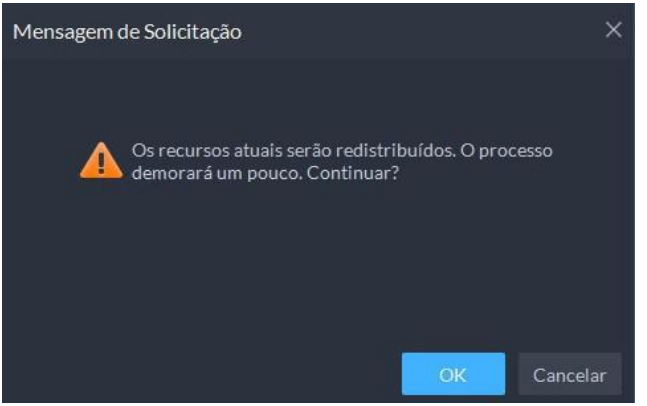
Alocação automática

Ao clicar no botão 

, uma janela com os servidores disponíveis será aberta. Selecione os servidores nos quais deseja realizar a alocação.



Clique em *OK* e em seguida, confirme a mensagem para continuar.

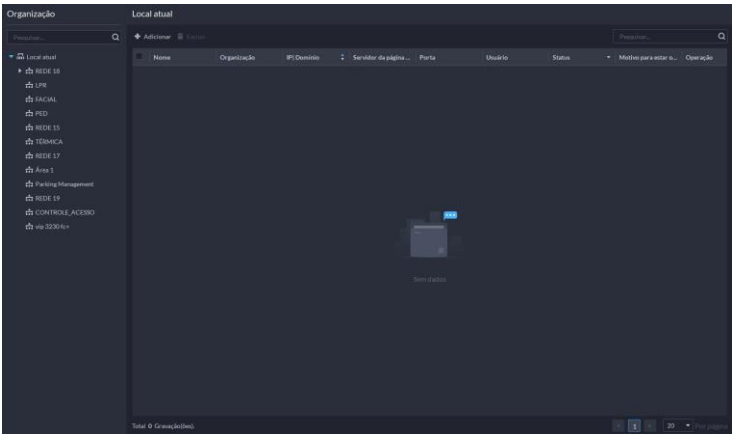


Ao confirmar a mensagem, a alocação automática iniciará, é possível acompanhar o processo pela barra de carregamento no canto superior da tela.

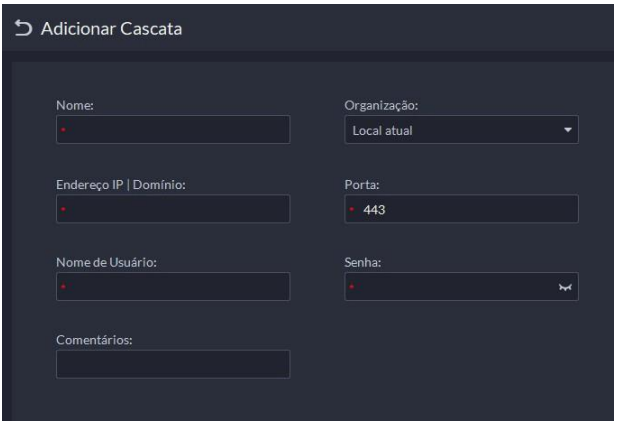
Ao finalizar, os dispositivos devem estar balanceados entre os servidores selecionados, desta forma, ambos os servidores atuam com uma carga de processamento computacional muito semelhante.

Configuração em cascata

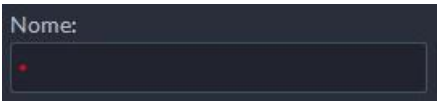
A plataforma Defense IA possui como característica expansiva a capacidade de estender dispositivos e gravações através da adição de um servidor adicional em forma de cascata. Ao incluir um servidor como um novo nível na cascata, é possível acessar todos os dispositivos e gravações por meio do servidor localizado no nível mais alto da cascata.



Para adicionar um servidor em cascata, clique em *Adicionar*  na guia superior da tela.

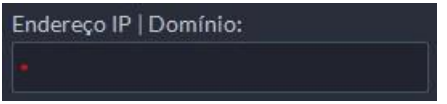


Preencha as informações necessárias do servidor que deseja adicionar.



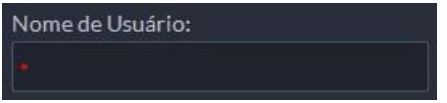
» **Nome:** nome que identificará a cascata.

» **Organização:** local no qual a cascata será alocada (os dispositivos estarão disponíveis no local selecionado).

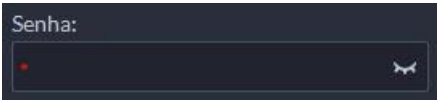


» **Endereço IP | Domínio:** endereço do servidor a ser adicionado.

» **Porta:** porta de conexão do servidor a ser adicionado.



» **Nome de Usuário:** nome de usuário para acessar a plataforma - e seus dispositivos - a serem adicionados.



» **Senha:** senha de usuário para acessar a plataforma - e seus dispositivos - a serem adicionados.

Ao adicionar a cascata, esta aparecerá na lista e seus dispositivos e gravações já podem ser acessados.

5.4. Licença

Para fazer ativação de funções do sistema e verificar recursos disponíveis para utilização na plataforma, acesse a página de licença.

Para utilizar funções da plataforma, estas devem ser habilitadas de acordo. Ao acessar a interface de gerenciamento da Licença, é possível visualizar a lista de recursos a serem habilitados. A tabela a seguir descreve cada recurso disponível.

Recurso	Descrição
Canal de Vídeo	Este recurso é compatível com dispositivos que enviam transmissão de vídeo à plataforma. Um canal de vídeo é um recurso que representa uma conexão entre a plataforma e a transmissão de vídeo do dispositivo. Para utilizar o recurso de vídeo enviado pelo dispositvo à plataforma, seja para visualização ao vivo, configuração de gravações, ou vinculação a eventos, utiliza-se o recurso de canais de vídeo. Ao adicionar, ou editar um dispositivo encoder ou decoder, é possível definir a quantidade de canais de vídeo que este consumirá. Por exemplo, ao adicionar à plataforma um gravador com 16 canais de vídeo, por padrão o Defense IA reconhecerá a quantidade e definirá 16 canais de vídeo a serem consumidos, este valor pode ser editado. Caso o gravador utilize apenas 12 dos 16 canais disponíveis, pode-se alterar a quantidade de canais de vídeo do dispositivo para 12. Ou seja, a quantidade de canais de vídeo não está relacionada diretamente à quantidade ou capacidade de dispositivos na pataforma, mas sim à quantidade de recursos de vídeo que estes dispositivos enviam.
Canal de Porta	Este recurso é compatível com dispositivos de controle de acesso. Um canal de porta é um recurso que representa uma conexão entre a plataforma e o relay de controle de acesso (abrir ou fechar). Ao adicionar dispositivos de controle de acesso, a platafomra adquire automaticamente informações sobre os canais de controle de acesso e define a quantidade de canais de porta a serem consumidos. A depender do modelo, um dipositivo controlador de acesso pode consumir recursos de canal de vídeo e canal de porta simultaneamente.
Canal de Controle do Elevador	Este recurso estará disponível em versões futuras.
Canal PDV	Este recurso é compatível com dispositivos do tipo NVR, DVR, iMHDX e iNVD que apresentam canais de PDV. Assim como um canal de vídeo, um canal PDV é um recurso que representa uma conexão entre a plataforma e a transmissão de dados de PDV do dispositivo.
Canal de Alarme EAS	Este recurso é compatível com dispositivos do tipo EAS (Emergency Alert System, ou Sistema de Alerta de Emergência). Este recurso estará disponível em versões futuras.
Dispositivo Vídeo Porteiro	Este recurso é compatível com dispositivos de vídeo portaria (PVIP e TVIP). Ao contrário dos recursos listados acima, a quantidade de licenças de dispositivos vídeo porteiro relaciona-se diretamente com a quantidade de dispositivos do tipo adicionados à plataforma. Para cada dispositivo a ser adicionado, uma licença deve ser adquirida.
Detector de Metais do Tipo Portal	Este recurso é compatível com dispositivos do tipo detector de metais. Este recurso estará disponível em versões futuras. Ao contrário de recursos listados acima, a quantidade de licenças de detectores de metais relaciona-se diretamente com a quantidade de dispositivos do tipo adicionados à plataforma. Para cada dispositivo a ser adicionado, uma licença deve ser adquirida.

Máquina de Triagem de Segurança	Este recurso é compatível com dispositivos de triagem de segurança. Este recurso estará disponível em versões futuras. Ao contrário de recursos listados acima, a quantidade de licenças de máquinas de triagem de segurança relaciona-se diretamente com a quantidade de dispositivos do tipo adicionados à plataforma. Para cada dispositivo a ser adicionado, uma licença deve ser adquirida.
Radar	Este recurso é compatível com dispositivos do tipo radar. Ao contrário de recursos listados acima, a quantidade de licenças de radares relaciona-se diretamente com a quantidade de dispositivos do tipo adicionados à plataforma. Para cada dispositivo a ser adicionado, uma licença deve ser adquirida.
Espaço da Vaga	Este recurso é compatível com dispositivos do tipo detector de vagas de estacionamento. A quantidade de licenças de espaços de vaga relaciona-se diretamente com a quantidade de vagas de estacionamento registradas ao dispositivos do tipo adicionado à plataforma. Para cada vaga a ser detectada, uma licença deve ser adquirida.
Dispositivos LED	Este recurso é compatível com dispositivos do tipo display de LED. Ao contrário de recursos listados acima, a quantidade de licenças de dispositivos LED relaciona-se diretamente com a quantidade de dispositivos do tipo adicionados à plataforma. Para cada dispositivo a ser adicionado, uma licença deve ser adquirida.
UVSS	Este recurso estará disponível em versões futuras.
Alto-falante IP	Este habilita a adição de um dispositivo corneta IP da linha SPK na plataforma.
Regras de Localização de Veículos	Este recurso é compatível com o módulo de estacionamento. Estará disponível em versões futuras.
Cascata	Este recurso habilita a adição de um outro servidor principal do Defense IA como cascata, permitindo acesso a seus dispositivos. A quantidade de licenças de cascata relaciona-se diretamente com a quantidade de servidores adicionados à plataforma. Para cada servidor a ser adicionado, uma licença deve ser adquirida.
Integração de Eventos	Este recurso habilita integração de eventos à plataforma pelo módulo síntese. Cada recurso permite a adição de 5 centrais.
Gerenciamento do estacionamento	Este recurso é único. Ao ativar, habilita a utilização do módulo de estacionamento na plataforma.
Vários Locais	Este recurso é único. Ao ativar, habilita a utilização da função Multi-site na plataforma.
Banco de Dados Independente	Este recurso é único. Ao ativar, habilita a conexão e utilização de banco dados externos na plataforma.
Chamada em Grupo	Este recurso é único. Ao ativar, habilita a utilização de chamadas em grupo com dispositivos BCM na plataforma.
Inspeção Inteligente	Este recurso é único. Ao ativar, habilita a utilização do plugin Inspeção Inteligente na plataforma.
Varejo	Este recurso é único. Ao ativar, habilita a utilização do plugin Varejo na plataforma.
InSearch	Este recurso é único. Ao ativar, habilita a utilização do plugin InSearch na plataforma.

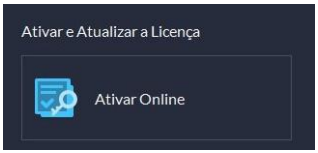
Veja o Datasheet do produto para consultar a capacidade do sistema.

Para utilizar plugins, é necessários instalá-los no servidor da plataforma.

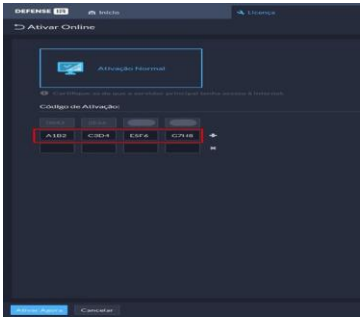
Contate seu consultor comercial para adquirir um código de licença com as capacidades desejadas, as licenças são únicas e incrementais, é possível expandir o sistema adicionando diversos códigos. Sua ativação pode ser feita de duas formas, de maneira Online ou Offline.

5.4.1 Ativação Online

Para realizar a ativação do código online, certifique-se que o servidor possua conexão com a internet. Clique em *Ativar Online* no lado esquerdo da página.



Insira o código de ativação no campo vazio, caso possua mais de um código de ativação, clique no ícone  para habilitar mais um campo.



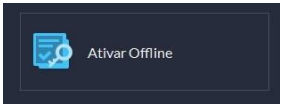
Clique em *Ativar Agora* para habilitar o(s) código(s) inserido(s). O client reiniciará.

O código de licença ativado fica vinculado à máquina em questão, o código é instransferível. Caso utilize algum firewall ou anti-vírus, atente-se

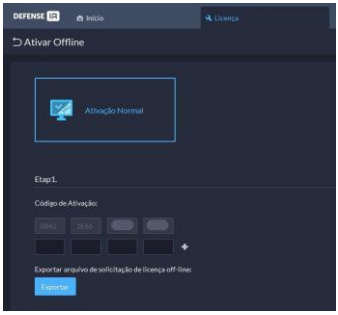
a bloqueios à aplicação. Caso utilize ambiente virtualizado, atente-se com regras de mudança de endereços de hardware, isso pode ocasionar perda da licença ativada.

5.4.2 Ativação Offline

Para realizar a ativação do código offline, clique em *Ativar Offline* no lado esquerdo da página.



Insira o código de ativação no campo vazio, caso possua mais de um código de ativação, clique no ícone  para habilitar mais um campo.



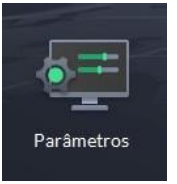
Clique em *Exportar* para exportar um arquivo .zip contendo as informações a serem habilitadas. Envie este arquivo a seu representante de vendas para ativá-lo.

Após ativado, importe o arquivo recebido clicando no ícone  e então, clique em *Ativar.*

Após o processo a licença deve ser ativada. O client reiniciará.

O código de licença ativado fica vinculado à máquina em questão, o código é instransferível. Caso utilize algum firewall ou anti-vírus, atente-se a bloqueios à aplicação. Caso utilize ambiente virtualizado, atente-se com regras de mudança de endereços de hardware, isso pode ocasionar perda da licença ativada.

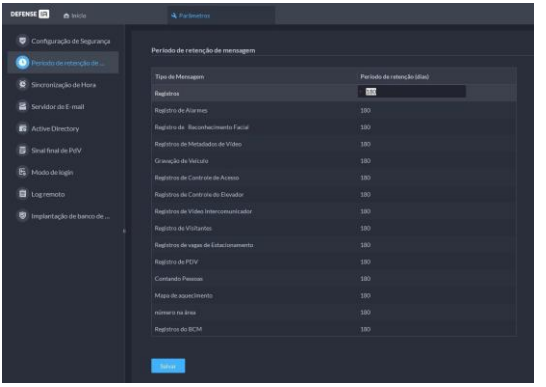
5.4.3 Parâmetros



Em parâmetros, é onde são realizadas as configurações do sistema como configurações de segurança, servidor de E-mail, Servidor AD, Sinal final de PdV, entre outras.

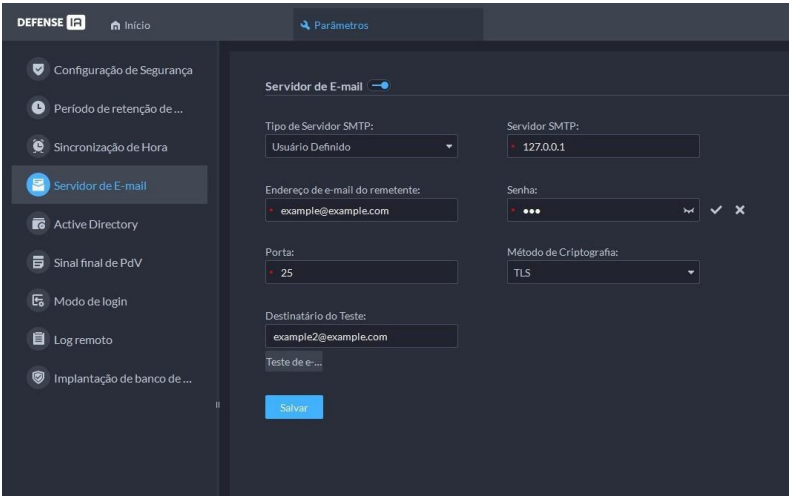
Período de retenção de mensagem

Em período de retenção de mensagem, é possível selecionar em dias o período para o servidor armazenar logs e informações do sistema.



5.4.4 Servidor de E-mail

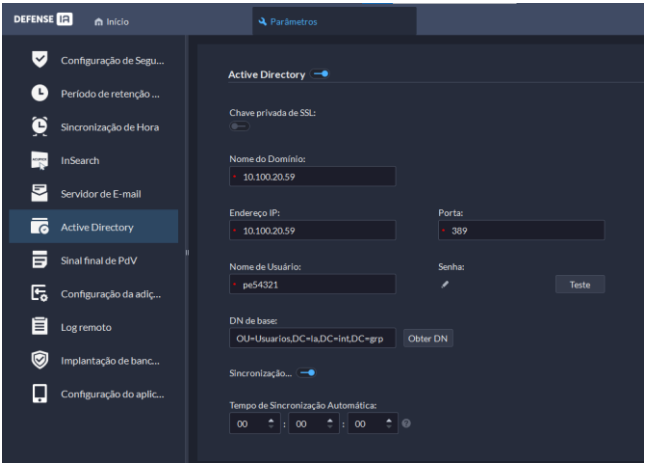
Em servidor de e-mail, é possível cadastrar um servidor SMTP como servidor de e-mail para a plata- forma, desta forma, é possível enviar e-mails para diferentes destinatários. Já existem três templa- tes de opções de servidores SMTP, como Gmail, Yahoo e Hotmail. Também é possível registrar um outro servidor selecionando a opção *Usuário definido* em *Tipo de Servidor SMTP.*



Preencha o Destinatário do teste, e clique em *Teste de e-mail* para enviar um e-mail teste e verificar seu funcionamento correto.

5.4.5 Active Directory

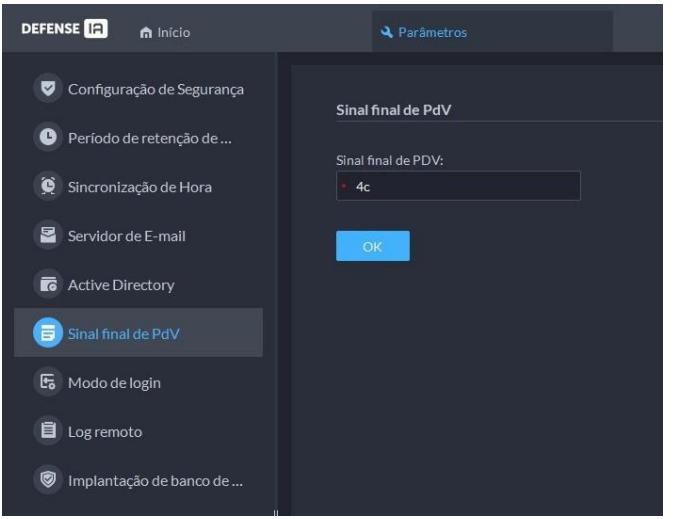
Em Active Directory, é possivel cadastrar um domínio para importar usuários, é possivel importar usuarios com base no domínio do servidor, podendo inserir uma Chave privada de SSL e Sincroni- zação automática.



Preencha o endereço de ip o nome do domínio, Nome de usuário e a Porta e clique em testar, o Defense deverá aparecer um menssagem afirmando o sucesso

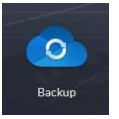
5.4.6 Sinal final de PdV

Em sinal final de PdV, preencha o sinal de PdV compatível com os pontos de venda resgistrados na plataforma.

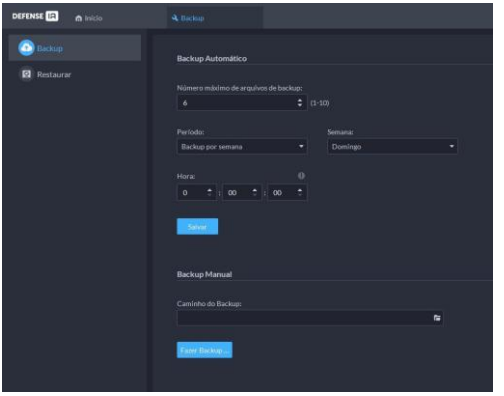


5.4.7 Backup

O backup é uma ferramenta crucial do sistema, pois permite exportar o banco de dados de forma segura e, posteriormente, restaurá-lo com facilidade. Você pode acessar a página de backup nas configurações do sistema, localizadas em *Backup.*



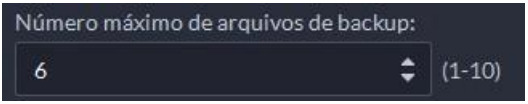
Baixar Backup



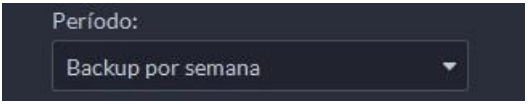
Há duas opções para realizar o backup do banco de dados na plataforma, que serão listadas abaixo:

***Backup* Automático:**

Em Backup automático é possível definir parâmetros de configuração para uma recorrência periódica do backup. Dentre essas configuram-se:

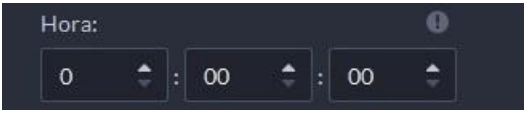


» **Número máximo de arquivos de backup:** define a quantidade entre 1 e 10 de arquivos de backup armazenados.



» **Período:** define a frequência do backup (nunca, diariamente, semanalmente, mensalmente).

» **Semana:** define o dia da semana que o backup deve ser realizado.



» **Hora:** define o horário que o backup deve ser realizado.

O caminho padrão para armazenamento de arquivos backup é localizado em "...".

Ao realizar o backup, a senha do usuário deve ser confirmada, assim como a inserção de uma se- nha de criptografia para uma camada de segurança do arquivo de backup.

***Backup* Manual:**

Em Backup manual configura-se o caminho para armazenar o arquivo clicando em  . Realize o backup clicando o botão *Fazer Backup Agora.*

Restaurar Backup

Caso deseje restaurar um arquivo de backup compatível, acesse *Restaurar.*

Nesta página você pode encontrar a lista de arquivos de backup, caso o backup automático esteja configurado. É possível restaurar o sistema a partir de um deles clicando em  ou baixar o arquivo de backup clicando em  .

Também é possível recuperar um arquivo de backup armazenado localmente selecionando o caminho do arquivo desejado clicando em  .

Os arquivos de backup possuem extensão .dbk

Para restaurar um arquivo de backup deve-se confirmar a senha de usuário e inserir a senha de criptografia definida ao gerar o arquivo.

A restauração de um arquivo de backup interromperá os serviços do servidor, e os reiniciarão. Todos os dados serão substituídos pelos presentes no arquivo de backup. O processo é irreversível.

A chave de licença é um dado vinculado à máquina, não sendo afetada pela restauração do backup. Caso a licença atual não suporte o arquivo restaurado, está deverá ser atualizada para funciona- mento pleno do sistema.

5.5. Síntese

Use uma Bridge para importar eventos para a plataforma a partir de sistemas de terceiros e, em seguida, use esses eventos para criar esquemas de alarmes e executar determinadas ações de ligação. Você também pode compartilhar o controle de acesso com bancos de dados de terceiros, que podem ser usados por pessoal de terceiros para formular seus próprios relatórios. Além disso, informações de dispositivos e pessoas podem ser sincronizadas com a plataforma para serem usadas em várias funções.

5.5.1 Sincronizando Eventos

Informações de Fundo

Uma Bridge serve como um conector entre a plataforma e sistemas de terceiros, e é responsável por importar eventos de um sistema de terceiros para a plataforma. Ela deve cumprir o protocolo de conexão entre o sistema de terceiros e a plataforma. Para diferentes sistemas, o protocolo pode variar e pode ser necessário desenvolver uma nova Bridge. Antes de usar essa função, certifique-se de que a Bridge tenha sido implantada e esteja funcionando.

Procedimento:

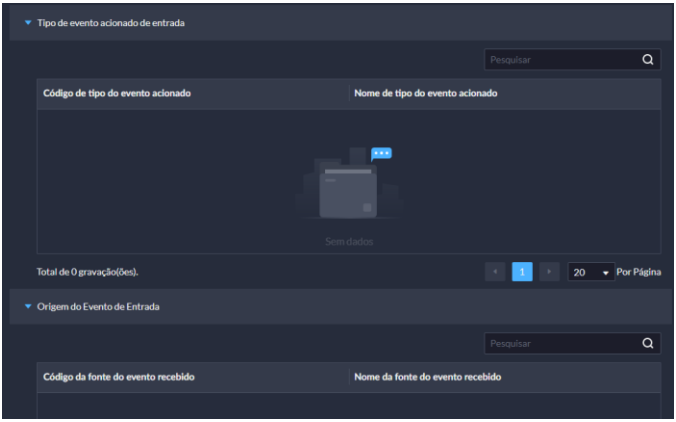
» **Passo 1:** faça login no Cliente Defense IA. Na página inicial, clique em *Configuração do Sistema* e selecione *Síntese* > *Sincronização de Eventos.*

» **Passo 2:** clique em *Adicionar.* Você pode adicionar até 5 Bridges para sincronizar eventos.

» **Passo 3:** configure os parâmetros e clique em *OK.*

Parâmetro	Descrição
Nome do Projeto	Insira um nome para este projeto.
Certificado de Identidade	Gerado automaticamente. Copie-os para a configuração da Bridge. Clique para verificar sua senha e, em seguida, gerar uma nova chave secreta. Clique para verificar sua senha e, em seguida, clique para copiar a chave secreta.
Chave Secreta	Personalize o conteúdo. Quando um evento é acionado e enviado para a plataforma, essa informação será exibida nos detalhes do evento.
IP/Domínio da Bridge Porta da Bridge	Insira o endereço IP ou nome de domínio e número da porta da Bridge.

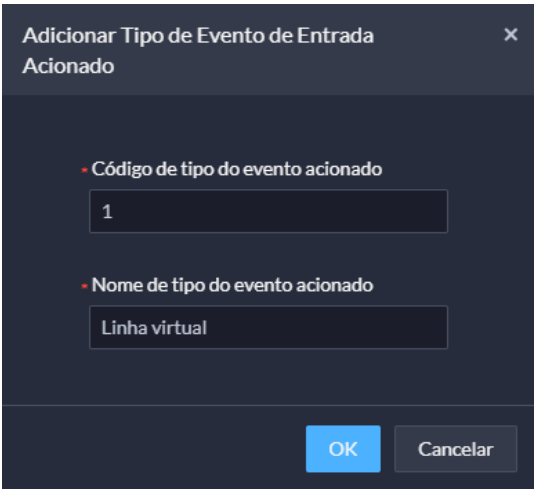
» **Passo 4:** clique em *Editar* na Bridge para configurar os eventos de gatilho de entrada e as fontes de eventos.



» **Passo 5:** Sincronize eventos de gatilho de entrada.

» **Um por um**

1. Clique em *Adicionar.*
2. Insira o código e o nome do evento de gatilho de entrada.
3. Clique em *OK.*



» **Em lote**

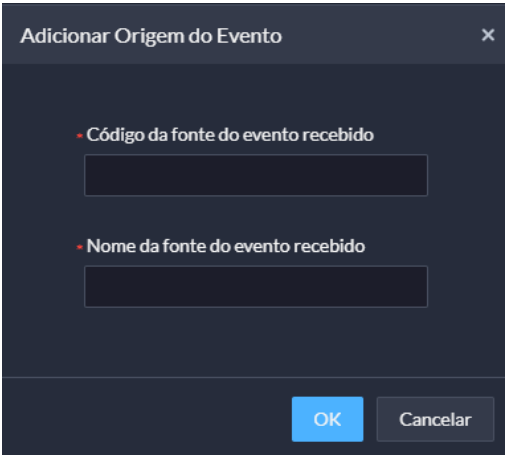
1. Clique em *Importar.*

2. Clique em *Baixar Modelo,* salve o modelo no seu PC e, em seguida, insira as informações nele.
3. Clique em *Importar Arquivo,* selecione o arquivo e clique em *Abrir.*

» **Passo 6:** sincronize fontes de eventos de entrada.

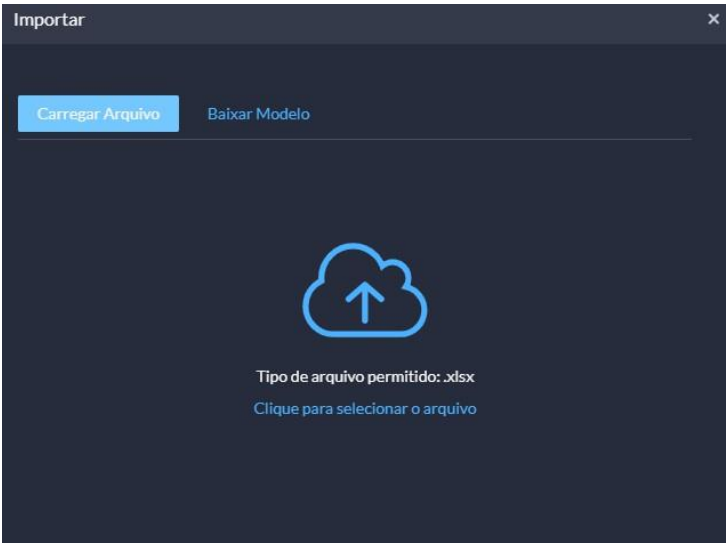
» **Um por um**

1. Clique em *Adicionar.*
2. Insira o número e o nome da fonte de evento de entrada.
3. Clique em *OK.*



» **Em lote**

1. Clique em *Importar.*



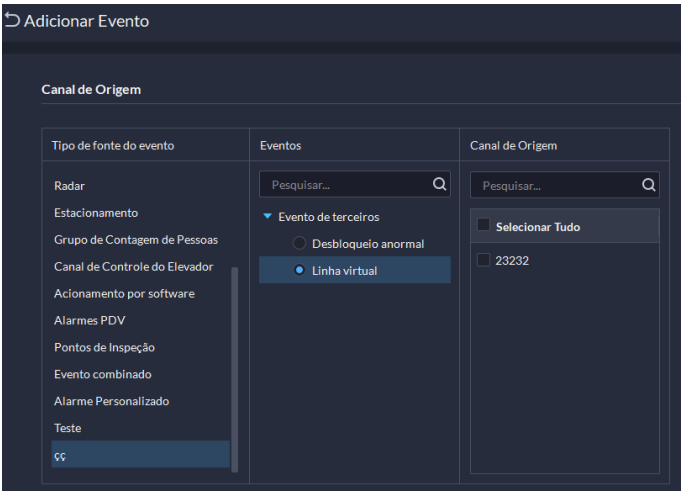
2. Clique em *Baixar Modelo,* salve o modelo no seu PC e, em seguida, insira as informações nele.
3. Clique em *Importar Arquivo,* selecione o arquivo e clique em *Abrir.*

» **Passo 7:** clique em *Fechar* no canto inferior esquerdo.

Operações Relacionadas

Configurar um esquema de eventos.

4. Vá para a página inicial, clique em *Configuração de Aplicações,* e selecione *Evento.*
5. Clique em *Adicionar.*
6. Na seção *Fonte de Evento,* selecione a que você importou do sistema de terceiros.



Sincronizando Dados

Você pode sincronizar manual ou regularmente dados na plataforma para bancos de dados de terceiros.

Procedimento:

» **Passo 1:** faça login no **C**liente Defense IA. Na página inicial, clique em *Configuração do Sistema* e selecione *Síntese* > *Sincronização de Dados.*

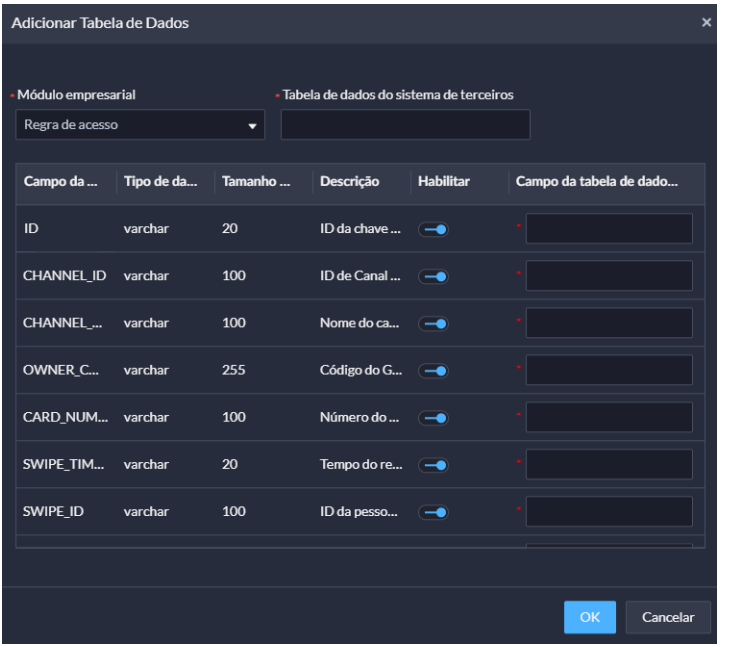
» **Passo 2:** clique em *Adicionar.* Você só pode adicionar um banco de dados.

» **Passo 3:** configure os parâmetros básicos do banco de dados e clique em **Testar**. Se a conexão puder ser estabelecida, o sistema informará que está conectado ao banco de dados com sucesso.

» **Passo 4:** clique e em *Configurar Sincronização Automática* e, em seguida, con- figure quando a plataforma sincronizará automaticamente os dados todos os dias. Você só pode configurar entre 4:00 e 23:00.

» **Passo 5:** configure os dados a serem sincronizados.

1. Clique em *Adicionar* na seção de *Dados de Sincronização.*



2. Defina o Módulo de Negócio como Controle de Acesso e insira o nome da tabela de dados no sistema de terceiros. Você só pode adicionar o módulo de controle de acesso uma vez.
3. Ative o tipo de dados a serem sincronizados. Você deve desativar os dados que não deseja sincronizar.
4. Insira os nomes correspondentes na tabela no sistema de terceiros para os dados a serem sincronizados.
5. Clique em *OK.*

Operações Relacionadas

Estas operações permitem a gestão eficiente da sincronização de dados e integração de sistemas na plataforma **Defense IA**:

» **Editar:** altere as informações do banco de dados ou dos dados que estão sendo sincronizados. Você pode visualizar cada resultado de sincronização no log do sistema. Para mais detalhes, consulte *8.1.3 Log do Sistema.*

» **Sincronização Manual Agora:** sincronize os dados imediatamente. Na primeira tentativa, todos os dados serão sincronizados, incluindo após você excluir e adicionar o banco de dados novamente. Somente novos dados serão atualizados em sincronizações subsequentes.

Integração de Sistema

A integração de sistemas permite a sincronização de informações de dispositivos, pessoas e veículos de uma plataforma de terceiros para a plataforma **Defense IA**, para serem utilizados em diversas funções, tais como:

» **Gerenciamento de Dispositivos:** visualize os parâmetros dos dispositivos.

» **Informações de Pessoas e Veículos:** visualize informações de organizações, pessoas e veículos.

» **Eventos:** Configure esquemas de eventos e receba e processe alarmes.

» **Centro de Monitoramento:** visualize vídeos em tempo real vinculados, vídeos gravados, informa- ções de mapas e muito mais.

» **Gerenciamento de Zonas:** pontos de acesso serão criados para cada canal de controle de acesso.

» **Controle de Acesso:** visualize vídeos em tempo real vinculados, e abra e feche portas.

» **Registros de Controle de Acesso:** exiba registros em tempo real e históricos, extraia registros de acesso de dispositivos e visualize estatísticas de entrada e saída de pessoas.

Procedimento de Integração de Sistema

Aqui está o procedimento detalhado para integrar um sistema de terceiros à plataforma Defense IA:

» **Passo 1:** faça login no Cliente Defense IA. Na página inicial, clique no ícone correspondente e, em seguida, na seção *Configuração do Sistema,* selecione *Síntese > Integração de Sistema.*

» **Passo 2:** clique em *Adicionar.* Você pode adicionar até 5 pontes para integração de sistemas.

» **Passo 3:** configure os parâmetros necessários e clique em *OK.*

Parâmetro	Descrição
Nome do Projeto	Insira um nome para este projeto. Este nome será usado em diferentes recursos, como nome de organização e tipo de fonte de evento.
Tipo de Plataforma Integrada	Selecione o tipo de plataforma de terceiros. Atualmente, apenas a plataforma de controle de acesso é suportada.
Certificado de Identidade	Gerado automaticamente. Copie-os para a configuração da ponte. A ponte usará essas informações para verificar sua identidade na plataforma Defense IA.
Chave Secreta	Clique para verificar sua senha e, em seguida, gerar uma nova chave secreta Clique para verificar sua senha e, em seguida, você pode clicar para copiar a chave secreta.
Observações	Personalize o conteúdo. Quando um evento é acionado e enviado para a plataforma, essas informações serão exibidas nos detalhes do evento.
Endereço IP/ Nome de Domínio do Bridge	Insira o endereço IP ou nome de domínio e o número da porta da ponte.
Porta do Bridge	
Certificado de Identidade	Insira o certificado de identidade e a chave secreta da ponte. A plataforma Defense IA usará essas informações para verificar sua identidade na ponte.
Chave Secreta	
Frequência de Coleta	Configure a frequência e o horário para a plataforma Defense IA adquirir automaticamente dados da plataforma de terceiros.
Tempo de Coleta	

» **Passo 4:** importe eventos da plataforma de terceiros para a plataforma Defense IA.

» **Um por um:**

1. Clique em *Adicionar.*
2. Configure os parâmetros e clique em *OK.*
   - » **Código do Tipo de Evento:** insira o código do evento na plataforma de terceiros.
   - » **Nome do Tipo de Evento:** insira o nome do evento na plataforma de terceiros.
   - » **Tipo de Fonte do Evento:** selecione o tipo de fonte que irá acionar o evento.
   - » **Tipo de Evento:** quando o tipo de fonte de evento é canal, você precisa configurar o tipo de evento. Eles correspondem aos tipos de eventos de controle de acesso da plataforma Defense IA, incluindo normal, anormal e alarme.

» **Em lotes:**

1. Clique em *Importar.*

2. Clique em *Baixar Modelo,* salve o modelo no seu PC e, em seguida, insira as informações nele.
3. Clique em *Importar Arquivo,* selecione o arquivo e depois clique em *Abrir.*

6. Gerenciamento

6.1. Gerenciamento de logs

Visualização e exportação de logs de operador, logs de dispositivo e logs do sistema, e habilitação do modo de depuração do log de serviço para solução de problemas.

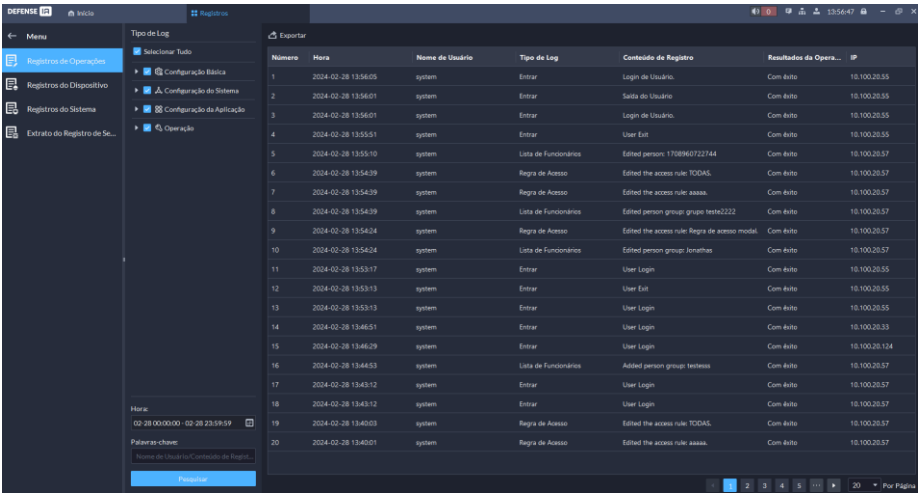
6.1.1 Log de Operações

Visualize e exporte logs que registram as operações dos usuários, como visualização de vídeo em tempo real de um canal.

Procedimento:

» Faça login no Cliente Defense.
» Na página inicial, selecione Gerenciamento > Logs > Logs de Operação.
» Selecione um ou mais tipos de logs.
» Especifique o tempo e palavras-chave e clique em Buscar.
» É possível pesquisar até 1 mês de logs por vez.
» Para exportar os logs, clique em Exportar e siga as instruções na tela.
» Ao buscar os logs serão listados com as seguintes características: data, hora, nome do usuário, conteúdo do registro, resultados da operação, ip e porta.

Na imagem abaixo está o exemplo de uma busca realizada:



6.1.2 Log de Dispositivo

Visualize e exporte logs gerados por dispositivos.

Procedimento:

» Faça login no Cliente Defense.

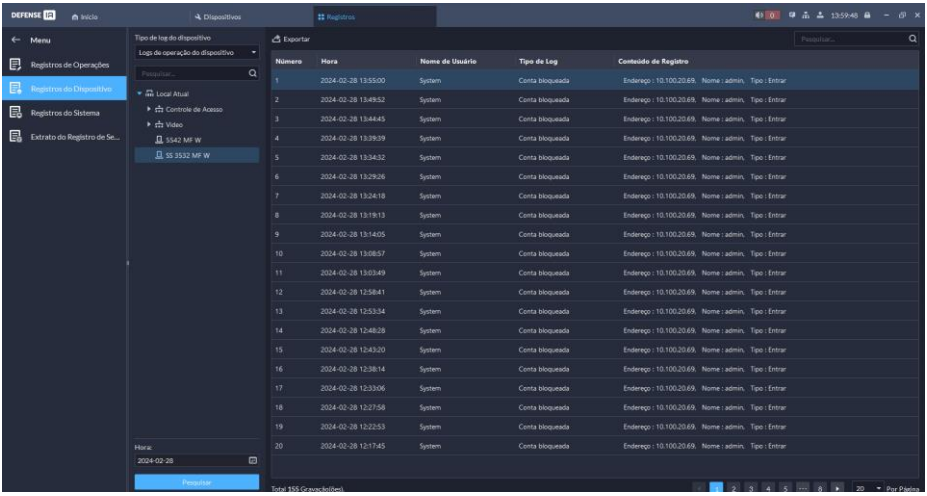
» Na página inicial, selecione *Gerenciamento* > *Logs* > *Logs de Dispositivo.*

» Selecione um dispositivo e tempo e clique em *Buscar.*

» Para exportar os logs, clique em Exportar e siga as instruções na tela.

» Ao buscar os logs serão listados com as seguintes características: data, hora, nome do usuário, tipo de log e conteúdo do registro.

Na imagem abaixo está o exemplo de uma busca realizada:



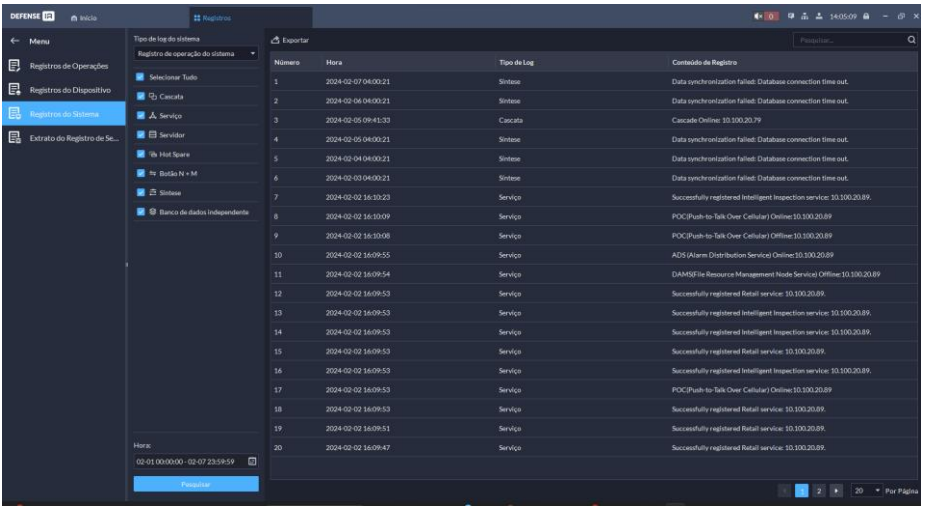
6.1.3 Log do Sistema

Visualize e exporte logs sobre como a plataforma está sendo executada, como por exemplo um erro do sistema.

Procedimento:

» Faça login no Cliente Defense.
» Na página inicial, selecione *Gerenciamento* > *Logs* > *Logs do Sistema.*
» Selecione um tipo de log.
» Especifique o tempo e clique em *Buscar.*
» É possível pesquisar até 1 mês de logs por vez.
» Para exportar os logs, clique em Exportar e siga as instruções na tela.
» Ao buscar os logs serão listados os logs com as seguintes características: data, hora, tipo de log e conteúdo e registro.

Na imagem abaixo está o exemplo de uma busca realizada:



6.1.4 Log de Serviço

Os serviços gerarão logs quando estiverem em execução. Esses logs podem ser usados para solu- ção de problemas. Se precisar de logs ainda mais detalhados, habilite o modo de depuração para que a plataforma gere logs detalhados.

Procedimento:

» Faça login no Cliente Defense.
» Na página inicial, selecione *Gerenciamento* > *Logs* > *Extrair Logs de Serviço.*
» Clique para baixar os logs do serviço dentro de um período especificado para o seu computador.
» (Opcional) Clique para habilitar o modo de depuração de um serviço e, em seguida, clique para baixar os logs detalhados dentro de um período especificado para o seu computador.

Após a habilitação do modo de depuração, a plataforma gerará uma grande quantidade de logs que ocuparão mais espaço em disco. Recomendamos que você desabilite o modo de depuração após concluir a solução de problemas.

7. Definindo as Configurações locais

Após realizar o login no cliente pela primeira vez, você precisa configurar os seguintes campos em parâmetros do sistema: Configurações Básicas, Parâmetros de vídeo, Reprodução de gravação, instantâneo, gravação, alarme, Vídeo Wall, Configurações de segurança e teclas de atalho.

7.1. Configurações Locais

Configuração do idioma do cliente, Tamanho do cliente, Horas e mais.

Procedimento:

» **Passo 1:** efetue o login no Defense Cliente. Na Página Inicial, selecione *Gerenciamento* > *Configu- ração Local.*

» **Passo 2:** clique em *Geral* e em seguida configure os parâmetros.

Parâmetros	Descrição
Tamanho do Cliente	one uma resolução adequada para o cliente de acordo com a tela ição do PC.
Exibir fuso horário em registros de clientes e eventos	lo selecionado, o cliente e o tempo dos alarmes mostrarão tanto o o e fuso horário.
Informação do nó do dispositivo	one que a arvore de dispositivos exibe os dispositivos e seus canais enas canais
Exibir miniaturas de visualização ao vivo ao passar o mouse sobre canais na árvore de dispositivos	lo selecionada, você pode passar o mouse sobre um canal na de dispositivos na Central de Monitoramento e um instantâneo de nagem de vídeo ao vivo será exibido.
Sincronização de tempo	ilitado, o cliente começa a sincronizar a hora da rede com o servidor oncluir a sincronização de tempo
Execução automática na inicialização	nbrar senha tiver sido selecionado na página de login, selecione ialização automática após a reinicialização, e o sistema ignorará a de login e abrirá diretamente a página inicial depois que reiniciar o próxima vez. nbrar senha não estiver selecionado na página de login, selecione alização automática após a reinicialização a página do cliente erá depois de reiniciar o PC.
Login automático	e o sistema para ignorar a página de login e abrir diretamente a inicial ao fazer login na próxima vez. nbrar senha e Login automático tiverem sido selecionados na página n, a função já estará ativada. nbrar senha já estiver sido selecionado enquanto Login automático stiver selecionado na página de login, selecione login automático na básica para habilitar essa função.
Limite de alarme da CPU	ário será solicitado a abrir mais um vídeo quando o uso da CPU er o limite definido
Criptografia de transmissão de áudio e vídeo	grafe todo o áudio e vídeo para garantir a segurança das informações.
Bloqueio automático do Client	nt será bloqueado após o período definido e voce não poderá r nenhuma operação. Clique para desbloquear o Client e verifique ia da conta atual para desbloquear o cliente.
Parâmetros de conversação de áudio auto adaptáveis	ivado, o sistema se adapta automaticamente à frequência de ragem do dispositivo, ao bit de amostragem e ao formato de áudio onversa de áudio.
Acesso ao modo de entrada e exibição do cartão	one um modo para a plataforma usar e exiba cartões de acesso. Por lo, quando você emite manualmente um cartão para uma pessoa, ode inserir A-F e números na numeração do cartão se Hex estiver nado, mas você só pode inserir 0-9 se Decimal estiver selecionado.
Sensibilidade do joystick	one a sensibilidade para quando você operar o joystick. Quanto a sensibilidade, mais frequentes comandos de joystick são os, e maior a possibilidade de que as operações sejam atrasadas ao baixo desempenho das câmeras PTZ.

» **Passo 3:** clique *Salvar.*

7.2. Definindo as Configurações de vídeo

Configurar a divisão de janela, modo de exibição, tipo de fluxo e modo de reprodução da visualiza- ção ao vivo e duração da reprodução instantânea

Procedimento:

» **Passo 1:** efetue o login no Defense Cliente. Na Página Inicial, selecione *Gerenciamento > Configu- ração local.*

» **Passo 2:** clique em vídeo e em seguida configure os parâmetros.

Parâmetros	Descrição
Divisão de janela padrão	Definir o modo de divisão da janela de vídeo
Escala de exibição de janela	Selecione entre Escala original e Tela cheia
Regra de comutação de fluxo	Quando o número de divisões de janela for maior do que o valor definido, o vídeo ao vivo alternará do tipo de fluxo principal para o tipo de subfluxo.
Modo de aquisição de fluxo em tempo real	Selecione-o de acordo com a situação. Se você selecionar Adquirir diretamente do dispositivo, os clients adquirirão fluxos de vídeo diretamente do canal. Se a aquisição direta falhar, a plataforma encaminhará os fluxos de vídeo para os clients. Quando o dispositivo e os clients estão conectados corretamente à rede, a aquisição direta pode reduzir o uso da largura de banda de encaminhamentos da plataforma. Se muitos clients estiverem adquirindo fluxos de vídeo de um canal, a aquisição poderá falhar devido ao desempenho insuficiente do dispositivo. As transmissões de vídeo serão encaminhadas aos clients pela plataforma.
Clique Duplo no vídeo para maximizar a janela e alternar para o fluxo principal	Se selecionado, você pode clicar duas vezes em uma janela de vídeo para maximizá-la e alternar do sub-fluxo para o fluxo principal. Clique duas vezes novamente para restaurar o tamanho da janela e em seguida, o sistema irá alterna-lo de volta para o sub-fluxo
Modo de Reprodução	» Prioridade em tempo real: o sistema pode diminuir a qualidade da imagem para evitar o atraso do vídeo. » Prioridade de fluência: o sistema pode diminuir a qualidade da imagem e permitir atraso para garantir fluência de vídeo. Quanto maior a qualidade da imagem, menor será a fluência do vídeo. » Prioridade de equilíbrio: o sistema equilibra a prioridade em tempo real e a prioridade de fluência de acordo com o desempenho real do servidor e da rede. » Personalizado: o sistema ajusta o buffer de vídeo e reduz o impacto na qualidade de vídeo causado pela rede instável. Quanto maior o valor, mais estável será a qualidade do vídeo.
Modo de decodificação Limite da CPU	» Decodificação de software pela CPU: Todos os vídeos serão decodificados pela CPU. Quando você está vendo vídeos ao vivo de grande quantidade de canais, ele vai ocupar muitos recursos da CPU que afeta outras opções. » Decodificação de software por GPU: Todos os vídeos serão decodificados pela GPU. A GPU é a melhor em operação simultânea do que a CPU. Essa configuração liberará recursos da CPU significativamente. » Modo de desempenho (CPU primeiro): Todos os vídeos serão decodificados pela CPU primeiro. Quando os recursos da CPU são levados até o limite de- finido, a plataforma usará a GPU para decodificar vídeos.
Exibir a exibição ao vivo anterior após a reinicialização	Se selecionado, o sistema exibirá a última visualização ao vivo automaticamente depois que você reiniciar o cliente.
Fechar vídeos sendo reproduzidos após longo período de inatividade	O sistema fecha a visualização ao vivo após automaticamente após a inatividade por um período de tempo pré-definido. Suporta até 30 minutos.
Tempo de inatividade	
Status do vídeo do dispositivo de exibição	Depois de ativado, se o dispositivo estiver gravando um vídeo, um ícone será exibido no canto superior da janela.

Tempo de reprodução instantânea	Clique  na página de visualização ao vivo para reproduzir o vídeo do período anterior. O período pode ser definido pelo usuário. Por exemplo, se você definir 30 segundos, o sistema reproduzirá o vídeo dos 30 segundos anteriores.
Tipo de pesquisa do fluxo de vídeo do dispositivo	Selecione um tipo de fluxo padrão ao reproduzir gravações de um dispositivo. Se somente a Sub-fluxo 2 estiver selecionado, mas o dispositivo não suportar o sub-fluxo 2, as gravações do sub-fluxo 1 serão reproduzidas
Rodar prioritariamente	Selecione um local padrão para vídeos gravados ao reproduzi-los, incluindo Priorizar Gravação de Dispositivo para reproduzir vídeos gravados armazenados em dispositivos e Priorizar Gravação Central para reproduzir vídeos gravados armazenados na plataforma.
Modo de extração de quadro	A extração de quadros é útil para garantir fluência e diminuir a pressão na decodificação, largura de banda e encaminhamento ao reproduzir vídeos de alta definição. Quando a extração de quadros estiver habilitada, determinados quadros serão ignorados. » Não extrair: A extração de quadros não será habilitada em nenhuma situação. » Auto adaptável: A plataforma permitirá a extração de quadros com base na resolução e na velocidade. » Força: A extração de quadros está sempre ativa.
Intervalo de instantâneo continuo	Defina o número e o intervalo entre cada Instantâneo. Por exemplo, se o Intervalo de Instantâneo Continuo for de 10 segundos e o Número de Instantâneos Contínuos for 4, quando você clicar com o botão direito do mouse no vídeo ao vivo/Reprodução e selecionar instantâneos, 4 imagens serão tiradas a cada 10 segundos
Número de instantâneo contínuos	

» **Passo 3:** clique *Salvar.*

7.3. Definindo a configurações do Vídeo Wall

Configure o modo de vinculação padrão e o tipo de fluxo do Vídeo Wall.

Procedimento:

» **Passo 1:** efetue o login no Defense Cliente. Na Página Inicial, selecione *Gerenciamento* > *Configu- ração local.*

» **Passo 2:** clique em *Vídeo Wall* e em seguida configure os parâmetros.

Parâmetro	Descrição
Tipo padrão de Fluxo	Selecione Fluxo principal, Sub Fluxo 1, Sub Fluxo 2 ou Sinal Local como o tipo de fluxo padrão para a exibição de vídeo.
Regra de comutação de fluxo	Quando o número de divisões de janela for maior do que o valor negado, o vídeo ao vivo alternará do tipo de fluxo principal para o tipo de subfluxo.
Clique duplo no vídeo para maximizar a janela e alternar o para o fluxo principal	Clique duplo no vídeo para maximizar a janela e em seguida, seu tipo de fluxo alternará para o fluxo principal.
Duração da reprodução da fonte de vídeo	Defina o intervalo de tempo padrão entre os canais para exibição do tour. Por exemplo, se estiver configurado 5 segundos e você estiver visitando 3 canais de vídeo, a imagem de vídeo ao vivo de cada canal será reproduzida 5 segundos antes de mudar para o próximo canal.
Modo de decodificação para vídeo wall	» Tour: Vários canais de vídeo alternam para decodificar em uma janela por padrão. » Bloco: Os canais de vídeo são exibidos nas janelas por bloco por padrão. » Pergunte toda vez: Ao arrastar um canal para a janela o sistema pedirá que você selecione o modo tour ou bloco

» **Passo 3:** clique *Salvar.*

7.3.1 Definição da Configuração de Alarmes

Configurar o som do alarme e o método de exibição do alarme no cliente

Procedimento:

» **Passo 1:** efetue o login no Defense Cliente. Na Página Inicial, selecione *Gerenciamento* > *Configu- ração local.*

» **Passo 2:** clique em *Alarme* e configure os parâmetros.

Parâmetro	Descrição
Padrão	Todos os tipos de alarmes usarão o mesmo som de alarme padrão quando acionados
Customizado	Clique em Modificar som de alarme em seguida você pode alterar o som do alarme e seu modo de reprodução de cada tipo de alarme.
Abrir Ligação de vídeo quando alarme ocorrer	Se selecionada a plataforma abrirá automaticamente o(s) vídeo(s) vinculado(s) quando ocorrer um alarme: » Como pop-up: O vídeo de alarme será reproduzido em uma janela pop-up. » Abrir na visualização ao vivo: O vídeo do alarme será reproduzido em uma janela na Central de monitoramento. Para essa função funcionar devidamente, você deve habilitar Quando um alarme é acionado, exibir visualização ao vivo da câmera no cliente ao configurar um evento.
Duração da Exibição Pop-up Quando um alarme é acionado a janela pop-up do alarme e o cliente serão exibidos a parte superior da tela	Ao configurar os vídeos de alarme para serem exibidos como janelas pop-up, você pode selecionar por quanto tempo as janelas pop-up serão exibidas e se deseja exibir as janelas pop-up e o cliente na parte superior da tela
Dispositivo no mapa pisca quando alarme ocorre	Defina um ou mais tipos de alarme para notificação de alarme no mapa. Quando ocorre um alarme o dispositivo correspondente pisca no mapa.

» **Passo 3:** clique *Salvar.*

7.4. Definir configuração Armazenamento de arquivos

Configure o caminho de armazenamento, regra de nomenclatura, tamanho do arquivo e o formato de gravações e instantâneos.

Procedimento:

» **Passo 1:** efetue o login no Defense Cliente. Na Página Inicial, selecione *Gerenciamento* > *Configu- ração local.*

» **Passo 2:** clique em *File Storage* e configure os parâmetros.

Parâmetro	Descrição
Regra de nomenclatura de vídeo	Selecione uma regra de nomenclatura para gravações manuais.
Caminho de armazenamento de vídeo	Defina um caminho de armazenamento de gravações manuais durante a visualização ao vivo ou a reprodução. O caminho padrão é C:\Users\Pubilc\ Defense IA\Record.
Tamanho do arquivo de vídeo	Configure o tamanho máximo de um arquivo de vídeo. Se você baixar um vídeo maior do que um tamanho definido a plataforma o dividirá em vários arquivos. O tamanho máximo pode ser de até 4GB para sistemas operacionais de 32 bits e 1024 GB para sistemas operacionais de 64 bits.
Formato da imagem	Selecione um formato para instantâneos.
Regra de nomenclatura de imagem	Selecione uma regra de nomenclatura para instantâneos.
Caminho de armazenamento de imagem	Defina um caminho de armazenamento para instantâneos. O caminho padrão é C:\Users\Public\Defense IA\Picture.

» **Passo 3:** clique *Salvar.*

7.5. Exibindo teclas de atalho

Exibir teclas de atalho para operar o cliente rapidamente

Procedimento:

» **Passo 1:** efetue o login no Defense Cliente. Na Página Inicial, selecione *Gerenciamento* > *Configu- ração local.*

» **Passo 2:** clique em *Tecla de atalho* para ver as teclas de atalho do teclado do PC e do joystick USB.

7.6. Exportando e importando configurações

Para os parâmetros nas configurações locais configurados pelo usuário atualmente conectado ao cliente PC, eles podem ser exportados e importados para outro client PC. Isso é útil para que o usu- ário não precise configurar os parâmetros novamente ao usar uma nova plataforma.

Procedimento:

» **Passo 1:** efetue o login no Defense Cliente. Na Página Inicial, selecione *Gerenciamento* > *Configu- ração local.*

» **Passo 2:** clique em *Exportar/Importar Configurações* no canto inferior direito.

» **Passo 3:** exportar ou Importar configurações.

7.6.1 Configurações de exportação.

Os parâmetros de alarme, som e mapa de Flashs não serão incluídos nas configurações exportadas.

1. Clique em *Exportar configurações.*
2. Selecione *Exportar para arquivo* e em seguida, exporte as configurações para o caminho especifi- cado do seu computador. Ou selecione Enviar por e-mail e envie as configurações para o endereço de e-mail especificado.
3. Clique *OK.*

7.6.4 Importar configurações.

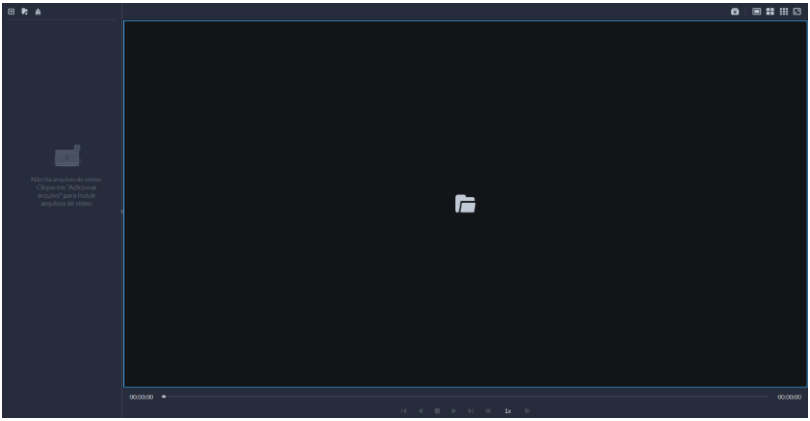
1. Clique em importar configurações.
2. Clique em  em seguida, abra o arquivo exportado de configurações.
3. Clique em *OK.*

7.7. Reproduzir Vídeos Locais

Você pode reproduzir vídeos locais diretamente na plataforma.

Procedimento:

» **Passo 1:** efetue o login no Defense Cliente. Na Página Inicial, selecione *Gerenciamento* > *Vídeo local.*



» **Passo 2:** clique para selecionar um ou mais arquivos, ou para abrir todos os arquivos em uma pasta.

» **Passo 3:** arraste um arquivo para a janela à direita ou clique nele com o botão direito do mouse para reproduzir.

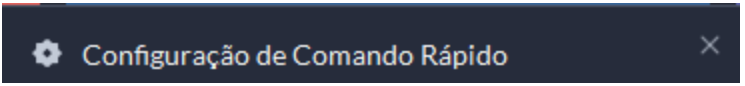
Parâmetro	Descrição
Menu com o botão direito do mouse	» Instantâneo contínuo: tire instantâneos da imagem atual (três instantâneos de cada vez por padrão). » Ajuste de vídeo: ajuste o brilho, contraste, saturação e croma do vídeo » Zoom digital: clique nele e em seguida, clique duas vezes na imagem do vídeo para ampliar a imagem. Clique duas vezes na imagem novamente para sair do zoom
	Feche todos os vídeos em reprodução
	Divida a janela em várias e reproduza um vídeo em tela cheia.
	Tire um instantâneo da imagem atual e salve-a localmente.
	Feche a Janela
1x	Reprodução rápida/lenta suporta 64X ou 1/64X
	Reprodução quadro a quando/ Quadro a quadro para trás
	Capture o destino na janela de reprodução. Clique para selecionar o método de pesquisa e em seguida o sistema vai para a página com os resultados da pesquisa. Mais operações: » Mova a área de seleção. » Ajuste o tamanho da área de seleção. » Clique com o botão direito do mouse para sair da pesquisa por instantâneo.

7.8. Comandos Rápidos

Personalize comandos HTTP e execute-os rapidamente. Os métodos de solicitação de GET, POST, PUT e DELETE são suportados.

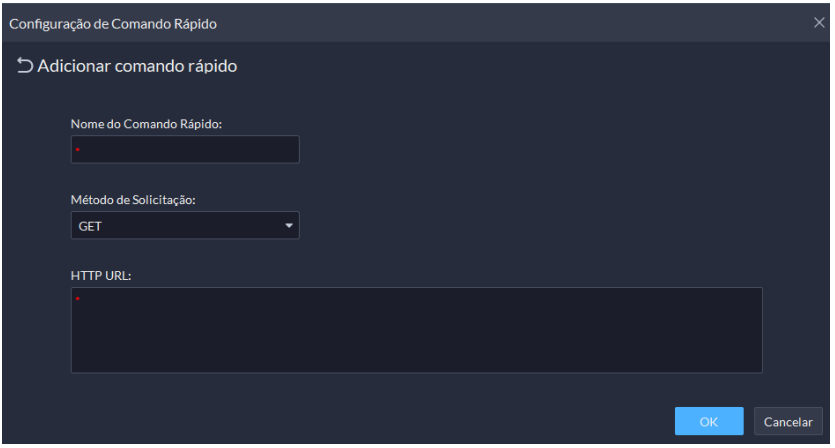
Procedimento:

» **Passo 1:** efetue o login no Defense Cliente. Na Página Inicial, selecione *Gerenciamento* > *Coman- dos Rápidos.*

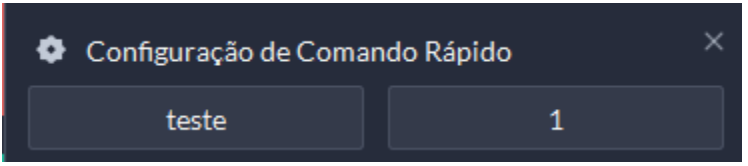


» **Passo 2:** clique .

» **Passo 3:** clique *Adicionar.*



» **Passo 4:** configure os parâmetros e clique *OK.*



» **Passo 5:** clique no nome de um comando rápido e execute-o

intelbras

fale com a gente

Suporte a clientes: (48) 2106 0006
Fórum: forum.intelbras.com.br
Suporte via chat: chat.apps.intelbras.com.br
Suporte via e-mail: suporte@intelbras.com.br
SAC / Onde comprar? / Quem instala? : 0800 7042767

Importado no Brasil por: Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira
Rodovia SC 281, km 4,5 – Sertão do Maruim – São José/SC – 88122-001
CNPJ 82.901.000/0014-41 – www.intelbras.com.br

01.24
Origem: China