Manual do usuário

DEFENSE IA 3.1

Defense IA 3.1
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.

11.1. 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.

21.2. 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.

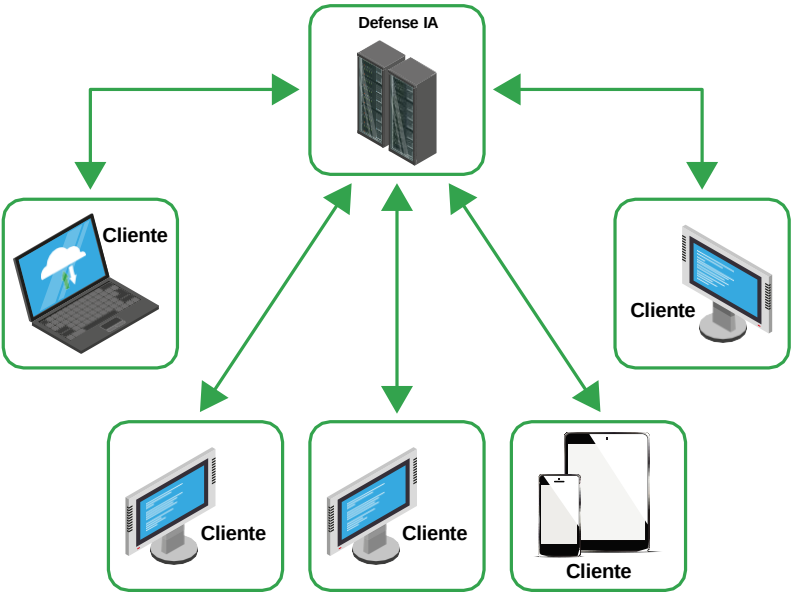
» Se houver alguma incerteza ou controvérsia, consulte nossa explicação final.

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 principais 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 Recomendada	CPU: Intel® Xeon® Silver 4310T @ 2.3 GHz 10 núcleos RAM: 16 GB Interface de Rede: 4× portas Ethernet @ 1000 Mbps Armazenamento: SSD/HDD Classe Enterprise 1 TB @ 7200 RPM Espaço Livre: 500 GB	Windows Server 2016 Windows Server 2019 Windows Server 2022
Configuração mínima	CPU: Intel® Xeon® E-2224 @ 3.4 GHz 4 núcleos RAM: 8 GB **disponível** Interface de Rede: 1x porta Ethernet @ 1000 Mbps Armazenamento: HDD Classe Enterprise 1 TB @7200 RPM Espaço Livre: 500 GB	Windows 10 Pro - 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*

12.1. Implantação de servidor único

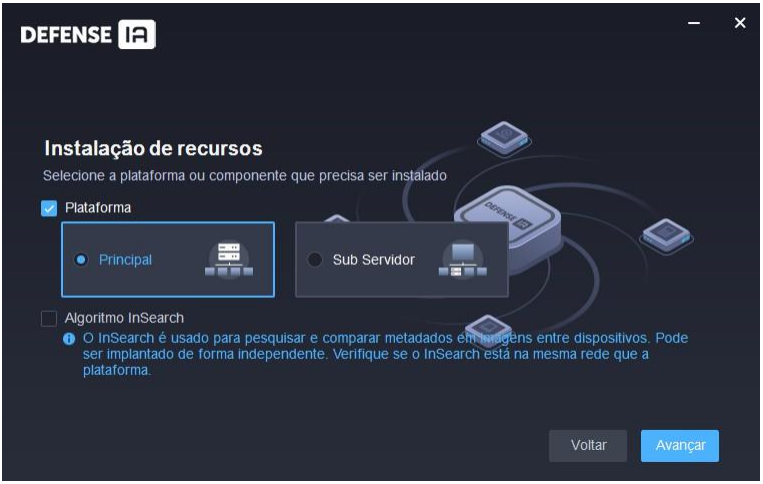
Essa estrutura é recomendada para projetos envolvendo um menor números de dispositivos, dessa forma, apenas um servidor Defense IA é necessário.

22.2. 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 algoritmo 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.

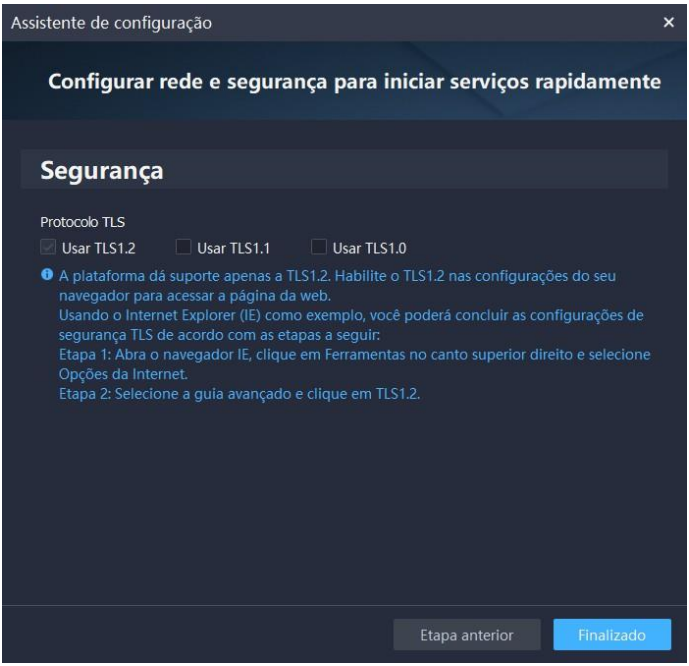
Verifique se o local de instalação cumpre os requisitos de espaço disponível.

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.

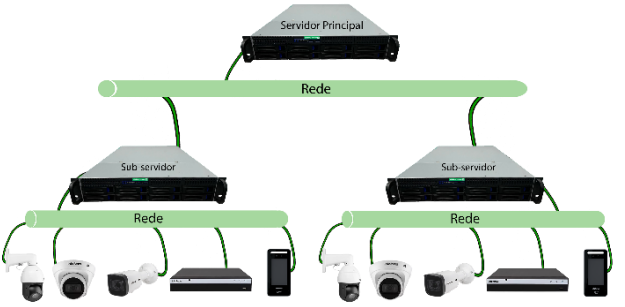
32.3. Atualizar e desinstalar

» 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.

2.3. 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.



12.1. 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.

22.2. 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.*

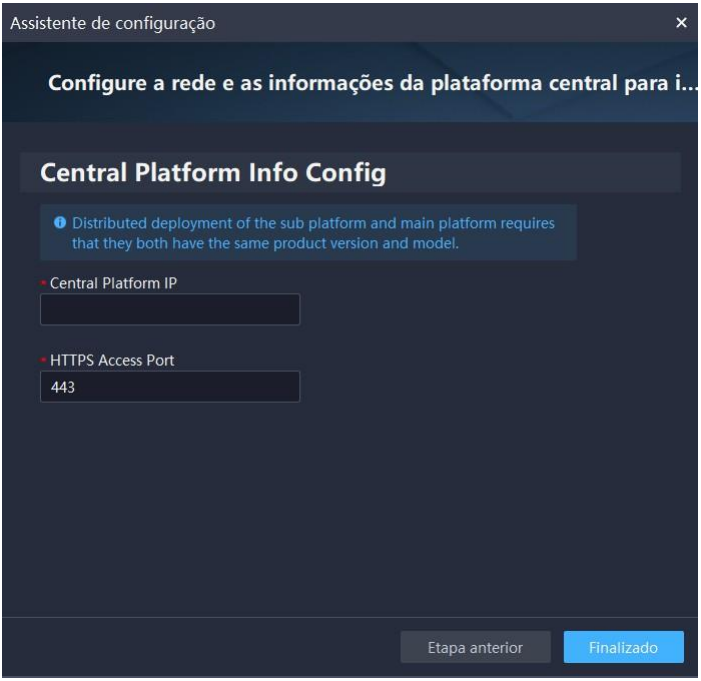
Verifique se o local de instalação cumpre os requisitos de espaço disponível.

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.*

32.3. 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.

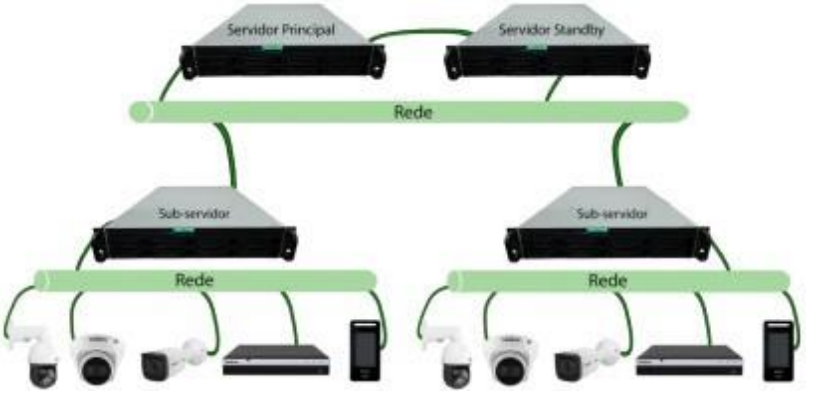
» Ao selecionar o tipo de servidor como standby, a lista de servidores auxiliares será atualizada, selecione o servidor o qual deseja acompanhar.

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*.

2.4. Hot Standby

Utilizado com sistemas que exigem alta estabilidade. O servidor em espera assume o sistema quando ocorre mau funcionamento no servidor (como desligamento e desconexão de rede). Você pode mudar de volta ao servidor ativo original depois que ele se recupera.



12.1. N+M

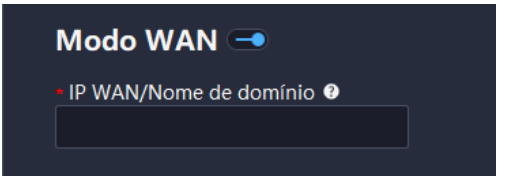
Cada sub-servidor tem um servidor em espera para manter a estabilidade. Quando um sub-servidor não funciona, o sistema o substitui por um servidor ocioso em espera. Quando o servidor com defeito se normaliza, você pode alternar manualmente de volta para ele. Se você não os alterna manualmente, o sistema fará automaticamente o switch se o servidor em espera funcionar mal.

2.5. 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: *www.intelbras.com.br.*

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.

13.1. Primeiro acesso à plataforma

Para o primeiro acesso à plataforma, você deve cadastrar uma senha para o usuário system, usuário 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.

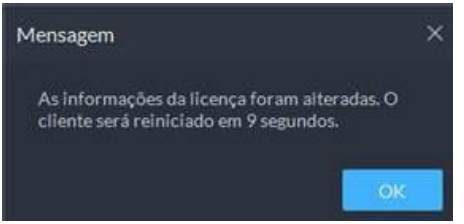
Para cadastrar a senha, insira o endereço e porta do servidor em seus respectivos campos, ou selecione o servidor a partir da lista suspensa, caso este apareça. Após isso você será diretamente encaminhado para o cadastro da senha.

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.

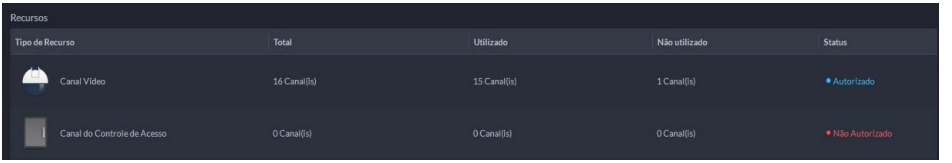
3.2. Licenciamento

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.

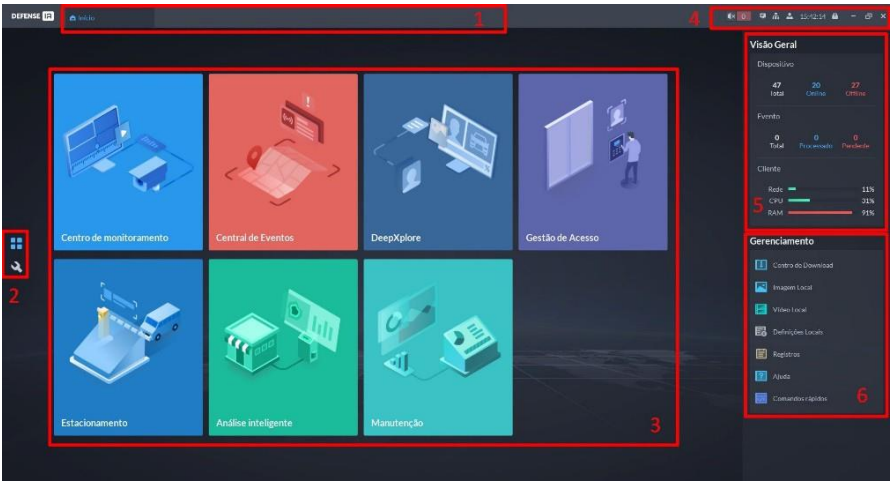


Você pode verificar as informações da licença no menu de configurações da licença, onde é apresentado o recurso total disponibilizado pela licença ativada, o total já consumido e o total disponível para uso. Além disso, também é possível verificar se um módulo está ou não Autorizado para uso:



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.

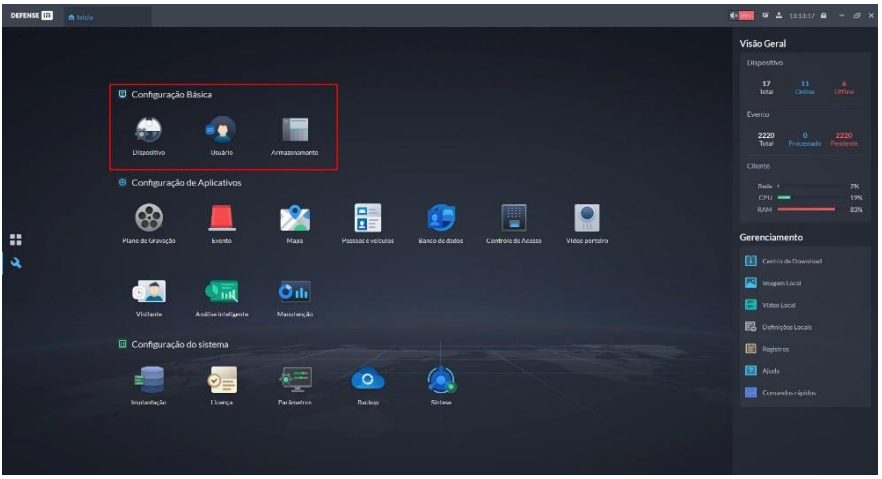


Alguns módulos necessitam de licenças e permissões específicas para visualização. Verifique se o usuário de utilização possui as permissões necessárias e as devidas licenças estão ativadas.

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. Menu de configurações

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



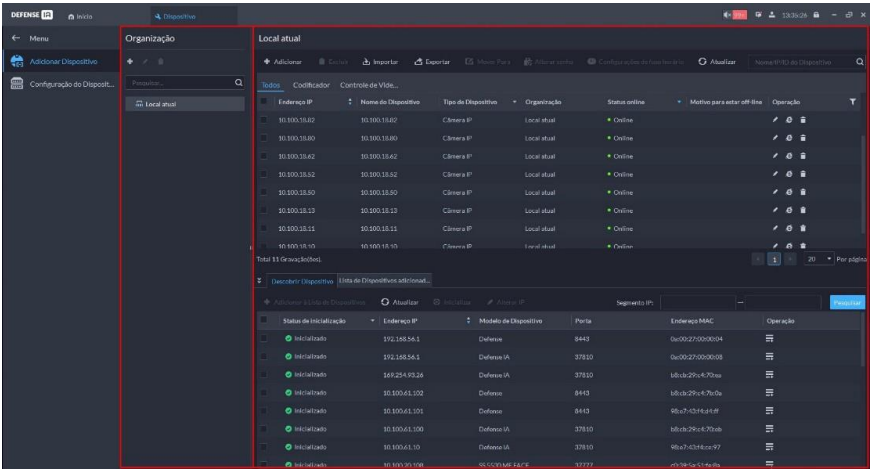
13.1. Configuração de dispositivos

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:

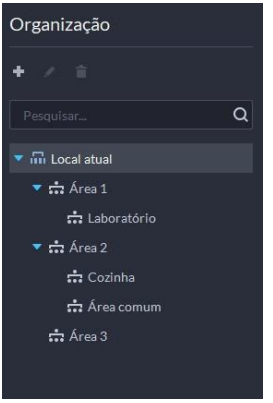


13.1. Organização

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.*

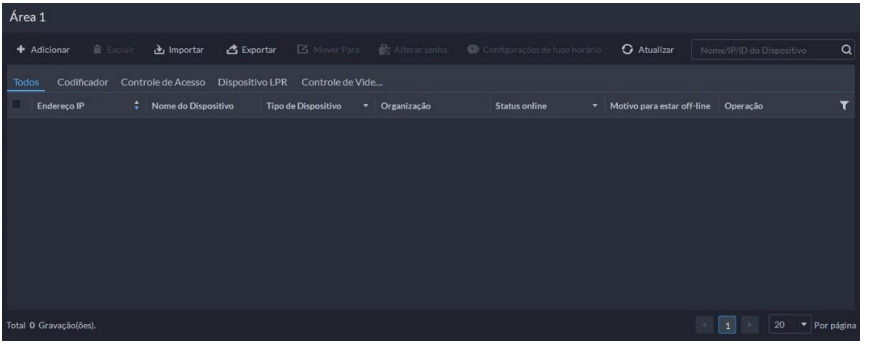
Recomenda-se dividir os dispositivos adicionados no sistema entre diferentes organizações para melhor gerenciamento destes, como por exemplo, caso tenha-se um local dividido entre três áreas (área 1, 2 e 3), e cada área apresenta seus próprios cômodos, com seus respectivos dispositivos, estes podem ser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



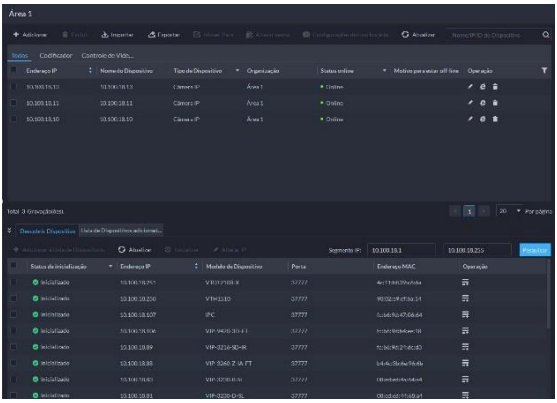
Na janela ao lado, apresentada no próximo tópico, é possível realizar o gerenciamento de dispositivos da organização selecionada.

23.2. Local

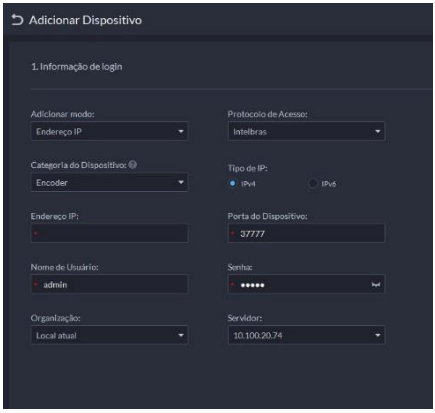
É nessa janela onde é possível gerenciar a conexão de dispositivos. É possível adicionar/excluir dispositivos um a um, ou em lotes. Neste módulo também é possível exportar, mover, alterar senhas e configurar fuso-horário de dispositivos. No topo, identifica-se a organização selecionada, e logo abaixo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

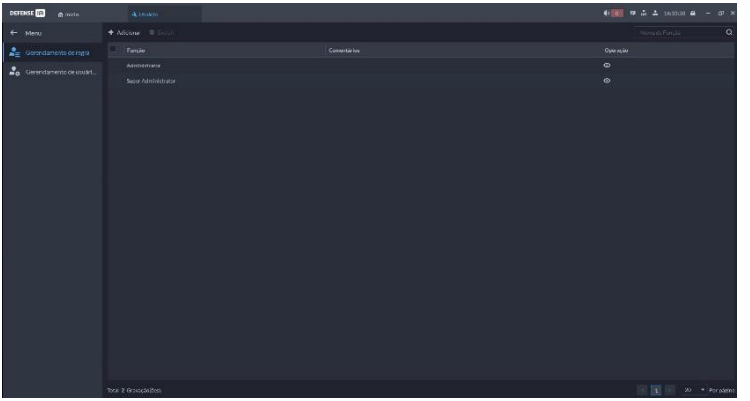
Com os dispositivos adicionados, você pode gerenciá-los a partir das funções dessa página. Mais informações sobre gerenciamento de dispositivos e métodos de adicioná-los são apresentadas no capítulo *Gerenciamento de Dispositivos*.

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 

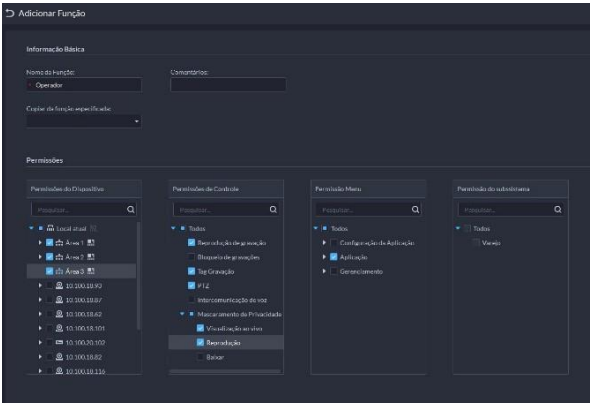
, em configurações.

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.



13.1. 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:

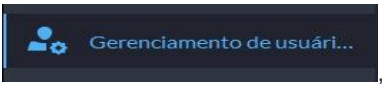


É possível selecionar dispositivos específicos, organizações e interface gráfica que o usuário com essa função terá acesso, também é possível selecionar quais permissões essa função concederá ao usuário, tanto para gerenciamento de dispositivos, quanto para gerenciamento do sistema.

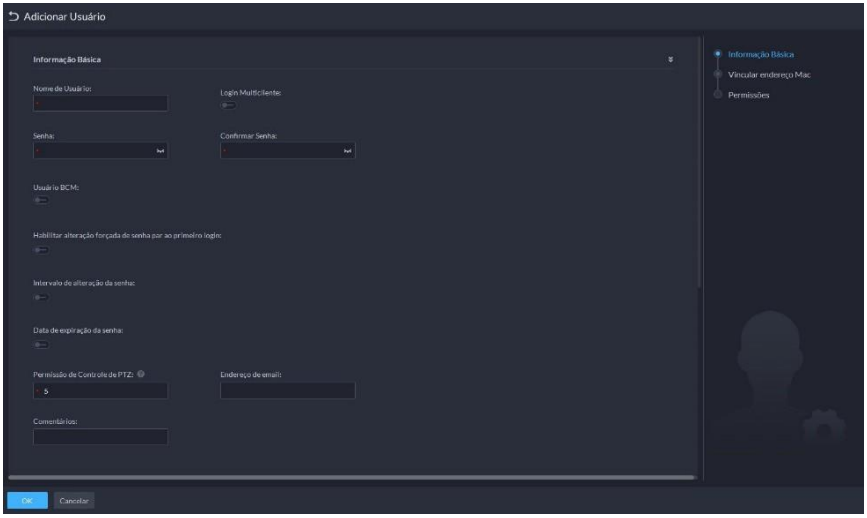
23.2. Adicionar usuários

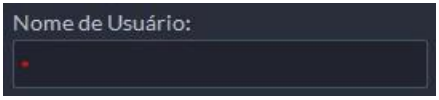
A plataforma apresenta dois modos de adição de usuários diferentes, é possível adicionar manualmente um usuário por vez e/ou sincronizar e importar usuários de um servidor AD previamente configurado.

Adicionar um usuário

Na aba *Gerenciamento de usuários* 

, no menu de configuração de usuários, clique em Adicionar no topo. Uma tela para preenchimento será aberta. Preencha as informações 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 encontradas em nosso datasheet.

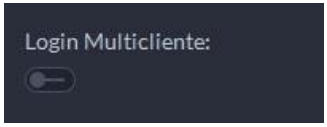


» 

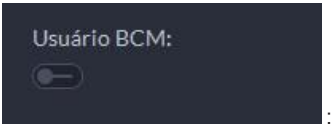
: identificador do usuário, não pode existir mais de um usuário com o mesmo nome.

» 

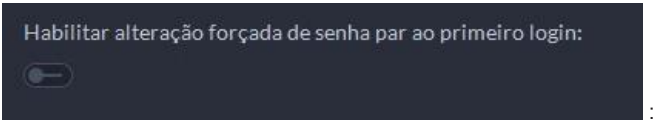
: senha do usuário, recomenda-se utilizar uma senha forte.

» 

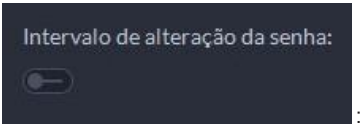
: botão Multicliente, caso selecionado, indica que o usuário pode efetuar o login em mais de um cliente simultaneamente.

» 

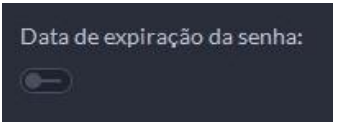
: botão de usuário BCM, caso selecionado, indica que o usuário pode participar de chamadas de grupo. Um usuário BCM não pode ser um usuário Multicliente.

» 

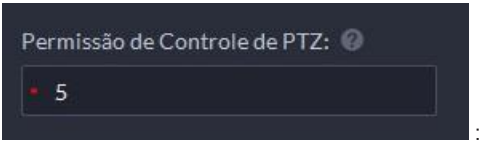
: botão de forçar troca de senha após primeiro login, caso selecionado, o usuário deverá trocar a senha registrada ao efetuar o login pela primeira vez.

» 

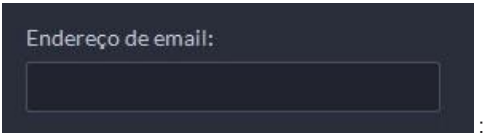
: botão de Intervalo de alteração de senha, caso selecionado, o usuário deverá trocar a senha após um período contínuo definido entre 1 e 365 dias.

» 

: 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.

» 

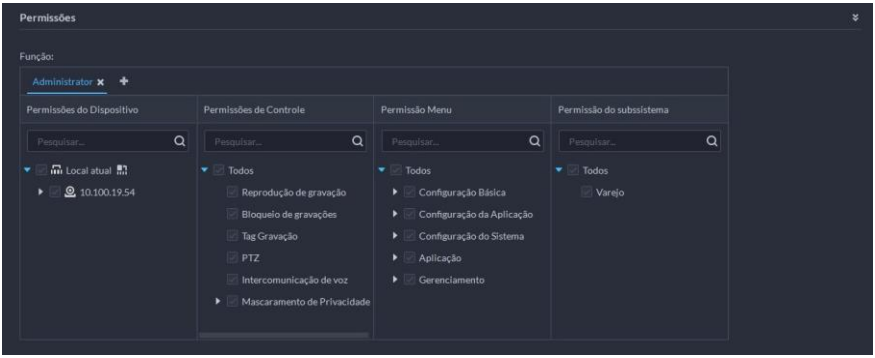
: vincula um endereço de e-mail ao usuário.

» 

: texto auxiliar vinculado ao usuário.

» 

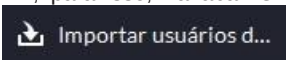
: botão para vincular endereços MAC ao usuário.



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

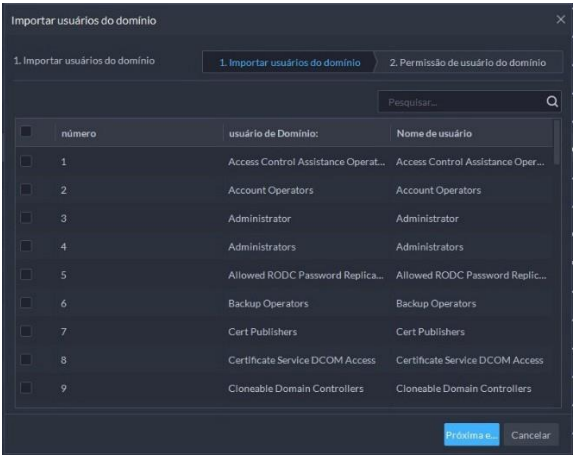
Sincronizar com servidor AD

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 *"Organizational Unit"* como um grupo de domínio, (Usuários adicionados do tipo ***"Security/Distribution Group - Universal/Global"*** serão reconhecidos como ***usuários*** no Defense e não como um ***grupo***).

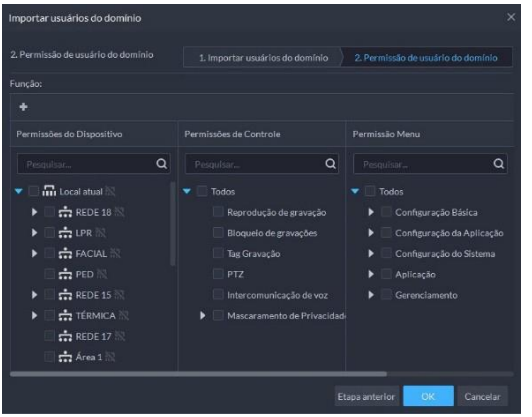
Após um servidor AD configurado na plataforma, você pode importar usuários do domínio para o Defense IA, para isso, na aba "Gerenciamento de usuários" clique em Importar usuários do domínio 

no topo. Um pop-up deve aparecer com a lista de usuários do domínio. 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

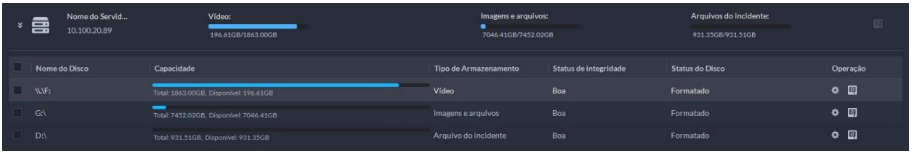
O Defense IA permite diferentes configurações de discos em seu ambiente (tanto em volume local, quanto em volume de rede), apresentando 3 configurações de disco: disco de vídeo, disco de imagens e arquivos e disco de arquivos de incidente.

Acesse Armazenamento 

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

13.1. 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  .

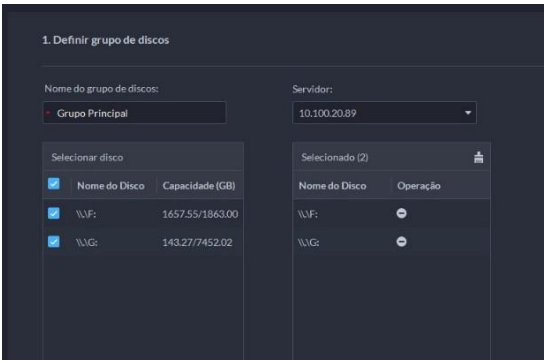


Na janela expandida é possível ver a capacidade, integridade, status e realizar operações de disco. Clicando na engrenagem é possível selecionar o tipo de disco que deseja configurar; o botão ao lado formata o disco apagando todos os dados nele.

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

23.2. 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 dis- cos. 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.*

Para informações sobre capacidades e armazenamento, verifique a ficha técnica do produto em nosso site: *www.intelbras.com.br.*

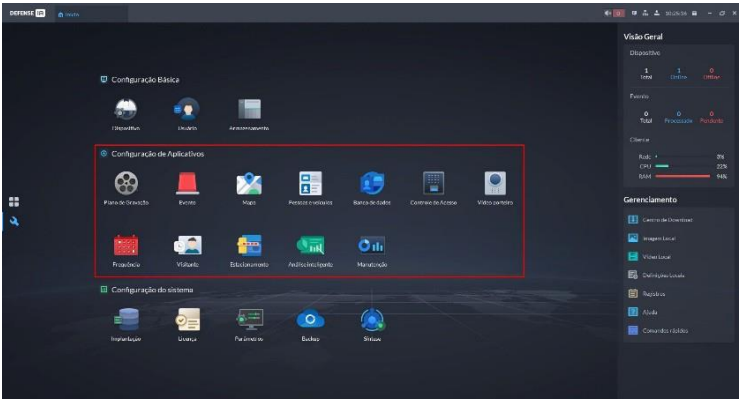
Caso tenha servidores auxiliares configurados, também é possível gerenciar seus discos pela interface.

4. Configurações iniciais de aplicativos

Após concluir as configurações básicas, você pode avançar na preparação de alguns módulos essenciais 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, destas 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. Plano de Gravação

Acessando a página de Plano de Gravação 

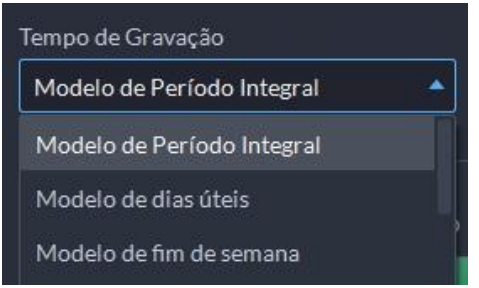
, é possível navegar entre duas janelas, Plano e Recuperação de gravação.

14.1. Criar plano de gravação

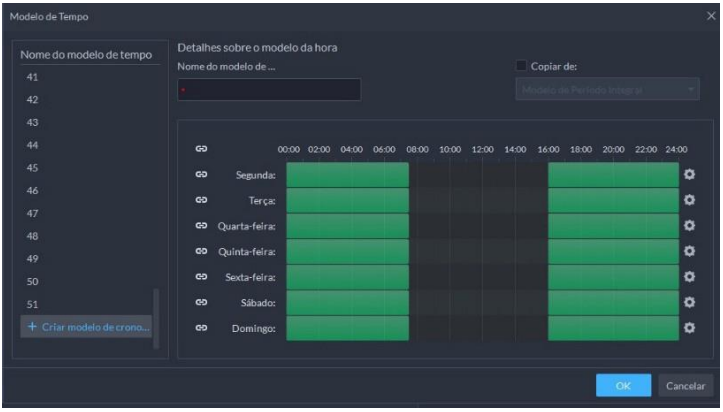
É nesta janela em que adiciona-se os planos de gravação dos dispositivos adicionados no servidor, podendo optar pelo plano geral de gravação, ou plano de gravação por detecção de movimento. Assim como na página de “Configuração de dispositivos”, os dispositivos aparecem na aba de Organização. Para adicionar 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 quando 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.

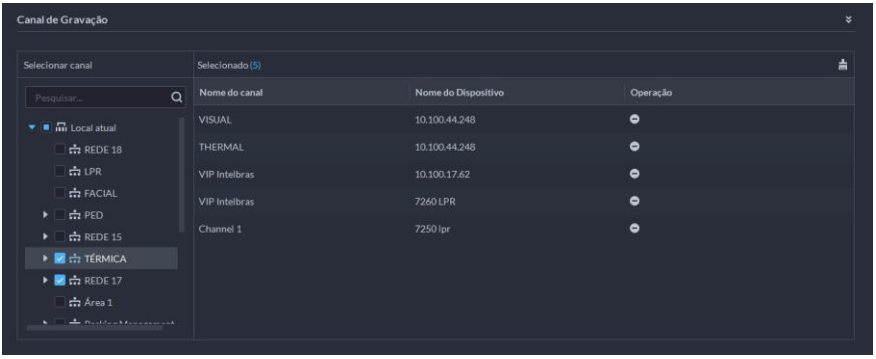


Além desses, também é possível criar um período de gravação personalizado clicando em *Criar modelo de cronograma.*



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.



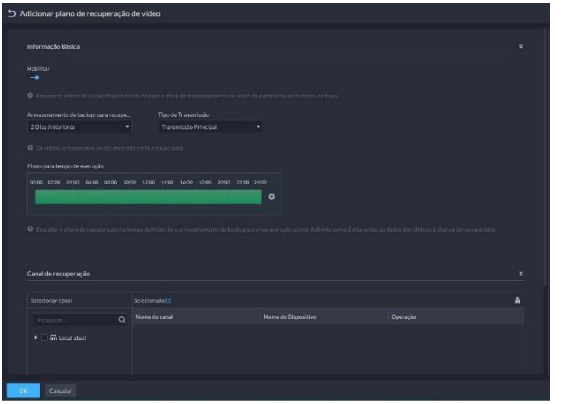
Todos os dispositivos selecionados serão vinculados ao mesmo plano de gravação, mas é possível gerenciá-los de forma separada.

24.2. 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.

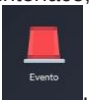
A recuperação de gravação tem como objetivo agendar um cronograma para que vídeos e/ou arquivos sejam copiados do armazenamento do dispositivo para o armazenamento do servidor. Possuindo prazo máximo de 7 dias e mínimo de 1 dia (dia anterior), o plano pra recuperação de vídeos e arquivos pode ser configurado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

4.3. 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 

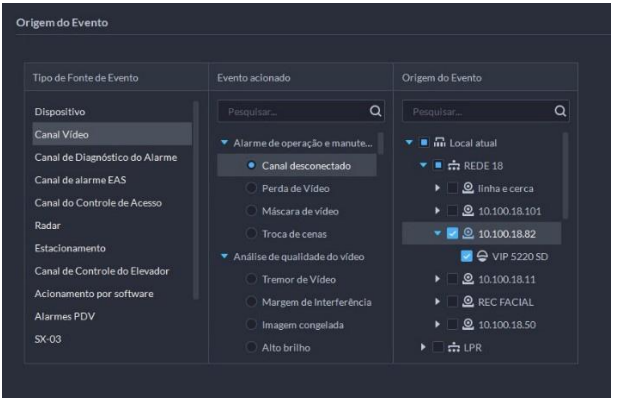
.

14.1. Adicionar Eventos

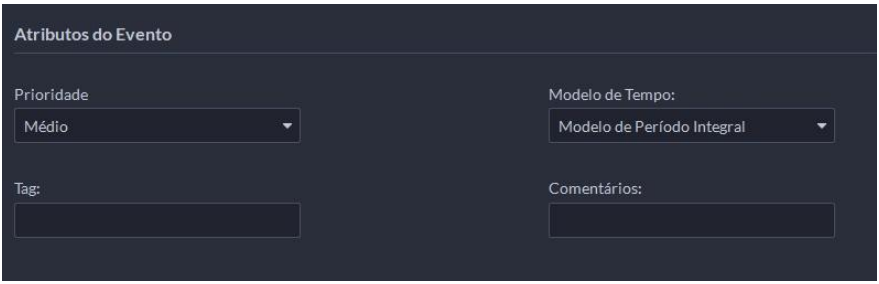
Para adicionar um evento, clique em Adicionar, a interface de criação de evento será aberta. Nessa interface deve-se selecionar parâmetros do sistema e de dispositivos, vinculando-os ao evento desejado, este processo é realizado em 5 etapas.

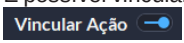
Primeiramente, deve-se indicar o tipo e origem do evento, selecionando um dos eventos disponíveis na lista e o dispositivo que será responsável pelo gatilho do evento.

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 personalizado, veja aqui). Também é possível definir uma Tag e adicionar comentários ao evento.

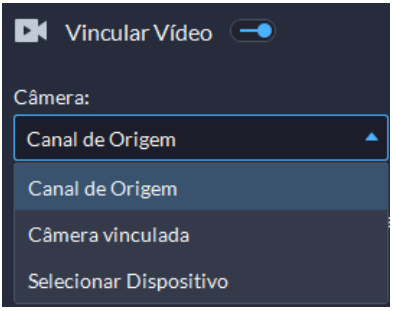


É possível vincular ações a partir do acionamento do evento, para isso, ative o botão *Vincular ação* 

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.



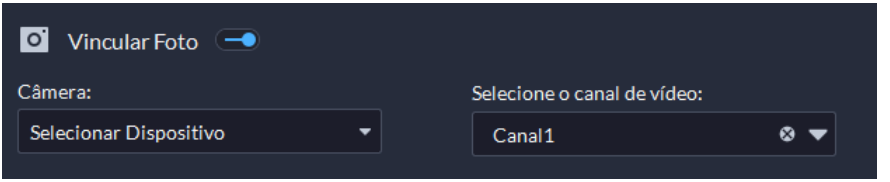
» **Canal de Origem:** vincula ao evento o próprio canal de vídeo que o gerou.

» **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



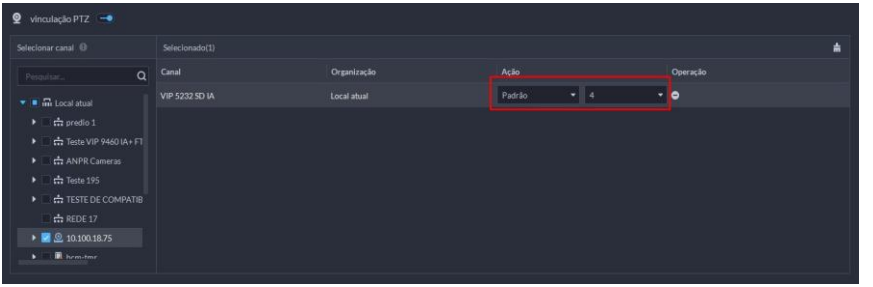
Assim como a anterior, esta ação vincula um canal de vídeo ao evento e um snapshot é realizado, capturando a imagem durante o acionamento do evento.

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

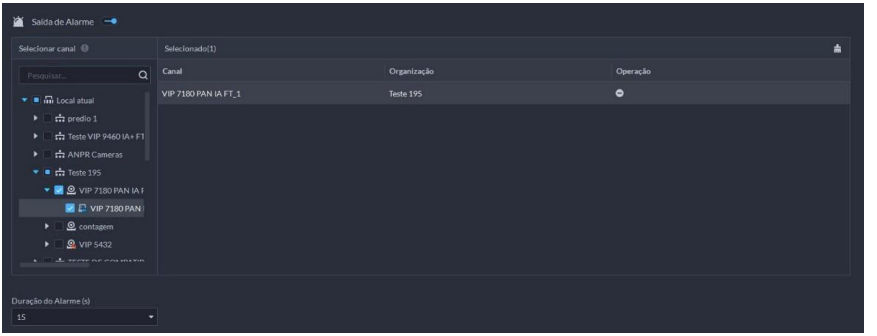
Vincular PTZ

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.



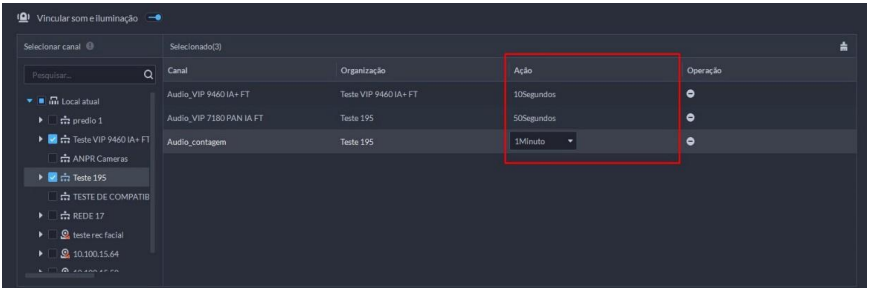
Saída de Alarme



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

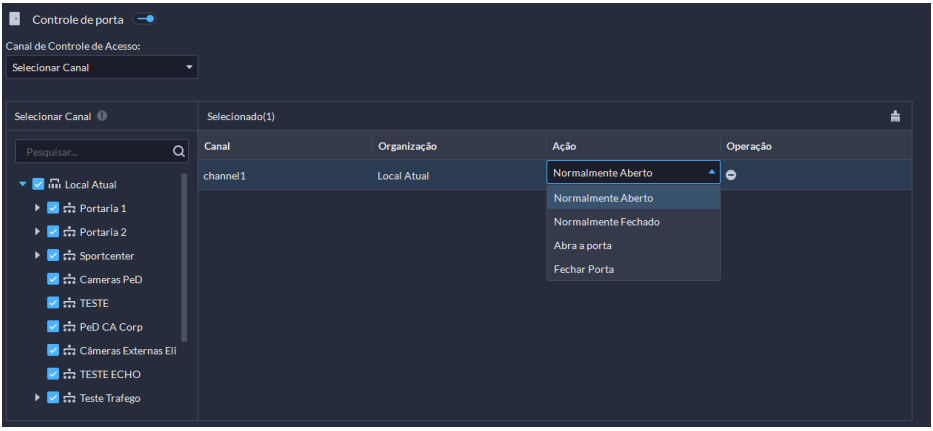
Assim como a anterior, esta ação vincula saídas de dispositivos a partir do acionamento do evento. Saídas sonoras e luminosas são vinculadas, e sua duração pode ser selecionada na coluna *Ação.*



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.

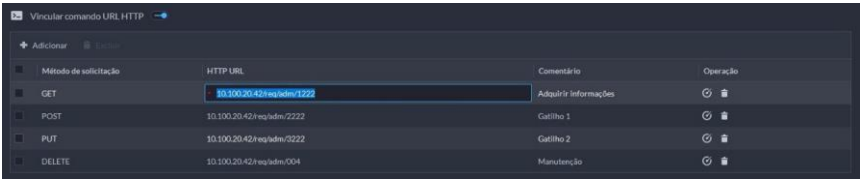
É possível aplicar a regra a todos os canais de controle de acesso da plataforma, ou selecionar os canais desejados e aplicar caso a caso.



Comando URL HTTP

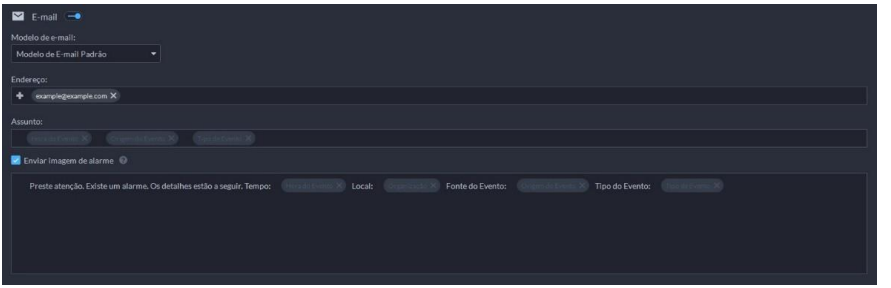
É possível vincular comandos HTTP a partir do acionamento do evento. Para isso, clique em *Adicionar* 

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 comentários e testar o comando configurado.



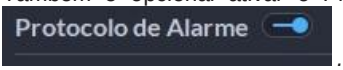
E-mail

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

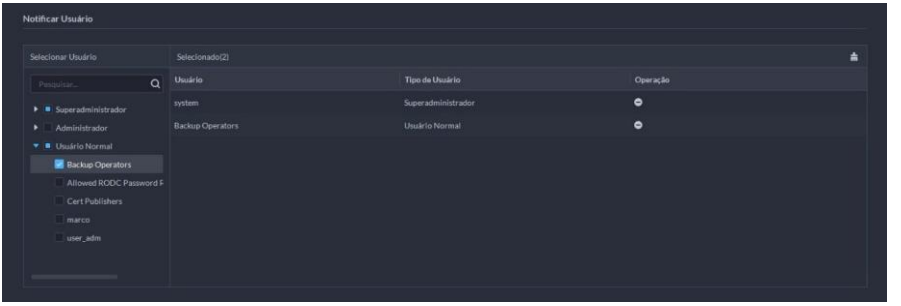
Também é opcional ativar o Protocolo de Alarme ativando o botão *Protocolo de Alarme*



.

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  .

4.4. Vinculação de eventos

Este capítulo apresenta os negócios básicos, como plano de armazenamento, monitoramento de vídeo, controle de acesso, controlador de alarme, Vídeoporteiro, detecção de alvos, reconhecimento facial, estacionamento e análise inteligente

14.1. Configurando Eventos

Para receber alarmes disparados por dispositivos, é preciso configurá-los na plataforma.

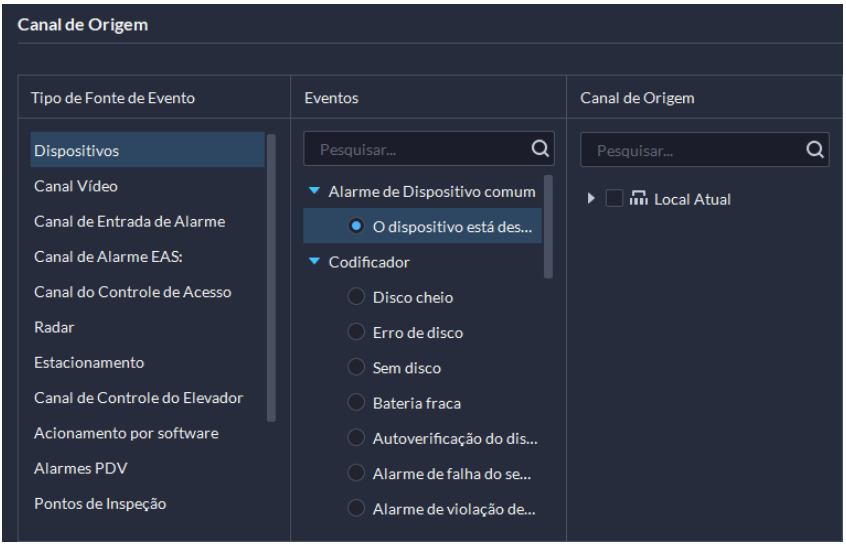
Configurando a vinculação de eventos

Configure a origem do evento e as ações vinculadas. Quando o evento é acionado, a plataforma executará as ações que você definiu, como tirar um instantâneo gravando um vídeo.

Procedimento:

» **Passo 1:** Faça o login no cliente do Defense. Na página inicial, clique , e na seção de *Configuração de aplicativo,* selecione *Eventos > Configuração de eventos.*

» **Passo 2:** clique *Adicionar.*



» **Passo 3:** configure a fonte de evento.

Parâmetro	Descrição
Dispositivo, canal de vídeo, canal de entrada de alarme, canal de alarme EAS, canal de controle de acesso, radar, estacionamento, canal de controle de elevador e alarme POS	Selecione o tipo de acordo com o tipo do dispositivo ou canal. » Antes de realizar o evento, verifique se os recursos do canal correspondem ao tipo de evento, caso contrário, o tipo de evento não poderá ser selecionado como a fonte de alarme. » Se a opção *Canal de entrada de alarme* estiver selecionada, verifique se o Evento acionado selecionado corresponde ao recurso de canal do canal de entrada de alarme selecionado. Caso contrário, o evento não ser acionado.
Evento Combinado	Quando um evento combinado é acionado, a plataforma executa as ações vinculadas definidas.
Alarme customizável	**Evento** » **Evento padrão estendido:** é usado para eventos que os dispositivos suportam, mas não o faz. Clique em *Adicionar evento padrão estendido* e, em seguida configure os parâmetros. » **Fonte de alarme:** acesse eventos de dispositivos codificadores, canais de vídeo e canais de entrada de alarme. » **Imagem do evento:** ao configurar um evento para um canal vídeo, você pode escolher se deseja se inscrever em imagens do evento. Ao assinar as fotos, a plataforma receberá imagens de alarme. No entanto, se a fonte de alarme não gerar imagens de alarme, assinar as imagens do evento fará com que a plataforma não receba o alarme. » **Nome e código de alarme:** digite o nome e o código do evento.

» **Passo 4:** configure a prioridade, quando o evento pode ser acionado e outras informações.

Parâmetro	Descrição
Prioridade	O nível de prioridade é usado para saber rapidamente a urgência do evento quando ele é acionado.
Modelo de Hora	Selecione um modelo de horário para quando o evento pode ser acionado.
Modelo de Feriado	Selecione um modelo de feriado para quando o evento não será acionado. Para criar um novo modelo, siga as etapas abaixo. 2. Na caixa suspensa, clique em *Criar Modelo de Feriado Personalizado.* 3. Digite um nome para o feriado 4. Clique em *Adicionar* em seguida, adicione um ponto e ajuste a hora. Você pode adicionar até 50 períodos. 5. (Opcional) Se houver outros modelos de feriado, você pode selecionar Copiar de, e em seguida sele- cionar um modelo para copiar seus períodos. 6. Clique em *OK.*
Etiqueta/Tag	Insira algum conteúdo usado para filtrar uma grande quantidade de eventos.

» **Passo 5:** configurar ações de vinculação de alarme.

Para vincular vídeo, habilite *Ação vinculada* > *Vincular vídeo* e configure os parâmetros.

Parâmetro	Descrição
Câmera	» Origem do evento: a câmera do alarme em si é ligada quando o alarme ocorre » Câmera acoplada: se o canal estiver vinculado a um ou mais canais de vídeo, você poderá visualizar os vídeos em tempo real do canal vinculado quando um alarme for acionado. » Selecionar Câmera: selecione uma câmera para que você possa visualizar o vídeo da câmera quando o alarme associado for acionado.
Quando um alarme é acionado, exiba a visualização ao vivo da câmera no client	Habilite esse parâmetro, em seguida a plataforma abrirá o vídeo em tempo real do canal onde um alarme é acionado e o reproduzirá no tipo de fluxo definido. Depois que o evento for configurado, selecione *Configurações Locais* > *alarme ative Ligação de Alarme Aberta.*
Gravação de eventos	A plataforma gravará vídeos quando um alarme for acionado. Ele será salvo no disco de vídeo da plataforms
Tipo de fluxo	Defina o tipo de fluxo do vídeo gravado. Se você selecionar o fluxo principal, o vídeo gravado terá uma qualidade superior ao subfluxo, mas requer mais armazenamento.
Tempo de gravação	A duração do vídeo gravado.
Tempo de pré-gravação	Quando há um vídeo gravado que é armazenado no dispositivo ou plataforma antes que o alarme seja acionado, a plataforma terá a duração definida desse vídeo, em seguida, adicionará ao vídeo alarme. Por exemplo quando o tempo de pré-gravação é definido como 10 s a plataforma adicionará 10 s de vídeo antes que o alarme seja acionado para o vídeo do alarme. Se o vídeo de alarme estiver armazenado no dispositivo, recomendamos que você configure um plano de gravação para garantir que haja conteúdo pré-gravado para adicionar ao vídeo de alarme. Se o alarme for armazenado na plataforma, a plataforma gravará vídeos e usará uma determinada de largura de banda continuamente. Esse parâmetro não é aplicado aos alarmes das vagas do estacionamento.

Para ativar o instantâneo, habilite o *Ativar Instantâneo.* A plataforma captura 2 instantâneos, e salva eles no disco de imagem.

Selecione o Canal de vídeo, e então ele pegará instantâneos quando o alarme for acionado.

» Para vincular uma ação *PTZ,* clique em *Vincular PTZ* e selecione os canais e predefinições PTZ e serem vinculados.

» Clique em *Saída de alarme,* selecione um canal de saída de alarme e defina a duração. O canal enviará sinal de alarme quando for acionado.

» Para vincular áudio e luz, clique em *Vincular áudio e luz,* selecione os canais de áudio e luz e selecione a duração da ação.

» Clique em *Vincular Dispositivo de Controle de Acesso,* selecione canais de porta e selecione uma ação vinculada. Quando um alarme é acionado, os canais da porta que você selecionou serão bloqueados, destrancados, normalmente abertos ou normalmente fechados.

» Exiba o vídeo ao vivo de canais especificados em uma parede de vídeo quando os alarmes forem acionados. Clique em *Vincular Parede de Vídeo* e em seguida, selecione os canais e o mural de vídeo.

Se você selecionar Câmera, para selecionar Câmera, poderá configurar quais canais serão exibidos na parede de vídeo especificada. Quando a parede de vídeo selecionada é configurada com o modo de substituição, você também pode selecionar Personalizar janela de alarme e, em seguida selecione quais canais serão exibidos nas janelas especificadas da parede de vídeo.

» Para executar uma HTTP URL, clique em *Vincular Comando de HTTP URL*. Clique em adicionar e configure seu método de solicitação, HTTP URL e observações. Você pode clicar para testar se o comando é válido.

» Para vincular e-mail, habilite E-mail e clique para adicionar o endereço de e-mail, e em seguida um e-mail será enviado para o endereço de e-mail selecionado quando um alarme for acionado. Você também pode inserir manualmente um endereço de e-mail, mas deve pressionar Enter para torná-lo valido. Para configurar o modelo de e-mail, selecione *Adicionar modelo de e-mail na lista suspensa Modelo de e-mail.*

Ou você pode clicar em adicionar modelo de protocolo para criar um novo protocolo.

» **Passo 6:** selecione um ou mais usuários que receberão a notificação quando um alarme for acionado. Os usuários só receberão notificações quando estiverem conectados.

» **Passo 7:** clique *OK.*

Configurando Eventos Combinados

Configure a relação entre o tempo de disparo de 2 evento e em seguida você pode configurar quais ações executar quando o evento for acionado.

Procedimento:

» **Passo 1:** efetue o login no Defense. Na Página inicial, clique em  e na seção *Configuração do Aplicativo,* selecione *Evento > Regra de Evento Combinada.*

» **Passo 2:** clique  para adicionar uma regra para eventos combinados

» **Passo 3:** insira um nome para a regra e configure os detalhes.

Por exemplo, selecione o evento B e configure o X e o Y para 10 e 50 segundos, respectivamente. Se o evento B ocorrer durante os 10 segundos a 50 segundos após a ocorrência do evento A um evento combinado será acionado e em seguida, a plataforma executará ações vinculadas definidas.

» **Passo 4:** clique em *OK.*

» **Passo 5:** clique em *Adicionar,* e configure os parâmetros do evento combinado.

Parâmetros	Descrição
Nome	Insira um nome para o evento combinado.
Regra	Selecione a regra.
Origem do Evento Combinado	Selecione o evento e a origem do evento para o evento A e B.

» **Passo 6:** clique em *OK.*

Operações Relacionadas:

Configure as ações vinculadas para o evento combinado. Para obter detalhes, consulte a seção anterior.

74.7. Configurando Parâmetros de Alarmes

Se determinados alarmes forem acionados com frequência, você poderá determinar um intervalo durante o qual eles só poderão ser acionados uma vez. Por exemplo, um alarme tripware só pode ser acionado uma vez em 10 segundos.

Procedimento:

- » **Passo 1:** efetue o login no Defense. Na página inicial, clique em  e na seção *Configuração do aplicativo* selecione *Evento > Configuração de alarmes > Configuração de Enxurrada de Alarmes.*
- » **Passo 2:** clique *Adicionar.*
- » **Passo 3:** selecione um evento e então configure o intervalo.
- » **Passo 4:** clique em *OK.*

Configurando Alarme no Vídeo Wall

Quando um alarme é acionado, o vídeo ao vivo de um canal pode ser vinculado a uma janela no Vídeo Wall. A plataforma suporta os modos de substituição e loop.

Pré-requisitos: vídeo Wall precisa ser adicionado primeiramente.

Procedimento:

- » **Passo 1:** efetue o login no Defense. Na Página inicial, clique em  e na seção *Configuração do Aplicativo,* selecione *Evento > Alarme no Video Wall.*
- » **Passo 2:** clique  .
- » **Passo 3:** selecione o modo e configure os parâmetros relacionados.

Parâmetros	Descrição
Alarmes no modo Vídeo Wall	» **Modo de substituição:** quando ocorre um alarme, um vídeo ao vivo é aberto na janela espe- cificada de um Vídeo Wall. Por exemplo, se o vídeo ao vivo do canal 1 for aberto na janela 1, outro alarme será disparado. A plataforma exibirá o vídeo ao vivo do canal 2 na janela 1. » **Modo Loop:** vídeo ao vivo vinculados serão exibidos em janelas de um Vídeo Wall de acordo com a ordem das janelas. Se não houver nenhuma janela disponível, a primeira janela será usada. O número no final do nome de uma janela indica sua ordem. Por exemplo, Janela (2) indica que é a segunda janela.
Duração de Permanência	Em ambos os modos, se nenhum outro alarme for acionado, o vídeo atual será fechado após a duração da estadia. Se um novo alarme for acionado: » No modo de substituição, a duração da estadia do novo vídeo começa a partir do momento em que o alarme é acionado. Ele será exibido na janela após o término da duração da estadia é definida como 30 s. Um alarme é disparado quando o vídeo 1 está reproduzido por 15s. Às 30 horas, o vídeo 1 será fechado e o vídeo 2 será reproduzido. Após 15 s o vídeo 2 será fechado. » No modo de loop, um novo vídeo será exibido imediatamente, mesmo que a duração da estadia do vídeo atual não termine.
O vídeo de alarme mais recente substituirá imediatamente o que está sendo reproduzido no Vídeo Wall.	Esse parâmetro só está disponível para o modo de substituição. Depois de habilitada, a duração da estadia não funcionará e novos vídeos serão exibidos imediatamente

» **Passo 4:** configure o tamanho, o local e outros parâmetros de uma janela.

Parâmetros	Descrição
Definir o número de janelas	Há apenas 1 janela por padrão. Clique nele em seguida você pode definir o número de janelas para 4, 9, 16, 32 ou 64
Redimensionar uma janela	» Clique em uma janela e arraste seu quadro para perto do canto inferior direito para redimensioná-lo.  » Clique com o botão direito do mouse em uma janela e selecione Propriedades. Configure a margem esquerda, a margem superior, a largura e a altura para redimensionar a janela.
Ajustar a localização das janelas	Arraste as Janelas para ajustar suas localizações. Estas operações não alterará a ordem das janelas. A ordem é usada para determinar qual janela será usada para exibir vídeos primeiro no modo de loop. O número final do nome de uma janela indica sua ordem. Por exemplo, uma janela chamada Janela (2) significa que é a segunda janela.
Alterar os nomes das janelas	» Clique com o botão direito do mouse em uma janela e selecione Renomear para renomear uma janela. » Clique com o botão direito do mouse em uma janela selecione Propriedades e renomeie em Nome da janela

» **Passo 5:** clique em *OK*.

Configurando a pré-gravação de vídeo de alarme

Você pode configurar o modo de pré-gravação de um dispositivo. Quando um alarme é configurado para vincular a pré-gravação de um dispositivo, o dispositivo aplicará o modo que você especificou.

Informações Básicas:

Os modos de pré-gravação incluem Cache da plataforma e Obter do dispositivo.

» **Cache da plataforma:** os vídeos de alarme serão armazenados na plataforma, a plataforma gravará vídeos e ocupará determinada largura de banda de entrada continuamente.

» **Obter do dispositivo:** os vídeos de alarme serão armazenados no dispositivo. Recomendamos que você faça um plano de gravação de 24 horas para garantir que haja conteúdo pré-gravado para o momento dos alarmes.

Procedimento:

» **Passo 1:** efetue o login no Defense. Na Página inicial, clique em e na seção *Configuração do Aplicativo,* selecione *Evento > Configuração de alarme > Configuração de Enxurrada de alarmes.*

» **Passo 2:** clique em uma organização e em seguida, todos os dispositivos e canais nessa organização serão exibidos à direita

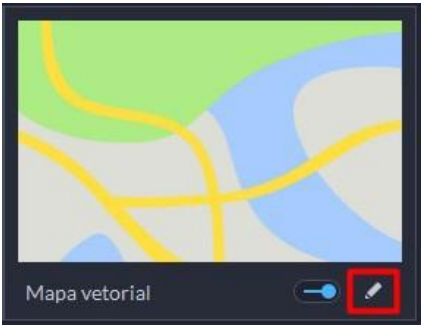
» **Passo 3:** configure o modo de pré-gravação.

» Clique em um canal, selecione um modo e clique em *OK.*

» Selecione vários canais, clique em Editar, selecione um modo e, em seguida clique em *OK.*

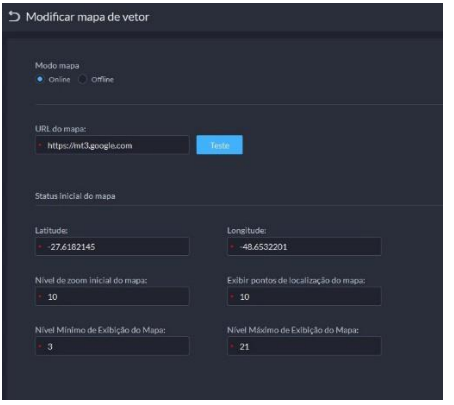
4.5. Configuração de Mapa

Por padrão, o Defense IA tem configurado em seu ambiente o mapa vetorial da Google Maps, este se encontra em Mapa , nas configurações. Caso queira utilizar outro mapa vetorial, você pode editá-lo clicando no ícone de edição do mapa vetorial como mostra a imagem abaixo:



14.1. 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

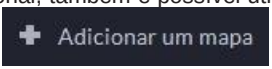
Caso selecione o modo online, insira neste campo a URL do mapa vetorial, o endereço no qual a plataforma se conectará ao mapa.

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

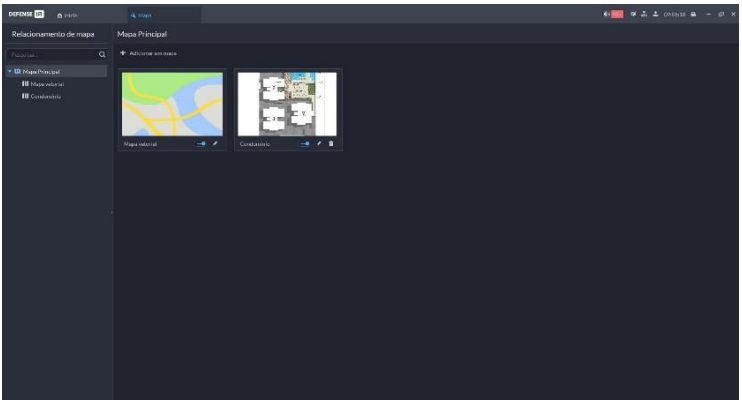
Status inicial do mapa

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

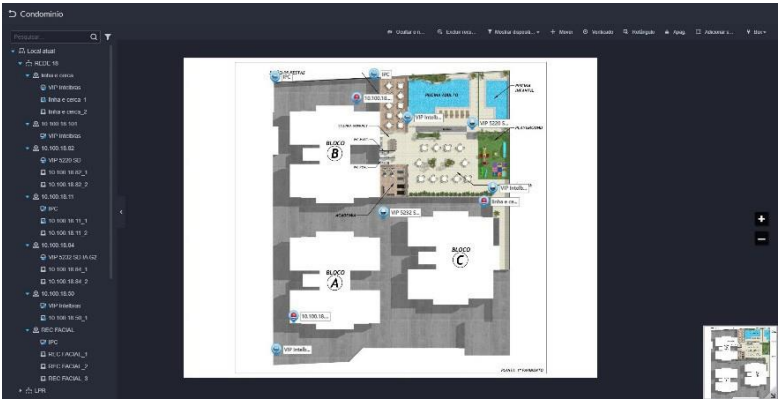
Mapas personalizados

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

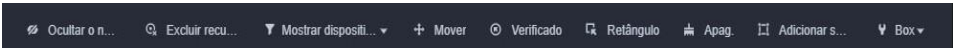
para enviar a imagem (suporta formatos de imagem JPEG/JPG e PNG). O mapa adicionado aparecerá como um mapa principal.



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.

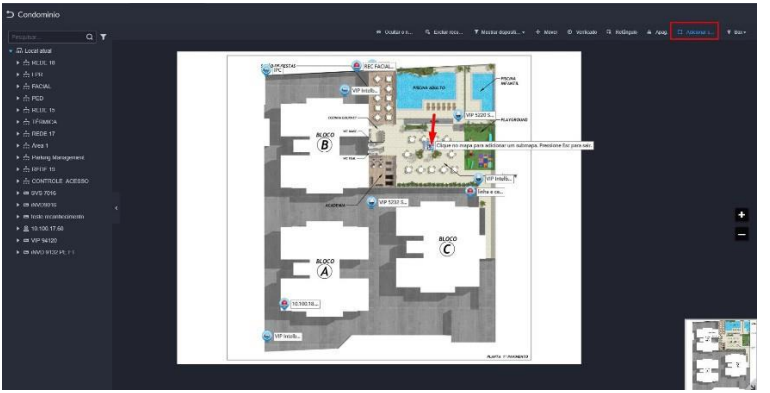
» Adiciona um submapa como elemento no mapa.

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

» Redefine a visualização do mapa para encaixar na tela.

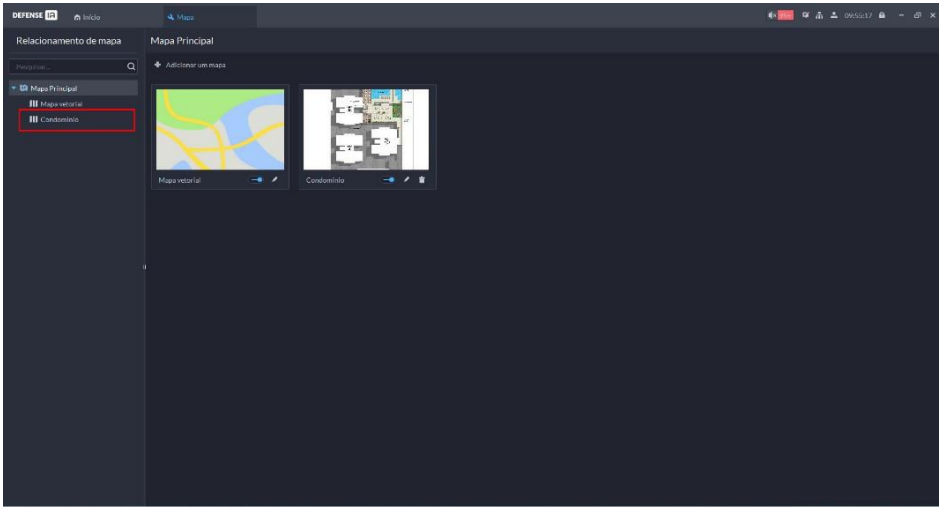
Submapas

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.

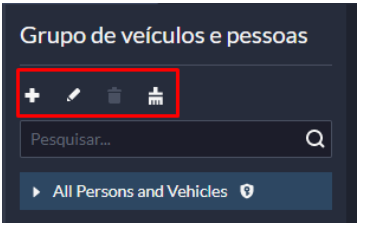
4.6. Configuração de Pessoas e Veículos

No Defense IA, você pode registrar pessoas e veículos para integração de inteligências a um banco 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.

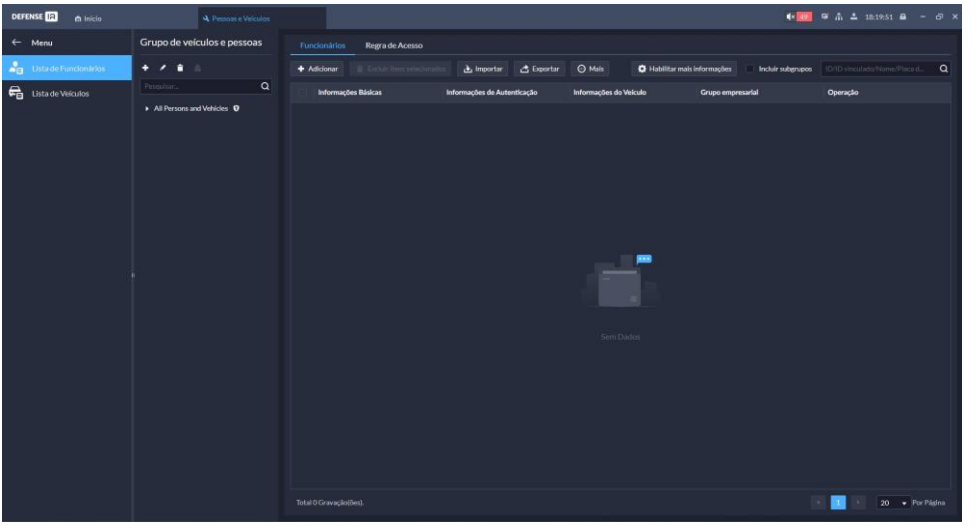
Essas funcionalidades podem ser encontradas no menu de configurações de Pessoas e Veículos.

14.1. 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 módulos do programa, é possível criar hierarquias entre os grupos criados.

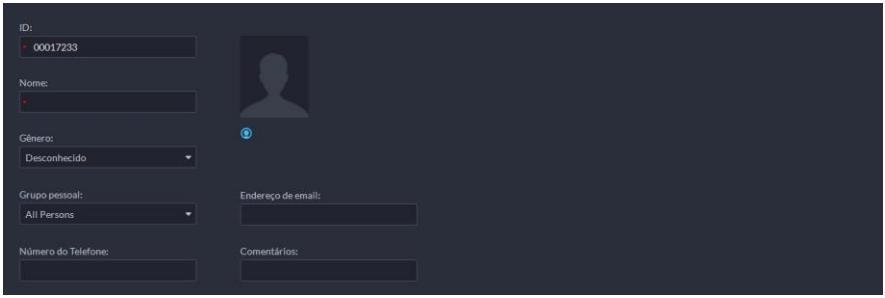


Existem dois métodos gerais para cadastrar pessoas na plataforma. Diretamente pelo módulo, preenchendo informações manualmente, ou a partir da importação de dados, seja de dispositivos compatíveis, ou uma planilha modelo preenchida. No capítulo *Gerenciamento de dados* a importação de dados para plataforma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



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

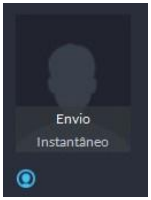
Informações Básicas



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

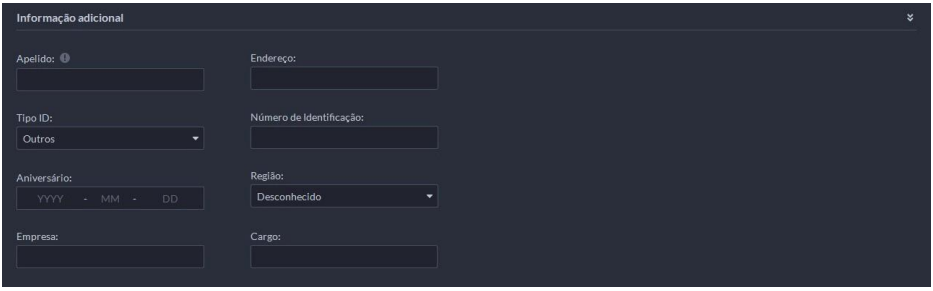
O ID é um Código único identificador da pessoa no sistema. O Defense IA gera um ID aleatório não existente. É possível alterar este campo.

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



Informações Adicionais

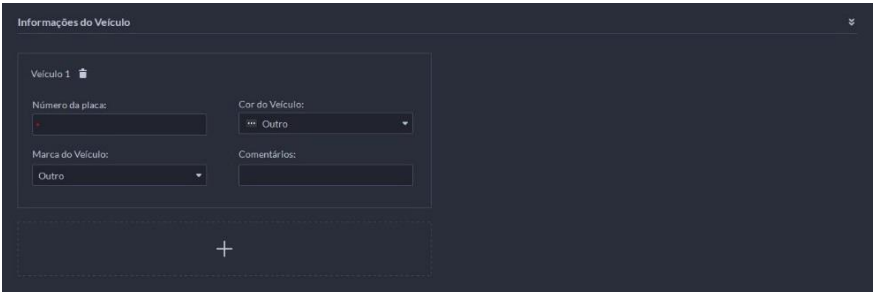
É possível adicionar informações adicionais ao cadastro. Expandindo a aba de informações adicionais, campos extras para preenchimento aparecem, como Apelido, Endereço, Documento de identificação, data de nascimento, naturalidade, empresa e cargo. Outras informações adicionais podem ser configuradas na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



Informações do proprietário

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

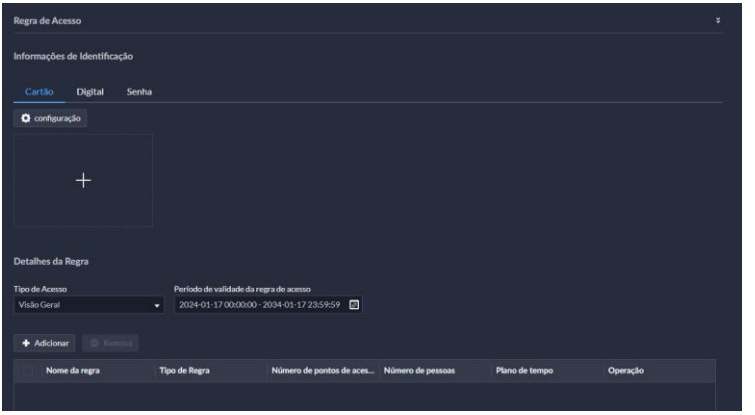


Para vincular um veículo à pessoa cadastrada, clique em "+" na aba Informações do Veículo. Preencha as informações como:

- **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



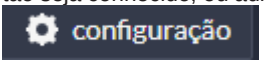
Em *Regra de Acesso,* você pode inserir métodos de autenticação da pessoa cadastrada, tais métodos poderão ser usados para acesso a dispositivos de controle de acesso presentes no sistema (veja em Controle de acesso mais detalhes de como cadastrar regras de acesso).

Os métodos de autenticação são:

Cartão

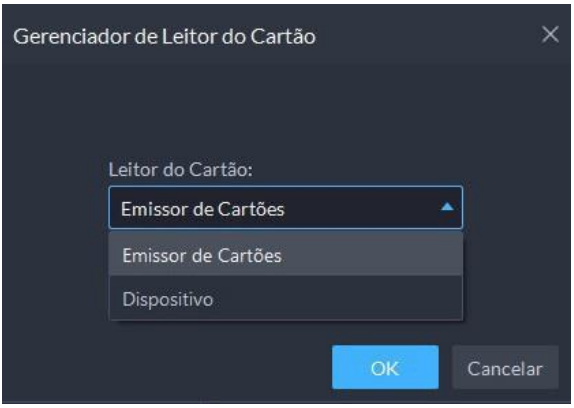
Uma pessoa cadastrada pode possuir até 5 cartões, um deles deve ser o principal. O cartão deve apresentar um código hexadecimal de 8 à 16 dígitos.

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



.

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.

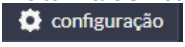
» **Cartão de coação:** selecione este ícone para definir o cartão como cartão de coação. Cartão de coação emite um evento de coação quando passado numa leitora conectada ao Defense IA (o evento deve ser devidamente configurado para notificar a plataforma, veja em Eventos como configurar um evento).

» **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 

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

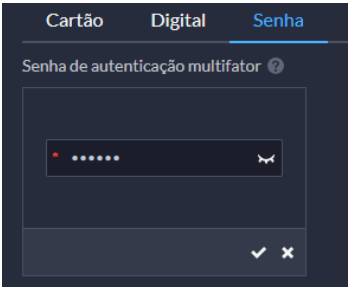
» **Digital de coação:** selecione este ícone para definir a impressão digital como digital de coação. Digital de coação emite um evento de coação quando passada numa leitora conectada ao Defense IA (o evento deve ser devidamente configurado para notificar a plataforma, veja em Even- tos como configurar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

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

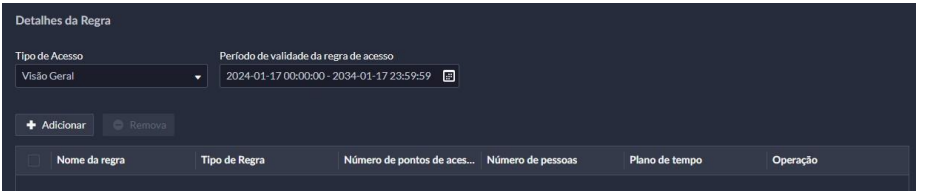
» **Excluir impressão digital:** selecione este ícone para excluir a digital da plataforma.

Senha de autenticação multifator

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



Detalhes da regra



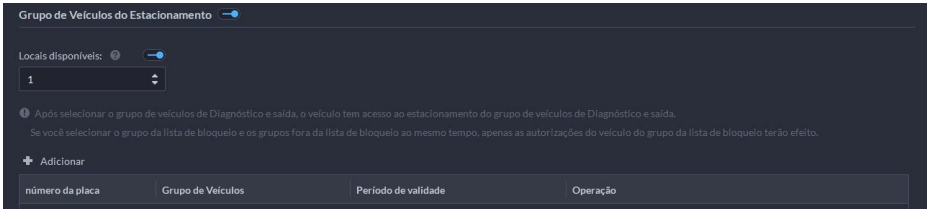
Também é possível vincular um tipo de acesso e um período de validade, que indica o nível de permissão e prazo para vencimento dos métodos de autenticação da pessoa.

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* 

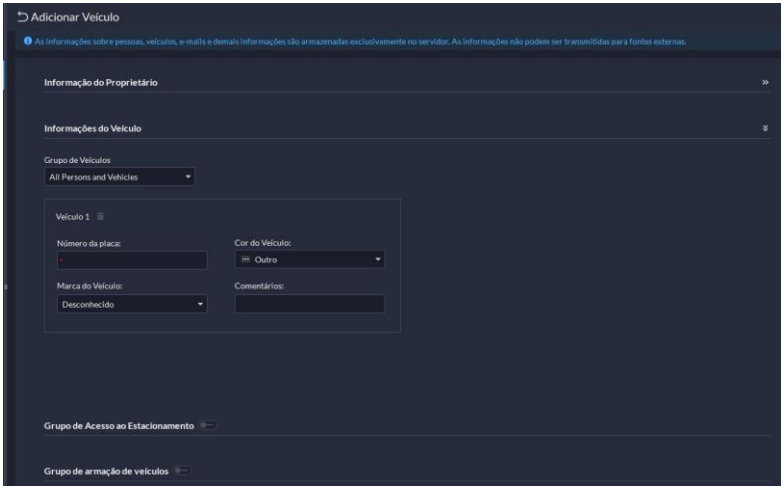
, vincula a pessoa cadastrada e seus veículos a grupos de veí- culos. Veja *Estacionamento* para mais informações sobre como gerenciar grupos de veículos.

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.

24.2. Cadastrar veículos

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



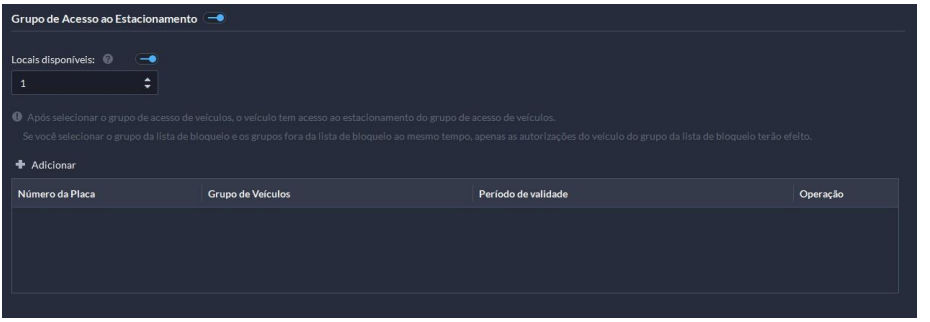
Informação do Proprietário

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 *Estacionamento* 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

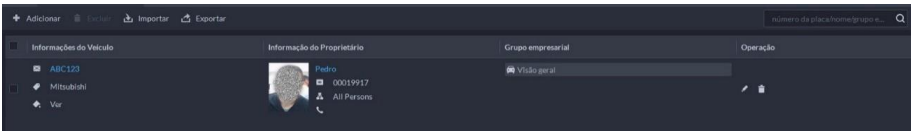
Clicando em *Adicionar* 

, 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  .

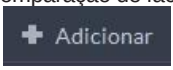
É possível visualizar detalhes do cadastro e editá-lo clicando duas vezes sob o mesmo.



34.3. 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* 

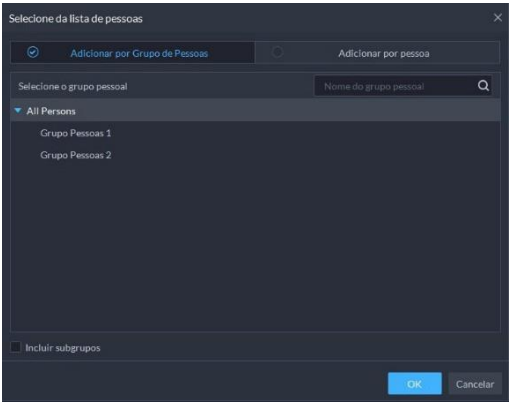
para criar o grupo.

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.

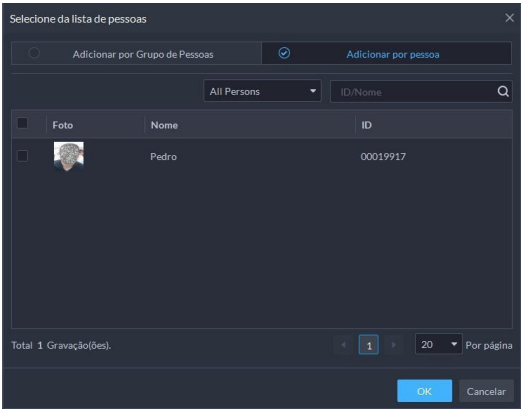
»  Botão para adicionar pessoas ao grupo a partir da lista de pessoas. Existem duas opções.

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



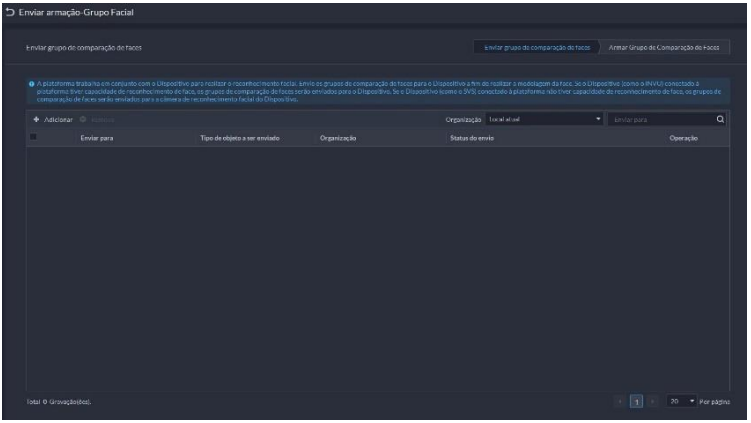
Selecione o grupo de pessoas no qual deseja buscar as pessoas na lista suspensa mostrada abaixo.

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.

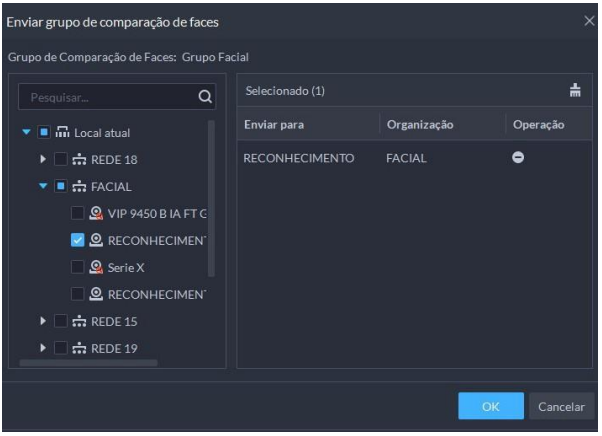
Enviar grupo de comparação e faces

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.



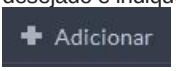
Para enviar o grupo, clique em em *Adicionar* 

e selecione os dispositivos que deseja enviar o grupo.

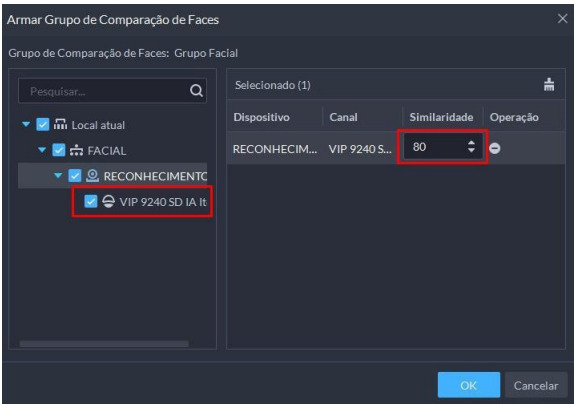


Ao clicar em *OK,* o(s) dispositivo(s) aparecerão na lista, assim como o status do envio do grupo facial para este(s). Clique em *Próxima etapa* no final da página.

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.

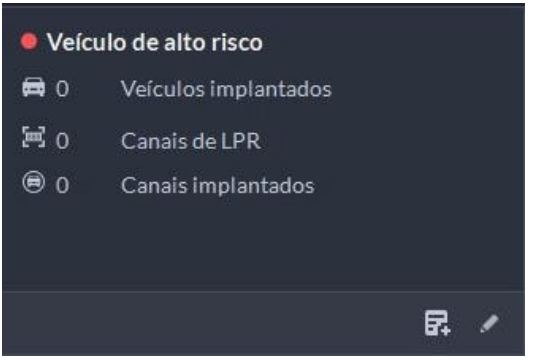
É possível adicionar mais pessoas ao grupo facial após armação e configuração dos canais, o sistema atualiza o envio ao dispositivo automaticamente. Caso o dispositivo esteja indisponível, o ícone  aparecerá, indicando a falha no envio.

»  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 identificação, mas não é possível renomeá-lo.

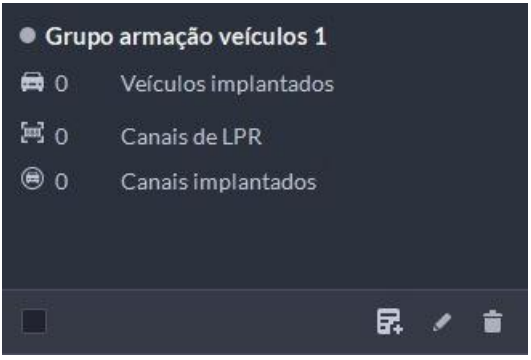


Ao contrário do banco de dados facial, não é necessário enviar o grupo a dispositivos de inteligência, uma vez que estes já identificam e vinculam-se automaticamente a dispositivos LPR cadastrados no sistema.

Clique em *Adicionar* 

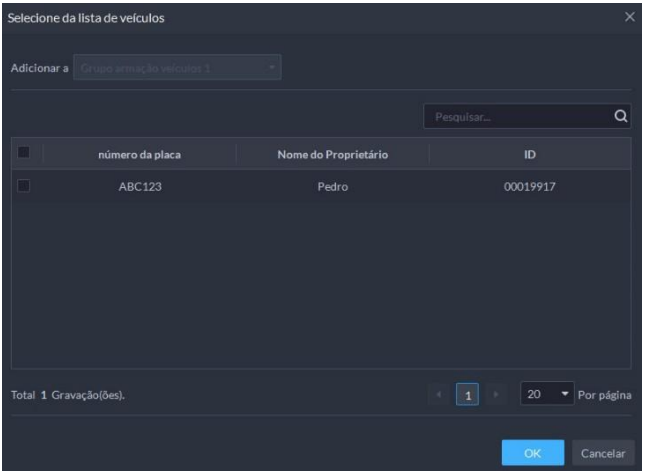
na aba de ferramentas acima na tela para criar um novo grupo de armação de veículos.

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.

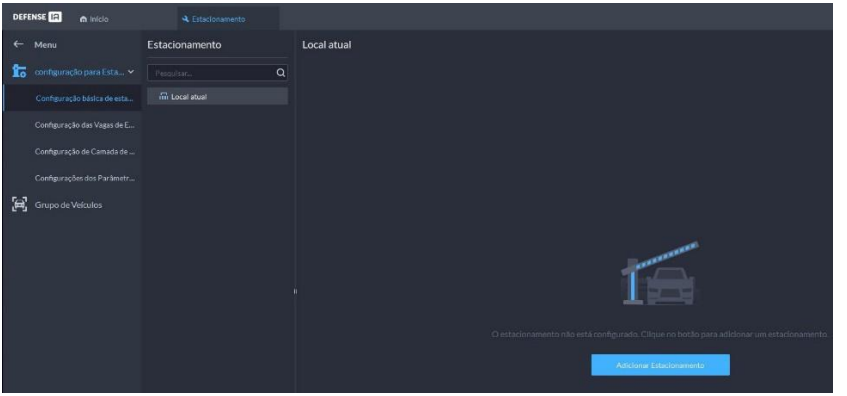
»  Botão para excluir o grupo de armação de veículos.

44.4. Estacionamento

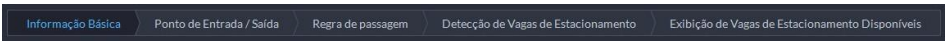
As configurações de estacionamento e grupo de veículos podem ser feitas pelo módulo de configuração de estacionamento.

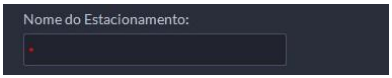
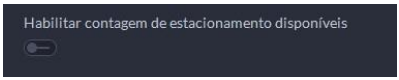
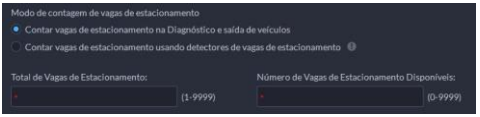
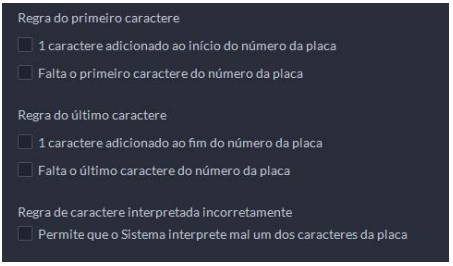
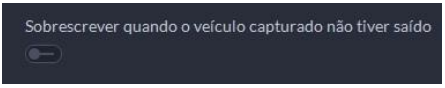
Configuração básica de estacionamento

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

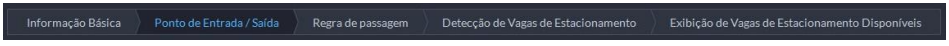


Preencha as infromações básicas do Estacionamento:

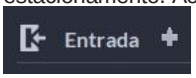


Campo	Descrição
	Insira na caixa o nome que deseja chamar o estacionamento. O asterísco indica campo obrigatório.
	Botão para habilitar contagem de vagas. Quando habilitado apresenta novas opções. Selecione a opção que deseja para contagem de vagas entre Contagem por entrada e saída ou Contagem por detector 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.

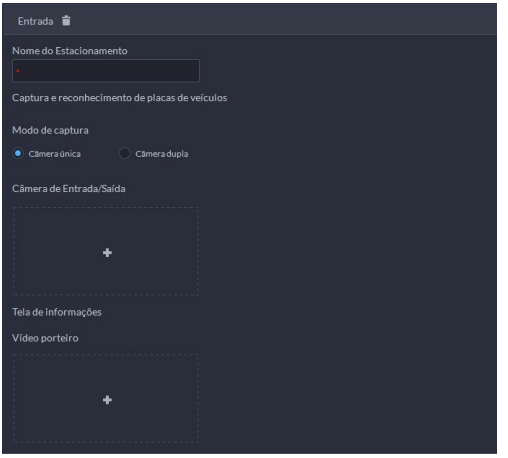
Na próxima etapa, em *Ponto de Entrada/Saída,* adiciona-se os pontos de acesso e dispositivos LPR de acesso do estacionamento.



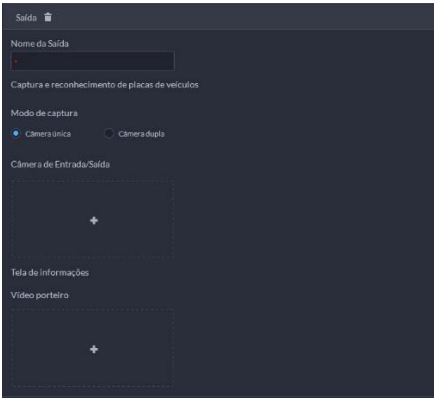
Clique em *Adicionar Ponto de Entrada e Saída* para adicionar um ponto de acesso do estacionamento. Ao nomeá-lo, as entradas e saídas do estacionamento poderão ser adicionadas



.



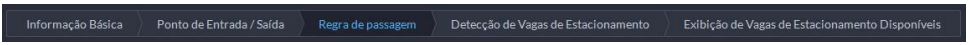
Campo	Descrição
Nome do Estacionamento	Insira na caixa o nome que deseja chamar a entrada do estacionamento. O asterísco indica campo obrigatório.
Modo de captura	Selecione o modo de captura entre câmera única ou câmera dupla. Caso o modo *câmera dupla* seja selecionado, aparecerá espaço para inserir 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.
Vídeoporteiro	Clique em "+" para adicionar dispositivos compatíveis com controle (controladoras de acesso ou Vídeoporteiros) 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.
Vídeoporteiro	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 estacionamento 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.

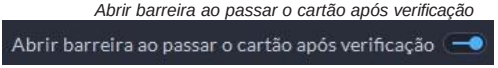
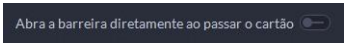
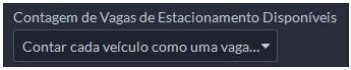
Permitir passagem quando o espaço disponível for 0.

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 estacionamento 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.

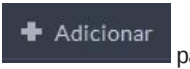
Regra	Descrição
	Quando habilitada, permite acesso de todos os veículos. Permite a seleção de um período para a regra ser válida, assim como filtrar ou não veículos na lista de bloqueio. Ao ativar esta regra, deve-se selecionar para quais grupos permitidos essa regra valerá. Essa regra ativada habilita 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

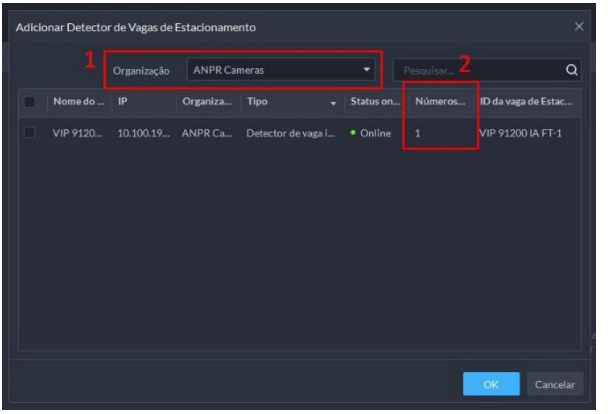
Esta regra habilita o envio de listas de permissão e bloqueio de veículos ao dispositivo de acesso LPR. Caso a plataforma esteja desconectada, o dispositivo fará a gestão de acesso com base em tais listas.

Em Detecção de vagas de estacionamento, na quarta etapa de configuração, dispositivos de detecção 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.

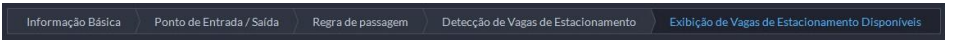
Clique em *Adicionar* 

para selecionar da lista de dispositivos os sensores de vagas.

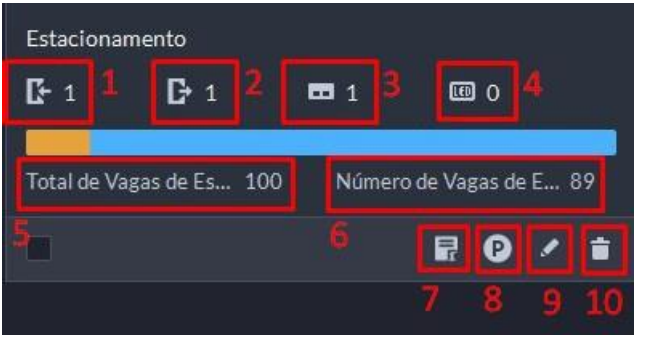


5. Filtre por organização para obter o(s) dispositivo(s) desejado(s).
6. O número de vagas configurado no dispositivo aparece na coluna indicada, este número fará parte da quantidade de vagas do estacionamento.

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



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



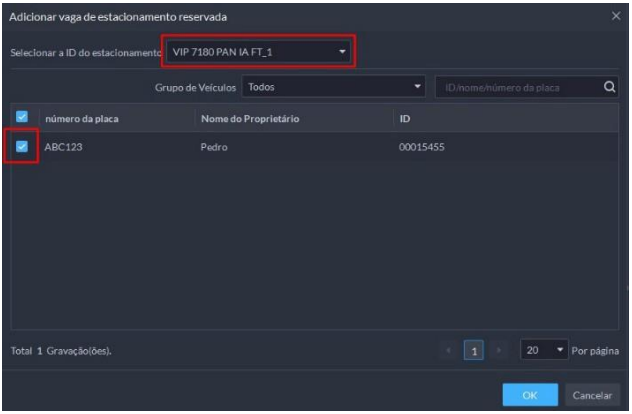
Índice	Descrição
1	Número de entradas no estacionamento
2	Número de saídas no estacionamento
3	Número de sensores de vagas no estacionamento
4	Número de painéis LED de contagem de vagas no estacionamento
5	Tota de vagas existentes no estacionamento
6	Total de vagas disponíveis no estacionamento
7	Edição 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 veículos) 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 esquerda e então clique em *Adicionar* 

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



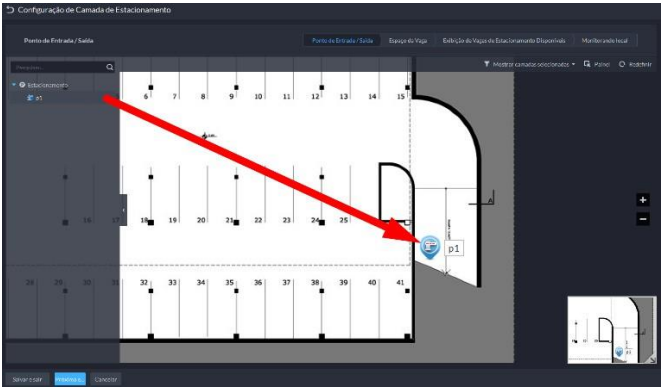
É possível selecionar mais de um veículo por vaga, desta forma, é possível cadastrar um evento para identificar quando veículos sem permissão ocuparem a vaga.

Configuração de camada de estacionamento

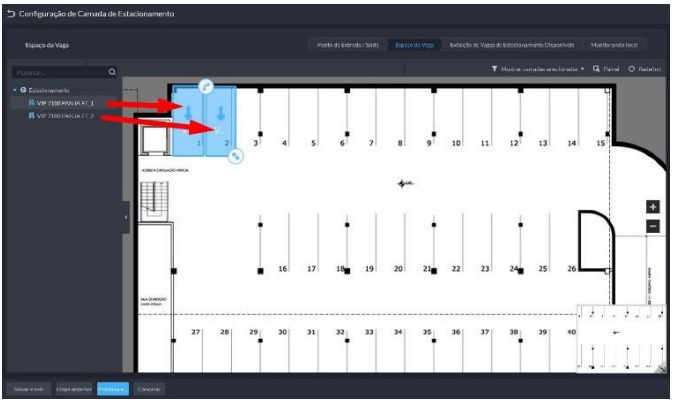
Uma camada de estacionamento é uma imagem que representa o estacionamento, para cadastrar uma, selecione o estacionamento desejado na árvore de estacionamentos à esquerda e então clique em *Adicionar* 

.

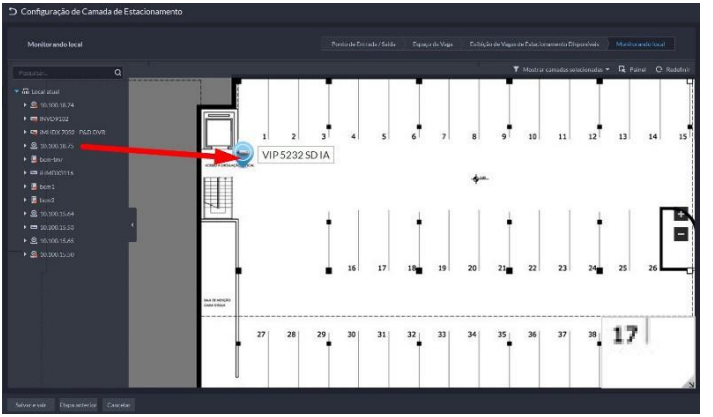
Nomeie e selecione a imagem desejada para prosseguir para configuração. Na primeira etapa, ar- raste para o mapa as entradas e saídas.



Durante a segunda e terceira etapa, arraste as vagas com detectores e os pontos de exibição de vagas 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.



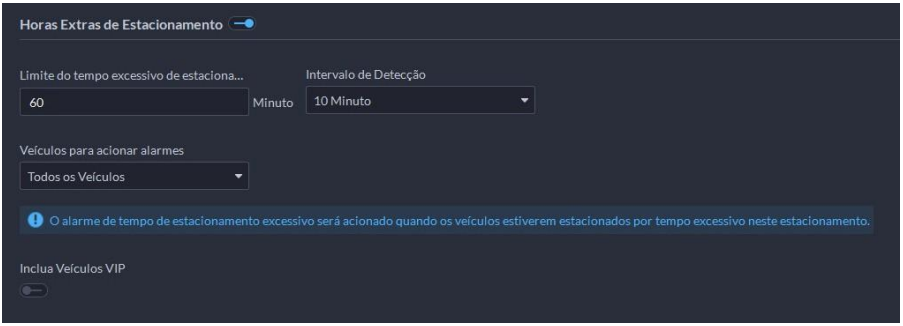
A camada configurada pode ser visualizada no módulo *Estacionamento.*

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.*

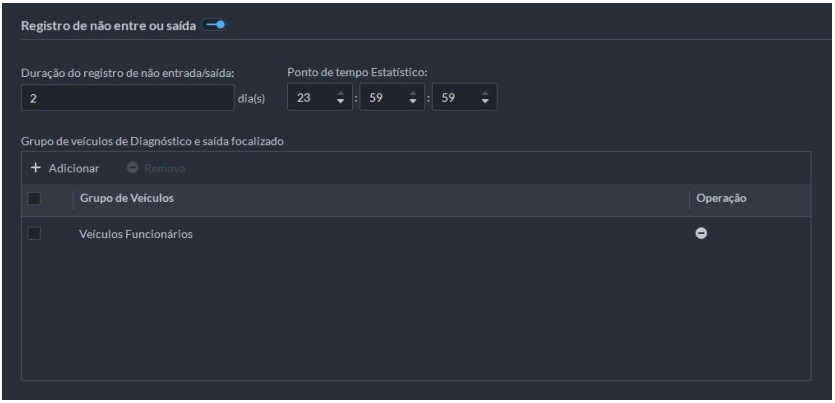
Horas extras de estacionamento



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



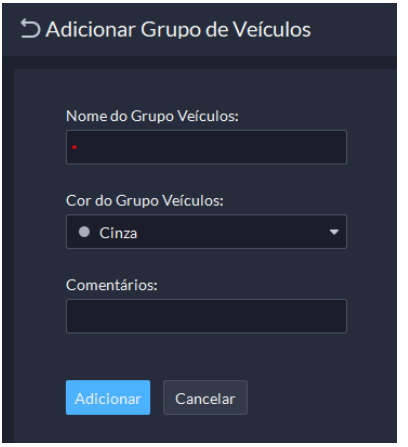
Insira parâmetros como Duração do registro e ponto de tempo estatístico. Caso algum veículo do grupo focalizado não entre ou saia do estacionamento no período definido (quando a duração do registro, em dias, for excedida), o evento será acionado. A plataforma utiliza o ponto de tempo estatístico para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

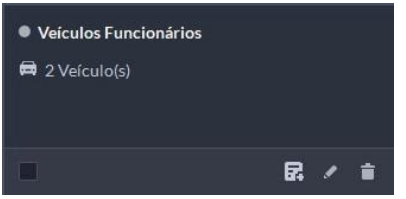
Grupo de veículos

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

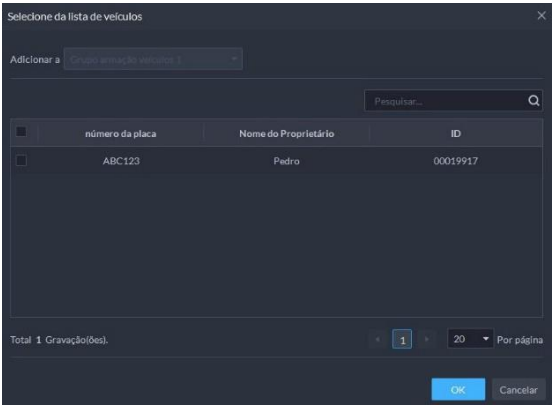
Por padrão, 3 grupos já vêm configurados: Visão geral, VIP e Lista negra. É possível adicionar veículos à tais grupos da Lista de veículos. Para criar um novo grupo, clique em *Adicionar.*



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.

5. Vídeoporteiro

5.1. Preparações

Certifique-se de que foram feitos os seguintes preparativos:

- Os dispositivos de controle de acesso são implantados corretamente. Para obter detalhes, consulte os manuais do usuário correspondentes
- As configurações básicas da plataforma foram concluídas.
  - Ao adicionar dispositivos de Vídeoporteiro na página *Dispositivo,* selecione Vídeoporteiro como a categoria do dispositivo.
  - Ao adicionar dispositivos de controle de acesso que oferecem suporte a interfone, selecione Categoria de dispositivo para Controle de acesso em Informações de login e, em seguida, selecione Terminal de reconhecimento de controle de acesso.
- A plataforma cria automaticamente uma sala depois que você adiciona um VTH.
- Qualquer modificação de configuração no dispositivo não será reportada à plataforma. Você precisa vá para a página de modificação de dispositivo do Web Manager para sincronizar manualmente a modificação.

5.2. Gerenciamento de Chamadas

Criar grupo de chamadas, grupo de gerenciamento e grupo de relações, respectivamente, e defina relações de chamadas restritas. Esta função só está disponível para administradores.

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

15.1. Configurando o grupo de chamadas

Somente dispositivos no mesmo grupo de chamadas podem ligar uns aos outros.

» Um grupo de chamadas será gerado automaticamente depois que você adicionar à plataforma um VTO ou dispositivo de controle de acesso que suporte interfone. Todos os VTHs na mesma unidade também serão adicionados automaticamente ao grupo. 2 VTHs ou um VTH e VTO no grupo podem chamar um ao outro.

» Um grupo de chamadas será gerado automaticamente depois que você adicionar uma segunda estação de confirmação à plataforma. Adicione os VTHs na mesma casa ao grupo, em seguida, a segunda estação de confirmação e os VTHs podem ligar uns aos outros.

Um grupo de chamadas será gerado automaticamente depois que você adicionar uma estação de cerca à plataforma. Todos os VTHs na plataforma serão adicionados automaticamente ao grupo por padrão, então a estação de cerca e os VTHs podem chamar uns aos outros. Você também pode clicar  para editar os VTHs no grupo, para que a estação de cerca só possa chamar determinados VTHs.

» Depois de adicionados à plataforma, os VTHs serão automaticamente adicionados aos grupos correspondentes se estiverem associados a VTOs, segundas estações de confirmação ou estações de cerca, para que possam ligar uns aos outros.

25.2. Adicionando Grupo de Gerentes

Divida os administradores em grupos diferentes e vincule-os a grupos de chamadas em combinações diferentes. Isso é útil quando determinados administradores só podem atender chamadas de determinados dispositivos. Os administradores incluem VTS e usuários com permissões para usar a função de Vídeoporteiro e operar os dispositivos. O VTS será adicionado automaticamente ao grupo de gerenciadores padrões após a adição.

Procedimento:

» **Passo 1:** faça o login no Defense. Clique na *Página Inicial,* clique  , e em seguida, na *Configuração do aplicativo,* selecione *Vídeoporteiro.*

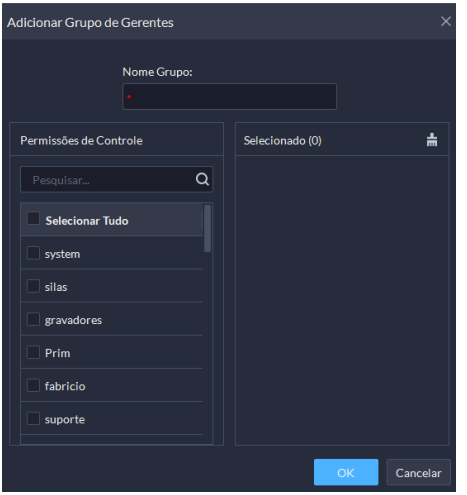
» **Passo 2:** clique  .

» **Passo 3:** clique em *Configuração do Grupo de Gerenciamento.*

» **Passo 4:** clique *Adicionar Grupo.*

» **Passo 5:** insira o nome do grupo, selecione a conta de administrador ou VTS e clique em *OK.*

O grupo de gerenciamento adicionado é exibido na lista.



35.3. Configurando o grupo de Relações

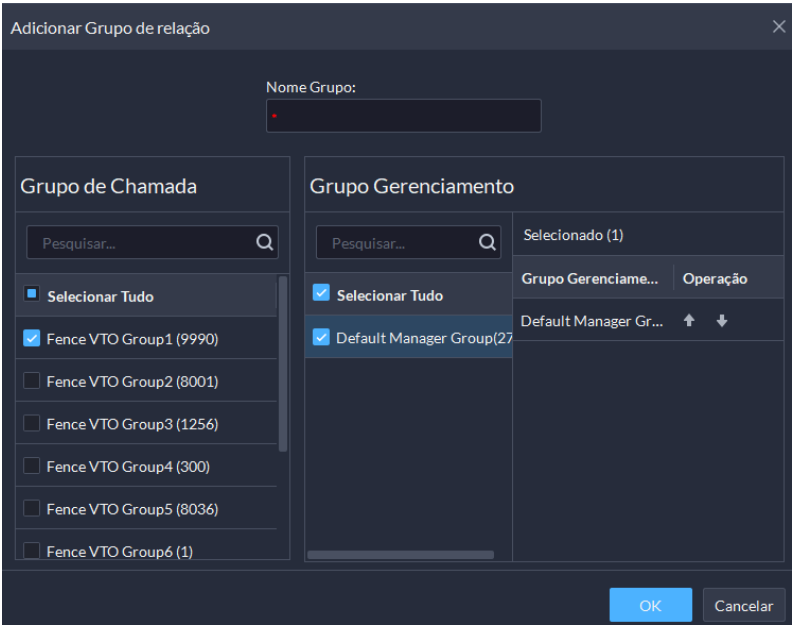
Vincular grupos de chamadas e grupos de gerentes, e VTOs ou VTHs em um grupo de chamadas só podem chamar administradores ou VTSs de um grupo de gerentes vinculado. Existem 2 tipos de relações:

- Um grupo de chamadas vincula a 1 grupo de gerentes. Todos os administradores online no grupo de gerentes receberão a chamada quando qualquer dispositivo estiver chamando. Se um administrador responder, ele deixará de tocar para outros administradores. A chamada só será rejeitada se todos os administradores a rejeitarem.
- Um grupo de chamadas vincula a vários grupos de gerentes.

As prioridades variam para diferentes grupos de gestores. Quando qualquer dispositivo estiver chamando, todos os administradores online no grupo de gerentes com a prioridade mais alta receberão a chamada primeiro. Se ninguém atender por 30 segundos, a chamada será encaminhada para o grupo de gerentes com a segunda maior prioridade. Se ainda assim ninguém atender, o dispositivo avisará que não há resposta para a chamada.

Procedimento:

- **Passo 1:** faça o login no Defense. Clique na Página Inicial, clique  , e em seguida, na Configuração do aplicativo, selecione Vídeoporteiro.
- **Passo 2:** clique  .
- **Passo 3:** clique *Configurações da Relação de Grupo.*
- **Passo 4:** clique *Adicionar.*
- **Passo 5:** insira o nome do grupo e selecione um ou mais grupos de chamadas e grupos de gerentes.



Como apenas até 2 grupos de gerentes receberão uma chamada, recomendamos que você selecione no máximo 2 grupos de gerentes.

- **Passo 6:** clique  ou  para ajustar as prioridades do gerenciamento de grupo, e em seguida clique em *OK*.

  Os gerentes superiores têm prioridades maiores.

5.3. Configurando o modo de construção/unidade e chamada

Verifique se o status do prédio e da unidade do cliente DSS é o mesmo do VTO. Se o edifício e a unidade estiverem habilitados na plataforma, eles também devem estar habilitados no dispositivo, e vice-versa; caso contrário, o VTO ficará offline depois de adicionado. Isso também afeta a regra de discagem.

- Se o edifício estiver habilitado enquanto a unidade não estiver, o número da sala será *1#1001.*
- Se o edifício estiver habilitado e a unidade também estiver habilitada, o número da sala será *1#2#1001.*
- Se o edifício não estiver habilitado e a unidade também não estiver habilitada, o número da sala será *1001.*

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

Procedimento:

- **Passo 1:** faça login no Defense. Na Página inicial, clique em  e em seguida, na seção de Configuração de Aplicativo, selecione Vídeoporteiro.
- **Passo 2:** clique  .
- **Passo 3:** habilite ou Desabilite o edifício e a unidade conforme necessário e clique em *OK.*

  Essa configuração deve ser a mesma que as configurações do dispositivo. Caso contrário, as informações dos dispositivos podem estar incorretas. Por exemplo, se apenas a Criação estiver habilitada em um VTO, você deverá habilitar somente a Criação na plataforma.
- **Passo 4:** configure o modo de chamada.
  - **Chamada Simultânea:** quando um quarto está sendo chamado, todos os VTHs e usuário de aplicativo irão receber a chamada.
  - **Chamada em Grupo:** ao ligar para uma sala, apenas o VTHs nela receberá a chamada. Se o encaminhamento de chamadas estiver habilitado nos VTHs, todos os usuários do aplicativo receberão a chamada.
- **Passo 5:** clique em *Salvar.*

5.4. Configurando uma Sala

Adicione uma sala para incluir os VTHs e os usuários do aplicativo nela

15.1. Informações Básicas

Quando você adiciona um VTH à plataforma, a plataforma cria automaticamente uma sala. Você também pode criar uma sala e adicionar o VTH mais tarde. O VTH ingressará automaticamente na sala correspondente. As salas criadas automaticamente não podem ser excluídas. Você só pode excluir aqueles que são criados manualmente.

Procedimento:

- **Passo 1:** faça login no Defense. Na Página inicial, clique em  e em seguida, na seção de *Configuração de Aplicativo,* selecione *Vídeoporteiro > Configuração da Sala.*
- **Passo 2:** clique em *Adicionar.*
- **Passo 3:** selecione uma organização, insira um nome para a sala e o número da sala e clique em **Adicionar.**

Se o VTH com o mesmo número de quarto tiver sido adicionado à plataforma, ou o proprietário com o mesmo número de quarto tiver se registrado, o VTH ou o usuário do aplicativo ingressará no quarto automaticamente.

25.2. Operações Relacionadas

Operações nos usuários do aplicativo:

»  : defina um usuário do aplicativo para ser o proprietário da casa depois que ele for vinculado a uma pessoa.

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

»  : vincular um usuário do aplicativo a uma pessoa.

»  : excluir um usuário do aplicativo.

5.5. Sincronizando contatos

Sincronize as informações de contatos com o VTO e, em seguida, você pode exibir os contatos no VTO ou em sua página da Web.

Procedimento:

» **Passo 1:** faça login no Defense. Na Página inicial, clique em  e em seguida, na seção de *Configuração de Aplicativo,* selecione Vídeoporteiro.

» **Passo 2:** clique em  .

» **Passo 3:** selecione um nó da organização (VTO) e clique em *Enviar contatos.*

» **Passo 4:** selecione um ou mais VTHs conforme necessário e clique em *OK.*

Agora você pode ver os contatos no VTO ou na página da Web. Se os contatos não forem enviados, os motivos serão fornecidos.

5.6. Definindo senha privada

Defina as senhas da porta da sala para que a porta da sala possa ser aberta digitando a senha na VTO (estação externa).

Certifique-se de que os contatos sejam enviados para o VTO; caso contrário, você não pode definir senha privada.

Procedimento:

» **Passo 1:** faça login no Defense. Na Página inicial, clique em  e em seguida, na seção de *Configuração de Aplicativo,* selecione Vídeoporteiro.

» **Passo 2:** clique em  .

» **Passo 3:** selecione um VTO e, em seguida, você pode ver todos os VTHs vinculados a este VTO.

» **Passo 4:** selecione um VTH e clique em  , ou selecione vários VTHs e clique em *Alterar senha.*

» **Passo 5:** digite a senha e clique em *OK.*

Você pode usar a nova senha para desbloquear no VTO.

O formato deve ser número do quarto + senha privada, e o número do quarto consiste em 6 dígitos. Por exemplo, uma pessoa que mora em 1001 com a senha privada do VTO no prédio sendo *123456,* pode entrar *001001123456* para destrancar a porta.

5.7. QR Codes

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

Procedimento:

» **Passo 1:** faça login no Defense. Na Página inicial, clique em  e em seguida, na seção de *Configuração de Aplicativo,* selecione *Vídeoporteiro > QR Codes.*

» **Passo 2:** insira um nome e algumas anotações para sua comunidade e clique em *Salvar.*

Os proprietários podem escanear o QR Code para download do aplicativo para baixar e instalar o aplicativo no telefone e, em seguida, digitalizar o QR Code para registro do aplicativo para se registrar. Para saber como se cadastrar, consulte o manual do usuário do App.

5.8. Usuário de Aplicativo

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

15.1. Pré-requisitos

Os usuários do aplicativo se cadastraram escaneando o código QR na plataforma ou no VTH. Para obter detalhes, consulte o manual do usuário do aplicativo.

Pré-requisitos:

» **Passo 1:** faça login no Defense. Na Página inicial, clique em  e em seguida, na seção de *Configuração de Aplicativo,* selecione *Vídeoporteiro.*

» **Passo 2:** clique  .

Operações	Descrição
Congelar usuário do Aplicativo	O usuário do aplicativo não pode fazer login por 600 s depois de ser congelado. A conta será congelada quando tentativas de senha inválidas excederem 5 por um usuário do aplicativo
Alterar senha de login de usuário do aplicativo	Clique e introduza uma nova senha na página *Reset de Senha* e, em seguida, clique em *OK.* » A senha deve ter de 8 a 16 caracteres e incluir números e letras. » Clique  para exibir a senha ou  para mascarar a senha.
Atualizar lista de usuários do Aplicativo	Clique em *Atualizar* para exibir os usuários do aplicativo que se registraram recentemente.
Apagar Usuário do Aplicativo	Clique  para excluir usuários do aplicativo, um por um, ou selecione vários usuários do aplicativo, clique em *Excluir* e siga as instruções para excluir os usuários.

6. Análise Inteligente

Antes de usar as funções de contagem de pessoas e relatórios programados, você deve primeiro configurá-las.

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

» **Relatório programado:** 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.

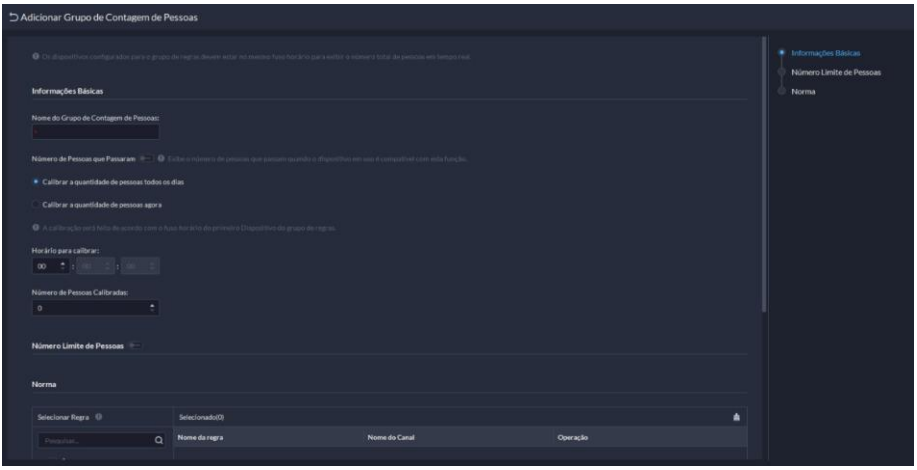
6.1. Grupo de contagem de pessoas

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 histórico e em tempo real de pessoas do grupo.

Procedimento:

» **Passo 1:** faça login na Defense. Na página inicial, clique em  , na seção *Configuração do aplicativo,* selecione *Análise inteligente* > *Configuração do grupo de contagem de pessoas.*

» **Passo 2:** clique em *Adicionar* no canto superior esquerdo.

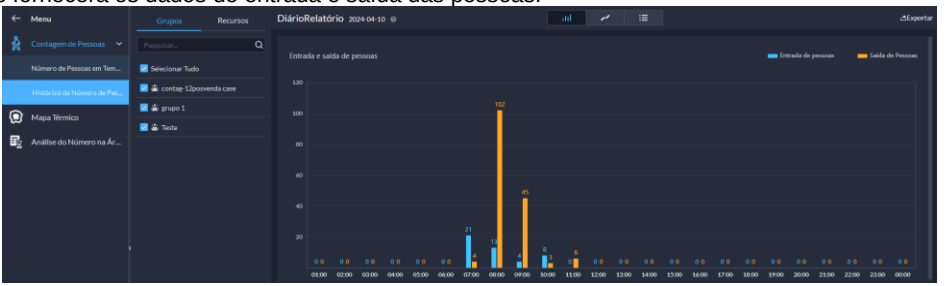


» **Passo 3:** configure os parâmetros e clique em *Adicionar.*

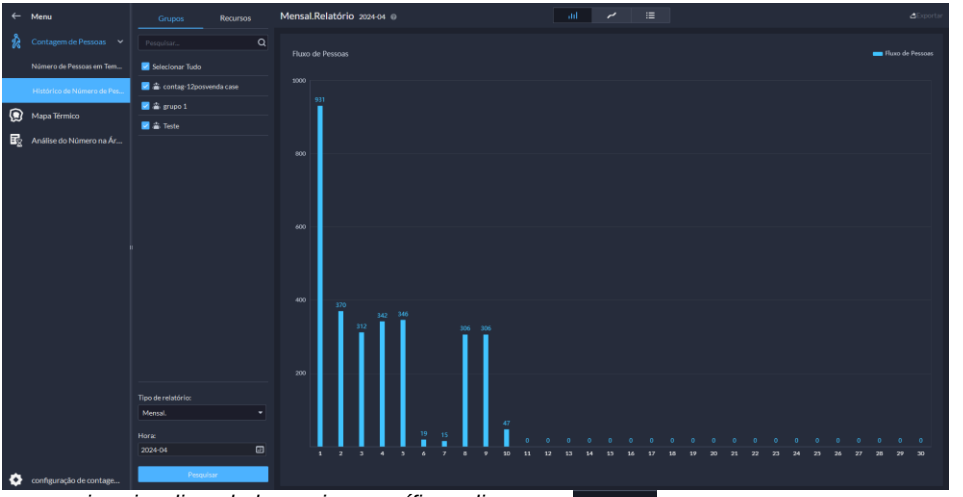
Parâmetro	Descrição
Nome do grupo de contagem de pessoas	Nome do grupo de contagem de pessoas.
Número de passagem. Calibrar o número de pessoas que ficam todos os dias. Tempo de calibração. Número calibrado de pessoas.	Tempo de calibração só pode ser configurado por hora. É o início de um ciclo de contagem. » O número de pessoas que ficarão todos os dias será definido para o valor definido todos os dias no horário de calibração. » Depois que o Número de passagem for ativado, o número de pessoas que passam será exibido. O valor será definido como 0 todos os dias no horário de calibração por padrão.
Calibrar o número de pessoas que ficarão agora. Número calibrado de pessoas.	O número de pessoas hospedadas será definido para o valor definido após a adição deste grupo. O valor não será calibrado todos os dias.
Limitar número de pessoas. Limite de luz vermelha. Limite de luz amarela.	» Quando ativado, você pode configurar o limite de luz vermelha e amarela das pessoas do grupo. » Quando o número de pessoas do grupo atingir o valor definido, a luz ficará vermelha. » Quando o número de pessoas no grupo atingir o valor definido, mas for menor que o valor da luz vermelha, a luz ficará amarela.
Regra	Selecione os dispositivos cujas regras de contagem de pessoas você deseja incluir no grupo e, em seguida, seus dados serão combinados.

6.2. Geração do Relatório Fluxo de Pessoas

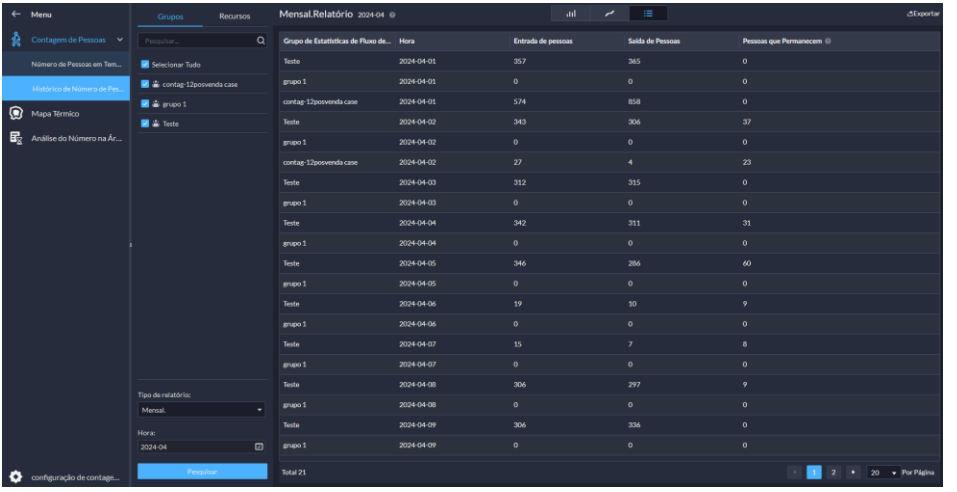
Para gerar o relatório deverá ser selecionado um grupo já criado, ao pesquisar os dados diários ele fornecerá os dados de entrada e saída das pessoas.



Já nos relatórios Semanais, Mensais e Anuais só será possivel visualizar o fluxo de entrada de pessoas.



Caso precise visualizar dados mais específicos clique em. 



6.3. Relatório agendado

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

Procedimento:

» **Passo 1:** faça login no Defense. Na página inicial, clique em  e, na seção *Configuração do aplicativo,* selecione *Análise inteligente* > *Configuração de relatório agendado.*

» **Passo 2:** configure um ou mais tipos de relatório.

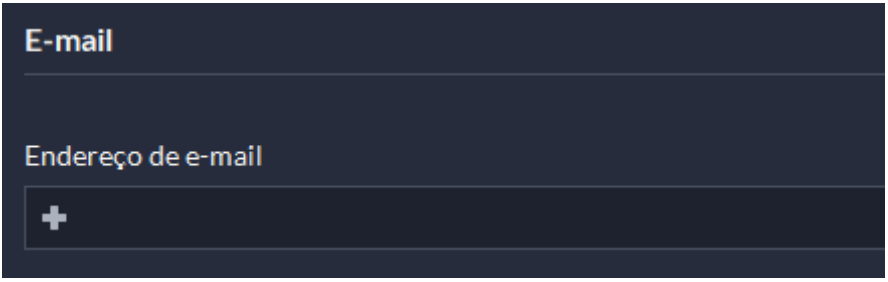
» **Relatório diário:** os dados de ontem serão enviados para seu e-mail em horário definido. Se definido como 03:00:00, os dados do dia anterior (00:00:00–23:59:59) serão enviados para seu e-mail às 03:00:00 todos os dias.

» **Relatório semanal:** os dados da semana passada serão enviados para seu e-mail em horário definido. Se definido para 03:00:00 de quarta-feira, os dados de quarta a terça de cada semana serão enviados para seu e-mail às 03:00:00 de todas as quartas-feiras.

» **Relatório mensal:** os dados do último mês serão enviados para seu e-mail em horário definido. Se definido para 03:00:00 do 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.

» **Passo 3:** configure um ou mais endereços de e-mail para enviar o relatório e o conteúdo do e-mail.

1. Clique para selecionar os usuários que possuem endereços de e-mail configurados ou insira um endereço de e-mail e pressione *Enter.*



2. Configure o conteúdo do e-mail.

» **Passo 4:** envie o relatório.

» Clique em *Enviar agora* para enviar imediatamente o relatório que você configurou.

» Clique em *Salvar* e o relatório será enviado no horário definido.

7. Centro de Manutenção

Configure regras de alerta para monitorar servidores e dispositivos para que você possa manipulá-los em tempo hábil para 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 for anormal.

7.1. Configurando a regra de alerta

Configure regras de alerta para monitorar servidores e dispositivos para que você possa manipulá-los em tempo hábil.

Procedimento:

» **Passo 1:** efetue o login no Defense. Na Página inicial, clique em  e na seção *Configuração do Aplicativo,* selecione *Centro de Manutenção > Configuração da Regra de Alerta.*

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

» **Passo 3:** configure os parâmetros, e então clique em *Próximo.*

Parâmetros	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 só será acionado dentro do período definido.
Alvos de Monitoramento	Os destinos incluem servidores e dispositivos. Você pode selecionar diferentes fontes de alerta para cada uma delas.
Condições da Regra	Defina o limite para cada condição. Quando o valor for maior ou igual ao limite, o alerta será disparado.
Notificação por Push	Depois de habilitado, você pode selecionar os usuários que receberão notificações quando o alerta for disparado.
Notificação por e-mail	Depois de habilitado, você pode personalizar o conteúdo a ser enviado para endereços de e-mail das seguintes maneiras: Clique  para selecionar os endereços de e-mail dos usuários. Introduza manualmente um endereço de e-mail e em seguida, pressione a tecla *Enter.*

8. Inspeção inteligente

Configure objetos e planos de inspeção para que a plataforma possa inspecionar regularmente dispositivos,comoequipamentosdeenergiaouumaárea,ecoletarimagensedadosduranteoprocesso. Antes de usar esta função, você deve:

1. Compre uma licença com função de inspeção inteligente e ative a licença.
2. Obter e instalar o plugin de inspeção inteligente.
3. Configure discos de imagem e arquivo e vídeo, para armazenar instantâneos e vídeos gravados durante as inspeções.
4. Adicione dispositivos usados para inspeção à plataforma e configure seus períodos de retenção de vídeo.

8.1. Configurando o modelo de objeto

Configure tipos de objeto e pontos de inspeção usados com frequência. Ao configurar um ponto de inspeção real, você pode selecioná-los para incluir automaticamente a maioria das informações.

8.2. Adicionando um tipo de objeto

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

Procedimento:

» **Passo 1:** efetue o login no Defense. Na Página inicial, clique em  e na seção *Configuração do Aplicativo,* selecione *Inspeção inteligente > Modelo de objeto.*

» **Passo 2:** clique  .

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

Operações Relacionadas:

» **Alterar o nome de um tipo de objeto:** selecione um tipo de objeto e clique para alterar seu nome.
» **Excluir um tipo de objeto:** selecione um tipo de objeto e clique para excluí-lo.

8.3. Adicionando ponto de inspeção

Configure as informações do ponto de inspeção de um tipo de objeto. Por exemplo, a área do disjuntor a ser inspecionada, itens a serem inspecionados e tecnologias a serem utilizadas.

Procedimento:

» **Passo 1:** efetue o login no Defense. Na Página inicial, clique em  e na seção *Configuração do Aplicativo,* selecione *Inspeção inteligente > Modelo de objeto.*
» **Passo 2:** clique em um tipo de objeto e em seguida clique em *Adicionar.*
» **Passo 3:** configure os parâmetros e clique em *OK.*

Ou clique em *Salvar e Continuar* para adicionar mais pontos de inspeção.

Parâmetro	Descrição
Área de inspeção	Clique na caixa de entrada para inserir um nome manualmente. Se houver pontos de inspeção adicionados, você poderá selecionar uma área de inspeção na lista suspensa.
Tipo de ponto	Digite um nome para o tipo de ponto.
Item de inspeção	Insira os itens a serem inspecionados.
Tecnologia de inspeção	» **Instantâneo visível:** a plataforma só tirará instantâneos. » **Monitoramento de Temperatura Térmica:** utiliza tecnologia térmica para monitorar a temperatura. Você pode configurar o limite de aviso de temperatura e o limite de aviso de temperatura diferente, mas eles são parâmetros opcionais. » **Limite de Aviso de Temperatura:** configure os limiares para baixo, médio e alto. Quando a tempera- tura for maior do que qualquer uma delas, um alarme será disparado. » **Limite de Aviso de Diferença de Temperatura:** configure os limites para baixo, médio e alto. Quando a diferença de temperatura for maior do que qualquer uma delas, um alarme será disparado. » 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.

8.4. Importando tipos de objeto e pontos de inspeção

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

Procedimento:

» **Passo 1:** efetue o login no Defense. Na Página inicial, clique em  e na seção *Configuração do Aplicativo,* selecione *Inspeção inteligente > Modelo de objeto.*
» **Passo 2:** clique  .
» **Passo 3:** clique em *Baixar modelo* e em seguida, salve o modelo em seu computador.
» **Passo 4:** preencha as informações e salve as alterações.

Clique  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 em seguida abra o modelo.

Caso haja pontos de fiscalização que estejam na plataforma, suas informações serão atualizadas.

8.5. Configurando Objeto de inspeção

Adicione objetos de inspeção para que a plataforma possa inspecionar um ou mais pontos. Os objetos de inspeção são gerenciados por organizações de inspeção. Somente funções e usuários especificados podem acessar determinadas organizações.

8.6. Adicionando organização de inspeção

As organizações de inspeção são usadas para gerenciar objetos e pontos de inspeção. Somente administradores podem configurá-los e especificar quais funções e seus usuários podem acessar determinadas organizações.

Procedimentos:

» **Passo 1:** efetue o login no Defense. Na Página inicial, clique em  e na seção *Configuração do Aplicativo,* selecione *Inspeção inteligente > Modelo de objeto.*

» **Passo 2:** clique  .

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

Ou clique em *Salvar e Continuar* para adicionar mais pontos de inspeção.

Parâmetro	Descrição
Organização principal	Isso é para controle de permissão. Por exemplo, se um usuário não pode acessar A, o usuário não pode acessar todas as organizações em A.
Nome da organização	Insira um nome para a organização
Acesso permitido às funções	Somente funções selecionadas e seus usuários podem acessar essa organização. Clique  para ver os usuários atribuídos com as funções.

8.7. Adicionando objeto de inspeção

Procedimento:

» **Passo 1:** efetue o login no Defense. Na Página inicial, clique em  e na seção *Configuração do Aplicativo,* selecione *Inspeção inteligente > Inspeção de objeto.*

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

» **Passo 3:** configure as informações básicas, e então clique em *Próximo.*

Parâmetros	Descrição
Nome do objeto de inspeção	Insira um nome para o objeto de inspeção
Organização	Exibe o nome da organização na etapa anterior. Você pode selecionar outro.
Tipo de objeto a ser enviado	Selecione um tipo de objeto que foi adicionado. Isso é opcional.

» **Passo 4:** clique *Adicionar Ponto.*

Se você selecionar e 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 em seguida, clique em *OK.*

Parâmetro	Descrição
Nome do ponto	Digite um nome para o ponto.
Área de Inspeção	Clique na caixa de entrada para inserir um nome manualmente. Se houver pontos de inspeção adicionados, você poderá selecionar uma área de inspeção na lista suspensa.
Tipo de ponto	Digite um nome para o tipo de ponto.
Item de Inspeção	Insira os itens a serem inspecionados.
Tecnologia de Inspeção	» **Instantâneo visível:** a plataforma só tirará instantâneos. » **Monitoramento de Temperatura térmica:** utiliza tecnologia térmica para monitorar a temperatura. Você pode configurar o limite de aviso de temperatura e o limite de aviso de temperatura diferente, mas eles são parâmetros opcionais. » **Limite de Aviso de Temperatura:** configure os limites para baixo, médio e alto. Quando a temperatura for maior do que qualquer um deles, um alarme será acionado. » **Limite de Aviso de Diferença de Temperatura:** configure os limites para baixo, médio e alto. Quando a diferença de temperatura for maior do que qualquer uma delas um alarme será disparado. » 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 *Acoplar Câmera.*

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

Parâmetros	Descrição
Selecionar Canal	Clique duas vezes em um canal a ser vinculado. Seu vídeo ao vivo e informações serão exibidas à direita.
PTZ	Se você estiver ligado um canal PTZ, você pode operá-lo usando o painel de controle PTZ. Além disso, você deve vincular a uma predefinição do canal PTZ. Clique em  e então clique  em seguida, clique em uma predefinição para vinculá-la ao ponto.
Parâmetros de monitoramento de temperatura	» Após ligar 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 terá a temperatura mais alta na área incluída pela regra definida. Por exemplo, se você adicionar um retângulo no vídeo ao vivo, o dispositivo terá a temperatura mais alta nesse retângulo. » **Limite de Aviso de temperatura:** configure os limites para baixo, médio e alto. Quando a temperatura for maior do que qualquer um deles, um alarme será acionado. » **Limite de Aviso de Diferença de Temperatura:** configure os limites para baixo, médio e alto. Quando a diferença de temperatura for maior do que qualquer uma delas, um alarme será disparado. » 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.*

8.8. Configurando plano de inspeção

Durante os períodos definidos, a plataforma inspecionará os objetos e pontos selecionados e salvará os dados relacionados à plataforma.

Procedimento:

» **Passo 1:** efetue o login no Defense. Na Página inicial, clique em  e na seção *Configuração do Aplicativo,* selecione *Inspeção inteligente > Plano de Inspeção.*

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

» **Passo 3:** configure as informações básicas, e então clique em *Próximo.*

Parâmetros	Descrição
Nome do plano	Insira um nome para o plano
ID do Plano	Isso é gerado automaticamente. Você pode editá-lo conforme necessário.
Organização de Inspeção	Exibe o nome da organização selecionada na etapa anterior. Você pode selecionar outro.
Tipo de Inspeção	Selecione um tipo para o plano. É utilizado para procurar determinados planos de inspeção
Tempo de processamento	O tempo de processamento funciona das seguintes 2 maneiras: » Para referência dos revisores quando analisam os resultados das inspeções. » Quando faltam 5 minutos e o plano de inspeção ainda não foi processado, todos os usuários que têm permissão para acessar a organização à qual este plano pertence são notificados.
Habilitar	Depois de habilitado, esse plano entra em vigor após a adição.

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

1. Clique em *Adicionar.*
   Somente a organização selecionada, suas sub-organizações e seus objetos e pontos são 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 *Próximo.*

» **Passo 5:** configure o tempo de execução, em seguida clique em *OK.*

Parâmetros	Descrição
Modo de execução	» **Por Período:** o plano é executado automaticamente dentro dos períodos especificados. » **Uma vez por dia:** o plano será executado em horário definido todos os dias. Você pode usar  para configurar vários dias ao mesmo tempo.
Estratégia de execução	» **Looping:** configure o intervalo de looping e em seguida, o plano será executado dentro dos períodos efetivos em cada intervalo que você configurar. » **Apenas uma vez:** o plano só será executado uma vez após adicionado ou em tempo definido.
Modo de Luz	Selecione se deseja acender a luz nos dispositivos durante a inspeção. Como pode levar tempo para que os dispositivos acendam a luz, você pode configurar um período de aquecimento para garantir que a luz possa ser normalmente acesa antes do início da inspeção.

8.9. Configurando o evento de monitoramento de temperatura

Se você configurou limites de aviso em inspeções, poderá configurar eventos para executar ações de vinculação quando os limites forem atingidos. Por exemplo, um ponto de inspeção monitorou uma temperatura maior que o limite, uma câmera gravará um vídeo da área que está monitorando.

9. Configurações do sistema

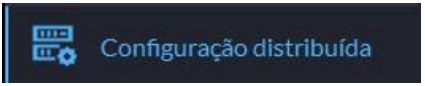
As configurações do sistema desempenham um papel essencial na personalização e gerenciamento do ambiente. Esses módulos são responsáveis por administrar diversos elementos que permitem uma customização precisa. Entre suas funcionalidades, incluem-se a configuração de servidores auxiliares, o gerenciamento 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.

9.1. 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.

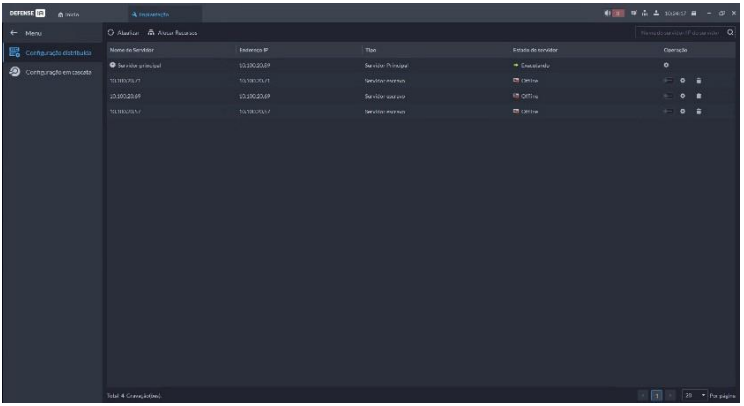
19.1. Configuração distribuída



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 processamento 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*  .

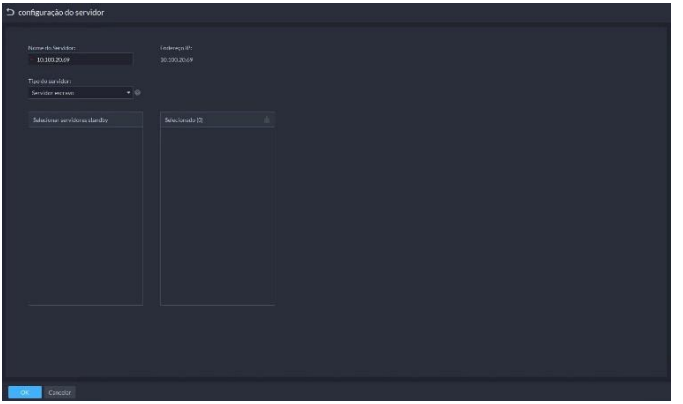
Ao ativar os servidores, aguarde alguns segundos até estes conectarem-se ao servidor principal e clique em *Atualizar* para visualizar o estado do servidor como *Executando* 

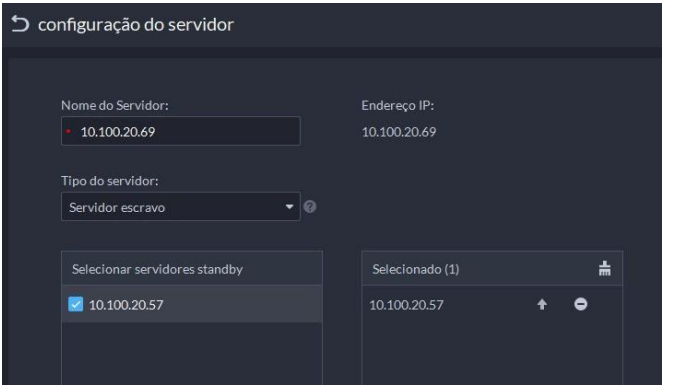
. Os servidores auxiliares (ou slave servers) suportam dois modos de configuração. Para configurá-los, clique na engrenagem  .

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 acessá-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:



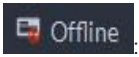


Servidor auxiliar standby

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.

» 

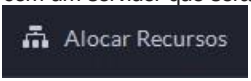
: servidor conectado e funcional.

» 

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

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.

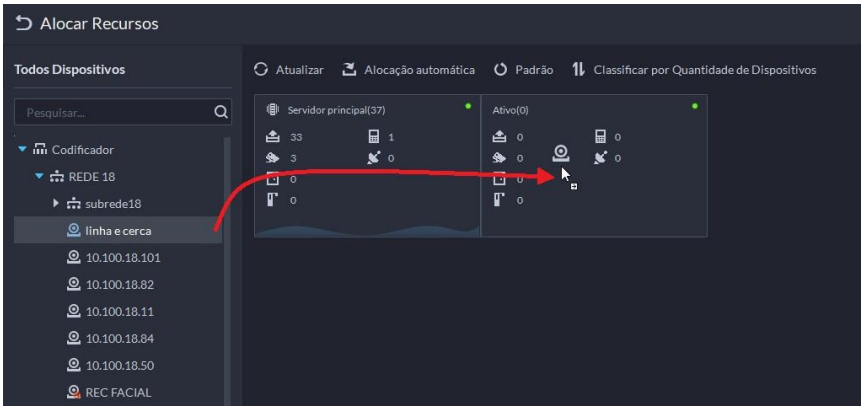
Para isso clique em *Alocar Recursos* 

na parte superior da tela.

Existem duas opções para a alocação de recursos.

Alocação manual

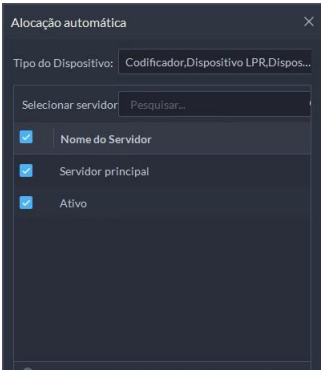
Aloca-se um dispositivo por vez, isso pode ser feito ao arrastar o dispositivo da árvore de dispositivos para o bloco do servidor.



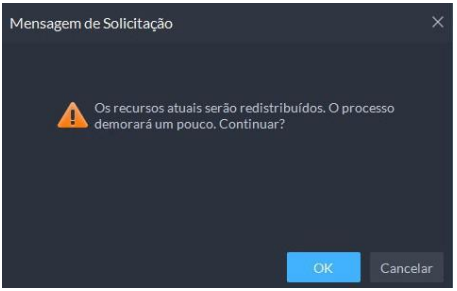
Alocação automática

Ao clicar no botão 

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

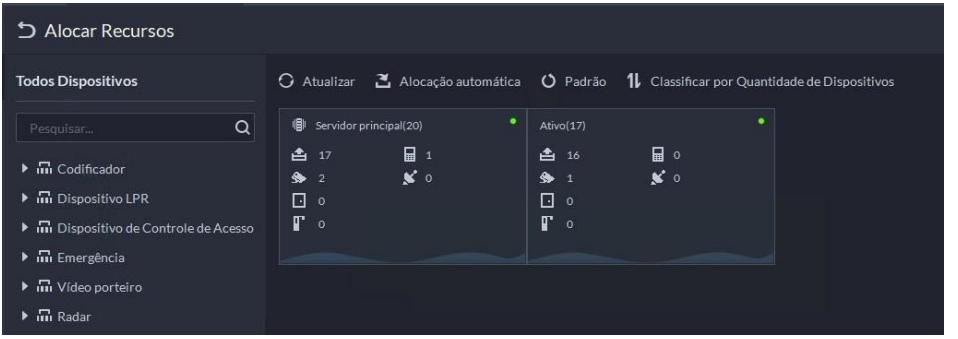


Clique em *OK* e em seguida, confirme a mensagem para continuar.

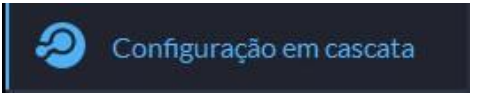


Ao confirmar a mensagem, a alocação automática iniciará, é possível acompanhar o processo pela barra de carregamento no canto superior da tela.

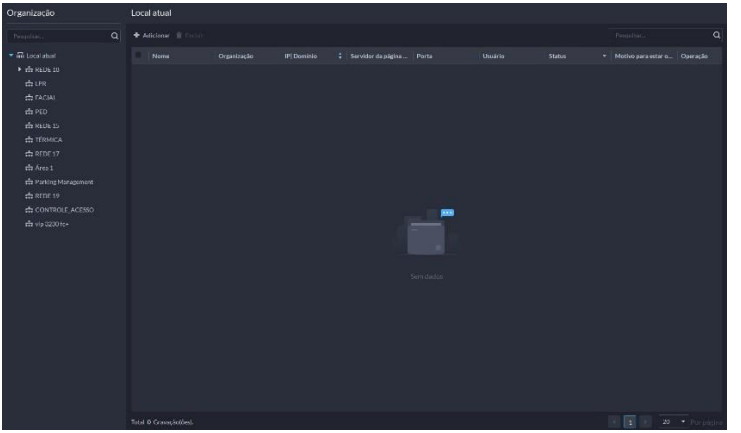
Ao finalizar, os dispositivos devem estar balanceados entre os servidores selecionados, desta forma, ambos os servidores atuam com uma carga de processamento computacional muito semelhante.



29.2. Configuração em cascata

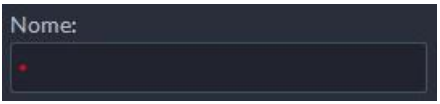


A plataforma Defense IA possui como característica expansiva a capacidade de estender dispositivos e gravações através da adição de um servidor adicional em forma de cascata. Ao incluir um servidor como um novo nível na cascata, é possível acessar todos os dispositivos e gravações por meio do servidor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



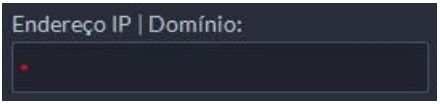
Para adicionar um servidor em cascata, clique em *Adicionar*  na guia superior da tela.

Preencha as informações necessárias do servidor que deseja adicionar.



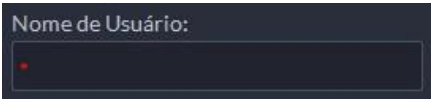
» **Nome:** nome que identificará a cascata.

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

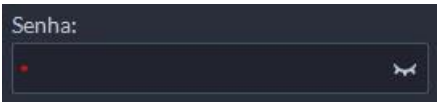


» **Endereço IP | Domínio:** endereço do servidor a ser adicionado.

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

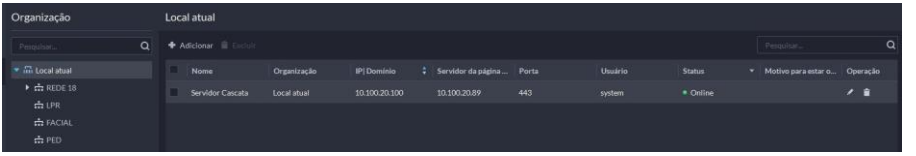


» **Nome de Usuário:** nome de usuário para acessar a plataforma - e seus dispositivos - a serem adicionados.



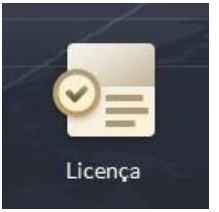
» **Senha:** senha de usuário para acessar a plataforma - e seus dispositivos - a serem adicionados.

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



9.2. 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 Vídeoporteiro	Este recurso é compatível com dispositivos de vídeo portaria (PVIP e TVIP). Ao contrário dos recursos listados acima, a quantidade de licenças de dispositivos Vídeoporteiro 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.
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.

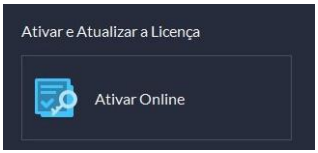
Alto-falante IP	Este habilita a adição de um dispositivo corneta IP da linha SPK na plataforma.
Regras de Localização de Veículos	Este recurso é compatível com o módulo de estacionamento. Estará disponível em versões futuras.
Cascata	Este recurso habilita a adição de um outro servidor principal do Defense 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.

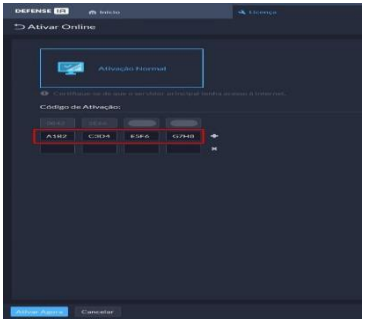
Para utilizar plugins, é necessários instalá-los no servidor da plataforma.
Contate seu consultor comercial para adquirir um código de licença com as capacidades desejadas, as licenças são únicas e incrementais, é possível expandir o sistema adicionando diversos códigos. Sua ativação pode ser feita de duas formas, de maneira Online ou Offline.

19.1. 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.

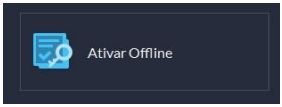


Clique em *Ativar Agora* para habilitar o(s) código(s) inserido(s). O client reiniciará.

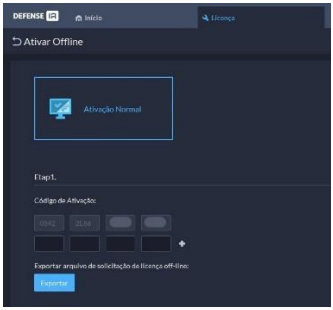
O código de licença ativado fica vinculado à máquina em questão, o código é instransferível. Caso utilize algum firewall ou anti-vírus, atente-se a bloqueios à aplicação. Caso utilize ambiente virtualizado, atente-se com regras de mudança de endereços de hardware, isso pode ocasionar perda da licença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

29.2. 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.

9.3. Parâmetros do Sistema

Configure parâmetros de segurança, duração de retenção de armazenamento, email do servidor, sincronização de tempo, Log remota, método de login e muito mais.

19.1. Configurando parâmetros de segurança

Efetue o login no Client Defense. Na página inicial clique em  , e na seção de *Configuração do sistema,* selecione *Parâmetros > Parâmetros de segurança,* e em seguida configure os parâmetros.

Parâmetros	Descrição
Gestão de Certificado	Um certificado de CA é usado para validar legitimidade da plataforma. Ao acessar a plataforma através de um navegador, o navegador irá validar a certificação. Se o certificado não estivar instalado no Navegador, o Navegador considerará a plataforma como segura e irá conceder acesso. Se o Certificado não estiver instalado no Navegador, o navegador não considerará a plataforma como segura, e não lhe concederá acesso. Você pode criar, importar e baixar certificados na plataforma. » **Criar uma certificação:** depois de criar uma certificação, importe-a para o computador que acessará a plataforma » **Importar um certificado:** você pode importar um certificado que tenha sido criado para a plataforma.
Políticas de segurança de arquivos	Proteja seus dados verificando a senha de login ao fazer o download ou exportar informações e criptografar arquivos de exportação. » Autenticação de senha de exportação ou downloads de arquivos: » Você precisa digitar a senha da conta corrente para exportar ou baixe os arquivos. » Para todos os usuários que fazem login na plataforma, eles não precisam inserir a senha quando estiverem exportando ou baixando os arquivos » Criptografia de exportação e download de arquivos: você precisa definir uma senha de criptografia para os arquivos para serem exportados ou baixados. Quando alguém utiliza os arquivos eles precisam verificar a senha de criptografia.
Lista de permissões HTTP	Depois que o Firewall do servidor estiver habilitado, você precisa adicionar o endereço de IP do computador onde o cliente Defense está instalado para a Lista de permissões HTTP possa acessar o servidor.
Lista de permissão de redirecionamento RTSP	Depois que o Firewall do servidor estiver habilitado, somente os endereços IP que estiverem na lista de acesso RSTP pode solicitar transmissão de vídeo através da mídia serviço de Gateway. Os endereços de IP dos Decoders irão ser adicionados automaticamente. Se houver outros endereços de IP que precisam solicitar transmissão de vídeo através da mídia serviço de Gateway, você precisa adiciona-los manualmente a lista de permissão RSTP.

29.2. Configurando Período de retenção de dados do sistema

Definir os períodos de retenção para logs, Mensagem de alarme, Registro de reconhecimento de faces, Registro de passagem de veículos, registro de acesso instantâneo, registro de comunicação de vídeo, registro de visitantes, mensagem POS, e mais. Registros além da definição do período de retenção serão automaticamente deletados.

Procedimento:

» **Passo 1:** faça o login no cliente do Defense. Na página inicial, clique , e na seção de *Configuração de Sistema,* selecione *Parâmetros de Sistema.*

» **Passo 2:** clique no *Período de retenção de mensagem.*

» **Passo 3:** se um clique duplo para alterar os valores dos números.

» **Passo 4:** clique em *Salvar.*

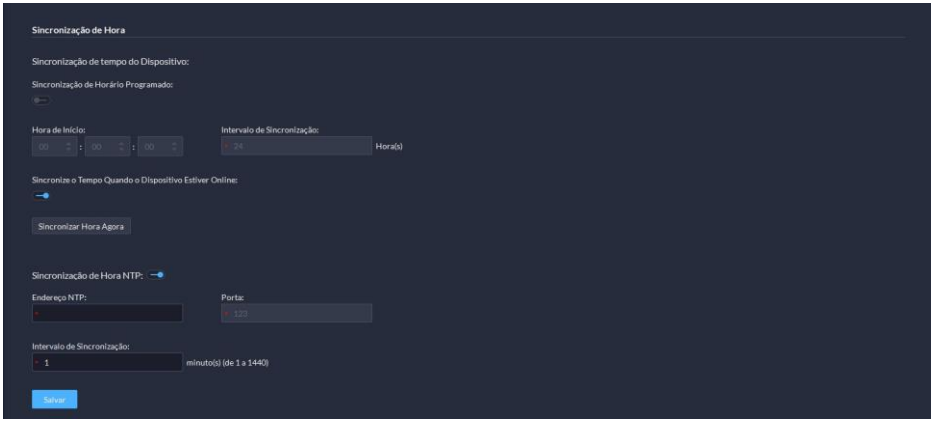
39.3. Sincronização de tempo

Sincronize a hora do sistema de todos os dispositivos conectados, do cliente do PC e do servidor. Caso contrário, o sistema pode funcionar mal. Por exemplo, Pesquisa de vídeo poderá falhar. A plataforma suporta a sincronização do tempo de múltiplos dispositivos, nos quais tem o mesmo fuso horário da plataforma. Você pode sincronizar o tempo manualmente ou automaticamente.

Procedimento:

» **Passo 1:** faça o login no cliente do Defense. Na página inicial, clique , e na seção de *Configuração de Sistema,* selecione *Parâmetros de Sistema.*

» **Passo 2:** clique na guia de *Sincronização de Hora.* Habilite os métodos de sincronização, e defina os parâmetros.



» **Sincronização de horário programado:** habilite a função, insira a hora de inicio na sincronização de tempo para cada dia, e o intervalo.

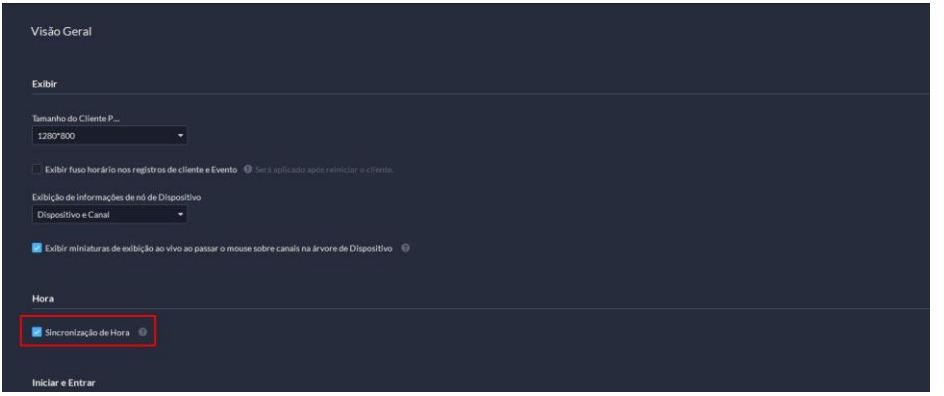
» **Sincronize o tempo quando o dispositivo estiver online:** sincronize a hora do dispositivo quando o dispositivo ficar online.

» **Sincronização de hora NTP:** se houver um servidor NTP no sistema, você poderá ativar essa função, para que o sistema habilite o tempo com o servidor NTP.

» **Passo 3:** clique em *Salvar.*

» **Passo 4 (Opcional):** habilite a sincronização do client do Defense.

4. Faça o login no client do Defense, e na seção Gerenciamento, clique *Definições Locais.*
5. Clique na aba Visão Geral, marque a caixa de seleção ao lado de Sincronização de Hora e clique em *Salvar.*
   O sistema irá sincronizar imediatamente a hora após você reiniciar o cliente para manter a hora do servidor e do Pc sincronizadas.



69.6. InSearch

Configure os parâmetros do InSearch para que ele possa funcionar normalmente.
Pré-requisitos: compre uma licença com a função InSearch, e ative a licença.
Procedimento:

» **Passo 1:** faça o login no cliente do Defense. Na página inicial, clique , e na seção de *Configuração de Sistema,* selecione *Parâmetros de Sistema.*

» **Passo 2:** clique na aba *InSearch.*

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

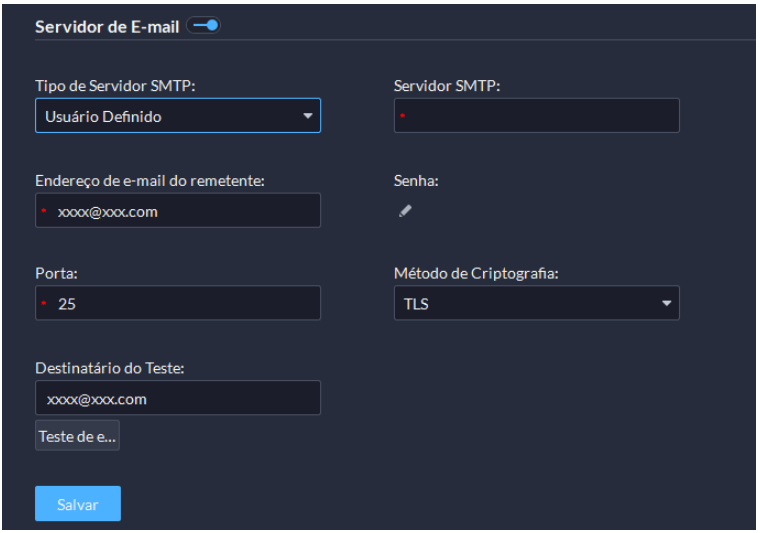
Parâmetros	Descrição
Método de comparação InSearch	» **Inteligência de borda:** após você selecionar a imagem, você pode pesquisar por ele apenas no dispositivo que suporta pesquisa por imagem. » **Inteligência Central:** você pode pesquisar a imagem que você selecio- nou em múltiplos dispositivos.
IP/Nome do domínio/porta	Adicione o endereço IP ou nome do domínio, e o numero da porta do servidor disponível com os algoritmos do InSearch.
Certificado de identidade/ Chave Secreta	» Clique para copiar o certificado de identidade e chave secreta, então configure eles para o servidor do Defense. » Clique para gerar uma nova chave secreta.
Teste da função do InSearch	Clique no botão para verificar se a função está funcionando normalmente. Caso contrário, resolva o problema solicitado pela plataforma, então cheque novamente. Repita os passos até que funcione normalmente.

79.7. Configurando Servidor de E-mail

Procedimento:

» **Passo 1:** faça o login no cliente do Defense. Na página inicial, clique , e na seção de *Configuração de Sistema,* selecione *Parâmetros de Sistema.*

» **Passo 2:** clique na aba do Servidor de E-mail, habilite Servidor de E-mail, e configure os parâmetros requeridos.



Parâmetros	Descrição
Tipo de servidor SMTP	Selecione de acordo com o tipo do servidor SMTP para se conectar. Os tipos incluem Yahoo, Gmail, Hotmail, e Usuário Definido.
Endereço de E-mail do remetente	O remetente é exibido quando um e-mail é enviado do Defense.
Servidor SMTP Senha Porta	Endereço IP, Senha, e número da porta do servidor SMTP.
Método de criptografia	Não suporta criptografia, Criptografia TLS e criptografia SSL.
Destinatário teste Teste E-mail	Defina o destinatário, e em seguida clique no Teste de e-mail para testar se a caixa de mensagem está disponível.

» **Passo 3:** clique em *Salvar.*

89.8. Configurando o Active Directory

Quando os usuários em um domínio podem ser usados como usuários na plataforma, você pode usar essa função para importar rapidamente para a plataforma.

Procedimento:

» **Passo 1:** configure as informações do domínio.

1. Faça o login no cliente do Defense. Na página inicial, clique , e na seção de *Configuração de Sistema,* selecione *Parâmetros de Sistema > Active Directory.*
2. Clique  para habilitar a função, e então configurar os parâmetros do domínio.
3. Clique em *Obter DN* para obter automaticamente informações básicas do DN.
4. Clique em *Teste* para checar se a informação do domínio está correta.

5. (Opcional) Habilite a função de sincronização automática e defina um horário. Em seguida a plataforma sincronizará automaticamente os usuários de noticias nos grupos de domínio que você tiver importado anteriormente, e atualizará a informação dos usuários importados via seleção manual no horário negado todos os dias.
6. Por exemplo, você importou um Grupo de domínio A inteiro. A plataforma vai sincronizar novos usuários ao Grupo de domínio A todos os dias no horário definido. Clique , para remover um grupo da lista, e então ele não irá ser sincronizado. Para usuários importados via seleção manual, a plataforma irá checar a informação, e atualizará se acontecer mudanças.
7. Clique em *Salvar.*

» **Passo 2:** importar usuários do domínio

1. Faça o login no cliente do Defense. Na página inicial, clique , e na seção de *Configuração Básica, selecione Usuário > Gereciamento de usuário*
2. Clique em *Importar usuários do domínio.*
3. Selecione como você quer importar os usuários, e clique próximo passo.
   » **Importar por Grupo de Domínio:** importe todos os usuários do grupo selecionado.
   Se você importar um grupo de domínio inteiro e após a sincronização automática função estará habilitada, a plataforma vai lembrar desse grupo e automaticamente sincronizar seus novos usuários no horário negado todos os dias.
   » **Importar por usuário de domínio:** importar usuários selecionados em um grupo.
4. Clique para selecionar um cargo para o usuário.
   Todas as permissões no cargo irão ser associadas ao usuário
5. Clique em *OK.*

69.6. Customizando Sinal Final de PdV

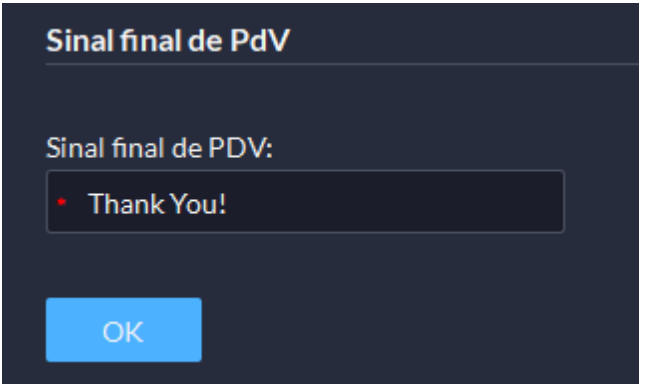
Configure o sinal que aparece no final do recebimento PdV.

Procedimento:

» **Passo 1:** faça o login no cliente do Defense. Na página inicial, clique , e na seção de *Configuração de Sistema,* selecione *Parâmetros de Sistema.*

» **Passo 2:** clique na aba *Sinal Final de PdV.*

» **Passo 3:** insira o Sinal Final de PdV, e clique em *OK.*



79.7. Configuração de parâmetros de acesso ao dispositivo

Para garantir que você possa usar os dispositivos com segurança, recomendamos usar o modo de segurança, se o dispositivo suportar esse modo para evitar riscos de segurança. A plataforma também suporta habilitar e desabilitar a adição de dispositivos através do P2P.

Procedimento:

» **Passo 1:** faça o login no cliente do Defense. Na página inicial, clique , e na seção de C*onfiguração de Sistema,* selecione *Parâmetros de Sistema > Configuração de adição de dispositivos.*

» **Passo 2:** selecione modo de login do dispositivo e depois clique em *Salvar.*

» **Passo 3:** habilite ou desabilite a função *P2P.*

Se desabilitada, você não poderá adicionar dispositivos pela plataforma através do P2P.

89.8. Log Remoto

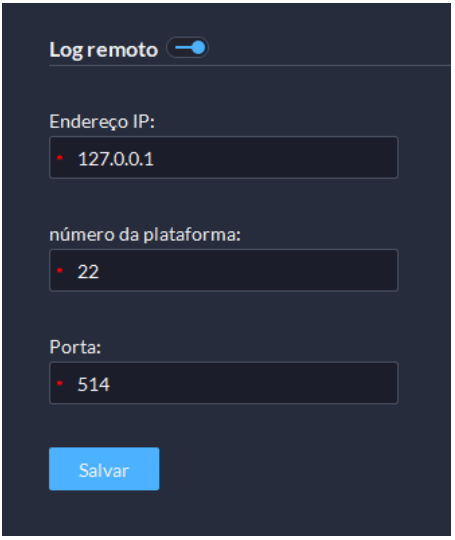
Para garantir o uso seguro da plataforma, o sistema envia logs do administrador e do operador para o log do servidor para backup às 3 da manhã todos os dias.

Procedimento:

» **Passo 1:** faça o login no cliente do Defense. Na página inicial, clique , e na seção de *Configuração de Sistema,* selecione *Parâmetros de Sistema.*

» **Passo 2:** clique na aba de Log remoto.

» **Passo 3:** habilite a função e defina os parâmetros conforme o necessário. O numero da plataforma deve ser o mesmo no servidor remoto e na plataforma.



» **Passo 4:** Clique em *Salvar.*

99.9. Configurando Implantação de Banco de Dados Independente

A plataforma suporta a conexão a um banco de dados independente e o armazenamento de dados nele, incluindo imagens de resto, metadados de vídeos, eventos, informações de LPR. Apenas licenças oficiais suportam essa função.

Pré-requisitos:

Você preparou um banco de dados pronto para ser executado. Observe que o nome do banco de dados deve ser: ExternalIdependentDB. Caso contrário, os dados não serão armazenados corretamente no banco de dados.

Procedimento:

» **Passo 1:** faça o login no cliente do Defense. Na página inicial, clique , e na seção de *Configuração de Sistema,* selecione *Parâmetros de Sistema.*

» **Passo 2:** clique na aba Implantação de Banco de Dados Independente.

» **Passo 3:** clique para habilitar a função, e então configurar os parâmetros.

Parâmetro	Descrição
Tipo de Banco de Dados	Suporta apenas MySQL
Endereço de IP	Adicione o endereço de IP ao banco de dados
Porta	Adicione a porta ao banco de dados
Usuário/Senha	Adicione o Usuário e a senha utilizado para acessar ao banco de dados

» **Passo 4:** clique em *Salvar.*

Um banco de dados independente só pode se conectar a uma plataforma.

Resultados:

Após um banco de dados independente é implantado, Imagens da Face, Metadados de Vídeo, even- tos e LPR, as informações serão armazenadas apenas no banco de dados independente e não serão armazenadas no local banco de dados. Além disso, quando você pesquisar por esses 4 tipos de dados a plataforma só pesquisará a base de dados que foram gerados anteriormente no banco de dados independente. Os dados que foram gerados anteriormente no banco de dados local não serão disponíveis para a pesquisa.

109.10. Configurando do aplicativo móvel

Se você precisar enviar mensagens para o aplicativo, você deve habilitar essa função. Depois de habilitadas, as mensagens irão ser enviadas através para o aplicativo através dos servidores de provedores Push de notificação. Dados relacionados a essas mensagens não será enviada de volta para nós.

Procedimento:

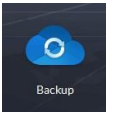
» **Passo 1:** faça o login no cliente do Defense. Na página inicial, clique , e na seção de *Configuração de Sistema,* selecione *Parâmetros de Sistema > Configuração do aplicativo móvel.*

» **Passo 2:** habilite ou desabilite Notificação Push.

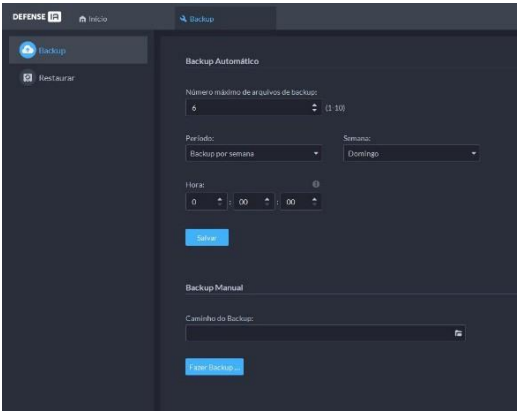
Se desativada, o aplicativo não receberá nenhuma mensagem, alarmes e chamadas

9.4. 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.*



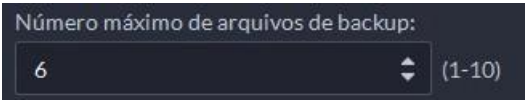
19.1. Baixar Backup



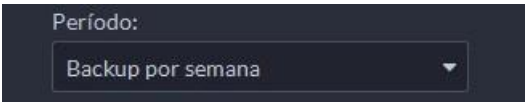
Há duas opções para realizar o backup do banco de dados na plataforma, que serão listadas abaixo:

Backup Automático

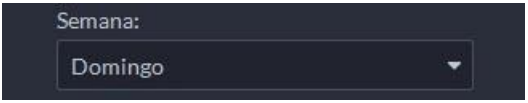
Em Backup automático é possível definir parâmetros de configuração para uma recorrência periódica do backup. Dentre essas configuram-se:



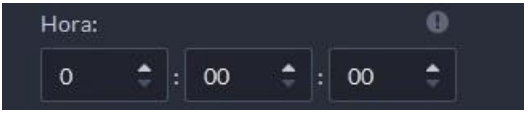
» **Número máximo de arquivos de backup:** define a quantidade entre 1 e 10 de arquivos de backup
armazenados.



» **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 "...".

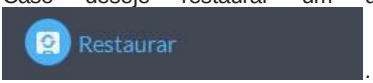
Ao realizar o backup, a senha do usuário deve ser confirmada, assim como a inserção de uma senha de criptografia para uma camada de segurança do arquivo de backup.

Backup Manual

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

29.2. 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 funcionamento pleno do sistema.

10. Gerenciamento

110.1. 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.

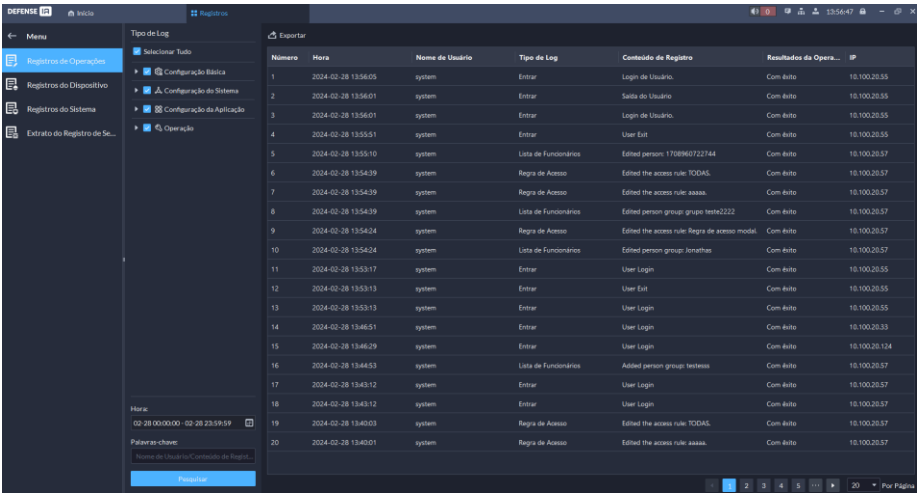
Log de Operações

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:



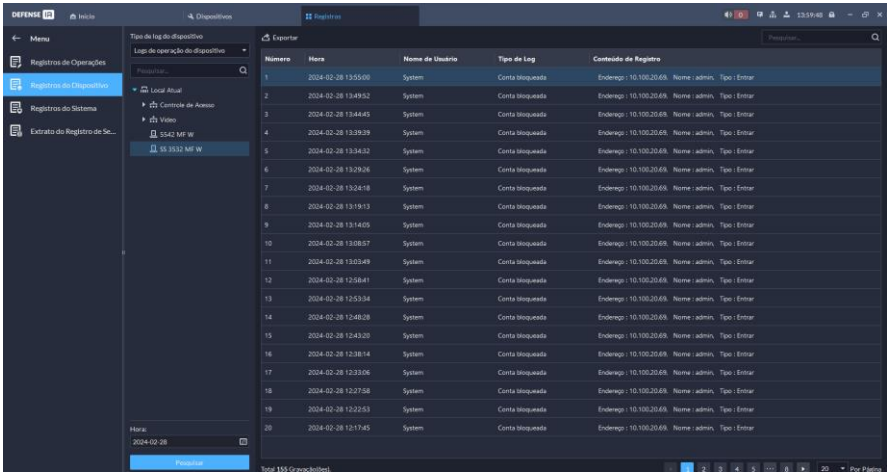
Log de Dispositivo

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 caracteísticas: data, hora, nome do usuário, tipo de log e conteúdo do registro.

Na imagem abaixo está o exemplo de uma busca realizada:



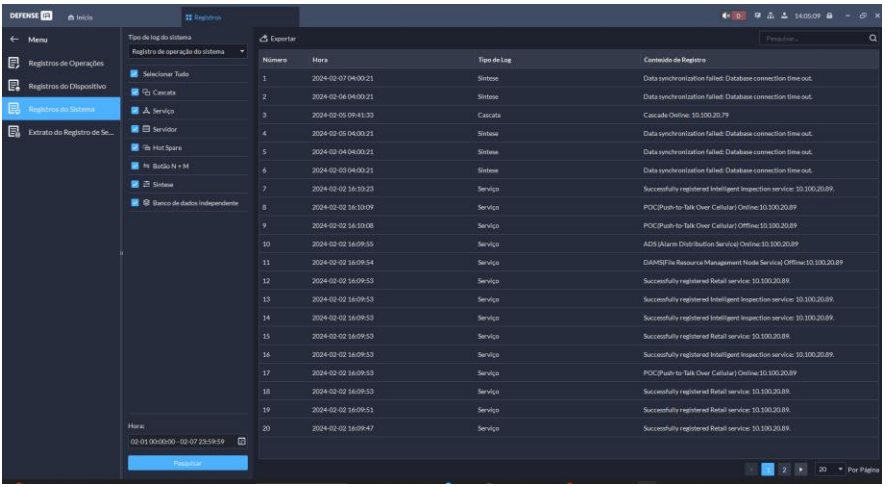
Log do Sistema

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:



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.

11. 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.

111.1. 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* > *Configuração Local.*

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

Parâmetros	Descrição
Tamanho do Cliente	Selecione uma resolução adequada para o cliente de acordo com a tela de exibição do PC.
Exibir fuso horário em registros de clientes e eventos	Quando selecionado, o cliente e o tempo dos alarmes mostrarão tanto o Horário e fuso horário.
Informação do nó do dispositivo	Selecione que a arvore de dispositivos exibe os dispositivos e seus canais ou apenas canais
Exibir miniaturas de visualização ao vivo ao passar o mouse sobre canais na árvore de dispositivos	Quando selecionada, você pode passar o mouse sobre um canal na árvore de dispositivos na Central de Monitoramento e um instantâneo de sua imagem de vídeo ao vivo será exibido.
Sincronização de tempo	Se habilitado, o cliente começa a sincronizar a hora da rede com o servidor para concluir a sincronização de tempo
Execução automática na inicialização	Se lembrar senha tiver sido selecionado na página de login, selecione Reinicialização automática após a reinicialização, e o sistema ignorará a página de login e abrirá diretamente a página inicial depois que reiniciar o PC da próxima vez. Se lembrar senha não estiver selecionado na página de login, selecione reinicialização automática após a reinicialização a página do cliente aparecerá depois de reiniciar o PC.
Login automático	Habilite o sistema para ignorar a página de login e abrir diretamente a página inicial ao fazer login na próxima vez. Se lembrar senha e Login automático tiverem sido selecionados na página de login, a função já estará ativada. Se Lembrar senha já estiver sido selecionado enquanto Login automático não estiver selecionado na página de login, selecione login automático na página básica para habilitar essa função.
Limite de alarme da CPU	O usuário será solicitado a abrir mais um vídeo quando o uso da CPU exceder o limite definido
Criptografia de transmissão de áudio e vídeo	Criptografe todo o áudio e vídeo para garantir a segurança das informações.
Bloqueio automático do Client	O Client será bloqueado após o período definido e voce não poderá realizar nenhuma operação. Clique para desbloquear o Client e verifique a senha da conta atual para desbloquear o cliente.
Parâmetros de conversação de áudio auto adaptáveis	Se ativado, o sistema se adapta automaticamente à frequência de amostragem do dispositivo, ao bit de amostragem e ao formato de áudio para conversa de áudio.
Acesso ao modo de entrada e exibição do cartão	Selecione um modo para a plataforma usar e exiba cartões de acesso. Por exemplo, quando você emite manualmente um cartão para uma pessoa, você pode inserir A-F e números na numeração do cartão se Hex estiver selecionado, mas você só pode inserir 0-9 se Decimal estiver selecionado.
Sensibilidade do joystick	Selecione a sensibilidade para quando você operar o joystick. Quanto maior a sensibilidade, mais frequentes comandos de joystick são enviados, e maior a possibilidade de que as operações sejam atrasadas devido ao baixo desempenho das câmeras PTZ.

» **Passo 3:** clique em *Salvar.*

211.2. Definindo as Configurações de vídeo

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

Procedimento:

» **Passo 1:** efetue o login no Defense Cliente. Na Página Inicial, selecione *Gerenciamento* > *Configuração 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 definido, 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 em *Salvar.*

311.3. 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* > *Configuração 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 em *Salvar.*

411.4. 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* > *Configuração 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 em *Salvar.*

511.5. 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* > *Configuração 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 em *Salvar.*

611.6. 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* > *Configuração local.*

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

711.7. 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* > *Configuração local.*

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

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

» 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 especificado do seu computador. Ou selecione *Enviar por e-mail* e envie as configurações para o endereço de e-mail especificado.
3. Clique em *OK.*

» Importar configurações.

1. Clique em importar configurações.

1. Clique em em seguida, abra o arquivo exportado de configurações.

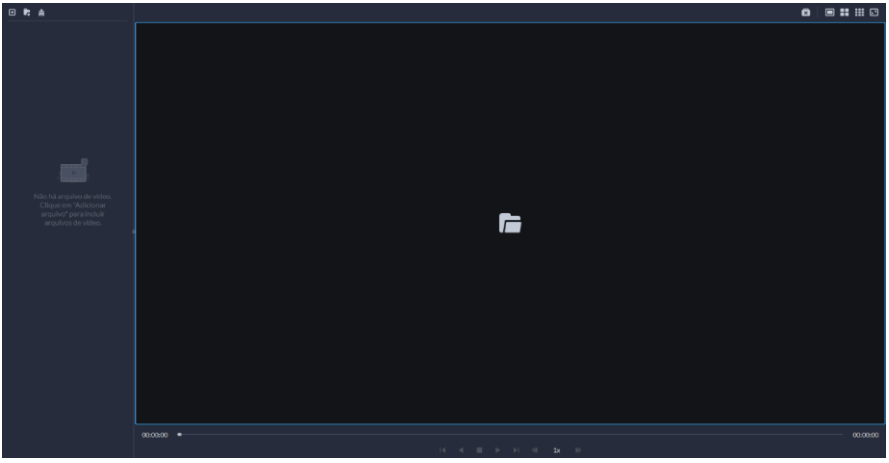
1. Clique em *OK.*

11.1. 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.

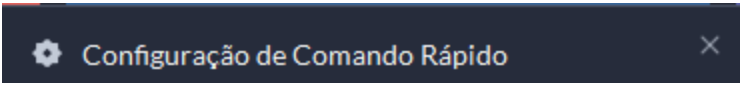
Parâmetro	Descrição
Menu com o botão direito do mouse	» **Instantâneo contínuo:** tire instantâneos da imagem atual (três instantâneos de cada vez por padrão). » **Ajuste de vídeo:** ajuste o brilho, contraste, saturação e croma do vídeo. » **Zoom digital:** clique nele e em seguida, clique duas vezes 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.

111.1. Comandos Rápidos

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

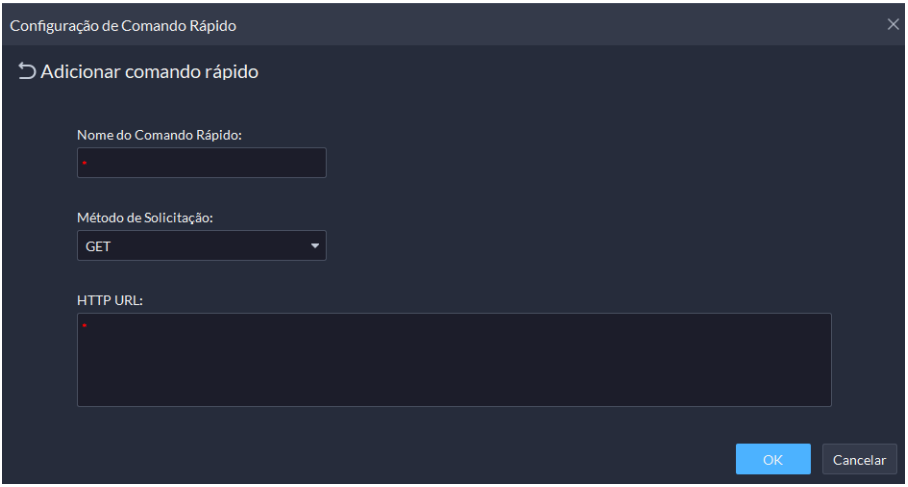
Procedimento:

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

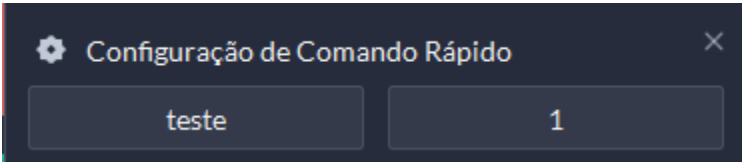


» **Passo 2:** clique  .

» **Passo 3:** Clique em *Adicionar*.



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



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

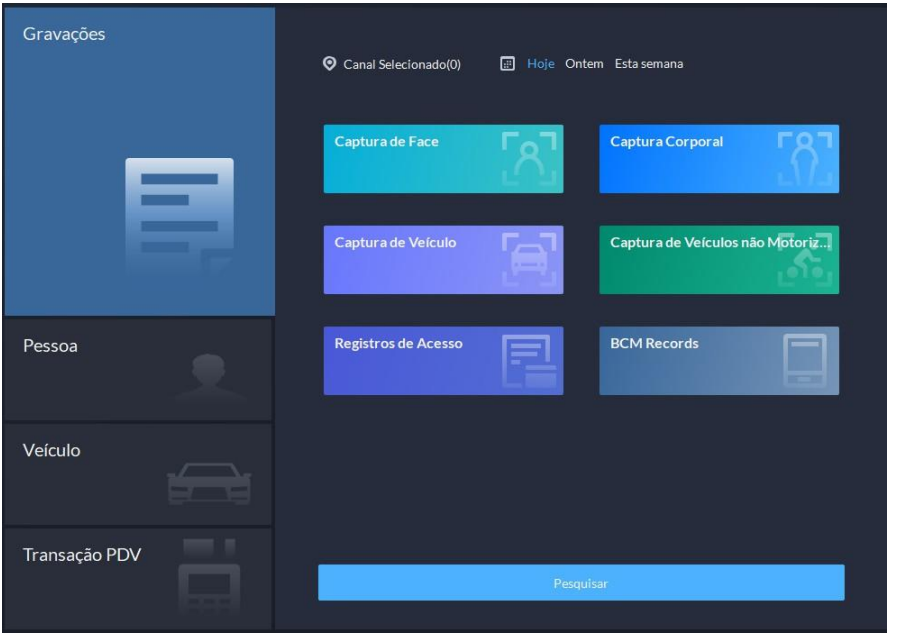
12. DeepXplore

Nesta seção você pode visualizar registros integrados de pessoas, veículos, controle de acesso, transações PDV. E dispositivos MPT.

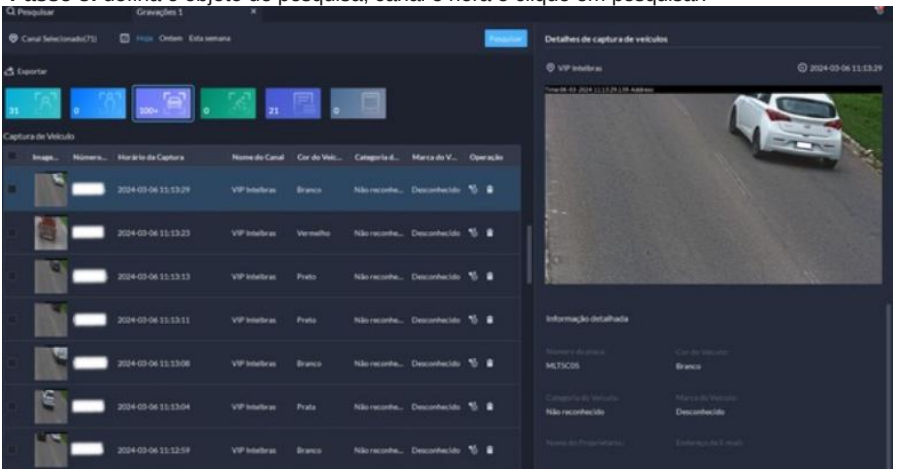
Procedimento:

» **Passo 1:** faça o login no Defense. Na Página inicial, clique em e selecione DeepXplore.

» **Passo 2:** clique em e selecione *Gravar.*



» **Passo 3:** defina o objeto de pesquisa, canal e hora e clique em pesquisar.



Para o resultado da pesquisa, você pode realizar as seguintes operações.

» Clique ao lado do registro para adicioná-los aos registros temporários

» Você pode passar o mouse sobre a pequena imagem à direita e clicar para procurar imagens semelhantes a esta. A plataforma comparará a imagem que você carrega com os registros e as imagens em grupos de comparação de rostos e em seguida retornará resultados com base na semelhança definida.

» Clique para deletar um por um.

» Clique em Exportar para exportar registros para o armazenamento local.

» **Passo 4:** selecione um registro e no lado direito, você poderá ver os detalhes. Clique na imagem do vídeo para visualizar a gravação vinculada.

Clique no canto superior direito para visualizar todos os registros adicionados aos registros temporários. Dentro dele você pode clicar para gerar o rastreamento alvo e clicar para remover o registro do banco.

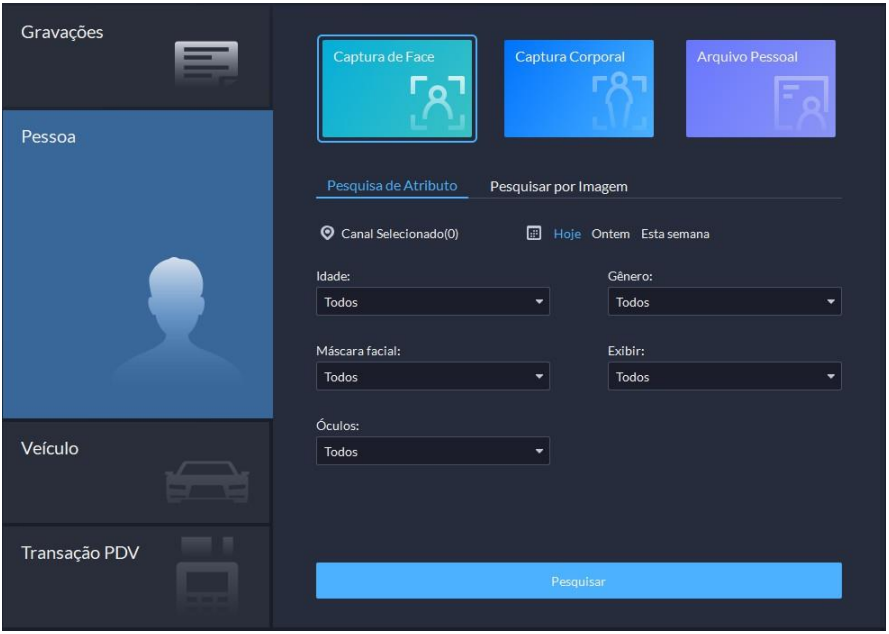
12.1. Procurando pessoas

Com base nas condições de pesquisa visualizar registros de captura de rostos, corpos e outras informações.

Procedimento:

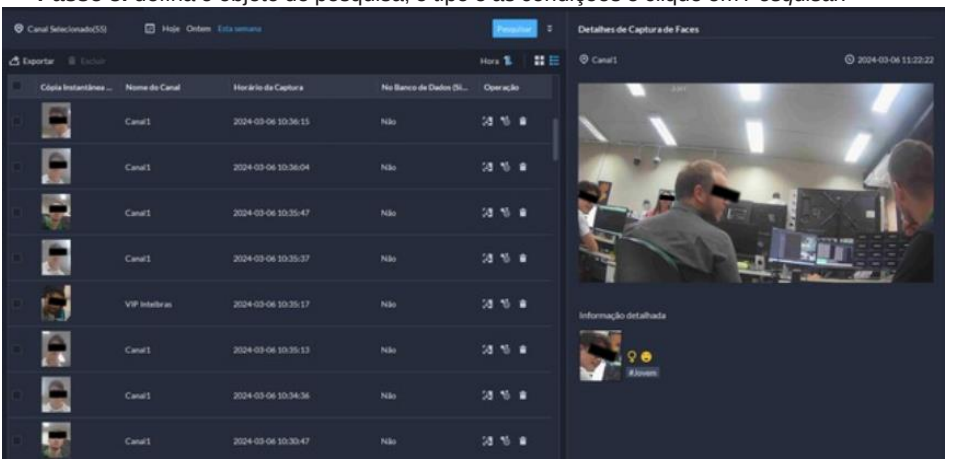
» **Passo 1:** faça o login no Defense. Na Página inicial, clique em e selecione DeepXplore.

» **Passo 2:** clique em e selecione *Pessoa.*



» **Objeto de pesquisa:**
  » **Captura facial:** pesquise registros no banco de captura facial.
  » Captura corporal: pesquise registros no banco de dados de captura corporal.
  » Arquivo Pessoal: pesquise registros no banco de dados de informações pessoais.
» **Tipo de pesquisa:**
  » **Pesquisa de atributos:** pesquise registros pelos recursos definidos, como idade, sexo, cor da roupa, identificação e muito mais.
  » **Pesquisar por Imagem:** pesquise os registros pela imagem enviada, e somente os registros acima da Semelhança definida serão exibidos.
  » **Canal de Pesquisa:** selecione os canais do dispositivo dos registros clicando em Canal Selecionado.
  » **Tempo de Pesquisa:** selecione o período de tempo dos registros de Hoje, Ontem e esta Semana.

» **Passo 3:** defina o objeto de pesquisa, o tipo e as condições e clique em *Pesquisar.*



  » Clique  ao lado do registro para adicioná-lo aos registros temporários.

  » Você pode passar o mouse sobre a pequena imagem à direita e clicar  para procurar imagens semelhantes a esta. A plataforma irá comparar a imagem que você carrega com os registros e as imagens em grupos de comparação de rostos e, em seguida, retornar resultados com base na similaridade definida.

  » Você também pode clicar  para adicioná-lo a um grupo de comparação de rostos. Depois de enviar o grupo aos dispositivos e configurar um evento, os dispositivos poderão disparar alarmes quando o rosto for reconhecido.

  » Clique  para excluí-los um por um.
  » Clique em *Exportar* para exportar registros para o armazenamento local.

» **Passo 4:** selecione um registro e, no lado direito, você poderá ver os detalhes. Clique na imagem do vídeo para visualizar a gravação vinculada.

Clique  no canto superior direito para visualizar todos os registros adicionados aos registros temporários. Dentro dele, você pode clicar  para visualizar a trilha alvo e clicar  para remover o registro do banco.

» **Passo 5:** volte para Pesquisando pessoas e clique em *Arquivo de pessoas.*
» **Passo 6:** digite o ID, nome ou número do cartão da pessoa que você deseja procurar.
» **Passo 7:** clique duas vezes na gravação.

Você pode ver a captura de rosto, captura de veículo, registros de acesso e outras informações da pessoa correspondente.

12.2. Procurando Veículos

Procedimento:

» **Passo 1:** faça o login no Defense. Na Página inicial, clique em  e selecione *DeepXplore.*

» **Passo 2:** clique em  e selecione *Veículo.*

» **Objeto de pesquisa:**

» **Captura de Veículos:** busca por registros no banco de dados de captura de veículos.

» **Arquivo de Veículos:** pesquise registros no banco de dados de informações de veículos.

» **Tipo de pesquisa**

» **Pesquisa de atributos:** pesquise registros pelos atributos definidos, como veículo cor e marca.

» **Pesquisa por imagem:** pesquisa registros pela imagem enviada e apenas registros acima do conjunto Similaridade será exibida.

» **Canal de pesquisa:** selecione canais de dispositivos dos registros clicando em Canal Selecionado.

» **Tempo de pesquisa:** selecione o período de tempo dos registros de Hoje, Ontem e Esta Semana. Disponível apenas para registros de captura de veículos.

» **Condições de pesquisa:** defina condições de pesquisa como número da placa (número completo da placa opcional), marcas do veículo, nome do proprietário e muito mais para pesquisar registros específicos.

» **Passo 3:** defina as condições de pesquisa e clique em *Pesquisar.*

Para o resultado da pesquisa, você pode realizar as seguintes operações.

» Clique  ao lado de Pesquisar para alterar as condições de pesquisa.

» Clique  para alterar a organização dos registros.

» Clique  ao lado do registro para adicioná-lo aos registros temporários.

» Clique  ao lado do registro para excluí-lo um por um ou selecione os registros e clique em *Excluir* para excluí-los em lotes.

» Clique em Exportar para exportar registros para o armazenamento local.

» **Passo 4:** selecione um registro e, no lado direito, você poderá ver os detalhes. Clique na imagem do vídeo para visualizar a gravação vinculada.

Clique  no canto superior direito para visualizar todos os registros adicionados aos registros temporários. Dentro dele, você pode clicar  para gerar o rastreamento alvo e clicar  para remover o registro do banco.

12.3. Procurando por Ocorrências de PDV

Você pode pesquisar transações de PDV por palavras-chave e campos de PDV.

Procedimento:

» **Passo 1:** faça login no cliente DSS. Na página inicial, selecione  > *DeepXplore* > *DeepXplore* > *Ocorrências POS.*

» **Passo 2:** configure o campo POS.

1. Clique em *Configuração de campo POS.*
2. Configure um campo POS para seu campo de recibo e clique  para habilitá-lo.
3. Clique em *OK.*

» **Passo 3:** configure as condições de pesquisa.

1. Configure as informações que deseja pesquisar.
   - » **Informações POS:** palavras-chave nas informações da transação. Isto pode ser usado com um ou mais campos POS ao mesmo tempo.
   - » **Campos POS:** os campos POS que você configurou no passo 2 serão utilizados para buscar determinadas informações nas transações. Por exemplo, o campo POS para preço total é TTL, então a plataforma obterá o número do TTL e retornará os resultados.
2. Selecione os canais PDV, configure o período e clique em *Pesquisar.*

» **Passo 4:** gerencie os resultados da pesquisa.

» **Ver detalhes.**

Selecione uma transação e então você poderá visualizar as informações detalhadas e o vídeo no momento da transação à direita.

Se precisar de vídeo no momento da transação, você deverá vincular canais POS com canais de vídeo e configurar planos de gravação para os canais de vídeo.

» **Adicionar a um caso.**

1. Clique  em uma transação para adicioná-la à biblioteca temporária.
2. Clique  no canto superior direito.
3. Selecione uma ou mais transações e clique em *Adicionar ao caso.*
4. Selecione um caso e clique em *OK.*

Na biblioteca temporária, selecione uma ou mais transações e clique  para removê-las. Esta operação apenas os removerá da biblioteca temporária, mas não os excluirá.

» **Ver trilha.**

1. Clique  em uma transação para adicioná-la à biblioteca temporária.
1. Clique  no canto superior direito.
1. Selecione transações e clique em  . A plataforma abrirá uma página e exibirá o rastreamento com base nas transações que você selecionar.

12.4. Adicionando banco de caso

Dentro do banco de casos, você pode integrar os registros de face, placa, acesso e muito mais em um caso completo, além de configurar detalhes dele para futuras investigações. A plataforma suporta o armazenamento de até 10.000 caixas.

Pré-requisitos:

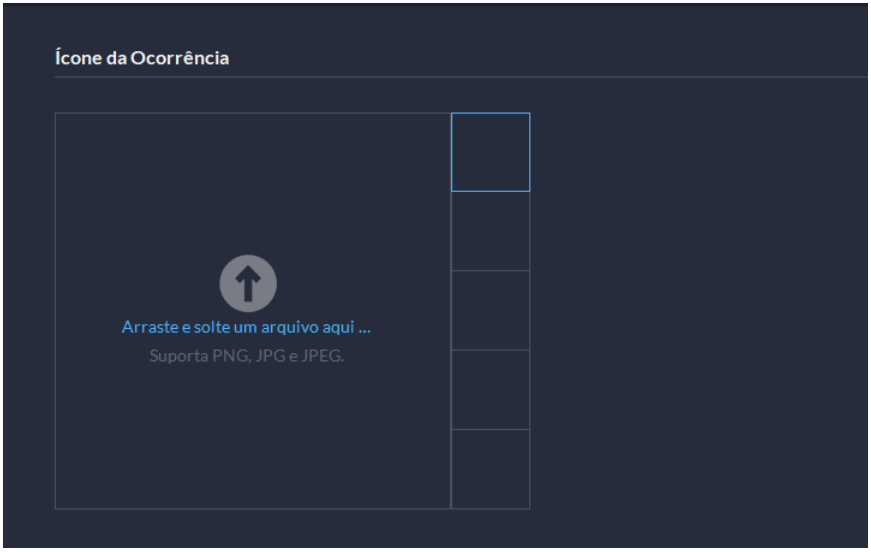
Os arquivos do caso só podem ser armazenados no disco *Arquivo de Incidentes.* Certifique-se de ter configurado esse tipo de disco antecipadamente.

Usuários com acesso ao *Banco de Caso:*

- **Super administrador:** visualize, edite e exclua arquivos de incidentes.
- **Administrador:**
  - Visualize arquivos de incidentes criados por eles próprios e por usuários comuns. Não há acesso aos arquivos de incidentes de outros administradores.
  - Edite e exclua arquivos abertos.
  - Não é possível editar ou excluir arquivos fechados.
- **Usuário comum:**
  - Só pode visualizar arquivos criados por eles próprios.
  - Edite e exclua arquivos abertos.
  - Não é possível editar ou excluir arquivos fechados.

Procedimento:

- **Passo 1:** faça login no Defense Na Página inicial, clique em  e selecione DeepXplore.
- **Passo 2:** clique em  .
- **Passo 3:** clique em *Adicionar* para adicionar um novo caso.
- **Passo 4:** Na seção Ícone do Caso, clique em um dos 5 quadrados pequenos, arraste o arquivo de imagem para o grande quadrado à esquerda ou passe o mouse sobre o quadrado grande, clique em  e carregue o arquivo de imagem. A imagem selecionada será exibida no canto superior esquerdo do caso que você exportar.



» **Passo 5:** selecione uma imagem do lado direito da seção *Ícone do Caso,* que estará localizada no canto superior esquerdo do arquivo do caso gerado. Você pode alterar o ícone arrastando a ima- gem do lado direito para a área esquerda da imagem.

» **Passo 6:** insira as informações básicas do caso.

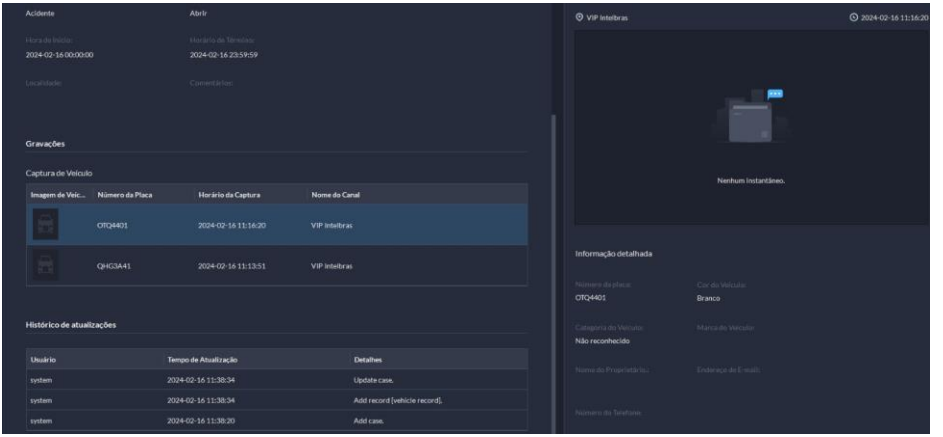
» **Tipo de caso:** usado para categorizar casos. Você pode clicar na lista suspensa para selecionar o tipo ou criar novos.

» **Status:** selecione o status do caso em Aberto e Fechado. A Plataforma integra casos em cada categoria de status.

» **Passo 7:** adicione registros, incluindo captura facial, captura corporal, ANPR, registro de acesso e muito mais.

Registros de outras categorias são adicionados da mesma forma. Nesta seção, tomamos a Captura de Rosto como exemplo.

1. Clique em *Adicionar em Captura de rosto.*
2. Selecione canais e horário e clique em *Pesquisar.* Você pode clicar no registro para visualizar seus detalhes.



3. Clique  ao lado do registro para adicioná-lo ao caso.
4. Clique  para voltar à página de adição de casos, você pode adicionar outros tipos de registros relacionados ao caso.

» **Passo 8:** role para baixo e clique em Adicionar em Anexo para fazer upload de imagens e vídeos relacionados ao caso.

» A plataforma suporta o upload de até 20 vídeos e cada vídeo não pode exceder 300 MB. O formato inclui dav, mp4, avi, fiv e asf.

» Até 20 imagens podem ser carregadas. O formato da imagem inclui png, jpg e jpeg.

O número de todos os arquivos de vídeo e imagens não pode ser superior a 20

» **Etapa 9:** clique em *OK.*

Operações Relacionadas

» **Excluir ou substituir um ícone:**

Passe o mouse sobre um pequeno quadrado e clique  para excluí-lo; clique em um quadrado pequeno e arraste um arquivo de imagem para o quadrado grande à esquerda ou passe o mouse sobre o quadrado grande,

clique em  e carregue o arquivo de imagem para substituí-lo.

» Insira o nome do caso na caixa de pesquisa no canto superior direito e pressione *Enter* ou clique  para pesquisar casos.

» Clique em  um caso temporário para visualizar os detalhes do caso. Se precisar editar os detalhes, clique em Editar e altere as informações conforme necessário.

» Clique em  um caso temporário para fazer o download ou clique em *Baixar na página de detalhes do caso.* Clique em *Progresso do download* no canto inferior esquerdo para verificar o progresso do download.

» Clique em  um caso para excluí-lo um por um ou selecione os casos e clique em *Excluir* para excluir em lotes.

12.5. Visualizando o rastreamento de dispositivos MPT

Pesquise e visualize o trajeto de um dispositivo MPT no mapa dentro do período definido.

Pré-requisitos:

» Configure o mapa vetorial.

» Adicione dispositivos MPT à plataforma.

» Dispositivos MPT enviam suas informações de GPS para a plataforma.

Procedimento:

» **Etapa 1:** faça login no Defense. Na página inicial, clique em e selecione *DeepXplore > MPT Track.*

» **Passo 2:** selecione um dispositivo MPT, configure a hora e clique em Pesquisar. A trilha do dispositivo MPT será exibida no mapa.

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