Defense IA
Manual

V01.2020

Defense IA

Software de monitoramento

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

O Software Defense IA é um sistema de vídeo monitoramento (VMS) que gerencia de forma unificada equipamentos de segurança eletrônica. Esse sistema é compatível com Câmeras, DVRs, NVRs e SVRs da Intelbras, podendo entregar o máximo disponível em nossos equipamentos. Com o Defense IA você pode gerenciar milhares de câmeras e gravadores, além de centralizar inteligências de ponta como Reconhecimento Facial, Leitura de Placas, Contagem de Pessoas, entre outros.

Prefácio

Geral

Este manual do usuário (doravante referido como Como "o manual") apresenta as funções e operações do Centro de Gerenciamento de Vigilância Geral do Defense IA (doravante referido como "o sistema" ou "a plataforma") e operações do cliente.

Instruções de segurança

Os seguintes símbolos abaixo com significados definidos abaixo podem aparecer no manual.

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

Histórico de Revisão

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.

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 oficial. 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.
- Todos 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 INSTALAÇÃO E IMPLANTAÇÃO

A plataforma Defense IA suporta tanto a implantação de servidor único quanto à implantação principal / subdistribuída.

1.1 REQUISITOS DO SERVIDOR

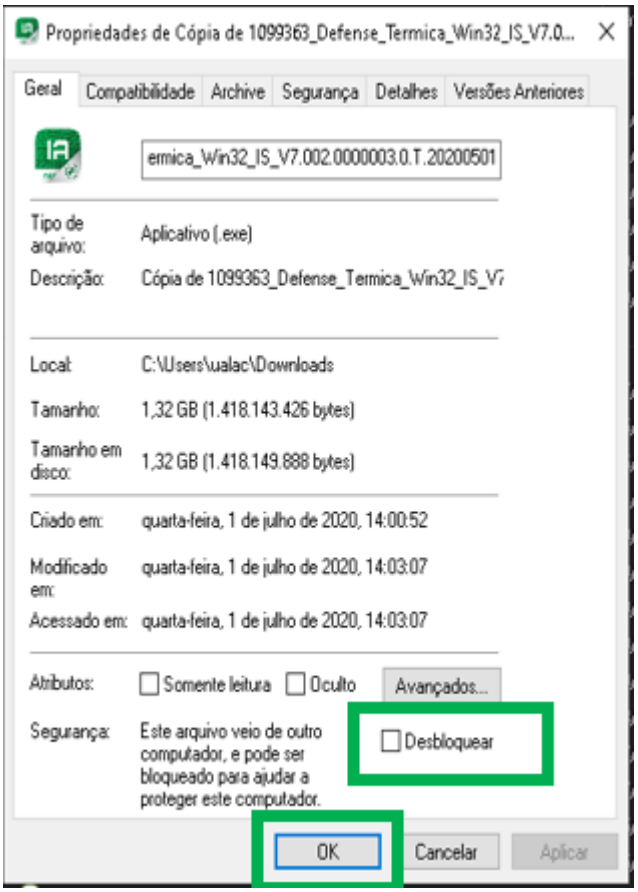
Tabela 1 - Requisito de hardware

Parâmetro	Requisitos de Hardware	Sistema operacional
Recomendado configuração	CPU: Processador Intel Xeon Silver 4114 @ 2.2 GHz 10 Core RAM: 16 GB Placa de rede: 4 portas Ethernet @ 1000 Mbps Tipo de disco rígido: HDD 1 TB Espaço do diretório de instalação: Em torno de 500 GB	Win10-64bit Servidor Windows 2008 Servidor Windows 2012 Servidor Windows 2016 Servidor Windows 2019
Mínimo configuração	CPU: E3-1220 v5@2.60GHz 4 Core Processor RAM: 8 GB Cartão de rede: 2 portas Ethernet @ 1000 Mbps Tipo de disco rígido: HDD 1 TB Espaço do diretório de instalação: Em torno de 500 GB	Win10-64bit

1.2 INSTALANDO O SERVIDOR PRINCIPAL

Passo 1. Desbloqueie o arquivo “.zip” antes da descompactação.

Figura 1 - Desbloqueio o arquivo “.zip”

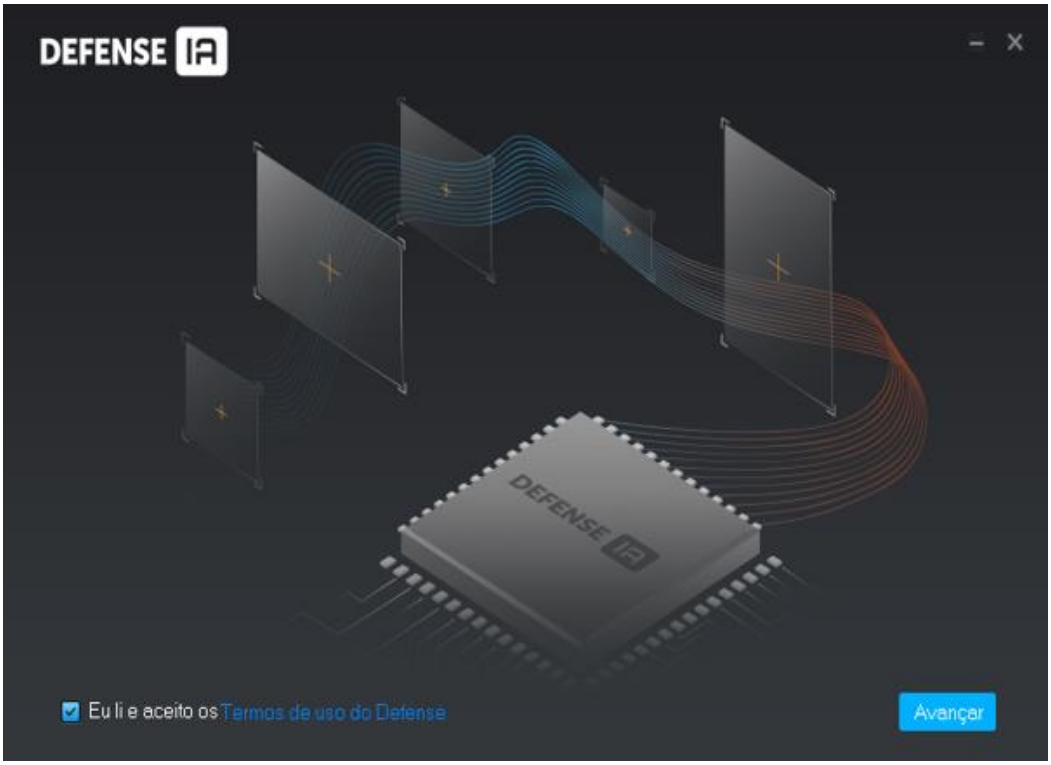


Passo 2. Extraia o arquivo completo e execute o defense.exe como administrador.

I.

- O nome do programa inclui o número da versão e os dados do programa, confirme antes da instalação.

Figura 2 - Interface de instalação



Passo 3. Clique em Termos de uso do Defense, leia e marque a caixa de seleção. Clique em Avançar.

Figura 3 - Selecione o tipo de servidor

Passo 4. Selecione o tipo de servidor e clique em Avançar.

- Selecione **Master** para o servidor atual de sua plataforma ou o servidor principal na implantação distribuída do sistema.

Figura 4 - Selecione o caminho de instalação

Passo 5. Selecione o caminho de instalação. Você pode clicar em Procurar para personalizar o diretório de instalação.

- Após selecionar o diretório de instalação, o sistema exibe o espaço necessário e o espaço livre atual.

- Não é recomendado que você instale a plataforma no Disco C porque recursos como o reconhecimento de rosto exigem um desempenho de disco superior.
- Se o botão Instalar estiver cinza, verifique se o diretório de instalação está correto ou se o espaço livre é maior que o necessário.
-

Passo 6. Clique em Instalar.

- O processo de instalação leva cerca de 3 a 5 minutos.

Passo 7. Clique em Executar.

- O botão iniciar é exibido após a conclusão da instalação.

Passo 8. Selecione uma placa de rede e clique em OK.

- A interface de configuração de segurança é exibida.

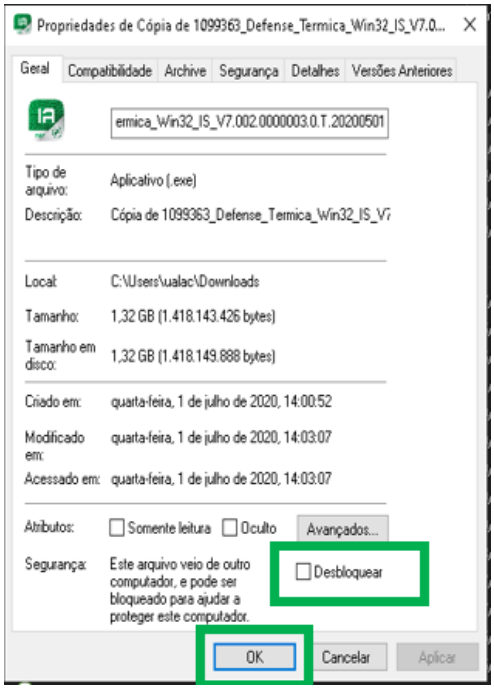
Passo 9. Ative ou desative o protocolo TLS1.0 conforme necessário.

Passo 10. Clique OK.

1.3 INSTALANDO SUB SERVER

Passo 1. Desbloqueie o arquivo ".zip" antes da descompactação.

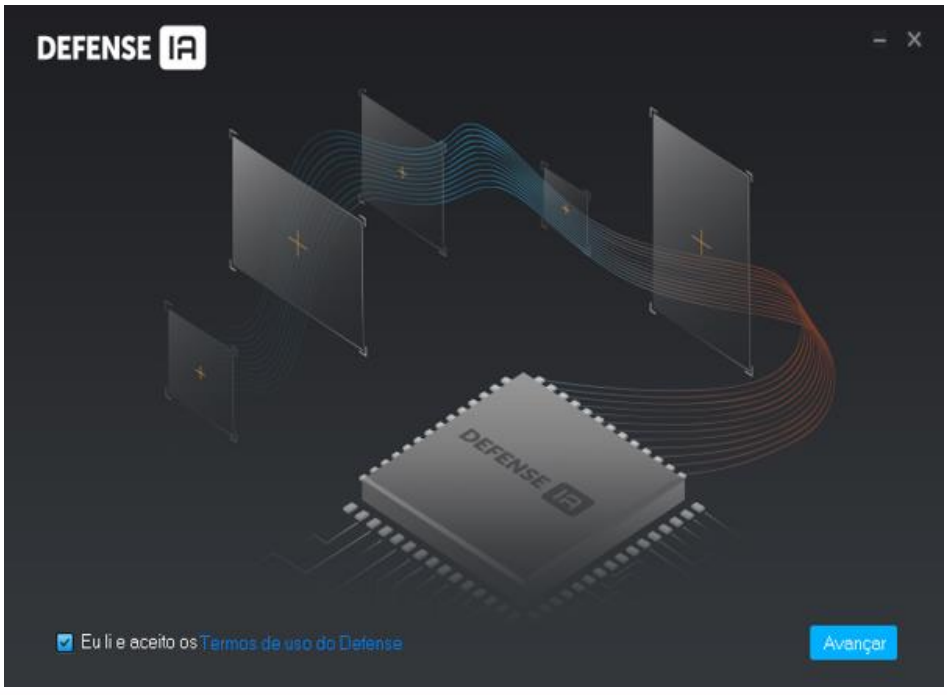
Figura 5 - Desbloqueio o arquivo ".zip"



Passo 2. Extraia o arquivo completo e execute o defense.exe como administrador.

- O nome do programa inclui o número da versão e os dados do programa, confirme antes da instalação.

Figura 6 - Interface de instalação



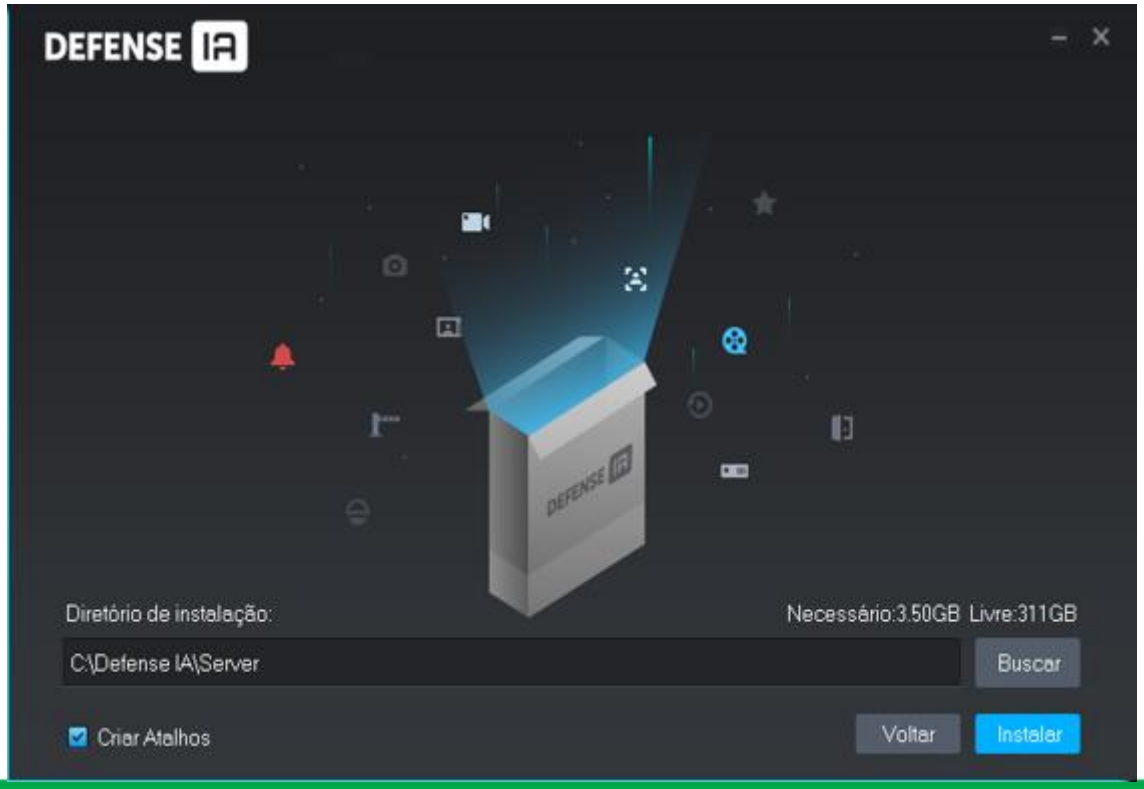
Passo 3. Clique em Termos de uso do Defense, leia e marque a caixa de seleção. Clique em Avançar.

Figura 7 - Selecione o tipo de servidor

Passo 4. Selecione o tipo de servidor e clique em Avançar.

- Selecione **Slave** se o servidor atual for um sub servidor.

Figura 8 - Selecione o caminho de instalação



Passo 5. Selecione o caminho de instalação. Você pode clicar em Procurar para personalizar o diretório de instalação.

II. Após selecionar o diretório de instalação, o sistema exibe o espaço necessário e o espaço livre atual.

- Não é recomendado que você instale a plataforma no Disco C porque recursos como o reconhecimento de rosto exigem um desempenho de disco superior.
- Se o botão Instalar estiver cinza, verifique se o diretório de instalação está correto ou se o espaço livre é maior que o necessário.

Passo 6. Clique em Instalar.

- O processo de instalação leva cerca de 3 a 5 minutos.

Passo 7. Selecione a placa de rede necessária e clique em OK.

Passo 8. Configure as informações do servidor principal no sub-servidor.

III. Duplo clique  no sub servidor.

IV. Clique  no canto superior direito da interface.

V. Defina IP central, IP local e cada número de porta e clique em OK.

- Digite o endereço IP do servidor principal na caixa Center IP e os números da porta do servidor principal nas caixas de número da porta.
- Insira o endereço IP do sub-servidor e o endereço IP WAN na caixa IP local e na caixa IP de mapeamento.

Se os endereços IP e portas forem válidos, os serviços do sub servidor serão reiniciados.

1.4 GERENCIANDO SERVIÇOS DE PLATAFORMA

Visualize o status do serviço, inicie ou pare os serviços e modifique as portas do serviço.

Faça login no servidor e clique duas vezes  .

Figura 9 - Interface de gerenciamento de serviço

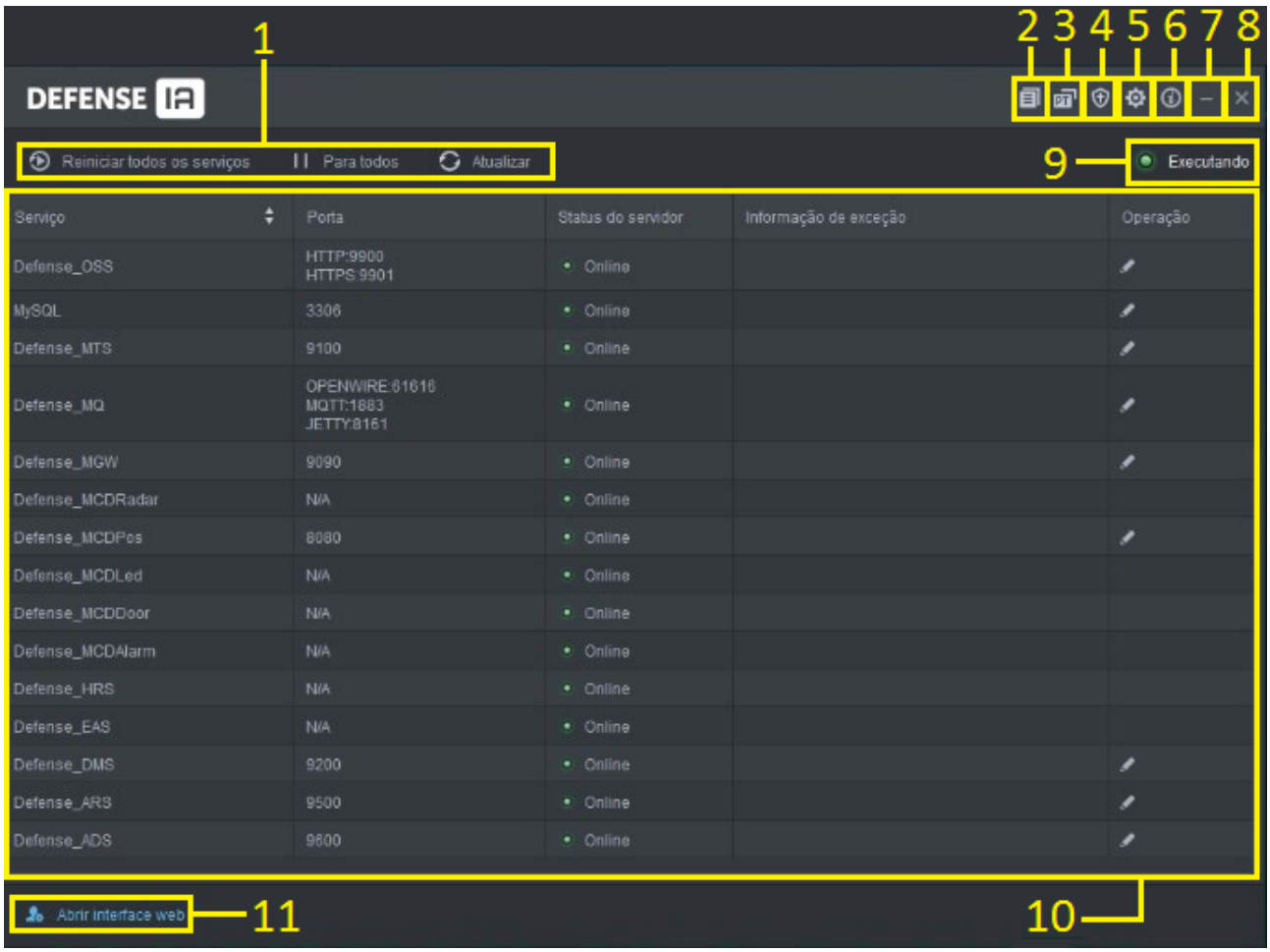


Tabela 2 - Parâmetros

Nº.	Função	Descrição
1	Gestão de Serviços	Gerenciamento de serviços, ele suporta os seguintes três tipos de operação: Clique em “Reiniciar todos os serviços” para reiniciar todos os serviços. Clique em “Para todos” para interromper todos os serviços. Clique em “Atualizar” para atualizar os serviços.
2	Manual de usuário	Acesso ao manual do usuário.
3	Idioma	Mudar de idioma.
4	Configuração de segurança	Ative ou desative o protocolo TSL 1.0. O protocolo TSL 1.0 não é um protocolo de segurança e é recomendado que seja fechado. Se o protocolo TLS 1.0 estiver desabilitado, certifique-se de que o navegador tenha acesso adequado à plataforma. Para habilitar TLS1.1 e TLS 1.2, abra seu navegador e busque em Configurações.
5	Configuração	Habilita o IP do servidor como plataforma IP CMS. Se a rede deve passar por LAN e WAN, você precisa inserir o IP WAN na caixa de IP de mapeamento.
6	Sobre	Informação da versão do software.
7	Minimizar	Minimize a interface.
8	Fechar	Fechar o Defense IA.
9	Status do serviço	Iniciando (metade verde) Indisponível: Exceção de serviço (vermelho completo) Parando (metade vermelho) Executando: O serviço está funcionando normalmente (verde completo) Parado. (cinza)
10	Serviços	Exibe cada serviço e status do serviço. Clique no lápis para modificar o número da porta de serviço e os serviços serão reiniciados automaticamente após a modificação.
11	Abrir Administrador Cliente	Vai para o Gerenciador Web que é usado pelos administradores do sistema.

1.5 CONFIGURANDO LAN OU WAN

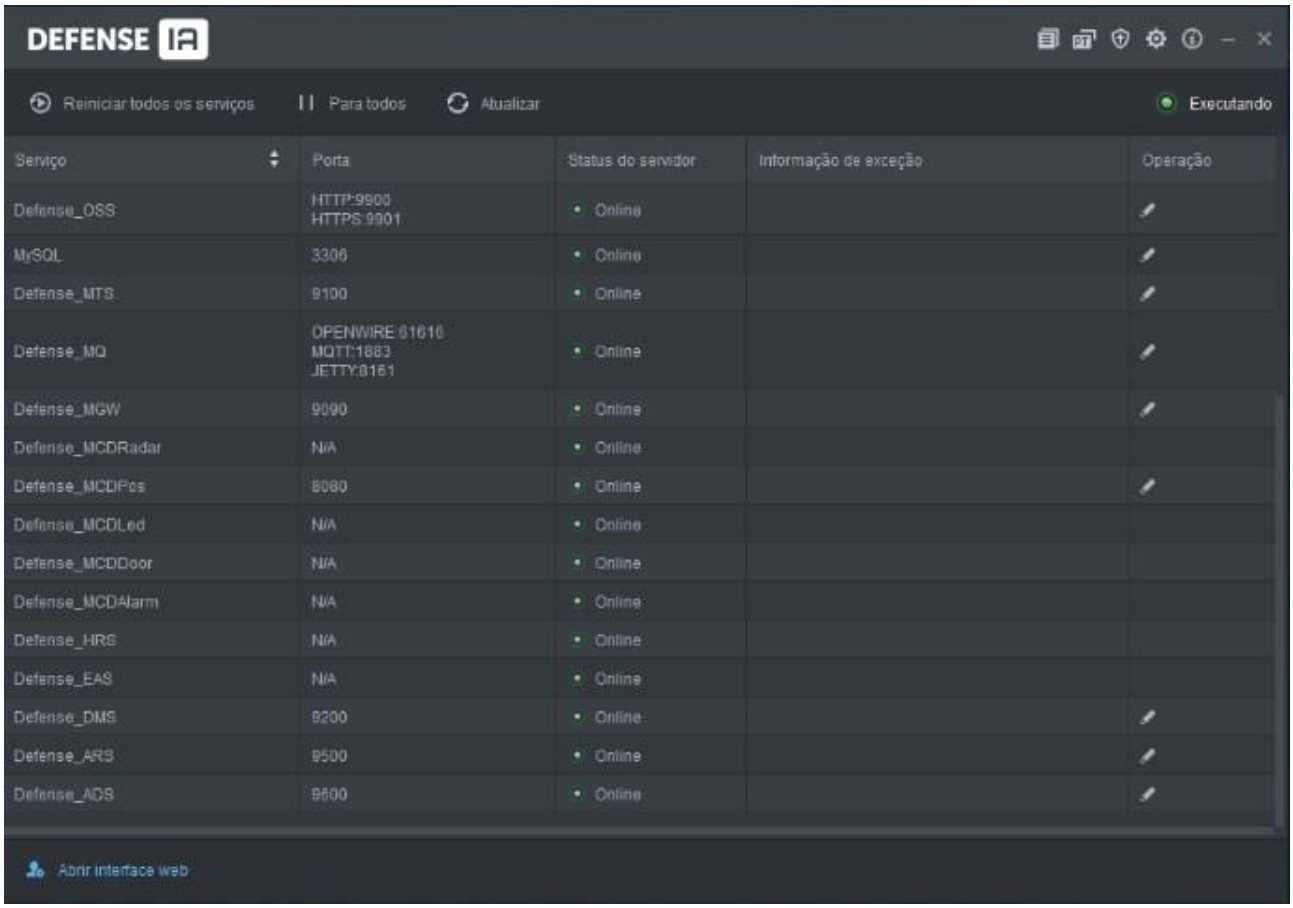
1.5.1 Configurando o roteador

Se a plataforma estiver em uma rede local, para acessá-lo via rede pública, você precisa fazer o mapeamento da porta. Para a lista de portas que precisam ser mapeadas, veja "**Erro! Fonte de referência não encontrada.** Introdução ao Módulo de Serviço".

1.5.2 Configurando a plataforma Defense IA

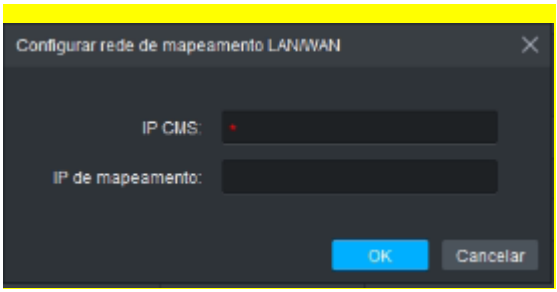
Passo 1. Faça login no servidor Defense IA e clique duas vezes  .

Figura 10 - Estado dos serviços



Passo 2. Clique na  no canto superior direito.

Figura 11 - Configuração



Passo 3. Insira o endereço WAN na caixa IP de Mapeamento e clique em OK.

Passo 4. Clique em OK e reinicie os serviços.

1.6 DESINSTALANDO A PLATAFORMA

Passo 1. No servidor, vá para o diretório de serviço "...\Defense IA\Server\uninstall" e clique duas vezes em "uninst.exe".

Passo 2. Clique em Sim.

Passo 3. Clique em Concluir

2 CONFIGURAÇÕES BÁSICAS

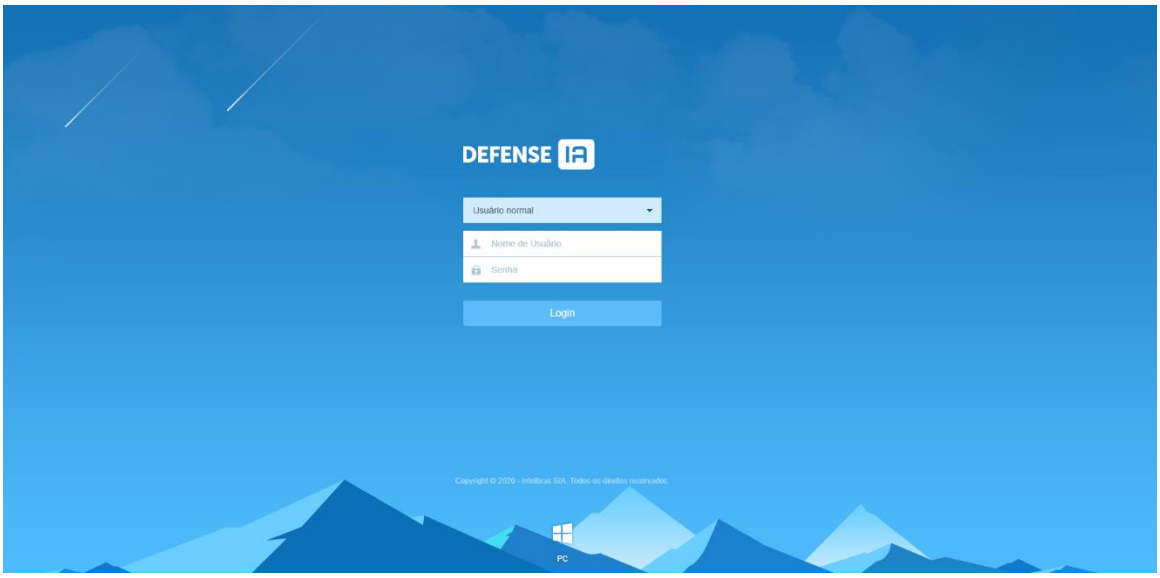
Defina as configurações básicas das funções do sistema antes de usá-las, como ativação do sistema, organização e gerenciamento de dispositivos, criação de usuário, planejamento de armazenamento e gravação e configuração de regras de eventos. As configurações básicas são feitas no Gerenciador Web, o cliente web do Defense IA. Para logar no Gerenciador Web, são recomendados os navegadores Google Chrome 70 ou superior, Firefox 56 ou superior e IE 11.

2.1 LOGIN NO GERENCIADOR WEB

Acesse o Gerenciador Web via navegador para executar configuração remota de o sistema.

Passo 1. Insira o endereço IP da plataforma no navegador e pressione Enter.

Figura 12 - Faça login no Gerenciador Web

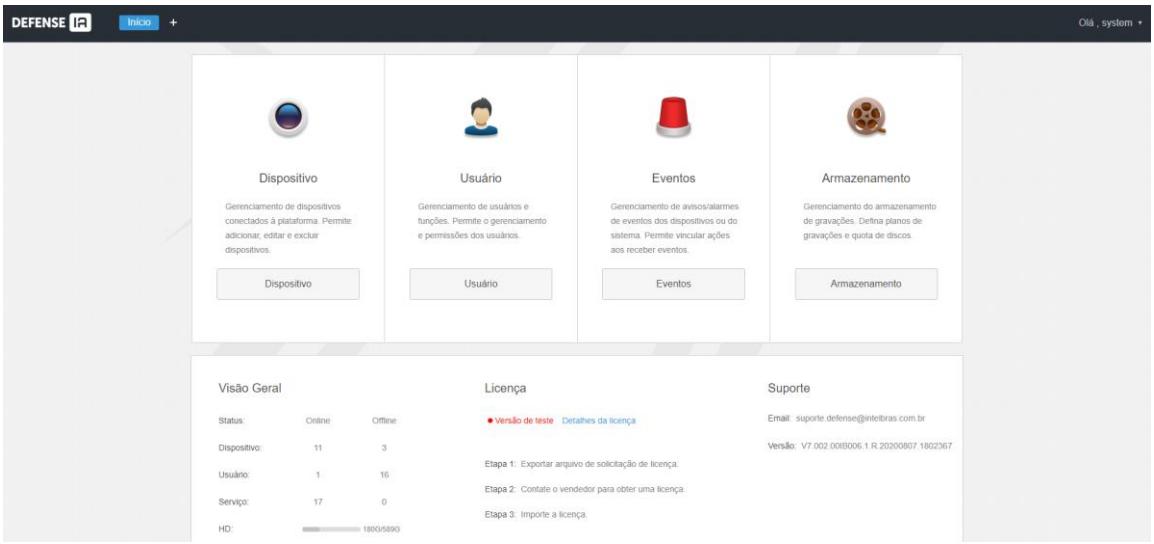


Passo 2. Digite o nome de usuário e a senha e clique em Login.

O nome de usuário padrão é system.

- O sistema abrirá a interface de modificação de senha se for a primeira vez em que se faz login no sistema. Pode-se continuar a fazer login no sistema depois que a senha for modificada a tempo.
- Adicione o endereço IP da plataforma nos sites confiáveis do navegador se for a primeira vez que você se conecta ao Defense IA Gerenciador Web.

Figura 13 - Página inicial



- Posicione o mouse ponteiro no nome de usuário em canto superior direito, e então você pode modificar a senha ou fazer logoff do usuário atual.
- O atalho de acesso dos módulos gerais é exibido na parte superior da interface, clique + na página inicial para apresentar todos os módulos e abrir novos módulos.
- Visão geral: exibe o status online / offline dos dispositivos, usuários e serviços, e a proporção de uso do disco rígido.
- Licença: Ativar ou atualizar a licença, verificar os detalhes da licença.

2.2 ATIVANDO A PLATAFORMA

Ative a plataforma com uma licença de teste ou paga na primeira vez que fizer login nela. Caso contrário, você não pode usá-lo.

Esta seção apresenta a capacidade da licença, como solicitar uma licença, como usar a licença para ativar a plataforma e como renovar sua licença.

2.2.1 Capacidade de licença

- Uma licença de teste oferece capacidade limitada e expira em 90 dias.
- Para adquirir capacidade total e uso permanente, você deve comprar uma licença formal.
- Depois de ativar a primeira licença paga, se quiser aumentar sua capacidade de licença, você pode comprar mais códigos de licença. Para por exemplo, se você tem 500 canais atualmente, pode comprar outros 500 canais. Depois de ativar os novos 500 canais, você terá 1.000 canais no total.

- A versão oficial ativada não pode ser rebaixada para uma versão de teste.

2.2.2 Solicitando uma licença

Para obter uma licença, entre em contato com o executivo de vendas da Intelbras.

2.2.3 Ativando ou Atualizando Licença

Ative a plataforma com uma licença de teste ou formal para o primeiro login. Caso contrário, você não pode usar a plataforma.

Durante o uso da plataforma, você também pode atualizar sua licença de teste ou formal com uma nova, de modo a obter maior capacidade ou uso mais longo.

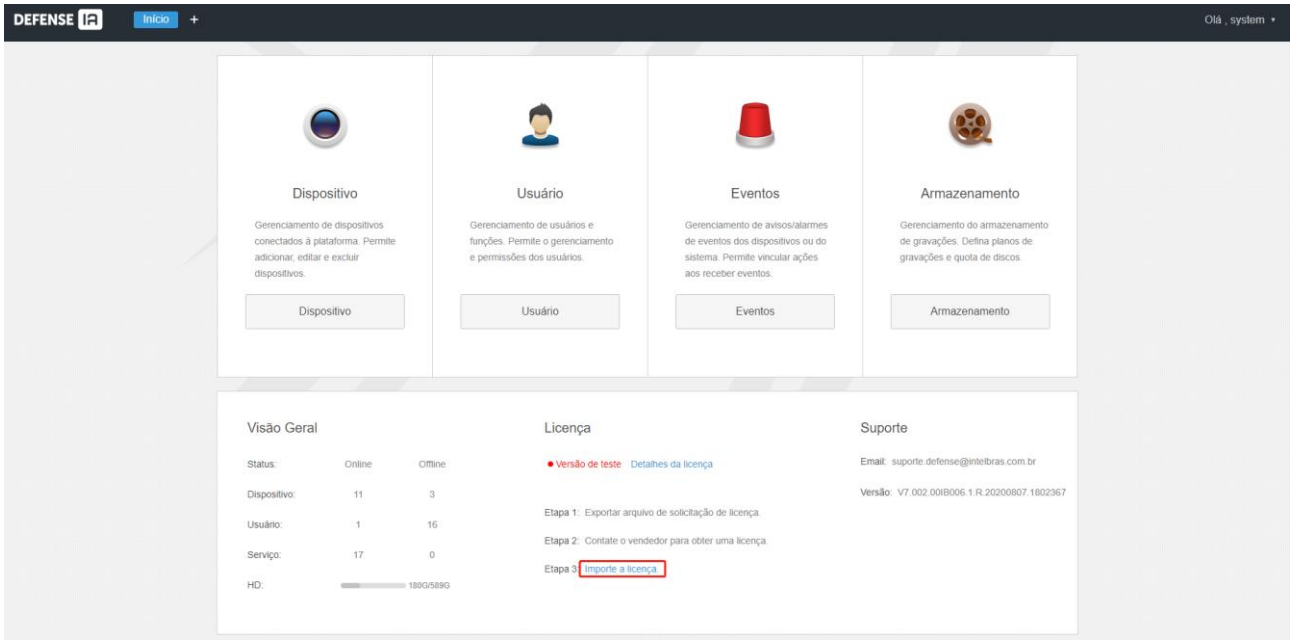
Para ativar ou atualizar sua licença, consulte os procedimentos a seguir.

VI. 🕮

- Os procedimentos de ativação e atualização da licença são os mesmos. Esta seção considera a ativação da licença como exemplo. A interface real deve prevalecer.

Na interface inicial do Gerenciador Web, clique em Importar licença.

Figura 14 - Licença de atualização

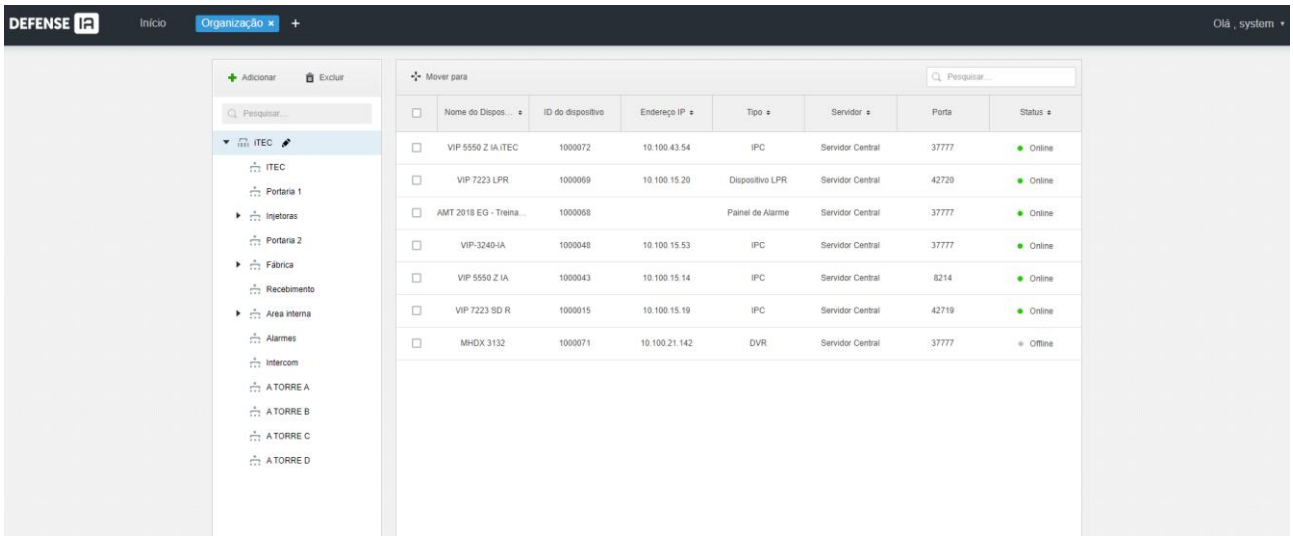


2.3 ADICIONANDO ORGANIZAÇÃO

Classifique os dispositivos por organização lógica para facilitar o gerenciamento.

Passo 1. Faça login no Gerenciador Web. Clique + e selecione Organização na interface da nova guia.

Figura 15 - Dispositivo organização



Passo 2. Selecione o nó raiz da árvore do dispositivo à esquerda e clique em Adicionar para adicionar novas organizações no nó raiz.

Figura 16 - Adicionar uma organização

Passo 3. Insira o nome da organização e pressione Enter.

Operações

- Mover dispositivo: Selecione o dispositivo na organização raiz, clique em Move To, selecione Nova Organização 1 e clique em OK.
- Editar: Clique no ao lado da organização e modifique o nome da organização.
- Excluir: selecione uma organização e clique em Delete.

2.4 GERENCIANDO DISPOSITIVOS

Adicione dispositivos antes de usá-los para monitoramento de vídeo. Esta seção apresenta como adicionar, inicializar e editar dispositivos e como modificar o endereço IP do dispositivo.

2.4.1 Procurando Dispositivos Online

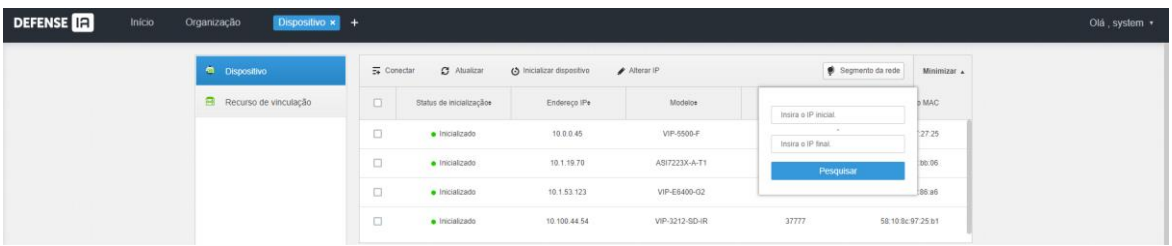
Pesquise dispositivos na mesma LAN com a plataforma antes de adicioná-los à plataforma.

Passo 1. Faça login no Gerenciador Web. Clique e selecione Dispositivo.

- A plataforma procura e exibe dispositivos na mesma LAN que o servidor da plataforma durante o primeiro uso.
- A plataforma procura e exibe dispositivos de acordo com o segmento de rede conforme definido da última vez, se não for o primeiro uso.

Passo 2. Clique em Segmento de rede.

Figura 17 - Definir segmento de rede



Passo 3. Digite o IP inicial e o IP final e clique em Pesquisar.

2.4.2 Inicializando dispositivos

Você precisa inicializar os dispositivos não inicializados antes de adicioná-los à plataforma.

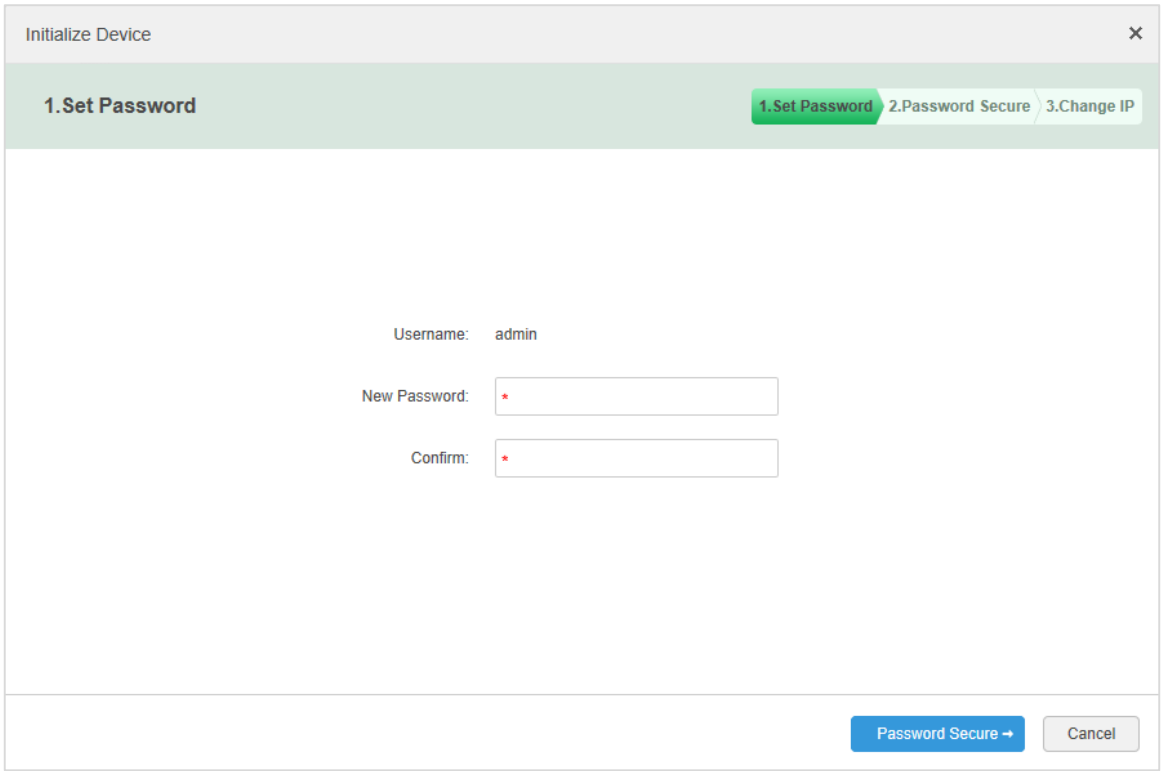
Passo 1. Faça login no Gerenciador Web. Clique e selecione Dispositivo.

Passo 2. Pesquise dispositivos. Vejo "2.4.1 Procurando Dispositivos Online"

Passo 3. Selecione um dispositivo não inicializado e clique em Inicializar.

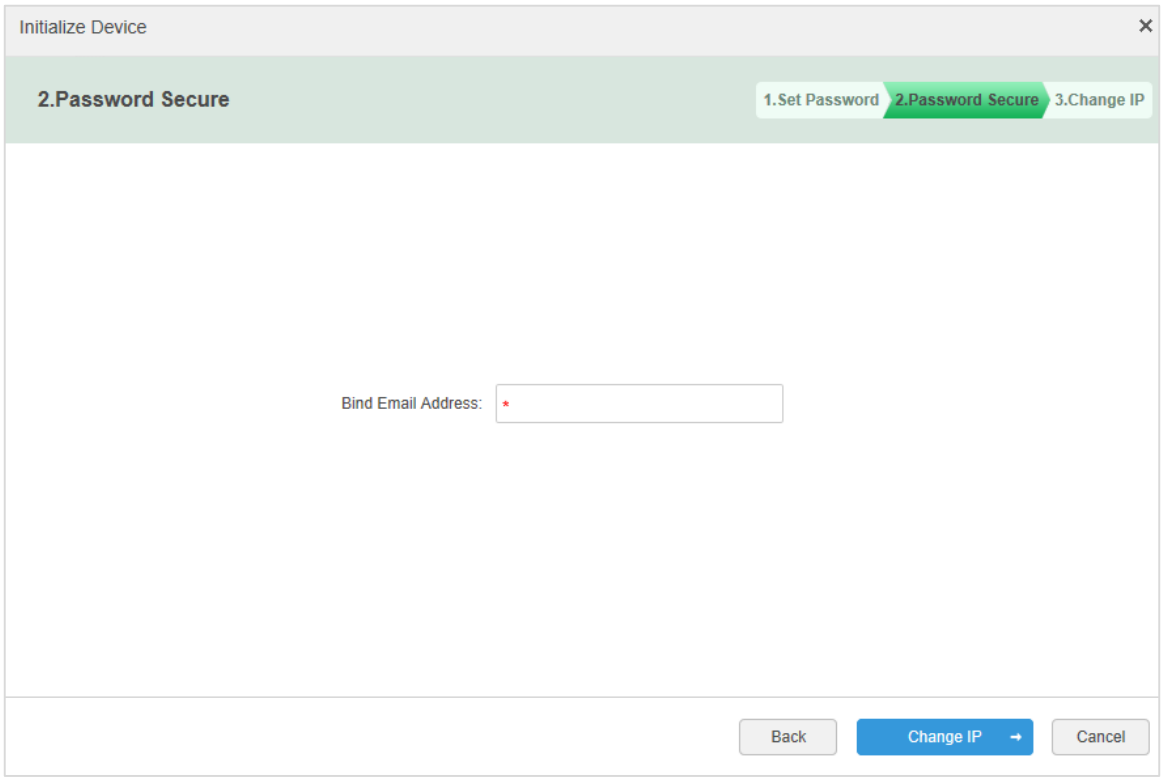
- Você pode selecionar vários dispositivos para inicializá-los em lotes. Certifique-se de que os dispositivos selecionados tenham o mesmo nome de usuário, senha e informações de e-mail.
- Clique ou ao lado de Status de inicialização para classificar rapidamente a coluna de status e, em seguida, você pode ver todos os dispositivos não inicializados.

Figura 18 - Configurar senha



Passo 4. Digite a senha e clique em Senha segura.

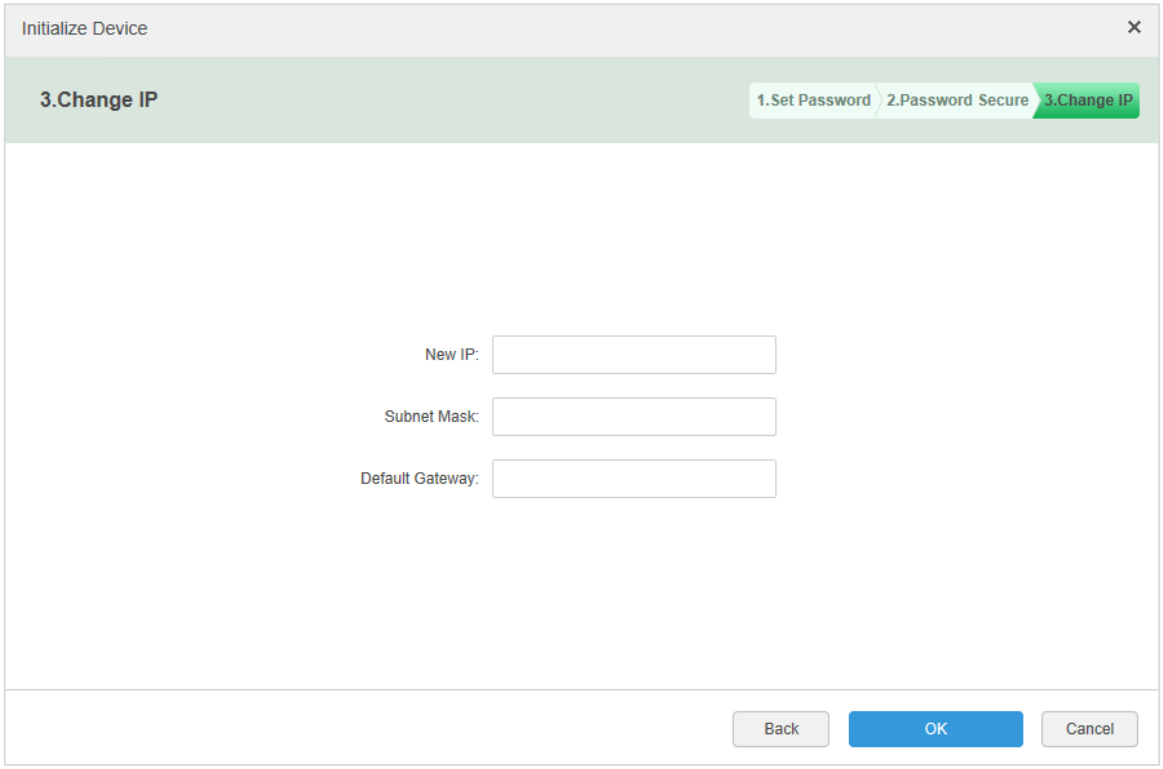
Figura 19 - Segurança de senha



Passo 5. Insira o endereço de e-mail e clique em Alterar IP.

- O e-mail é usado para receber o código de segurança para redefinir a senha.

Figura 20 - Alterar IP



Passo 6. Insira o endereço IP e clique em OK.

2.4.3 Modificando o endereço IP do dispositivo

Você pode modificar os endereços IP dos dispositivos que ainda não foram adicionados à plataforma.

Passo 1. Faça login no Gerenciador Web. Clique e selecione Dispositivo.

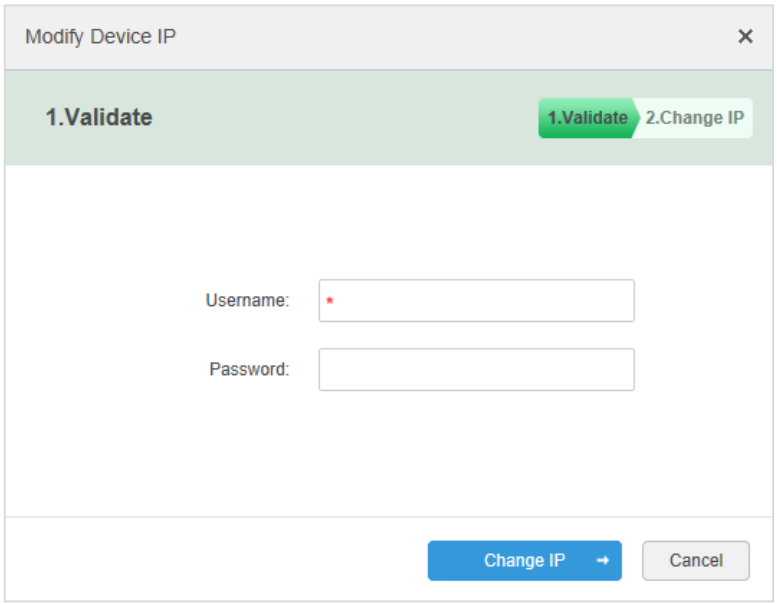
Passo 2. Pesquise dispositivos. Vejo "2.4.1 Procurando Dispositivos Online"

Passo 3. Selecione um dispositivo e clique em Alterar IP.

- Para dispositivos que têm o mesmo nome de usuário e senha, você pode selecionar e modificar seus endereços IP em lotes.

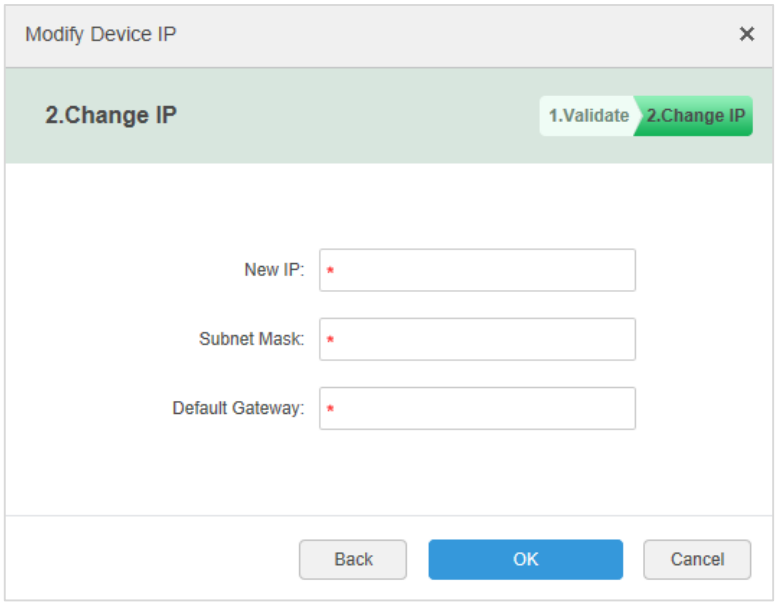
Passo 4. Modifique o endereço IP e clique em OK.

Figura 21 - Verificação



Passo 5. Insira o nome de usuário e a senha para fazer login no dispositivo e clique em Alterar IP.

Figura 22 - Alterar IP



Passo 6. Insira o endereço IP e clique em OK.

Passo 7. Clique OK.

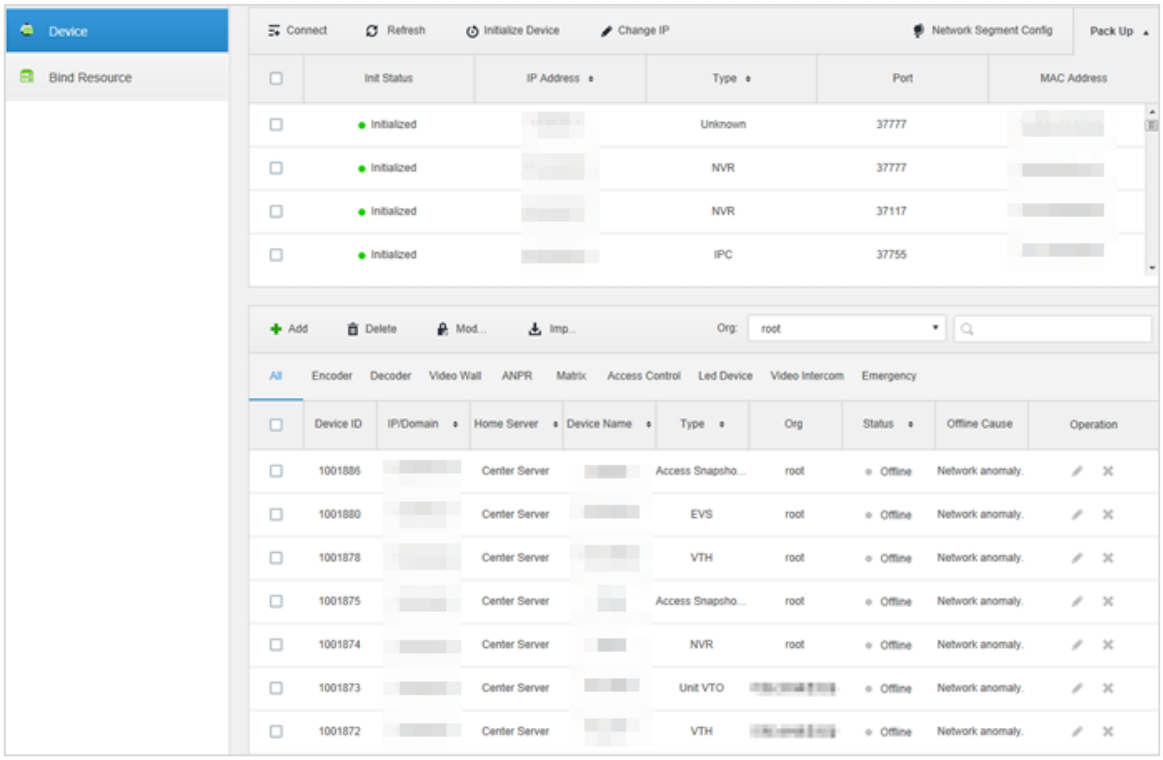
2.4.4 Adicionando Dispositivos

Você pode adicionar diferentes tipos de dispositivos, tal como encoder, decodificador, dispositivo LPR, controle de acesso, LED, vídeo porteiro e dispositivo de atendimento de emergência. Neste capítulo, é adicionado um encoder como exemplo. Para outros dispositivos, a interface de configuração real deve prevalecer.

2.4.4.1 Adicionando dispositivos um por um

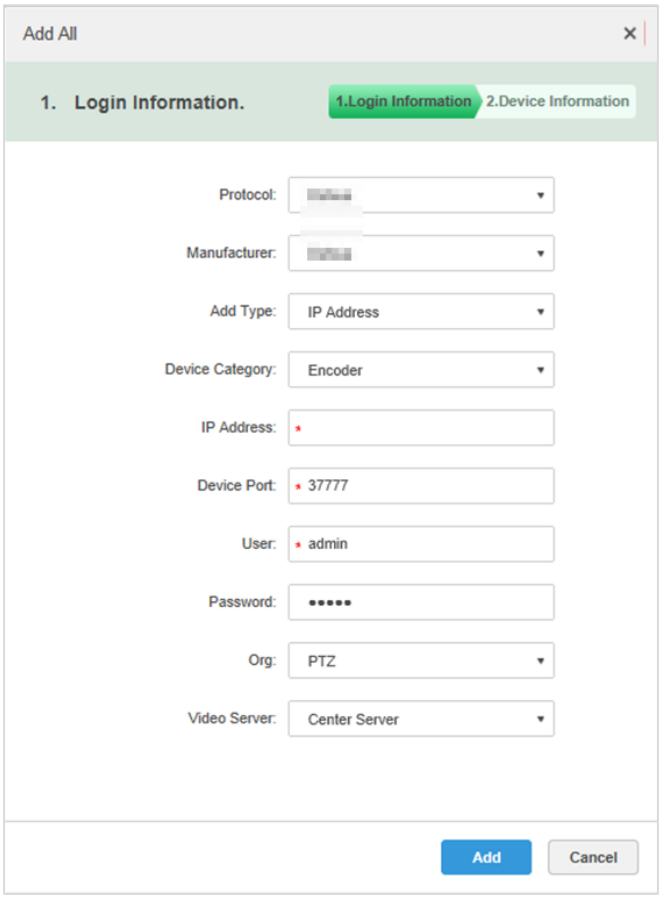
Passo 1. Clique + e selecione Dispositivo na interface Nova guia.

Figura 23 - Dispositivo



Passo 2. Clique em Adicionar.

Figura 24 - Adicionar um dispositivo (1)



Passo 3. Defina os parâmetros.

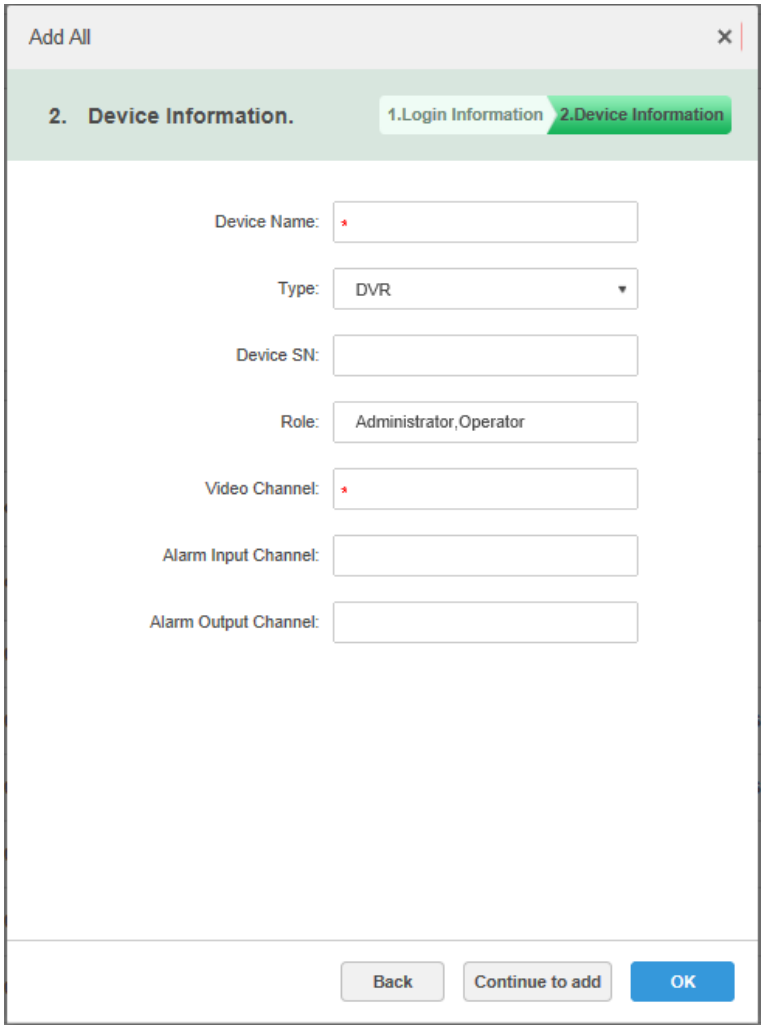
- Os parâmetros variam com os protocolos selecionados. A interface real deve prevalecer.
- Para adicionar uma central de alarme o protocolo deve ser **Intelbras** ao invés de **Intelbras-1**.

Na lista suspensa adicionar tipo,

- Quando a opção cadastramento automático é selecionada, insira o ID de registro do dispositivo. O método de registro automático serve apenas para adicionar encoders e dispositivos de alarme de emergência. O ID de registro automático deve estar de acordo com o ID registrado configurado no encoder. O número da porta deve ser o mesmo na plataforma e no dispositivo. A porta de registro automático é 9500 na plataforma por padrão. Para modificar, abra a ferramenta de configuração do sistema para modificar o número da porta DEFENSE_ARS.
- Quando a opção **Nome do domínio** é selecionada, as opções são de a domínio configurado durante a implantação.
- A opção **Seção de IP** pode ser utilizada para cadastramento de dispositivos em lote.
-

Passo 4. Clique em Adicionar.

Figura 25 - Adicionar um dispositivo (2)



Passo 5. Defina os parâmetros.

Passo 6. Clique OK.

Clique em Continuar para adicionar mais dispositivos.

2.4.4.2 Adicionar dispositivos por meio de pesquisa

Dispositivos na mesma LAN que o servidor da plataforma podem ser adicionados usando a função de pesquisa automática.

Passo 1. Clique + e selecione Dispositivo na interface Nova guia.

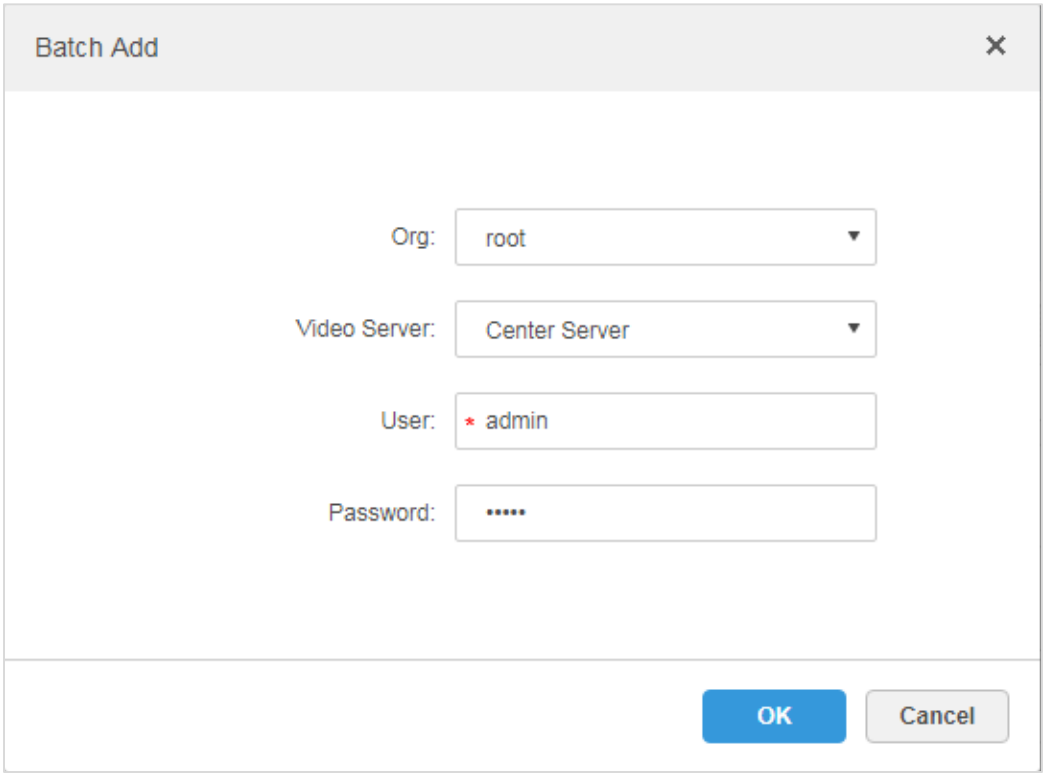
Passo 2. Pesquise dispositivos online.

Os resultados da pesquisa são exibidos.

Passo 3. Selecione o dispositivo que precisa ser adicionado e clique em Conectar.

- Você pode selecionar vários dispositivos para adicioná-los em lotes, se eles tiverem o mesmo nome de usuário e senha.

Figura 26 - Adicionar em lote



Passo 4. Defina os parâmetros e clique em OK.

O dispositivo é adicionado à organização correspondente.

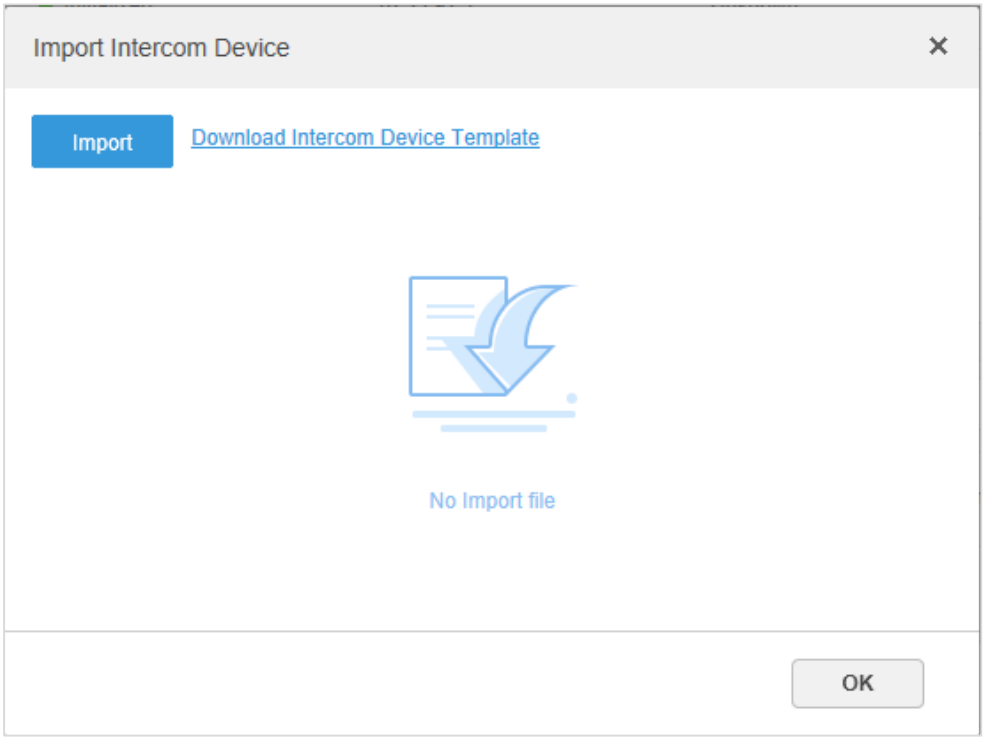
2.4.4.3 Importando dispositivo de intercomunicação de vídeo

Preencha o modelo do dispositivo de intercomunicação, e depois você pode adicionar dispositivos de intercomunicação em lotes.

Passo 1. Clique + e selecione Dispositivo na interface da Nova guia.

Passo 2. Clique em Importar.

Figura 27 - Importar dispositivos de intercomunicação de vídeo (1)



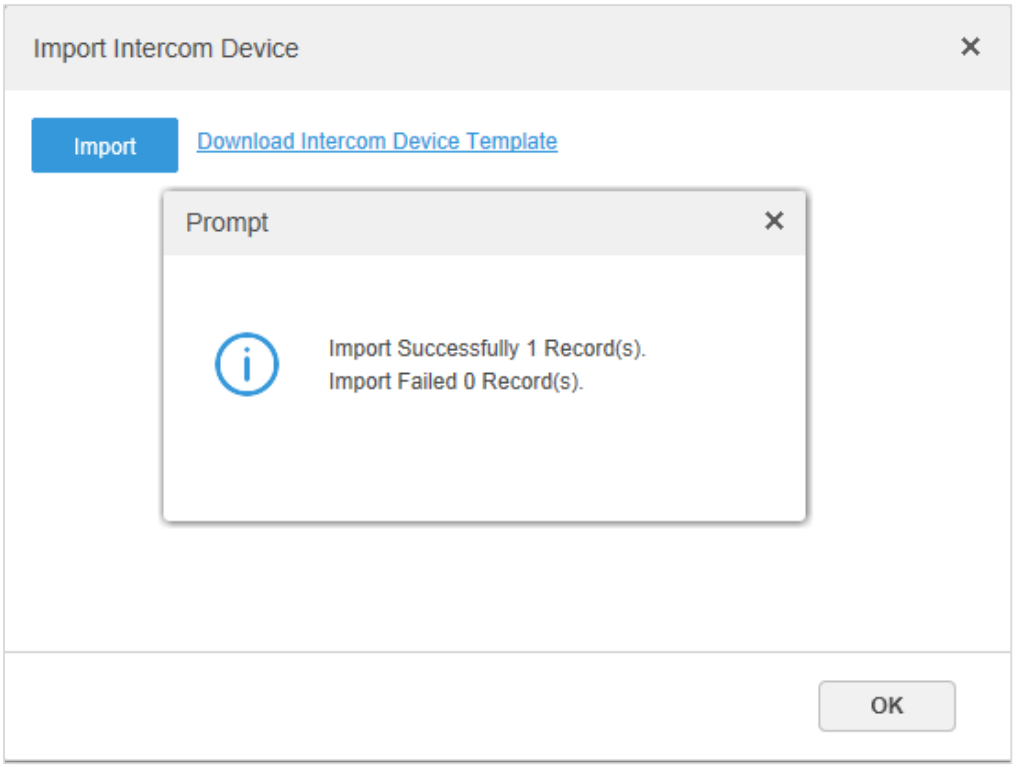
Passo 3. Clique em Baixar modelo de dispositivo de intercomunicação e salve o modelo no PC de acordo com as dicas de interface.

Passo 4. Preencha o modelo de acordo com a situação real da rede e salve as informações.

Passo 5. Clique em Importar e selecione o modelo preenchido de acordo com as dicas de interface.

- Se o dispositivo já estiver adicionado ao Defense IA, o sistema perguntará se deve cobrir o dispositivo existente. Você pode selecionar de acordo com a situação real.

Figura 28 - Importar dispositivos de intercomunicação de vídeo (2)



Passo 6. Clique ✕ e feche a caixa de prompt.

Passo 7. Clique OK.

2.4.5 Dispositivos de edição

Modificar informações e organização do dispositivo.

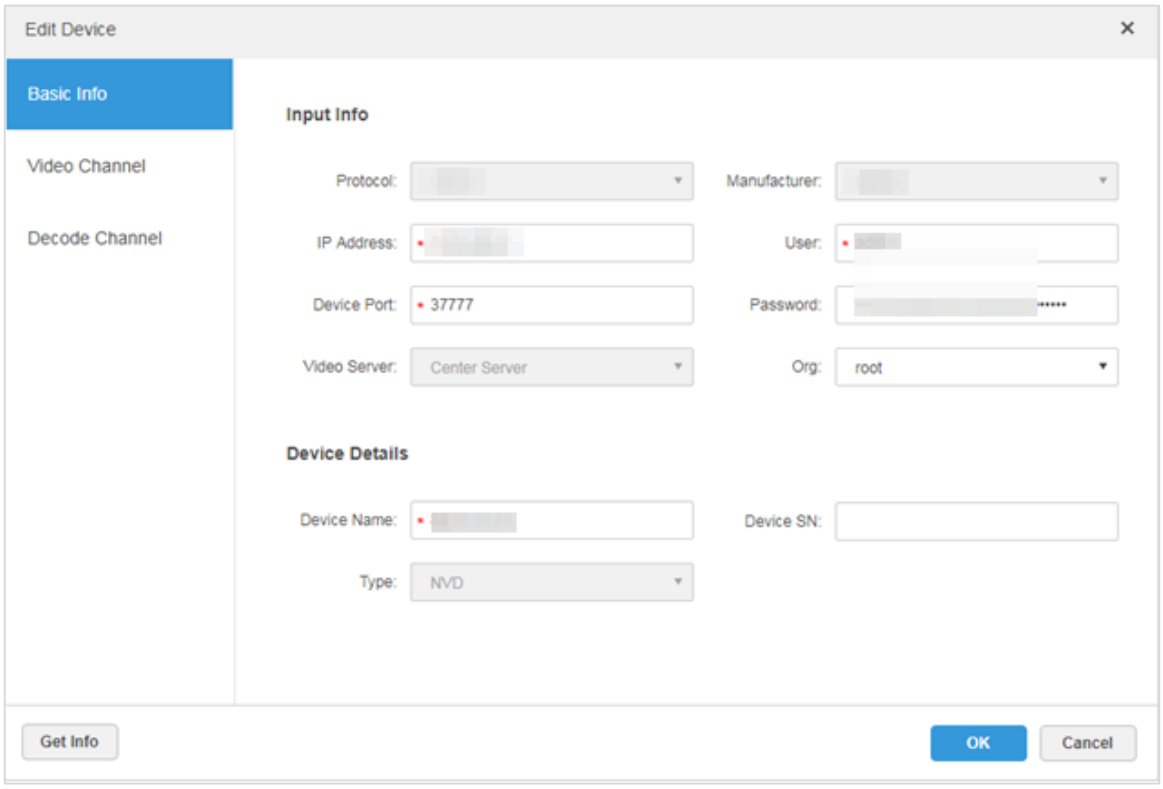
2.4.5.1 Modificando Informações do Dispositivo

Passo 1. Clique + e selecione Dispositivo na interface Nova guia.

Passo 2. Clique no correspondente da lista de dispositivos.

- Clique em Obter informações e o sistema sincronizará as informações do dispositivo.

Figura 29 - Informação básica

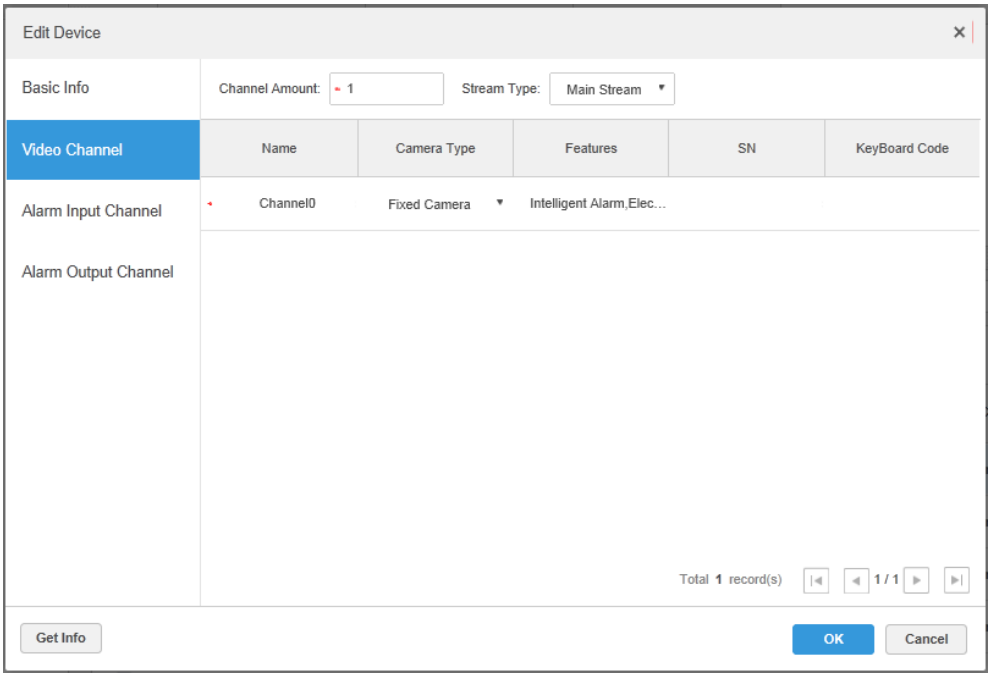


Passo 3. Modifique as informações básicas do dispositivo na interface de informações básicas.

Passo 4. Clique em Canal de vídeo e defina o nome do canal do dispositivo, recursos do canal, número de série, tipo de câmera e código do teclado.

- Diferentes tipos de dispositivos possuem diferentes recursos; a interface real deve prevalecer.
- Os recursos do dispositivo incluem alarme inteligente, fisheye, detecção facial, reconhecimento facial entre outras. Selecione os recursos de acordo com as características do dispositivo em questão.

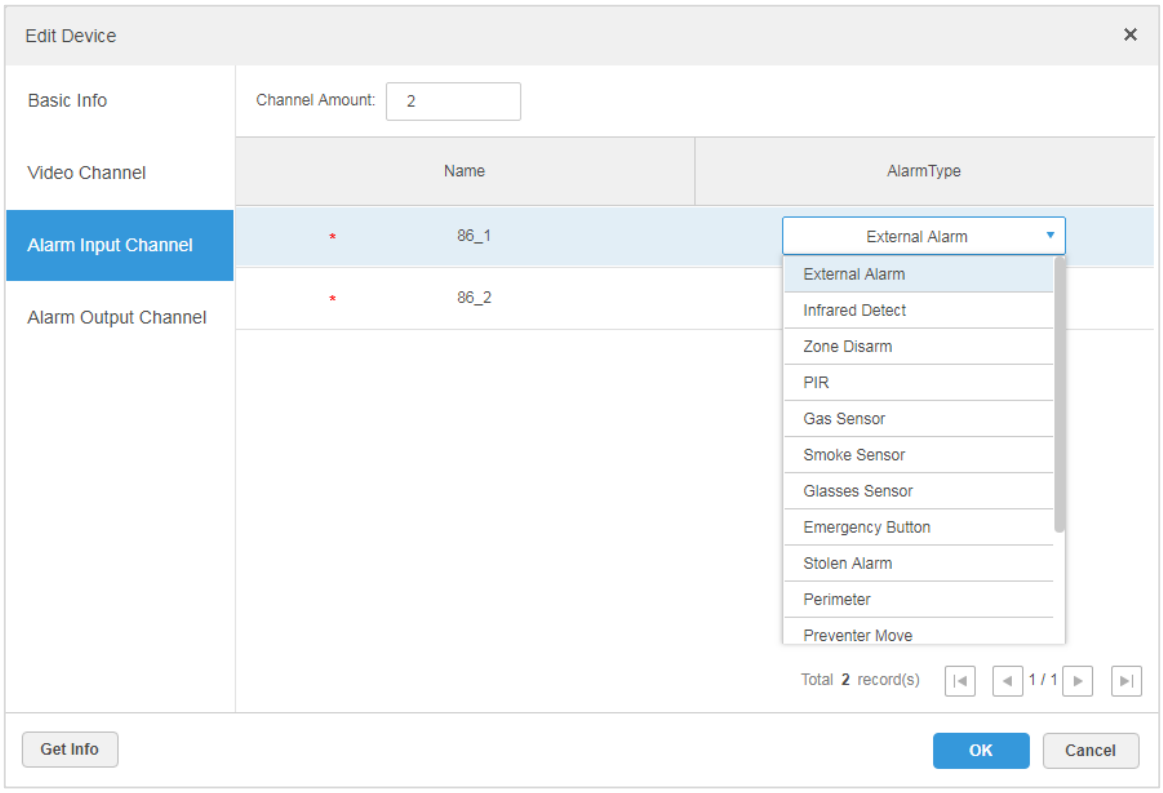
Figura 30 - Definir recursos do canal de vídeo



Passo 5. Clique na guia Canal de entrada de alarme e configure o nome do canal e o tipo de alarme de entrada de alarme.

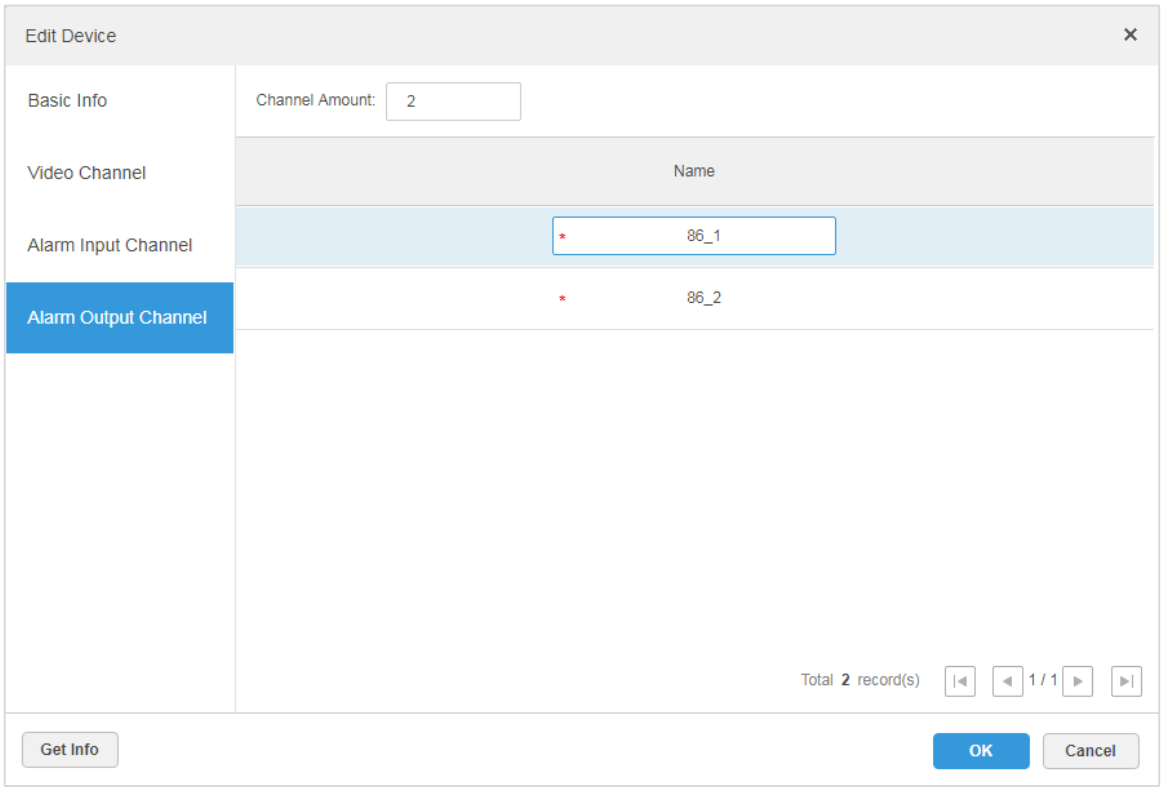
- Pule a etapa, a menos que os dispositivos adicionados suportem entrada de alarme.
- O canal de entrada de alarme do Painel de alarme tem sua configuração baseada em partições e zonas; os outros dispositivos utilizam Alarme externo como canal de entrada de alarme por padrão.

Figura 31 - Tipo de alarme



Passo 6. Clique na guia Canal de saída de alarme e modifique o nome do canal de saída de alarme.

Figura 32 - Modificar nome de saída de alarme



Passo 7. Clique em OK para terminar a modificação.

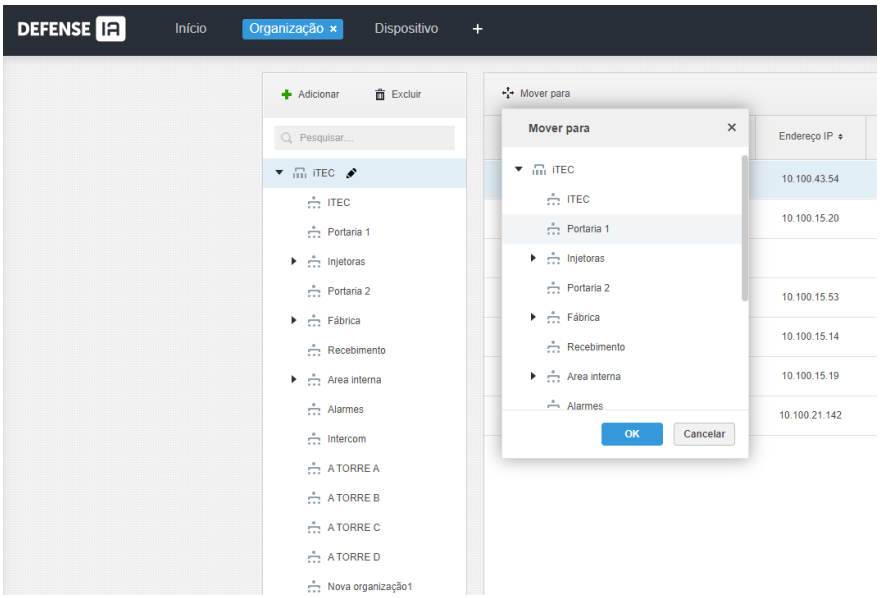
2.4.5.2 Modificando a Organização do Dispositivo

Você pode mover um dispositivo de um nó da organização para outro.

Passo 1. Clique . Na interface da Nova guia, selecione Organização.

Passo 2. Selecione um dispositivo a ser movido e clique em Mover para.

Figura 33 - Mover dispositivo



Passo 3. Selecione o nó da organização de destino e clique em OK.

2.4.6 Recursos de vinculação

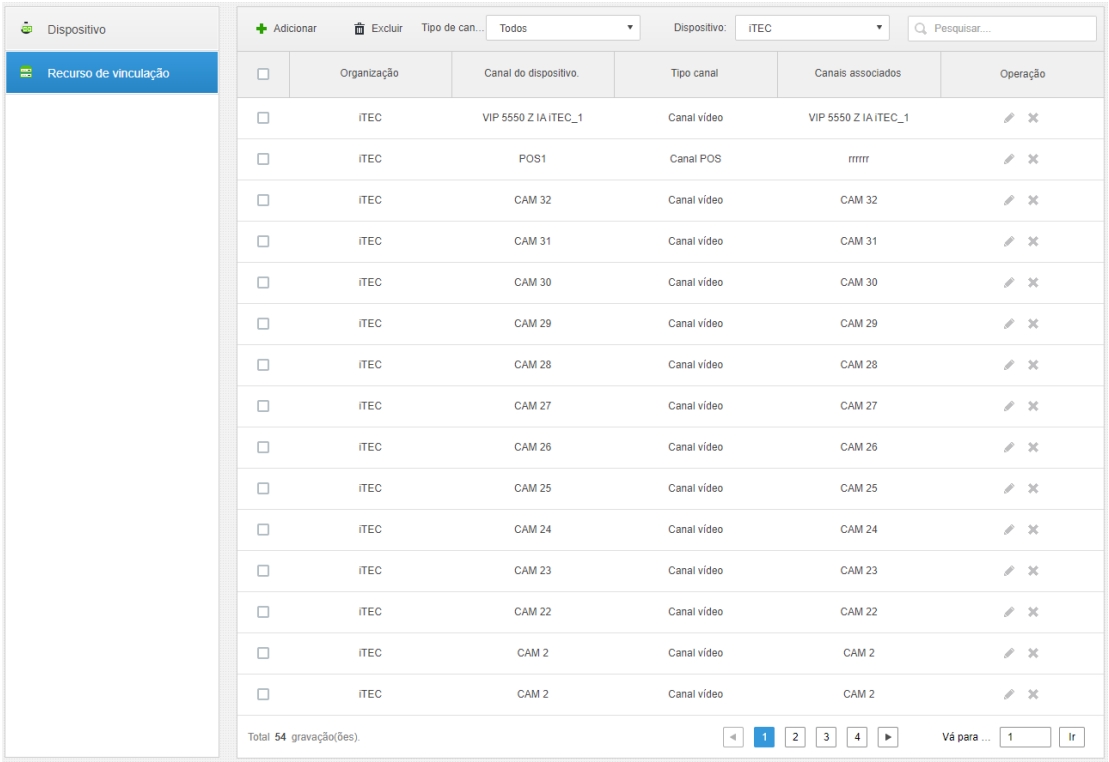
A plataforma suporta recursos de ligação para links ações. Você pode ligar um canal de vídeo com um canal de entrada de alarme, canal LPR, canal POS, canal de controle de acesso ou outro canal de vídeo, para que você possa ver o vídeo associado para eventos.

Adicionando recurso de vinculação

Passo 1. Faça login no Gerenciador Web. Clique e selecione Dispositivo.

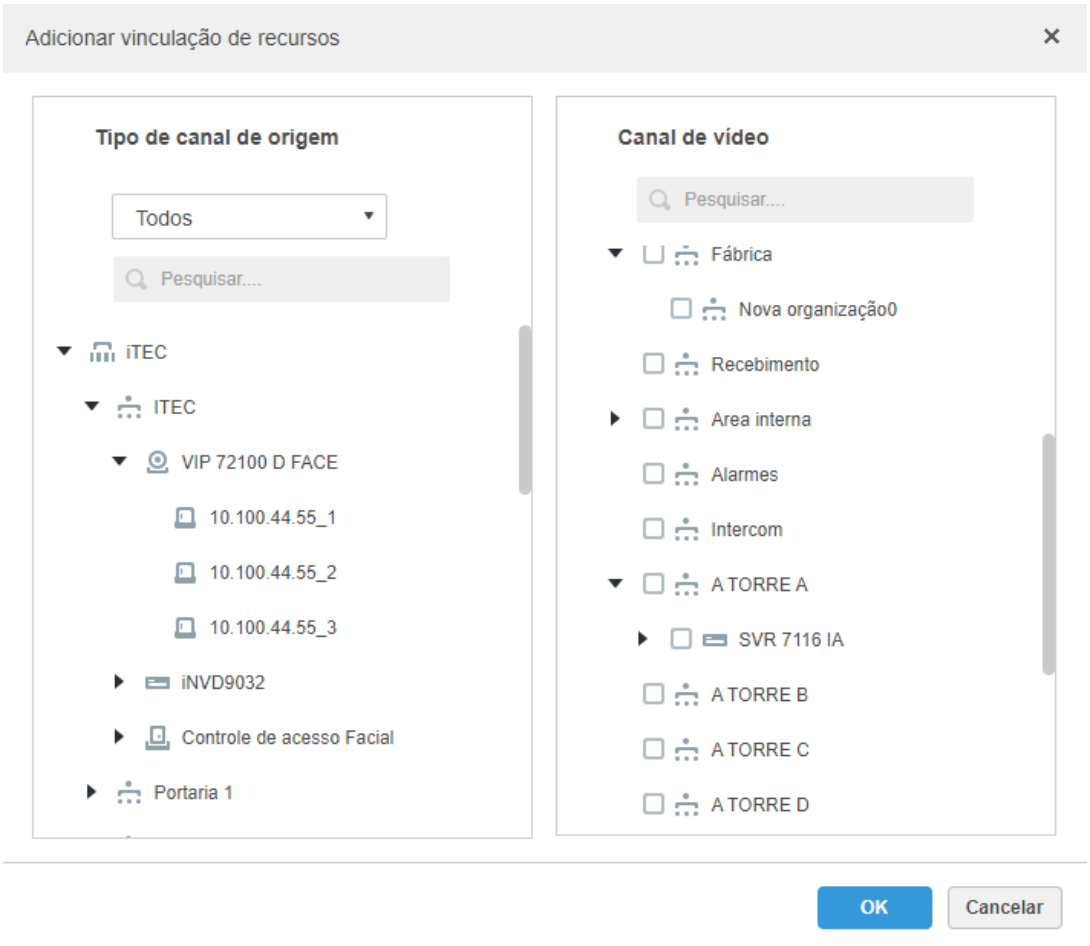
Passo 2. Clique em Vinculação de recursos.

Figura 34 - Recurso de vinculação



Passo 3. Clique em Adicionar.

Figura 35 - Adicionar recurso para vincular



Passo 4. Selecione o canal de origem e o canal de vídeo respectivamente e clique em OK.

2.5 ADICIONANDO FUNÇÃO E USUÁRIO

Usuários de funções diferentes têm permissões diferentes de acesso e operação do dispositivo. Ao criar um usuário, atribua uma função a ele para fornecer as permissões correspondentes.

2.5.1 Adicionando função de usuário

A função de usuário é um conjunto de permissões. Classifique usuários da plataforma em diferentes funções para que possam ter diferentes permissões para operar os dispositivos, funções e outros recursos do sistema.

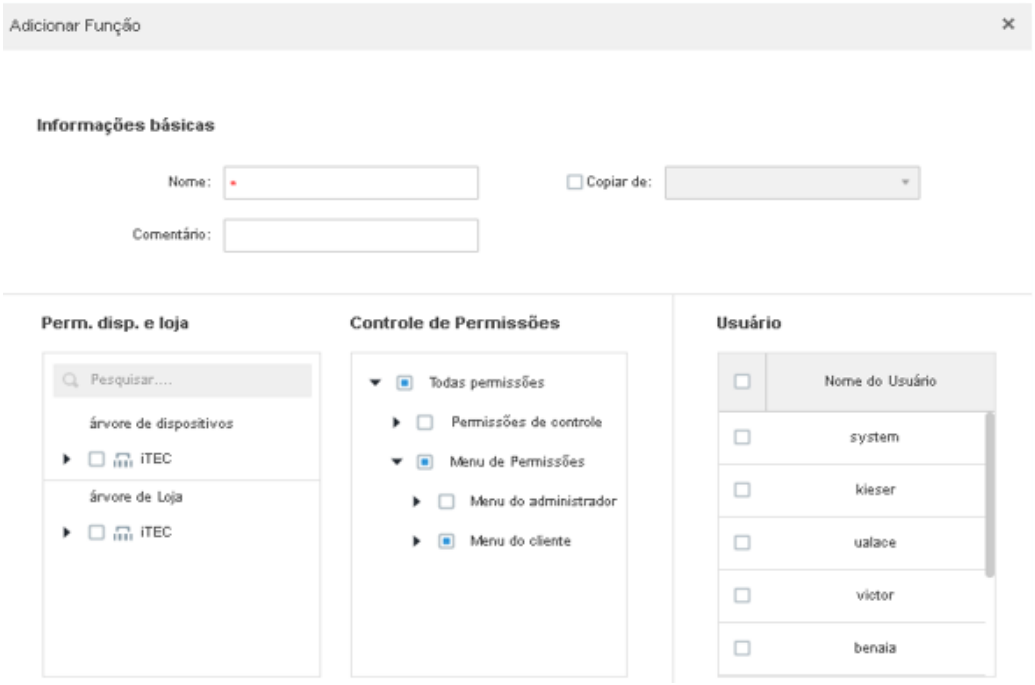
Passo 1. Faça login no Gerenciador Web. Clique + e selecione Usuário.

Passo 2. Clique na guia Função.

Passo 3. Clique em Adicionar, defina as informações da função e selecione o dispositivo e as permissões de controle e atribua a regra aos usuários.

- Selecione uma função na lista suspensa Copiar de para copiar as configurações para as regras selecionadas.
- Se nenhum dispositivo e permissões de controle forem selecionados para o usuário, este usuário não terá as permissões correspondentes.

Figura 36 - Adicionar uma função



Passo 4. Clique OK.

2.5.2 Adicionando usuário

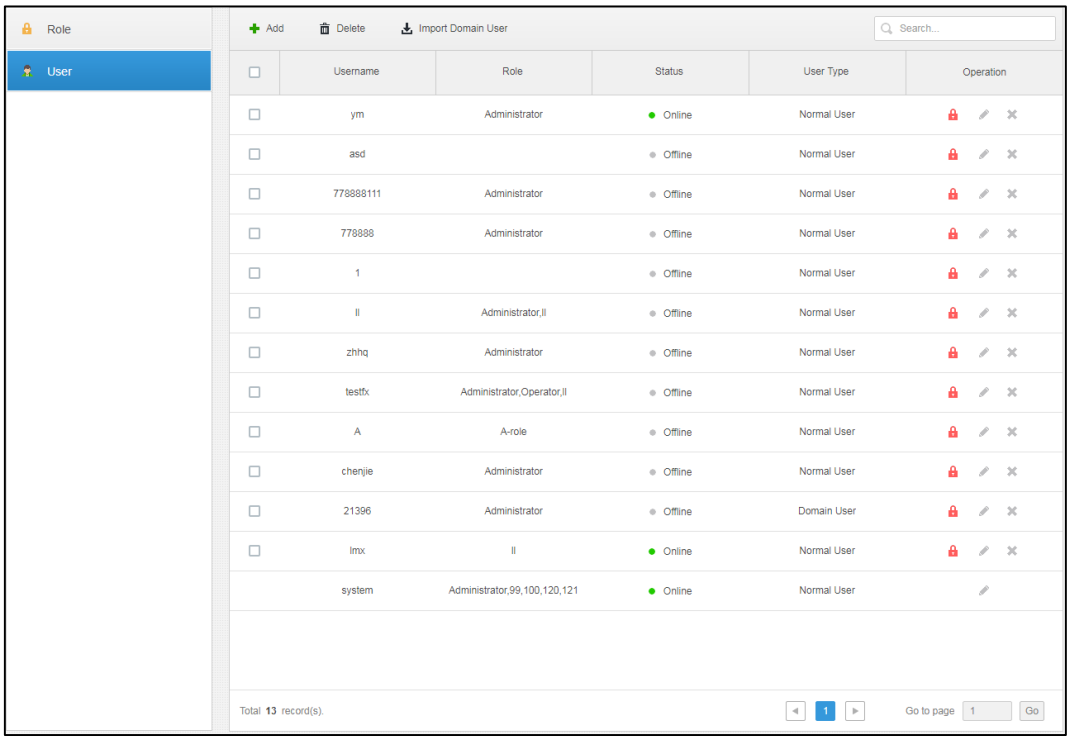
Crie uma conta de usuário para fazer login na plataforma.

Procedimento

I. Faça login no Gerenciador Web. Clique e selecione Usuário.

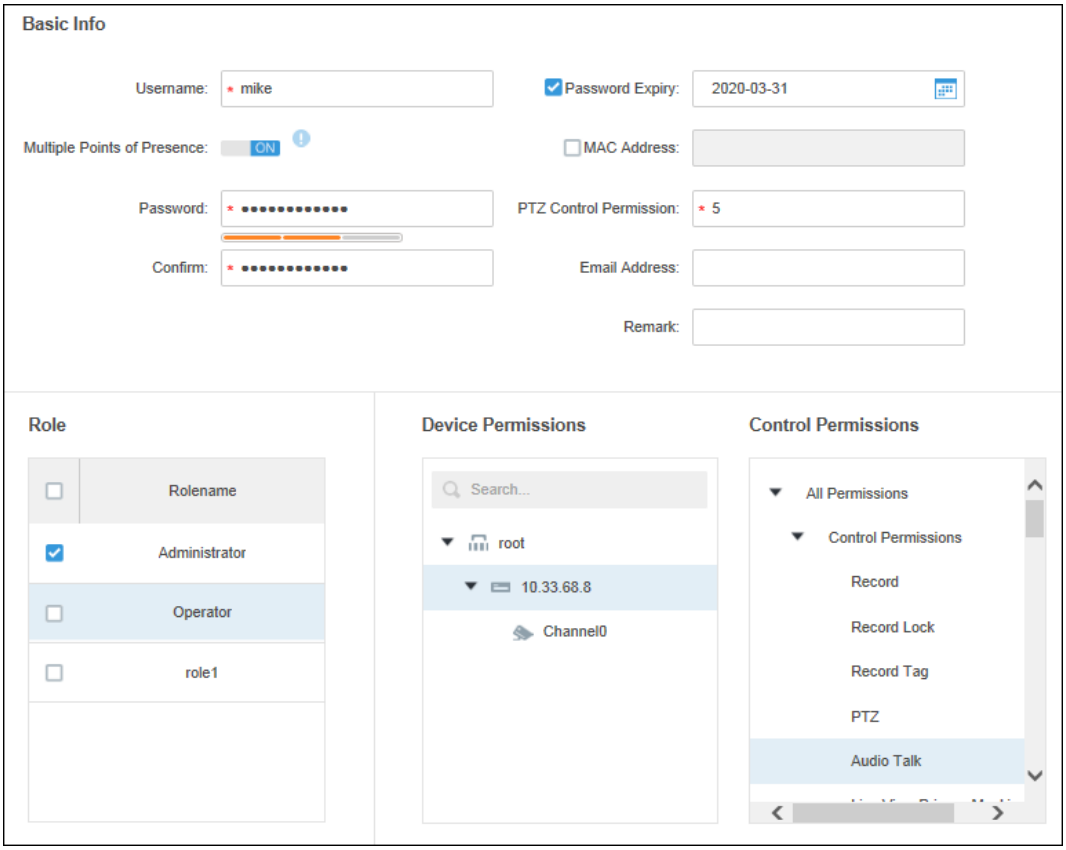
II. Clique na guia Usuário.

Figura 37 - Adicionar um usuário (1)



III. Clique em Adicionar.

Figura 38 - Adicionar um usuário (2)



Passo 5. Configure as informações do usuário, selecione a função abaixo e exibirá a permissão do dispositivo e a permissão de operação da função correspondente à direita.

- Você pode selecionar várias funções ao mesmo tempo.

IV. Clique em OK para adicionar o usuário.

Operações

- Clique para congelar o usuário. O usuário congelado não pode efetuar login no Defense client, Gerenciador Web e Aplicativo.
- Clique para modificar as informações do usuário, exceto o nome de usuário.
- Clique para excluir o usuário.

2.5.3 (Opcional) Configurando o usuário do domínio

É uma configuração é opcional. Você pode importar usuários de domínio do sistema de domínio de sua organização atual para criar usuários de plataforma.

I. Configurando Informações de Domínio

II. Faça login no Gerenciador Web. Clique e selecione Sistema na interface da nova guia.

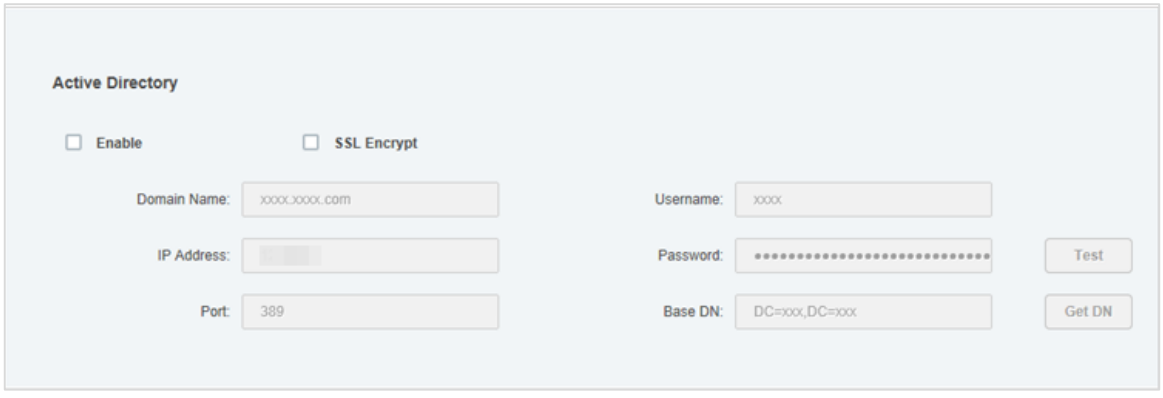
III. Clique em Diretório Ativo e configure as informações do domínio.

IV. Marque a caixa de seleção Habilitar e defina as informações do domínio.

- Depois de definir as informações do domínio, clique em Obter DN e ele irá adquirir as informações básicas de DN automaticamente.

V. Depois de obter as informações de DN, salve e clique em Testar para testar se as informações de domínio estão disponíveis.

Figura 39 - Definir diretório ativo



Clique em **Salvar**.

Passo 1. Importe usuários de domínio.

I. Faça login no Gerenciador Web, clique e selecione Usuário na interface da nova guia.

II. Clique na guia Usuário e em Importar Usuário de Domínio.

Selecione os usuários a serem importados e clique em Avançar.

Você também pode pesquisar um usuário inserindo palavras-chave na caixa de pesquisa.

Selecione as funções e clique em OK.

Para fazer login usando uma conta de usuário de domínio, inicie o Client e selecione Usuário de Domínio para o tipo de usuário.

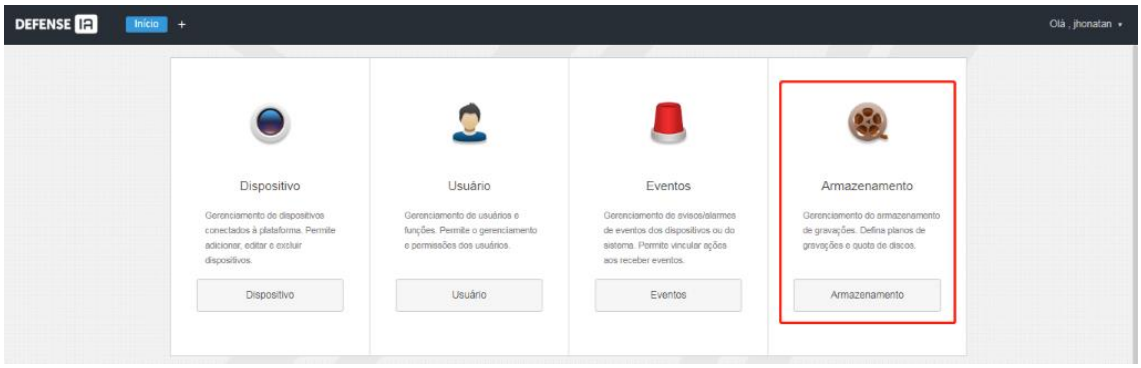
Figura 40 - Login do usuário de domínio

2.6 CONFIGURANDO A GRAVAÇÃO DOS DISPOSITIVOS

O Defense IA suporta a configuração de gravação por dispositivos, configurando o plano de gravação para gravar diretamente nos dispositivos da borda ou no servidor onde tais dispositivos estão alocados. Sendo estes dispositivos da borda gravadores ou câmeras com cartão SD. E a gravação no servidor feita em discos locais e/ou em discos de rede.

É possível configurar a gravação por modelos de tempo, como mostrado nesta seção ou por eventos, tais como acionamento de inteligências.

Figura 41 - Menu de Armazenamento



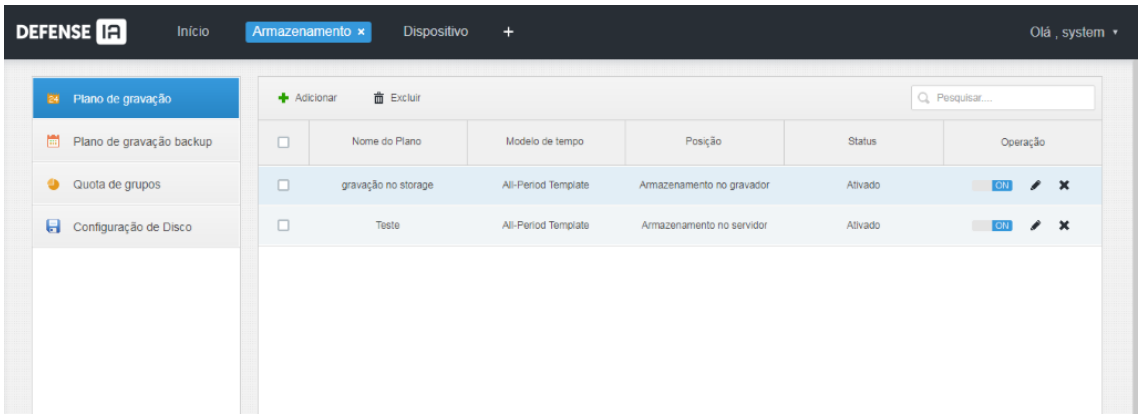
Obs: para gravação por acionamento de inteligências como detecção de movimento, linha e cerca virtual ou outras, é necessário configurar no menu de Eventos do Defense IA.

2.6.1 Configurando o Plano de Gravação

Dentro do menu Plano de gravação é onde se pode configurar os perfis de tempo para gravação regular nos gravadores ou no servidor.

Quando selecionada a opção de armazenamento no servidor a gravação de vídeo de cada dispositivo será configurada no servidor ao qual o dispositivo está alocado, seja ele um servidor master ou um servidor slave.

Figura 42 - Menu de Armazenamento



Nesta aba você pode criar novos planos, excluir os planos existentes, ativar/desativar e também editar os planos.

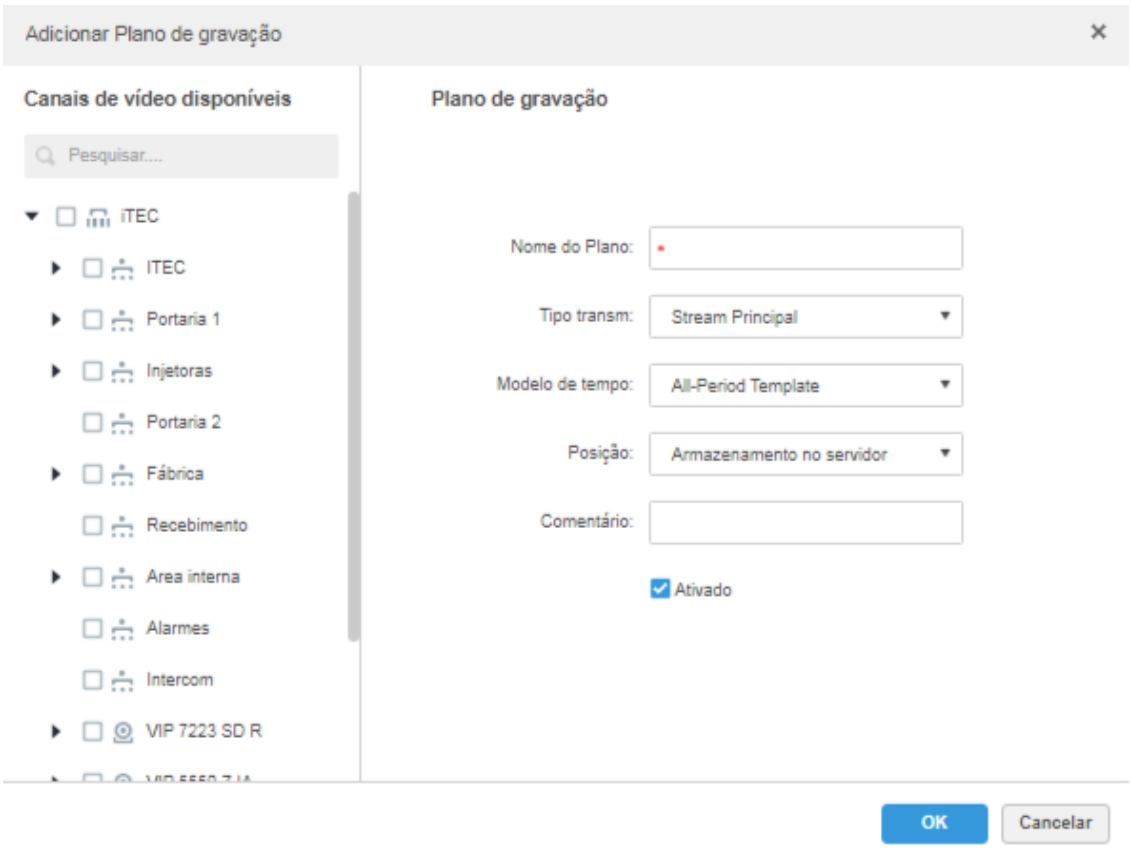
Operações

- Ativar / desativar plano geral

- Na coluna de operação, ON significa que o plano foi habilitado, clique no ícone e ele se torna OFF, e isso significa que o plano foi desativado.
- Editar Plano Geral
- Clique do plano correspondente para editar o plano geral.
- Excluir Plano Geral
- Selecione o plano geral, clique Delete para excluir planos em lotes.
- Clique do plano geral correspondente para excluir o plano geral individual.

I. Clique no botão adicionar e o seguinte menu, Adicionar Plano de gravação, será aberto na tela.

Figura 43 - Adicionar Plano de Gravação



A esquerda do menu encontra-se a parte de seleção dos dispositivos, onde pode-se selecionar os dispositivos que terão sua gravação de acordo com o plano. Todos os dispositivos da organização aparecerão aqui.

Os dispositivos podem ser adicionados em mais de um plano ao mesmo tempo.

A direita, na parte Plano de gravação eis o que os campos selecionáveis representam:

Tipo transmissão	Tipo do stream que será gravado. Tendo como opções **stream principal** e **stream extra**. No caso do stream extra, o mesmo deve estar habilitado na câmera.
Modelo de tempo	Agendamento da gravação. O campo possui alguns modelos pré-configurados e também a possibilidade de criar planos personalizados. Verifique a parte do manual Adicionando Modelo de Tempo.
Posição	Local onde as gravações serão armazenadas. A opção **armazenar no gravador** designa armazenamento nos dispositivos de borda, tais como gravadores e câmeras com cartão SD. A outra opção, **armazenar no servidor** designa que gravação do vídeo de cada dispositivo ocorrerá no servidor onde o mesmo está alocado, ou seja, se o dispositivo estiver alocado no servidor master a gravação ocorrerá nos discos do servidor master e se o dispositivo estiver alocado em um servidor slave a gravação ocorrerá nos discos do servidor slave. Sejam estes discos locais ou discos de rede.
☑ Ativado	Assim como o botão on/off do menu acima este check box habilita ou desabilita o plano de gravação.

II. Preenche os campos conforme o plano de gravação que deseja configurar.

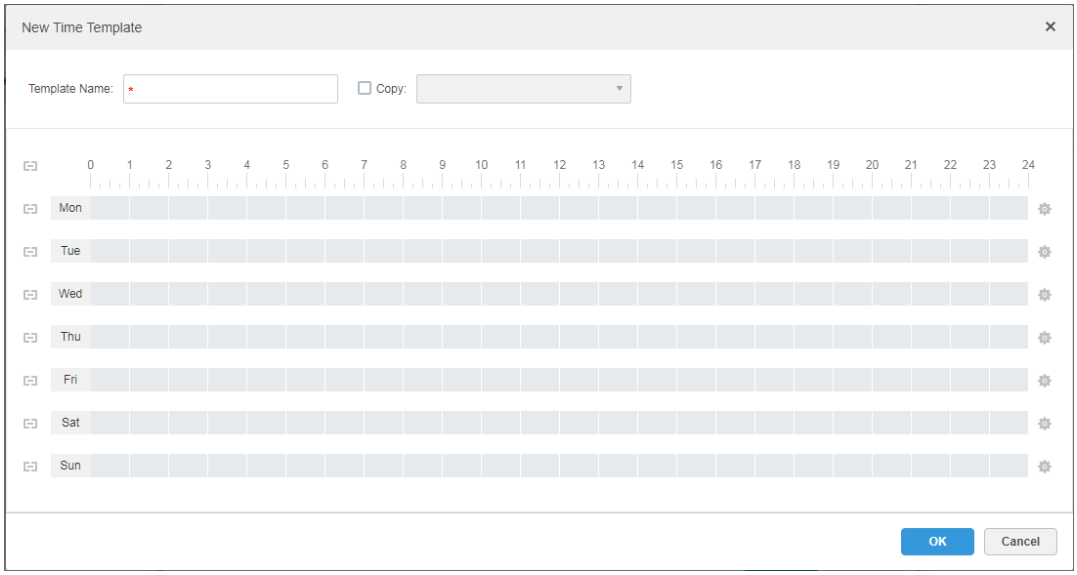
III. Salve o plano.

2.6.2 Adicionando Modelo de Tempo

Passo 1. Clique + e selecione Armazenamento na interface da nova guia.

Passo 2. Selecione Novo modelo de tempo na caixa suspensa Modelo de tempo.

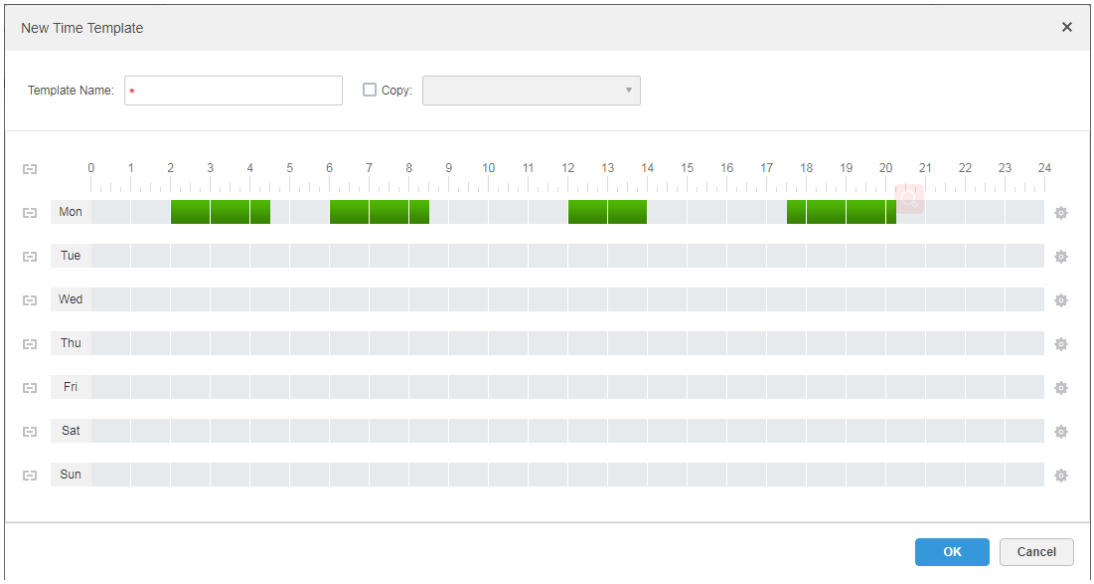
Figura 44 - Novo modelo de tempo



IV. Define o nome do modelo e o período de tempo.

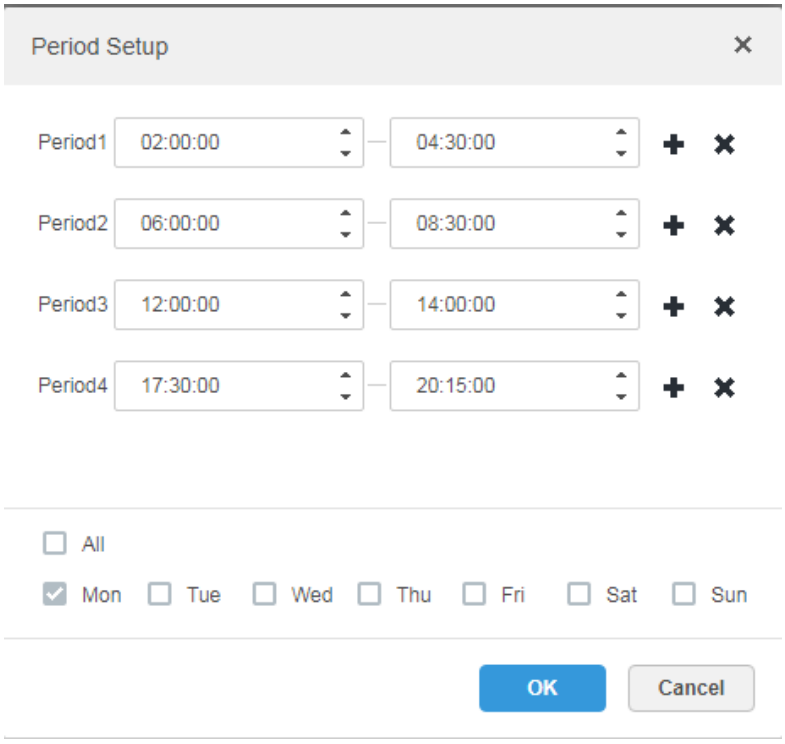
- Pressione o botão esquerdo e arraste-o para desenhar o período de tempo na linha do tempo.

Figura 45 - Defina o período de tempo por desenho



- Clique no ⚙ do dia correspondente, defina o período de tempo na interface de configuração do período. Vejo0.

Figura 46 - Defina o período de tempo selecionando

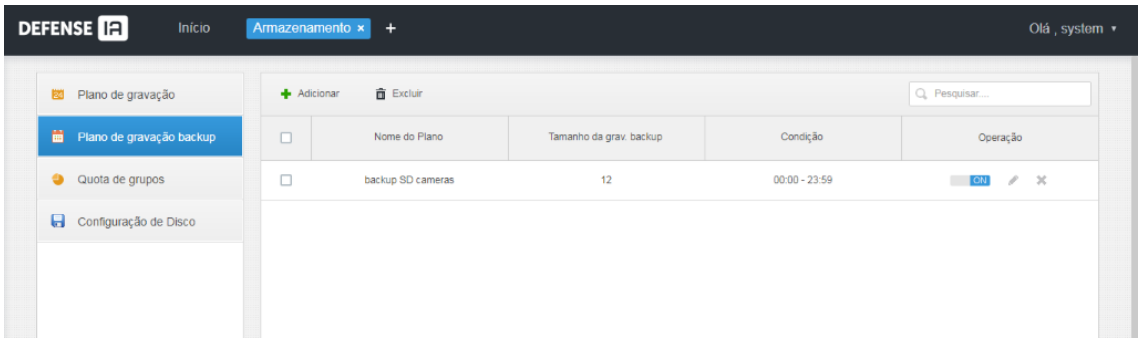


2.6.3 Configurando o backup de armazenamento

Dentro do menu Plano de gravação backup é onde se pode configurar tarefas para copiar as gravações dos dispositivos de borda para o servidor.

Cabem aqui algumas observações importantes, o plano de gravação backup puxa todas as gravações do período estipulado, sobrescrevendo as gravações do servidor.

Figura 47 - Plano Backup



Operações

- Ativar / desativar plano de registro de backup.

I. Na coluna de operação, ON significa que o plano foi ativado; clique no ícone e ele se tornará OFF, significa que o plano foi desativado.

- Editar plano de registro

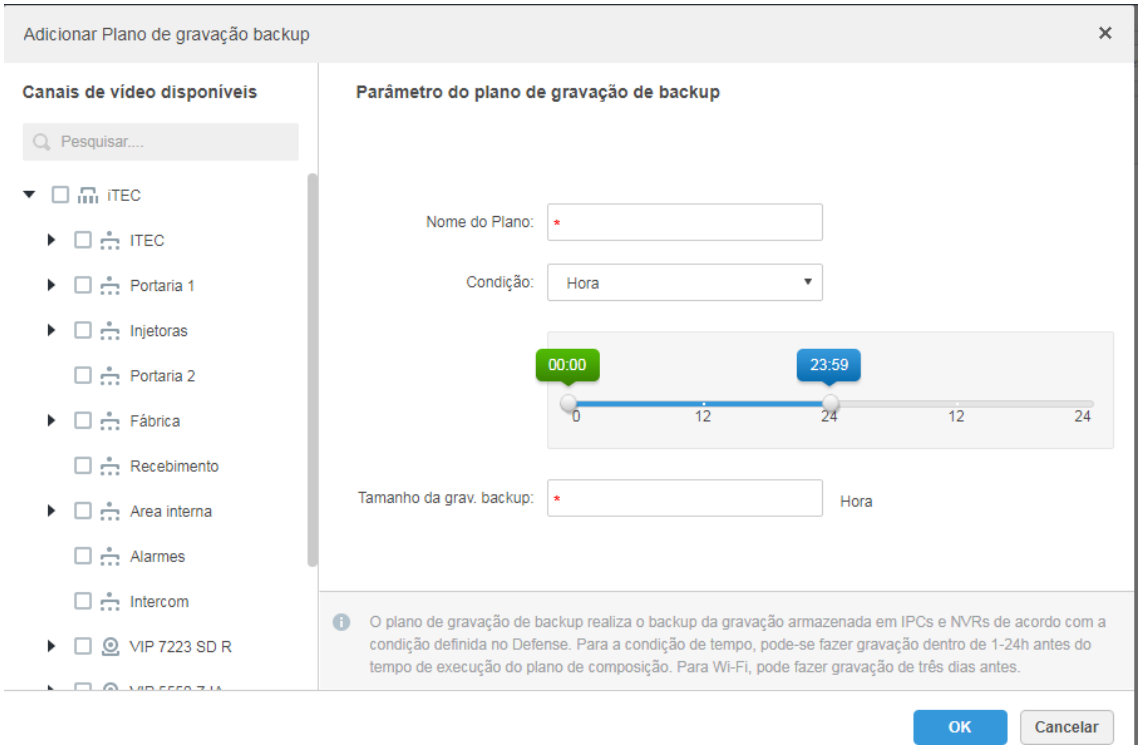
- Clique no correspondente do plano e, em seguida, você pode editar o plano de registro de backup.

- Excluir plano de registro

  Selecione o plano de registro, clique Delete para excluir o plano em lotes.
  Clique no correspondente do plano de registro, então você pode excluir o plano individualmente.

- Clique no botão adicionar e o seguinte menu, Adicionar Plano de gravação backup, será aberto na tela.

Figura 48 - Adicionar plano de backup



A esquerda do menu encontra-se a parte de seleção dos dispositivos, onde pode-se selecionar os dispositivos para o plano de gravação backup. Todos os dispositivos da organização aparecerão aqui.

Os dispositivos podem ser adicionados em mais de um plano ao mesmo tempo.

A direita, na parte Parâmetros do plano de gravação de backup eis o que os campos selecionáveis representam:

Condição	1) Condição de início para o plano de gravação backup. As opções são **Hora** ou **Wi-Fi**.

	2) Selecionando a opção Hora, o processo de backup será feito dentro da linha de tempo estipulada no plano. Este tempo deve ser grande o suficiente para que o Defense IA puxe as gravações, caso contrário, o backup será incompleto. 3) Selecionando a opção Wi-Fi , o sistema fará o registro de backup automaticamente quando a rede do dispositivo de backup for comutada para Wi-Fi.
Tamanho da gravação	4) Quando selecionada a condição Hora, é possível puxar as gravações de 0h até 24h antes do início do procedimento. 5) Quando selecionada a opção WI-FI, automaticamente o sistema trará as gravações de até 3 dias.

2.6.4 Configurando os Discos de Armazenamento

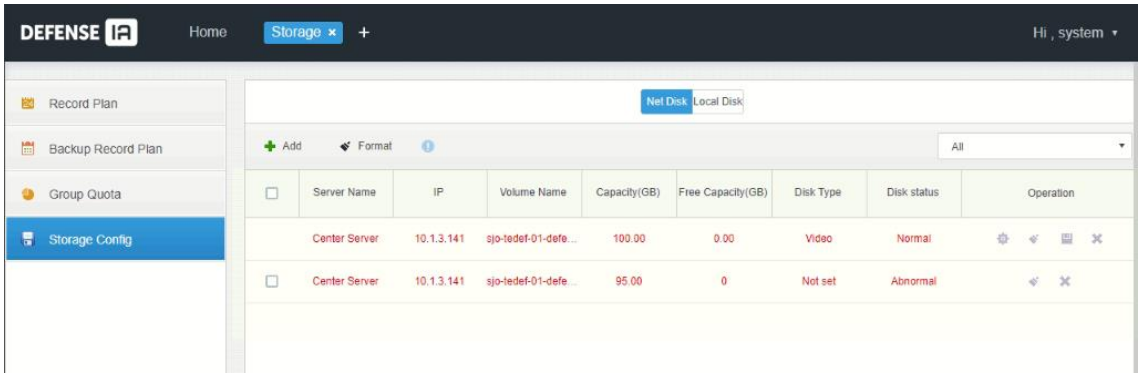
O Defense IA possui compatibilidade com gravação em discos locais nos servidores master e slave e com discos de rede.

- O Defense IA suporta o gerenciamento de até 200TB por servidor, ou seja, caso a necessidade seja maior que 200TB de armazenamento deverá ser utilizada uma arquitetura de servidor distribuída.
- O Defense IA trabalha com um tipo de formatação proprietário para os discos de gravação de vídeo e imagem de LPR. Esse tipo de formato fechado garante uma maior segurança dos dados, pois os mesmos não são acessíveis por outros sistemas.
- É importante verificar se a velocidade escrita/leitura dos discos suporta o throughput necessário para gravação do vídeo.

2.6.4.1 Configurando os Discos de rede

O Defense IA é pode adicionar discos de rede compatíveis com o protocolo iSCSI. Configure o disco de rede para armazenar diferentes tipos de arquivos, incluindo vídeos, instantâneos LPR e instantâneos de face ou alarme. Mas é necessário formatar o disco externo antes de usá-lo.

Figura 49 - Disco de rede



- O servidor de armazenamento deve ser implantado.
- Protocolo iSCSI utiliza por padrão a porta 3260.
- O protocolo iSCSI possui uma limitação de 16TB por disco, mas N discos podem ser adicionados, contanto que respeitem os 200TB que o Defense IA consegue gerenciar.
- Um volume de usuário do disco de rede atual só pode ser usado por um servidor ao mesmo tempo.
- O volume do usuário deve ser formatado ao adicionar o disco de rede.

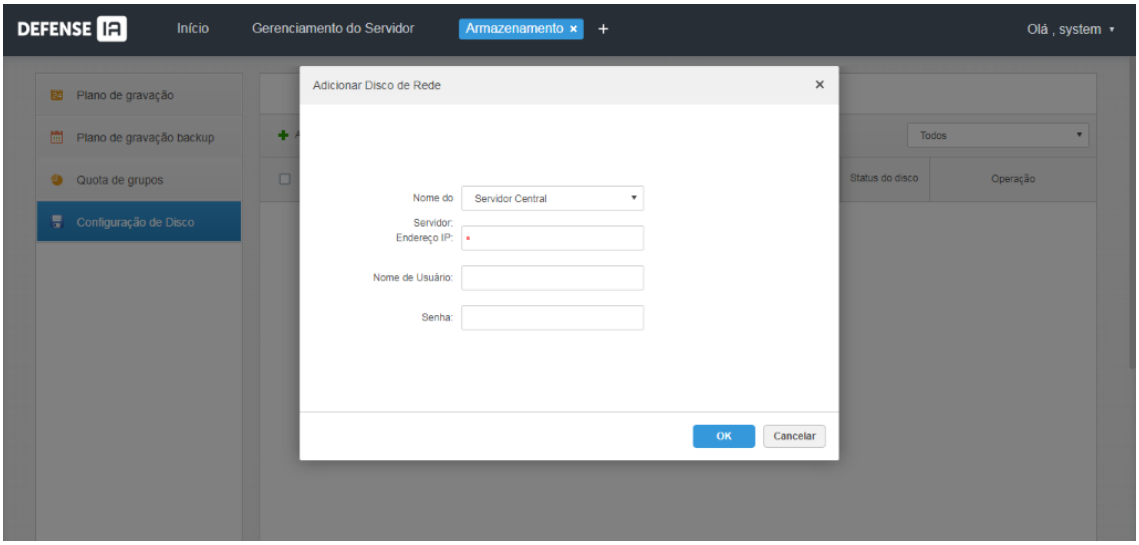
II. Clique em Adicionar.

III. Selecione o nome do servidor storage, digite o endereço IP do disco de rede e clique em OK.

- Os discos a serem adicionados podem ser configurados com o m[etodo de autenticação CHAP ou sem autenticação.
- Autenticação CHAP: Digite o nome de usuário e a senha de um usuário de disco que tenha permissão de volumes no disco de rede.
- Campo nome de usuário em branco a plataforma mostra os volumes não atribuídos a nenhum usuário no disco. Os volumes em vermelho estão sendo usados. Para forçar para pegá-lo, clique .

- Para forçar a obtenção do disco, você precisa formatá-lo. Os dados serão apagados após a formatação do disco. Recomenda-se que você faça backup dos dados com antecedência.

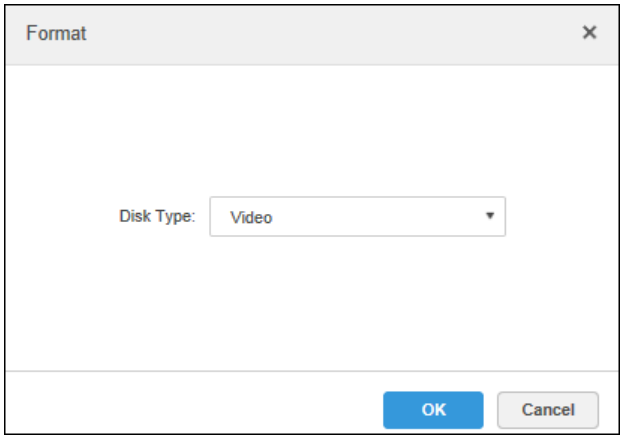
Figura 50 - Adicionar disco de rede



IV. Selecione o disco, clique em Formatar ou clique no próximo às informações do disco para formatar o disco correspondente.

V. Selecione o tipo de disco de formato e clique em OK.

Figura 51 - Formatar disco



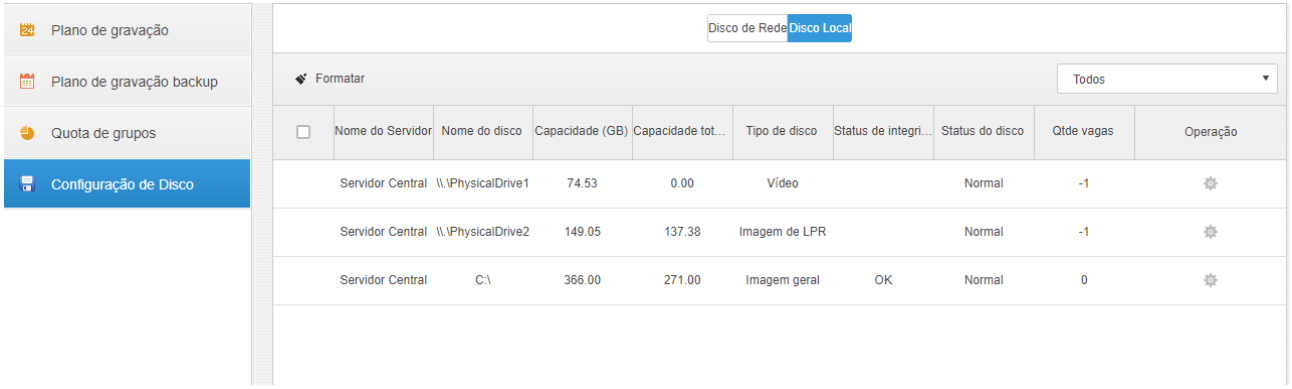
VI. Clique em OK na caixa de prompt para confirmar a formatação.

- Discos para gravação de vídeo e para imagens de LPR devem ser exclusivos para a aplicação, não sendo possível utilizar HDs particionados. Isso devido ao tipo fechado de formatação do disco para segurança dos dados.

2.6.4.2 Configurando Disco Local

Configure o disco local para armazenar diferentes tipos de arquivos, incluindo vídeos, instantâneos ANPR e instantâneos de rosto ou alarme. Mas é necessário formatar o disco antes de usá-lo.

Figura 52 - Discos locais



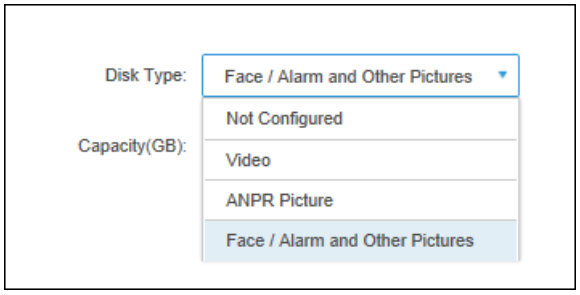
Passo 1. Clique e selecione Armazenamento.

Passo 2. Selecione Configuração de armazenamento> Disco local.

Passo 3. Configure o disco local.

- Clique e configure o tipo de disco de acordo com o prompt da interface.
-

Figura 53 - Selecione o tipo de disco



- Selecione o disco e clique em Formatar ou clique em próximo às informações do disco e formate o disco de acordo com o prompt da interface e configure o tipo de disco.

- Discos para gravação de vídeo e para imagens de LPR devem ser exclusivos para a aplicação, não sendo possível utilizar HDs particionados. Isso devido ao tipo fechado de formatação do disco para segurança dos dados.

2.6.5 Configurando a cota de grupos dos discos

Aloque grupos de discos para armazenamento de vídeo.

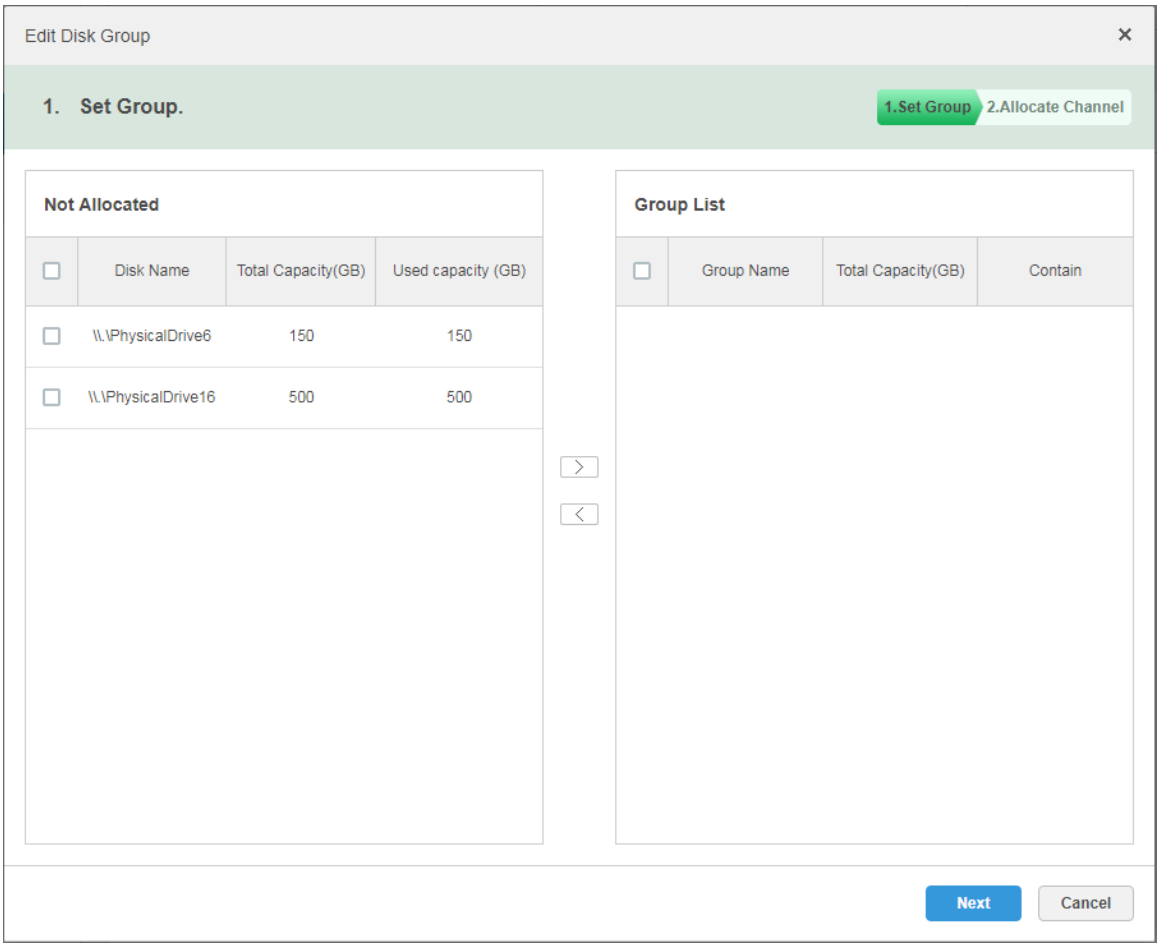
Passo 1. Clique e selecione Armazenamento na interface da nova guia.

Passo 2. Clique na guia Cota do grupo.

Figura 54 - Status do servidor

Passo 3. Clique próximo ao online / offline do servidor de status.

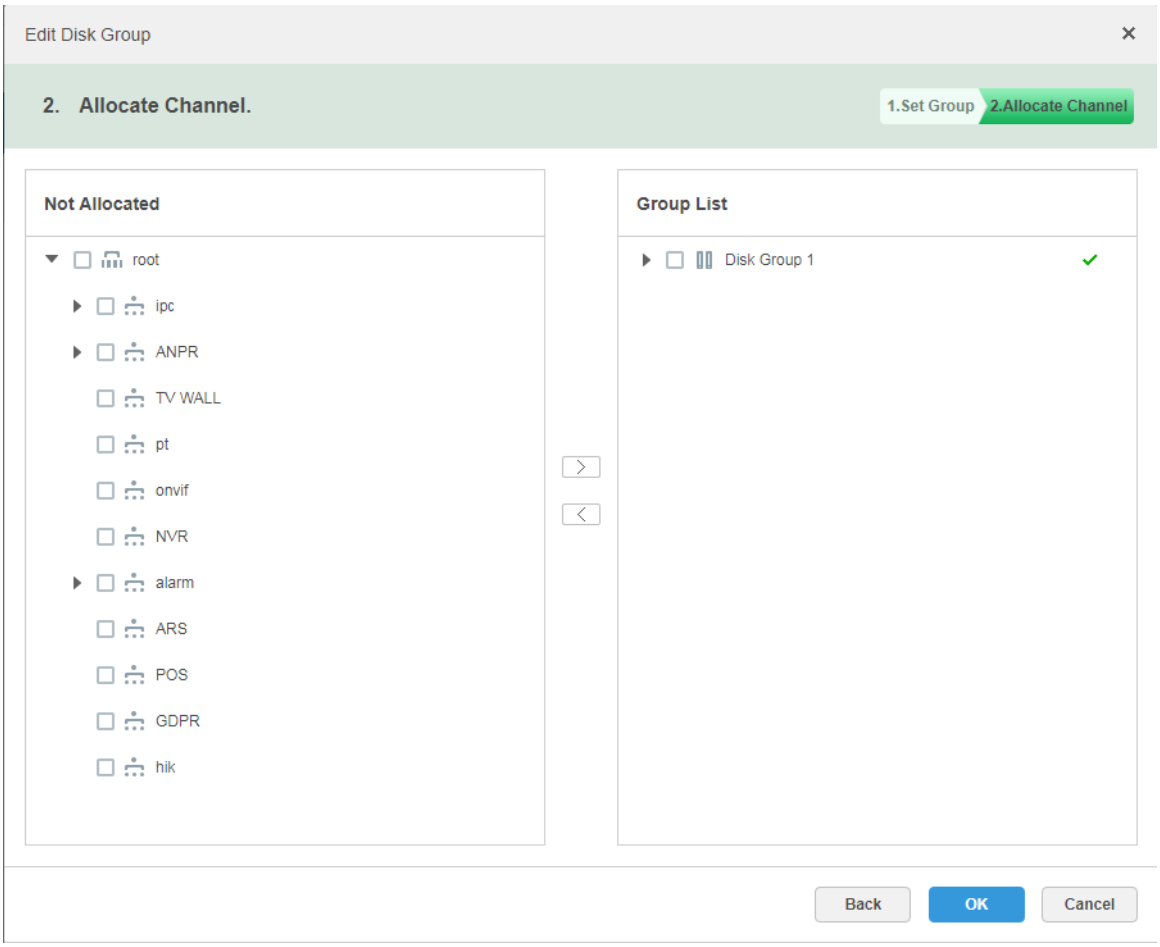
Figura 55 - Editar grupo de disco



Passo 4. Selecione os discos não distribuídos à esquerda, clique e adicione-o à lista de grupos de discos à direita.

Passo 5. Clique em Avançar para distribuir canais para o grupo de discos.

Figura 56 - Alocar canais



Passo 6. Selecione os canais na lista de dispositivos à esquerda e clique em > para adicioná-lo ao grupo de discos à direita.

Passo 7. Clique OK.

- O Defense IA distribui automaticamente a alocação dos dispositivos entre os discos, porém se alguma cota for criada é necessário alocar os dispositivos, caso contrário, os dispositivos não estarão gravando.

2.7 EVENTO E ALARME

A plataforma recebe alarmes de dispositivos e os exibe de acordo com suas configurações de alarme na plataforma.

Depois de habilitado e configurado o plano de alarmes no Gereciador Web, o Defense client pode exibir estes eventos alarmes na central de eventos. O sistema suporta as seguintes ações de vinculação de alarme:

- Vinculação de câmera

Quando o alarme acontecer, o Defense client reproduzirá o vídeo da câmera vinculada ou a câmera vinculada será acionada para iniciar a gravação ou tirar uma foto.

- Ação de PTZ
  Quando o alarme acontecer, a câmera PTZ vinculada será acionada para girar para um ponto predefinido específico.
- Saída de alarme
  Quando o alarme acontecer, o canal de saída de alarme vinculado emitirá um sinal de alarme. Se o canal estiver conectado com uma sirene, a sirene emitirá um som.
- Mural de vídeo
  Quando o alarme acontecer, o vídeo vinculado será exibido no video wall.
- E-mail de conexão
  Quando o alarme acontecer, o sistema enviará automaticamente um e-mail conforme configurado.
- Link de usuário
  Quando o alarme acontecer, o sistema notificará um usuário específico conforme configurado.
- Ligação porta
  Quando o alarme acontecer, a porta vinculada será aberta ou fechada conforme configurada.
-

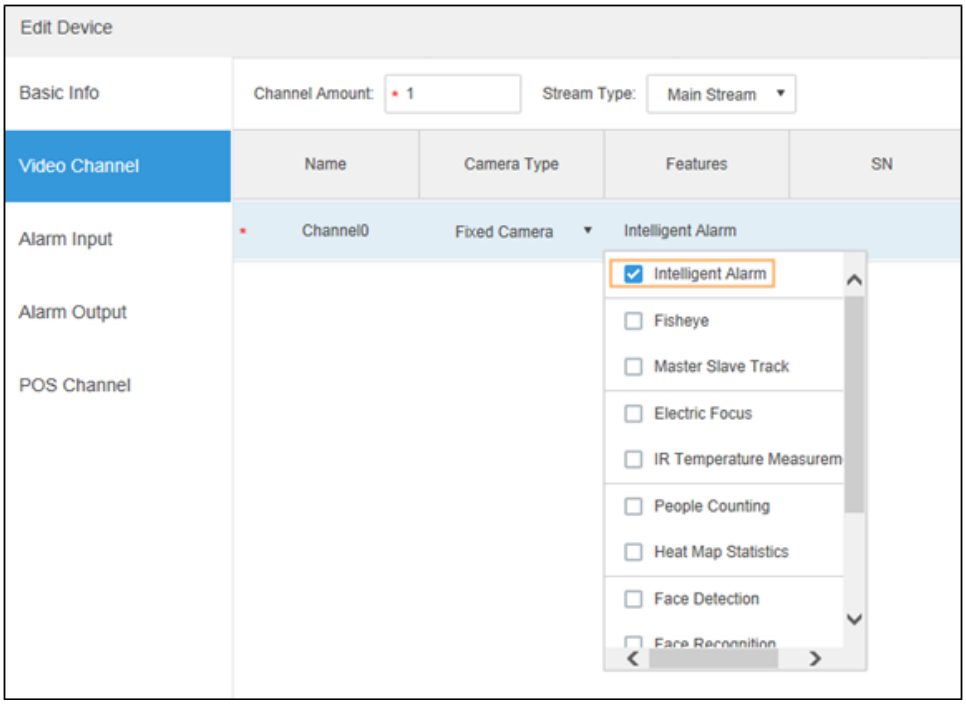
Você precisa configurar cada tipo de alarme no Gerenciador Web.
Um alarme pode ter várias ações de vinculação.

2.7.1 **Configurando Eventos**

2.7.1.1 Preparativos

- As informações básicas e de características dos dispositivos devem estar configuradas. Para obter detalhes, consulte os documentos correspondentes.
  Considere a configuração do alarme IVS, por exemplo. Na interface do dispositivo, clique em do dispositivo e, em seguida, selecione Alarme inteligente para recursos.

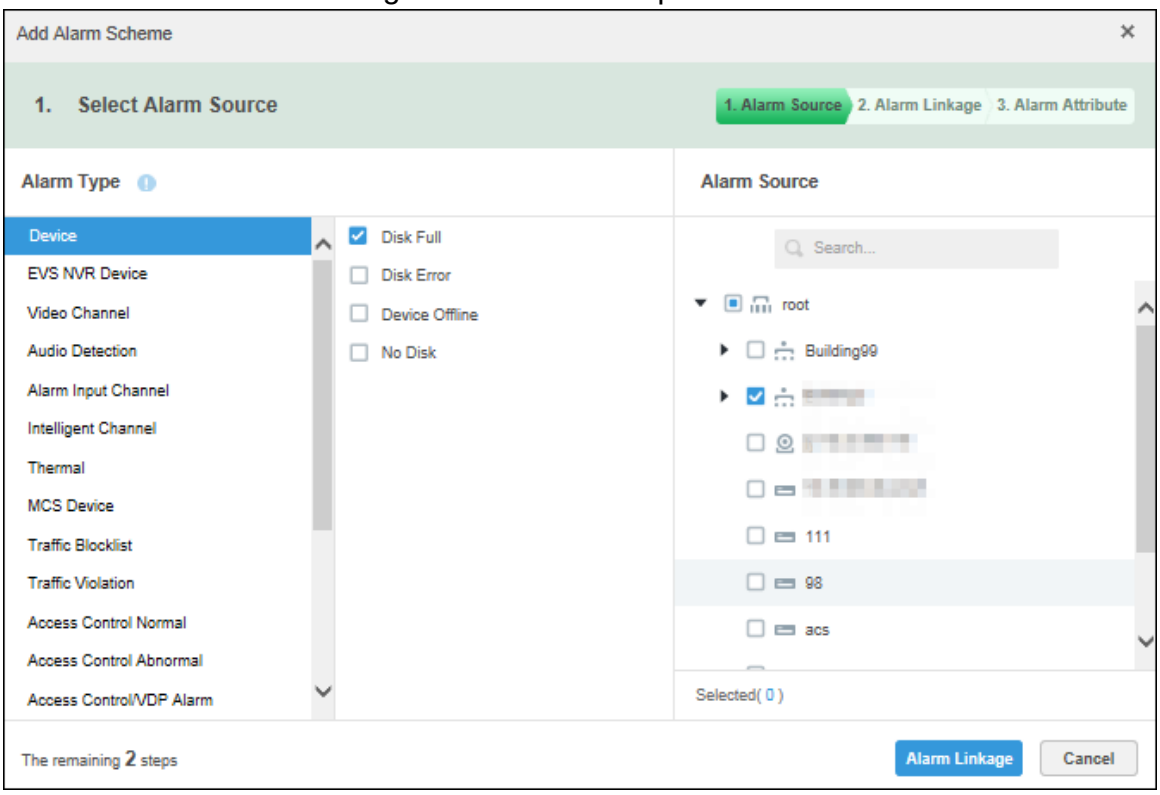
Figura 57 - Editar recursos (1)



2.7.1.2 Configurando Eventos

Dentro do menu de eventos do Gerenciador Web clique em Adicionar.

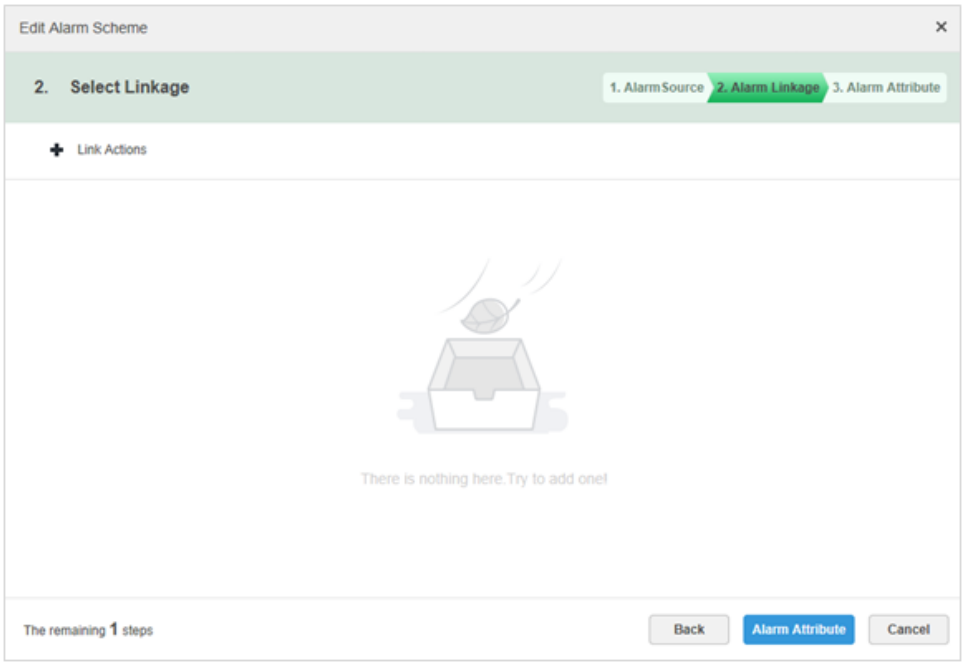
Figura 58 - Editar esquema de alarme



I. Configure a fonte de alarme.

II. Selecione um tipo de alarme e a fonte de alarme relevante e clique em Ligação de alarme.

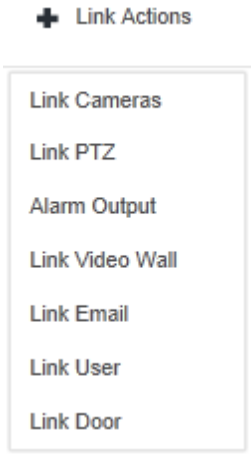
Figura 59 - Adicionar esquema de alarme



Passo 1. Configure ações de vinculação de alarme.

6) Clique ✚ .

Figura 60 - Ações de link



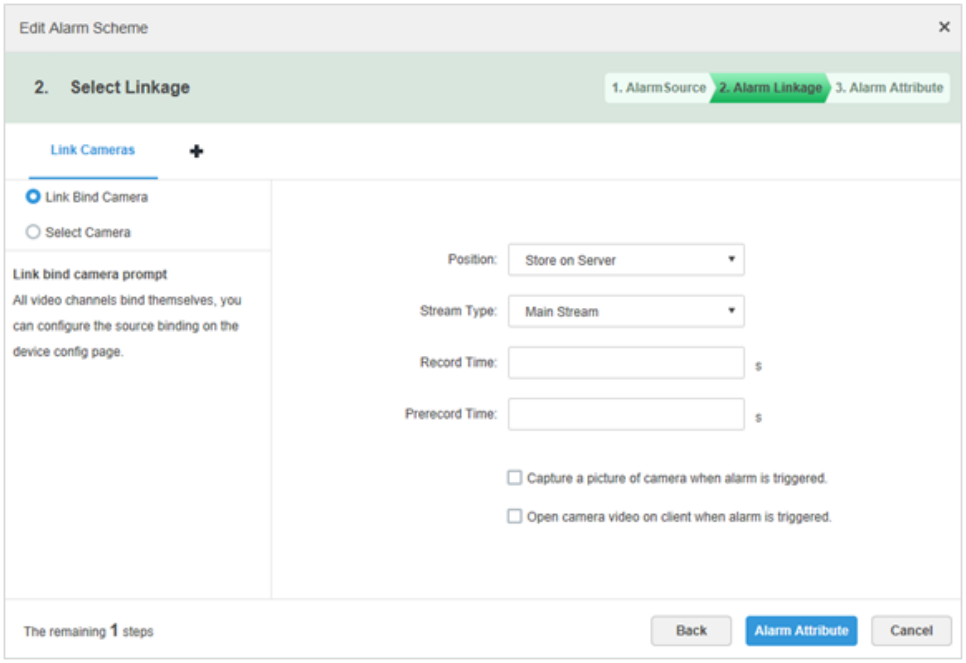
Selecione as ações de ligação.

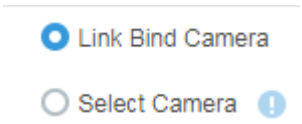
- Clique em Vinculação de câmeras , e depois definir parâmetros.

- Para obter pop-up de vídeo no Defense client quando o alarme associado for disparado, depois de definir as configurações de ligação da câmera aqui, lembre-se de selecionar Abrir vídeo da câmera no Defense client quando o

alarme for disparado e, em seguida, selecione Exibir vídeo de link de alarme quando o alarme ocorrer na Configuração local > Alarme no Defense client.

Figura 61 - Vincular câmera

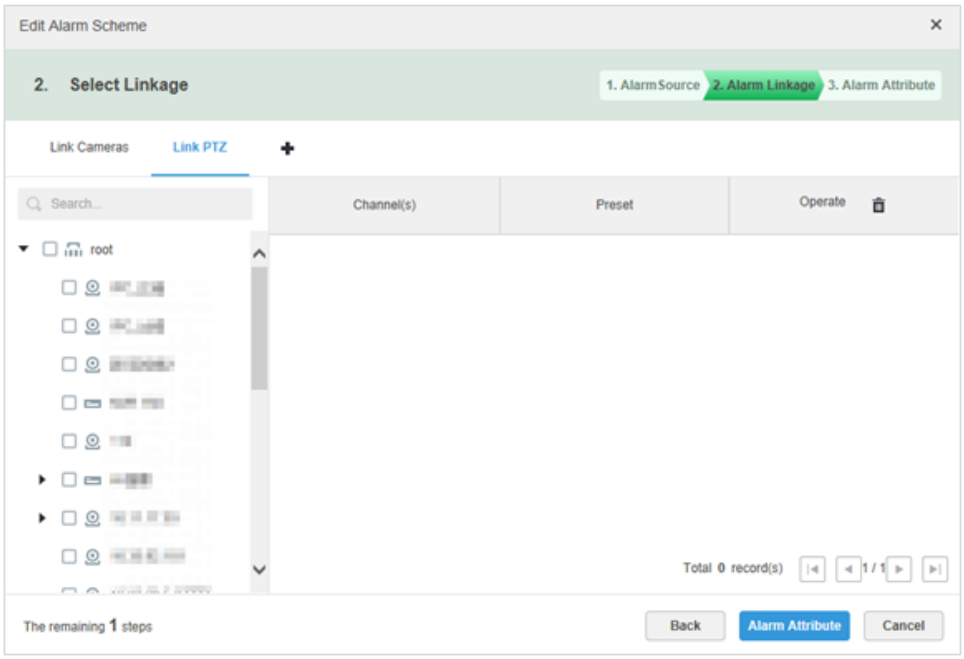


Parâmetro	Descrição
	Vincular câmera: Selecione esta opção para permitir que o alarme acione o vídeo da câmera que foi associada à câmera atual (a câmera para a qual está configurando o alarme). Se a câmera para a qual você está configurando o alarme não foi vinculada a nenhuma outra câmera (consulte "Recursos de vinculação"), a plataforma pensa que está vinculada a si mesma. Selecione uma Câmera para ligação: Selecionar manualmente uma câmera para conectar com o alarme.
Posição	Selecione para armazenar o vídeo no servidor ou não.
Tipo de fluxo	Selecione o tipo de fluxo de gravação de vídeo. O fluxo primario possui qualidade superior à do fluxo secundário, mas consome mais armazenamento e largura de banda do que sub stream.
Tempo de gravação	Configure a duração da gravação de vídeo.
Tempo de pré-gravação	É o tempo de gravação antes do recebimento do evento da câmera vínculada. É necessário que o dispositivo suporte gravação e que esteja incluso em algum plano de gravação.
Tire uma foto da câmera quando o alarme for disparado.	Confirme a captura de imagem da câmera.
Abra o vídeo da câmera no cliente quando o alarme for disparado.	Confirme se o evento deverá abrir um pop-up com o vídeo da câmera na tela do Defense client.

	• É necessário vincular os usuários de conexão para que recebam este tipo de alerta.

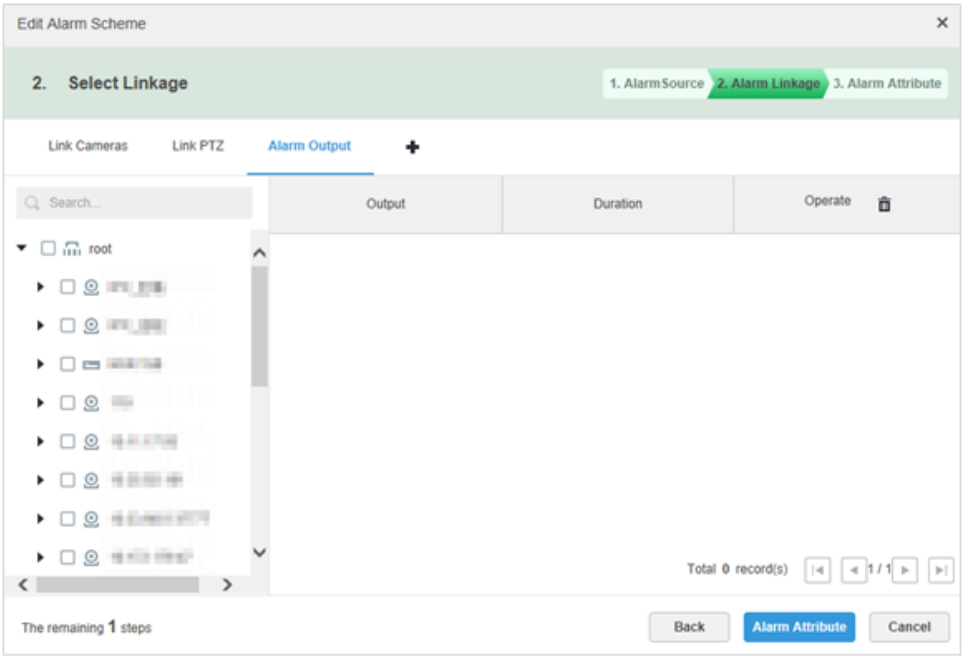
- Clique em Link PTZ, selecione os canais que precisam de PTZ para conectar o dispositivo, e depois definir ações pré-gravadas.

Figura 62 - Link PTZ



- Clique em Saída de alarme, selecione o canal de saída de alarme, e depois definir a duração.

Figura 63 - Saída de alarme de link



- Clique em Link Video Wall, selecione link camera à esquerda da interface, selecione video wall à direita da interface. Ao selecionar Link Bind Camera e Link Camera, as interfaces serão exibidas de forma diferente, baseie-se na exibição real. Clique em Configuração da janela de alarme de video wall para definir a duração e selecionar o canal de vídeo que precisa ser exibido na parede.

Figura 64 - Link vídeo wall (1)

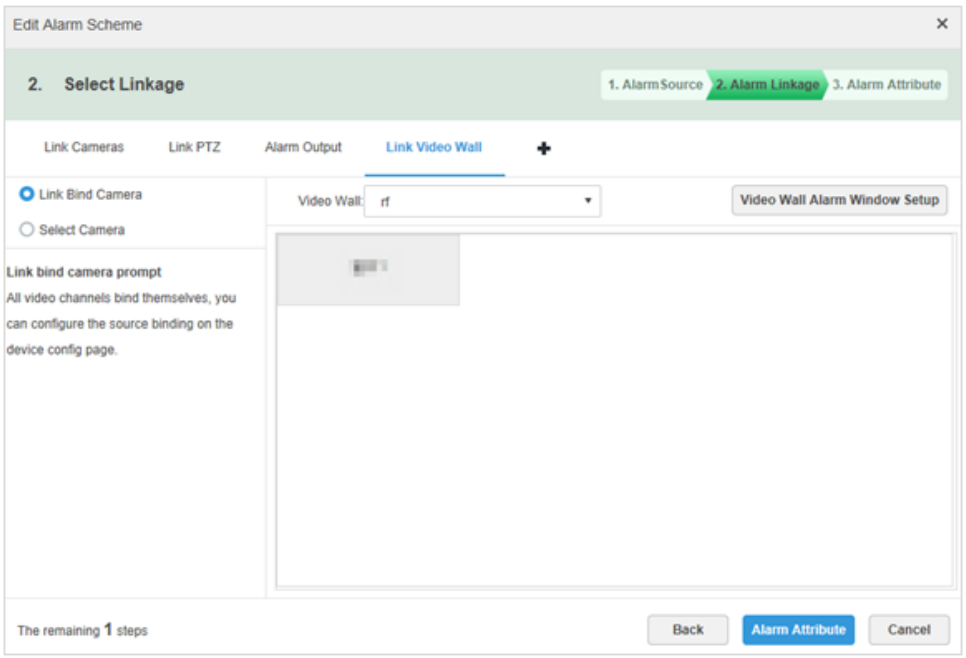
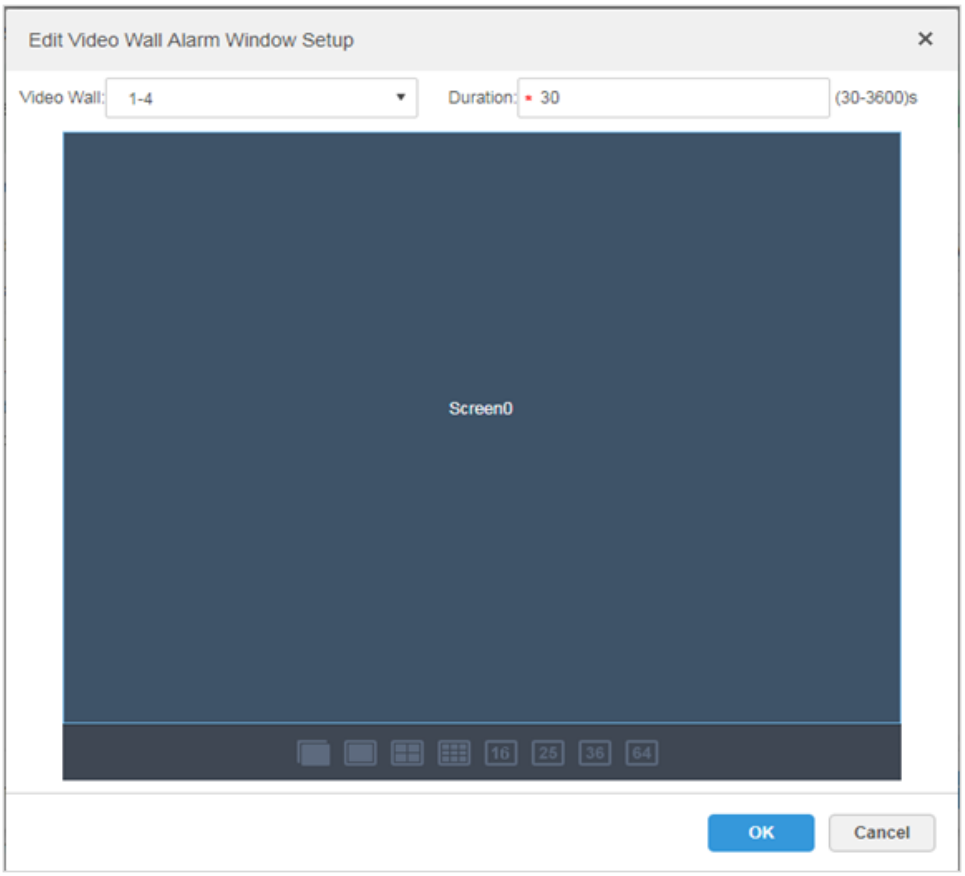


Figura 65 - Link vídeo wall (2)



- Clique em Link de e-mail, selecione o modelo de e-mail e o destinatário.
  Clique no modelo de e-mail pode ser configurado, clique no botão adicionar próximo a Modelo de Correio e selecione Novo Modelo de Correio, defina o novo modelo de correio.
  Aponte para Assunto e, em seguida, escale e selecione Evento **Tempo**, **Fonte de Eventos** e outro opçãos.

Figura 66 - Configuração de e-mail

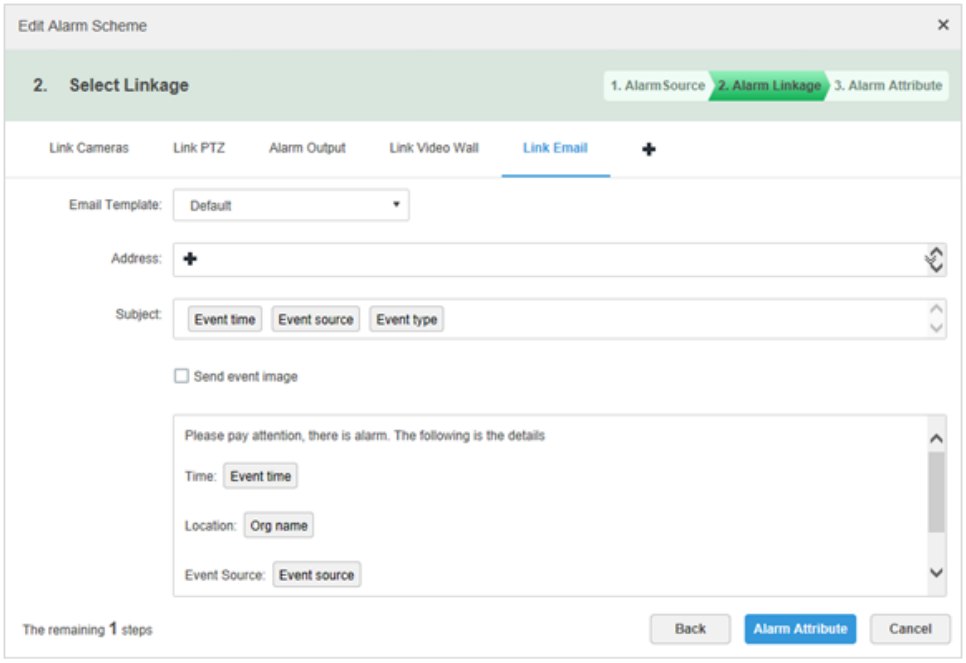
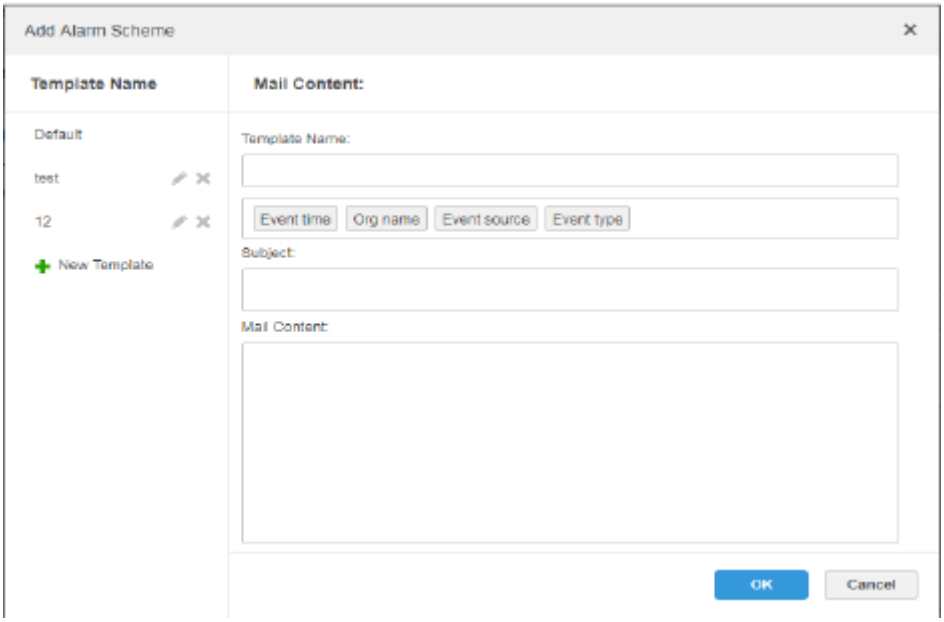
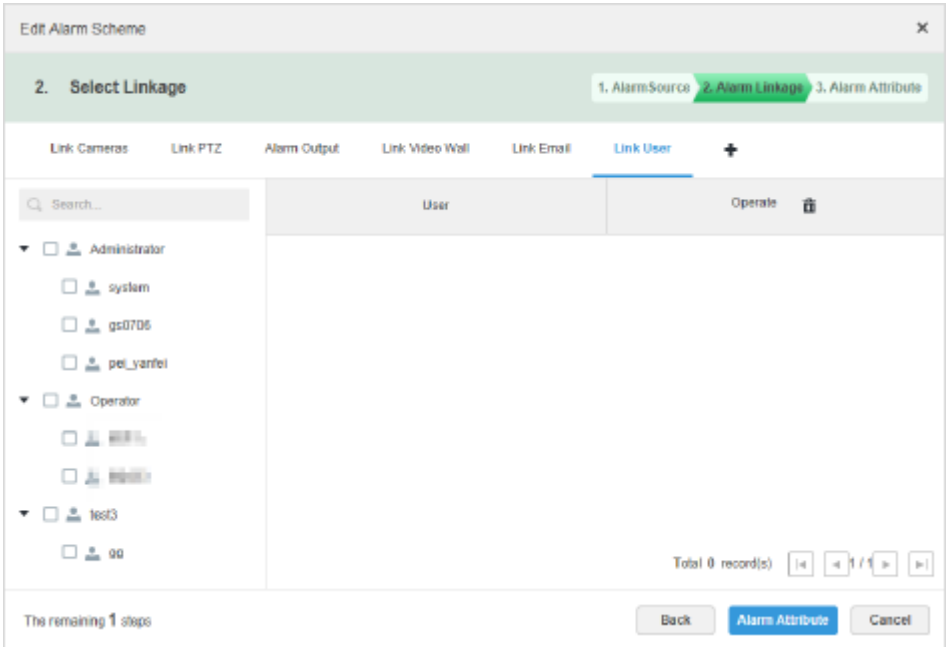


Figura 67 - Definir modelo de e-mail



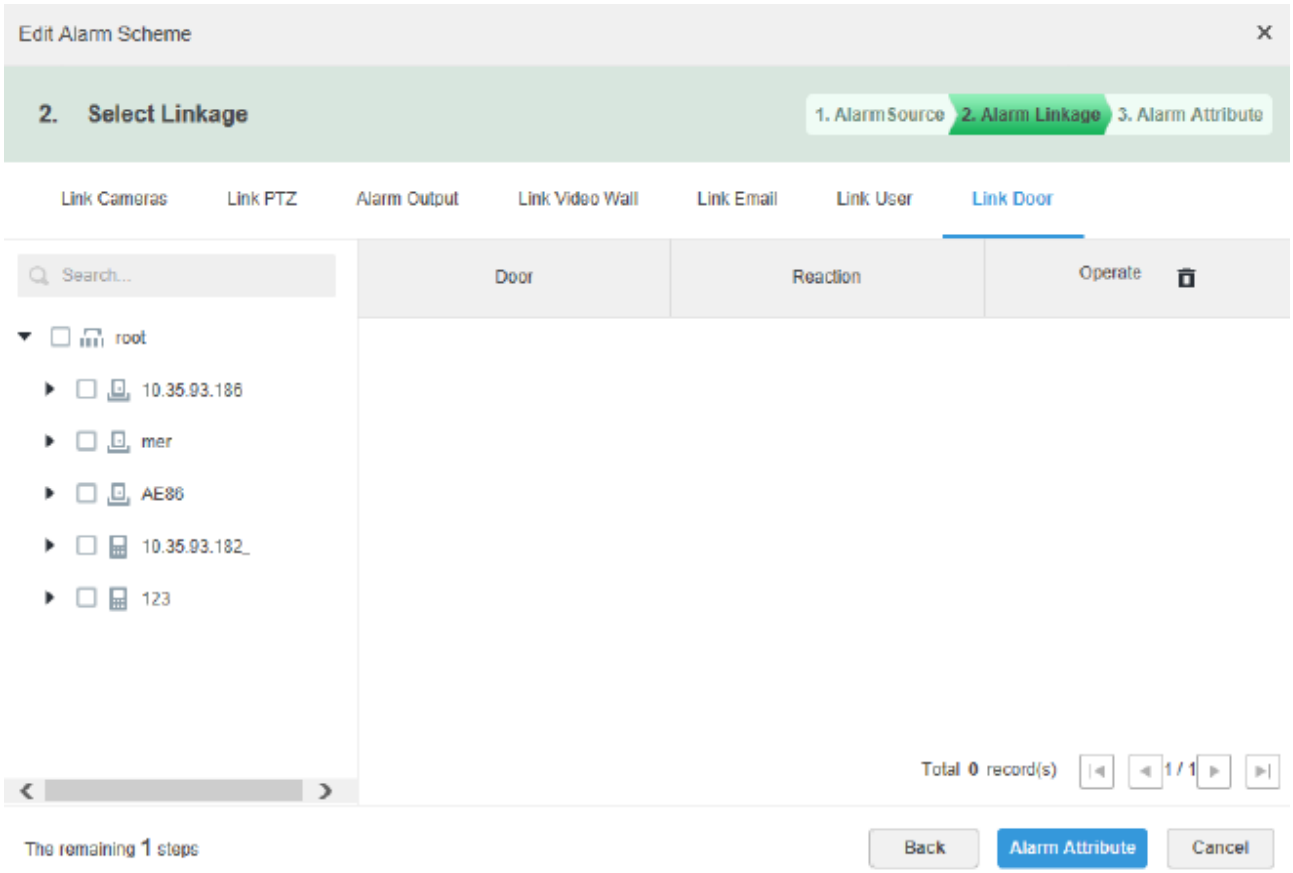
- Clique em Link de usuário, e depois selecione os usuários a serem informados.

Figura 68 - Link de usuário



- Clique em Link Door, selecione o dispositivo de controle de acesso e então definir o linkera açao.

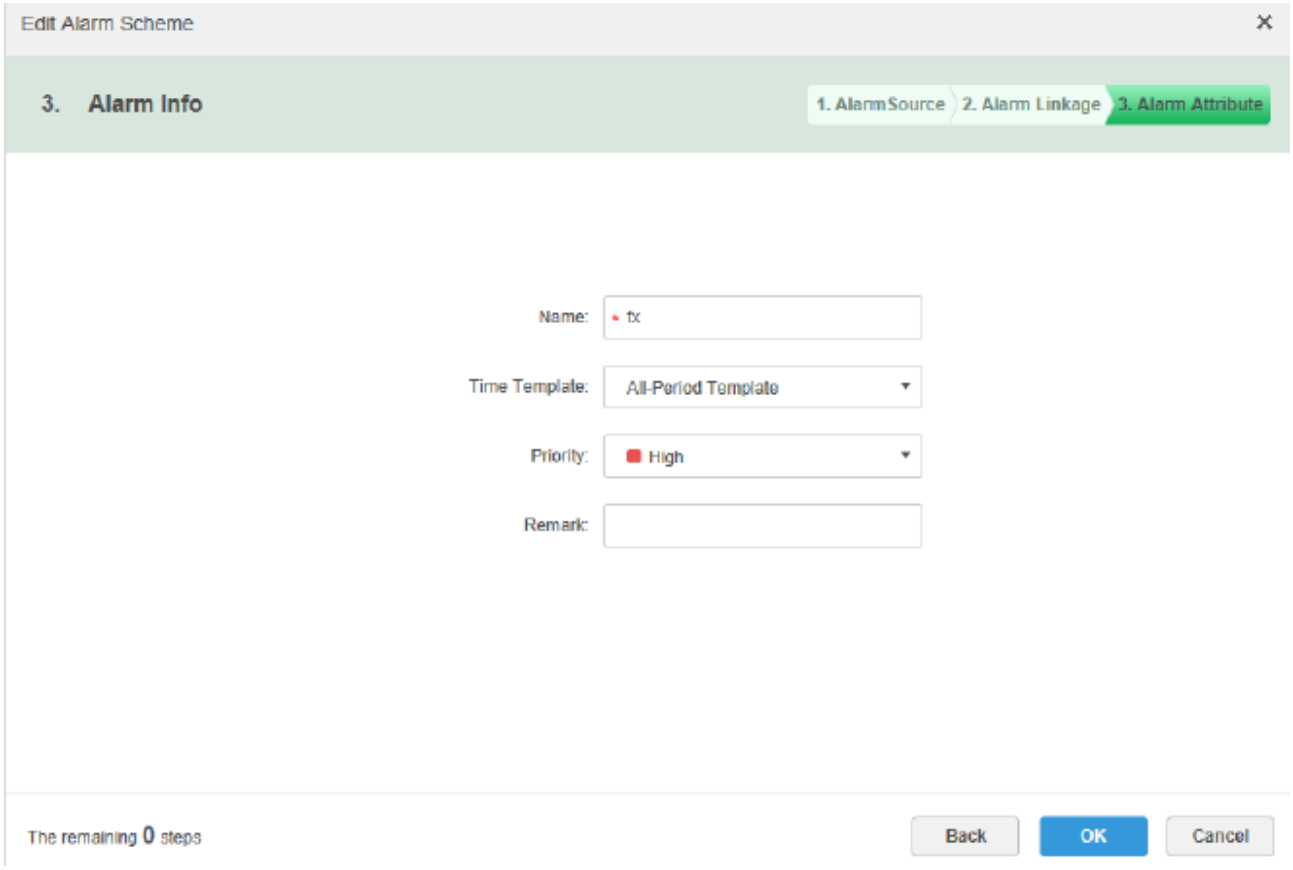
Figura 69 - Porta de ligação



Passo 2. Clique em atributo de alarme.

2.7.2 Configurar atributo de alarme

Figura 70 - Atributo de alarme



Passo 1. Configure o atributo de alarme.

- Defina o nome do alarme.
- Selecione o modelo de hora do alarme e a prioridade.
- Clique OK.
- Sistema exibe o esquema de alarme adicionado.

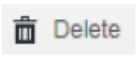
Passo 2. Na coluna Operação, clique em OFF para habilitar o esquema. Quando o ícone muda para ON, significa que o esquema foi habilitado.

Operações

- Editar

  Clique no do esquema correspondente, e então você pode editar o esquema de alarme.

- Excluir

Selecione o esquema de alarme, clique 

para excluir o esquema em lotes.

Clique no correspondente  do esquema de alarme, então você pode excluir o esquema de alarme individualmente.

- Desabilitar

  Na coluna Operação, clique em 

para desativar um evento. 

indica que o evento está desabilitado.

3 FUNÇÕES

Este capítulo apresenta a configuração e operação do cliente de monitoramento de vídeo, além da gestão de eventos de vídeo, analíticos, reconhecimento facial e LPR.

3.1 PREPARATIVOS

Instale o Cliente de monitoramento seguidos os passos abaixo.

3.1.1 Instalando o Cliente

O monitoramento de vídeo diário é feito através do Cliente de monitoramento e do cliente mobile.

3.1.1.1 Instalando o Cliente de monitoramento

3.1.1.1.1 Requisitos de instalação do cliente de controle

Para instalar o Cliente de monitoramento, prepare um computador de acordo com os seguintes requisitos.

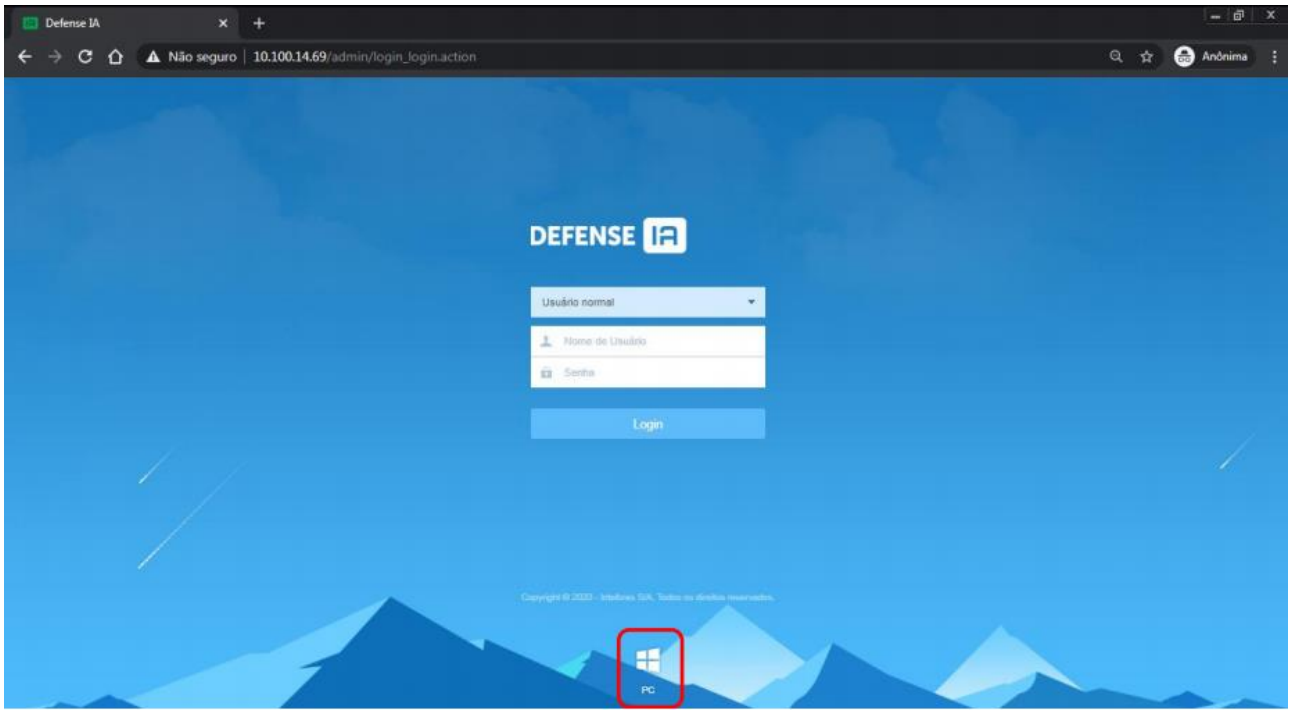
Tabela 3 - Requisitos de hardware

Parâmetros	Descrição
Configuração Recomenda	• CPU: i5-6500 • Frequência principal: 3,20 GHz • Memória: 8 GB • Gráficos: Inter HD Graphics 530 • Rede Placa: Placa de Rede Gigabit • Tipo de HDD: HDD 1T • DEFENSE IA espaço de instalação do cliente:200 GB
Configuração mínima	• CPU:i3-2120 • Memória:4 GB • Gráficos: Inter(R) Sandbridge Desktop Gra • Rede Placa: Placa de Rede Gigabit • Tipo de HDD: HDD 300 GB • DEFENSE IA espaço de instalação do cliente: 100 GB

3.1.1.1.2 Baixando e instalando o cliente de controle

Passo 1. Insira o endereço IP do Defense IA no navegador e pressione Enter.

Figura 71 - Faça login no gerenciador da web



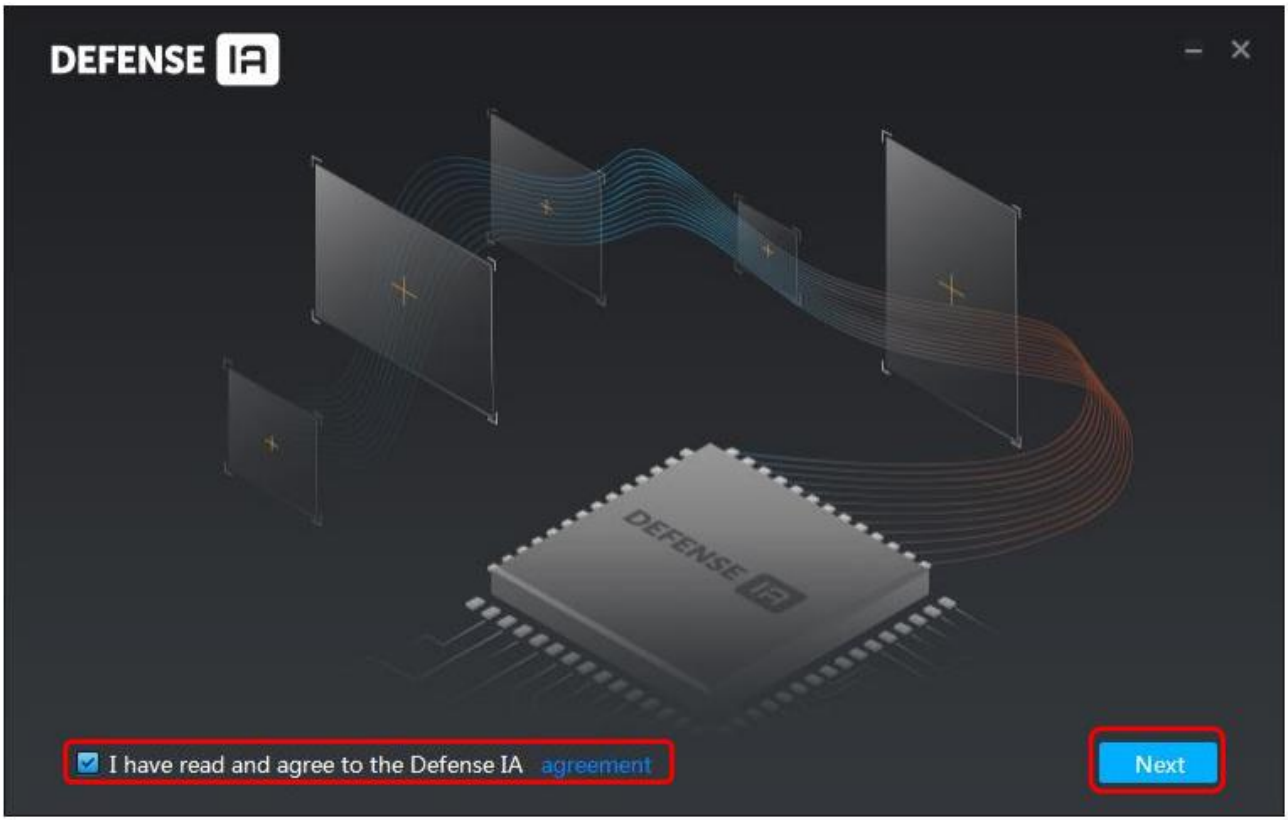
Passo 2. Clique em para baixar o Cliente de monitoramento.

A caixa de diálogo de Downloads de arquivos é exibida.

Passo 3. Clique em Salvar para salvar o pacote de software cliente no PC.

Passo 4. Clique duas vezes em setup.exe do cliente e comece a instalação.

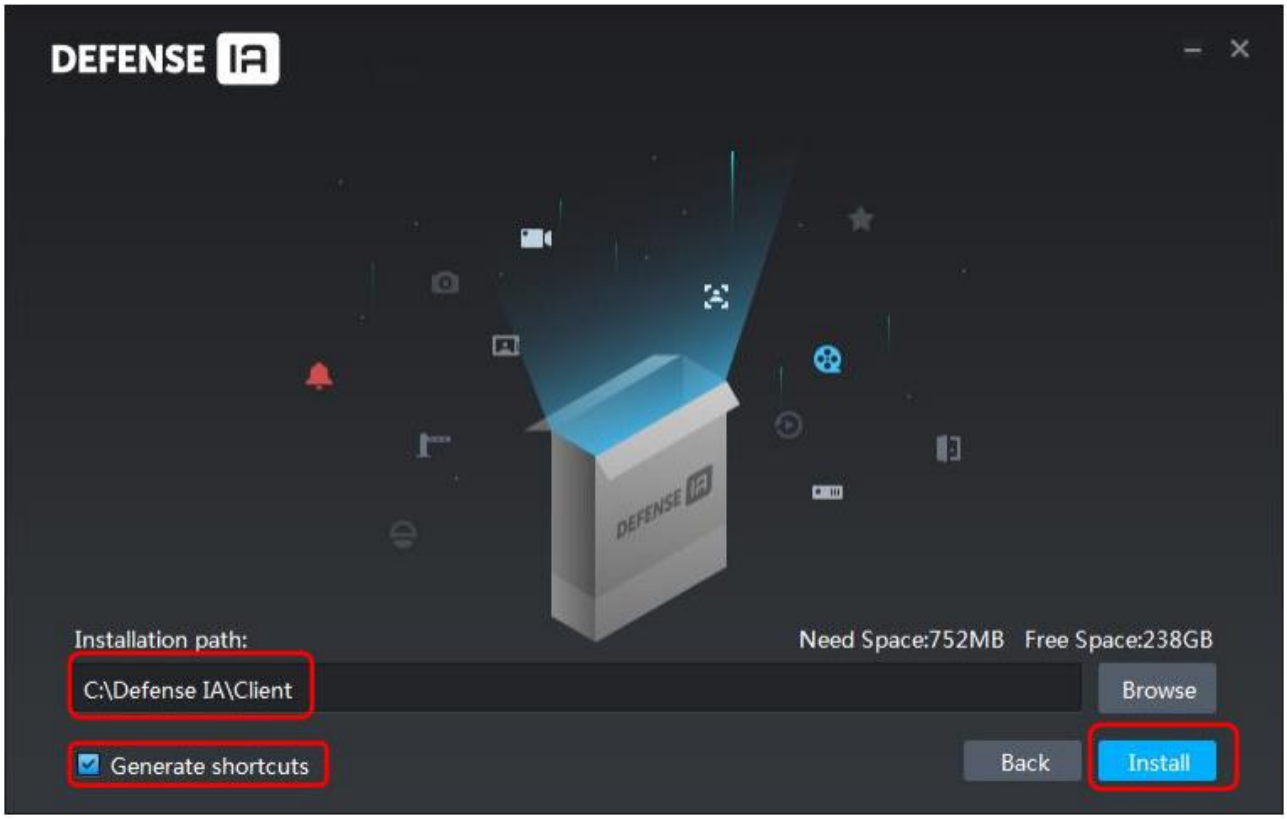
Figura 72 - Aceitar acordo



Passo 5. Selecione a caixa Li e concordo com o contrato DEFENSE IA e clique em Avançar para continuar.

Passo 6. Selecione o caminho de instalação.

Figura 73 - Definir caminho de instalação



Passo 7. Clique em Instalar para instalar o cliente.

O sistema exibe o processo de instalação. Leva de 3 a 5 minutos para ser concluído.

Por favor, seja paciente.

Figura 74 - Instalação completa

Passo 8. Clique em Executar para executar o cliente.

3.1.2 Login no cliente

Passo 1. Duplo clique no ícone 

que estará na área de trabalho.

- A primeira vez que você faz login, a seguinte interface é exibida.

Figura 75 - Login pela primeira vez

- Clique em Preencher Informações.

Figura 76 - Faça login no cliente de controle

Passo 2. Selecione o servidor detectado à esquerda da interface ou clique em Preencher informações do site, digite o endereço IP e o número da porta e clique em OK.

Passo 3. Digite o nome de usuário, a senha, o IP do servidor e a porta. IP do servidor significa o endereço IP para instalar o servidor Defense IA ou PC, a porta é 443 por padrão. Esta porta é configurável.

Passo 4. Clique em Login.

3.1.3 Página inicial do cliente de controle

Figura 77 - Página inicial

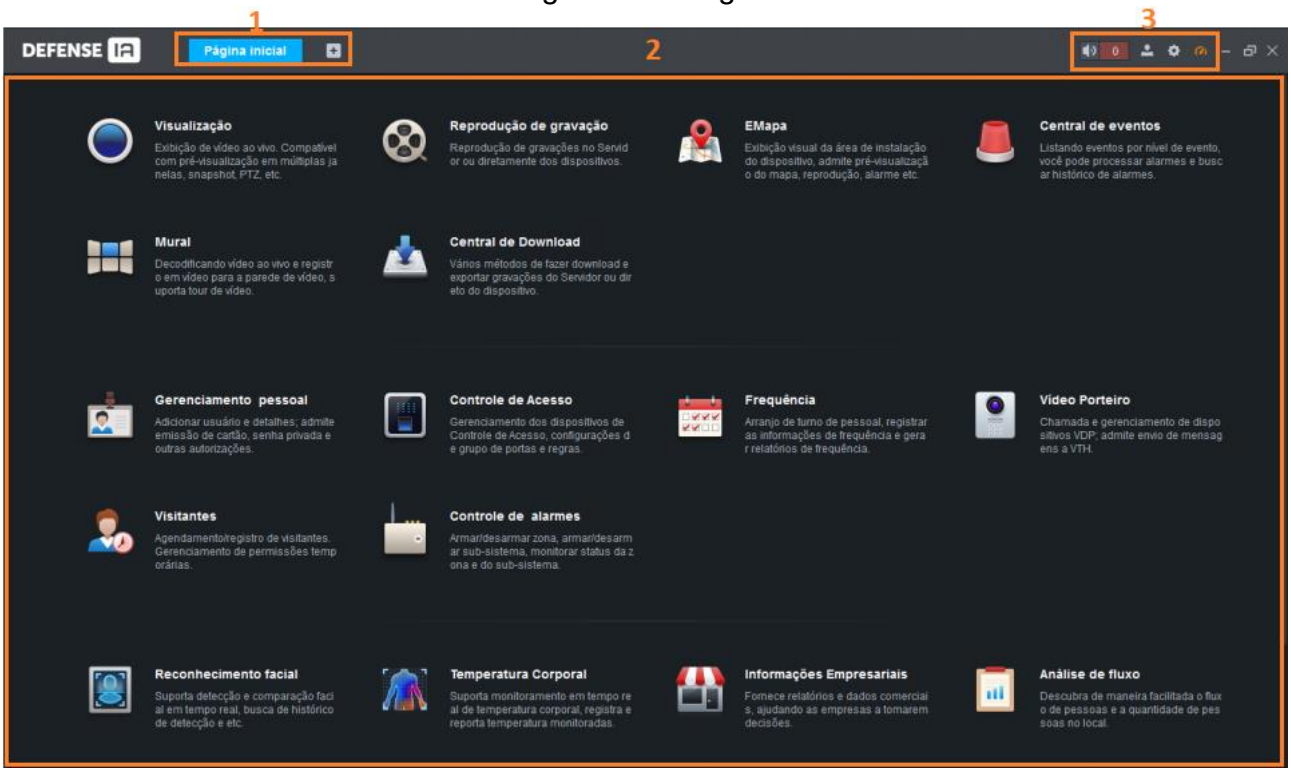


Tabela 4 - Descrição

N°.	Nome	Função
1	Aba	Exibir todas as guias válidas. Clique  e você pode abrir o módulo que deseja.
2	Aplicações	Acesse cada aplicação clicando no ícone
3	Definições do sistema	•  : Abrir / fechar o áudio do alarme. •  : Exibe a quantidade de alarmes. Clique no ícone para ir ao Central de Eventos. •  : Informações do usuário: clique no ícone e, em seguida, você pode fazer login na página Web clicando no endereço IP do sistema, modificar a senha, bloquear o cliente, visualizar o arquivo de ajuda e fazer logout. •  : Configuração local. Você pode definir as configurações gerais, configurações de vídeo, configurações de reprodução, configurações de instantâneo, configurações de gravação, configurações de alarme, vídeo wall, configurações de segurança e configurações de atalho. Vejo "3.1.4 Configuração local "para obter detalhes. •  : Visualize o status do sistema, incluindo status da rede, status da CPU e status da memória.

3.1.4 Configuração Local

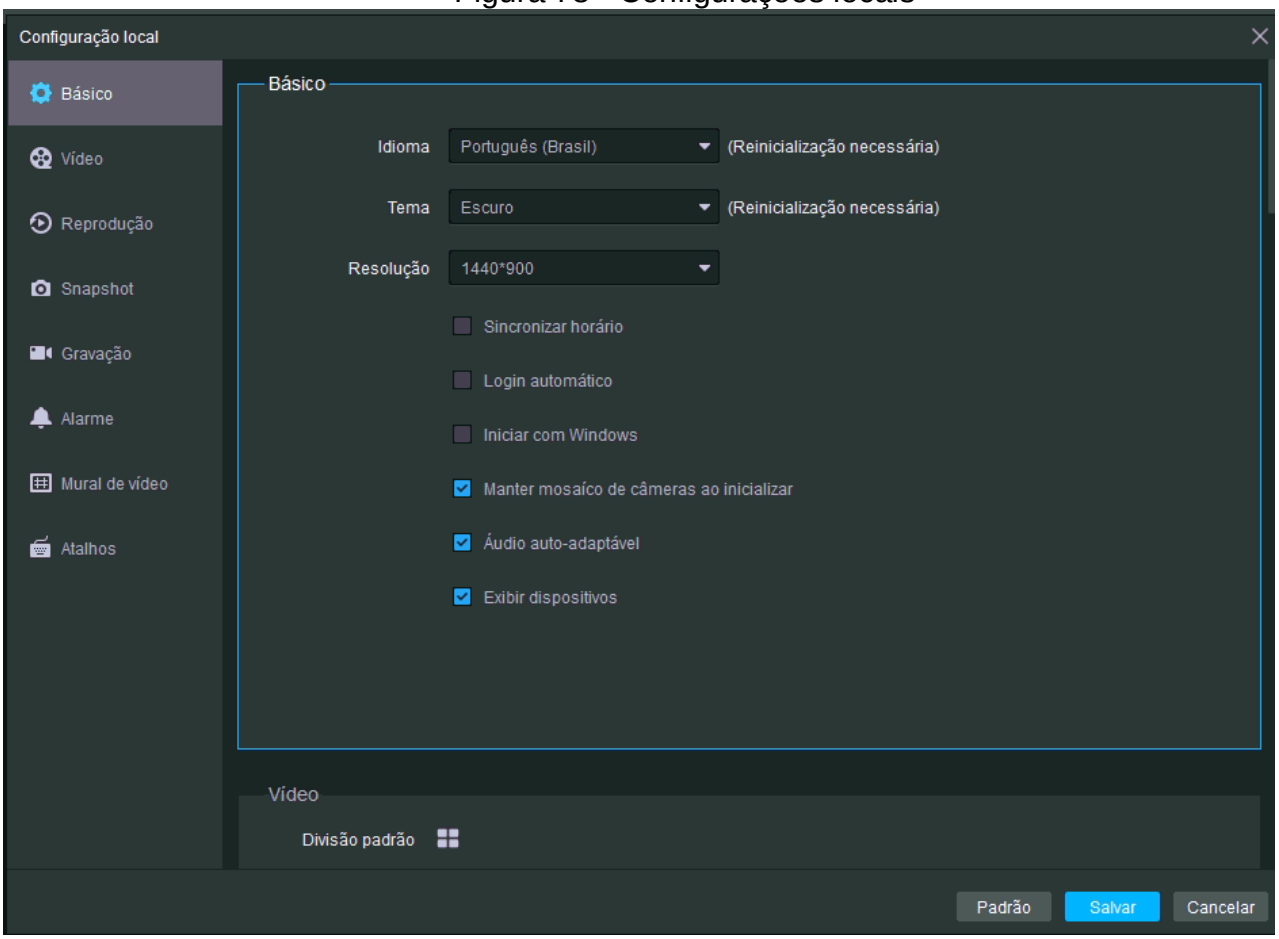
Depois de entrar para o cliente pela primeira vez, você precisa configurar os parâmetros do sistema envolvendo configurações básicas, parâmetros de vídeo, reprodução de gravação, snapshot, gravação, alarme, configurações de segurança e teclas de atalho.

3.1.4.1 Definição das configurações básicas

Configure o idioma do cliente, o tamanho do cliente e as configurações de hora.

Passo 1. Clique no canto superior direito da página inicial.

Figura 78 - Configurações locais



Passo 2. Clique em Básico para definir os parâmetros.

Tabela 5 - Parâmetros de vídeo

Parâmetros	Descrição
Idioma	Modifique o idioma exibido no cliente; reinicie o cliente para torná-lo válido após a configuração.

Parâmetros	Descrição
Tema	Defina a cor do tema do Cliente de Monitoramento. As opções são inclui Escuro e Branco. Reinicialize o cliente para torná-lo válido após a configuração.
Resolução	Selecione a resolução adequada do cliente de acordo com a tela do PC.
Sincronizar horário	Se marcado, o cliente irá sincronizar o horário do computador com o servidor do Defense IA.
Login automático	• E se **Lembrar senha** e **Login automático** são ambos selecionado na interface de Login, o Sistema irá pular a interface de login e abrir diretamente a página inicial na próxima vez que o Cliente de monitoramento for executado. • Se Lembrar senha não for selecionado enquanto Login automático estiver selecionado na interface de login, quando você fizer login novamente, você ainda precisará inserir a senha para fazer login.
Iniciar com o Windows	O cliente de monitoramento será executado automaticamente toda que vez que o Windows iniciar. Se Login Automático e Lembrar Senha não estiverem marcados, será necessário digitar o usuário e a senha.
Manter mosaico de câmeras ao inicializar	E se ativado, sistema o mosaico utilizado no momento que o software for fechado será carregado automaticamente depois reiniciando o cliente.
Áudio Auto adaptável	E se ativado, o sistema automaticamente adaptar para o áudio do cliente de monitoramento para o melhor possível a ser utilizado em uma conversar de áudio.
Exibir dispositivos	Exibe a árvore de dispositivos e os canais de vídeo abaixo de cada dispositivo. Caso contrário, ele exibe apenas canais.

Passo 3. Clique em Salvar.

3.1.4.2 Definição das configurações de Vídeo

Configure a divisão da janela, o tipo de transmissão e o modo de reprodução da exibição ao vivo e a duração da reprodução instantânea.

Passo 1. Clique no canto superior direito da página inicial.
Passo 2. Clique em Video para definir os parâmetros.

Figura 79 - Definir as configurações de vídeo

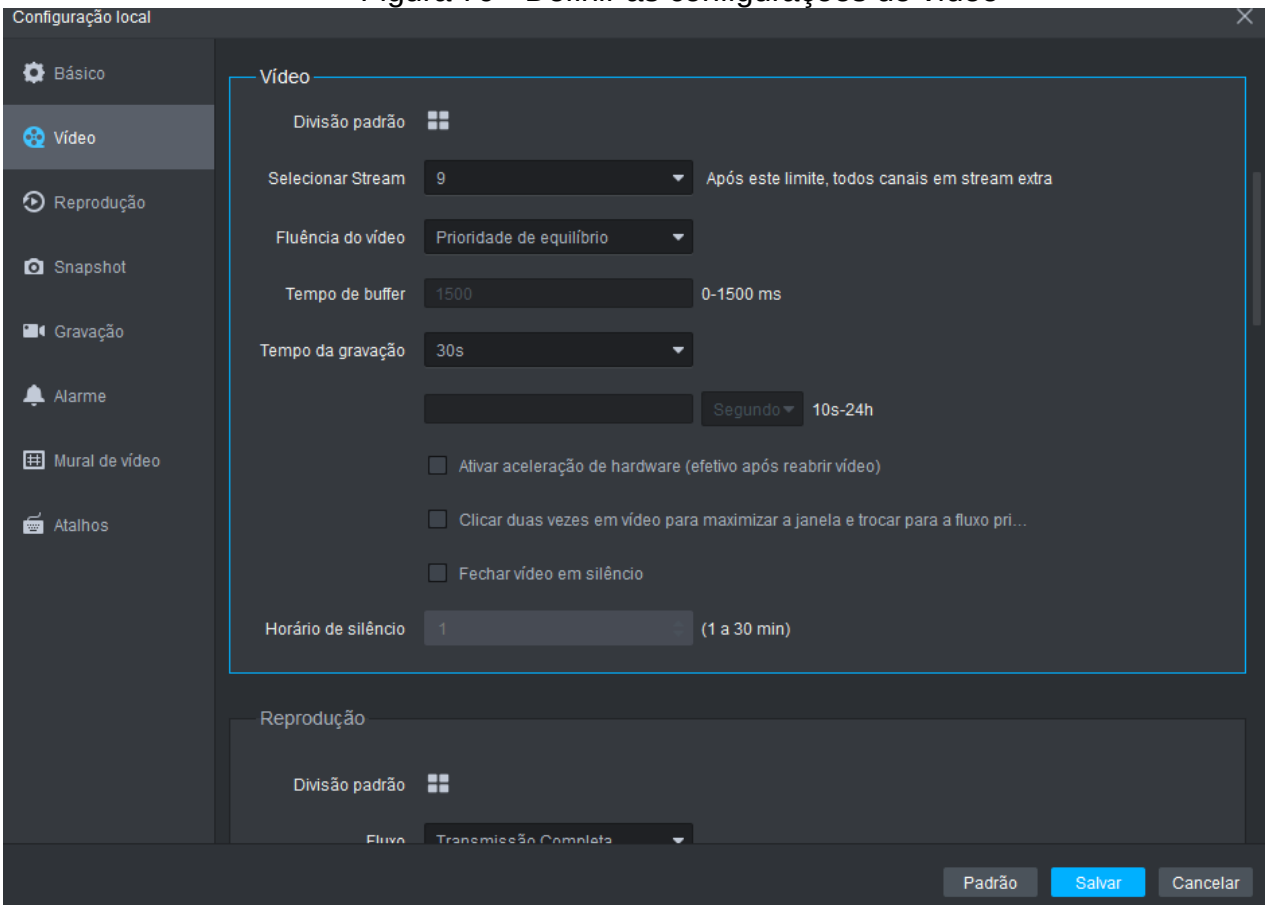


Tabela 6 - Parâmetros

Parâmetros	Descrição
Divisão Padrão	Definir divisão padrão da janela de visualização
Selecionar Stream	Se o número de streams aberto for igual ou maior que este número, o Defense IA irá abrir por padrão as câmeras como stream extra
Fluência de vídeo	Selecione o modo de fluência da exibição do vídeo. ● Prioridade de tempo real O sistema poderá diminuir a qualidade da imagem para evitar atrasos no vídeo. ● Prioridade de fluência O sistema pode diminuir a qualidade da imagem e permitir atrasos para garantir a fluência do 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 servidor real e o desempenho da rede. ● Customizar ● TO sistema ajusta o buffer de vídeo e reduz o impacto na qualidade do vídeo causado pela rede instável. Quanto maior o valor, mais estável será a qualidade do vídeo.

Parâmetros	Descrição
Tempo de Buffer	Configura o tempo de buffer de vídeo. Só é acessível quando a Fluência de Vídeo esta no moodo personalizado.
Tempo de gravação	Clique na interface de Visualização ao Vivo para reproduzir o vídeo no período configurado neste campo.Por exemplo, se você definir 30 s, o sistema reproduzirá o vídeo dos 30 s anteriores.
Ativar aceleração de hardware (Efetivo após reabrir o vídeo)	Habilitar a função para usar a atual GPU do computador para decodificação, de modo a reduzir o consumo da CPU e garantir a fluência do vídeo. Requisitos de GPU: • ATI HD2000 ou superior • NVIDIA Gefoce 8200 ou superior • Intel X4500 HD
Clicar duas vezes em vídeo para maximizar a janela e trocar para o fluxo primário	Selecione esta opçõa para habilitar a função. Se ativado, você pode clicar duas vezes em um vídeo janela para maximizar e mude de fluxo secundário para fluxo principal.
Fechar vídeo em silêncio	O sistema fecha a Visualização ao Vivo automaticamente após inatividade pelo período pré-definido.
Horário de silêncio	

Passo 3. Clique em Salvar.

3.1.4.3 Definição das configurações de reprodução

Configure o tipo de fluxo e a divisão da janela de reprodução.

Passo 1. Clique no canto superior direito da página inicial.
Passo 2. Clique em Gravar reprodução para definir os parâmetros.

Figura 80 - Definir as configurações de reprodução

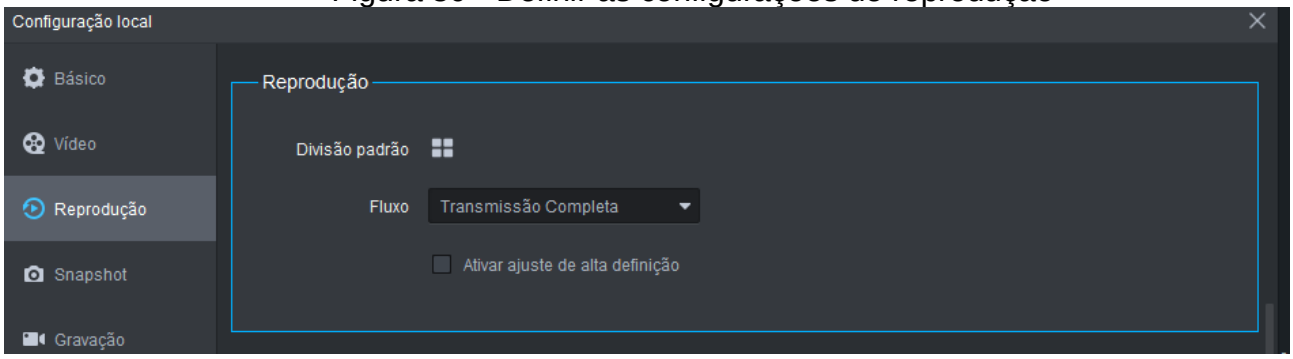


Tabela 7 - Parâmetros

Parâmetros	Descrição
Divisão Padrão	Definir divisão padrão da janela de reprodução

Parâmetros	Descrição
Fluxo	Selecione um tipo de stream padrão para reprodução de vídeo. Suporte selecionando de Main Stream, Sub Stream ou All Stream. Se não houver vídeo do tipo de stream selecionado, o sistema não reproduzirá o vídeo.
Ativar ajuste de alta definição	Se habilitado, quando o fluxo de reprodução é grande devido à alta definição, o sistema reserva quadros I para garantir a fluência do vídeo e reduzir a decodificação e largura de banda.

Passo 3. Clique em Salvar.

3.1.4.4 Definição de configurações de instantâneo

Configure o formato e o diretório de armazenamento das imagens capturadas durante a exibição ao vivo e a reprodução.

Passo 1. Clique no canto superior direito da página inicial.
Passo 2. Clique em Snapshot para definir os parâmetros.

Figura 81 - Definir configurações de snapshot

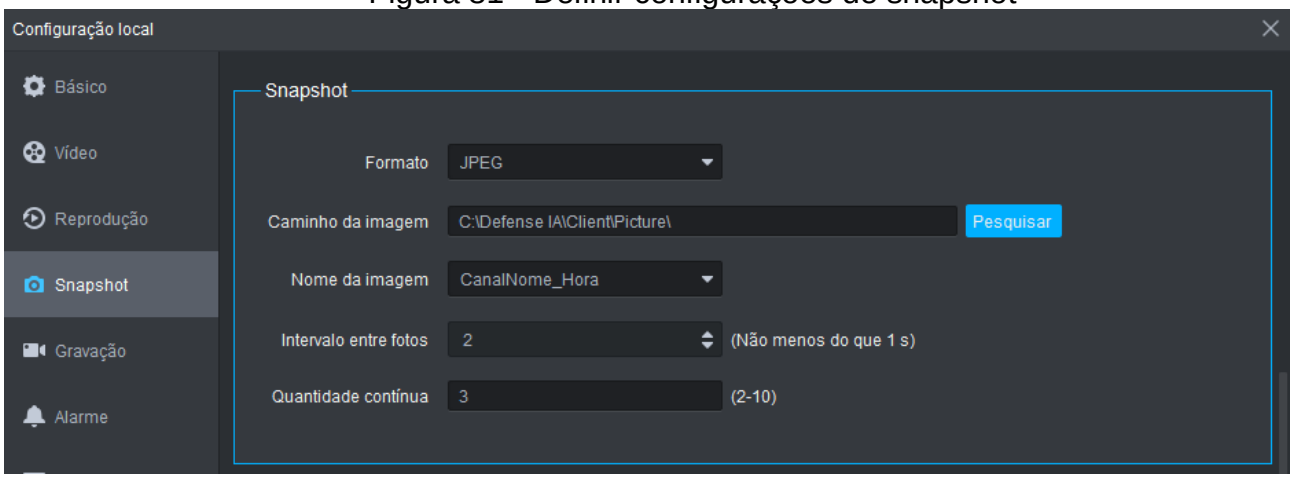


Tabela 8 - Parâmetros

Parâmetro	Descrição	
Formato	Escolhe o formato de imagem instantânea. Suporta BMP e JPEG.	Snapshot aqui se refere à função de Snapshot durante a exibição ao vivo ou reprodução.
Caminho da imagem	Configura o caminho de armazenamento de snapshot.	
Nome da imagem	Configura a regra de nomenclatura das imagens	
Intervalo entre fotos	Configura o intervalo e número de snapshots. Por exemplo, se o intervalo de snapshot for 10 e a Quantidade contínua for 4, quando você clicar com o botão direito na Vídeo ao vivo ou na Reprodução e seleciona Snapshot no menu, 4 fotos serão capturadas de uma vez e o intervalo de tempo entre elas é de 10 segundos.	
Quantidade Contínua		

Passo 3. Clique em Salvar.

3.1.4.5 Definição das configurações de gravação

Configure o diretório de armazenamento e o nome dos vídeos gravados manualmente durante a exibição ao vivo e a reprodução.

Passo 1. Clique no canto superior direito da página inicial.
Passo 2. Clique em Gravação para definir os parâmetros.

Figura 82 - Definir as configurações de gravação

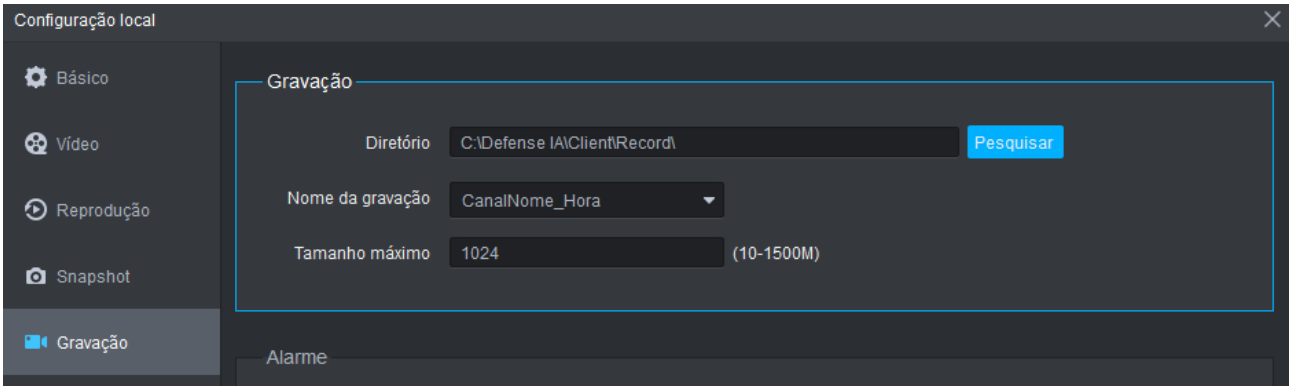


Tabela 9 - Parâmetros

Parâmetros	Descrição
Diretório	Configura o caminho do armazenamento dos arquivos de gravação manual durante a exibição ao vivo ou reprodução.
Nome da gravação	Configura a regra de nomenclatura do nome dos vídeos.
Tamanho máximo	Configura o tamanho do arquivo de vídeo.

Passo 3. Clique em Salvar.

3.1.4.6 Definição das configurações de alarme

Configure o som do alarme e o método de exibição do alarme no cliente.

Passo 1. Clique no canto superior direito da página inicial.
Passo 2. Clique em Alarme para definir os parâmetros.

Figura 83 - Definir configurações de alarme

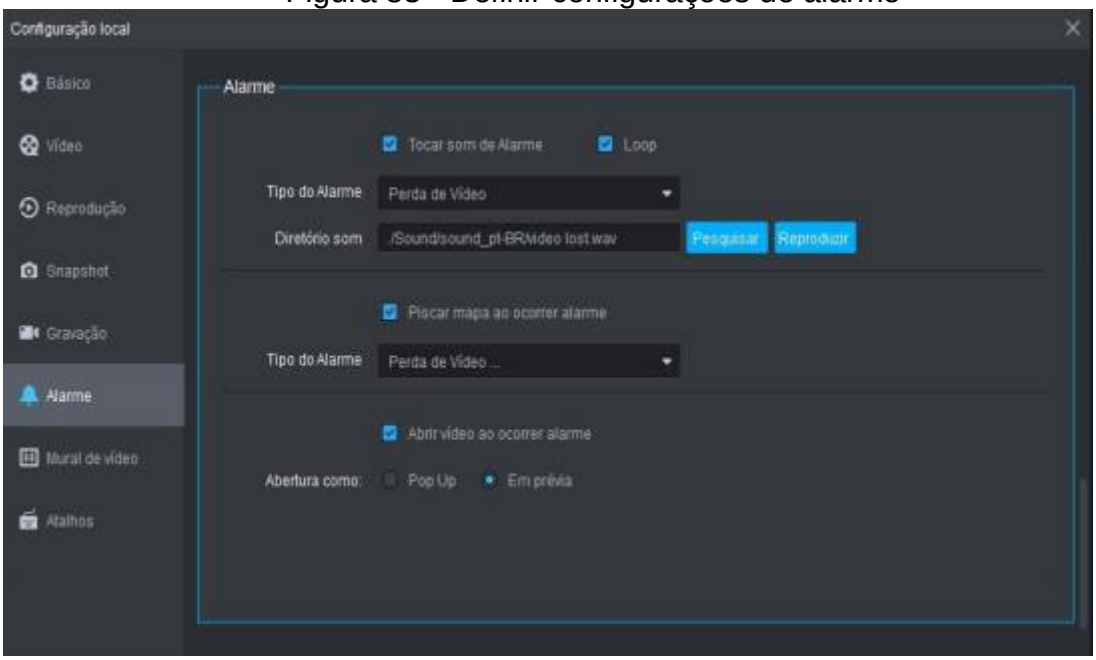


Tabela 10 - Parâmetros

Parâmetros	Descrição
Tocar som de alarme	O som do alarme é acionado no computador cliente quando o cliente recebe um alarme. Você pode configurar diferentes tipos de som para diferentes alarmes, de modo que, quando um alarme for disparado,
Ciclo	
Tipo de Alarme	

Parâmetros	Descrição
Caminho do Som	você saiba imediatamente o que acontece. Você pode fazer upload de arquivos de som locais enquanto o alarme soa. • Selecione a caixa de seleção Tocar som do alarme para habilitar o som do alarme. • Selecione Loop para habilitar a reprodução de loop do som para aviso repetido. • Selecione Tipo de alarme para definir o som do alarme para o tipo de alarme selecionado. Clique em Procurar para selecionar o arquivo de som local como aviso de alarme.
O mapa pisca quando o alarme ocorre	Define tipo de alarme para notificação de alarme no mapa. Quando ocorre o alarme correspondente, o dispositivo no mapa vai instantâneo.
Exibir vídeo do link do alarme quando o alarme ocorrer	Se ativado, o sistema abrirá automaticamente a interface de vídeo vinculada quando ocorrer um alarme.
Tipo de abertura de vídeo	Se Pop Up for selecionado, o vídeo de alarme será reproduzido em uma instante janela de pop-up; se In Preview selecionado, o vídeo de alarme será reproduzido na interface de exibição ao vivo.

Passo 3. Clique em Salvar.

3.1.4.7 Definição das configurações do Mural de Vídeo

Configure o modo de ligação padrão e o tipo de fluxo de parede de vídeo.

Passo 1. Clique no canto superior direito da página inicial.
Passo 2. Clique em Video Wall para definir os parâmetros.

Figura 84 - Definir configurações de vídeo wall

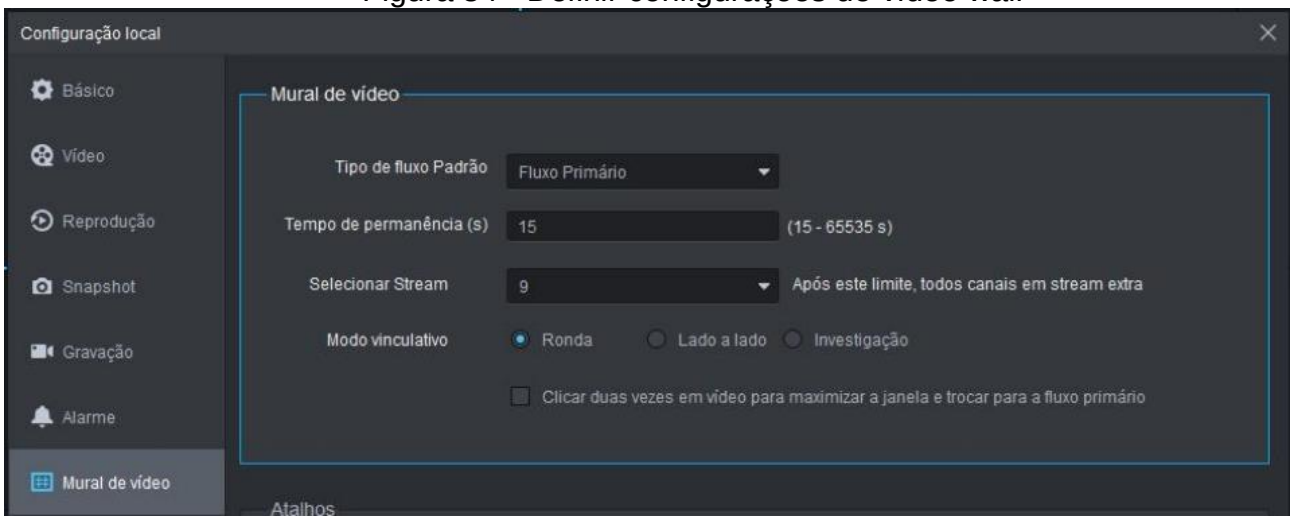


Tabela 11 - Parâmetros

Parâmetro	Descrição
Tipo de fluxo padrão	Selecione Fluxo primário, Fluxo secundário ou Local Sinal como o tipo de transmissão padrão para exibição de vídeo wall.
Tempo (s) de estadia	Defina o intervalo de tempo padrão entre os canais para o tour exibição. Por exemplo, se o tempo de permanência for cinco segundos e três vídeos canais estão mudando em uma janela (Tour), o vídeo alternar entre os três canais a cada cinco segundos
Tipo de fluxo	Defina o limite do número de divisão da janela. Por exemplo, se você selecione nove aqui, quando o número da divisão atingir ou exceder nove, todos os nove canais serão decodificados no fluxo secundário; caso contrário, o tipo de decodificação é stream principal.
Obrigatório Mtributo	● Tour: Múltiplos canais de vídeo mudam para decodificar em uma janela por padrão. ● Bloco: Os canais de vídeo são exibidos nas janelas por bloco por padrão. ● Consulta: Ao arrastar um canal para a janela, o sistema solicitará que você selecione o modo tour ou bloco.
Clique duas vezes no vídeo para maximizar a janela e trocar para a transmissão principal	Duplo clique em o vídeo para maximizar a janela, e entretanto, o tipo de stream mudará para stream principal.

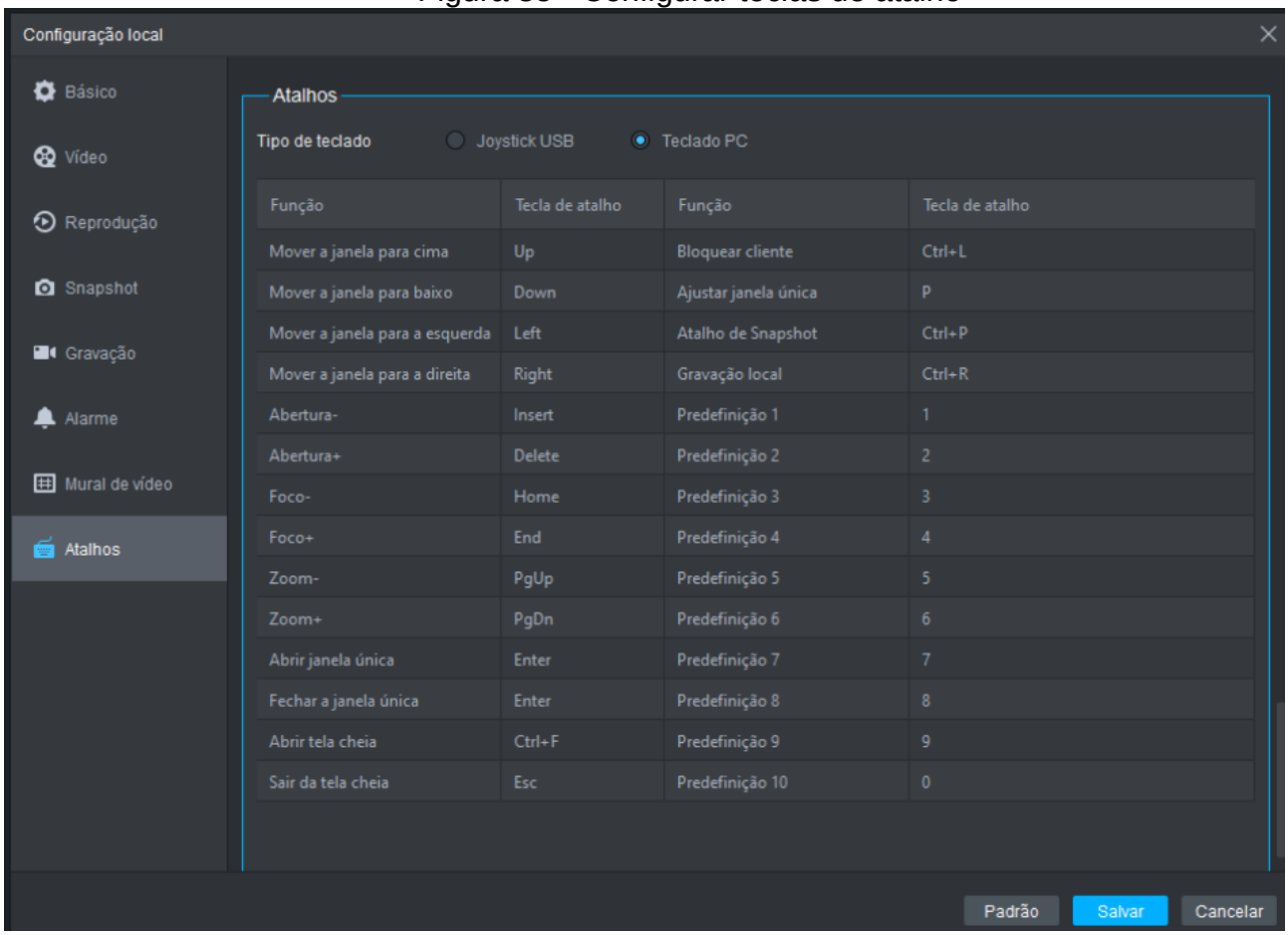
Passo 3. Clique em Salvar.

3.1.4.8 Tecla de atalhos

Configure as teclas de atalho para operação rápida do cliente.

Passo 1. Clique no canto superior direito da página inicial.
Passo 2. Clique em tecla de atalho para visualizar as teclas de atalho do teclado do computador e joystick USB.

Figura 85 - Configurar teclas de atalho



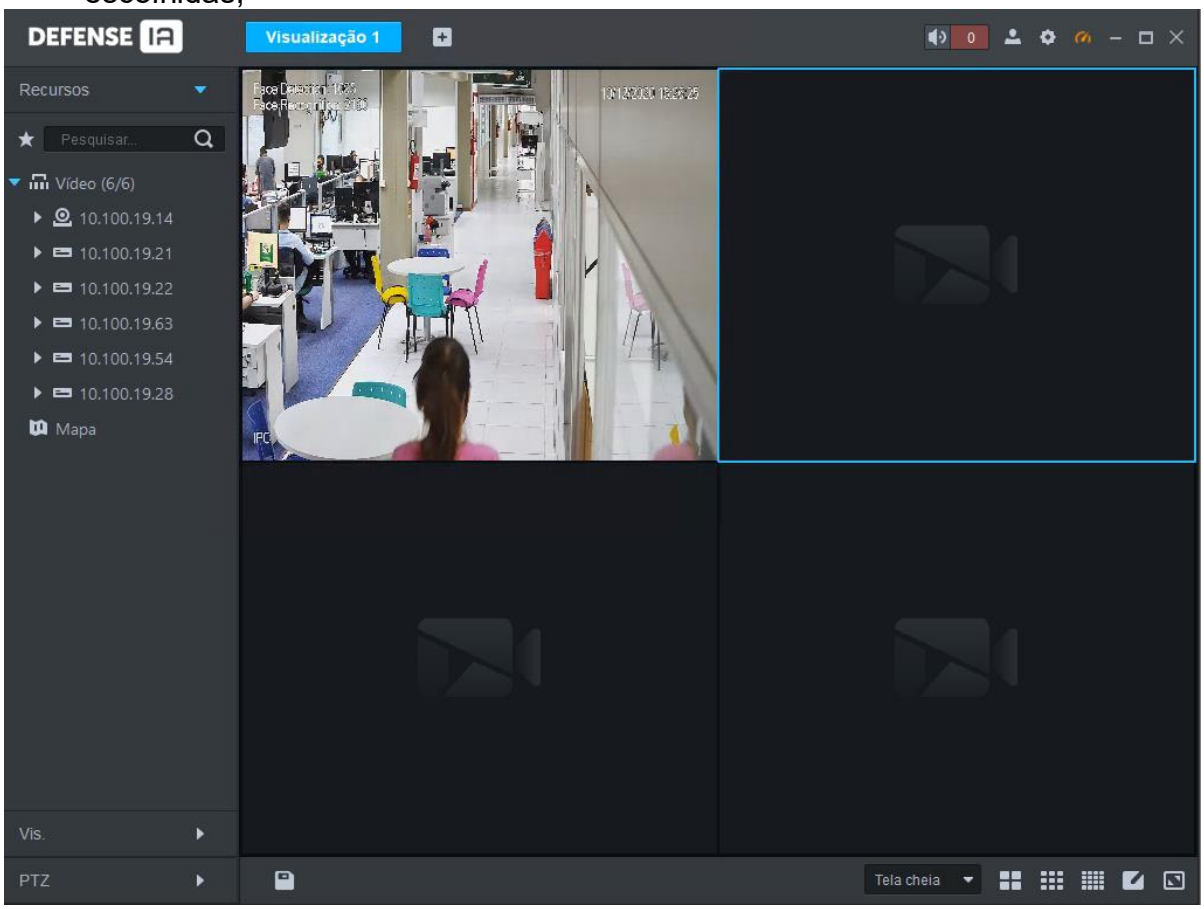
Passo 3. Clique em Salvar.

3.2 VISUALIZAÇÃO

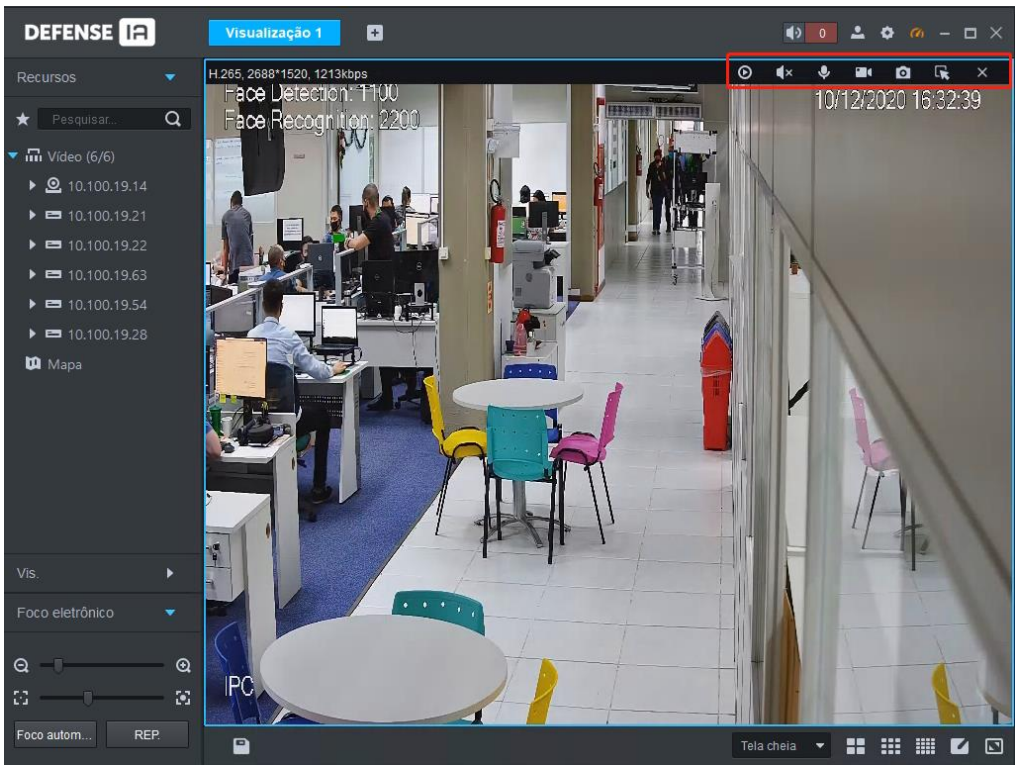
3.2.1 Visualizando Vídeo ao Vivo

Passo 1. Faça o Login no Defense Cliente
Passo 2. Selecione o menu Visualização
Passo 3. Clique duas vezes ou arraste um dispositivo da lista a esquerda para a tela da direita para visualizar ele em tempo real.

- Para visualizar todos os canais de um DVR ou SVR, arraste ele para a tela a direita, isso abrirá todos os dispositivos na quantidade de telas previamente escolhidas;



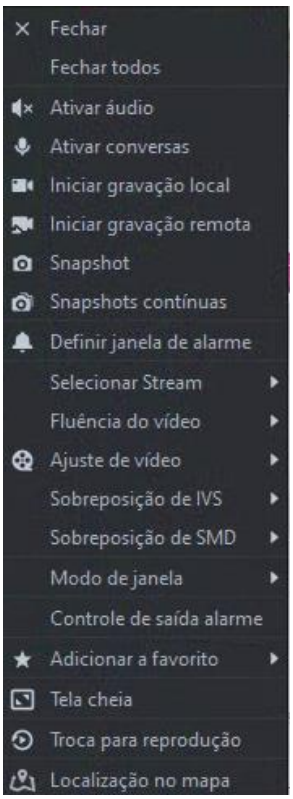
Passo 4. Você pode realizar operações durante a visualização ao vivo, no menu acima da janela de visualização. Conforme imagem a seguir.



Ícone	Nome	Descrição
	Gravação Instantânea	Abre / fecha a reprodução instantânea. Vá para Configuração local> Geral para definir o tempo de reprodução instantânea. Certifique-se de que haja um registro na plataforma ou no dispositivo.
	Áudio	Habilita/Desabilita o áudio
	Ativar conversas	Habilita/Desabilita o áudio bidirecional
	Gravação Local	O sistema começará a gravar a visualização ao vivo em um arquivo local e você poderá ver o tempo de gravação no canto superior esquerdo. Clique novamente e o sistema interrompe a gravação e salva o arquivo no computador.
	Snapshot	Clique para tirar um print da tela
	Zoom	Possibilita dar um Zoom digital na imagem.
	Fecha	Fecha a visualização.

Na janela de visualização ao vivo, clique com o botão direito do mouse e o menu de atalho será exibido.

Este menu poderá variar dependendo das inteligências que o dispositivo possui.

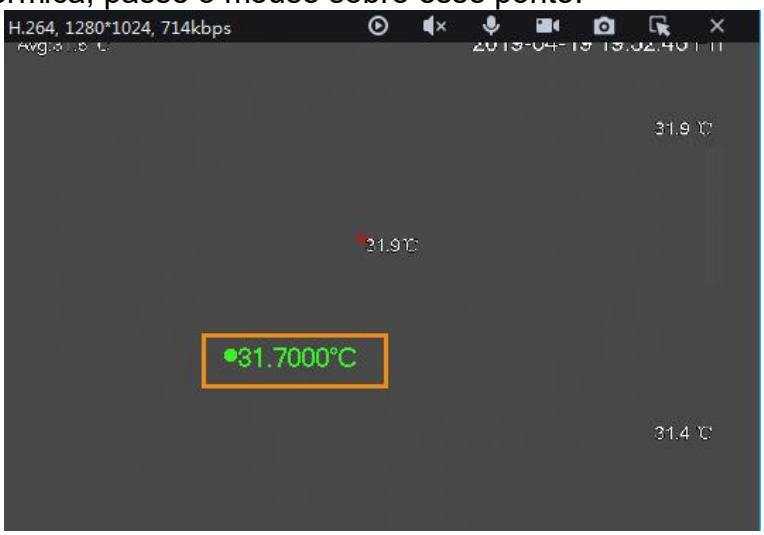


Nome	Descrição
Fechar	Fecha a janela atual
Fechar Todas	Fecha todas as janelas de visualização
Ativar áudio	Para ativar ou desativar o áudio da câmera.
Seleção de entrada de áudio	Se a câmera tiver mais de um canal de entrada de áudio, você pode selecionar um ou selecionar o áudio mixado. Esta configuração é eficaz tanto com visualização ao vivo quanto com reprodução.
Ativar conversas	Habilita/Desabilita o áudio bidirecional
Iniciar gravação local	O sistema começará a gravar a visualização ao vivo em um arquivo local e você poderá ver o tempo de gravação no canto superior esquerdo. Clique novamente e o sistema interrompe a gravação e salva o arquivo no computador.
Iniciar gravação remota	Clique para iniciar a gravação remota. Clique em Parar gravação remota e o sistema interromperá a gravação. Se a plataforma tiver configurado HD de armazenamento de vídeo, o arquivo de gravação será salvo no servidor da plataforma.
Snapshot	Clique para tirar um print da tela
Snapshots contínuas	Tire um print da imagem atual (três prints de cada vez por padrão).
Definir janela de alarme	Liga/desliga a saída de alarme

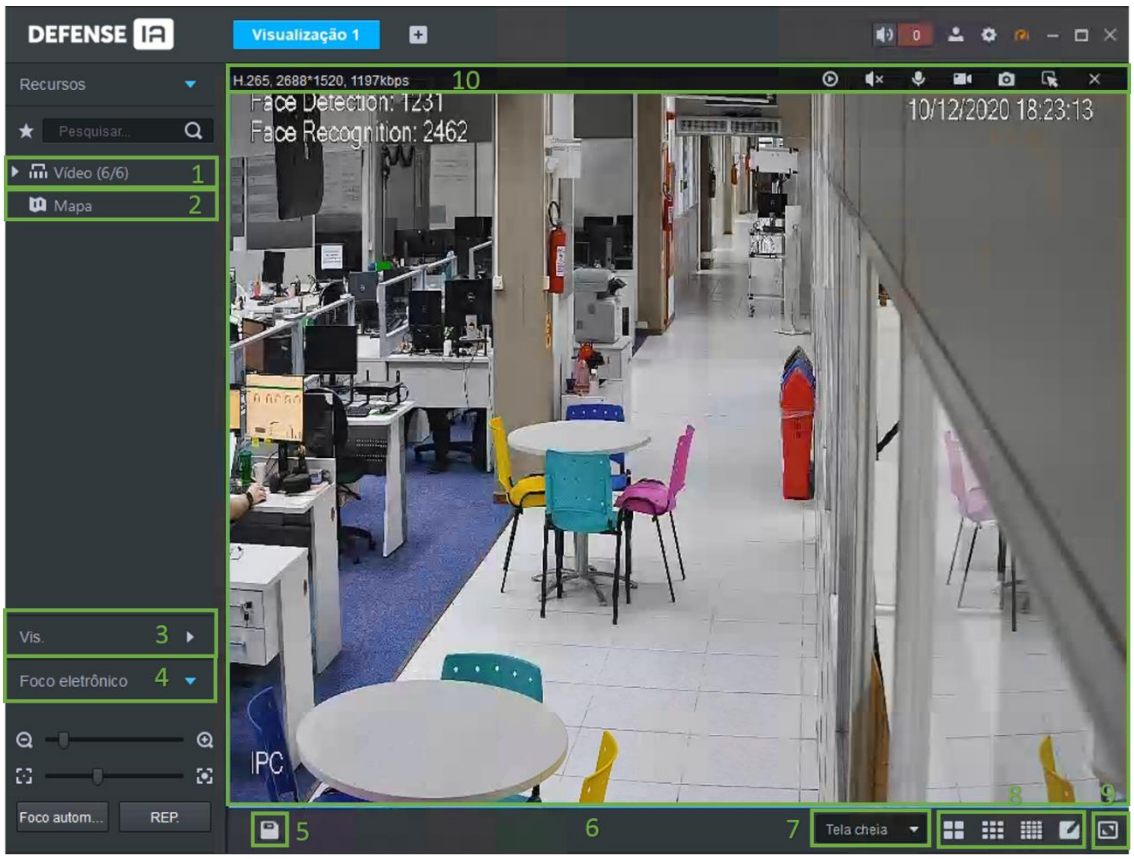
Nome	Descrição
Selecionar Stream	Alternar entre fluxo primário, fluxo secundário 1 e fluxo secundário 2. Você pode alternar o tipo de fluxo de vídeo quando o vídeo não estiver fluído o suficiente devido ao grande tamanho do fluxo ou largura de banda baixa. Grau de consumo de largura de banda: Fluxo primário > Fluxo secundário 1 > Fluxo secundário 2.
Fluência de vídeo	Alterne entre os modos de Prioridade de tempo real, Prioridade de fluência, Prioridade de equilíbrio e Personalizar. • Prioridade de tempo real: O sistema pode diminuir a qualidade da imagem para evitar atrasos no vídeo. • Prioridade de fluência: O sistema pode diminuir a qualidade da imagem e permitir atrasos para garantir a fluência do 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 servidor real e o desempenho da rede. • Personalizar: O sistema ajusta o buffer de vídeo e reduz o impacto na qualidade do vídeo causado por rede instável. Quanto maior o valor, mais estável será a qualidade do vídeo.
Ajuste de vídeo	Faça o ajuste e o aprimoramento do vídeo
Sobreposição de IVS	O cliente não mostra linhas de sobreposição sobre o vídeo ao vivo por padrão. Quando necessário, você pode clicar em **Sobreposição de IVS** e ativar **Sobreposição de regra** e **Sobreposição de objeto** e, em seguida, o vídeo ao vivo mostra linhas de sobreposição se as regras de detecção de IA estiverem habilitadas no dispositivo.
Sobreposição de SMD	Habilite **a Sobreposição de SMD** para mostrar o quadro alvo sobre o vídeo ao vivo. Quando SMD está habilitado no dispositivo, você pode habilitar **a Sobreposição de SMD** para o canal do dispositivo, e então o vídeo ao vivo exibirá quadros de destino dinâmicos. Esta configuração é efetiva com o canal selecionado atualmente tanto na exibição ao vivo quanto na reprodução.
Mapa de densidade de multidão aberta	Esta função está disponível apenas para câmera panorâmica multisensor + câmera PTZ. Depois de selecionar esta função, a densidade da multidão será exibida na imagem do vídeo. Clique duas vezes na imagem para ocultá-la e as pessoas no vídeo serão mostradas em pontos azuis.
Desativar máscara de privacidade	Para uma câmera que oferece suporte ao mascaramento de privacidade de rosto humano, você pode desativar o mascaramento aqui para visualizar a imagem do rosto.
Modo de instalação	Apenas para câmera fisheye. Ao alterar o fluxo de vídeo, o modo de visualização fisheye mantém a configuração antes de o fluxo ser alterado. De acordo com diferentes métodos de instalação, a visualização fisheye pode ser variada. • Teto: 1P + 1, 2P, 1 + 2, 1 + 3, 1 + 4, 1P + 6, 1 + 8. • Parede: 1P, 1P + 3, 1P + 4, 1P + 8. • Solo: 1P + 1, 2P, 1 + 3, 1 + 4, 1P + 6, 1 + 8.
Modo de janela	• Modo normal • Modo 1+3 • Modo 1+5

Nome	Descrição
Controle de saída alarme	Habilite ou desabilite a entrada / saída de alarme do canal.
Adicionar a favorito	Você pode adicionar o canal atual ou todos os canais aos Favoritos.
Tela cheia	Mude a janela de vídeo para o modo de tela inteira. Para sair da tela inteira, clique duas vezes na janela do vídeo ou clique com o botão direito para selecionar sair da tela inteira.
Troca para reprodução	Alterne entre a interface de exibição ao vivo atual e a interface de reprodução rapidamente, sem voltar para a página inicial primeiro.
Localização no mapa	Exibe a localização do dispositivo atual no mapa.

- Durante a exibição do tour, para sair do tour, clique em ; para fazer uma pausa, clique .
- Para visualizar a temperatura em tempo real de um ponto na visualização da câmera térmica, passe o mouse sobre esse ponto.



Consulte a imagem a seguir para obter uma introdução à interface de visualização ao vivo.



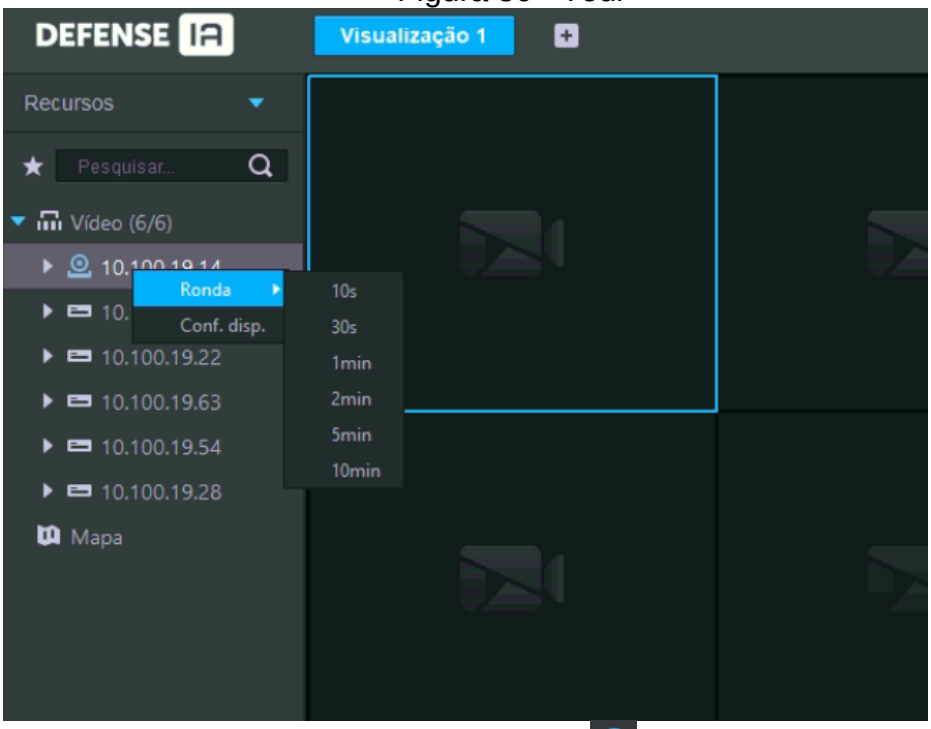
Nº.	Nome	Função
1	Recursos	• Você pode pesquisar um dispositivo ou canal por nome em Search... . Na pesquisa é possível que você possa simplesmente inserir parte do nome e selecionar o nome exato da lista de nomes fornecidos. • : Adicionar, excluir ou renomear os favoritos. A exibição de tours de canais favoritos é suportada. • Se você ativar Mostrar nó do dispositivo em Configuração local > Configuração básica, a árvore de dispositivos exibirá os dispositivos e seus canais; caso contrário, a árvore exibe apenas canais.
2	Mapa	O mapa pode ser aberto na janela de visualização, tanto o mapa GIS quanto o mapa Raster.
3	Vis.	• Salve a visualização atual da divisão da janela e dos canais de vídeo na seção de visualização ao vivo e nomeie a visualização. Você pode selecionar a visualização diretamente na guia Visualização para exibi-la rapidamente na próxima vez. Canais em uma visão ou grupo de visão podem ser exibidos por tour (por sua vez). Você pode definir o intervalo do tour como 10s, 30s, 1min, 2min, 5min ou 10min. Podem ser criadas no máximo 100 visualizações.
4	Foco eletrônico	Menu para operar as câmeras speed domes
5	Salv.	Clique para salvar a janela de vídeo atual como uma visualização.
6	Visualização	Reprodução de vídeo em tempo real. Aponte para a janela de reprodução de vídeo e você pode rolar para frente para aumentar o zoom e para trás para diminuir o zoom.

Nº.	Nome	Função
7	Modo de exibição	Proporção da janela de vídeo, selecionada a partir de dois modos de reprodução de vídeo: escala real e janela de ajuste.
8	Modo de divisão de janela	Defina o modo de divisão da janela. Suporta 1, 4, 6, 8, 9, 13, 16, 20, 25, 36 ou 64 divisões ou clique para definir um modo de divisão personalizado. Se o número do canal de exibição ao vivo for maior que o número de janelas atuais, você pode virar a (s) página (s) clicando em na parte inferior da interface.
9	Tela cheia	Mude a janela de vídeo para o modo de **Tela cheia**. Para sair da **Tela cheia**, você pode pressionar a tecla Esc ou clicar com o botão direito do mouse no vídeo e selecionar Sair da tela inteira.
10	Dados e ações	Dados de informação da câmera, como compressão de vídeo, dados de rede. Reprodução instantânea, áudio, áudio bidirecional, gravação manual, tirar uma foto, aumentar o zoom e muito mais.

3.2.5 Tour

Na interface **Visualização**, clique com o botão direito em um dispositivo ou nó, selecione **Tour** e selecione um intervalo. Os canais sob este dispositivo ou nó serão reproduzidos sucessivamente no intervalo predefinido. Você também pode personalizar o intervalo.

Figura 86 - Tour



Para interromper a reprodução da Tour, clique ou clique com o botão direito na janela e selecione Parar.

Para sair da reprodução do tour, clique em ; para fazer uma pausa, clique .

3.2.6 Visualização

O layout e os recursos atuais podem ser salvos como uma visualização para reprodução rápida na próxima vez.

3.2.6.1 Criando Visualização

As visualizações são categorizadas em grupos diferentes, convenientes para gerenciamento e uso rápido. O grupo inclui três níveis, nó raiz de primeiro nível, agrupamento de segundo nível e visualização de terceiro nível.

Passo 1. Faça login no Defense Client, clique em e selecione Visualização.
Passo 2. Crie um grupo de exibição.

1. Abra a janela de Visualização.
2. Clique com o botão direito na Aba de Vis. em Exibir e selecione Nova pasta.
3. Digite o nome da pasta e clique em OK.

Passo 3. Criar visualização.

1. Na aba de Visualização, selecione os dispositivos e o formato de visualização de acordo com suas necessidades e clique em Salvar .
2. Digite o nome da exibição, selecione Exibir grupo e clique em OK.

3. Para visualizar os grupos salvos, basta clicar no lado direito.

3.2.7 Favoritos

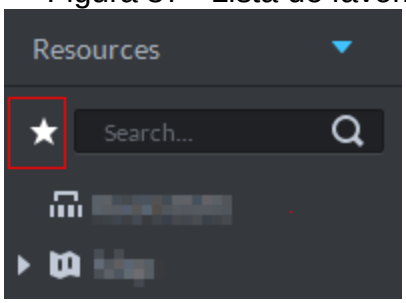
Adicione canais usados com frequência aos favoritos para realizar uma busca e chamada rápidas.

3.2.7.1 Criando favoritos

Passo 1. Criando favoritos

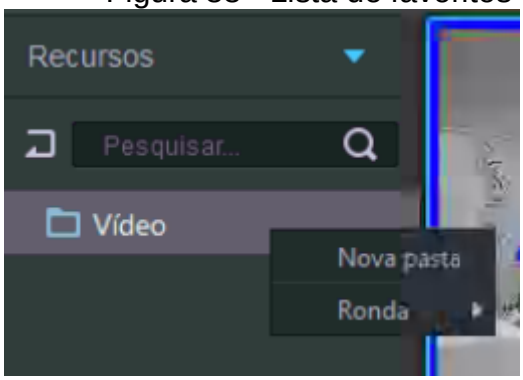
1. Na aba de **Visualização**, clique em .

Figura 87 - Lista de favoritos



2. Clique com o botão direito do mouse no nó raiz ou nos favoritos criados e selecione Nova pasta.

Figura 88 - Lista de favoritos

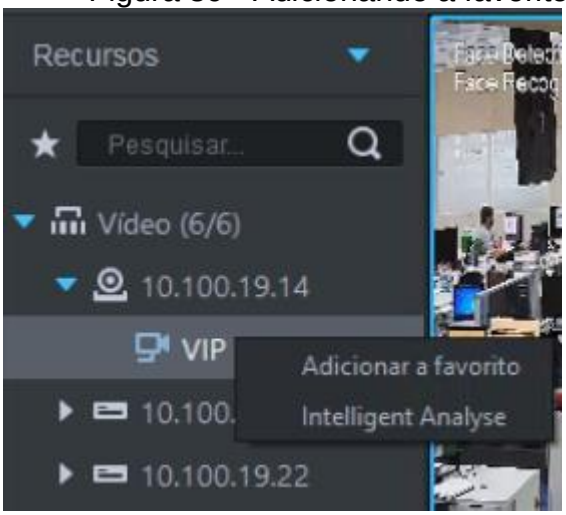


3. Insira o nome da pasta e clique em OK.
   O nó raiz ou os favoritos selecionados geram favoritos de nível inferior.
4. Clique em para voltar a lista de recursos de vídeo.

Passo 2. Canais favoritos.

1. Na lista de dispositivos na interface de Visualização, clique com o botão direito do mouse no canal, selecione Adicionar a favorito e adicione o canal aos favoritos de acordo com sua necessidade, selecione também a pasta que ele deverá ficar.

Figura 89 - Adicionando a favorito



3.2.7.2 Visualizando os Favoritos

- **Visualização**

Na aba de Visualização clique em ★, abra a lista de favoritos, selecione favorito ou canal, clique duas vezes ou arraste para a janela de vídeo e o sistema começa a reproduzir o vídeo ao vivo.

- **Tour**

Na aba de Visualização, clique em ★, abra a lista de favoritos, clique com o botão direito no nó raiz ou favorito, selecione a Tour e período da Tour. O sistema reproduz o nó raiz ou todos os canais favoritos em loop. Para sair da reprodução da Tour, clique em ⎋; para fazer uma pausa, clique ⏸.

3.2.8 Região de Interesse

Uma janela pode ser dividida em 4 ou 6 regiões de interesse durante a exibição ao vivo. Uma área é usada para reproduzir vídeo ao vivo e outras regiões são usadas para ampliar a imagem regional.

Na aba de Visualização, clique com o botão direito na janela, selecione Modo Janela e selecione um modo. Por exemplo, selecione o modo 1 + 3.

Figura 90 - Modo de janela

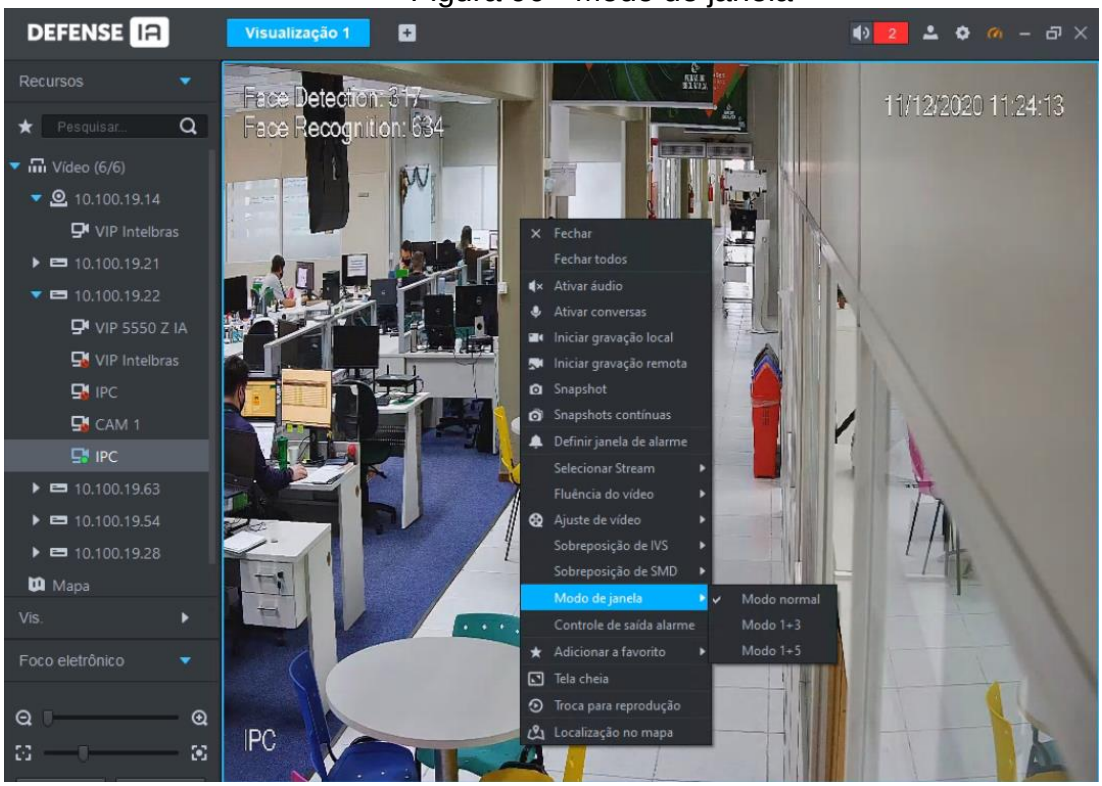
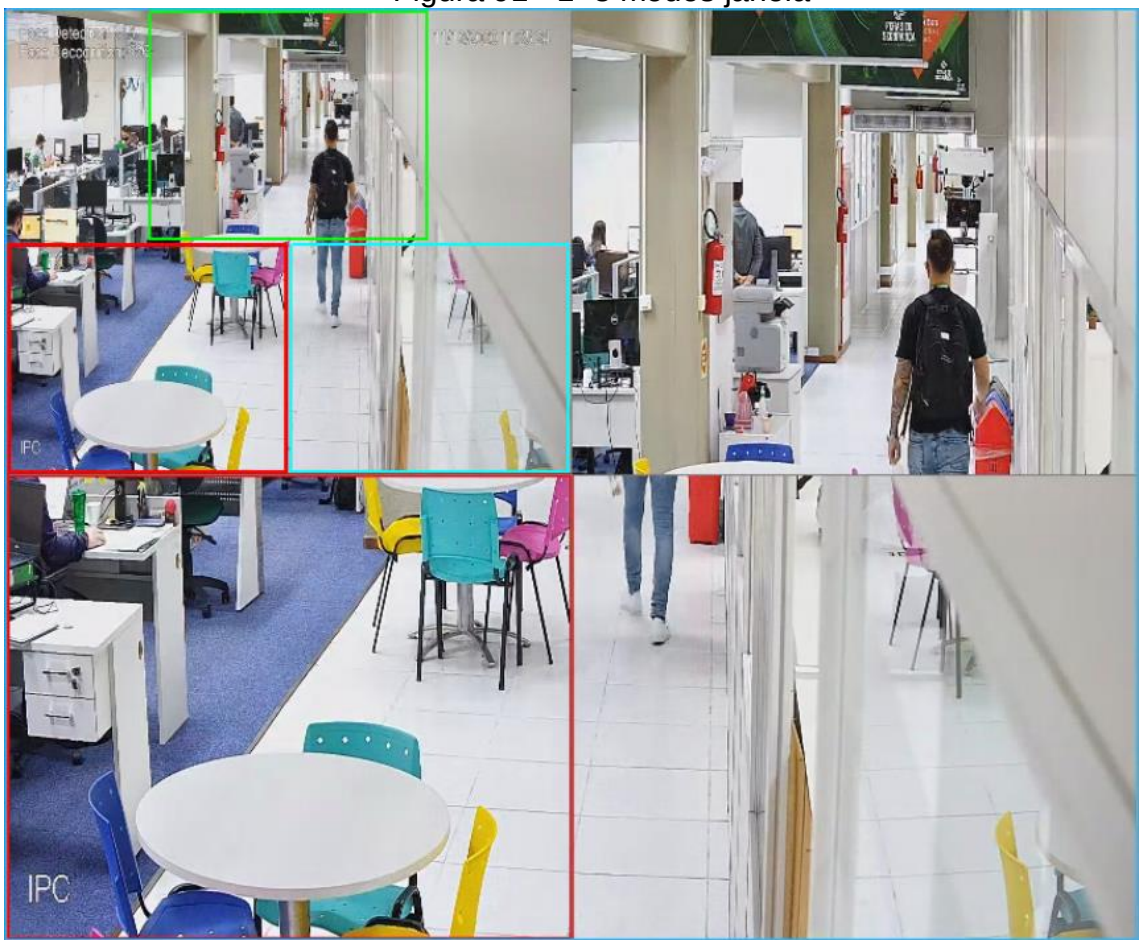


Figura 91 - 1+3 modos janela

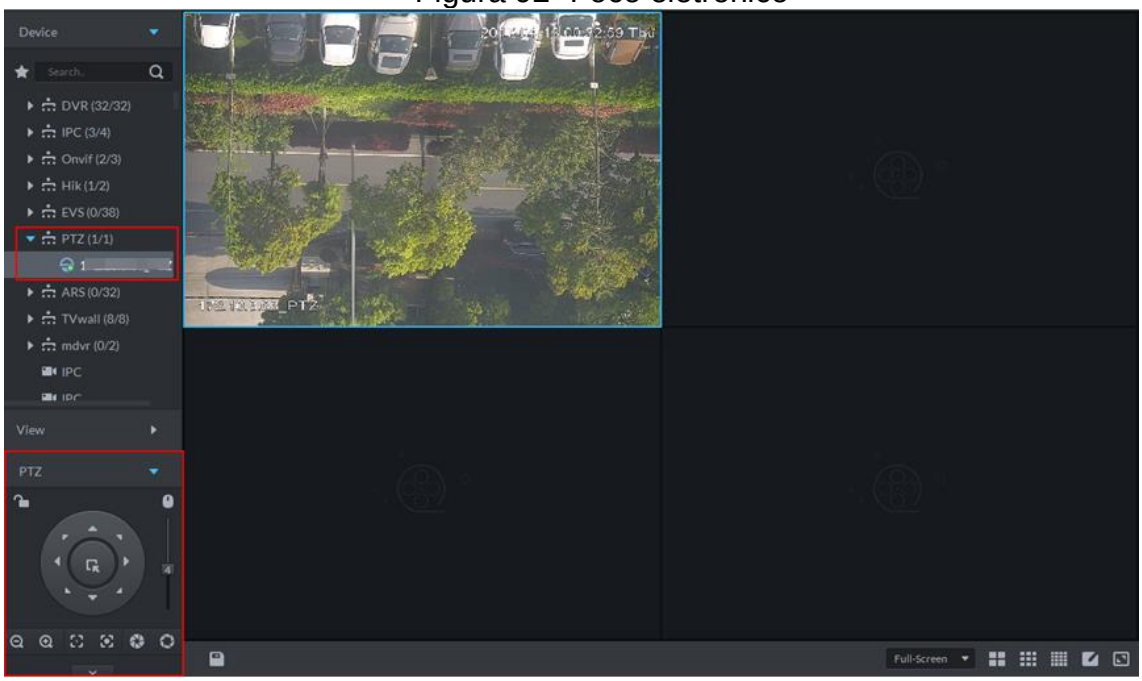


3.2.9 Foco eletrônico

Operar câmeras PTZ durante a exibição ao vivo no Defense Client.

Passo 1. Na aba Visualização, abra o vídeo da câmera PTZ.

Figura 92 -Foco eletrônico



Passo 2. Clique em [ ] para exibir a interface de Foco eletrônico.

Figura 93 - Menu foco eletrônico

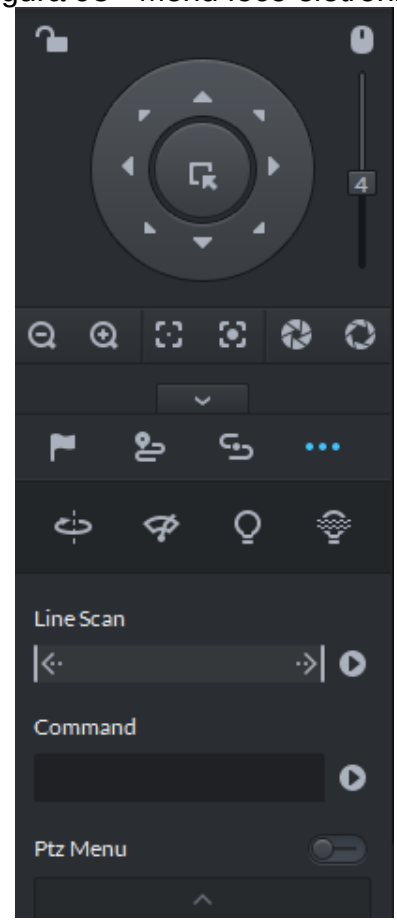
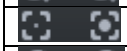


Tabela 12 - Parâmetros foco eletrônico

Parâmetros	Descrição
	Clique para bloquear o PTZ atual. indica que o PTZ está bloqueado. Diferentes usuários têm diferentes prioridades de operação de PTZ. • Quando um usuário de prioridade PTZ mais baixa bloqueia PTZ, o usuário de prioridade PTZ mais alta pode desbloquear e habilitar o PTZ clicando em . • Quando um usuário de prioridade PTZ mais alta bloqueia PTZ, o usuário de prioridade PTZ baixa não pode desbloquear o PTZ, a menos que a câmera PTZ se desbloqueie automaticamente. • Usuários com a mesma prioridade de PTZ podem desbloquear PTZ bloqueados entre si. O tempo padrão para desbloquear PTZ automaticamente é 30 segundos.
	Controla o PTZ pelo Mouse
Botões Direcionais	Define a direção de rotação do PTZ. Oito direções estão disponíveis no total: cima, baixo, esquerda, direita, superior esquerdo, superior direito, inferior esquerdo e inferior direito.
	Posicionamento 3D e zoom parcial. Esta função só pode ser controlada com o mouse.
	Ajuste a velocidade de rotação do PTZ de cima para baixo. Defina o tamanho do passo de 1 a 8.
	Zoom + e Zoom -
	Ajuste de foco
	Ajuste de Íris
	Definir preset, Tour, padrão, scan, rotação, limpador, luz, e iluminação de IR.

3.2.9.1 Configurando o Preset

Um preset é um conjunto de parâmetros que envolve a direção e o foco do PTZ. Ao chamar uma predefinição, você pode girar rapidamente a câmera para a posição predefinida.

Passo 1. Clique na tecla de direção do PTZ para girar a câmera na direção necessária.

Passo 2. Clique .

Passo 3. Aponte para 1 e clique em .

Passo 4. Insira o número do Preset e clique em .

Clique para um Preset específico, e então a câmera PTZ irá até a posição previamente definido.

3.2.9.2 Configurando Tour

Defina a Tour para permitir que a câmera vá para frente e para trás entre diferentes predefinições.

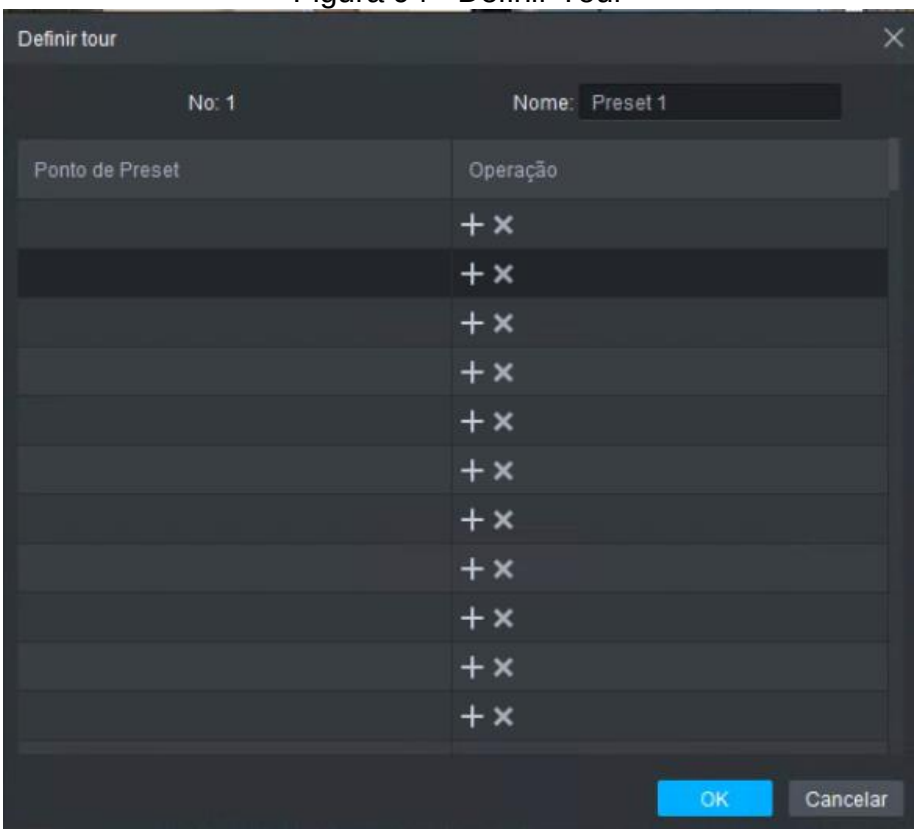
Para habilitar a Tour, pelo menos 2 preset's são necessários.

Defina a Tour para permitir que a câmera volte e avance automaticamente entre os diferentes preset's.

Para habilitar a Tour, certifique-se de ter configurado pelo menos 2 preset's com antecedência.

Passo 1. Clique .
Passo 2. Aponte para 1 e clique .

Figura 94 - Definir Tour



Passo 3. Escreva um nome para o Tour e clique em .
Passo 4. Selecione um preset na lista suspensa à esquerda.
Passo 5. Clique OK.
Passo 6. Para iniciar o Tour, aponte para 1 e clique , em seguida, a câmera vai e volta entre os presets do Tour 1.

3.2.9.3 Configurando Padrão

Um padrão é um registro de uma série consecutiva de operações PTZ. Você pode selecionar um padrão para repetir as operações correspondentes rapidamente. Consulte as instruções de configuração do padrão a seguir.

Passo 1. Clique .

Passo 2. Clique em e, em seguida, opere os 8 botões PTZ de PTZ para definir o padrão dos movimentos em que a PTZ deverá executar.

Passo 3. Clique para completar o padrão.

Passo 4. Clique em , e então a câmera fará automaticamente o padrão que você ajustou.

3.2.9.4 Configurando Escanear

A câmera faz a varredura horizontalmente automaticamente em uma determinada velocidade.

Passo 1. Clique em .

Passo 2. Clique no botão PTZ e gire o PTZ para a esquerda para uma posição e, a seguir, clique para definir o limite esquerdo.

Passo 3. Continue a girar PTZ para a direita para uma posição e clique para definir o limite direito.

Passo 4. Clique para iniciar a varredura, então o PTZ girará para um lado e para outro automaticamente dentro dos dois limites..

3.2.9.5 Habilitando/Desabilitando Pan

Clique , e então clique . PTZ gira 360° em uma velocidade especificada. Clique para parar a rotação da câmera.

3.2.9.6 Habilitando/Desabilitando limpador

Habilitar/desabilitar o limpador da câmera PTZ. Certifique-se de que a câmera suporta a função de limpador.

Clique , e então clique para ativar o limpador. Clique em para desativar.

3.2.9.7 Habilitando/Desabilitando luz

Ligue/desligue a luz da câmera. Certifique-se de que a câmera suporta luz.

Clique , e então clique para ativar a luz. Para desativar clique em .

3.2.9.8 Habilitando/Desabilitando a luz do IR

Clique , e então clique para ativar a luz IR. Para desativar, clique em.

3.2.9.9 Menu PTZ

Passo 1. Clique .

Figura 95 - Direcionais foco eletrônico

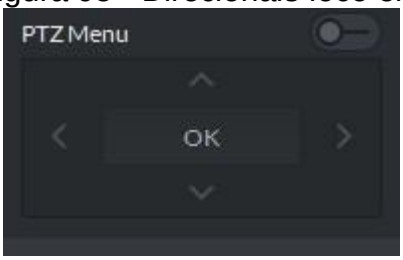


Tabela 13 - Parâmetros botões

Parâmetros	Descrição
/	Botão de navegação cima/baixo
/	Esquerda/direita. Mova o ponteiro do mouse para definir os parâmetros.
	Clique para habilitar a função do menu PTZ. O sistema exibe o menu principal na janela do monitor.
	Clique para fechar a função do menu PTZ.
OK	Botão de confirmação. Possui as seguintes funções. Se o menu principal possuir o submenu, clique em OK para entrar no submenu. Mova o ponteiro do mouse para Voltar e clique em OK para voltar ao menu anterior. Mova o ponteiro do mouse para Sair e clique em OK para sair do menu.

Figura 96 - Menu foco eletrônico

Tabela 14 - Parâmetros tour

Parâmetros	Descrição
Camera	Mova o ponteiro do mouse para Câmera e clique em OK para entrar na interface do submenu de configurações da câmera. Defina os parâmetros da câmera. Inclui imagem, exposição, luz de fundo, modo dia / noite, foco e zoom, desembaçamento e padrão.
PTZ	Mova o ponteiro do mouse para PTZ e clique em OK para entrar na interface do submenu PTZ. Defina as funções PTZ. Inclui predefinição, tour, varredura, padrão, rotação, reinicialização de PTZ, etc.
System	Mova o ponteiro do mouse para Sistema e clique em OK para entrar na interface do submenu do sistema. Defina o simulador de PTZ, restaure as configurações padrão da câmera, a versão do software da câmera de vídeo e a versão do PTZ.
Return	Mova o ponteiro do mouse para Retornar, clique em OK e volte ao menu anterior.

Parâmetros	Descrição
Exit	Mova o ponteiro do mouse para Sair e clique em OK e saia do menu PTZ.

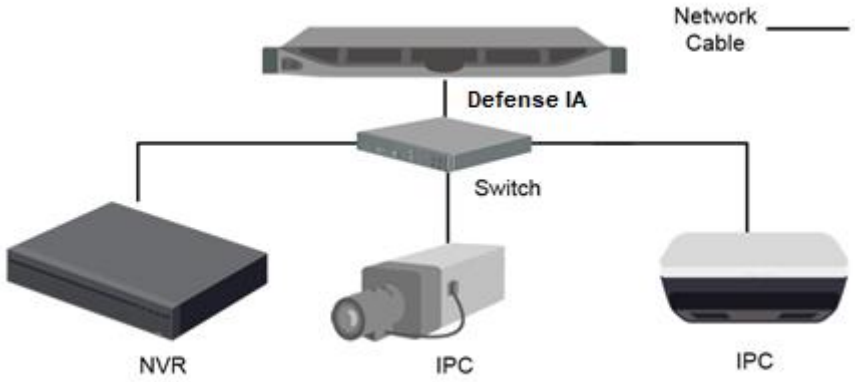
3.3 ANÁLISE INTELIGENTE

IVS inclui análise de tripwire, detecção de intrusão, objeto abandonado, detecção de vadiagem, movimento rápido, aglomeração de multidão, objeto perdido e detecção de estacionamento. A capacidade real da câmera deve prevalecer. Com o IVS configurado, quando um alvo é detectado, o sistema acionará um evento conforme você definiu e o exibirá na plataforma.

3.3.1 Topologia Típica

Análise inteligente executado por NVR, IVSS e IVS. Veja o NVR, por exemplo.

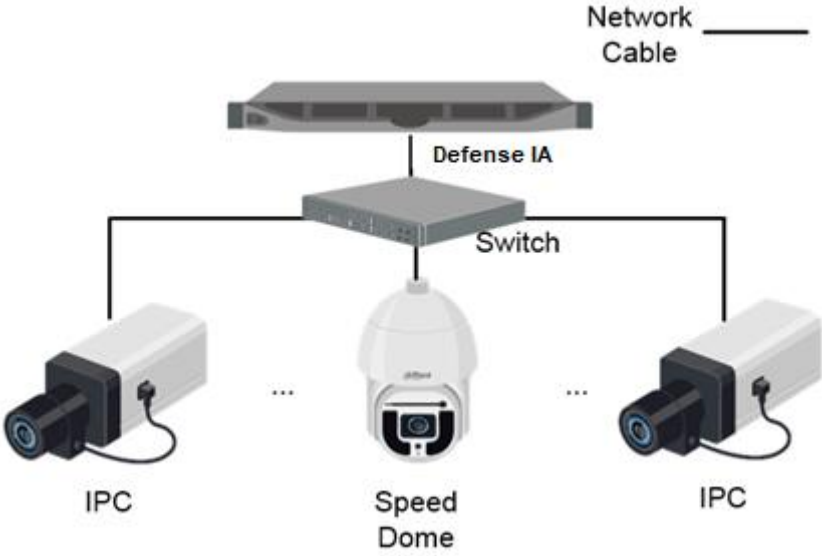
Figura 97 - Topologia de análise inteligente



- As câmeras coletam o fluxo de vídeo.
- Os dispositivos NVR, IVSS e IVS realizam análises inteligentes
- O Defense IA é usado para gerenciar todas as câmeras e dispositivos IVS e receber alarmes IVS.

Análise inteligente realizada pela câmera

Figura 98 - Topologia de análise inteligente (1)



- As câmeras coletam o fluxo de vídeo.
- O Defense IA é usado para gerenciar todas as câmeras e dispositivos IVS e receber alarmes IVS.

3.3.2 Configurando Análise Inteligente

- Você só pode definir as configurações do IVS para câmeras adicionadas diretamente à plataforma.

Veja os requisitos a seguir quando implantando dispositivos:

- A proporção total de destino não excede 10% da tela.
- O tamanho do alvo na imagem não é inferior a 10 pixels × 10 pixels, o tamanho do alvo do objeto abandonado não é inferior a 15 pixels × 15 pixels (imagem CIF); a altura e largura do alvo não são mais do que 1/3 da altura da imagem e a altura do alvo recomendada é 10% da altura da imagem.
- A diferença entre o valor de brilho do alvo e do fundo não é inferior a 10 níveis de cinza.
- Certifique-se, pelo menos, de que o alvo apareça continuamente por mais de 2 segundos no campo de visão, a distância de movimento exceda a largura do próprio alvo e não seja inferior a 15 pixels (imagem CIF).
- Minimize a complexidade do cenário de monitoramento e análise quando as condições permitirem. Não é recomendado usar a função de análise inteligente em cenários com alvos densos e mudanças frequentes de luz.
- Evitar reflexão do solo, de vidros/espelhos e superfície da água; evitar sombras e interferência de insetos; evite cenas com luz de fundo e luz direta.

3.3.2.1 Habilitando IVS Smart Plan

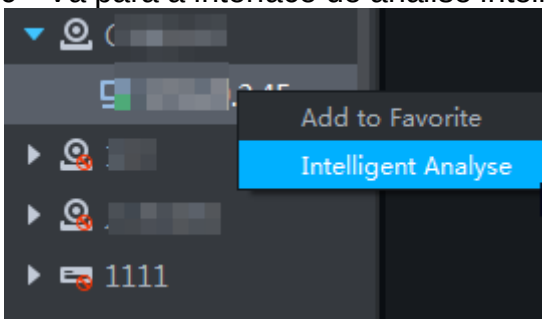
Habilite as funções IVS.

Passo 1. Vá para a interface de configuração IVS.

I. Faça login no Cliente do Defense IA, selecione **Visualização**.

II. Clique com o botão direito em um canal IPC na interface de **Visualização** e selecione **Intelligent Analyze.**

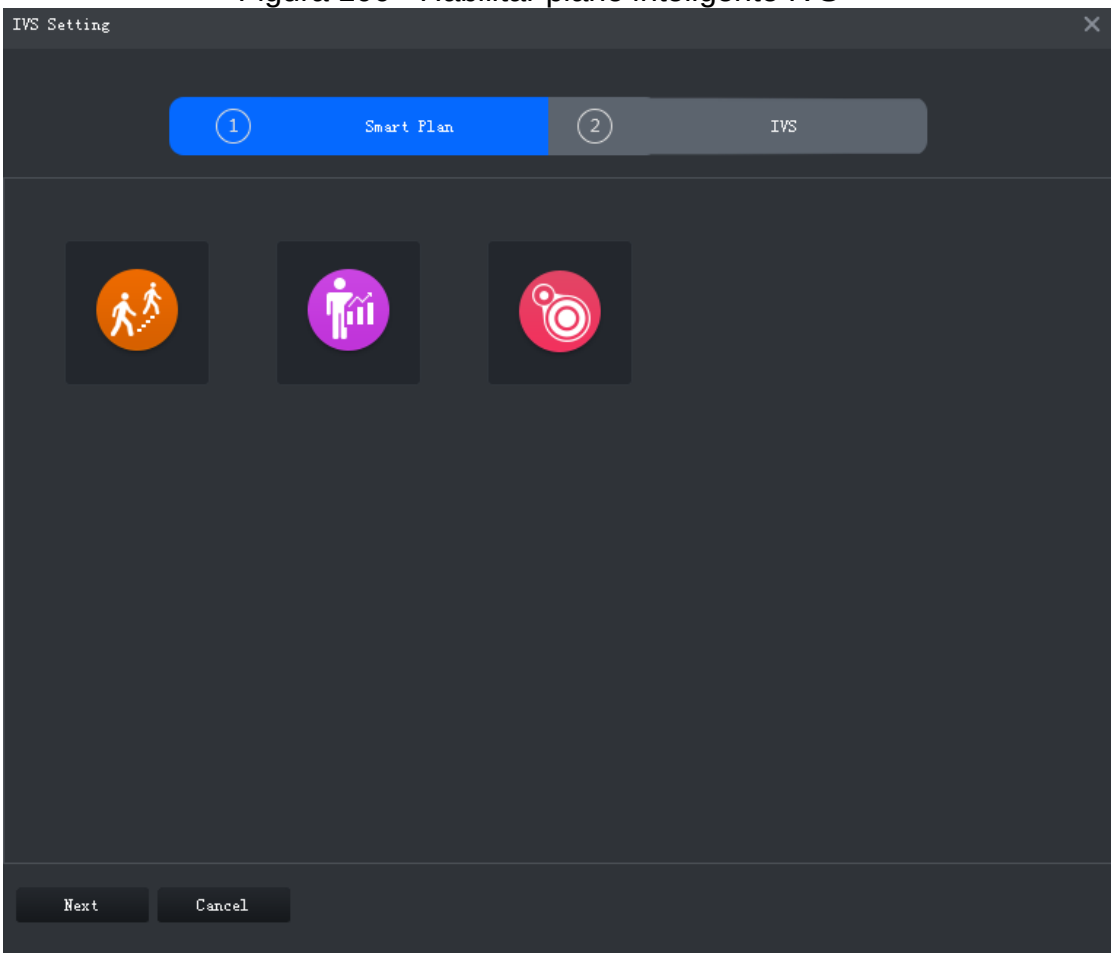
Figura 99 - Vá para a interface de análise inteligente



Passo 2. Ative o plano inteligente IVS.

III. Clique  na interface do plano inteligente para habilitar o plano inteligente IVS. Quando o ícone é exibido no quadro branco, significa que o plano inteligente está selecionado. Se outro plano inteligente foi selecionado, clique no ícone do plano inteligente para desmarcá-lo e clique em  para selecionar IVS.

Figura 100 - Habilitar plano inteligente IVS



Passo 3. Clique em Avançar para ir para a interface de configuração IVS.

3.3.2.2 Calibrando a profundidade de campo

Depois de definir um medidor horizontal e três medidores verticais e as distâncias geográficas reais de cada medidor, o sistema pode estimar os parâmetros internos (características geométricas internas e propriedades ópticas) e parâmetros externos (a posição da câmera de rede e direção no ambiente real) da rede câmera, de modo a trabalhar a relação entre a imagem bidimensional e os objetos tridimensionais no ambiente de vigilância atual.

- Calibre a profundidade de campo para detecção de movimento rápido. Pule esta seção se você não precisar desta função.

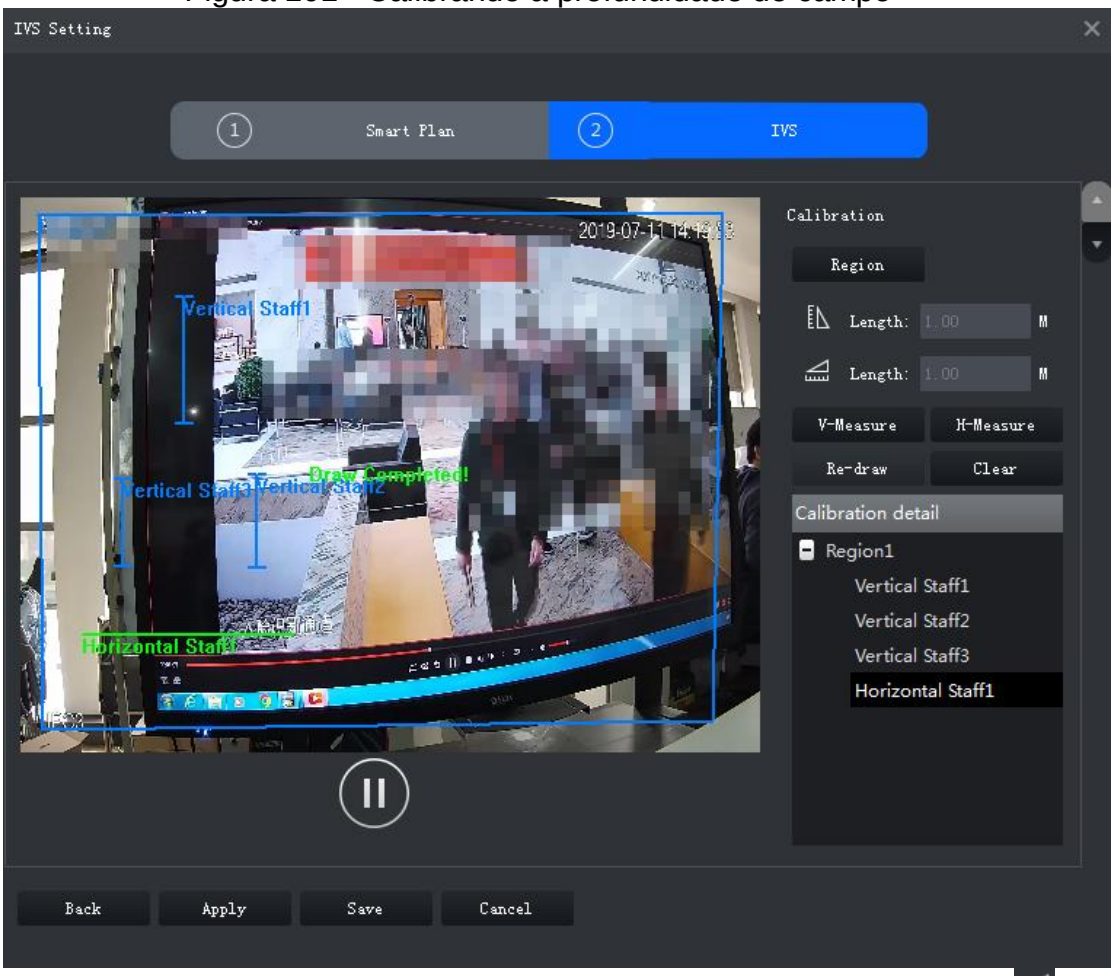
Passo 1. Depois de selecionar o plano inteligente na interface do **Plano inteligente**, clique em **Avançar.**

Passo 2. Clique em **Região** e desenhe a zona de calibração no vídeo. Clique com o botão direito para terminar.

Passo 3. Defina o valor do comprimento do medidor vertical. Clique e desenhe um medidor vertical na área de calibração. Clique para terminar.

Desenhe outros três medidores verticais na área de calibração.

Figura 101 - Calibrando a profundidade de campo



Passo 4. Defina o valor do comprimento do medidor horizontal. Clique e, em seguida, desenhe um medidor horizontal na área de calibração. Clique para terminar.

- Para modificar o medidor, você pode selecioná-lo e clicar em **Redesenhar**. Você também pode selecionar a calibração e clicar em **Redesenhar** para desenhar novas áreas de calibração e medidores.
- Para excluir um medidor, selecione-o e clique em **Excluir**. Para excluir uma área de calibração e os medidores nela, selecione a área e clique em **Excluir**.

Passo 5. Clique em **Aplicar** para salvar.

Passo 6. (Opcional) Medição vertical / horizontal

Siga os seguintes passos para medir a distância.

- Clique em **V-Measure** e desenhe uma linha vertical na área de calibração. O resultado da medição será exibido.
- Clique em **H-Measure** e desenhe uma linha horizontal na área de calibração. O resultado da medição será exibido.

3.3.2.3 Configurando a região de detecção

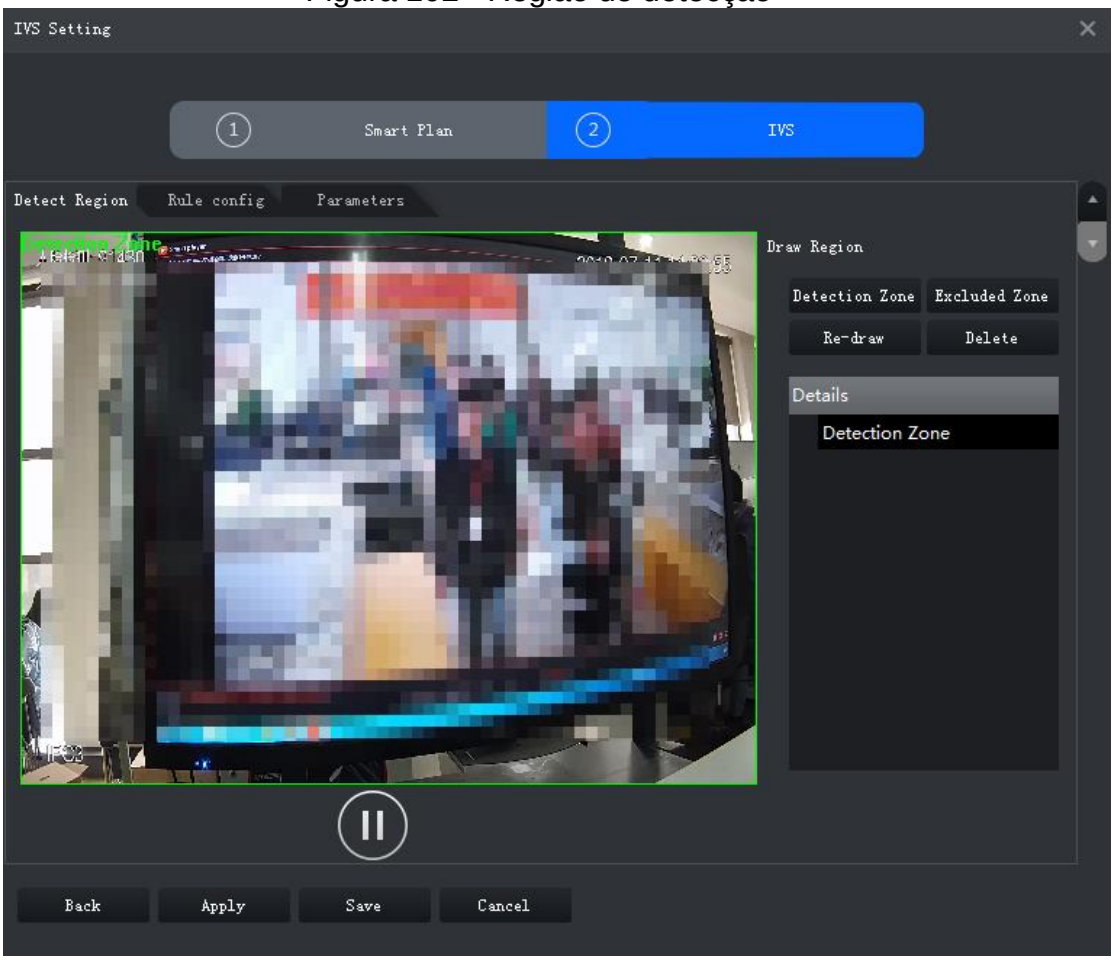
Configure a zona de detecção de IVS.

Passo 1. Clique .

Passo 2. Clique em **Zona de Detecção**, desenhe o quadro da zona de detecção no vídeo e clique com o botão direito para finalizar.

Passo 3. Clique em **Zona excluída**, desenhe o quadro da zona no vídeo e clique com o botão direito para finalizar.

Figura 102 - Região de detecção



3.3.2.4 Configurando a regra IVS

Configurar Detecções IVS, como cruzamento de cerca, cruzamento de linha, intrusão, objeto abandonado, detecção de vadiagem, movimento rápido, reunião de multidão, objeto perdido e detecção de estacionamento.

Funções	Descrição	Cenários Aplicáveis
Cruzamento de cerca	O alarme é acionado quando um alvo está cruzando a cerca pré-definida.	Estradas, aeroportos e outras áreas com zonas restritas.

Funções	Descrição	Cenários Aplicáveis
Cruzamento de linha	O alarme é disparado quando um alvo está cruzando o fio de disparo predefinido.	Limites da zona restrita
Intrusão	O alarme é acionado quando um alvo está entrando, saindo ou aparece na área de detecção.	Limites da zona restrita
Objeto Abandonado	O alarme é disparado quando um objeto é deixado na área de detecção e o tempo de existência é maior que o limite.	Lugares onde o não se tem mudanças de luz óbvias e frequentes. A área de detecção deve ser o mais simples possível.
Objeto ausente	O alarme é acionado quando um objeto é removido da área de detecção e não é colocado de volta após o período de tempo predefinido.	

Funções	Descrição	Cenários Aplicáveis
Movimento Rápido	O alarme é acionado quando a velocidade de movimento de um alvo excede o limite.	Lugares com baixa densidade alvo e nenhum bloqueio óbvio. A câmera deve ser instalada logo acima da área de monitoramento, e a direção da luz é o mais vertical possível com a direção do movimento.
Detecção de estacionamento	O alarme é acionado quando um alvo permanece parado dentro de um período de tempo maior do que a duração de tempo predefinida.	Monitoramento de estradas e gerenciamento de tráfego.
Aglomeração	O alarme é acionado quando a reunião de pessoas é detectada ou a densidade de pessoas é maior do que o limite.	Monitoramento de longa ou de média distância entre pessoas. Por exemplo, praças externas, portões do governo e entradas e saídas de estações.

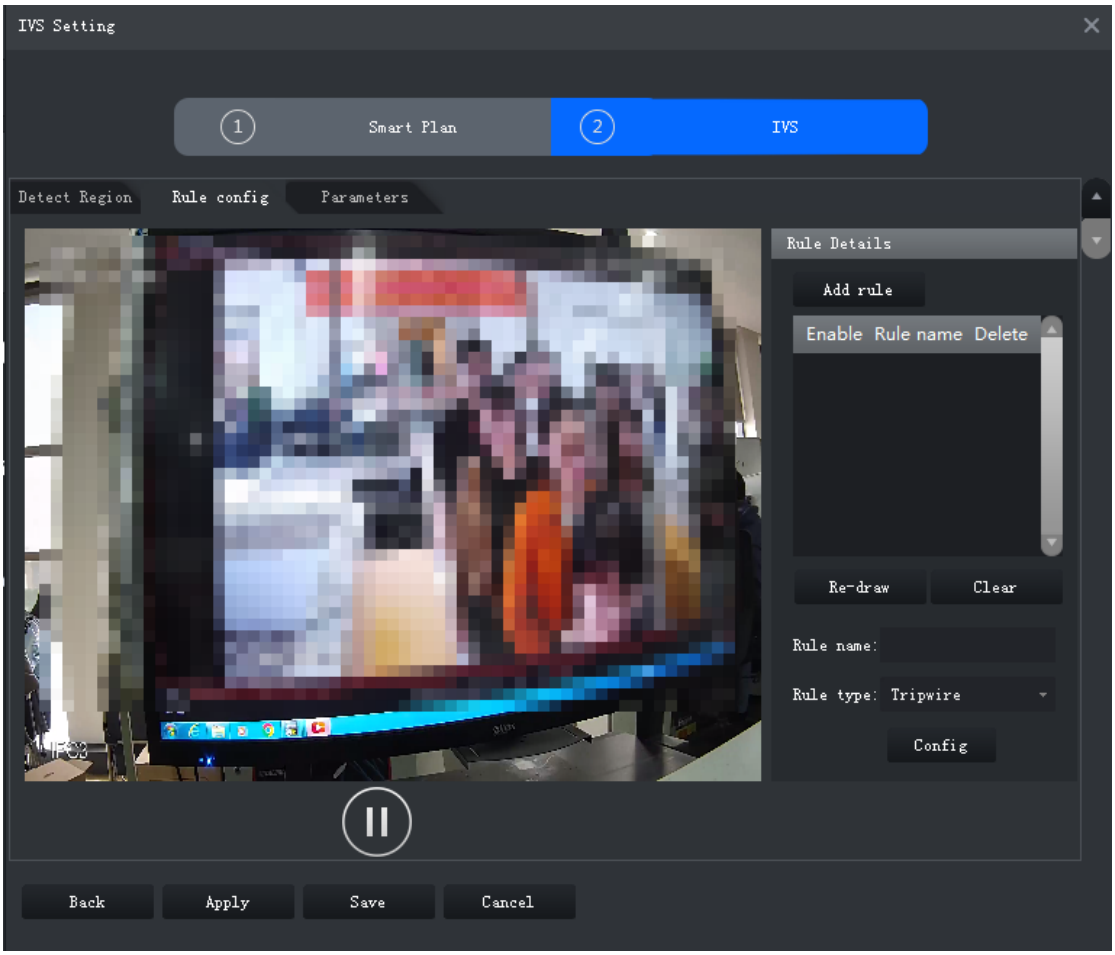
Funções	Descrição	Cenários Aplicáveis
Atitude Suspeita	O alarme é disparado quando um alvo fica perambulando por um período de tempo maior que o limite. O alarme será acionado novamente se o alvo permanecer na área de detecção após o primeiro alarme.	Empreendimento zonas, salões e muito mais.

3.3.2.4.1 Tripwire

Quando um alvo é detectado cruzando uma linha, um alarme será acionado imediatamente.

Passo 1. Na interface Configuração de IVS, clique em Configuração de regras.

Figura 103 - Interface de configuração de regra



Passo 2. Clique em Adicionar regra.

Passo 3. Habilite a regra e modifique o nome e o tipo.

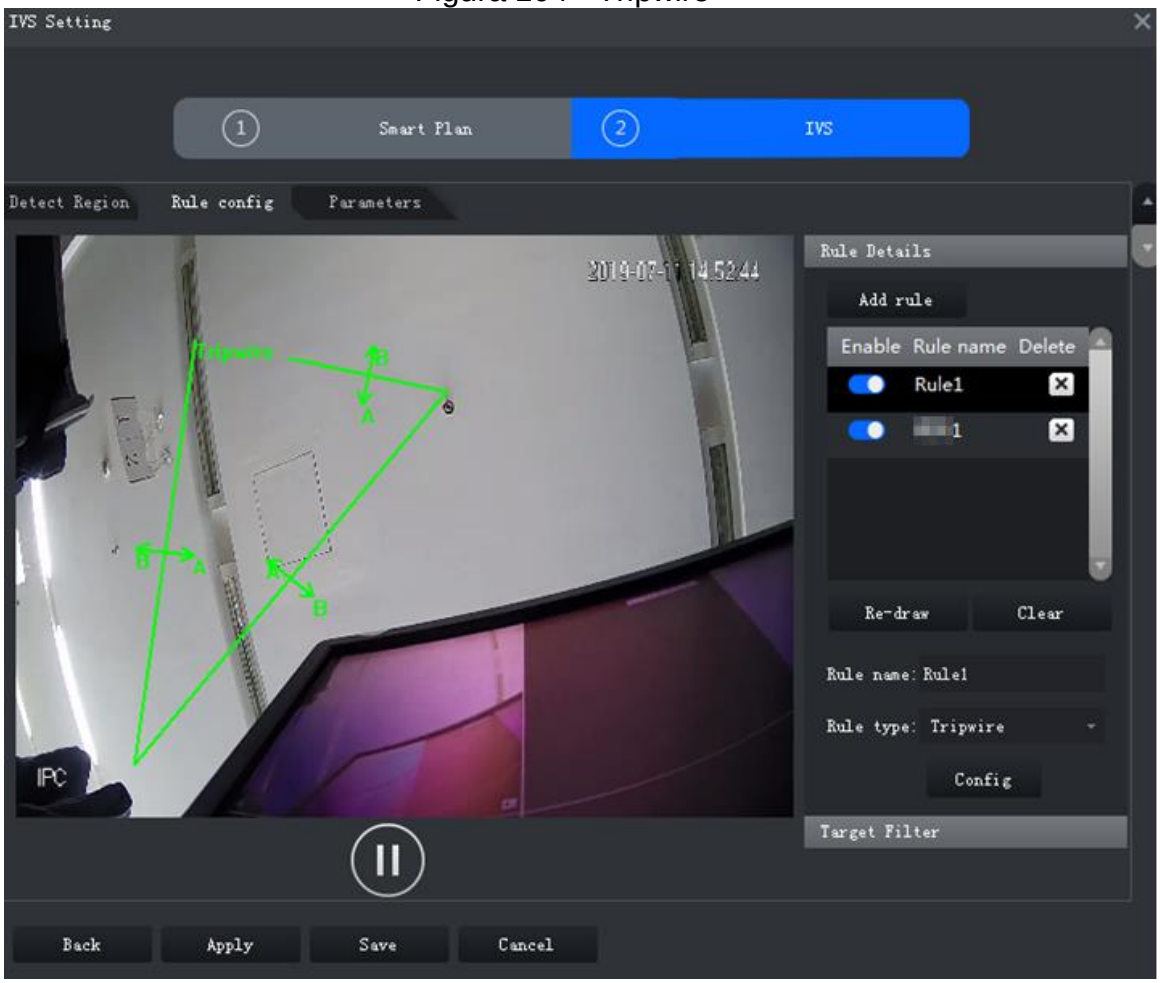
I. Ativar regra.  indica que a regra está habilitada.

II. Modifique o nome da regra.

III. Selecione **Linha Virtual** na lista suspensa do **Tipo de regra**.

Passo 1. Desenhe uma linha no vídeo e clique com o botão direito para finalizar.

Figura 104 - Tripwire



Passo 2. Defina parâmetros, programação de arme e ligação de alarme.

I. Clique em Configuração e defina os parâmetros.

Figura 105 - Definir parâmetros

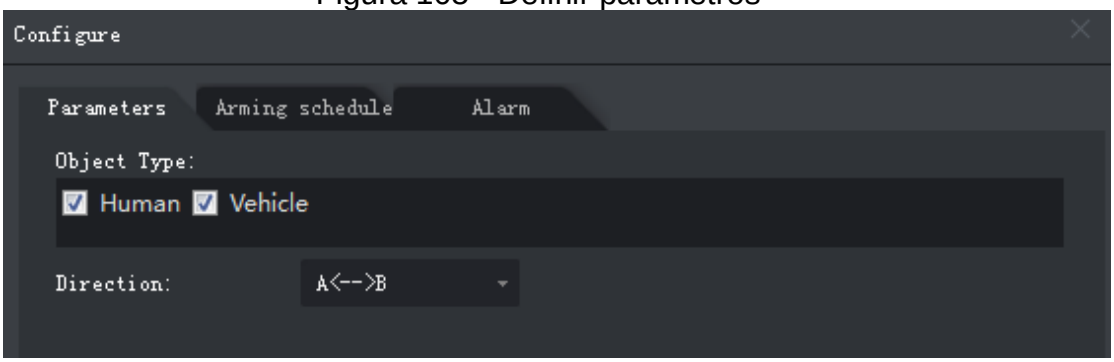


Tabela 15 - Parâmetros

Parâmetro	Descrição
Tipo de objeto	Somente humanos ou veículos podem disparar o alarme.
Direção	Quando o alvo está se movendo na direção da regra, é uma intrusão. As direções incluem A → B, B → A e A↔B.

I. Clique em **Programação de arme**, selecione o dia e as horas e defina a hora de início e de término.

- A programação de arme padrão é 24 horas por dia.

Figura 106 - Cronograma de arme

II. Clique em **Alarme** e defina as ações de ligação.

Figura 107 - Ligação de alarme

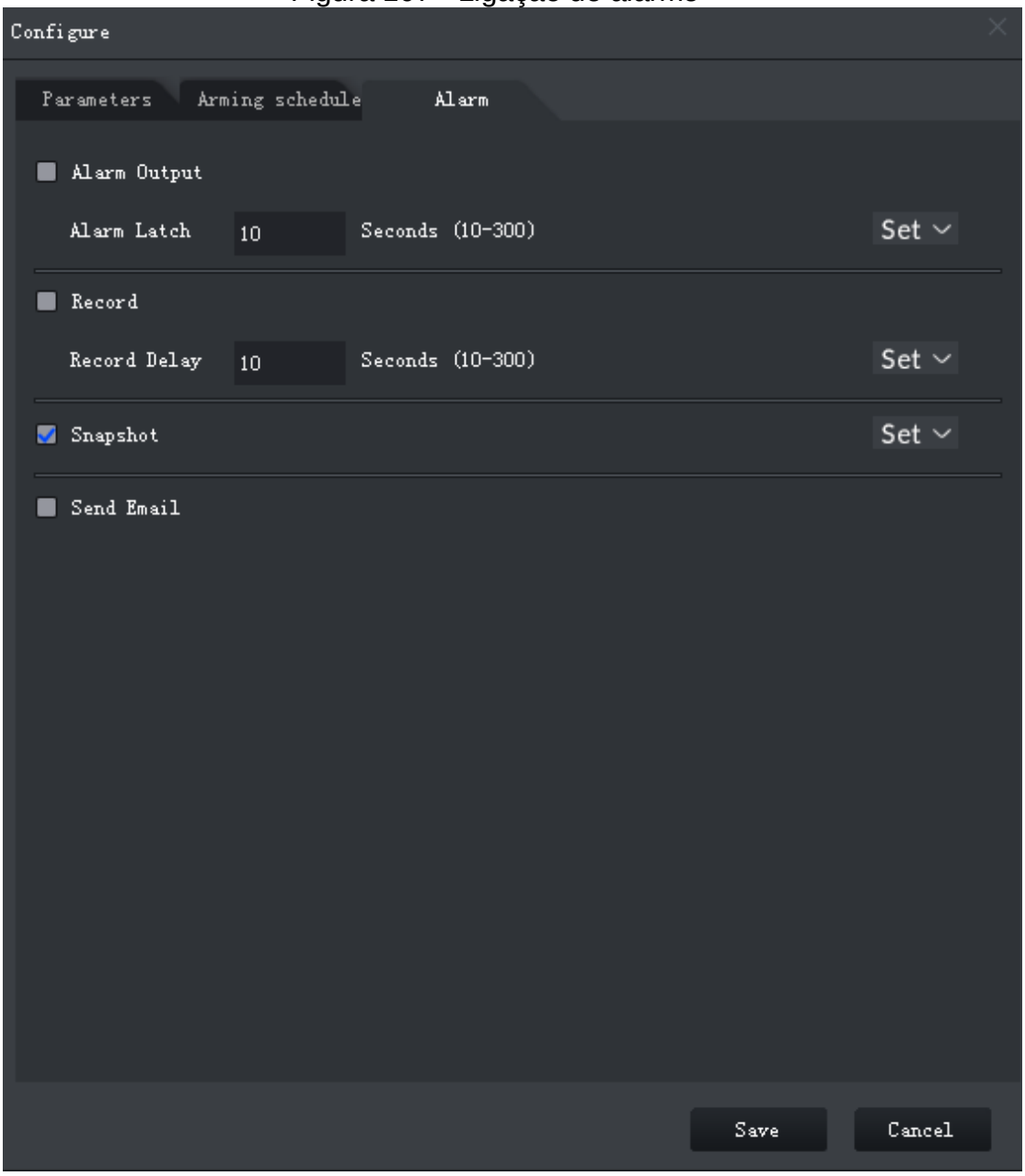


Table 1-1 Parâmetros

Parâmetro	Descrição	
Saída de Alarme	Conecte os dispositivos de saída de alarme às interfaces de saída de alarme. Quando um alarme é disparado, o sistema enviará o alarme para o dispositivo de saída de alarme.	Clique em **Definir** próximo a **Atraso de alarme** e selecione um canal de saída de alarme.
Atraso de Alarme	A ação de saída de alarme atrasará a parada após o término do evento de alarme.	

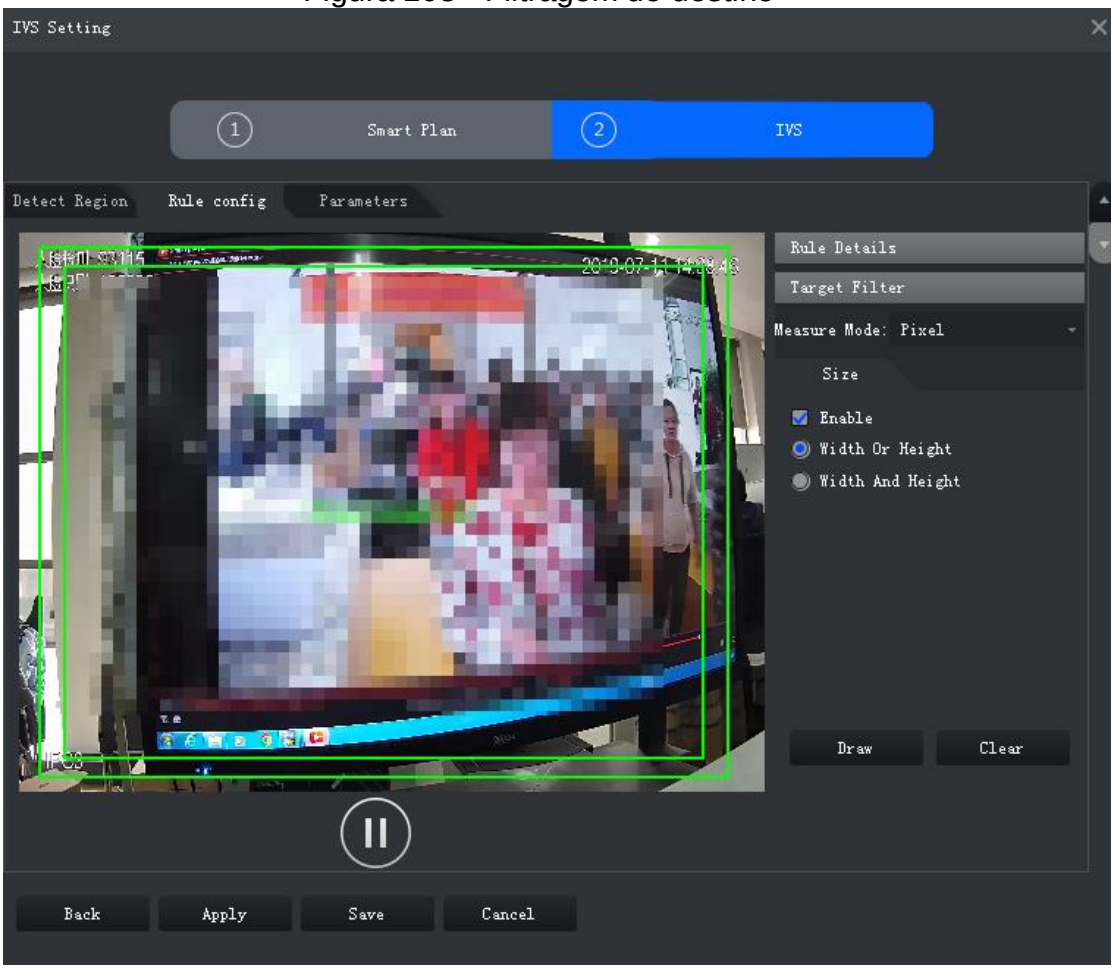
Parâmetro	Descrição	
Registro	Quando um alarme acontece, ele aciona a gravação de vídeo imediatamente. Requer que o dispositivo já tenha programações de gravação. Consulte o manual do dispositivo para obter instruções detalhadas.	Clique em **Definir** próximo a **Gravação** e selecione um canal de saída de alarme.
Atraso de registro	A gravação de vídeo atrasa, parando um pouco após o término do evento de alarme.	
instantâneo	O sistema irá tirar snapshots automaticamente quando um alarme acontecer. Requer que o dispositivo já tenha programações de instantâneos. Consulte o manual do dispositivo para obter instruções detalhadas.	Clique em **Definir** próximo a **Snapshot** para selecionar o canal de instantâneo.
Enviar email	O sistema enviará um e-mail para o endereço de e-mail relacionado quando ocorrer um alarme. Requer que o dispositivo já tenha o e-mail configurado. Consulte o manual do dispositivo para obter instruções detalhadas.	

III. Clique em **Salvar**.

Passo 3. Desenhe o quadro de filtragem de destino.

O quadro de filtragem é usado para filtrar alvos que são muito grandes ou muito pequenos. Quando o tamanho do alvo está dentro do valor predefinido, ele pode disparar o alarme.

Figura 108 - Filtragem de destino



IV. Clique em Filtro de destino.

V. Selecione **Ativar**.

VI. Selecione um método de filtragem, **Largura; Altura; Largura** e **Altura**. Selecione a moldura de filtragem e arraste os cantos da moldura para ajustar o tamanho.

7)

- Selecione o quadro de filtragem e clique em **Limpar** para excluí-lo.

Passo 4. Clique em **Aplicar**.

3.3.2.4.2 Intrusão

Quando um alvo é detectado entrando ou saindo de uma área, um alarme será disparado.

Passo 1. Na interface Configuração de IVS, clique em Configuração de Regra.
Passo 2. Clique em Adicionar regra.
Passo 3. Habilite a regra e modifique o nome e o tipo.

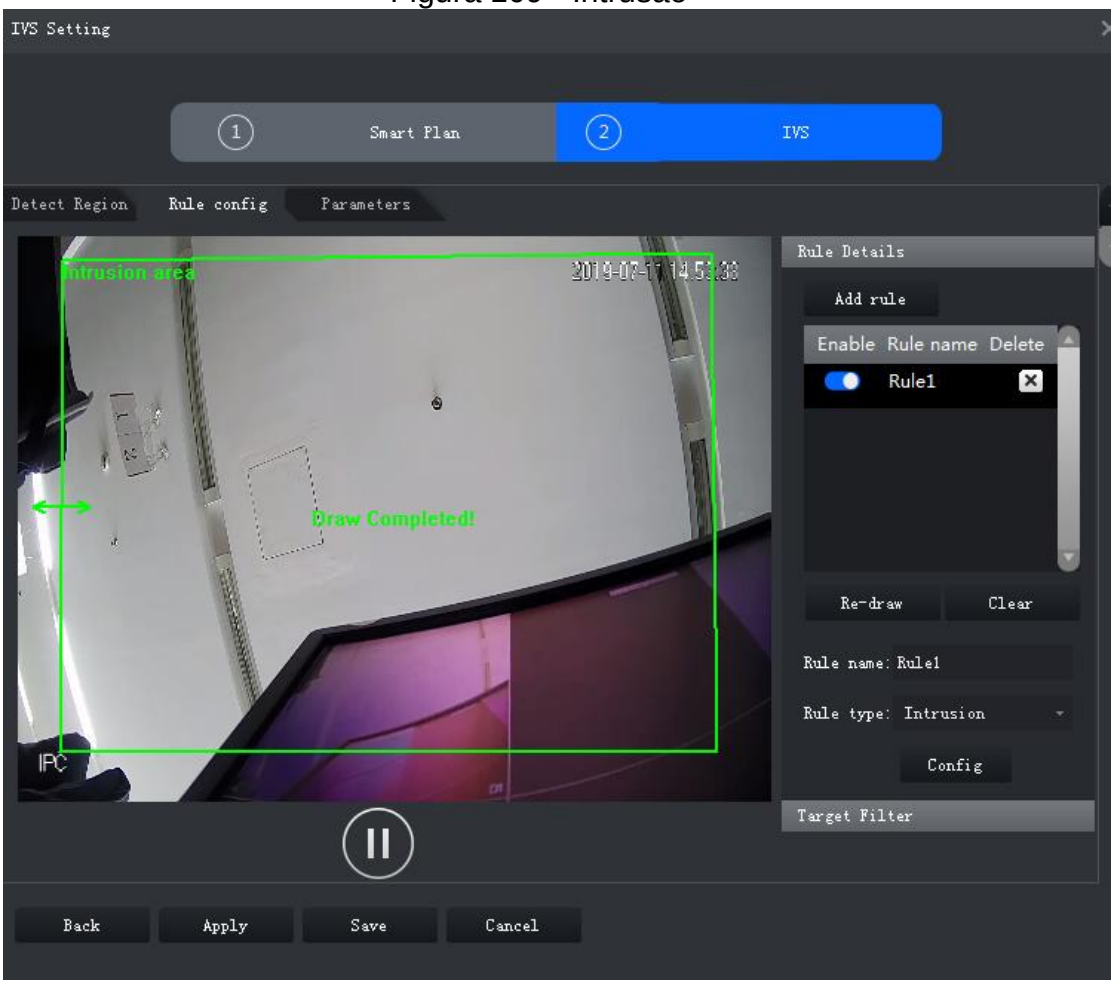
I. Ativar regra. indica que a regra está habilitada.

II. Modifique o nome da regra.

III. Selecione **Intrusão** na lista suspensa de **Tipo de regra.**

Passo 4. Desenhe uma zona de detecção no vídeo e clique com o botão direito para finalizar.

Figura 109 - Intrusão



Passo 5. Defina parâmetros, programação de arme e ligação de alarme. Desenhe um quadro de filtragem de destino. Vejo "3.3.2.4.1 Tripwire. "

Figura 110 - Definir parâmetros

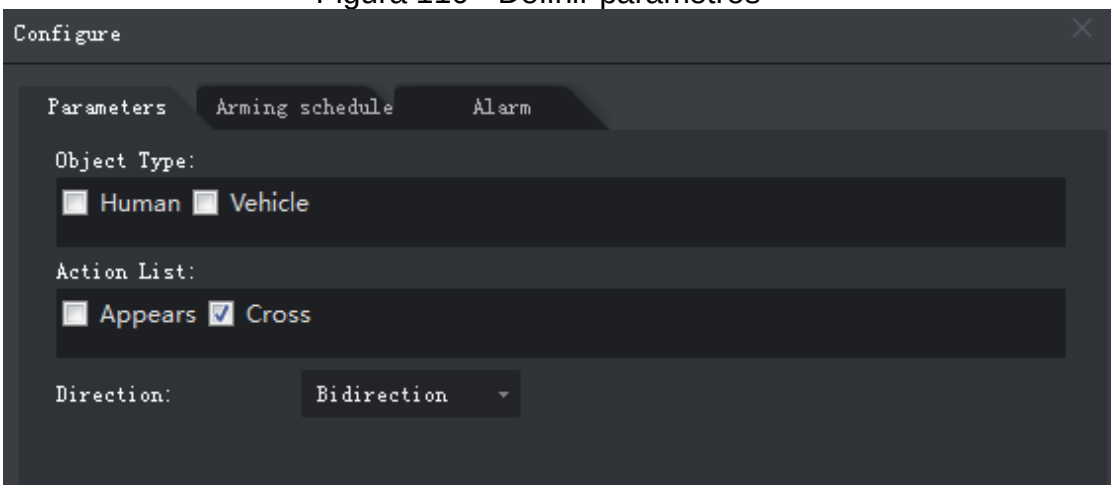


Tabela 16 - Parâmetros

Parâmetro	Descrição
Tipo de Objeto	Somente humanos ou veículos podem disparar o alarme.
Lista de Ação	Aparecer e cruzar
Direção	Quando uma ação de zona cruzada é selecionada, a configuração de **Direção** será utilizada. A direção inclui entrada, saída e mão dupla.

Passo 6. Clique em Aplicar.

3.3.2.4.3 Objeto Abandonado

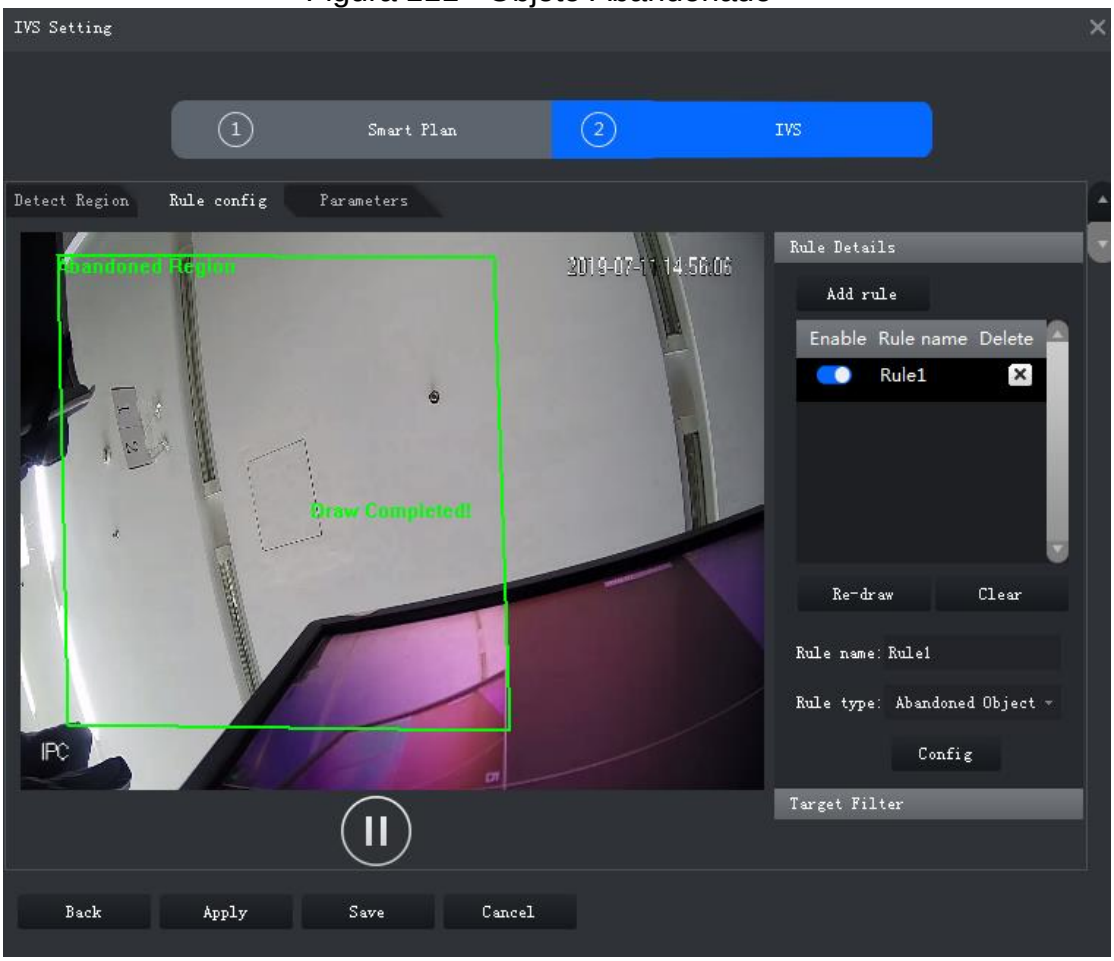
Quando um objeto aparece e permanece na área de detecção por um período de tempo, o sistema dispara um alarme.

Passo 1. Na interface Configuração de IVS, clique em Configuração de Regras.
Passo 2. Clique em Adicionar regra.
Passo 3. Habilite a regra e modifique o nome e o tipo.

I. Ativar regra.  indica que a regra está habilitada.
II. Modifique o nome da regra.
III. Selecione **Objeto abandonado** na lista suspensa de **Tipo de regra.**

Passo 4. Desenhe uma zona de detecção no vídeo e clique com o botão direito para finalizar.

Figura 111 - Objeto Abandonado



Passo 5. Defina parâmetros, programação de arme e ligação de alarme. Desenhe um quadro de filtragem de destino. Vejo "3.3.2.4.1 Tripwire. "

Figura 112 - Definir parâmetros

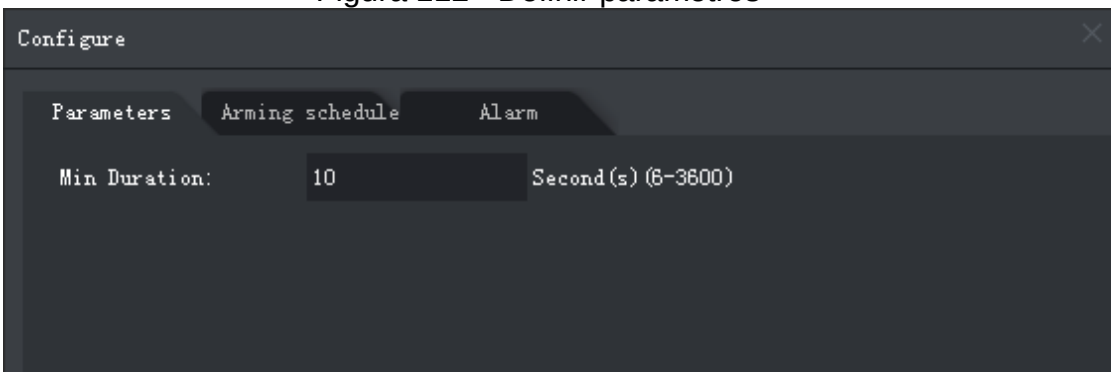


Tabela 17 - Parâmetros

Parâmetro	Descrição
Duração mínima	O período mínimo de tempo entre o aparecimento e o disparo do alarme.

Passo 1. Clique em **Aplicar.**

3.3.2.4.4 Movendo rápido

Quando um alvo aparece e sua velocidade de movimento é/excede o valor predefinido para o período de tempo predefinido, o sistema irá disparar um alarme.

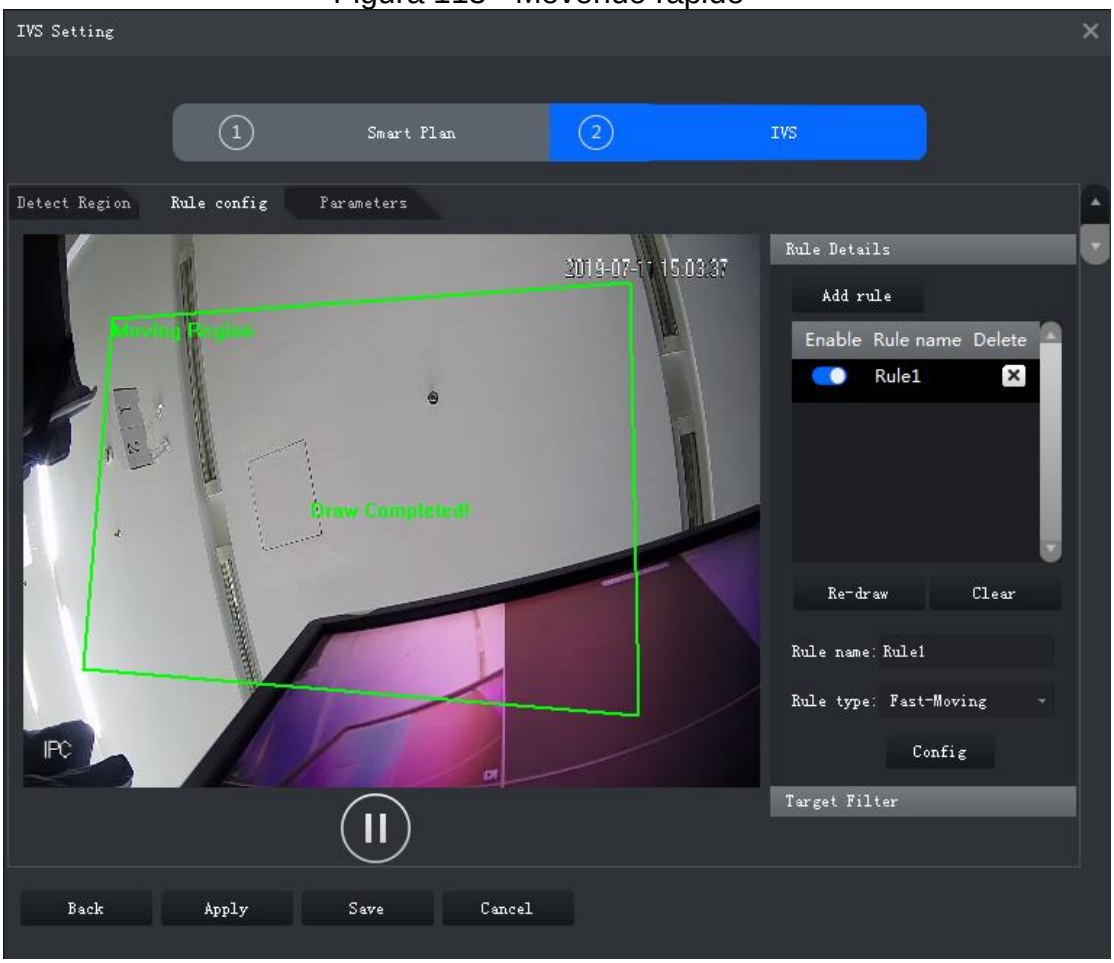
- Para garantir a precisão da detecção de movimento rápido, certifique-se de ter concluído a configuração da calibração. Vejo "3.3.2.2 Calibrando a profundidade de campo para detalhes."

Passo 1. Na interface Configuração de IVS, clique em Configuração de Regras.
Passo 2. Clique em Adicionar regra.
Passo 3. Habilite a regra e modifique o nome e o tipo.

I. Ativar regra. indica que a regra está habilitada.
II. Modifique o nome da regra.
III. Selecione Movimento rápido na lista suspensa de Tipo de regra.

Passo 4. Desenhe uma zona de detecção no vídeo e clique com o botão direito para finalizar.

Figura 113 - Movendo rápido



Passo 5. Defina parâmetros, programação de arme e ligação de alarme. Desenhe um quadro de filtragem de destino. Veja "3.3.2.4.1 Tripwire. "

Figura 114 - Definir parâmetros

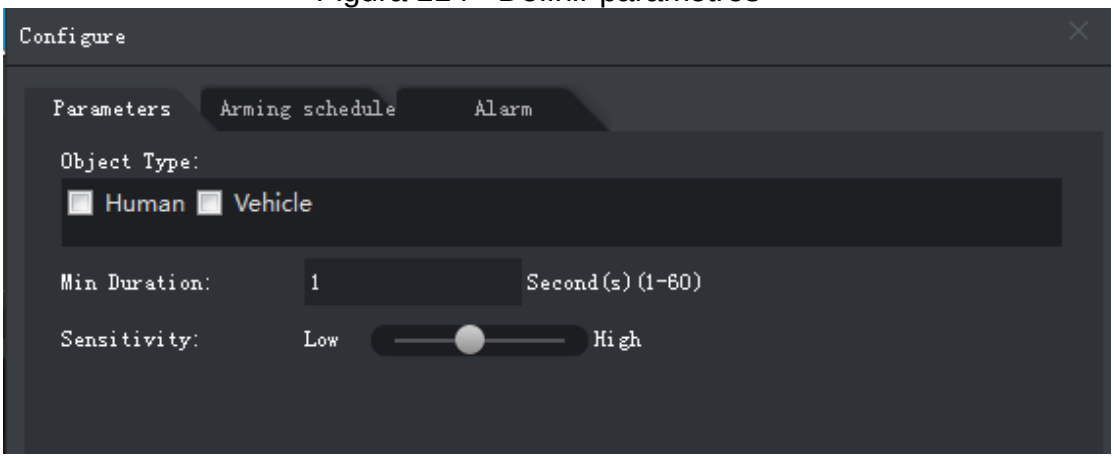


Tabela 18 - Parâmetros

Parâmetro	Descrição
Tipo de objeto	Somente humanos ou veículos podem disparar o alarme.
Duração mínima	A duração mínima do movimento rápido na zona de detecção.
Sensibilidade	Recomenda-se manter o valor padrão.

Passo 6. Clique em **Aplicar**.

3.3.2.4.5 Detecção de estacionamento

Quando um veículo é detectado estacionando em uma área, um alarme será acionado.

Passo 1. Na interface Configuração de IVS, clique em Configuração de Regras.
Passo 2. Clique em Adicionar regra.
Passo 3. Habilite a regra e modifique o nome e o tipo.

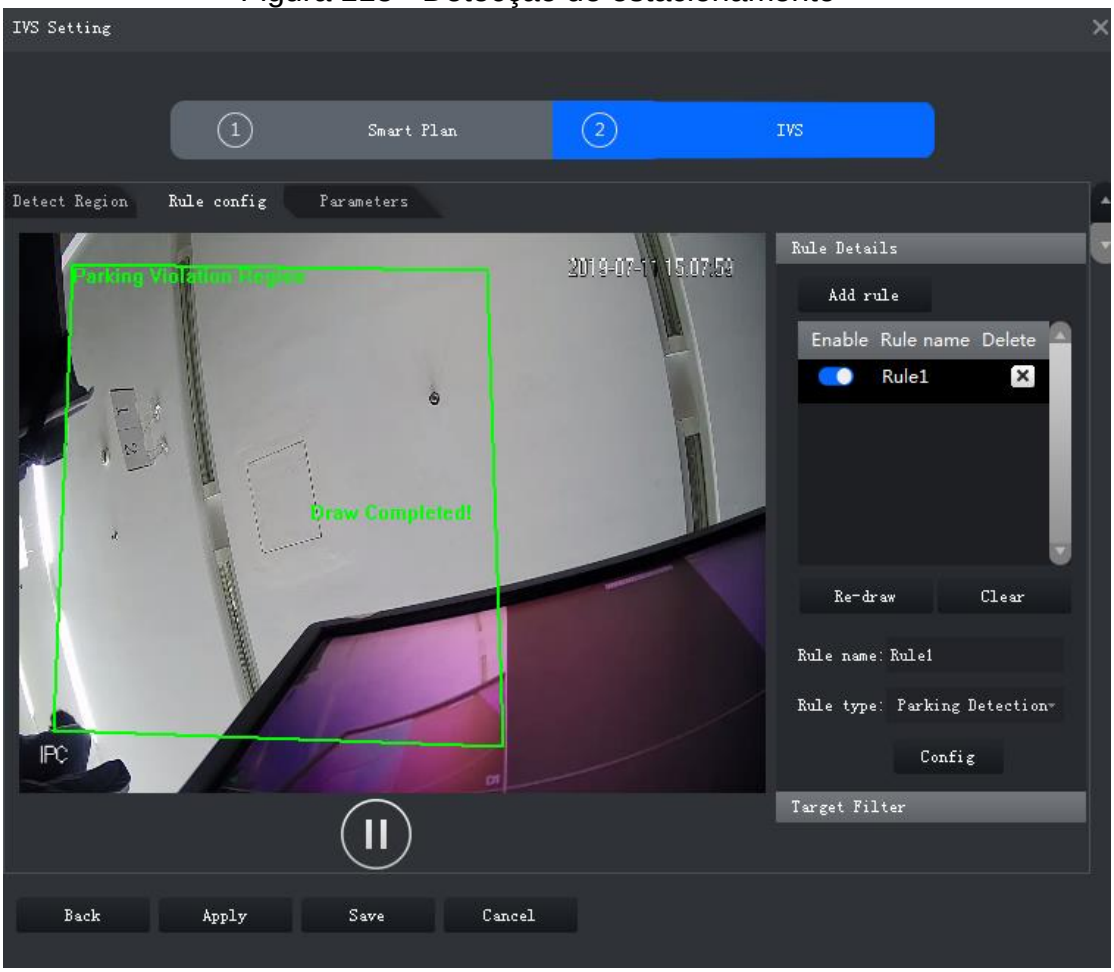
I. Ativar regra.  indica que a regra está habilitada.

II. Modifique o nome da regra.

III. Selecione Detecção de estacionamento na lista suspensa de Tipo de regra.

Passo 4. Desenhe uma zona de detecção no vídeo e clique com o botão direito para finalizar.

Figura 115 - Detecção de estacionamento



Passo 5. Defina parâmetros, programação de arme e ligação de alarme. Desenhe um quadro de filtragem de destino. Vejo "3.3.2.4.1 Tripwire. "

Figura 116 - Definir parâmetros

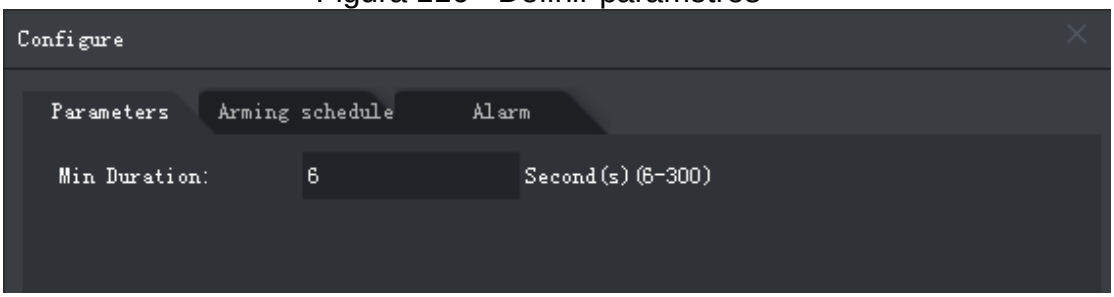


Tabela 19 - Parâmetros

Parâmetro	Descrição
Duração mínima	O tempo mínimo de duração do estacionamento até o acionamento do alarme.

Passo 6. Clique em **Aplicar**.

3.3.2.4.6 Multidão

Quando o tamanho da multidão de pessoas na zona de detecção excede o valor predefinido, o sistema dispara um alarme.

Passo 1. Na interface Configuração de IVS, clique em Configuração de Regras.
Passo 2. Clique em Adicionar regra.
Passo 3. Habilite a regra e modifique o nome e o tipo.

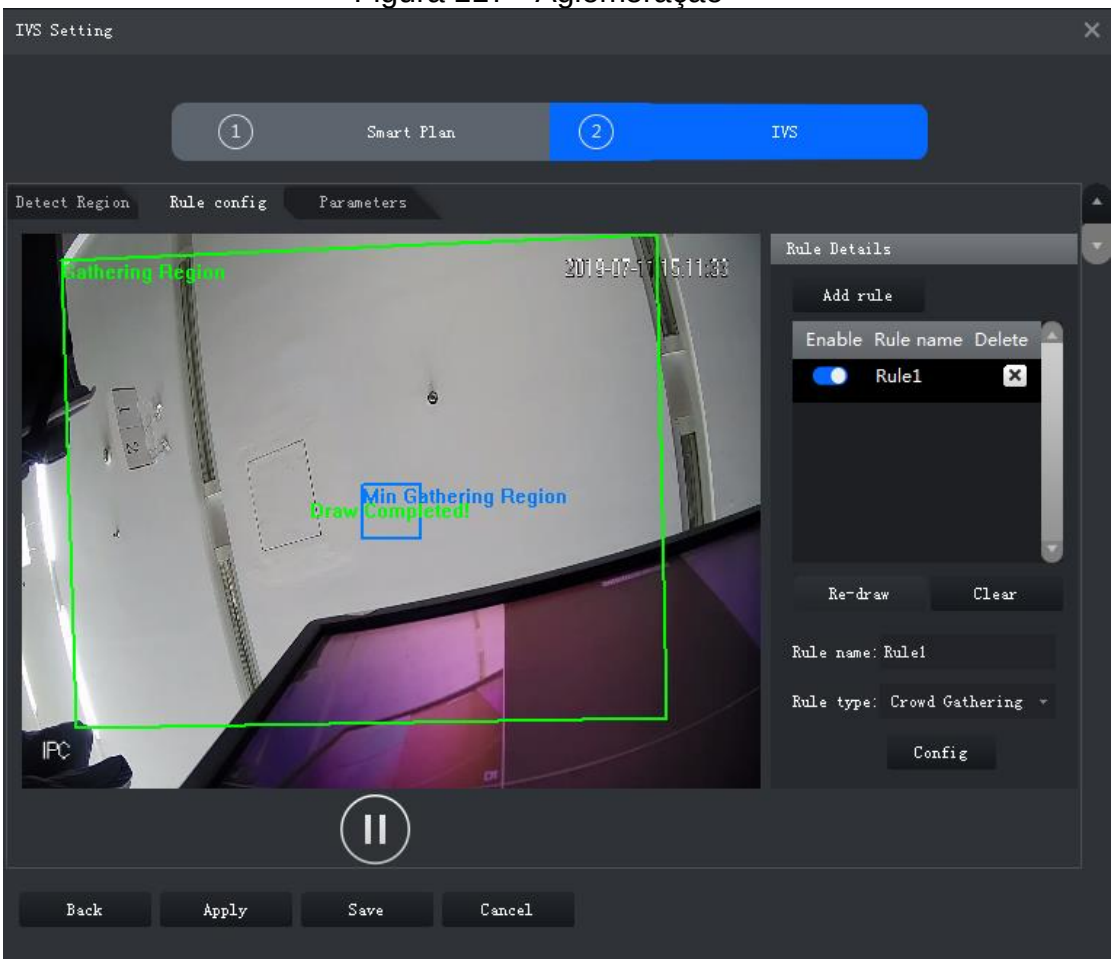
I. Ativar regra.  indica que a regra está habilitada.

II. Modifique o nome da regra.

III. Selecione Aglomeração na lista suspensa do **Tipo de regra**.

Passo 4. Desenhe uma zona de detecção no vídeo e clique com o botão direito para finalizar. Clique em Mínima Região de Aglomeração e arraste os cantos da zona para ajustar o tamanho.

Figura 117 - Aglomeração



Passo 5. Defina parâmetros, programação de arme e ligação de alarme. Desenhe um quadro de filtragem de destino. Vejo "3.3.2.4.1 Tripwire. "

Figura 118 - Definir parâmetros

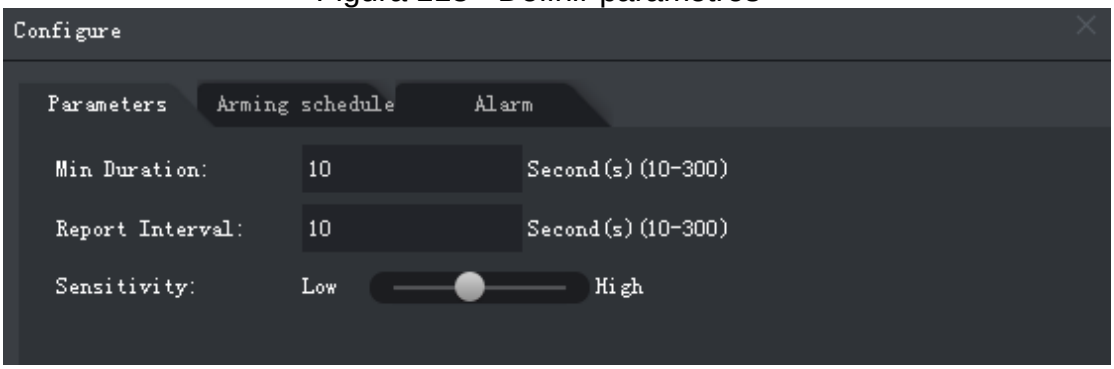


Tabela 20 - Parâmetros

Parâmetro	Descrição
Duração mínima	A duração mínima do tempo em que a multidão é detectada até o acionamento do alarme
Intervalo de relatório	Se o evento ainda existir após o primeiro alarme, o sistema acionará mais alarmes pelo intervalo de alarme predefinido.
Sensibilidade	Recomenda-se manter o valor padrão.

Passo 6. Clique em Aplicar.

3.3.2.4.7 Objeto ausente

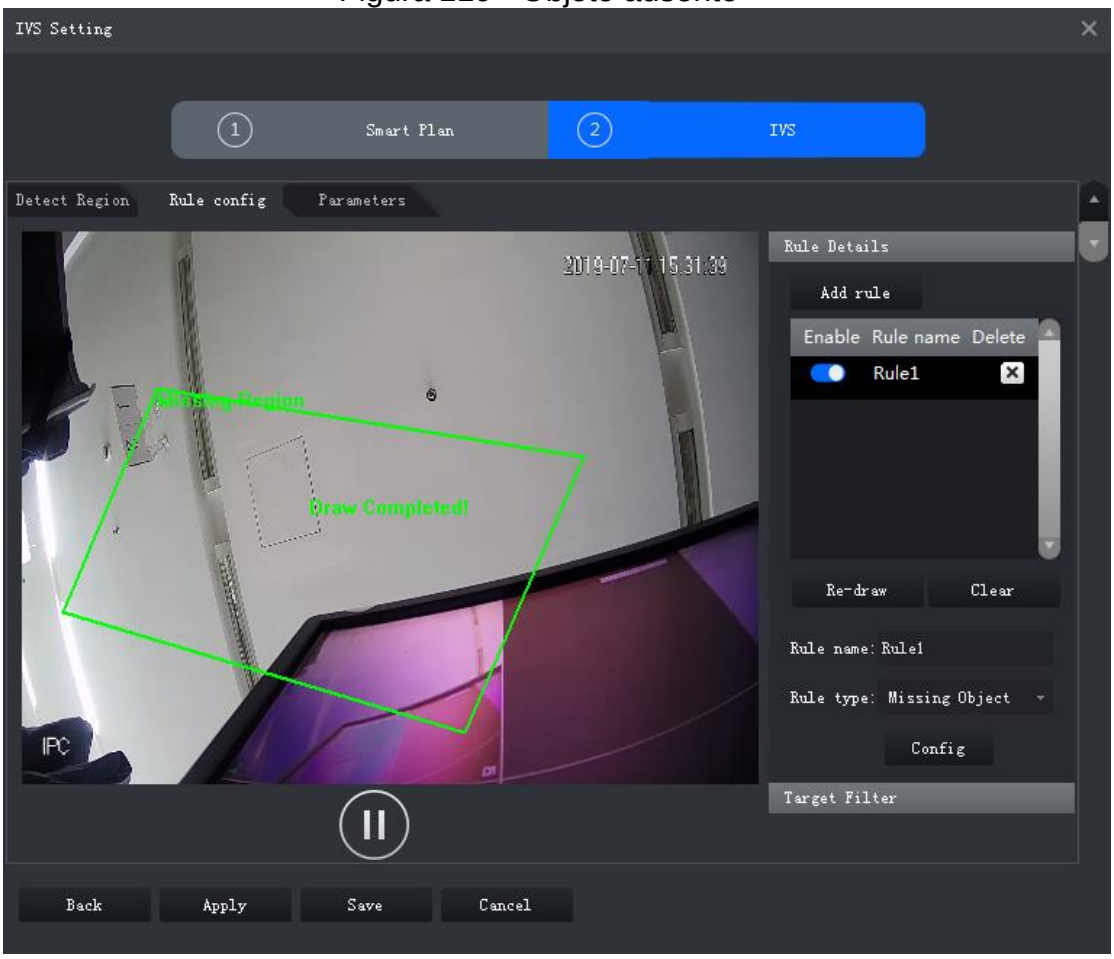
Se um objeto foi movido para fora da zona de detecção e não foi colocado de volta por um determinado período de tempo, o sistema disparará um alarme.

Passo 1. Na interface Configuração de IVS, clique em Configuração de Regras.
Passo 2. Clique em Adicionar regra.
Passo 3. Habilite a regra e modifique o nome e o tipo.

I. Ativar regra.  indica que a regra está habilitada.
II. Modifique o nome da regra.
III. Selecione Objeto ausente na lista suspensa do tipo de regra.

Passo 4. Desenhe uma zona de detecção no vídeo e clique com o botão direito para finalizar.

Figura 119 - Objeto ausente



Passo 5. Defina parâmetros, programação de arme e ligação de alarme. Desenhe um quadro de filtragem de destino. Vejo "3.3.2.4.1Tripwire. "

Figura 120 - Definir parâmetros

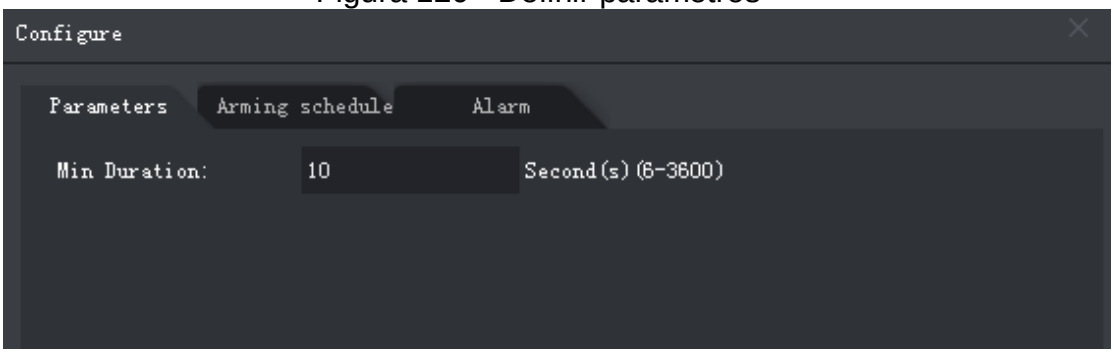


Tabela 21 - Parâmetros

Parâmetro	Descrição
Duração mínima	O tempo mínimo de duração desde o desaparecimento do objeto até o disparo do alarme.

Passo 6. Clique em Aplicar.

3.3.2.4.8 Atitude Suspeita

Quando um alvo permanece na zona de detecção após aparecer por um determinado período de tempo, um alarme será acionado.

Passo 1. Na interface Configuração de IVS, clique em Configuração de Regras.
Passo 2. Clique em Adicionar regra.
Passo 3. Habilite a regra e modifique o nome e o tipo.

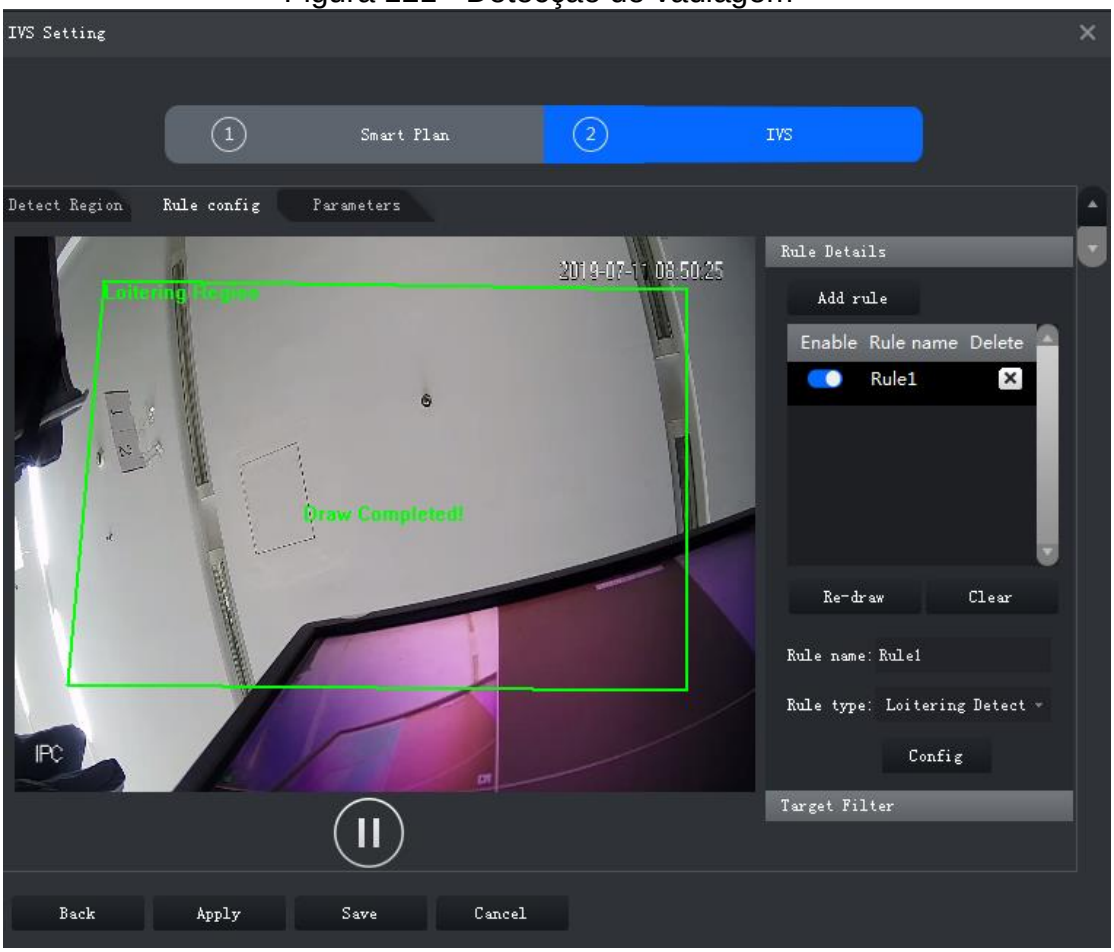
I. Ativar regra.  indica que a regra está habilitada.

II. Modifique o nome da regra.

III. Selecione **Atitude Suspeita** na lista suspensa de **Tipo de regra.**

Passo 4. Desenhe uma zona de detecção no vídeo e clique com o botão direito para finalizar.

Figura 121 - Detecção de vadiagem



Passo 5. Defina parâmetros, programação de arme e ligação de alarme. Desenhe um quadro de filtragem de destino. Vejo "3.3.2.4.1 Tripwire. "

Figura 122 - Definir parâmetros

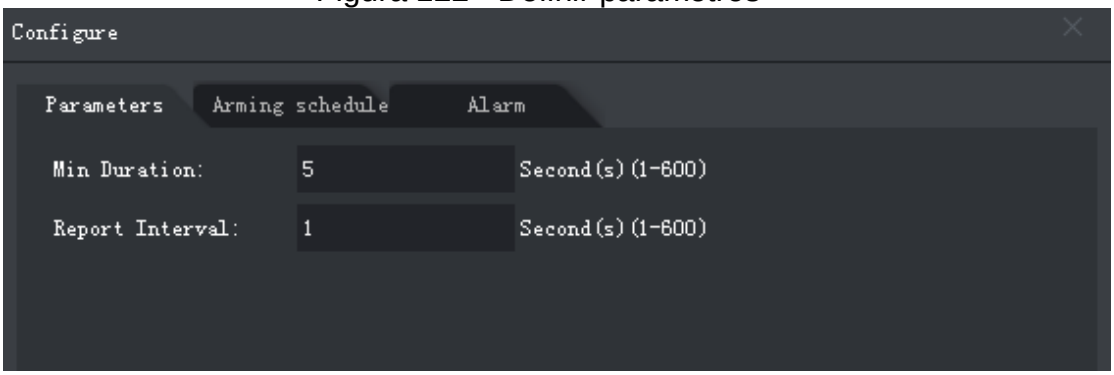


Tabela 22 - Parâmetros

Parâmetro	Descrição
Duração mínima	O tempo mínimo de duração desde o aparecimento do alvo até o acionamento do alarme.
Intervalo de relatório	Se o evento ainda existir após o primeiro alarme, o sistema acionará mais alarmes pelo intervalo de alarme predefinido.

Passo 6. Clique em **Aplicar.**

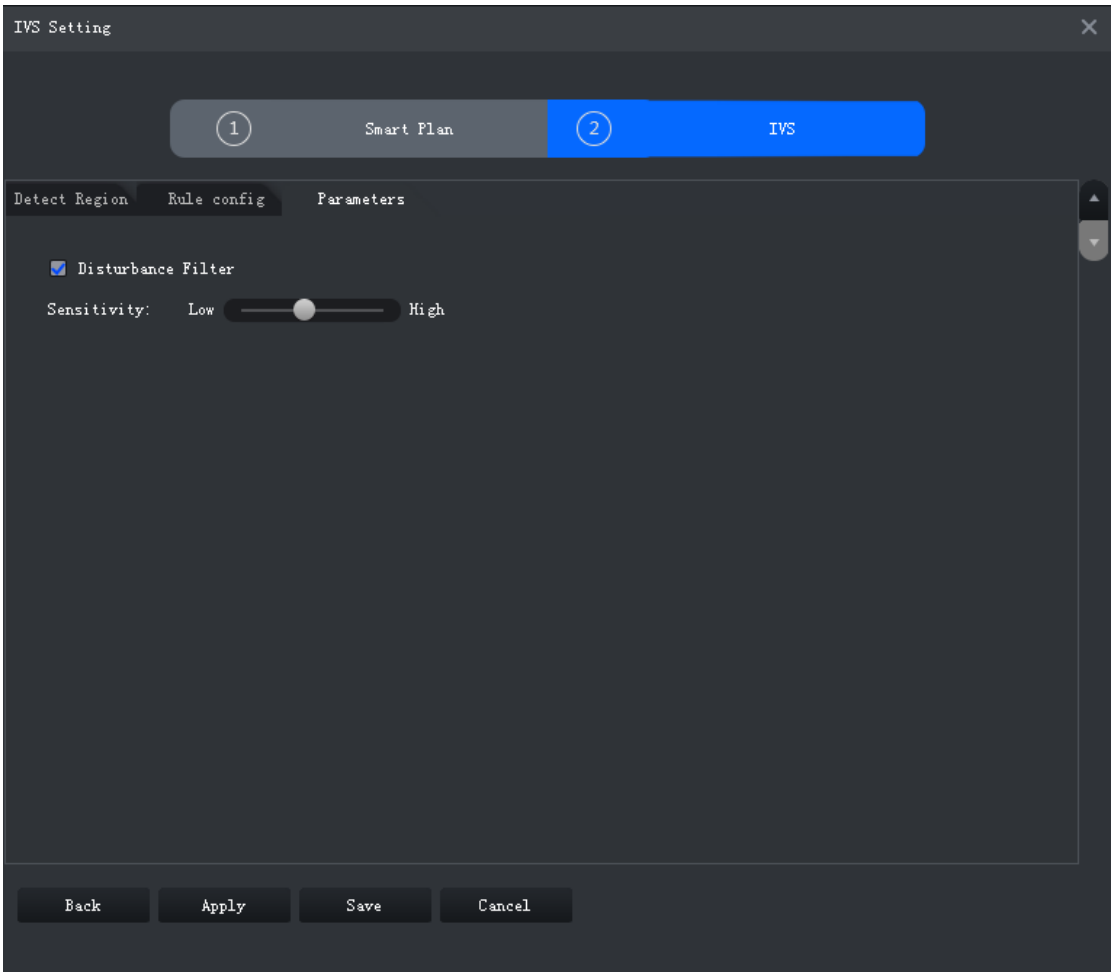
3.3.2.5 Parâmetros de configuração

Defina parâmetros comuns para o IVS, incluindo filtro de perturbação e sensibilidade.

Passo 1. Clique em **Parâmetros** após configurar as regras na interface de **Configuração da regra.**

Passo 2. Defina os parâmetros.

Figura 123 - Parâmetros



Parâmetro	Descrição
Filtro de Perturbação	Filtre alvos falsos, incluindo plantas ondulantes e ondas de água. Esta função pode causar omissões de alvo, pois algumas partes de um alvo verdadeiro podem ser julgadas como fatores falsos.
Sensibilidade	Sensibilidade de detecção de controle. Quanto menor for o valor, menor será a taxa de detecção falsas e maior será a taxa de omissão. Quanto maior for o valor, maior será a taxa de detecção falsos e menor será a taxa de omissão.

Passo 3. Clique em **Salvar.**

3.4 ANÁLISE DE FLUXO

O sistema fornece relatório de contagem de pessoas, relatório de permanência e relatório de mapa de calor.

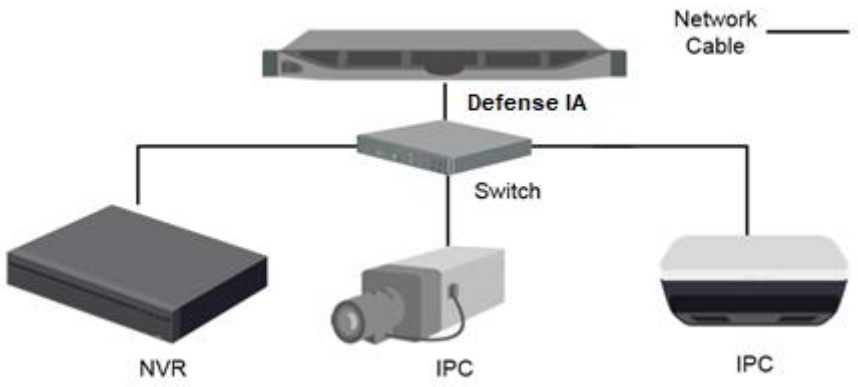
- Relatório de análise de fluxo

As câmeras relatam os resultados da análise para a plataforma, e então a plataforma pode processar e mostrar os relatórios correspondentes.

- Relatório de Pessoas Remanescentes
  A plataforma mostra a quantidade de pessoas remanescentes de acordo com os dados de análise informados pelas câmeras.
- Mapa de calor
  O mapa de calor mostra a distribuição das pessoas em uma área durante um período específico em cores diferentes, para que você possa ver qual seção é mais popular e qual é menos.

3.4.1 Topologia Típica

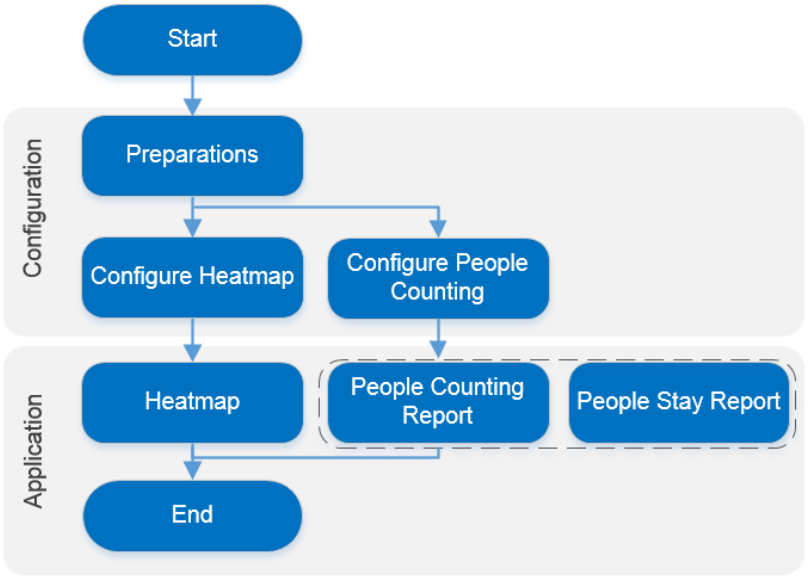
Figura 124 - Topologia típica



- As câmeras gravam vídeos e analisam o fluxo de pessoas. Além dos IPCs mostrados na topologia, o módulo de análise de fluxo também oferece suporte às câmeras PTZ com contagem de pessoas e recursos de mapa de calor.
- Os NVRs são conectados às câmeras. Eles analisam o fluxo de pessoas e armazenam vídeos.
- A plataforma gerencia centralmente todos os NVRs e câmeras, recebe os resultados da análise das câmeras e mostra os relatórios.
- A análise de fluxo pode ser feita por câmera de contagem de pessoas ou NVR inteligente.

3.4.2 Fluxo de Negócios

Figura 125 - Fluxo de análise de fluxo de negócios



3.4.3 Configurando a Análise de Fluxo

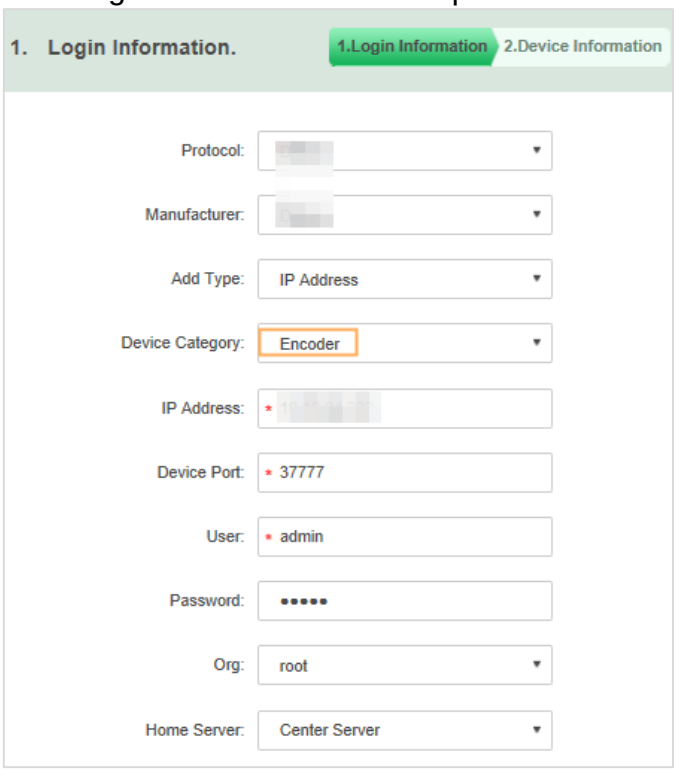
3.4.3.1 Preparativos

Certifique-se de que os seguintes preparativos foram feitos:

- Câmeras e NVRs com contagem de pessoas ou função de mapa de calor estão instalados corretamente. As regras de Mapa de Calor e/ou de contagem de pessoas foram configurados e ativados nos dispositivos. Para obter detalhes, consulte os manuais dos dispositivos correspondentes.
- As configurações básicas da plataforma foram concluídas. Para configurar, consulte "3 Configurações básicas."

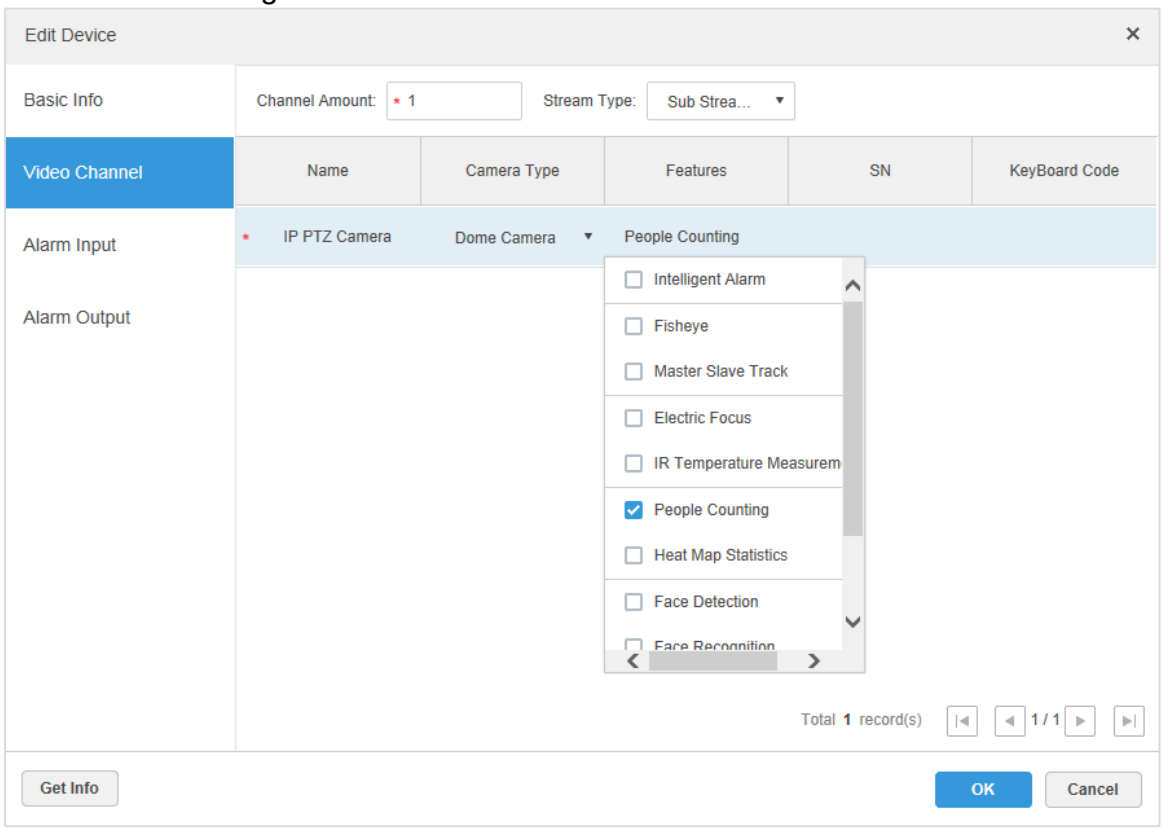
  Ao adicionar uma câmera ou NVR na interface de Dispositivos na interface Web do Servidor, selecione Encoder para a categoria de dispositivo.

Figura 126 - Adicionar Dispositivo



- Na interface do dispositivo, clique em , depois entre Canal de Vídeo e, em seguida, selecione Estatísticas do mapa térmico ou Estatísticas de linhas cruzadas como características.

Figura 127 - Editar recursos do canal de vídeo



3.4.3.2 Configurando Mapa de Calor

O mapa de calor exibe a distribuição de objetos em movimento em cores de tons diferentes. Ele indica a “temperatura” (quantidade de movimento na área) das regiões por cores diferentes. Por exemplo, vermelho significa que a quantidade de movimento na área está relativamente alta e azul significa que a quantidade de movimento na área está relativamente baixa. A configuração na interface pode variar dependendo do tipo de câmera. Esta seção leva a configuração de câmera de contagem de pessoas Stereo Vision, por exemplo.

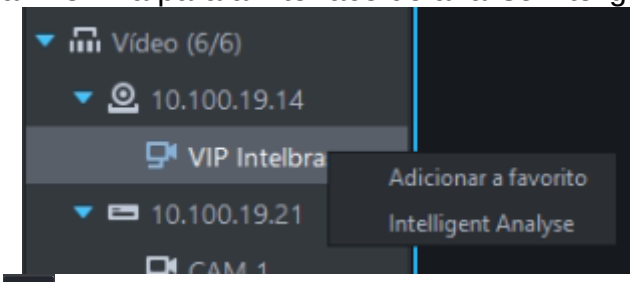
- Você pode configurar o mapa de calor na plataforma apenas quando a câmera está diretamente conectada à plataforma. Caso contrário, configure diretamente na interface da câmera ou NVR.

Passo 1. Vá para a interface do Intelligent Analyze.

I. Faça login no Control Client e clique em e selecione **Visualização.**

II. Clique com o botão direito em uma câmera e selecione **Intelligent Analyze.**

Figura 128 - Vá para a interface de análise inteligente



Passo 2. Clique para selecionar o mapa de calor.

Quando o ícone é exibido com destaque em branco, significa que ele está selecionado. Se outro plano inteligente, que está em conflito com o Mapa de calor, já estiver selecionado, clique no ícone do plano inteligente para desmarcá-lo e clique em para selecionar o mapa de calor.

Figura 129 - Plano inteligente

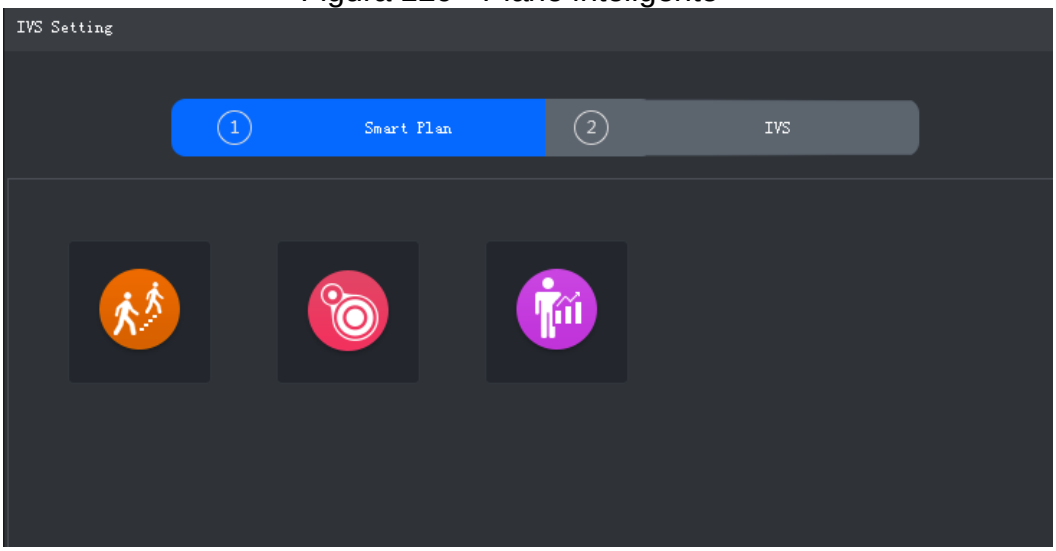
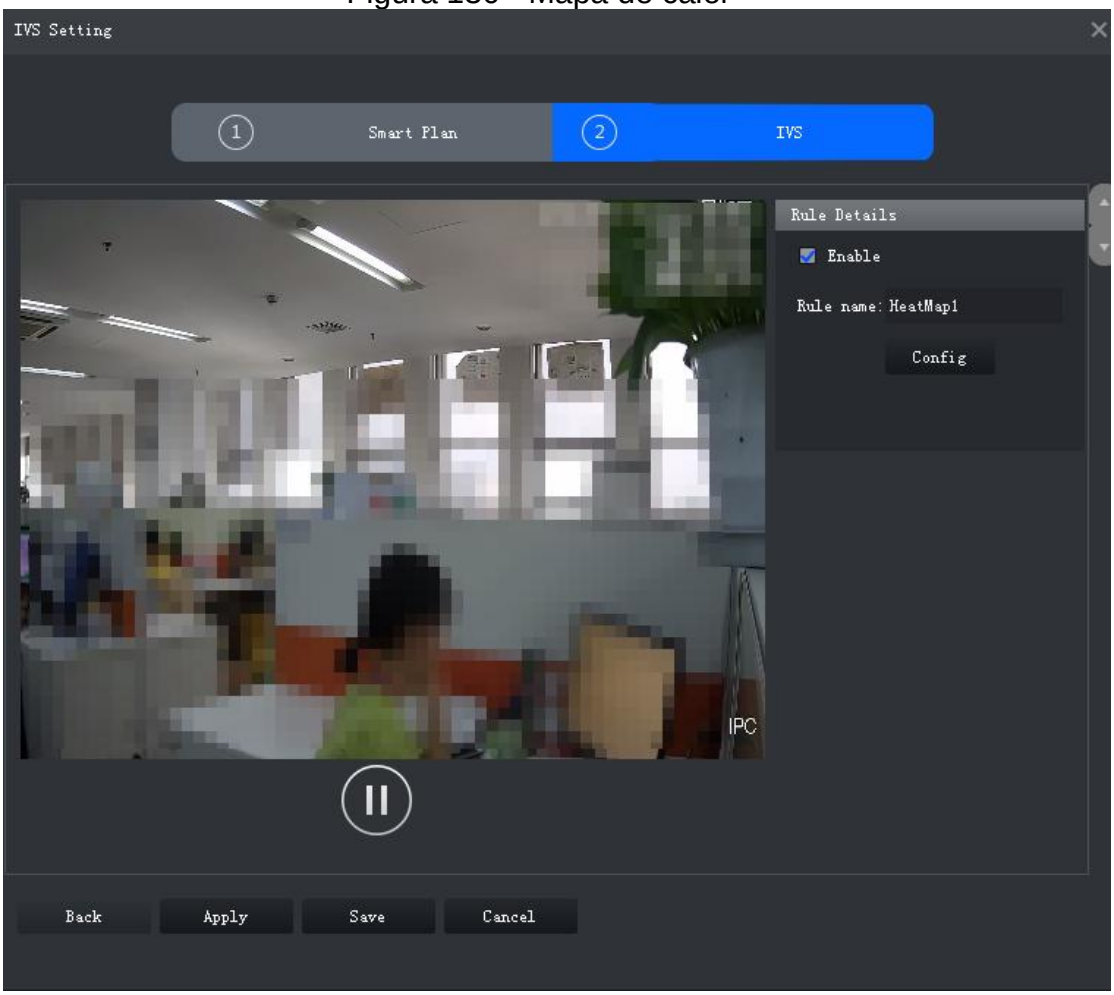


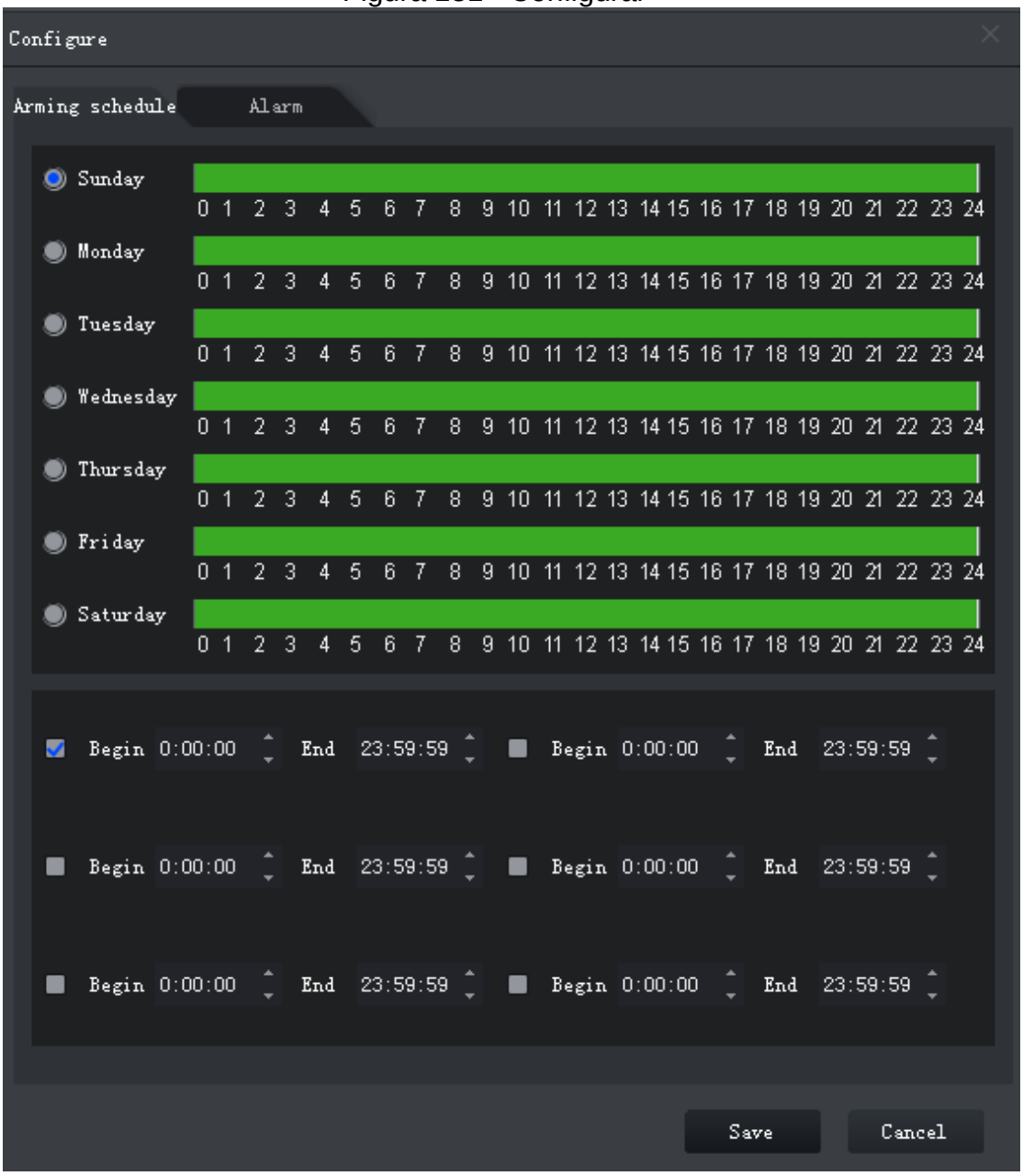
Figura 130 - Mapa de calor



Passo 3. Selecione a caixa de seleção **"Habilitar"** para habilitar o mapa de calor.
Passo 4. Modifique o nome da regra.
Passo 5. Configure a Agenda de Funcionamento e realize uma vinculação de alarme.

I. Clique em **Config.**

Figura 131 - Configurar

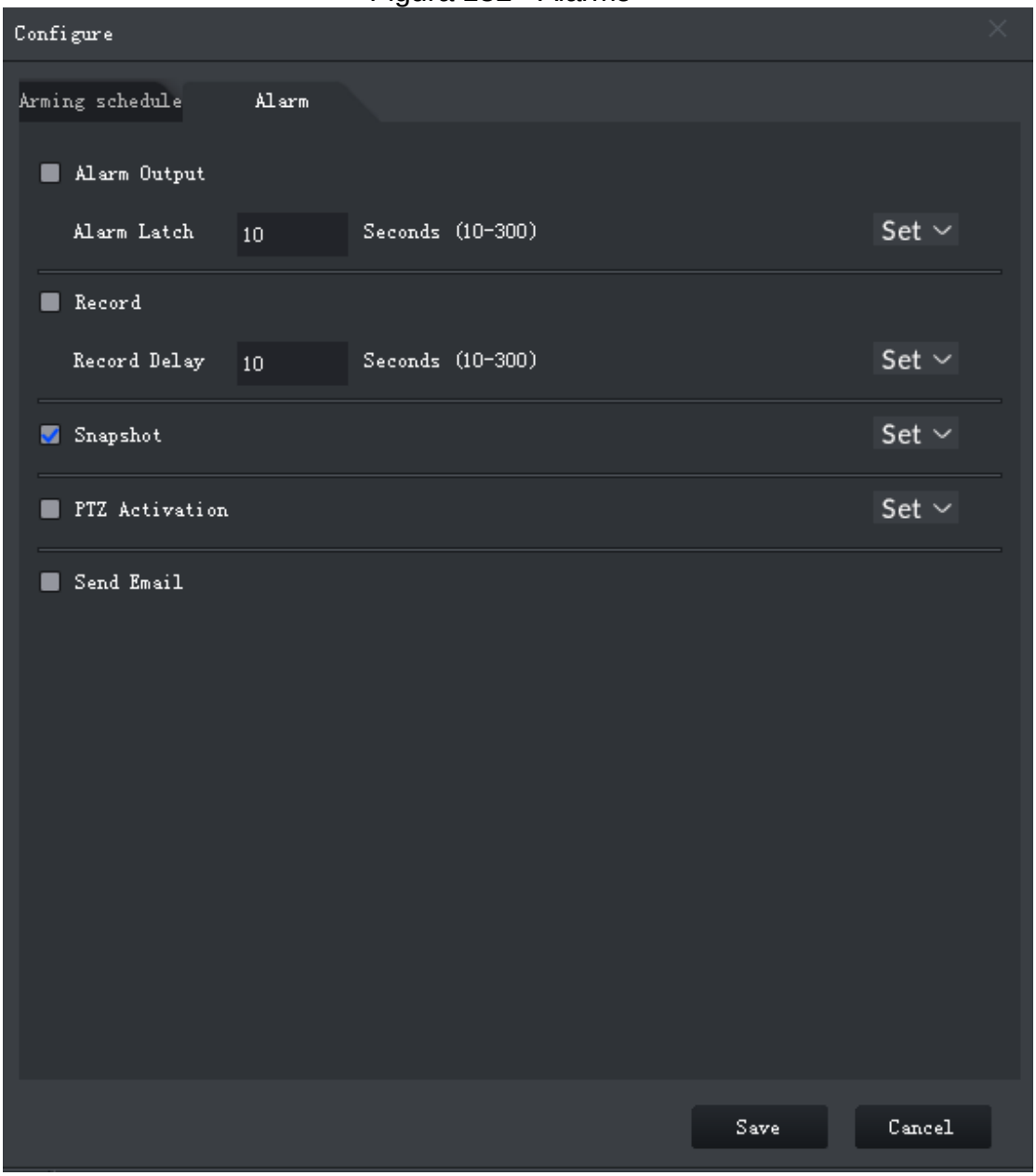


I. Clique em Agenda de Funcionamento, selecione os dia e as horas e, a seguir, defina a hora de início e de término.

- A Agenda de Funcionamento padrão é definida como 24 horas por dia.

II. Clique em Alarme para definir ações de vinculação.

Figura 132 - Alarme



Parâmetro	Descrição	
Saída de alarme	Conecte os dispositivos de saída de alarme às interfaces de saída de alarme. Quando o evento é disparado, o sistema enviará o alarme para a saída do dispositivo.	Clique em Definir (Set) para definir próxima Trava de alarme e selecione um canal de saída de alarme.
Trava de alarme	A ação de saída de alarme atrasará a parada após o término do evento de alarme.	

Parâmetro	Descrição	
Gravação	Quando um alarme acontece, ele aciona a gravação automática de vídeo imediatamente. Requer que o dispositivo já tenha programações de gravação. Consulte o manual do dispositivo para obter instruções detalhadas.	Clique em Definir **(Set)** próximo a **Gravar (Record)** para selecionar o canal de gravação.
Atraso de gravação	A gravação de vídeo atrasa, parando um pouco após o término do evento de alarme.	
Snapshots	O sistema irá tirar snapshots automaticamente quando um alarme acontecer. Requer que o dispositivo já tenha programações de instantâneos. Consulte o manual do dispositivo para obter instruções detalhadas.	Clique em Definir **(Set)** próximo a **Snapshot** para selecionar o canal de instantâneo.
Enviar email	O sistema enviará um e-mail para o endereço de e-mail relacionado quando ocorrer um alarme. Requer que o dispositivo já tenha o e-mail configurado. Consulte o manual do dispositivo para obter instruções detalhadas.	Nenhum

Passo 6. Clique em **Salvar.**

3.4.3.3 Configurando a contagem de pessoas

Defina as configurações de contagem de pessoas para analisar o número de pessoas que entram e saem.

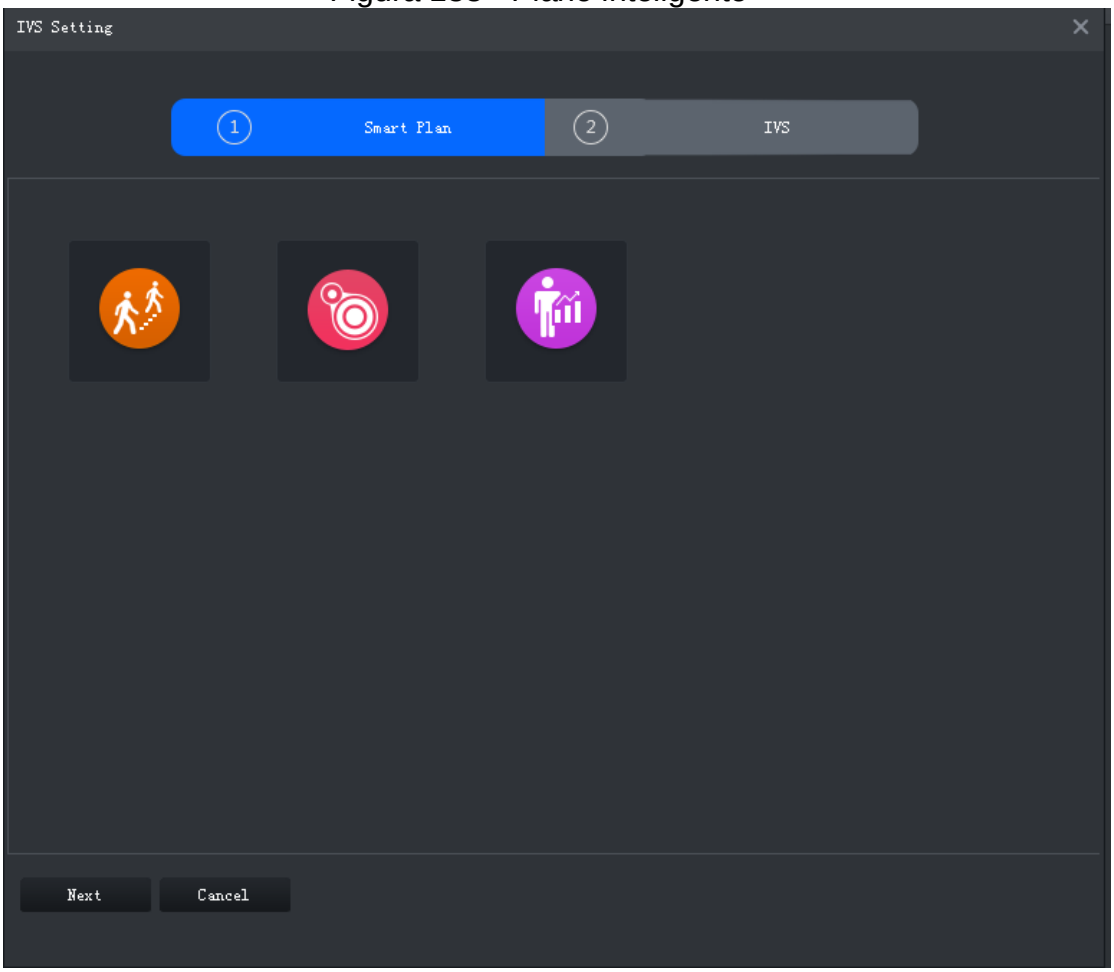
- Você pode configurar a contagem de pessoas na plataforma somente quando a câmera estiver conectada diretamente na plataforma. Caso contrário, configure-o na câmera ou NVR.

Passo 1. Vá para a interface do **Intelligent Analyze.**

Passo 2. Clique  para selecionar a contagem de pessoas.

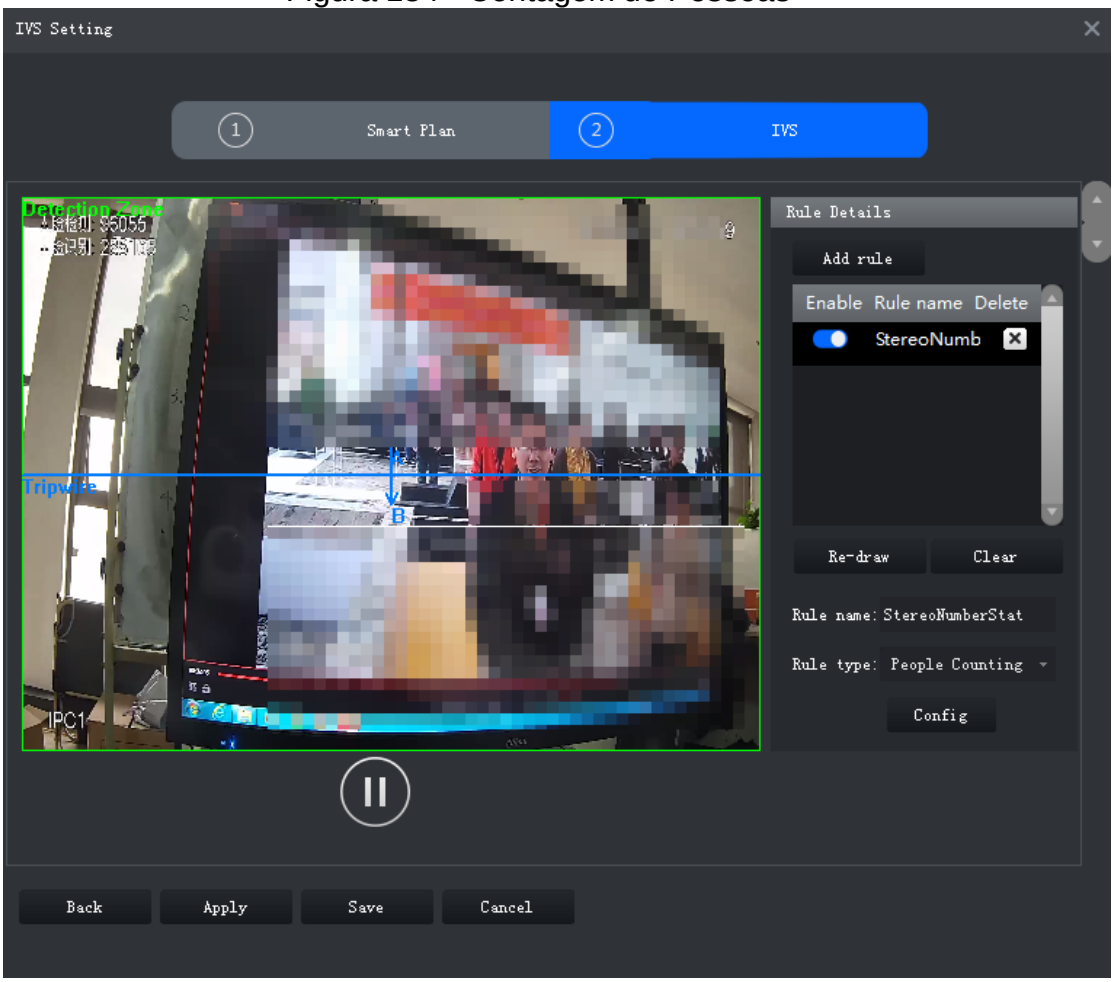
Quando o ícone é exibido com destaque em branco, significa que ele está selecionado. Se outro plano inteligente, que está em conflito com a contagem de pessoas, for selecionado, clique no ícone do plano inteligente para desmarcá-lo e clique em  para selecionar a contagem de pessoas.

Figura 133 - Plano inteligente



Passo 3. Clique em **Avançar.**
A interface de **configuração de IVS** é exibida.

Figura 134 - Contagem de Pessoas



Passo 4. Clique em Adicionar regra.

Passo 5. Habilite a regra e modifique o nome e o tipo.

I. Ative a regra.  indica que a regra está habilitada.

II. Modifique o nome da regra.

III. Selecione o tipo de regra na lista suspensa de **Tipo de regra.**

- **Contagem de Pessoas**: O sistema detecta o número de pessoas que entram e saem da zona de detecção. Quando o número de entrada / saída / permanência excede o valor predefinido, o sistema irá disparar um alarme.
- **ManNumDetection**: Sistema detecta número de pessoas e a duração da estadia dentro da zona de detecção. Quando o número de pessoas ou duração de estadia excede o valor predefinido, o sistema irá disparar um alarme.

Passo 6. Selecione a zona ou linha padrão no vídeo e clique em **Limpar** para excluí-la ou **Redesenhar** para desenhar uma nova.

A contagem de pessoas requer o desenho de uma zona de detecção e uma linha, enquanto ManNumDetection requer apenas uma zona de detecção.

- Ao traçar a linha da esquerda para a direita, a direção é A para B, e então o fluxo de pessoas de A para B é o número da entrada e B para A é o número da saída. Ao traçar a linha da direita para a esquerda, a direção é B para A, e então o fluxo de pessoas de B para A é o número da entrada e A para B é o número da saída.

Passo 7. Defina parâmetros, configure a Agenda de Funcionamento e realize uma vinculação de alarme.

I. Clique em **Config** e defina os parâmetros.

Figura 135 - Definir parâmetros (contagem de pessoas)

Figura 136 - Definir parâmetros (ManNumDetection)

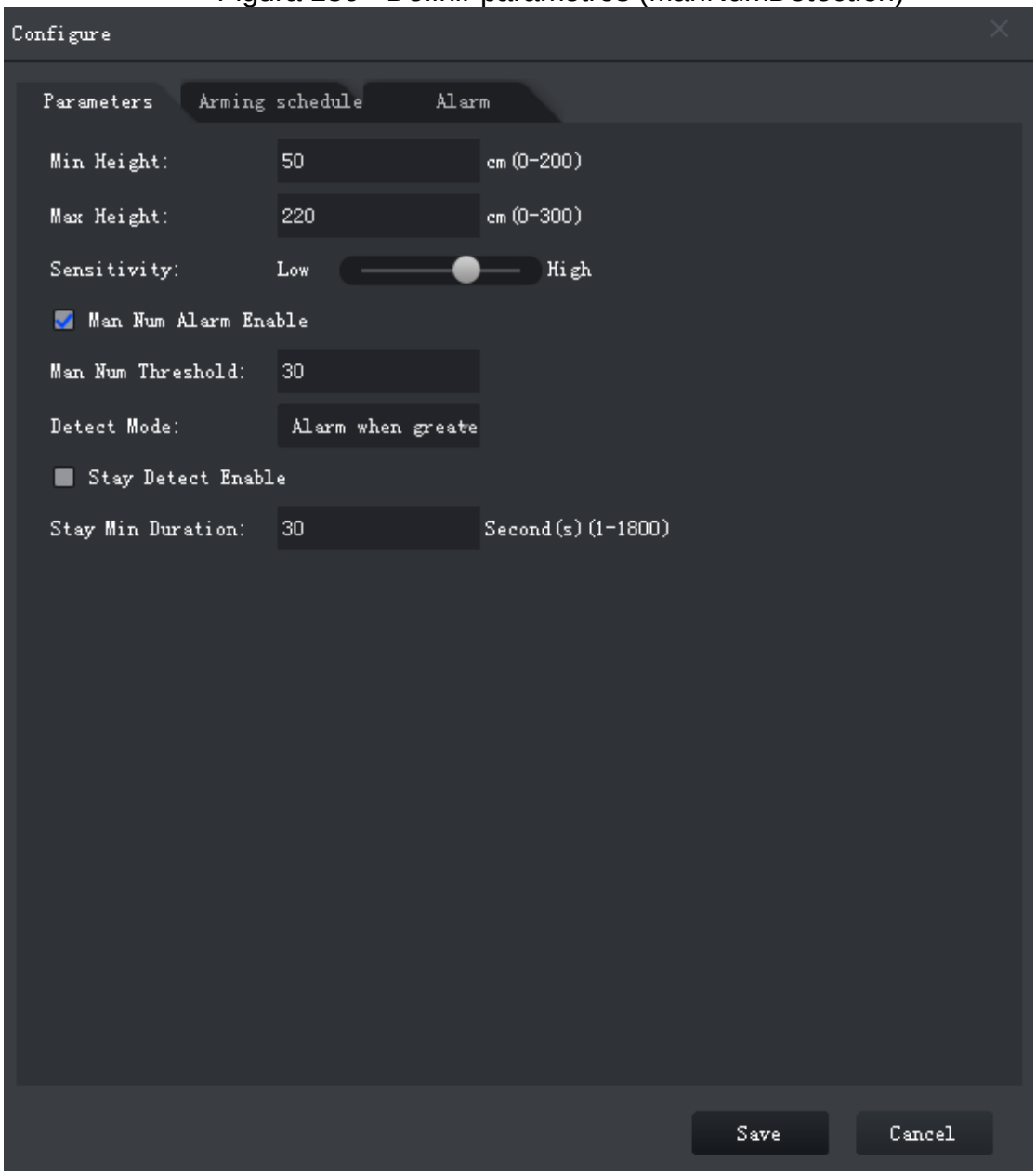


Tabela 23 - Parâmetros

Parâmetro	Descrição
Altura mínima	Quando a altura do alvo está entre a altura mínima e a altura máxima, o sistema acionará a regra de estatísticas.
Altura máxima	
Man Num Alarm Enable	Quando o número de pessoas na zona atinge, excede ou é menor do que o valor predefinido, o sistema irá disparar um alarme.
Man Num Threshold	
Modo de detecção	
Habilitar tempo de estadia	Quando o tempo de permanência das pessoas na zona ultrapassar o valor predefinido, o sistema acionará um alarme.
Duração mínima da estadia	
Nº de Entrada	Quando o número de entrada excede o valor predefinido, o sistema dispara um alarme.

Parâmetro	Descrição
Nº de saída	Quando o número de saída excede o valor predefinido, o sistema dispara um alarme.
Restante No.	Quando o número de pessoas restantes exceder o valor predefinido, o sistema disparará um alarme.
Sensibilidade	Recomenda-se manter o valor padrão.

I. Clique em Agenda de Funcionamento, selecione o dia e as horas e defina a hora de início e de término.

- A Agenda de Funcionamento padrão é definida como 24 horas por dia.

Figura 137 - Agenda de Funcionamento

II. Clique em **Alarme** para definir ações de vinculação.

Figura 138 - Alarme

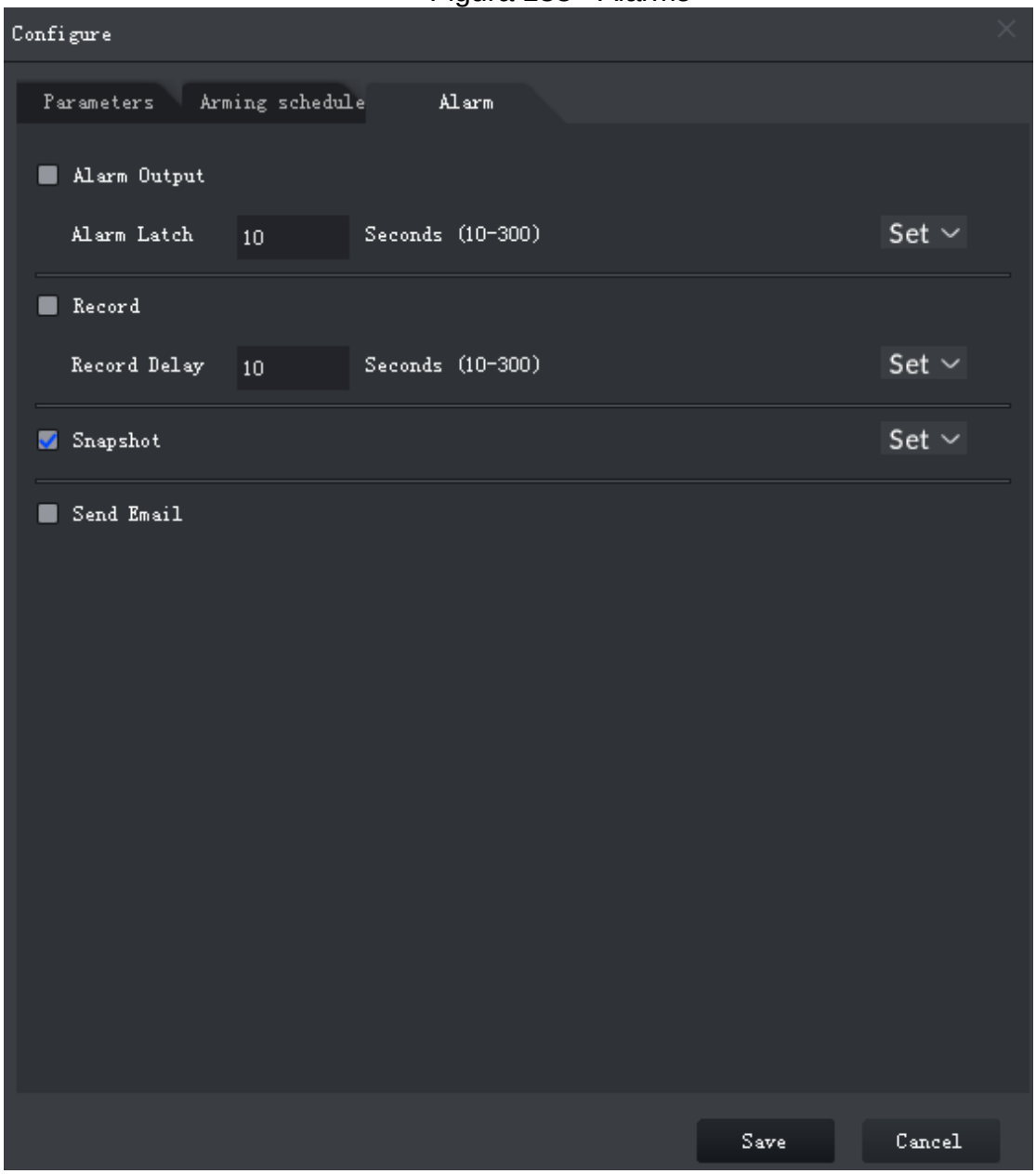


Tabela 24 - Parâmetros

Parâmetro	Descrição	
Saída de alarme	Conecte os dispositivos de saída de alarme às interfaces de saída de alarme. Quando o evento é disparado, o sistema enviará o alarme para a saída do dispositivo.	Clique em Definir (Set) para definir próxima Trava de alarme e selecione um canal de saída de alarme.
Trava de alarme	A ação de saída de alarme atrasará a parada após o término do evento de alarme.	

Parâmetro	Descrição	
Gravação	Quando um alarme acontece, ele aciona a gravação automática de vídeo imediatamente. Requer que o dispositivo já tenha programações de gravação. Consulte o manual do dispositivo para obter instruções detalhadas.	Clique em Definir **(Set)** próximo a **Gravar (Record)** para selecionar o canal de gravação.
Atraso de gravação	A gravação de vídeo atrasa, parando um pouco após o término do evento de alarme.	
Snapshots	O sistema irá tirar snapshots automaticamente quando um alarme acontecer. Requer que o dispositivo já tenha programações de instantâneos. Consulte o manual do dispositivo para obter instruções detalhadas.	Clique em Definir **(Set)** próximo a **Snapshot** para selecionar o canal de instantâneo.
Enviar email	O sistema enviará um e-mail para o endereço de e-mail relacionado quando ocorrer um alarme. Requer que o dispositivo já tenha o e-mail configurado. Consulte o manual do dispositivo para obter instruções detalhadas.	Nenhum

Passo 8. Clique em **Salvar.**

3.4.4 Aplicativos de análise de fluxo

3.4.4.1 Mapa de calor

O mapa de calor exibe a distribuição de objetos em movimento em cores de tons diferentes. Ele reflete a temperatura das regiões por cores diferentes. ou, por exemplo, vermelho significa que a temperatura está relativamente alta e azul significa que a temperatura está relativamente baixa.

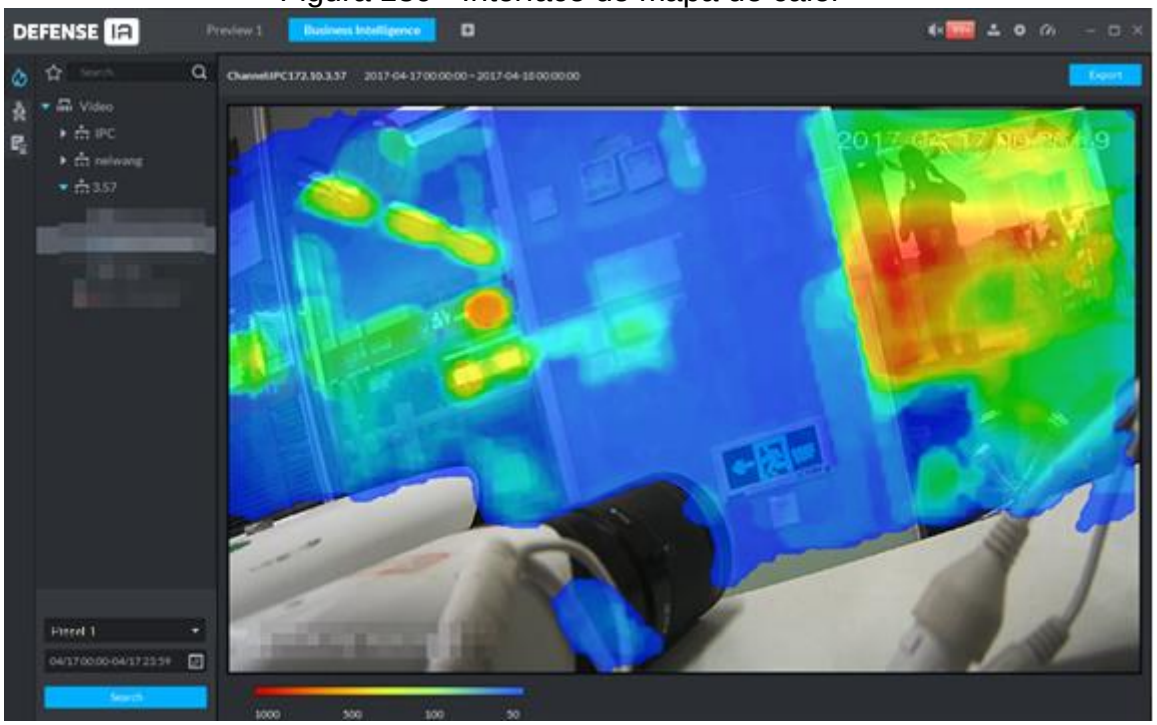
Passo 1. Clique na página inicial e clique em Análise de fluxo.

Passo 2. Clique na guia na interface de análise de fluxo.

Passo 3. Selecione um canal, defina a hora e uma predefinição (somente câmeras PTZ têm predefinições) e clique em **Pesquisar.**

- O dispositivo envia dados do mapa de calor para a plataforma em tempo real. Os dados de mapa de calor de um canal podem ser pesquisados assim que o canal for adicionado à plataforma. Você só pode pesquisar dentro de uma semana de cada vez.

Figura 139 - Interface de mapa de calor



Passo 4. Clique em **Exportar** no canto superior direito para exportar o mapa de calor no formato .bmp.

3.4.4.2 Relatório de contagem de pessoas

Visualize relatórios do número de entradas e saídas de pessoas em um período de tempo específico. Um relatório diário também inclui o número de pessoas que ainda não deixaram a área de destino no período definido.

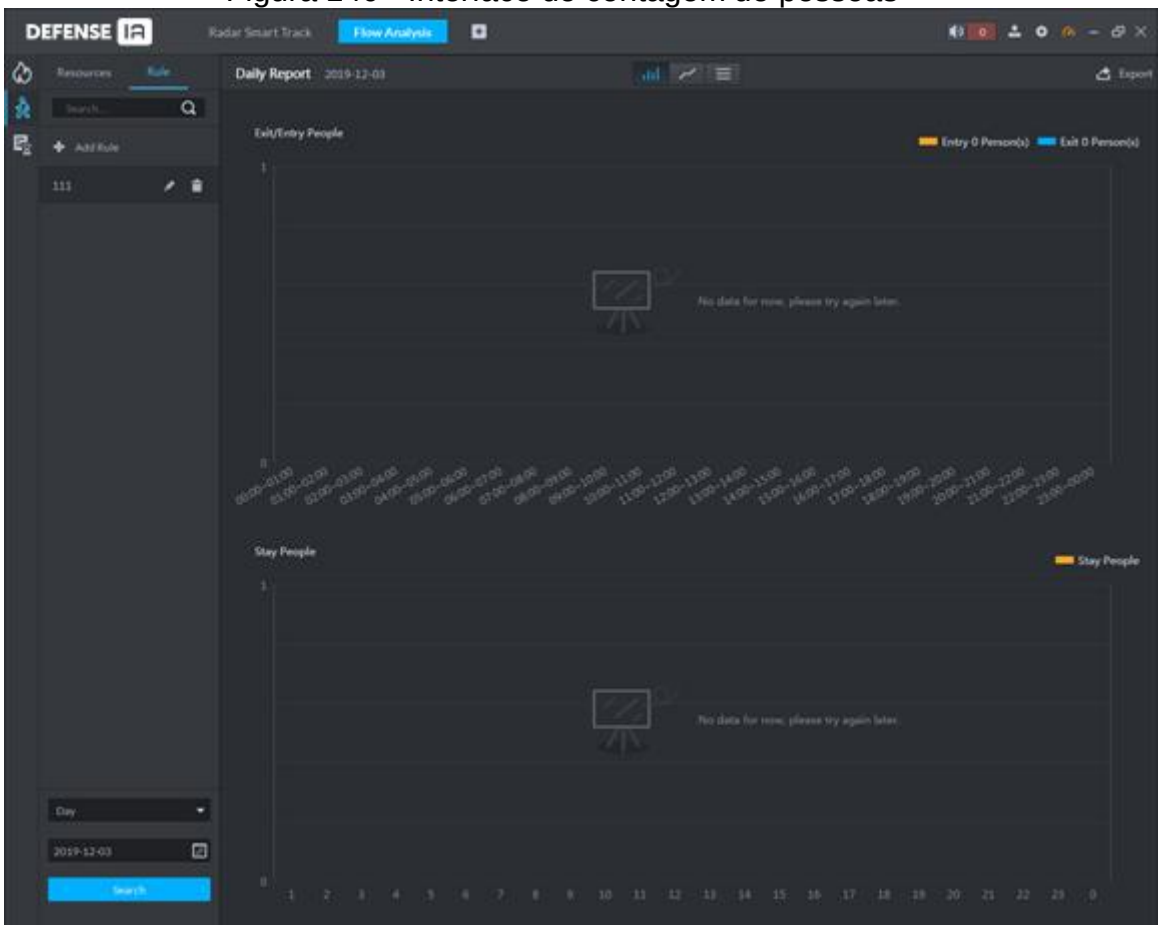
As estatísticas podem ser geradas por câmera ou por regra de contagem de pessoas.

3.4.4.2.1 Gerando Relatório de Câmera

Selecione a câmera de interesse para ver as estatísticas de contagem de pessoas. Por exemplo, se sua loja possui uma porta, para visualizar o número total de pessoas que entram e saem de sua loja, selecione a câmera de contagem de pessoas para gerar o relatório.

Passo 1. Na interface do Análise de Fluxo, clique em 

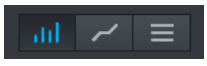
Figura 140 - Interface de contagem de pessoas



Passo 2. Clique na guia **Recursos**.

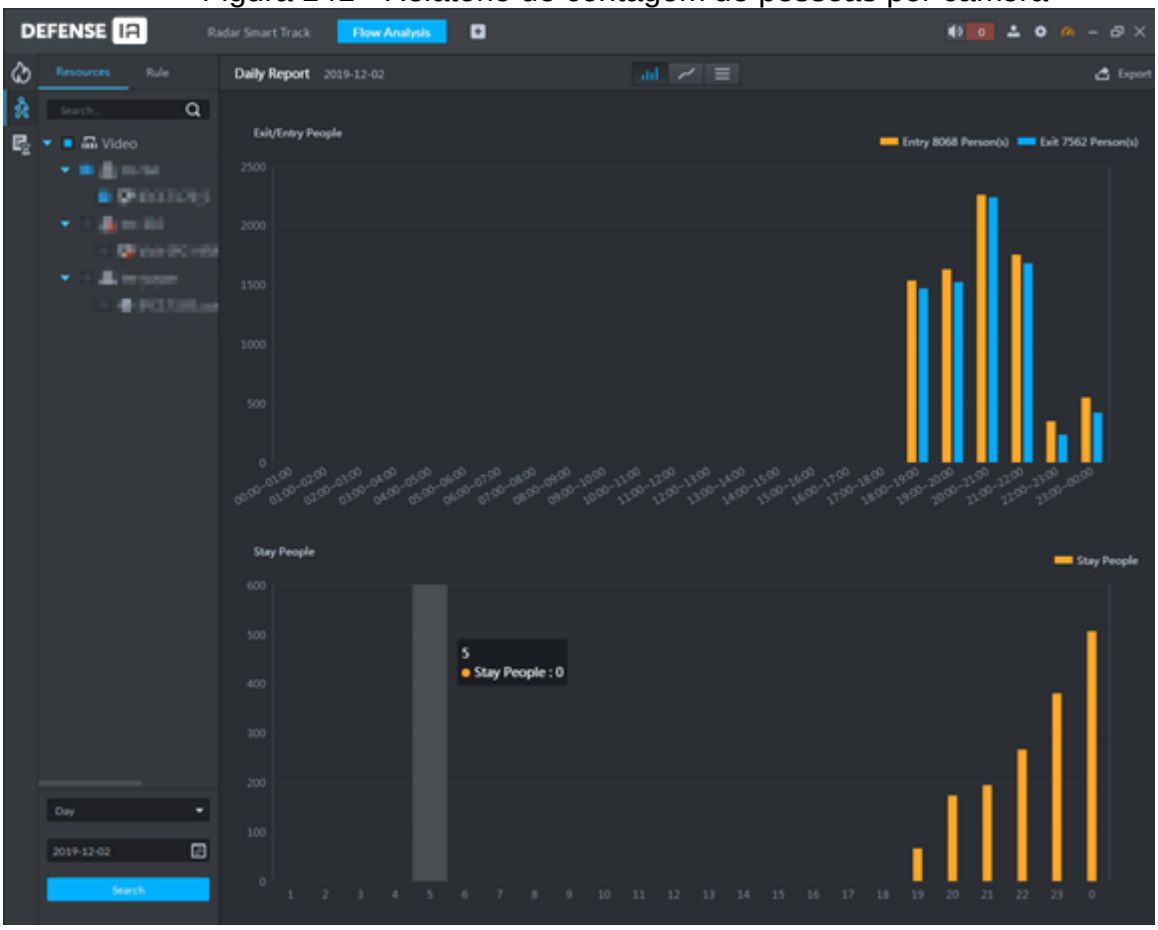
Passo 3. Selecione um canal de contagem de pessoas, defina o tipo de relatório e o tempo de pesquisa e clique em **Pesquisar**. O relatório é exibido.

Para mudar para gráfico de linha ou lista, clique nas guias correspondentes em



- Relatório de Pessoas Remanescentes (número de pessoas ainda em um local) está disponível apenas para o relatório diário.

Figura 141 - Relatório de contagem de pessoas por câmera



Passo 4. Para salvar o relatório, você pode clicar em **Exportar** no canto superior direito. O relatório é exportado no formato .pdf.

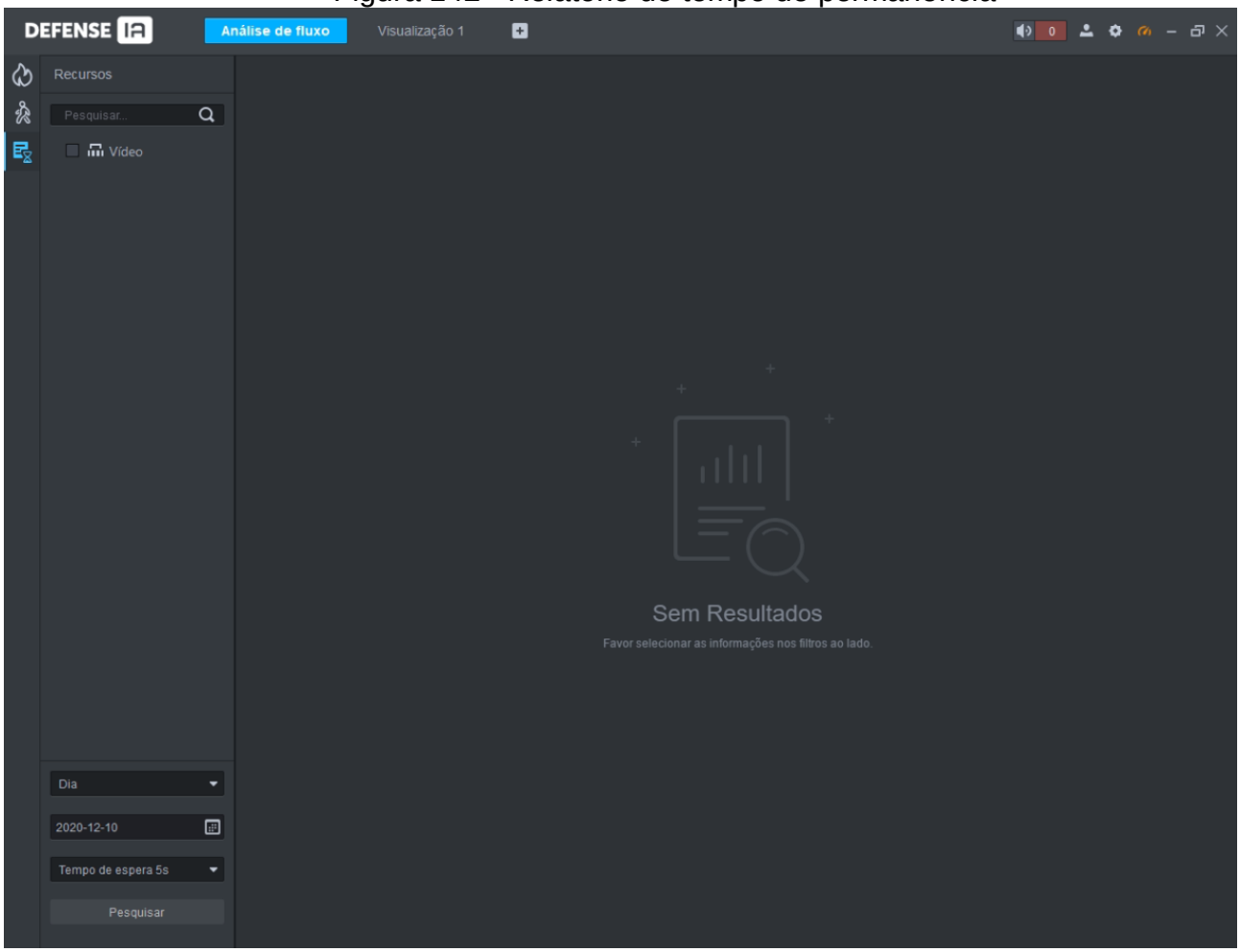
3.4.4.3 Relatório de tempo de espera

Com as câmeras de contagem de pessoas implantadas nas entradas e saídas, o sistema pode calcular a quantidade de pessoas que permaneceram em uma área por um determinado período. Você pode ver o relatório diário, semanal e mensal no Defense IA Client.

Por exemplo, para visualizar o relatório diário do número de pessoas que permaneceram em uma área por 5 segundos, consulte o procedimento a seguir.

Passo 1. Na interface de **Análise de Fluxo**, clique em

Figura 142 - Relatório de tempo de permanência



Passo 2. Selecione as câmeras, selecione o **Dia** na lista suspensa, defina uma data no calendário e selecione **Tempo de espera 5s** na lista suspensa correspondente. Clique em **Pesquisar.**

O relatório é exibido.

Passo 3. (Opcional) Para exportar o relatório, clique em **Exportar.**

3.5 RECONHECIMENTO FACIAL

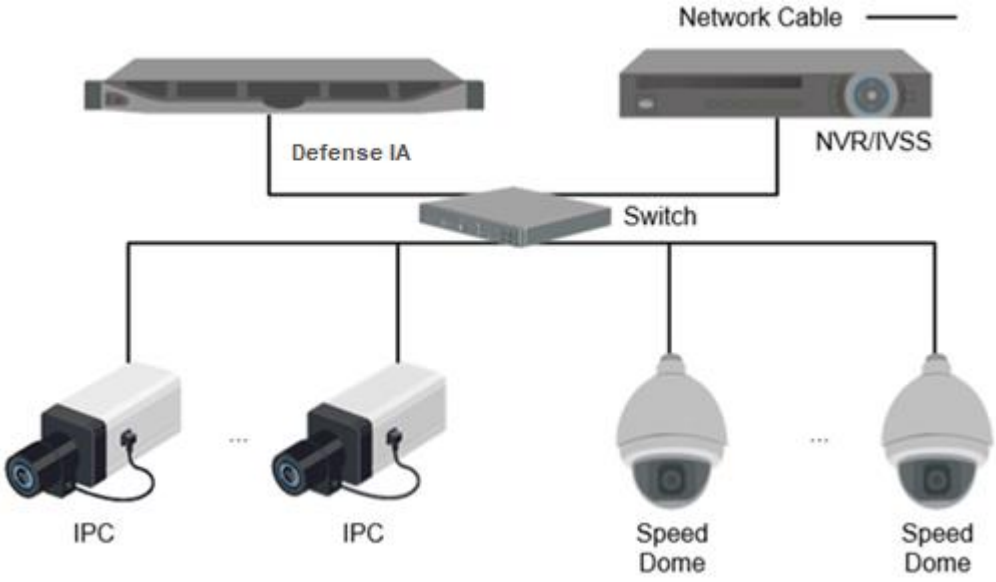
Defina as configurações de reconhecimento facial no dispositivo e na plataforma antes de ver os resultados do reconhecimento facial na plataforma.

3.5.1 Topologia Típica

O recurso de reconhecimento de rosto está disponível em modelos selecionados de câmeras NVR, IVSS e FR.

- Reconhecimento facial por NVR / IVSS

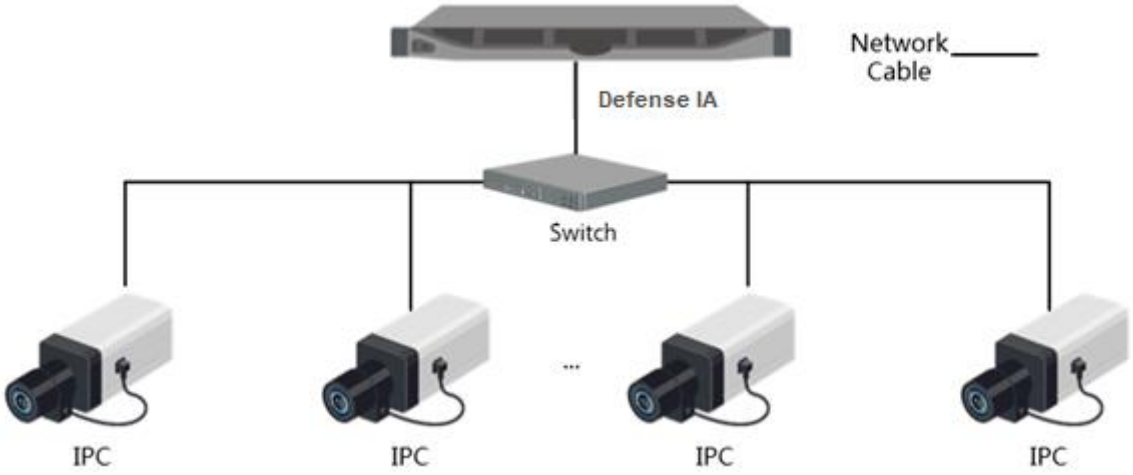
Figura 143 - Topologia típica (NVR / IVSS)



- Câmeras gravam vídeos.
- NVR / IVSS é usado para reconhecimento e armazenamento de rosto.
- O Defense IA gerencia câmeras, NVRs e banco de dados de rosto de maneira centralizada. Também oferece visualização ao vivo e pesquisa de rostos/faces.

Reconhecimento facial pela câmera

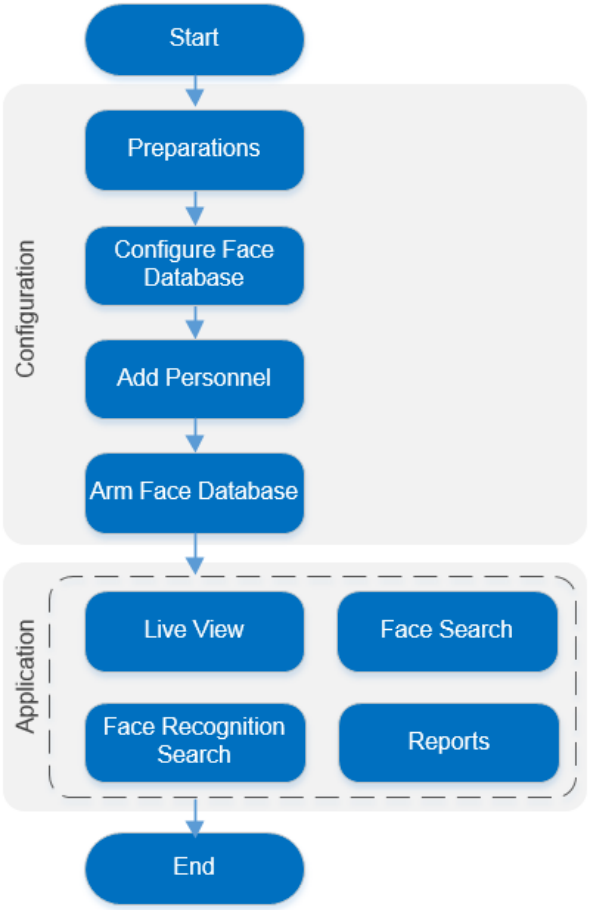
Figura 144 - Topologia típica (câmera)



- As câmeras gravam vídeos de rostos, detectam e então reconhecem rostos.
- O Defense IA gerencia câmeras, NVRs e banco de dados de rosto de maneira centralizada e oferece visualização ao vivo e pesquisa de rosto.

3.5.2 Fluxo de Negócios

Figura 145 - Fluxo de negócios de reconhecimento facial



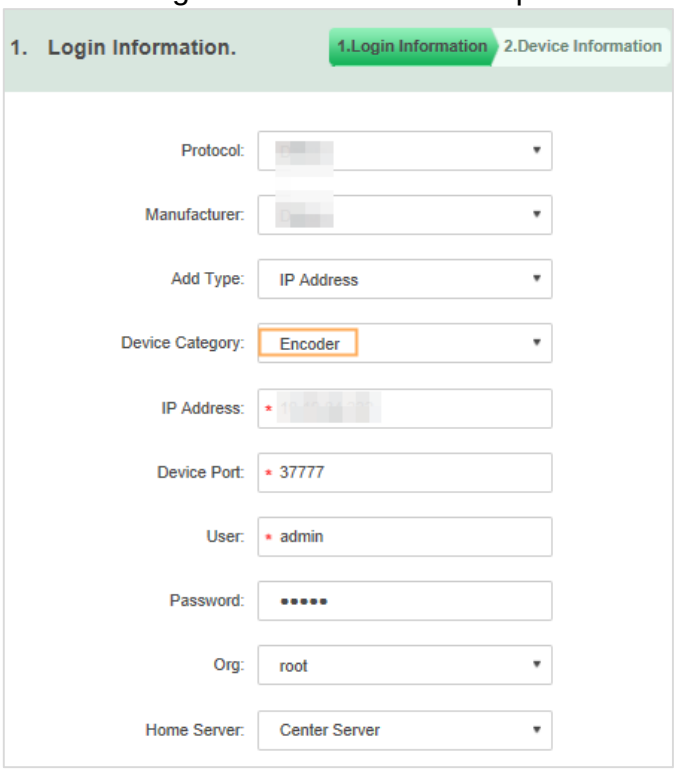
3.5.3 Configurando o reconhecimento facial

3.5.3.1 Preparativos

Certifique-se de que os seguintes preparativos foram feitos:

- Dispositivos de reconhecimento facial estão instalados corretamente. Para obter detalhes, consulte os manuais do usuário correspondentes.
- As configurações básicas da plataforma foram concluídas. Para configurar, consulte "3 Configurações básicas."
- Ao adicionar dispositivos de reconhecimento de face na interface de **Dispositivo** da interface Web do Defense IA, selecione **Encoder** como a categoria de dispositivo.

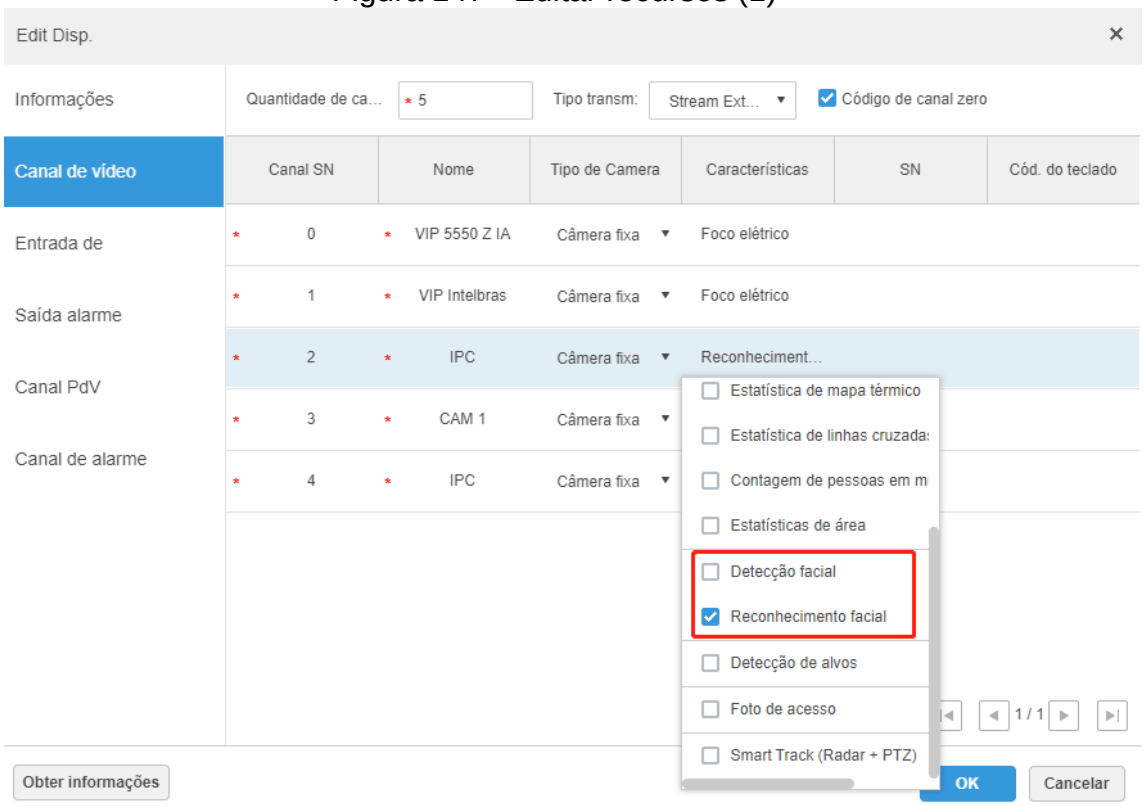
Figura 146 - Adicionar Dispositivo



- Depois de adicionar um NVR ou IVSS de reconhecimento facial, defina os recursos de reconhecimento facial para os canais correspondentes.

Na interface de **Dispositivo**, clique em do NVR ou IVSS e, em seguida, selecione **Reconhecimento facial** como característica.

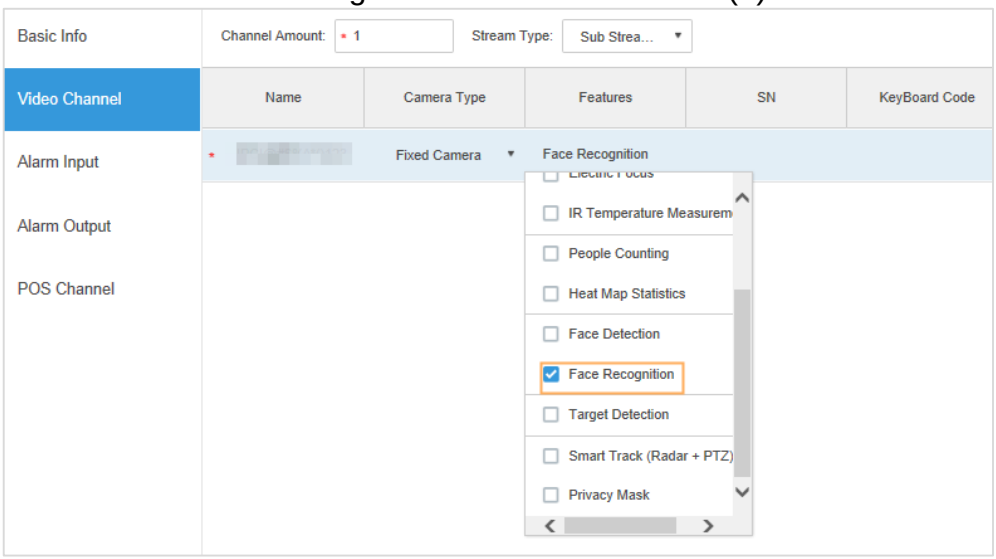
Figura 147 - Editar recursos (1)



- Na interface do **Dispositivo**, clique em da câmera de reconhecimento de rosto ou câmera de detecção de rosto e, em seguida, selecione **Reconhecimento Facial** ou **Detecção Facial** dependendo da tecnologia/característica a ser utilizada.

- A plataforma nem sempre obtém as características da câmera de reconhecimento facial.

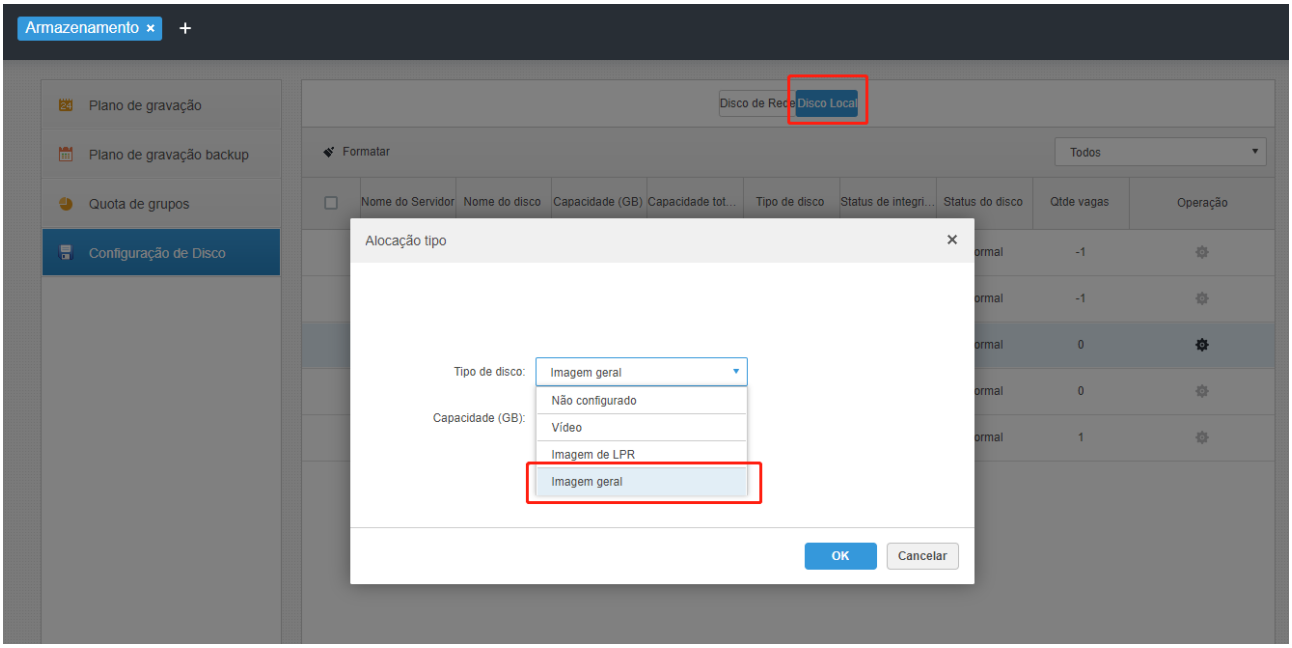
Figura 148 - Editar recursos (2)



- Snapshots Faciais são armazenados no disco de **Imagem Geral**. Na interface de **Configuração de Armazenamento**, configure pelo menos um disco local

para armazenamento de imagens. Caso contrário, a plataforma não exibirá os Snapshots.

Figura 149 - Definir disco de armazenamento de instantâneo de rosto



3.5.3.2 Configurando o Banco de Dados Facial

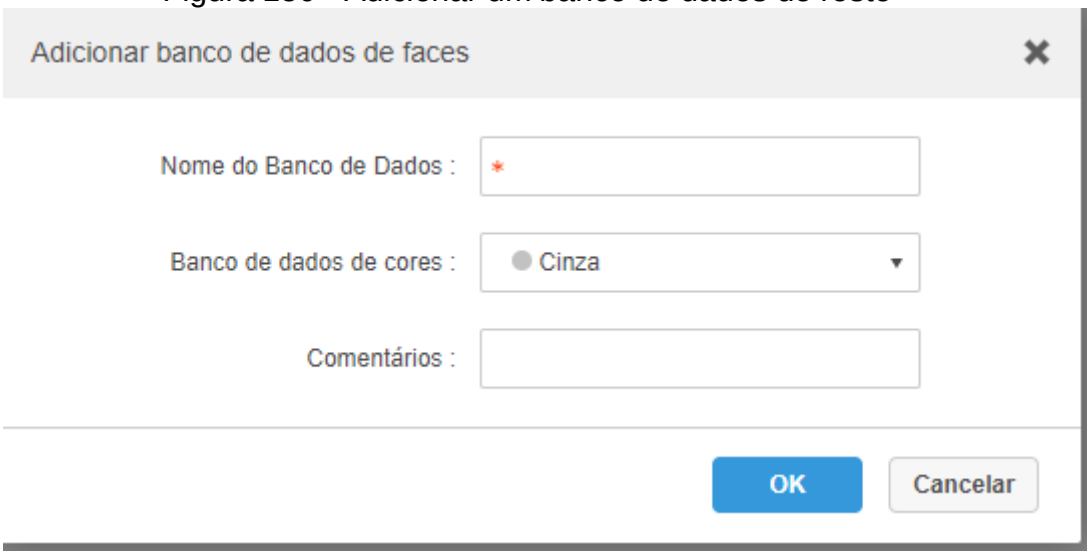
Configure o Banco de Dados Facial que contém informações sobre o rosto das pessoas, para que o sistema possa comparar o rosto detectado com aqueles no banco de dados para determinar quem é a pessoa detectada pelo sistema. A plataforma suporta até 50 bancos de dados faciais.

3.5.3.2.1 Criando Banco de Dados Faciais

Passo 1. Clique + na Interface Web do Defense IA e, em seguida, selecione **Banco de Faces.**

Passo 2. Clique em Adi**cionar.**

Figura 150 - Adicionar um banco de dados de rosto



Passo 3. Insira o nome do banco de dados, selecione uma cor e clique em **OK.**

Outras Operações

- Pesquisa deBanco de dados
  Filtrar o banco de dados por tipo de banco de dados Facial ou palavra-chave.
- Adicionar banco de dados facial

  Clique no para adicionar informações de identificação Facial.
- Modificar database
  Clique no para modificar o nome e a descrição do banco de dados.
- Excluir database
  Clique no .

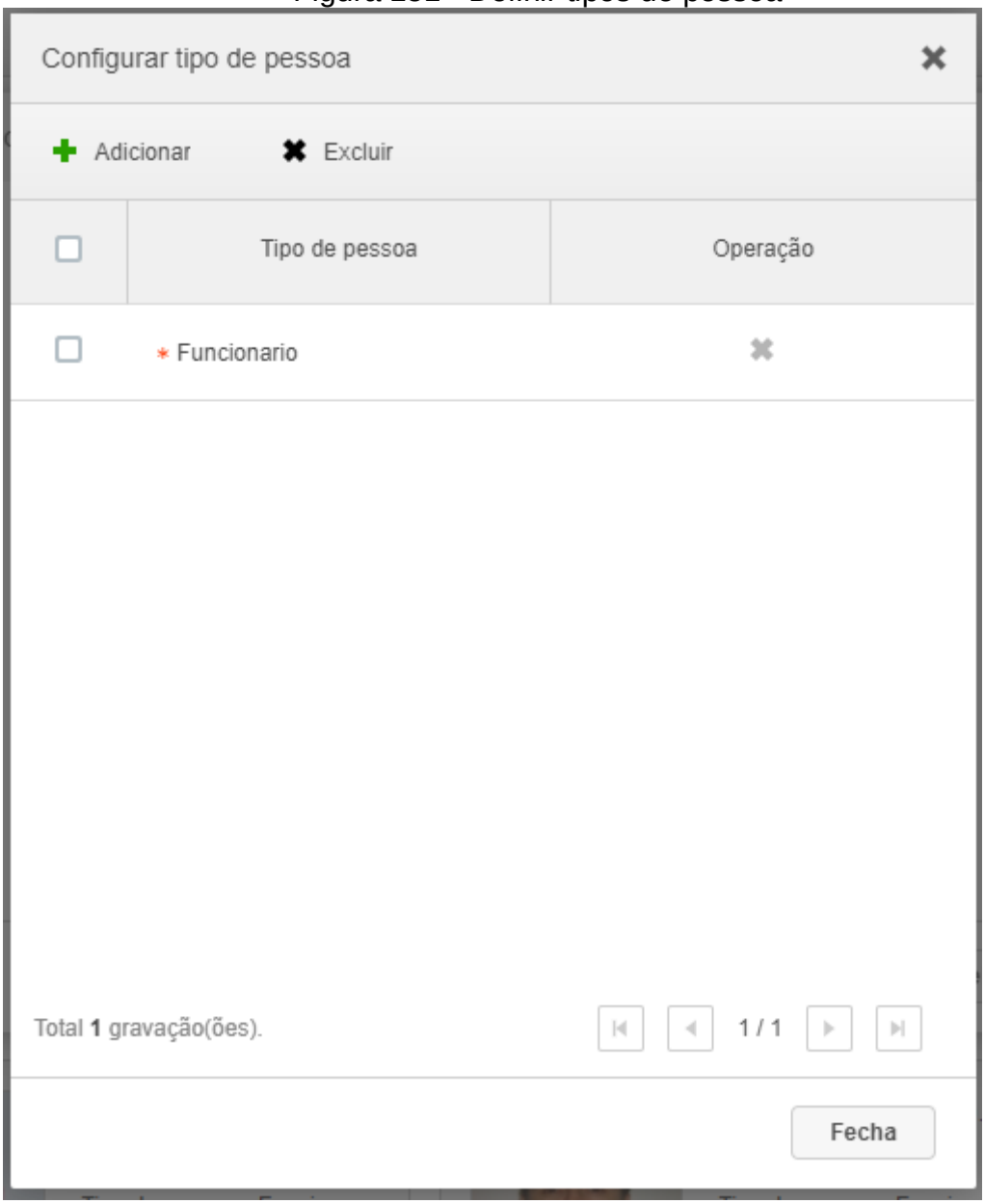
3.5.3.2.2 Configurando o tipo de pessoa

São permitidos até 16 tipos de pessoas. Os alarmes relacionados ao Facial podem ser configurados e acionados por tipo de pessoa.

Passo 1. Clique no banco de dados Facial que precisa ser adicionado o novo cadastro de pessoa.

Passo 2. Clique em Configurar tipo de pessoa

Figura 151 - Definir tipos de pessoa



Passo 3. Clique em **Adicionar** e insira o nome do tipo na coluna **Tipo de pessoa.**
Suporta adicionar até 16 tipos de pessoas.

Passo 4. Clique em ✖ para remover o tipo de pessoa na linha.

3.5.3.2.3 Adicionando informações de banco de dados facial

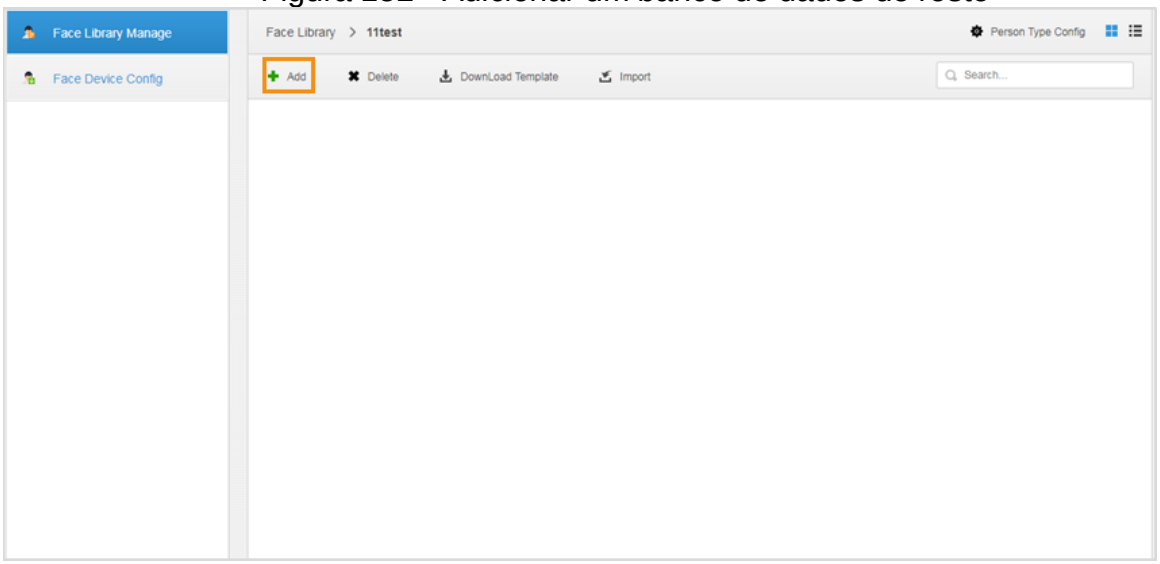
Adicione informações das pessoas uma a uma ou em lotes. O reconhecimento facial é baseado na correspondência entre rosto detectado e rostos no banco de dados. A plataforma suporta até 500 mil faces

Adicionando Informações de Pessoas/Faces de um a um

Passo 1. Insira a as informações de pessoas de duas maneiras:

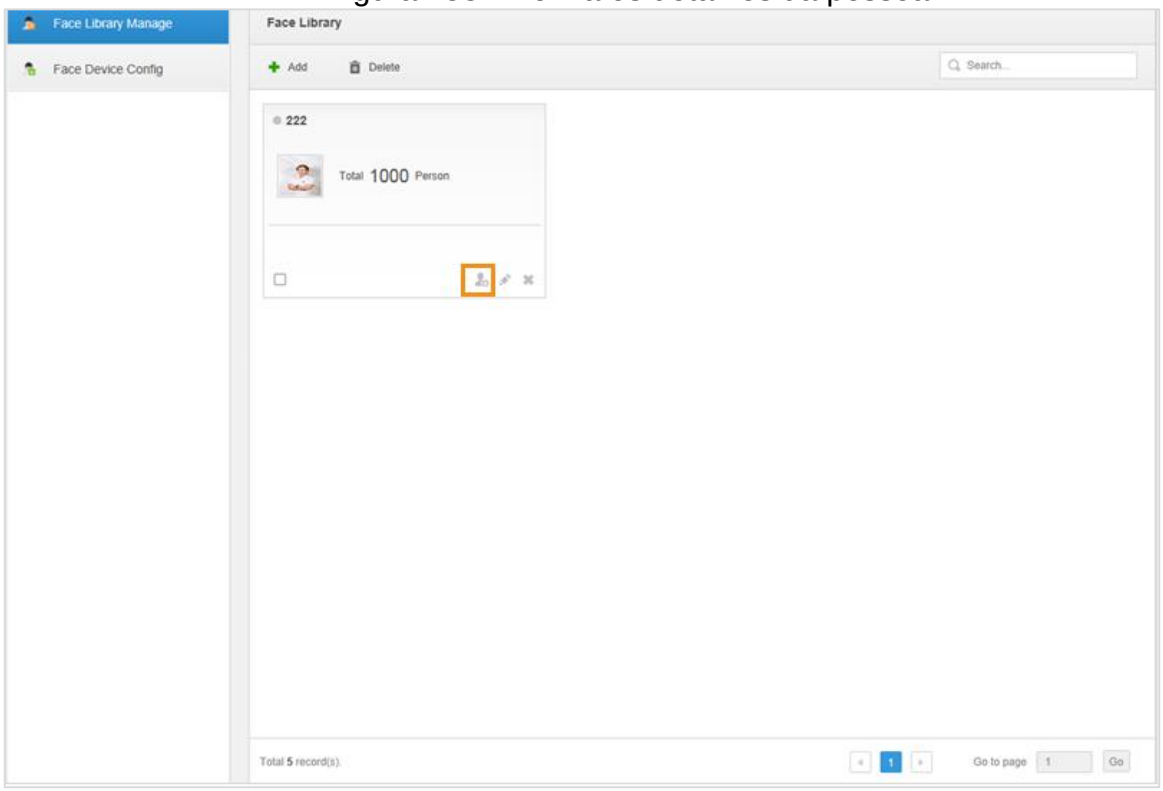
- Clique na base de dados que precisa adicionar pessoas na interface de gerenciamento do Banco de dados Facial.

Figura 152 - Adicionar um banco de dados de rosto



- Clique no cartão pessoal.

Figura 153 - Defina os detalhes da pessoa

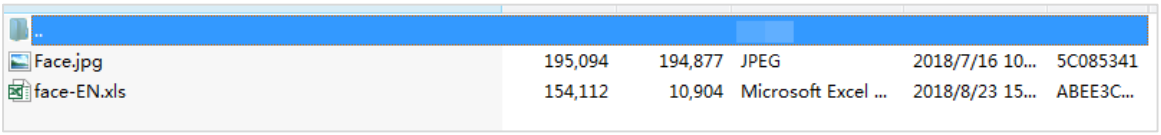


Passo 2. Insira as informações da pessoa.
Passo 3. Clique na foto do perfil e carregue uma foto do rosto.
Passo 4. Clique **OK**.

Adicionando informações de pessoas/faces em lotes

Prepare os registros faciais com antecedência, se você deseja importar em lotes. Compacte os arquivos em zip, rar ou 7z. O ID não pode ser repetido. Atualmente, a importação em lote suporta no máximo 1000 fotos de uma vez.

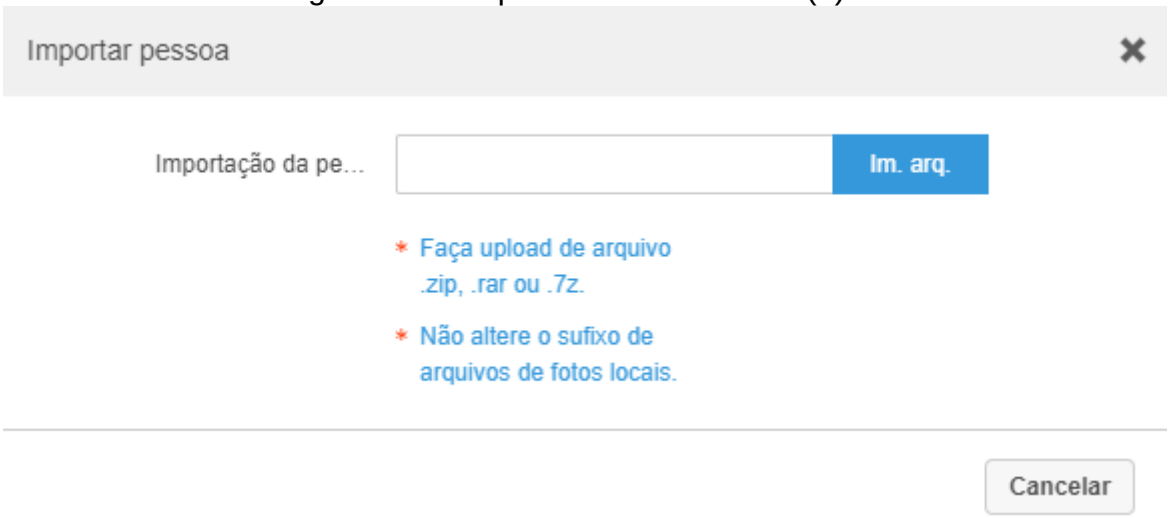
Figura 154 - Arquivo zip



Passo 5. Clique no banco de dados para adicionar pessoas na interface da **Biblioteca de Rostos** Facial (via página web do Defense IA Server).

Passo 6. Clique em **Importar**.

Figura 155 - Importar faces em lotes (1)



Passo 7. Clique em **Importar arquivo** e carregue o pacote compactado de acordo com o prompt.

Operações

- Consulta de Pessoas

  Insira palavras-chave na caixa de texto da consulta e pressione Enter ou clique em .

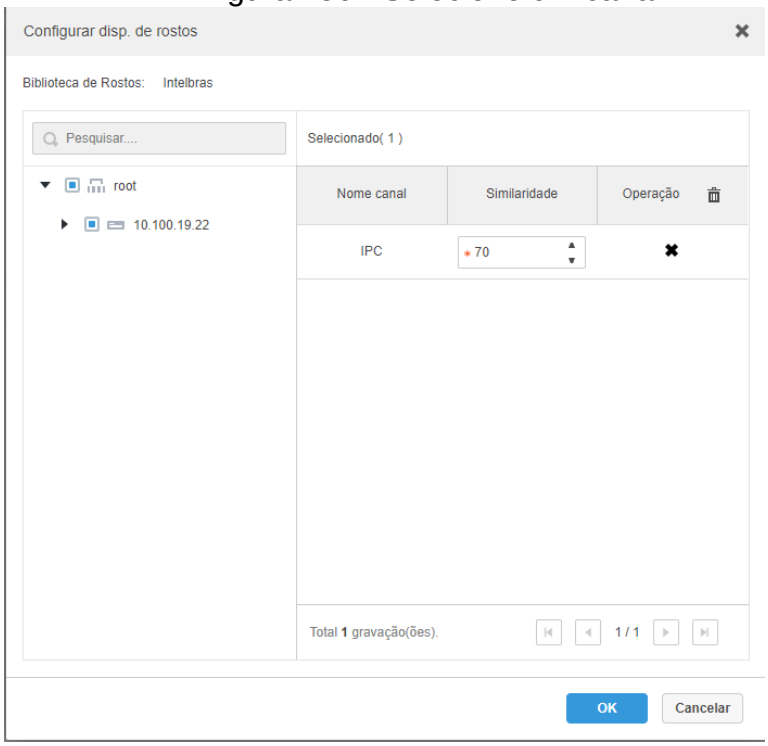
- Excluir pessoa
  - Clique na interface de pessoa e, em seguida, você pode excluir a pessoa individualmente.
  - Selecione múltiplas pessoas, e depois clique em Excluir para excluir a pessoa em lotes.

3.5.3.3 Armando canais de reconhecimento facial

Habilitar reconhecimento facial em tempo real. Para utilizar o banco de pessoas específicas, você pode armar apenas o banco de dados facial dessas pessoas. Os bancos de dados faciais armados são enviados por este menu para os dispositivos que farão o reconhecimento.

Passo 1. Clique e selecione **Banco de Faces** na interface da nova guia.
Passo 2. Clique em **Configurar disp. de rostos** à esquerda da barra de navegação.
Passo 3. Clique em para começar a configuração de envio das faces.

Figura 156 - Selecione um canal



Passo 4. Selecione os canais de destino e defina o nível de similaridade desejado.
Passo 5. Clique em **OK.**

- Se o envio solicitado falhou ou falhou parciamentel, o botão aparecerá no cartão de banco de dados. Envie novamente para garantir o envio de todo o banco.

Operações

- Modificar envio
  Após envio foi realizado; clique em e você poderá modificar o dispositivo relacionado e o valor de similaridade do Banco de Dados enviado.
- Desarmar
  Clique em na interface da página **Configurar disp de rostos** para remover o Banco de dados do dispositivo.

3.5.4 Aplicativos de reconhecimento facial

Veja vídeo de reconhecimento facial ao vivo ou gravados e pesquise por registros de face. Você pode pesquisar registros por atributos de rosto ou simplesmente fazendo o upload de uma imagem de rosto.

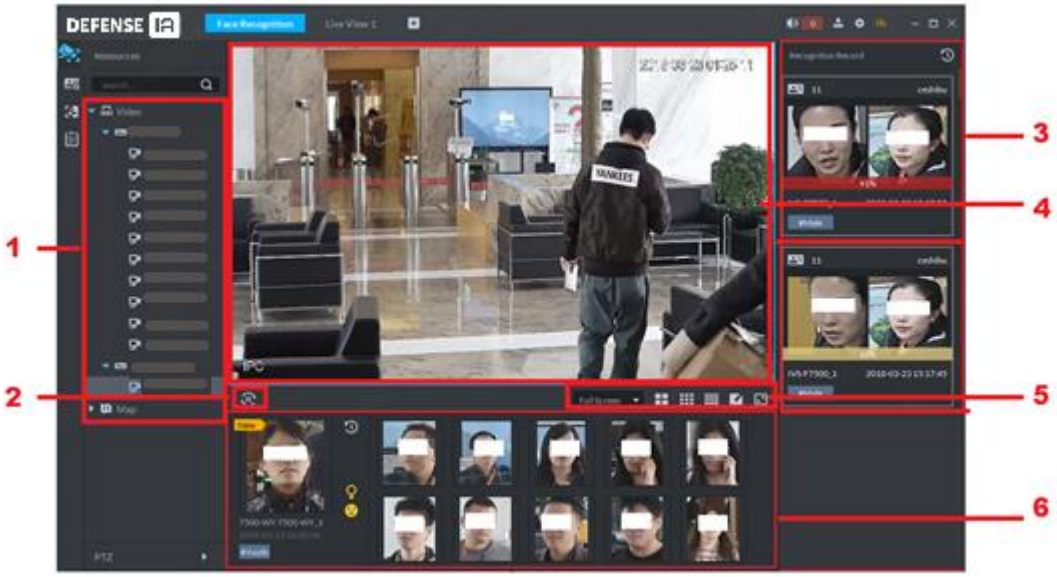
3.5.4.1 Reconhecimento facial em tempo real

Veja o reconhecimento de rosto em tempo real.

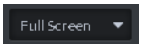
Passo 1. Clique em no Cliente de Controle e selecione **Reconhecimento Facial.**

Passo 2. Clique em .

Figura 157 - Vídeo ao vivo



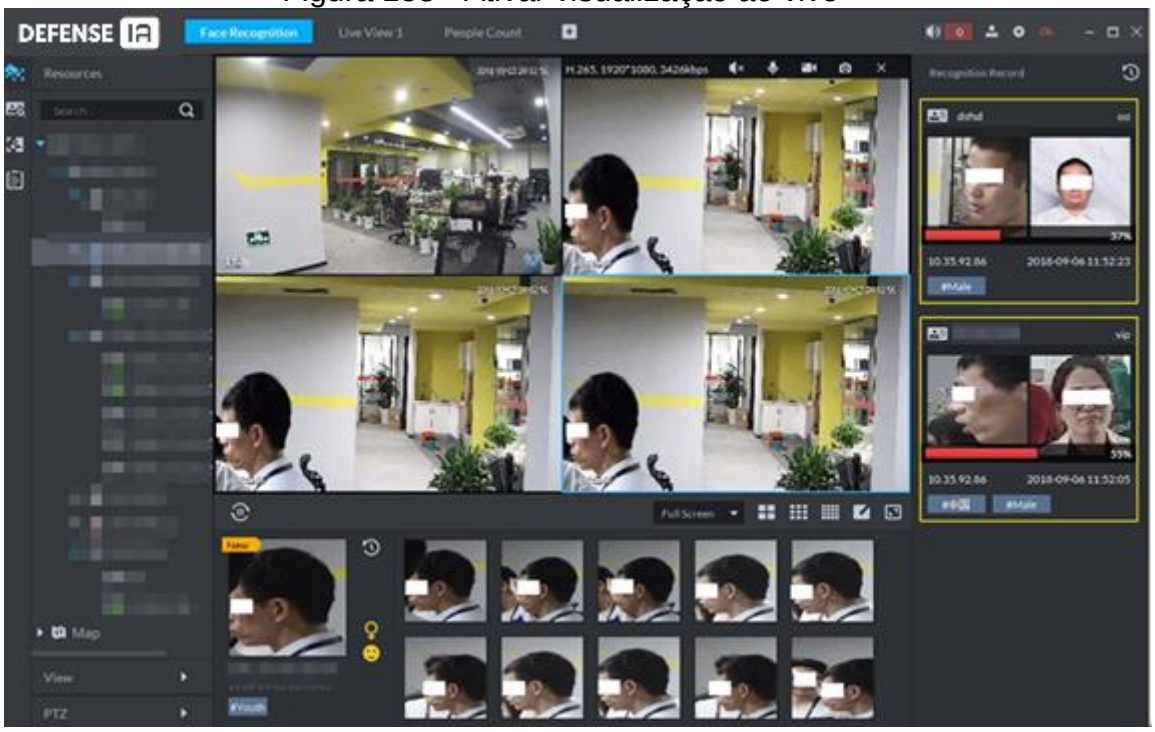
Nº	Nome	Descrição
1	Árvore de Dispositivos	Exibe os dispositivos que possuem as características de detecção de rosto e reconhecimento facial.
2	Pausar / Iniciar	: Quando este ícone está na interface, o painel de exibição de instantâneo não atualiza a imagem com snapshots de rostos humanos. Clique no ícone e o sistema passará a exibir as imagens/snapshots de rostos em tempo real. : Quando este ícone está na interface, o painel de exibição de instantâneo atualiza a imagem com snapshots de rostos humanos. Clique no ícone, e o sistema pausará o exibir as imagens/snapshots de rosto humano.

Nº	Nome		Descrição
3	Registros de reconhecimento facial		Exibe os reconhecimentos faciais obtidos nos canais de vídeo abertos.
4	Janela de Monitoramento		Exibe vídeo de visualização do canal. No modo de exibição de várias janelas, clique duas vezes na janela para alternar para o modo de exibição de 1 janela. Clique duas vezes na janela novamente para restaurar o modo original.
5		Proporção de visualização	Existem dois modos: tela inteira, e escala original. A tela inteira refere-se a uma janela em tela inteira.
		Divisão de Visualização	Exibir quantidade de janela comutada. O sistema oferece suporte a configurações personalizadas.
		Tela Cheia	O sistema exibe a janela em tela inteira.
6	Registro de detecções faciais		Exibe os registros de detecções faciais dos canais de vídeo abertos.

Passo 3. Ative a visualização ao vivo.

- Selecione uma janela de monitoramento, e então clique em um canal ou arquivo de gravação.
- Arraste o canal ou o arquivo de vídeo para a janela de monitoramento.

Figura 158 - Ativar visualização ao vivo



Passo 4. Monitoramento de Faces.

- Clique duas vezes em uma das snapshots / imagens para ver mais detalhes
- Clique com o botão direito na snapshot / imagem de detecção facial, e então você poderá fazer registro de faces, procure por faces, consultar por quais câmeras a pessoa passou na frente e exportar snapshots / imagem.
- Clique com o botão direito nos Registros de reconhecimento, e então você pode consultar mais detalhes do reconhecimento facial, consultar por quais câmeras a pessoa passou e exportar snapshots/instantâneos.

3.5.4.2 Pesquisa Facial

Com a função de reconhecimento facial, você pode pesquisar faces adicionadas nos bancos de dados faciais ou pesquisar nos registros de snapshots faciais, definindo características da pessoa, como idade e sexo, ou fazendo o upload de uma foto de rosto. O banco de dados de face contém todos os rostos registrados; os registros de snapshots contêm todos os rostos capturados pelas câmeras.

- A pesquisa por imagem está disponível apenas com IVSS e alguns NVR's.

Passo 1. Clique em no Cliente do Defense IA e selecione **Reconhecimento Facial.**

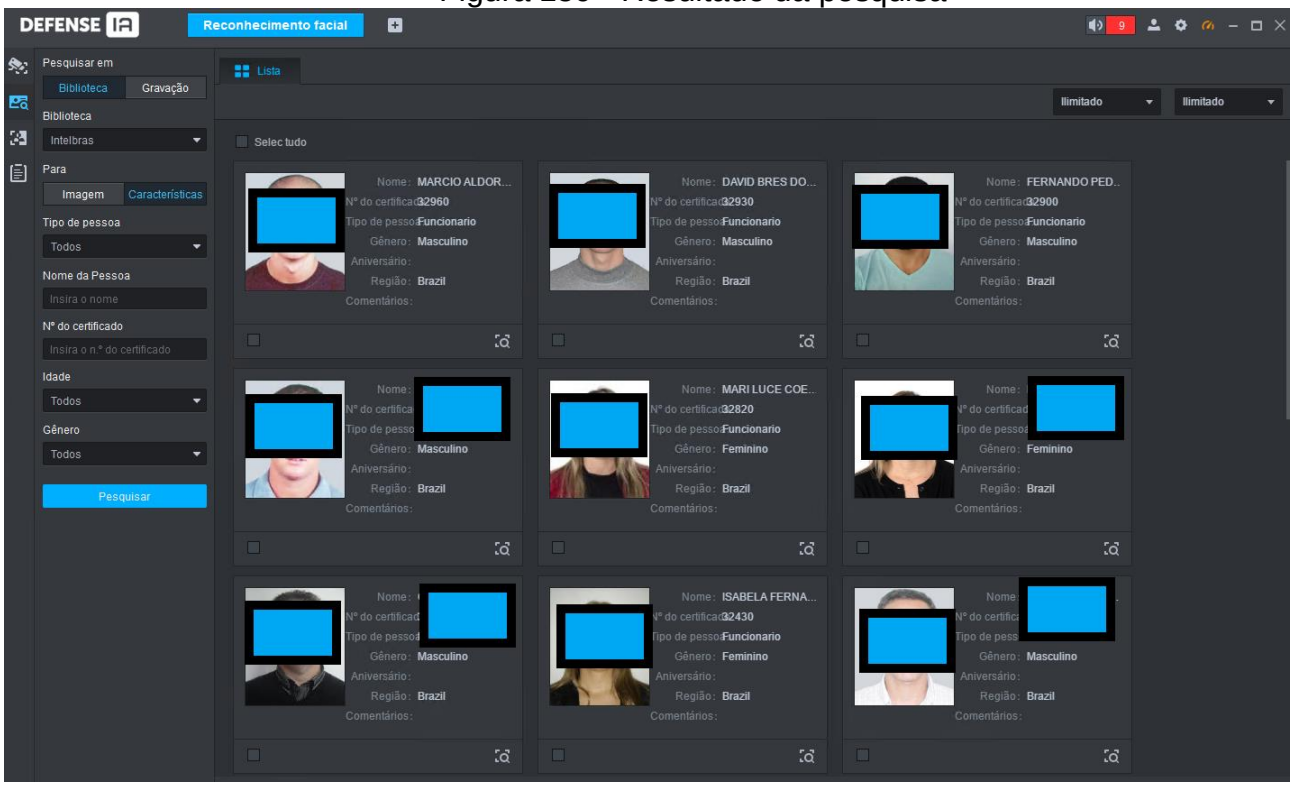
Passo 2. Clique em .

Passo 3. Defina as condições de pesquisa.

- Você pode pesquisar no banco de dados facial (selecionando a opção **Biblioteca** e clicando em **Pesquisar**) ou registros de snapshots faciais (selecionando a opção **Gravação** e clicando em **Pesquisar**).
- Você pode enviar uma fote do rosto para fazer uma pesquisa no banco de dados, também pode-se definir níveis de similaridade a ponto de restringir os resultados com maior similiradade facial.
- Quando você pesquisa por Gravações ou Imagens, você pode selecionar **Iniciar do horário mais atual** ou **Iniciar do horário mais cedo** na lista suspensa Sequência para definir a sequência de tempo para os resultados. Podem ser exibidos até 1000 resultados.

Passo 4. Clique em Pesquisar.

Figura 159 - Resultado da pesquisa



Ao pesquisar um banco de dados facial, os resultados são exibidos em lista; ao pesquisar os registros snapshots faciais, você pode escolher exibir os resultados em uma lista. Para apresentar os resultados da pesquisa, agora tomamos a pesquisa por gravações como exemplo.

- Ao pesquisar por gravações carregando uma foto de rosto, o andamento da pesquisa é exibido no canto superior direito. Para encerrar a pesquisa, clique em .
- Clique em **Lista** e os resultados da pesquisa são exibidos na lista.

Figura 160 - Resultados da pesquisa na lista

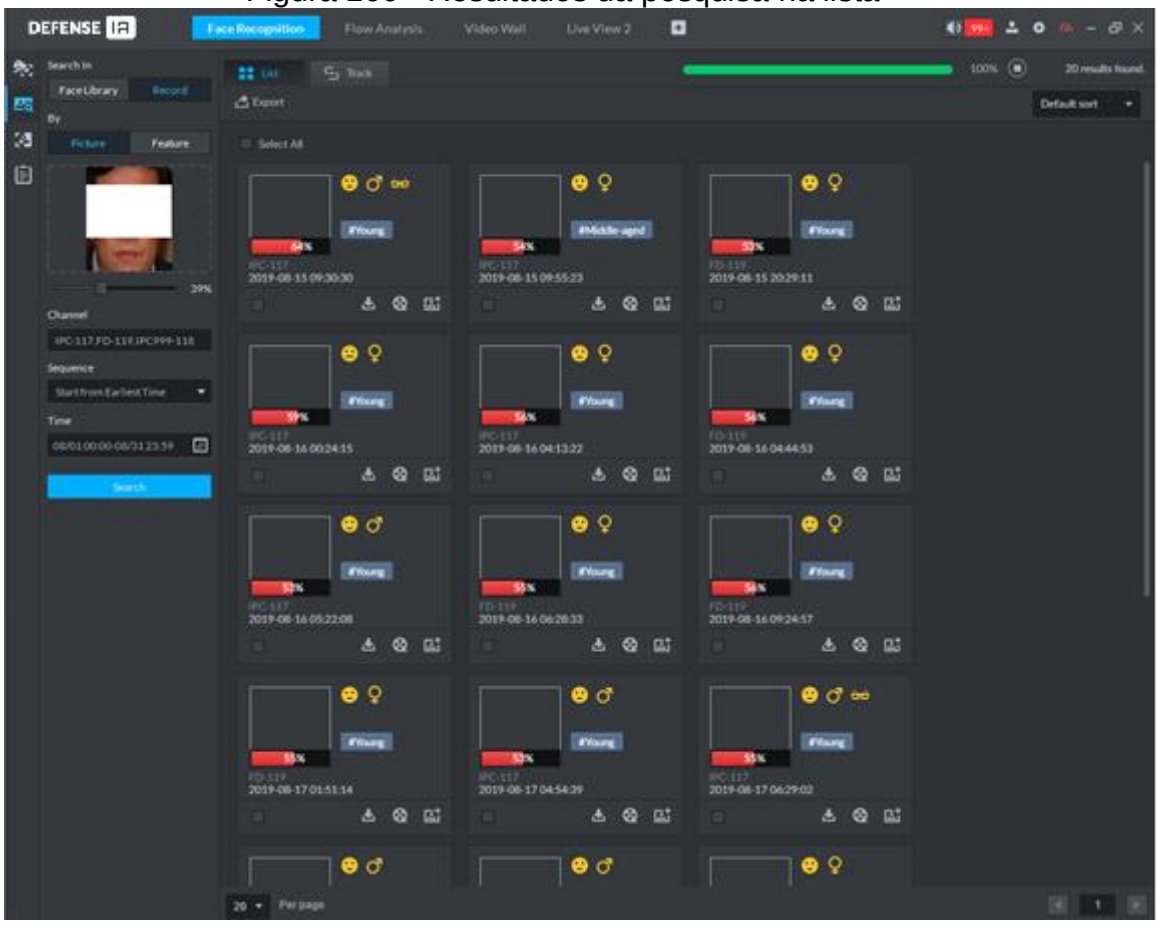


Tabela 25 - Descrição de funções

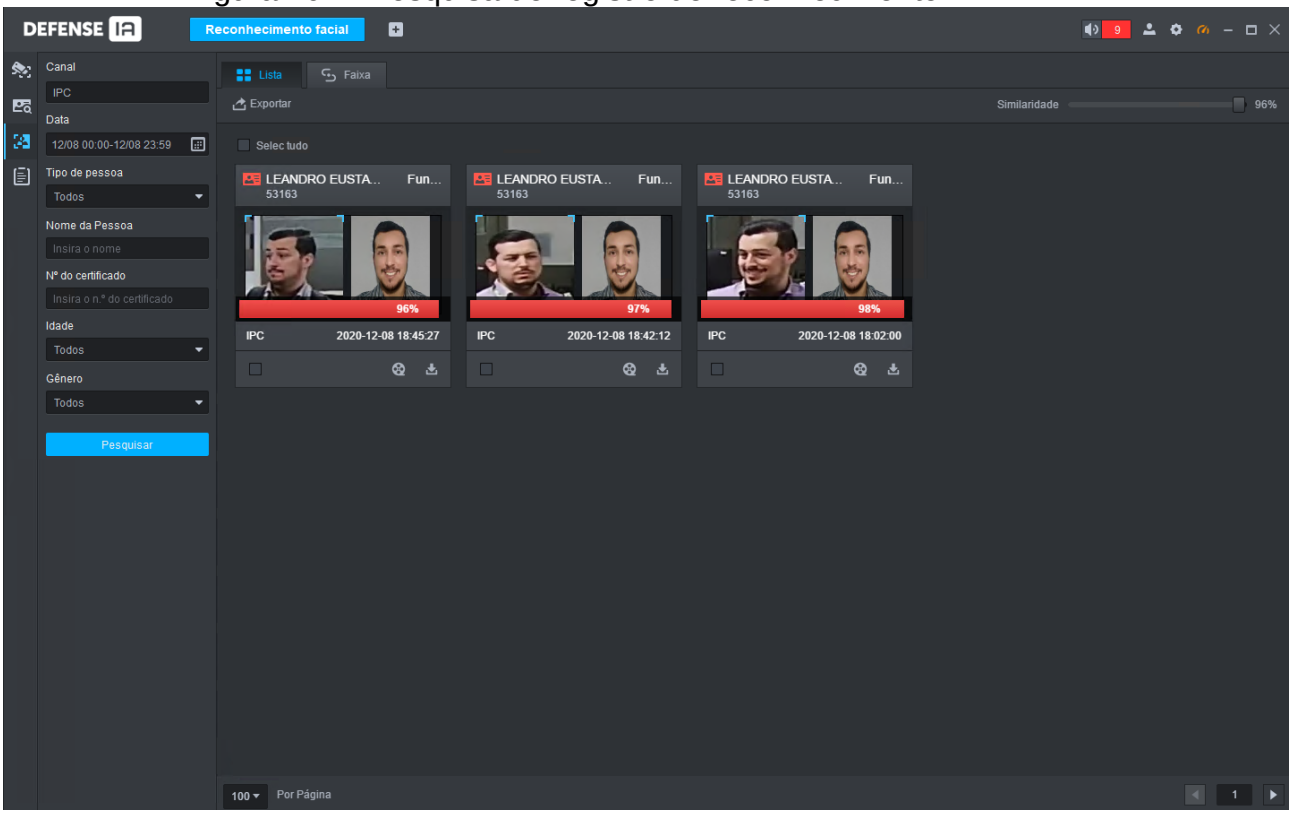
Ação	Descrição
Download de Gravações	Clique para salvar o arquivo rar no caminho especificado. O arquivo .rar contém as imagens /snapshots de rosto humano e imagens de contexto.
Registro de reprodução	Clique para reproduzir a gravação de vídeo de 15 segundos antes e depois do instantâneo.
Adicionar pessoa	1. Adicione a pessoa do snapshot ao banco de dados. 2. Clique . 3. Defina as informações da pessoa e clique em OK.
Pesquisa de Gravações	Você pode fazer upload de uma imagem de rosto para pesquisar nas gravações. 1. Clique , e então o sistema vai para a interface de pesquisa de rosto humano com a snapshot. 2. Clique em Pesquisar. Os resultados da pesquisa são exibidos.

3.5.4.3 Pesquisa de registro de reconhecimento facial

Pesquise rostos reconhecidos por hora, dispositivo, tipo de pessoa, nome, sexo, idade e número do certificado. Você pode ver os resultados da pesquisa em uma lista.

Passo 1. Na interface de **Reconhecimento Facial**, clique em .

Figura 161 - Pesquisa de registro de reconhecimento



Passo 2. Defina os critérios de pesquisa.

Você pode pesquisar por hora, dispositivo, tipo de pessoa, nome, sexo, idade e número do certificado.

Passo 3. Clique em Pesquisar.

Suporta a visualização de registros em lista.

- Clique em Lista e os registros são exibidos na lista. Clique duas vezes em um resultado da pesquisa e as informações detalhadas serão exibidas. Não haverá imagem à esquerda se você não fizer upload da imagem ao definir os critérios de pesquisa.

Figura 162 - Registros na lista

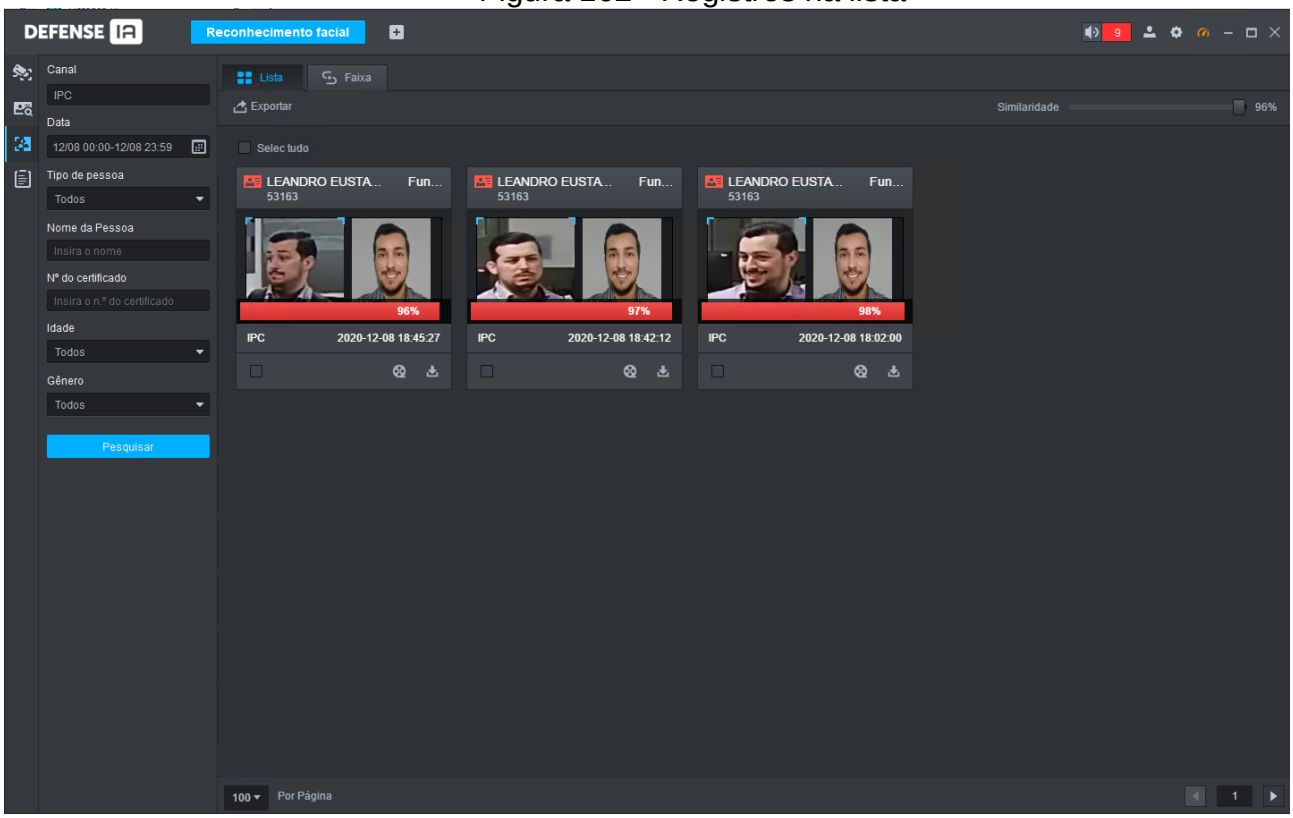


Figura 163 - Detalhes do registro

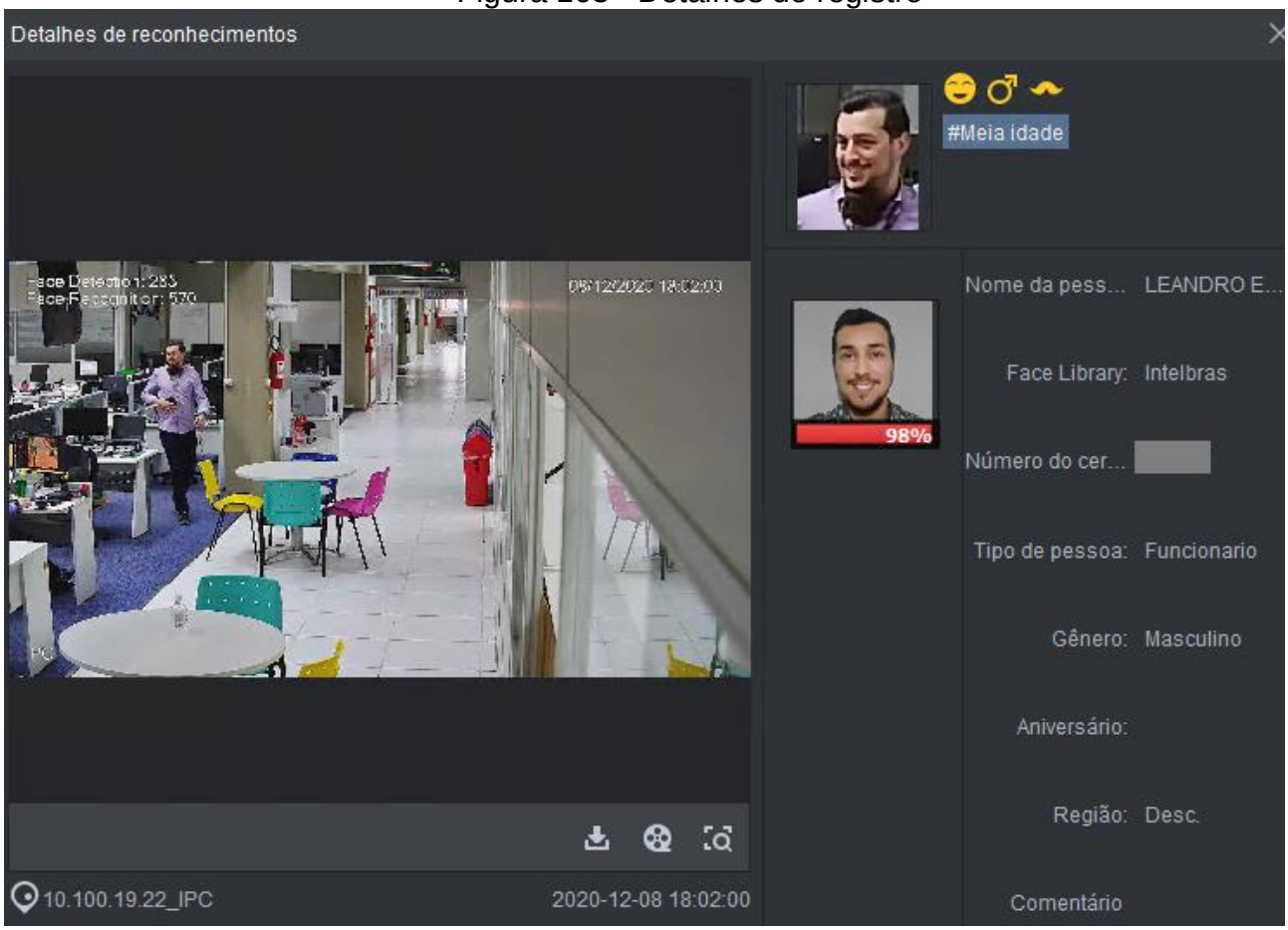


Figura 164 - Descrição de funções

Ação	Descrição
Baixar Gravação	Clique em para baixar o vídeo.
Reprodução de Gravação	Clique em para reproduzir as gravações de vídeo de 10 segundos antes e depois do evento.
Pesquisa de Registros	Clique para pesquisar outros registros relacionados a mesma pessoa.

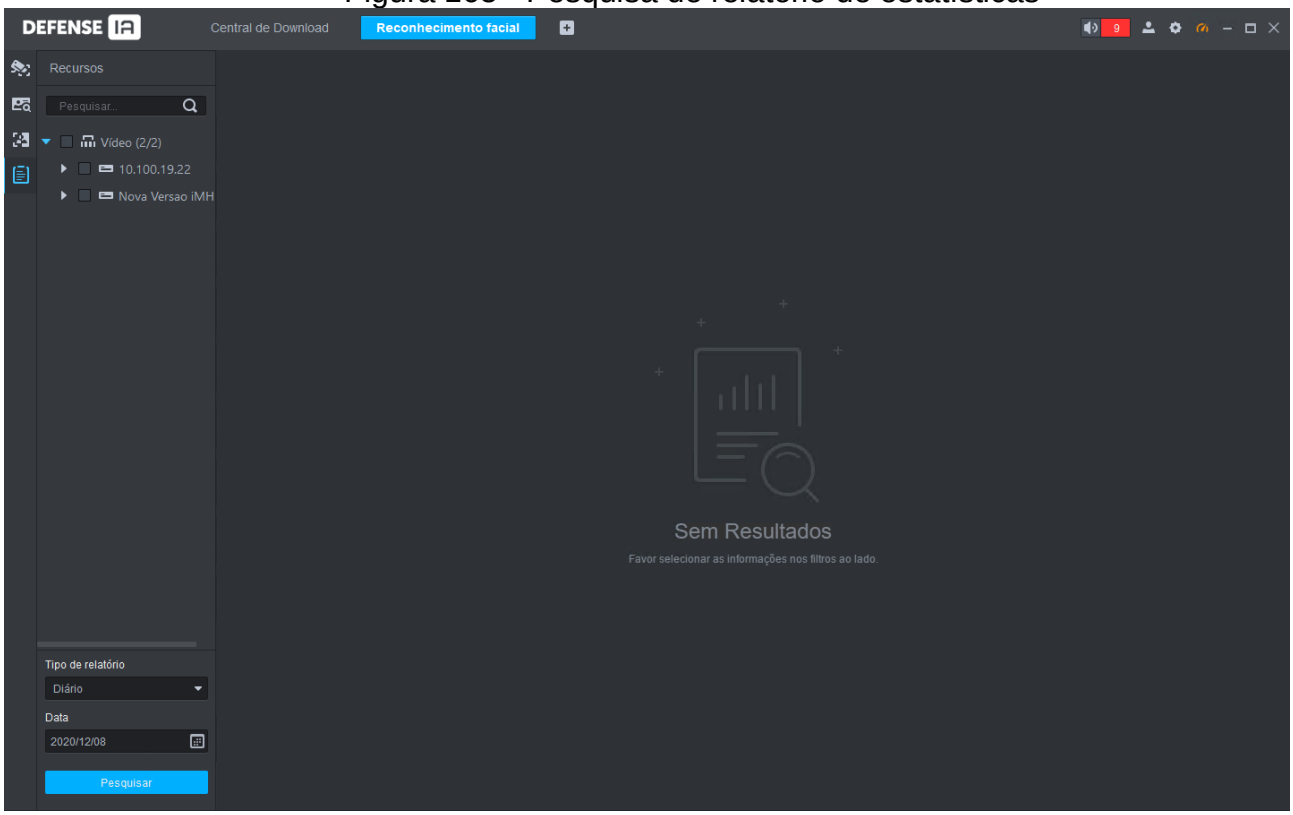
3.5.4.4 Relatórios Faciais

Visualize relatórios de rosto que mostram estatísticas de rosto envolvendo idade, sexo e outras propriedades.

Passo 1. Clique no Cliente do Defense IA e selecione **Reconhecimento Facial**.

Passo 2. Na interface de **Reconhecimento Facial**, clique em .

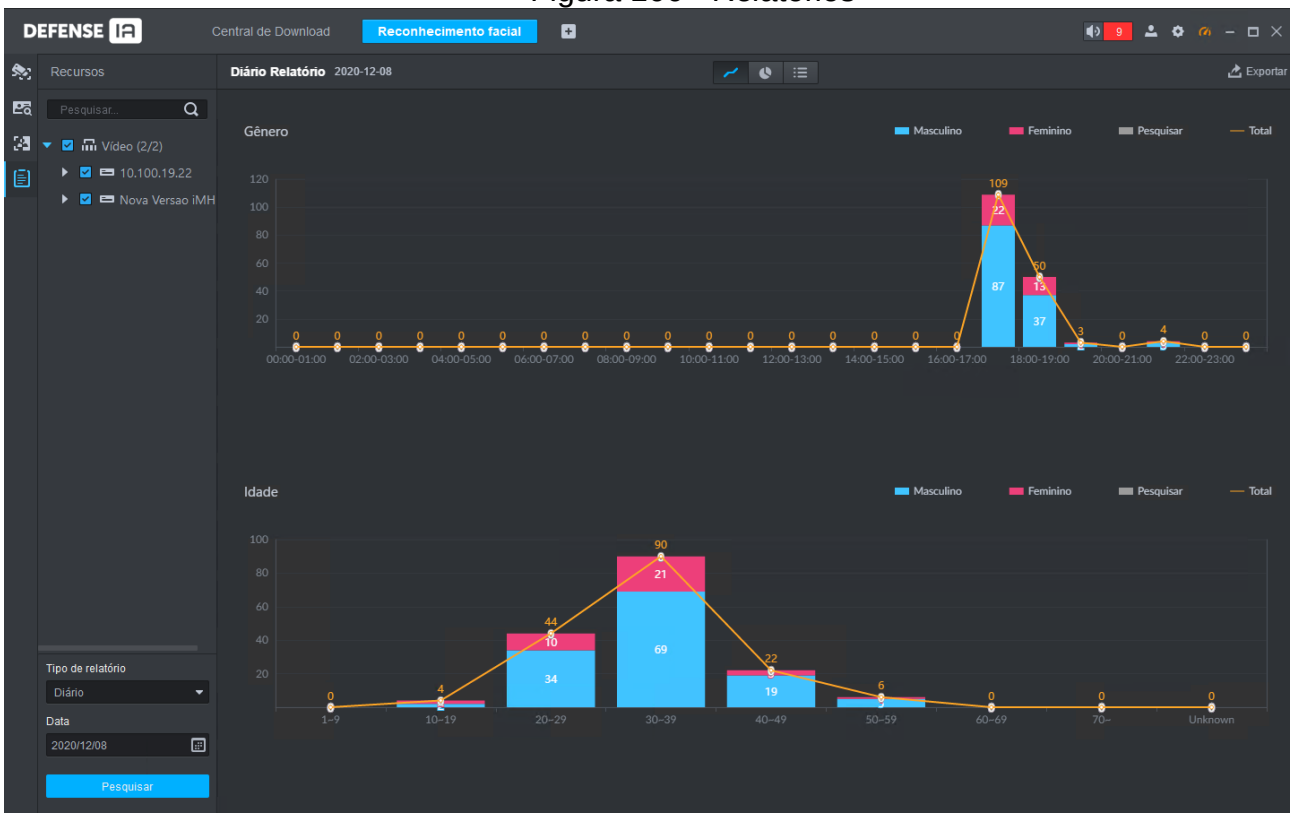
Figura 165 - Pesquisa de relatório de estatísticas



Passo 3. Defina os critérios de pesquisa.
Defina o canal do vídeo, tipo de relatório e tempo.

Passo 4. Clique em Pesquisar.

Figura 166 - Relatórios



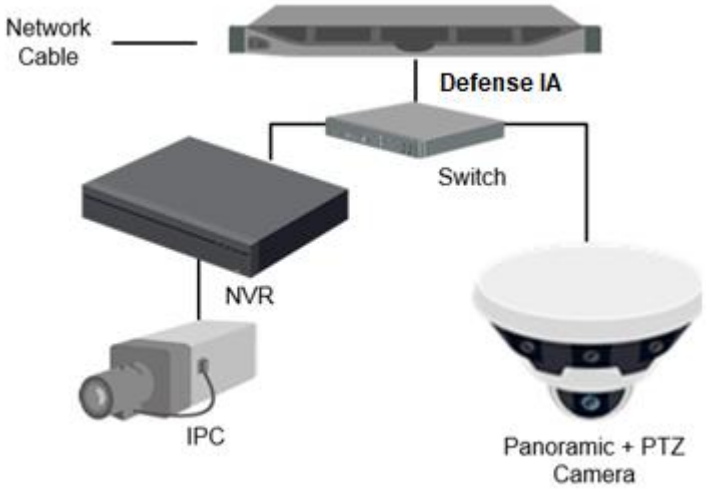
- Resultados serão exibidos por gráfico de linha por padrão.
- Clique para exibir por gráfico de pizza.
- Clique para exibir por lista.
- Clique em Exportar para exportar o resultado das estatísticas no formato .pdf.

3.6 ANÁLISE FORENSE

Visualize e pesquise metadados de pessoas e veículos.

3.6.1 Topologia Típica

Figura 167 - Topologia típica



- Câmeras gerais gravam vídeos.
- Câmeras de metadados de vídeo, como câmera panorâmica + PTZ, gravam vídeos e analisam pessoas, veículos e veículos não motorizados.
- Os NVRs gerenciam câmeras e analisam pessoas, veículos e veículos não motorizados.
- A plataforma gerencia centralmente NVRs e câmeras, recebe os resultados da análise das câmeras e mostra os relatórios.

- A detecção do alvo pode ser feita por câmeras de metadados de vídeo ou NVRs inteligentes.

3.6.2 Fluxo de Negócios

Figura 168 - Fluxo de negócios de detecção de alvos

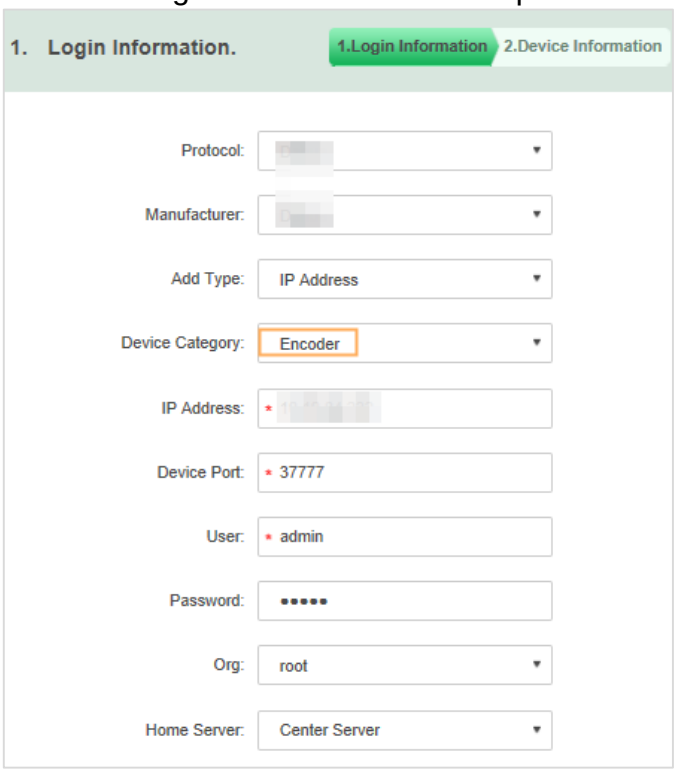
3.6.3 Aplicação de Análise Forense

3.6.3.1 Preparativos

Certifique-se de que os seguintes preparativos foram feitos:

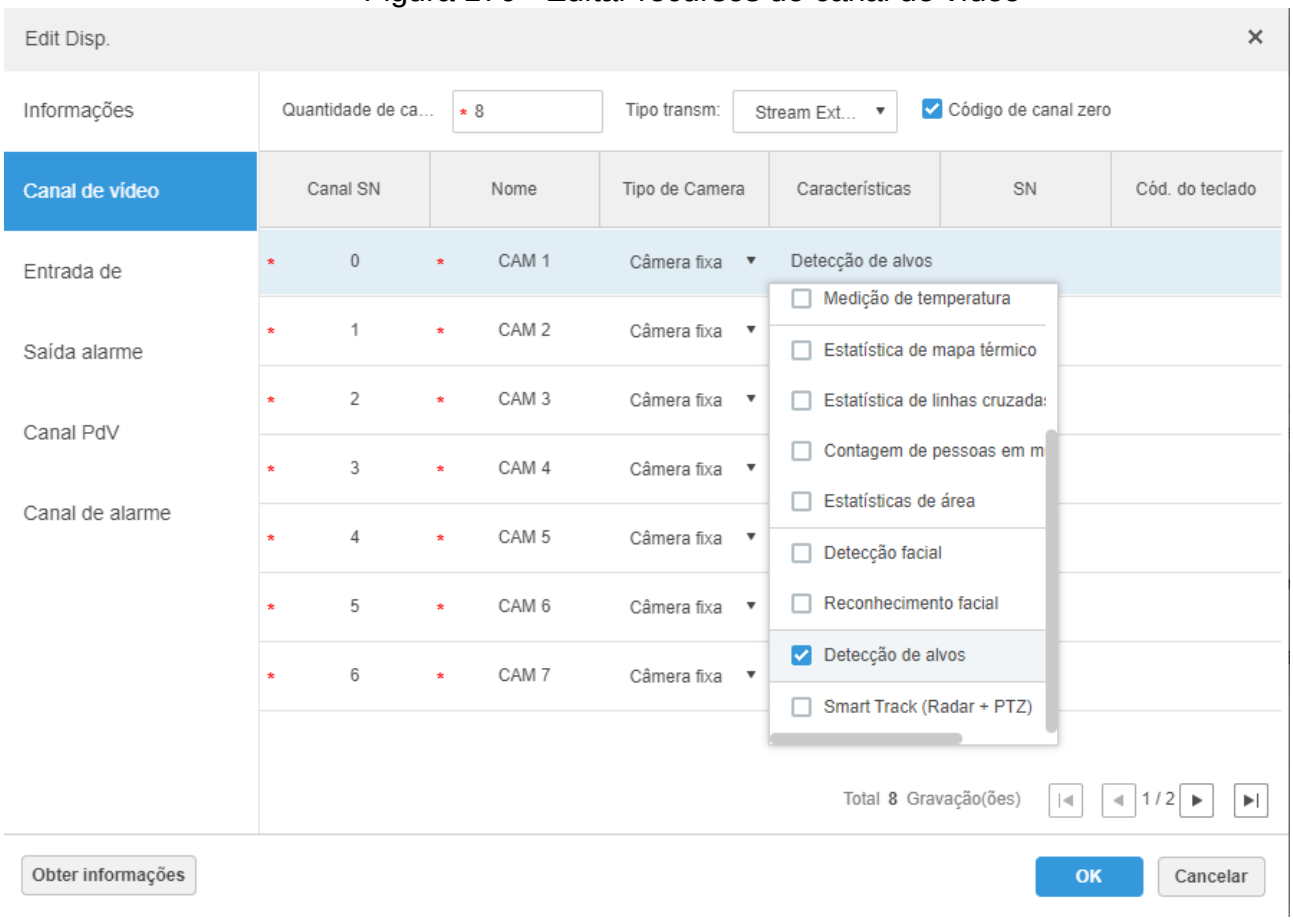
- Câmeras e NVRs estão instalados corretamente e os metadados de vídeo estão ativados neles. Para obter detalhes, consulte os manuais do usuário correspondentes.
- As configurações básicas da plataforma foram concluídas. Para configurar, consulte "3 Configurações básicas."
  - Ao adicionar uma câmera ou NVR na interface do dispositivo do Web Manager, selecione Codificador para a categoria de dispositivo.

Figura 169 - Adicionar Dispositivo



  - Na interface do **Dispositivo**, clique em ou da câmera ou NVR e, em seguida, selecione **Detecção de alvos** para recursos.

Figura 170 - Editar recursos do canal de vídeo



3.6.3.2 Visualização da detecção em tempo real

Para visualizar os snapshots em tempo real capturados pelas câmeras, incluindo informações sobre humanos, veículos e veículos não motorizados:

Passo 1. Faça login no Client do Defense IA e clique em  e selecione Análise Forense.

Passo 2. Clique em  .

A interface de detecção em tempo real é exibida.

Figura 171 - Interface de detecção em tempo real

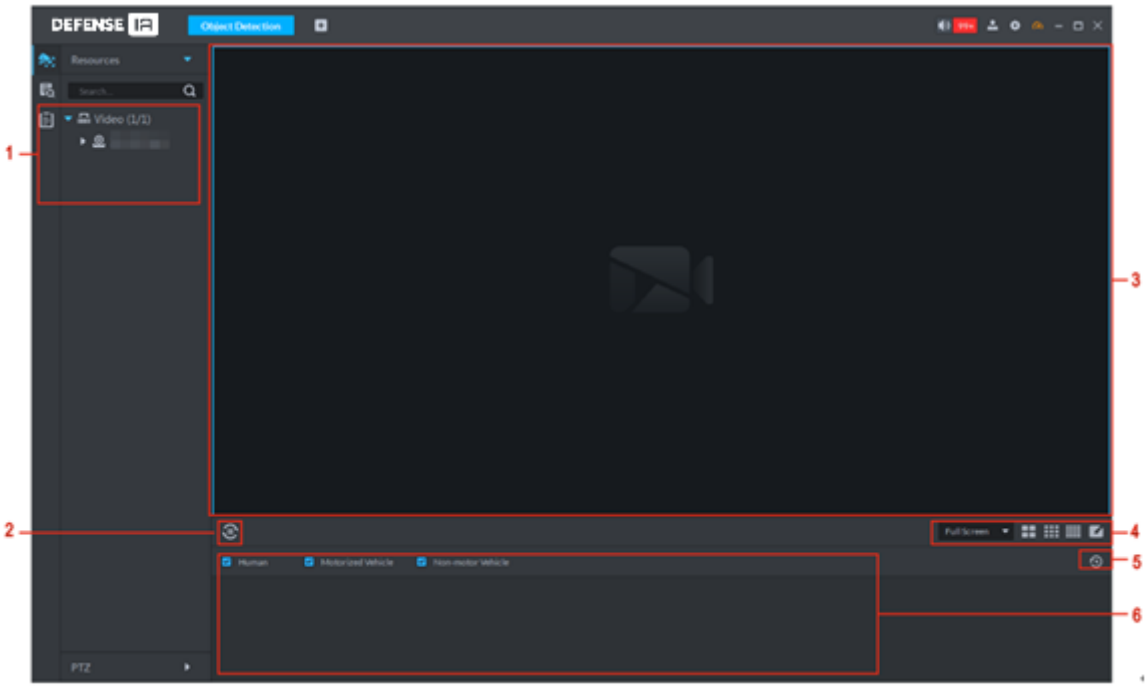


Tabela 26 - Descrição

N°	Nome		Descrição
1	Árvore de Dispositivos		Exibe informações do dispositivo.
2	Pausar atualização / Iniciar atualização		• Se a interface exibir  , a área de exibição de fotos não atualiza as snapshots. Clique neste ícone para atualizar os instantâneos do rosto em tempo real. • Se a interface exibir  , a área de exibição de fotos atualiza os snapshots. Clique neste ícone para parar de atualizar/receber snapshots.
3	Janela de monitoramento		Exibe vídeo de visualização do canal. No modo de exibição de várias janelas, clique duas vezes na janela para alternar para o modo de exibição de 1 janela. Clique duas vezes na janela novamente para restaurar o modo original.
4		Proporção de exibição da imagem	Existem dois modos: tela inteira, e escala original. A tela inteira refere-se a uma janela em tela inteira.
		Número de janelas	Exibir quantidade de janela comutada. O sistema oferece suporte a configurações personalizadas.

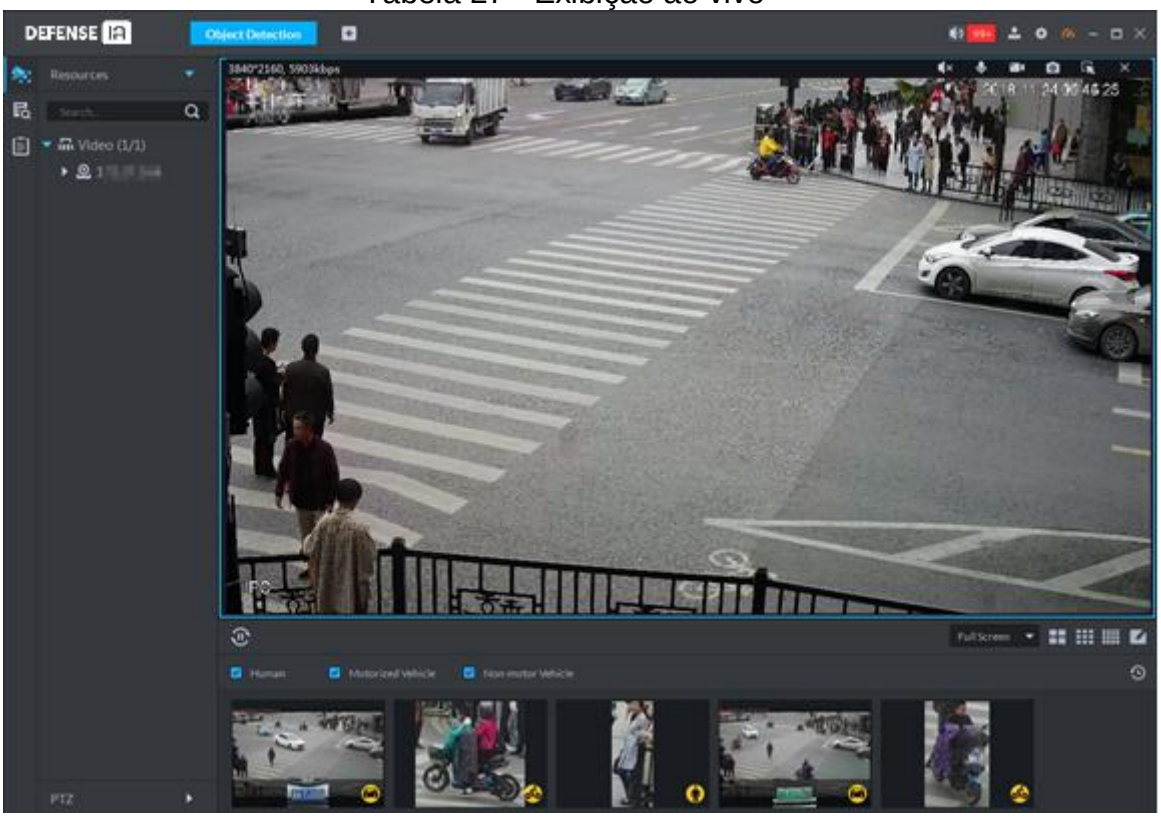
N°	Nome	Descrição
5	O botão permite pular para a interface de estatísticas do relatório.	Clique neste ícone para ir para a interface de estatísticas de relatório.
6	Área de exibição de fotos	Exibe os snapshots de veículos/pessoas capturadas.

Passo 3. Ative a exibição ao vivo.

- Selecione a janela de monitoramento (um quadro branco significa que a janela foi selecionada) e clique duas vezes em qualquer canal ou gravação de vídeo para habilitar o monitoramento em tempo real.
- Arraste o canal ou a gravação de vídeo para a janela de monitoramento.

Passo 4. Ligue a tela de exibição ao vivo. O Defense Client exibe snapshots em tempo real.

Tabela 27 - Exibição ao vivo



Passo 5. Clique duas vezes na Snapshot para ver os detalhes.

- Os snapshots de humanos exibem recortes do corpo, tipos roupas utilizadas na parte superior, cores das roupas superiores, tipos de roupas utilizadas na parte inferior, cores das roupas inferiores, com bolsas ou não, usando chapéus ou não, e o gênero. Se rostos forem gravados, o sistema exibirá snapshots de rosto, idade, expressão facial, uso de óculos ou máscaras faciais. Você pode ampliar qualquer parte da imagem do corpo humano, ir para a interface de pesquisa e visualizar as gravações.

- Os snapshots de veículo exibem a visão panorâmica dos veículos, tipo de veículo, cor do veículo, cor da placa e marca do veículo. Você pode visualizar snapshots de placas de veículos, reproduzir vídeos vinculados e ampliar partes específicas da imagem do veículo.
  - Clique e salve os arquivos .rar no caminho especificado.
  - Clique para reproduzir as gravações de vídeo cronometradas antes e depois do snapshot.
- Os snapshots de veículos não motorizados exibem a vista panorâmica, o tipo de veículo, a cor do veículo e o número de pessoas envolvidas.

3.6.3.3 Pesquisando Registros de Análise Forense

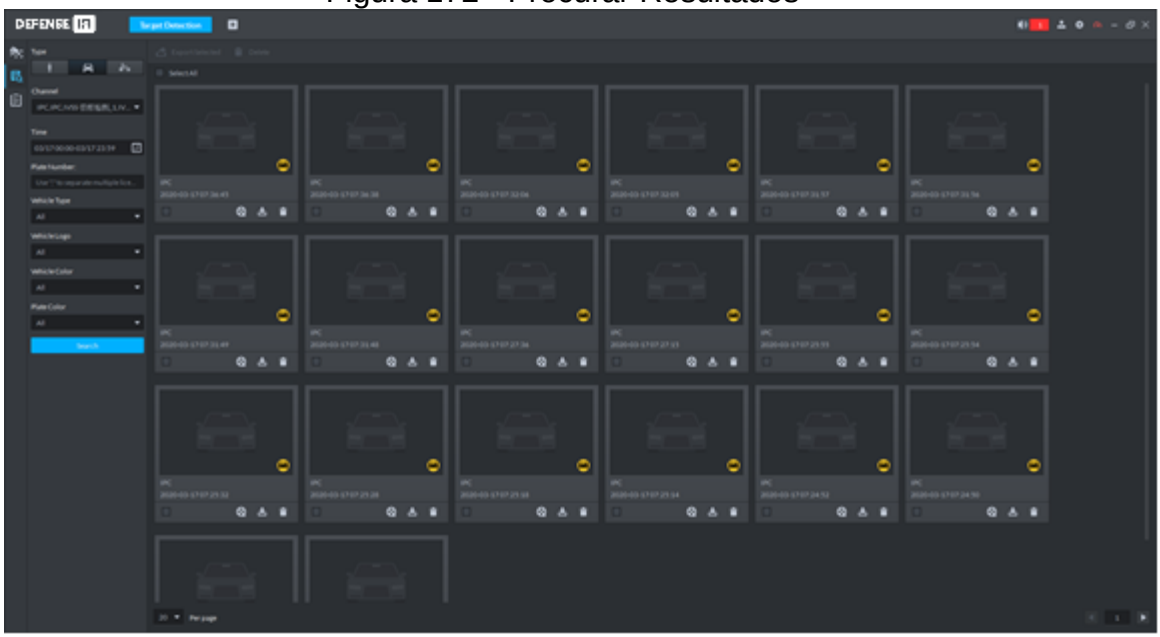
Passo 1. Faça login no Defense IA Client e clique em e selecione **Análise Forense.**

Passo 2. Clique em .

Passo 3. Defina as condições de pesquisa e clique em **Pesquisar**.

Você pode pesquisar por veículo humano, veículo e não motorizado. Se você usa IVSS para Análise Forense, pode carregar uma imagem para pesquisar alvos semelhantes.

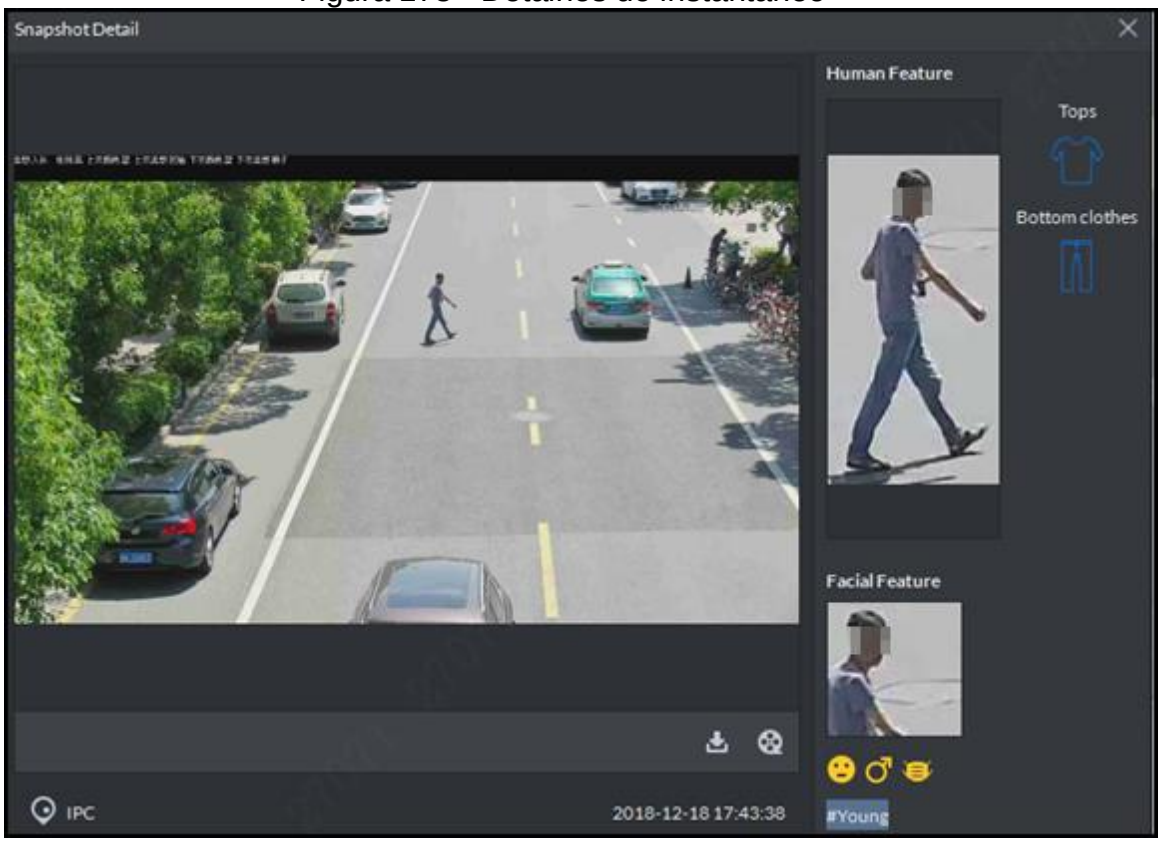
Figura 172 - Procurar Resultados



Passo 4. Ações disponíveis.

- Clique duas vezes no instantâneo para ver os detalhes.

Figura 173 - Detalhes do instantâneo



- Para baixar o vídeo, clique em .
- Para reproduzir o vídeo, clique em .
- Para exportar pesquisas, selecione os registros e clique em **Exportar selecionados.**

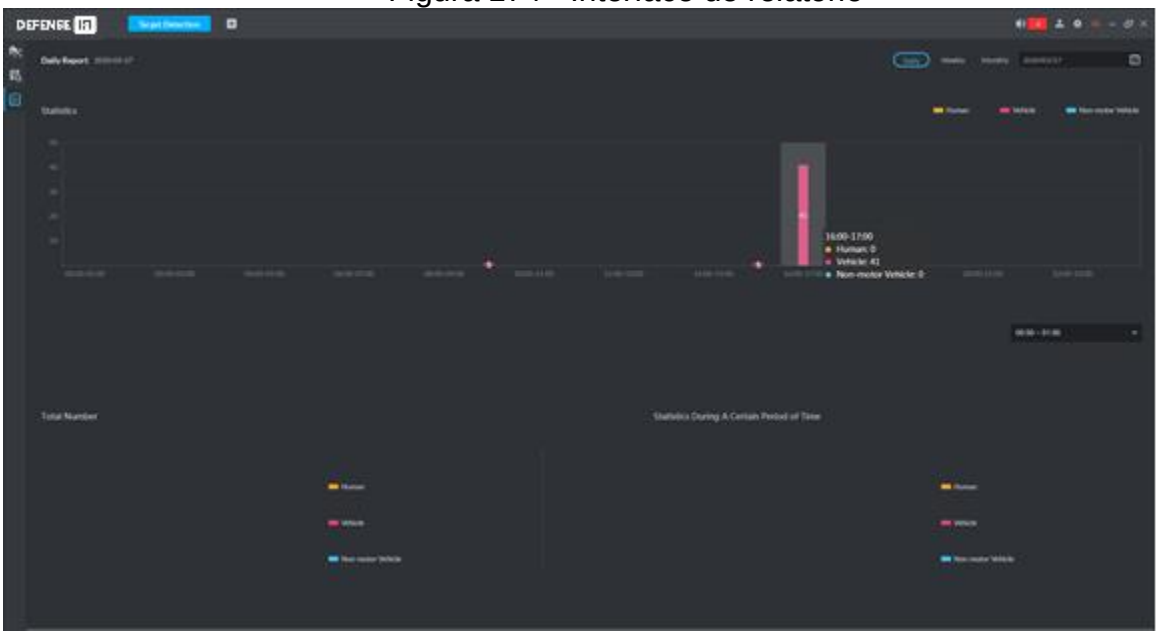
3.6.3.4 Relatórios

Passo 1. Clique no Defense IA Client e selecione Análise Forense.

Passo 2. Clique em .

Passo 3. No canto superior direito, selecione o tipo de período e a data. O relatório mostra os dados de pessoas, veículos motorizados e não motorizados durante o período definido.

Figura 174 - Interface de relatório



3.7 MÓDULO BI (BUSINESS INTELLIGENCE)

3.7.1 Análise de Fluxo e Demografia do Cliente

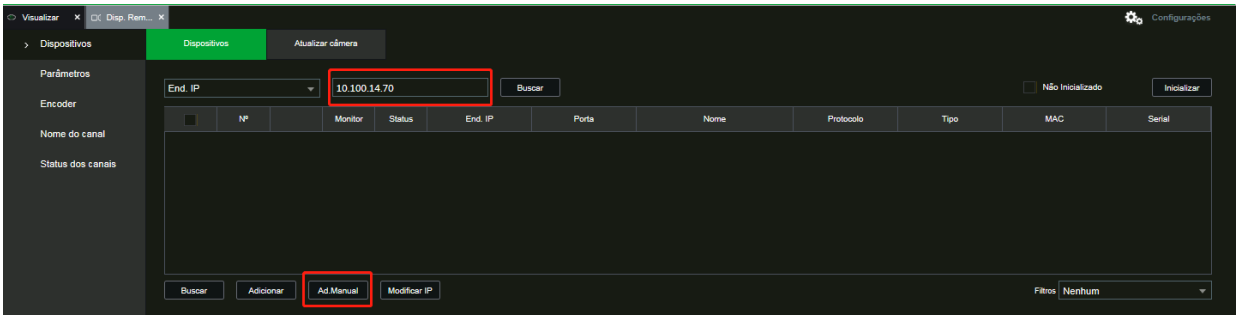
Com este módulo o cliente consegue trazer diversas informações de seu estabelecimento, são elas:

- Conhecer os horários de pico melhorando o atendimento aos clientes e de maneira mais satisfatória;
- Conhecer a faixa etária, saber qual o público alvo para direcionar melhor a quantidade e qualidade do atendimento para cada tipo de público;
- Saber qual gênero/idade tem seu público. Campanhas de marketing direcionadas e assertivas ao seu público alvo;
- Saber a satisfação dos seus clientes pelas emoções demonstradas enquanto estiverem dentro do estabelecimento;

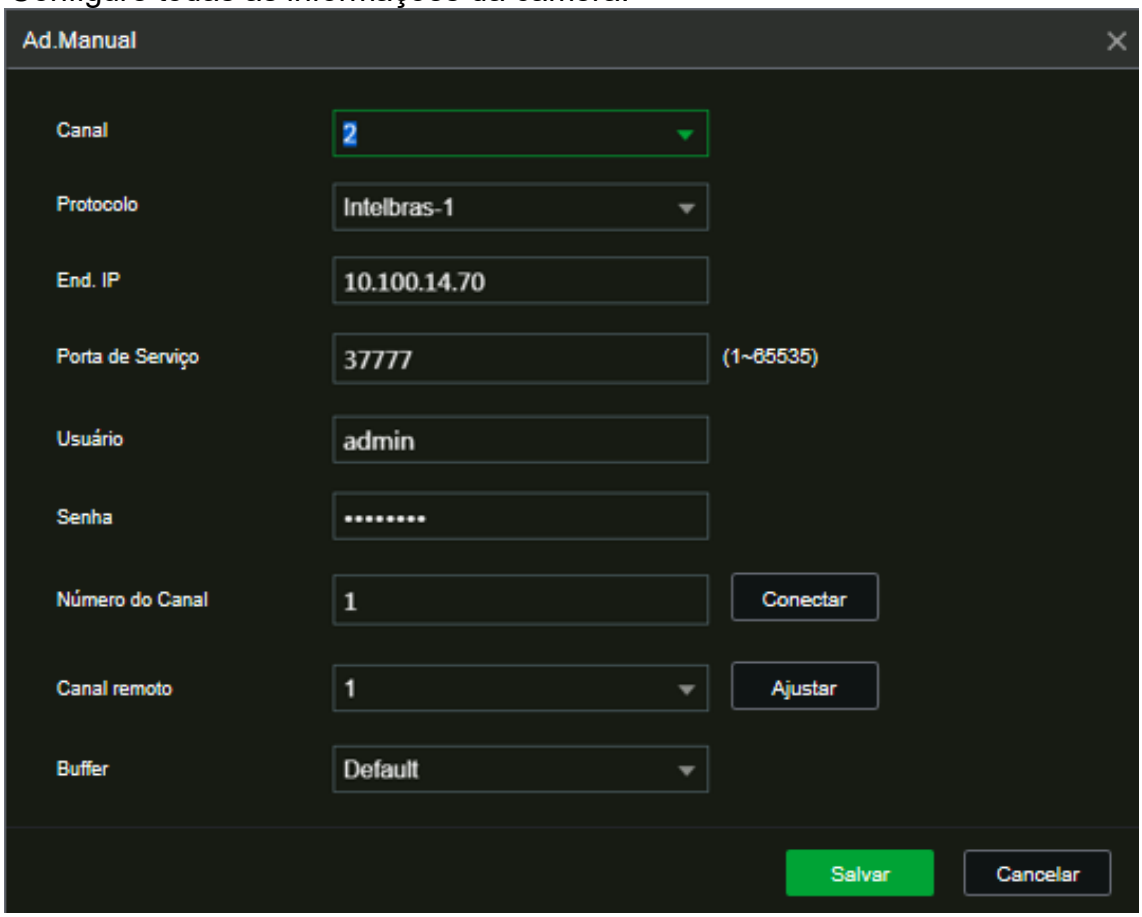
Para estes dois módulos serão utilizados uma câmera VIP genérica e um iNVD 9032 FT IA, que irá encaminhar a inteligência de reconhecimento facial. O primeiro passo é adicionar a câmera ao iNVD, para isso siga os passos abaixo:

3.7.1.1 Adicionando a câmera ao iNVD

I. Busque o IP da câmera, caso não encontre adicione-a manualmente



II. Configure todas as informações da câmera:



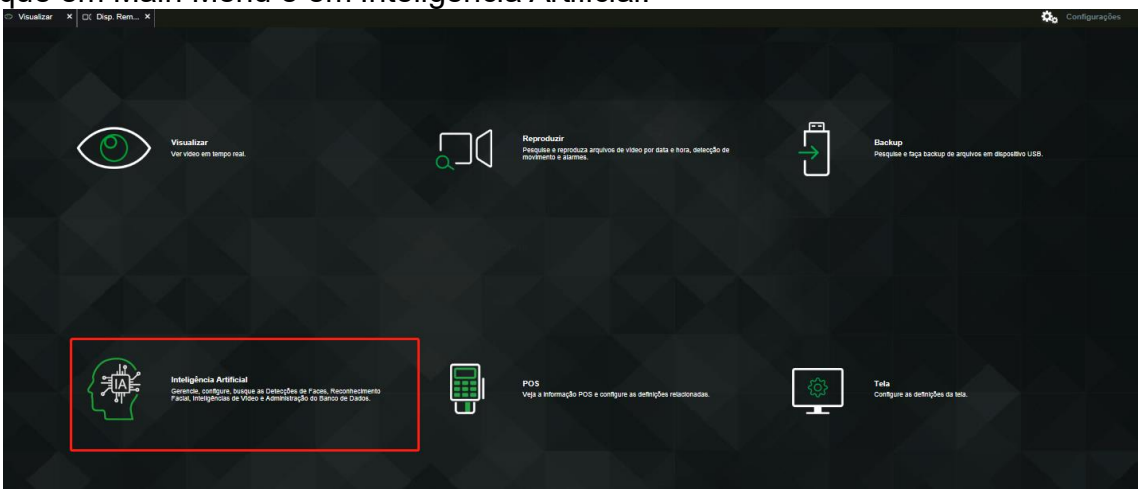
III. Verifique se o status da câmera ficou verde, caso esteja vermelha, clique em Atualizar e verifique se alterou o status. Caso continue vermelho, confirme as informações da câmera como IP, usuário, senha, porta, etc.

Adicionada com sucesso!

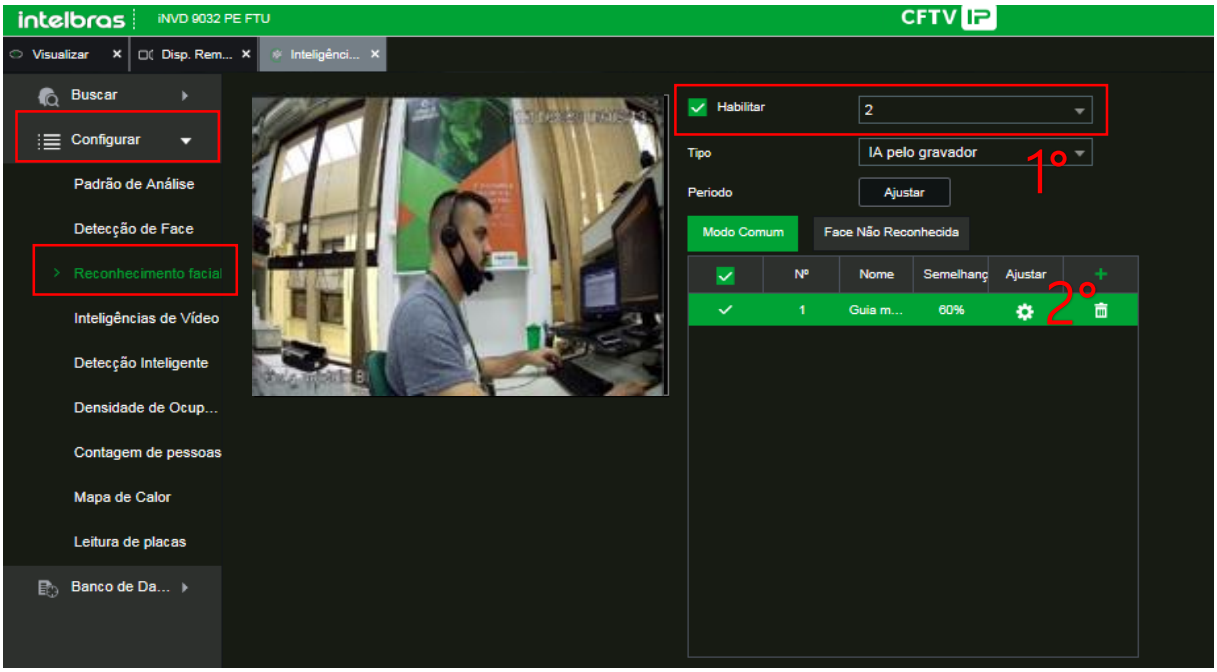
3.7.1.2 Configurando a inteligência no canal

Para a configuração da inteligência no canal siga os passos abaixo:

I. Clique em Main Menu e em Inteligência Artificial:



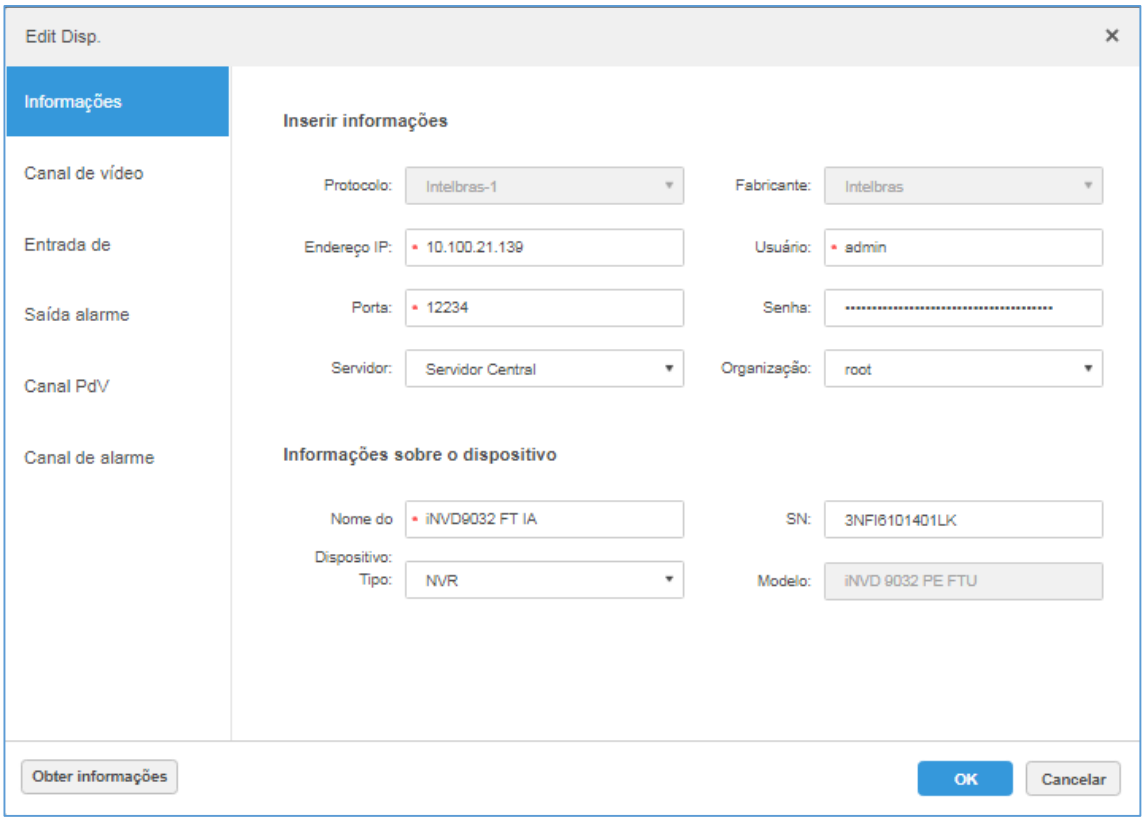
II. Siga os passos enumerados para configuração e habilite o reconhecimento facial para o canal.



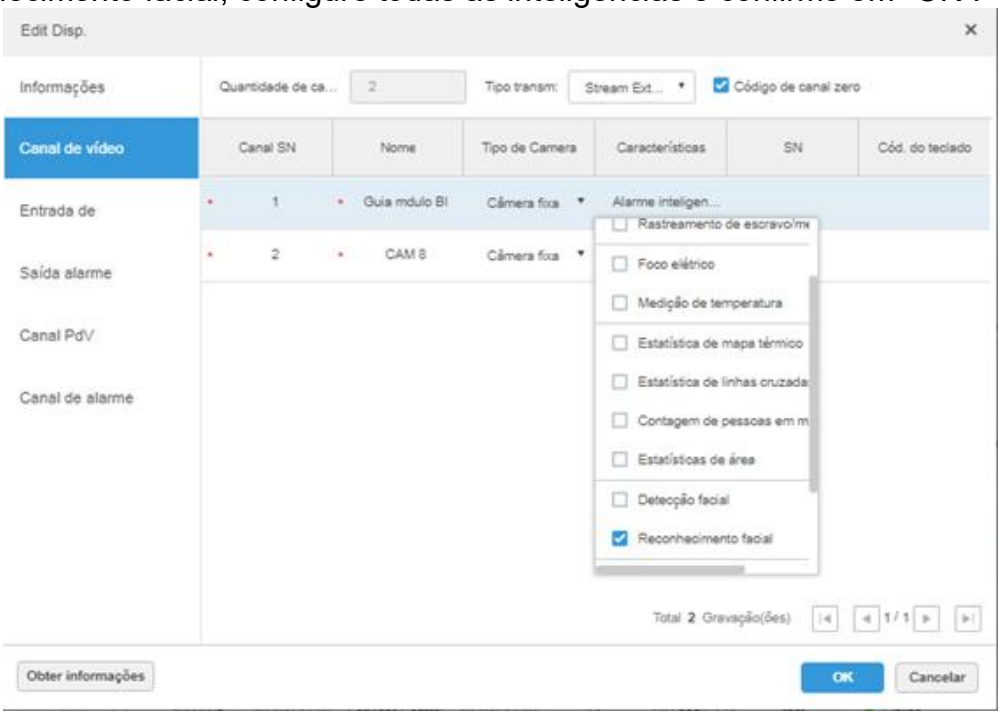
3.7.1.3 Adicionando o iNVD ao defense

Adicionar o iNVD e configurar os canais com inteligência.

I. Configure as informações para adicionar o iNVD 9032 FT IA ao Defense



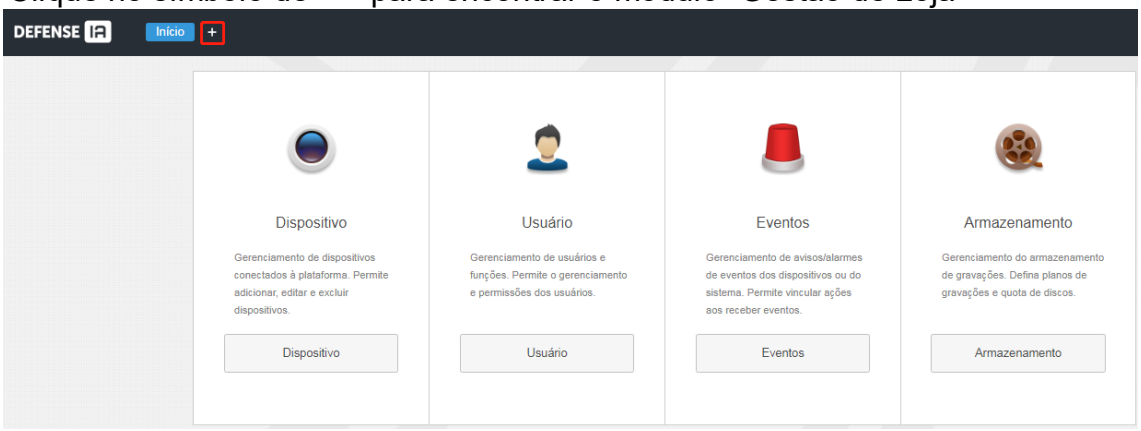
II. Na aba “Canal de vídeo” inclua as características da câmera que fará o reconhecimento facial, configure todas as inteligências e confirme em “OK”.

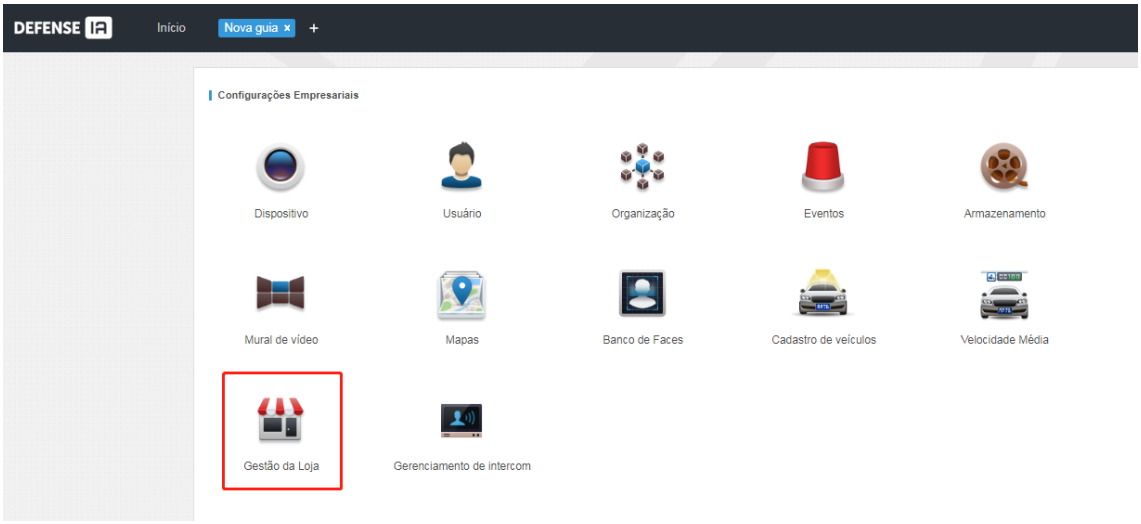


iNVD adicionado com sucesso!

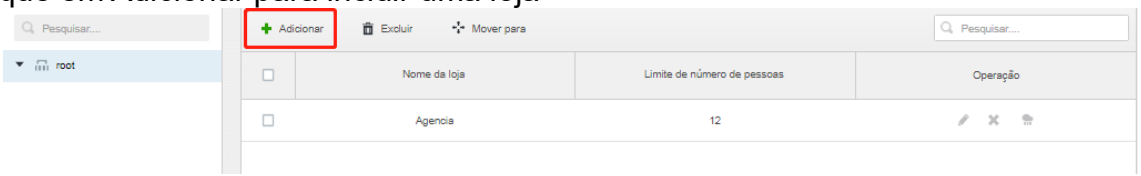
3.7.1.4 Configurando o módulo Gestão de Loja

I. Clique no símbolo de “+” para encontrar o módulo “Gestão de Loja”

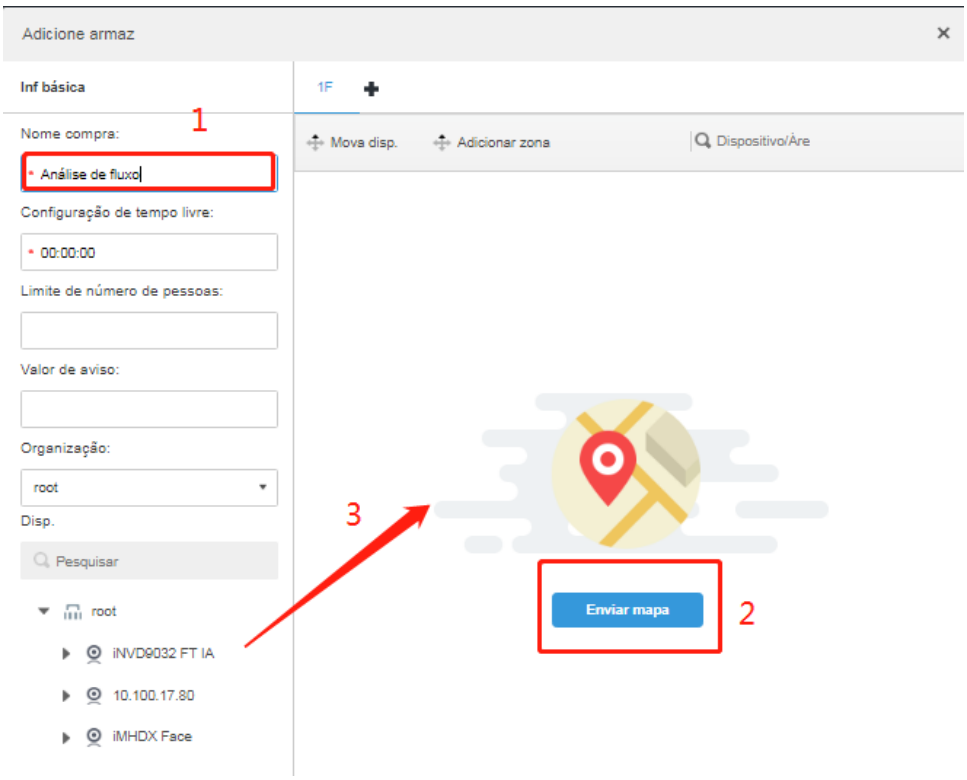




II. Clique em Adicionar para incluir uma loja

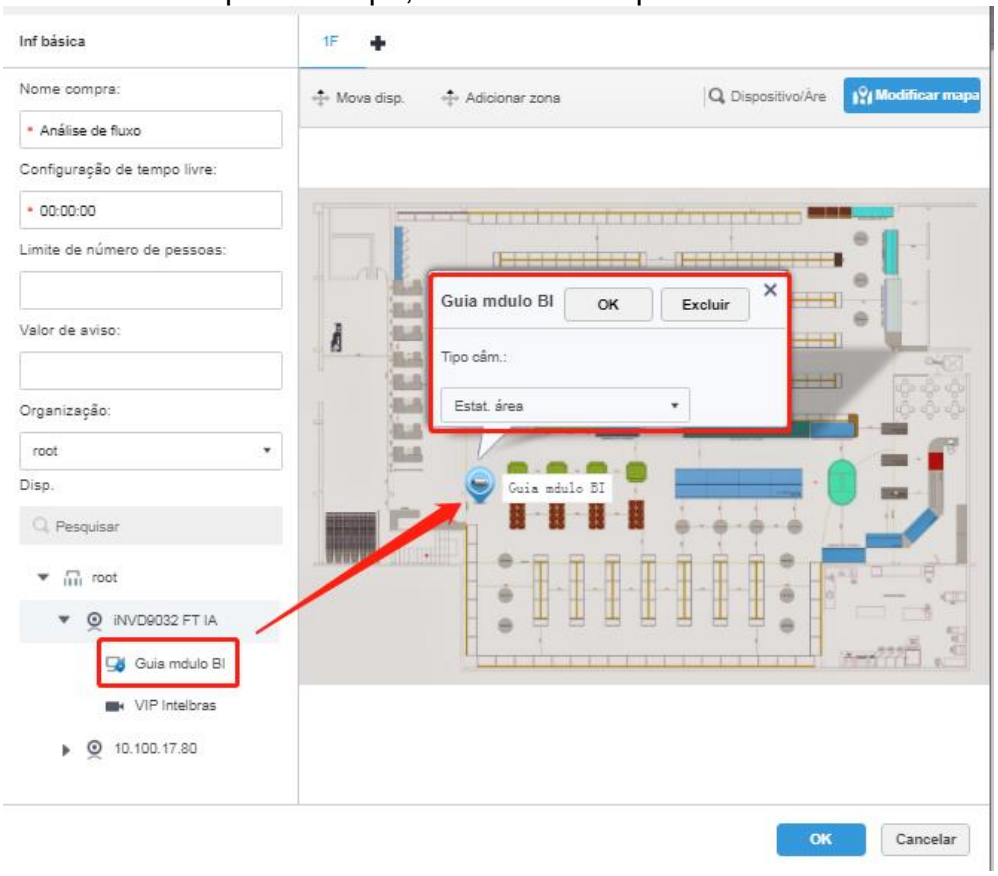


III. Para adicionar uma loja, é necessário configurar um nome (1), um mapa (2) e arrastar as câmeras para a área de interesse (3), conforme imagens abaixo:



...

IV. Após arrastar a câmera para o mapa, selecione em tipo de câmera “Estat. Área”



Após realizar esses passos de configuração, a câmera já estará pronta para gerar os relatórios no Defense Client.

As formas de exibir os relatórios estarão disponíveis na seção de utilização do Defense Client.

3.7.2 Análise de área

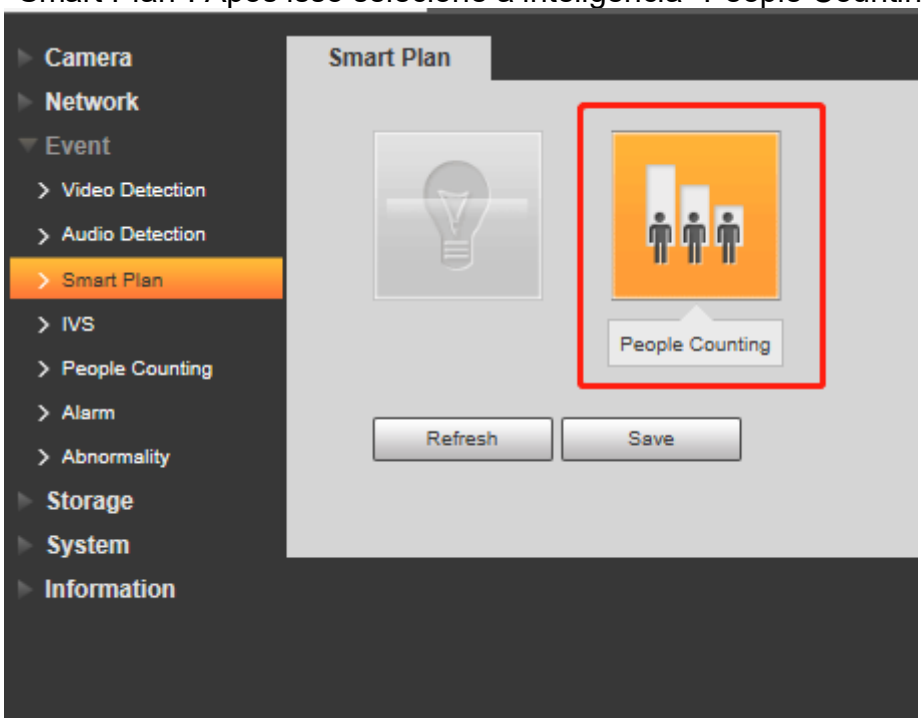
Com este módulo o cliente consegue buscar relatórios do tempo médio de estadia em áreas pré-definidas e quantas pessoas ficaram nesta área. Desta forma é possível saber o tempo médio que os clientes esperam em caixas eletrônicos, atendimento pessoal, qual o tempo para serem atendidas, quais zonas tem maior tempo de espera, avaliar os sistemas utilizados se estão sendo eficientes e atendimentos por bancada

Para este módulo será utilizada uma câmera VIP 91210 F IA, ela irá enviar a inteligência de ocupação de área para o Defense.

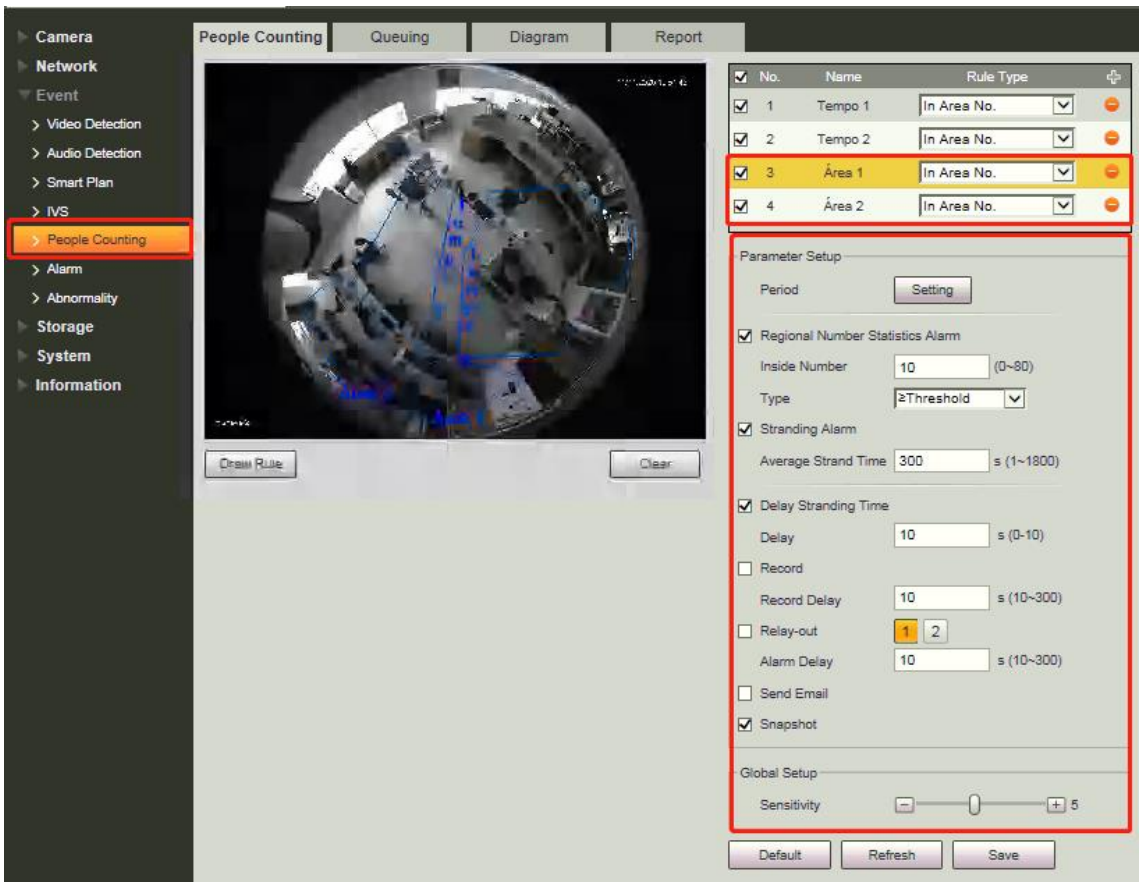
Para aprendizado, iremos adicionar agora a câmera diretamente ao Defense, sem passar pelo iNVD 9032 FT IA.

3.7.2.1 Configurando a câmera VIP 91210 F IA

I. No menu “Settings” que faz a configuração das inteligências da câmera, clique em “Event” e “Smart Plan”. Após isso selecione a inteligência “People Counting”.



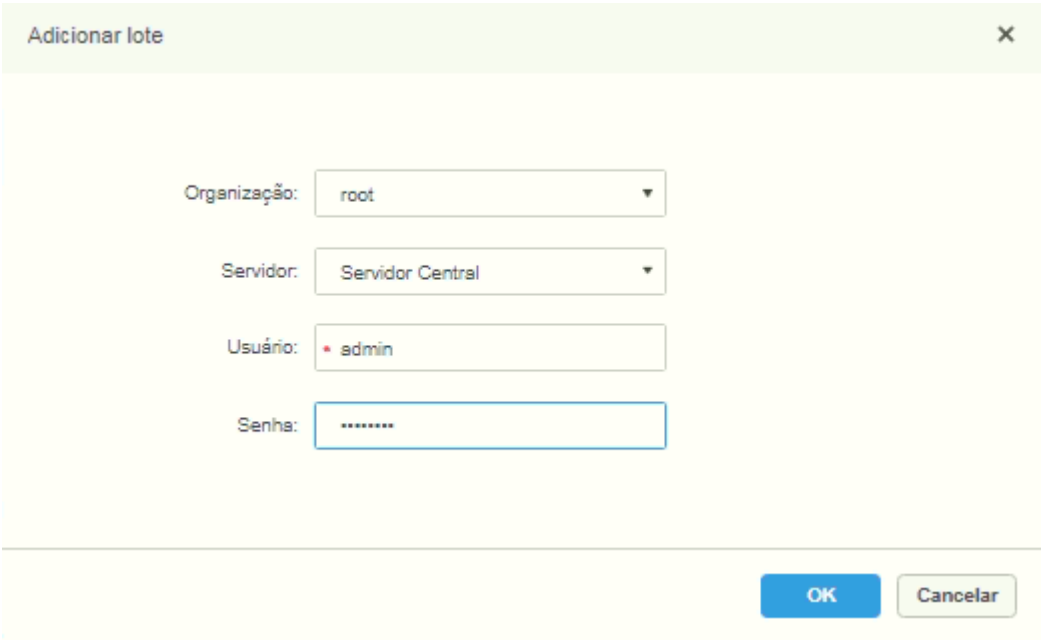
II. Após habilitar a inteligência de contagem de pessoas, clique em “People Counting” na coluna da esquerda para configurar a área a ser monitorada e desenhar a área desejada. Confira a imagem abaixo com as configurações.



3.7.2.2 Adicionando a câmera no Defense

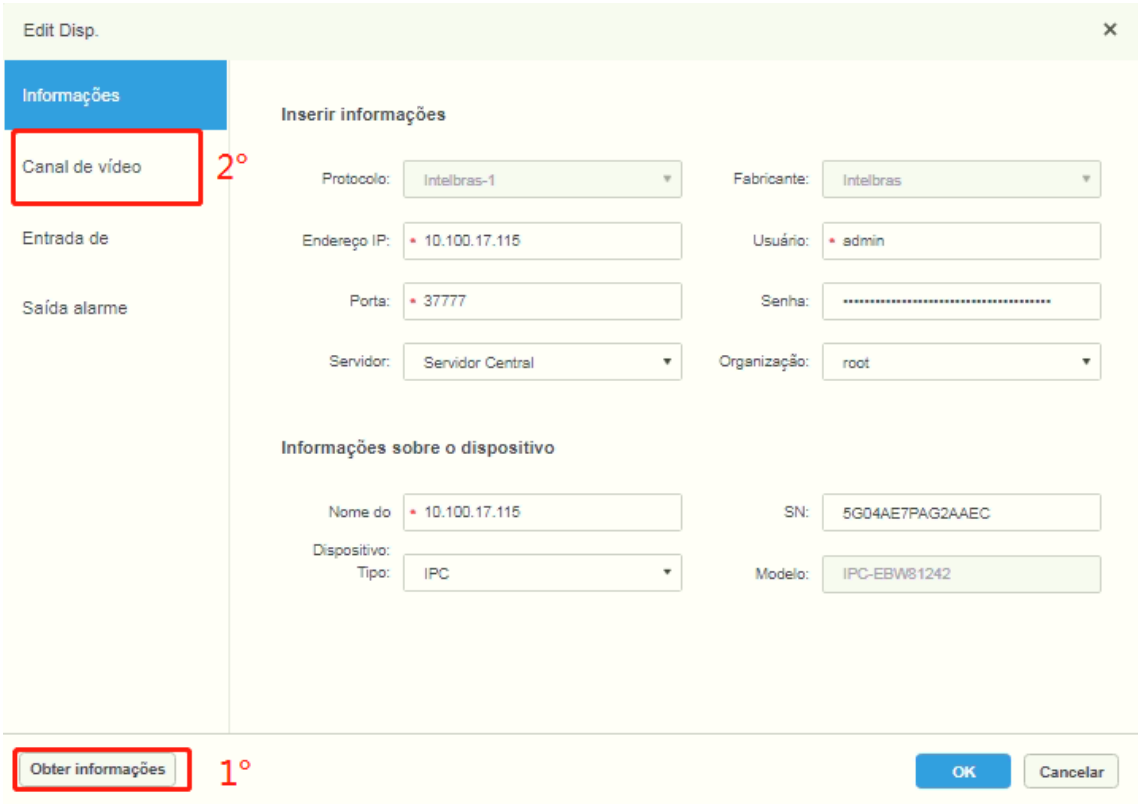
I. Acesso a página Web do servidor e clique em Dispositivos

II. Busque o IP da sua câmera no ícone de Segmento de rede, destacado abaixo, após encontrar, selecione a câmera e clique em “Conectar”

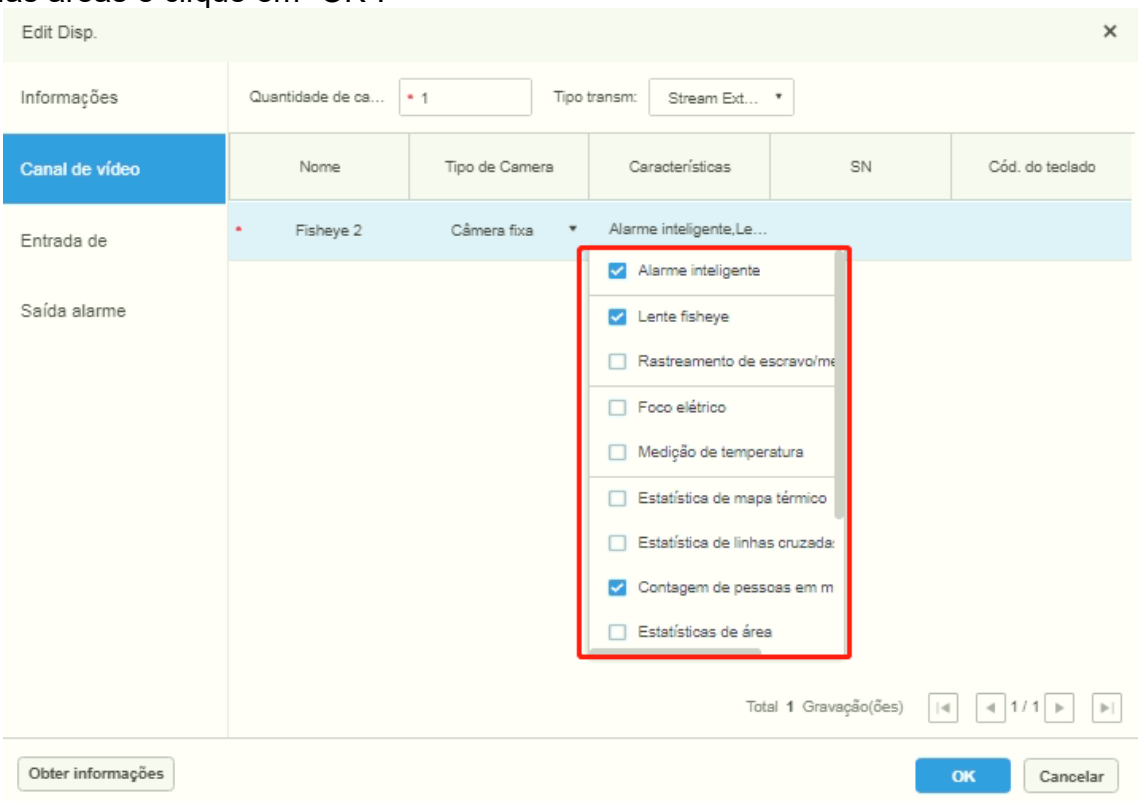


III. Após adicionado a câmera no Defense, na coluna Operação clique no ícone do lápis, para configurar as informações e inteligências da câmera.

IV. Abrirá a janela de configuração da câmera, clique em “Obter Informações” (1°) e depois clique em “Canal de vídeo” (2°)

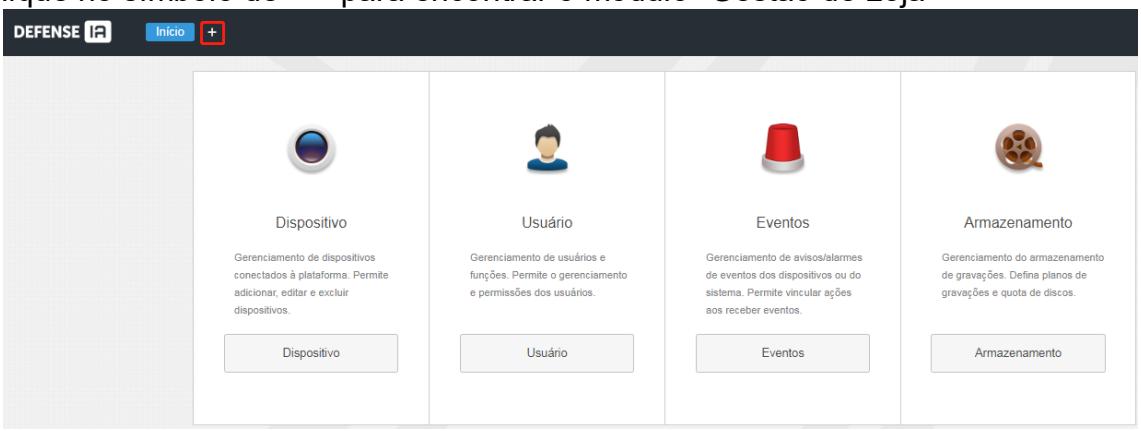


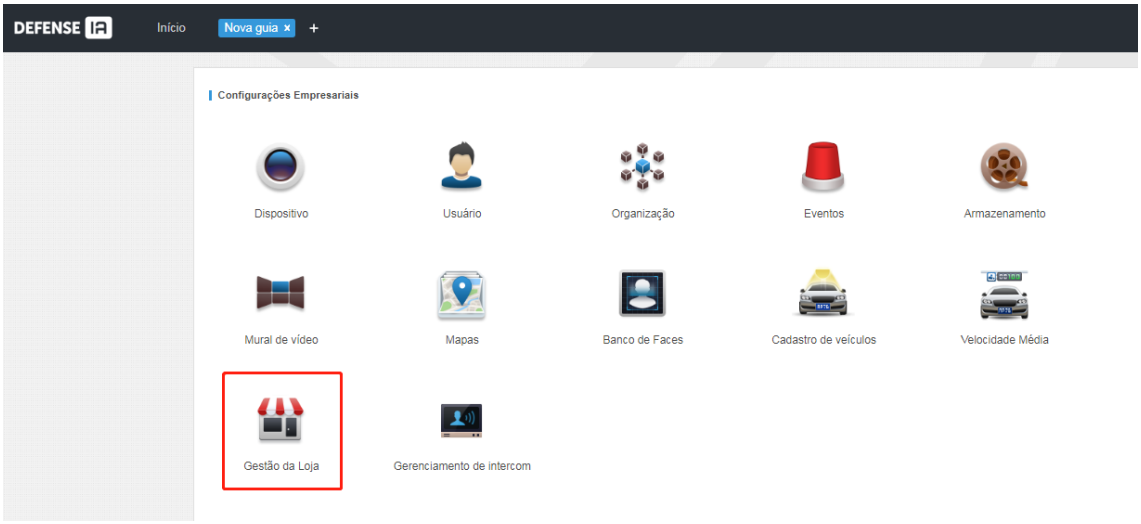
V. Clicando em Canal de vídeo, configure as inteligências da câmera, para a VIP 91210 F IA, selecionamos Alarme inteligente, Lente fisheye e Contagem de pessoas em múltiplas áreas e clique em “OK”.



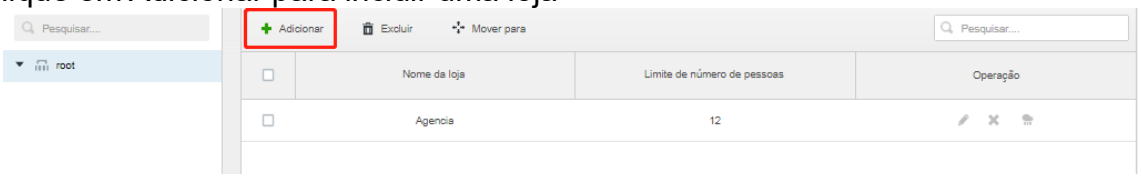
3.7.2.3 Configurando o módulo Gestão de Loja

I. Clique no símbolo de “+” para encontrar o módulo “Gestão de Loja”

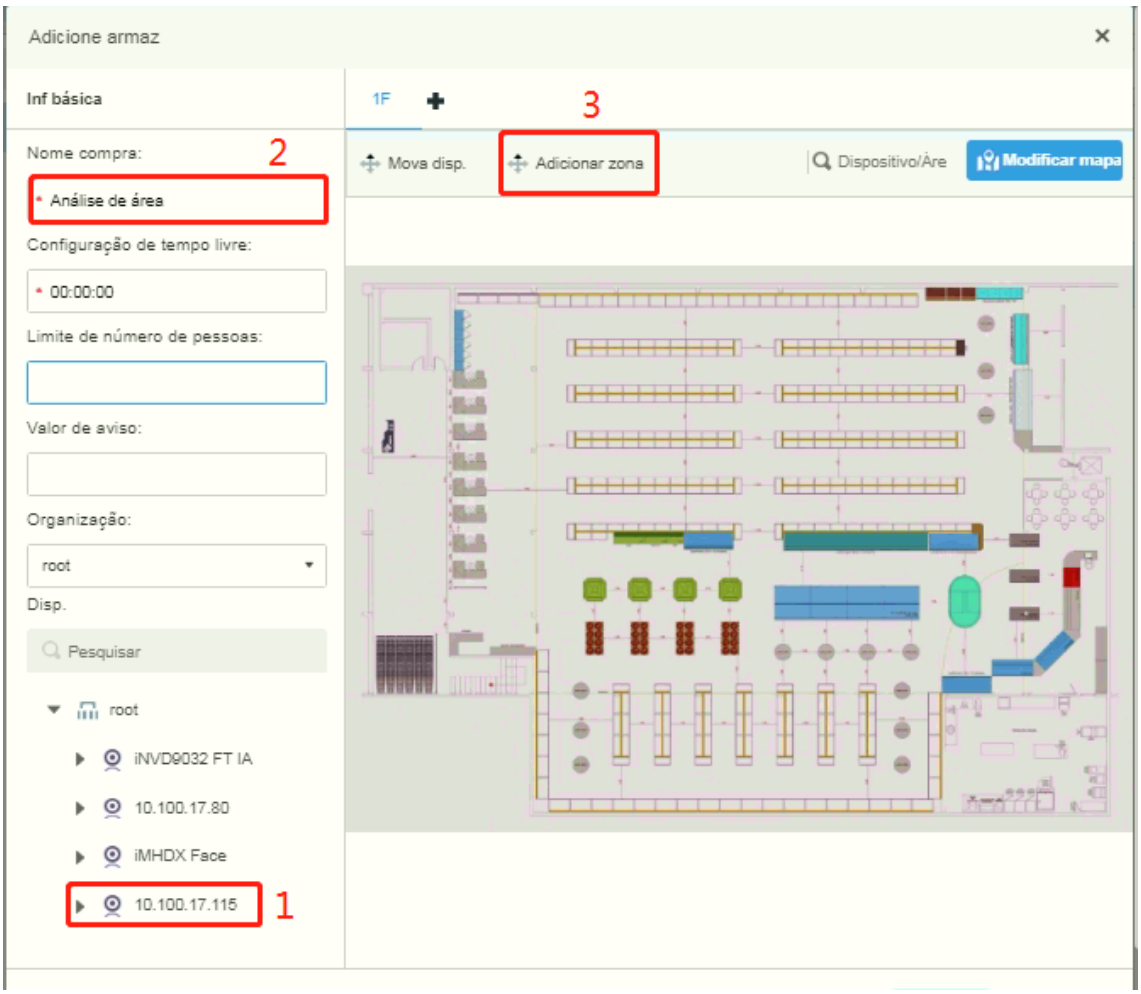




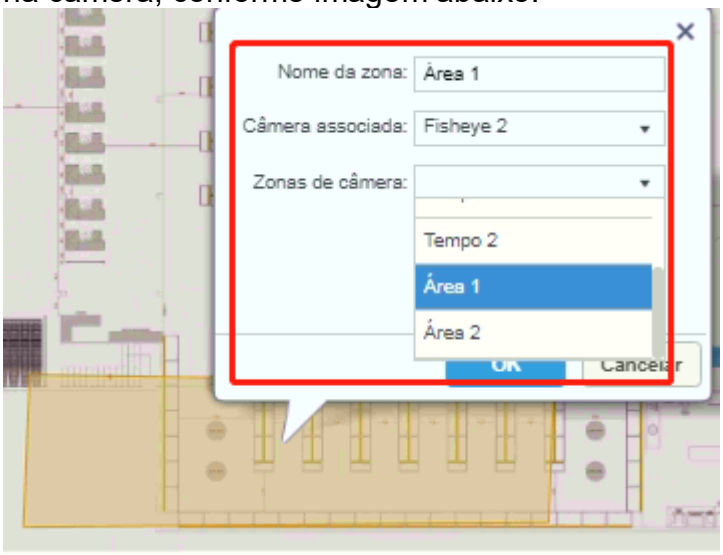
II. Clique em Adicionar para incluir uma loja



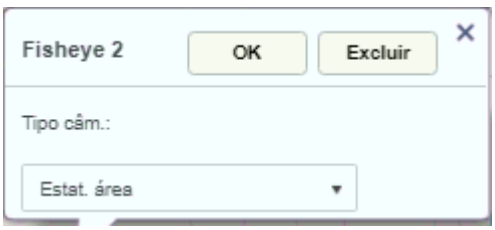
III. Confirme que a câmera aparece na lista de dispositivos para adicionar ao mapa (1). Para adicionar uma loja, é necessário configurar um nome (2), adicionar um mapa e adicionar uma Zona para a área de interesse (3), conforme imagens abaixo:



IV. Configure uma Zona de interesse e busque as informações que foram configuradas na câmera, conforme imagem abaixo:



Configurando Área 1



Configurando Área 2

V. Após realizar esses passos de configuração, a câmera já estará pronta para gerar os relatórios no Defense Client.

As formas de exibir os relatórios estarão disponíveis na seção de utilização do Defense Client.

3.7.3 Loja em tempo real

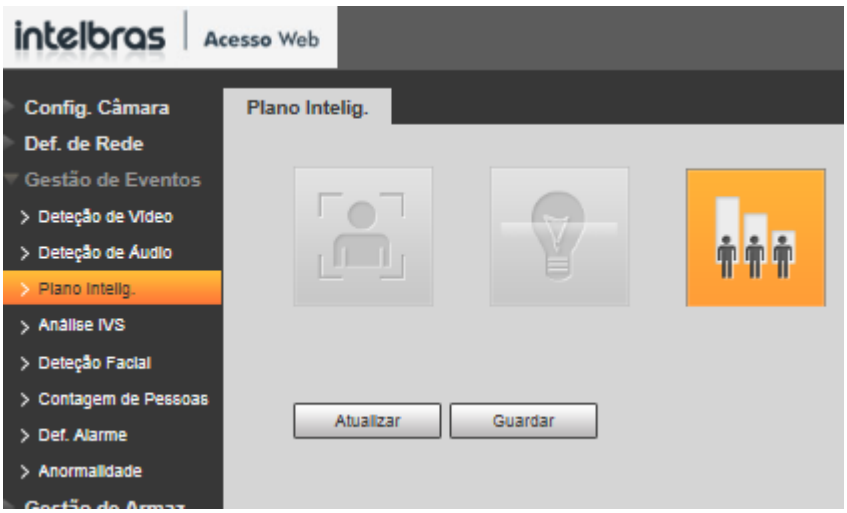
Com este módulo o cliente consegue controlar a taxa de ocupação da loja em tempo real, informando a quantidade de pessoas que estão na loja no momento, a quantidade de pessoas que podem entrar na loja e a quantidade de pessoas que entraram e saíram do estabelecimento.

Para este módulo será utilizada uma câmera VIP 9320 3D IA FT, ela irá enviar a inteligência de para o Defense.

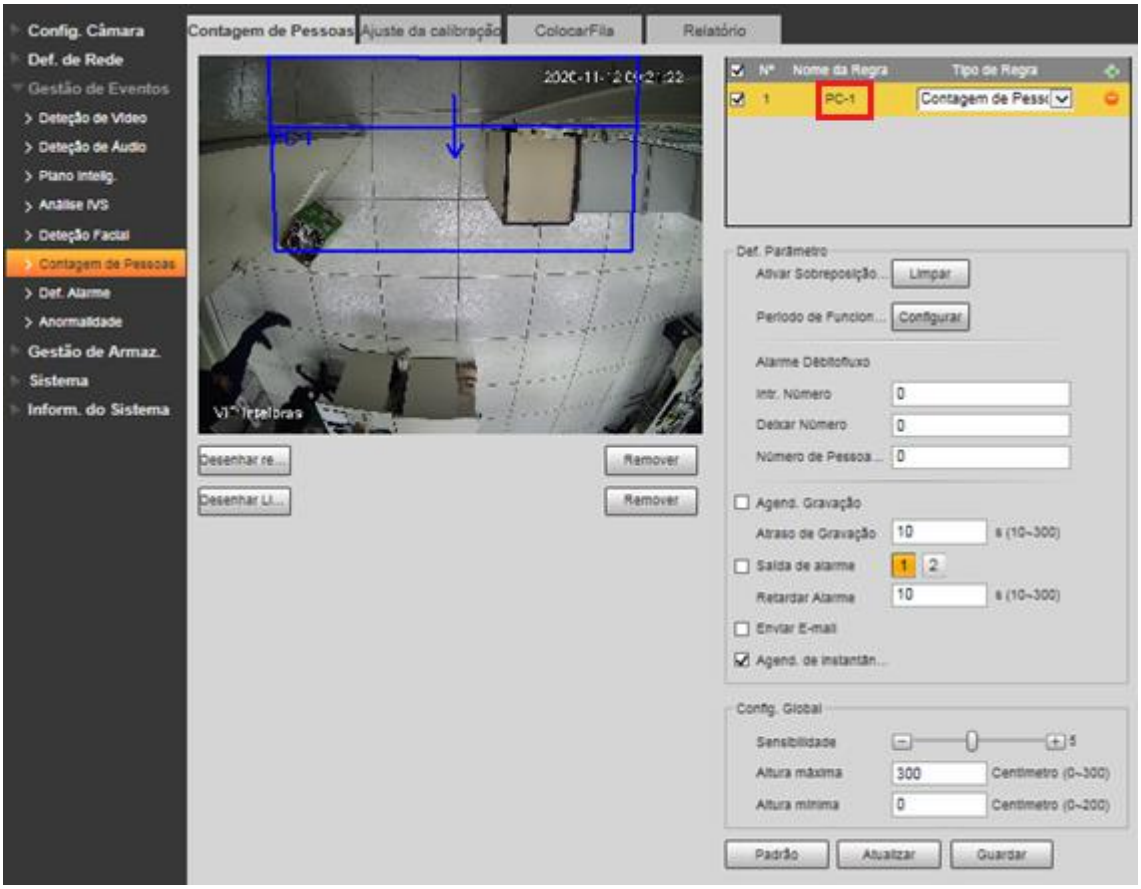
3.7.3.1 Configurando a câmera VIP 9320 3D IA FT

Será utilizada uma câmera VIP 9320 3D IA FT para entrada e outra para saída do estabelecimento:

I. No menu “Configurar” que faz a configuração das inteligências da câmera, clique em “Gestão de Eventos” e “Plano inteligente”. Após isso habilite a inteligência “Contagem de Pessoas”.

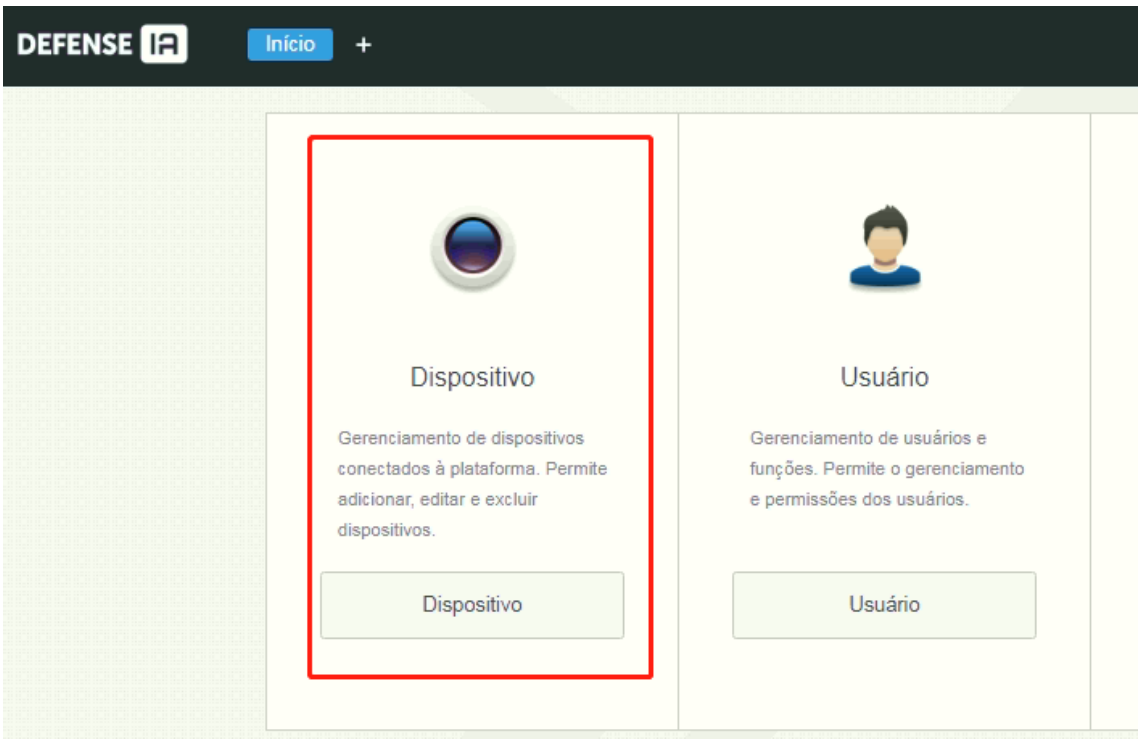


II. Após habilitar a inteligência de contagem de pessoas, clique em “Contagem de Pessoas” na coluna da esquerda para configurar a regra (PC-1) e área a ser monitorada e desenhar a área desejada. Confira a imagem abaixo com as configurações.

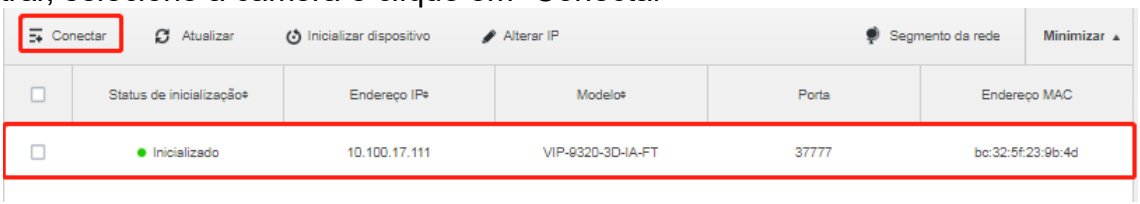


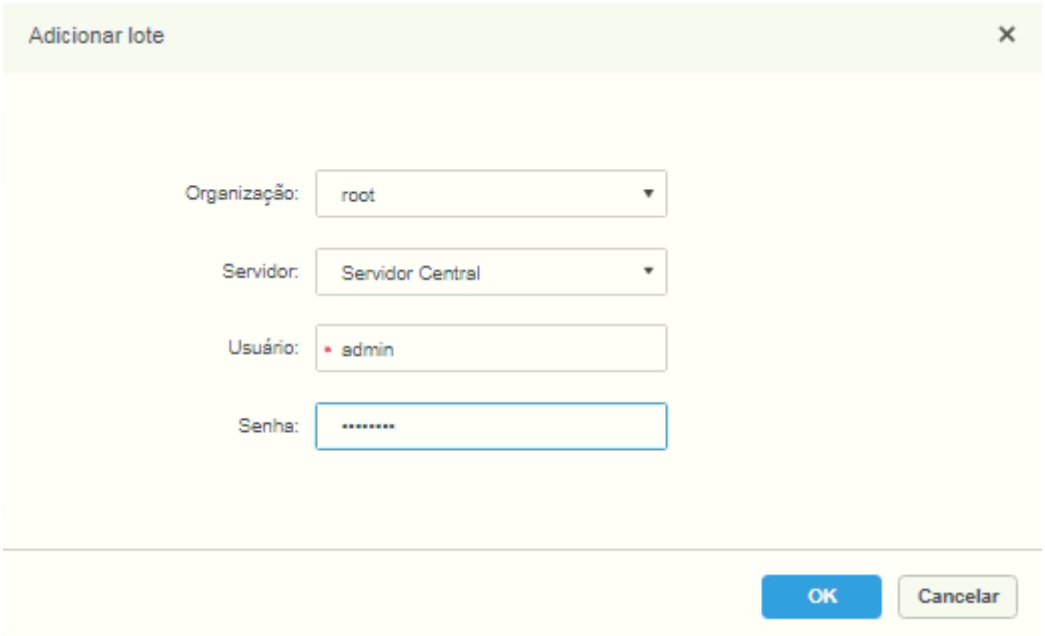
3.7.3.2 Adicionando a câmera no Defense

I. Acesso a página Web do servidor e clique em Dispositivos

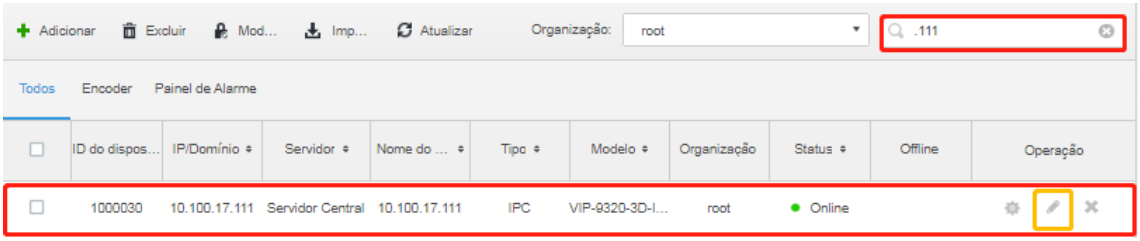


II. Busque o IP da sua câmera no ícone de Segmento de rede, destacado abaixo, após encontrar, selecione a câmera e clique em “Conectar”

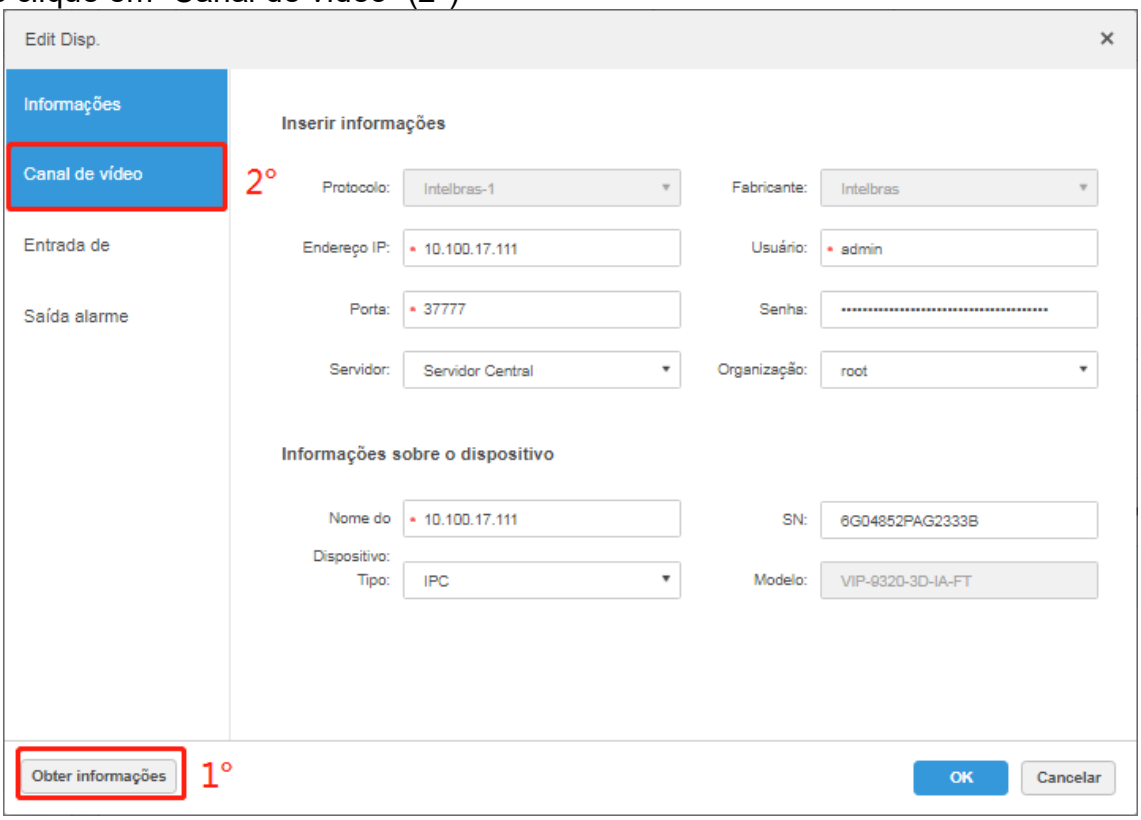




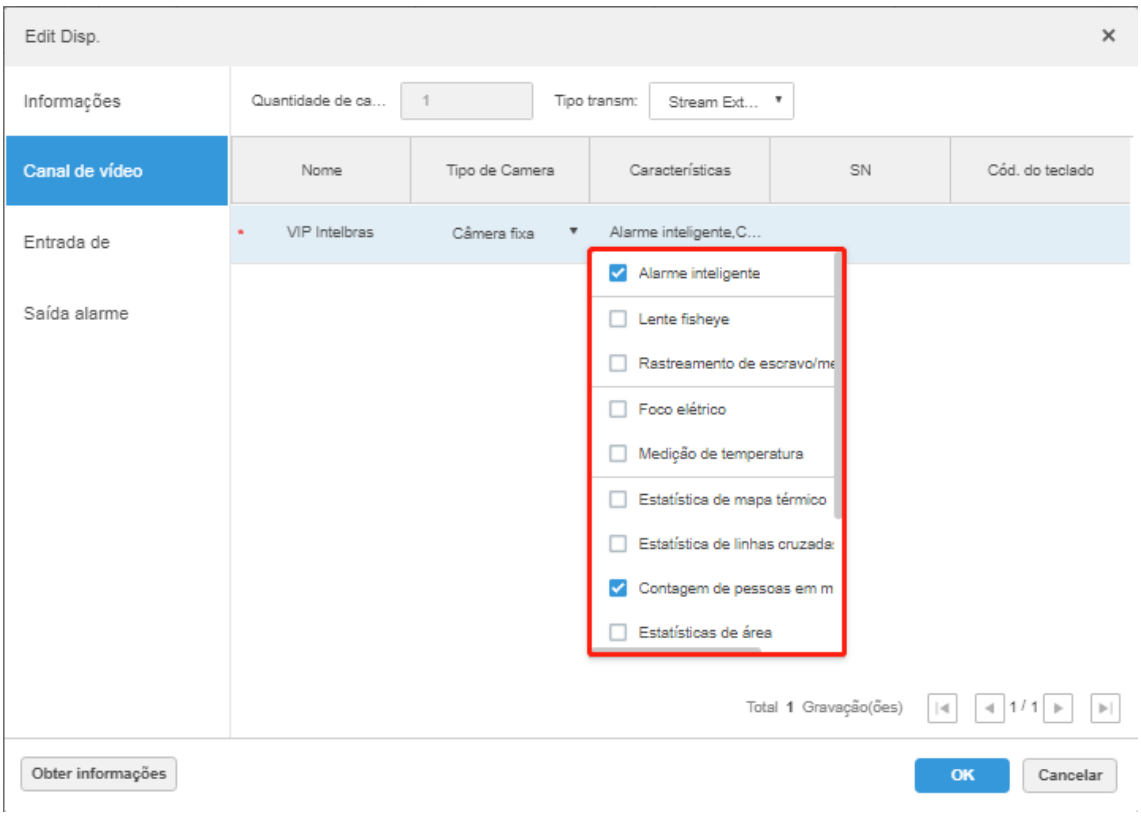
III. Após adicionado a câmera no Defense, na coluna Operação clique no ícone do lápis, para configurar as informações e inteligências da câmera.



IV. Abrirá a janela de configuração da câmera, clique em “Obter Informações” (1°) e depois clique em “Canal de vídeo” (2°)

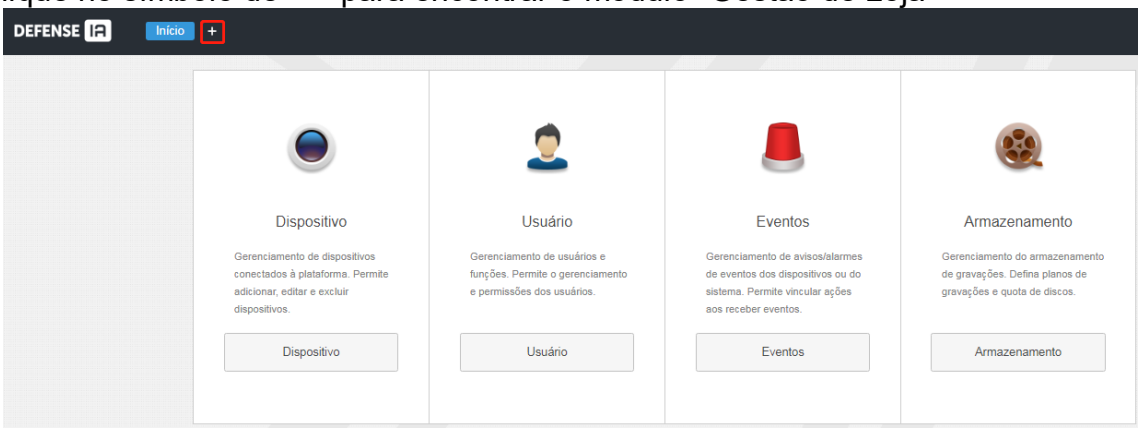


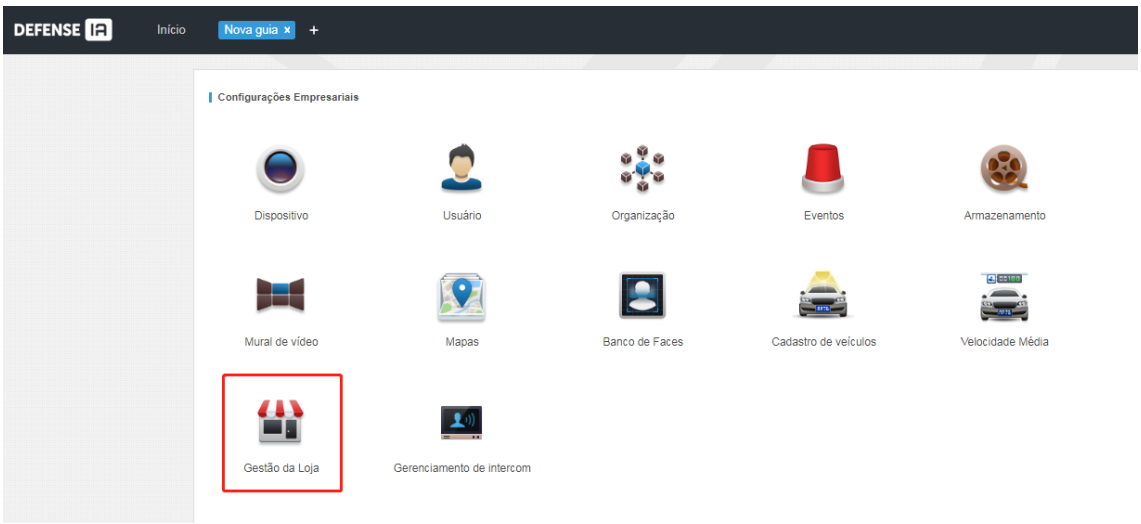
V. Clicando em Canal de vídeo, configure as inteligências da câmera, para a VIP 9320 3D IA FT, selecionamos Alarme inteligente e Contagem de pessoas em múltiplas áreas e clique em “OK”.



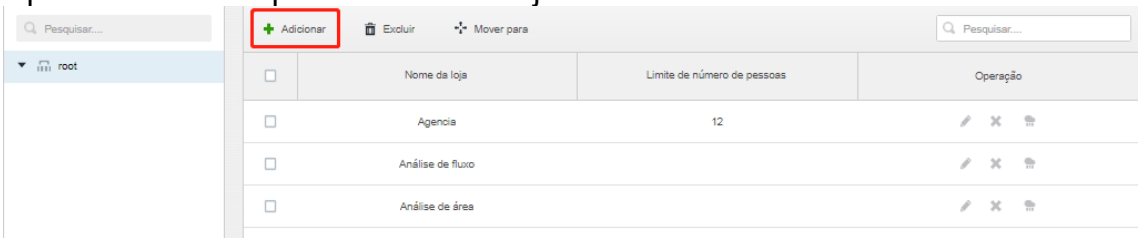
3.7.3.3 Configurando o módulo Gestão de Loja

I. Clique no símbolo de “+” para encontrar o módulo “Gestão de Loja”

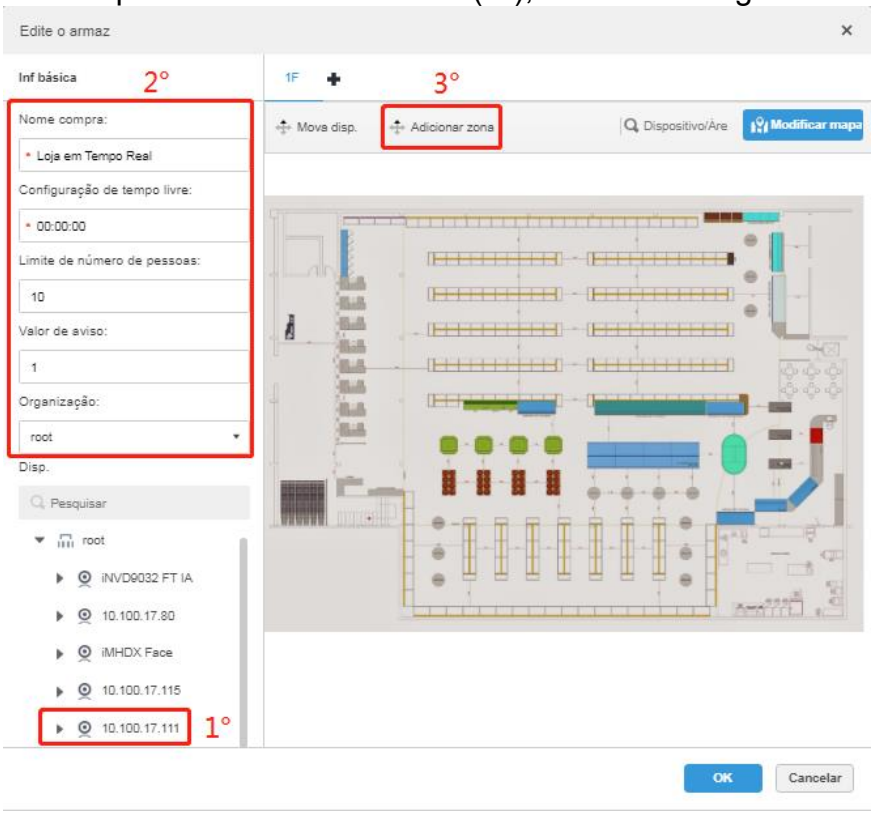




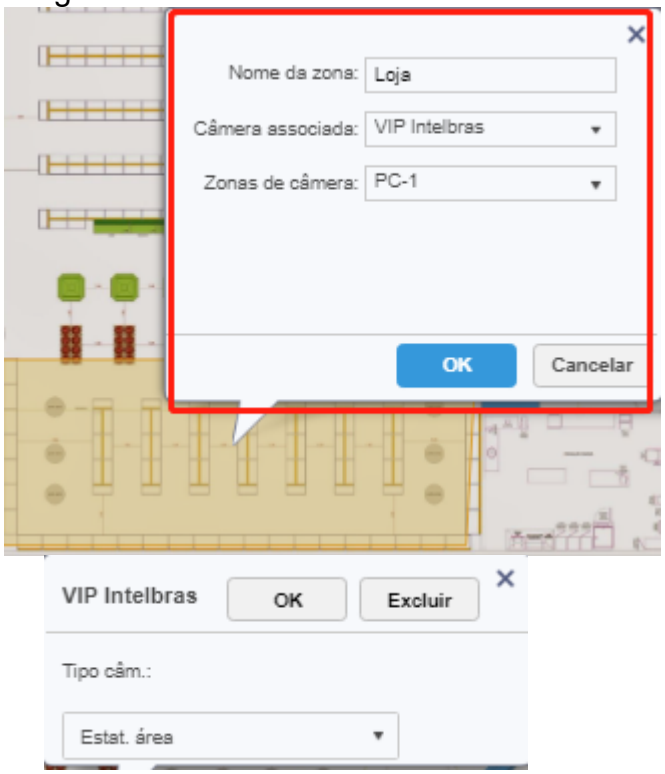
II. Clique em Adicionar para incluir uma loja



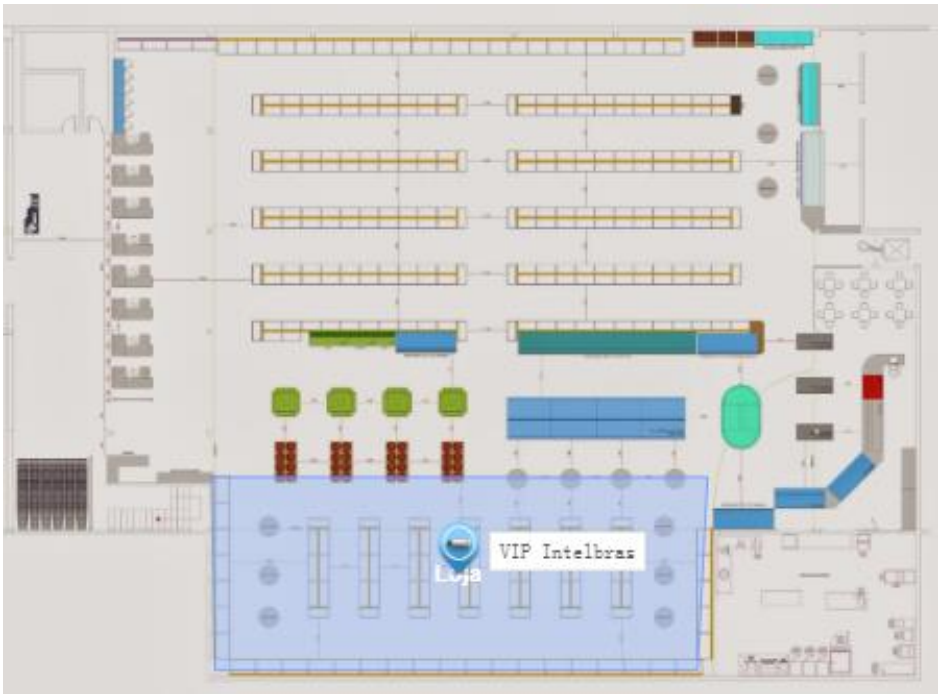
III. Confirme que as câmeras aparecem na lista de dispositivos para adicionar ao mapa (2°). Para adicionar a contagem em tempo real, configure o Limite de pessoas dentro do estabelecimento (nosso exemplo será utilizado 10) e configure o valor de aviso (nosso exemplo 1, então quando estiver faltando 1 pessoas para o limite máximo do estabelecimento, a sinaleira passa de verde para amarelo), (1°), adicionar um mapa e adicionar uma Zona para a área de interesse (3°), conforme imagens abaixo:



IV. Configure uma Zona de interesse e busque as informações que foram configuradas na câmera, conforme imagem abaixo:



V. O mapa fica da forma abaixo:

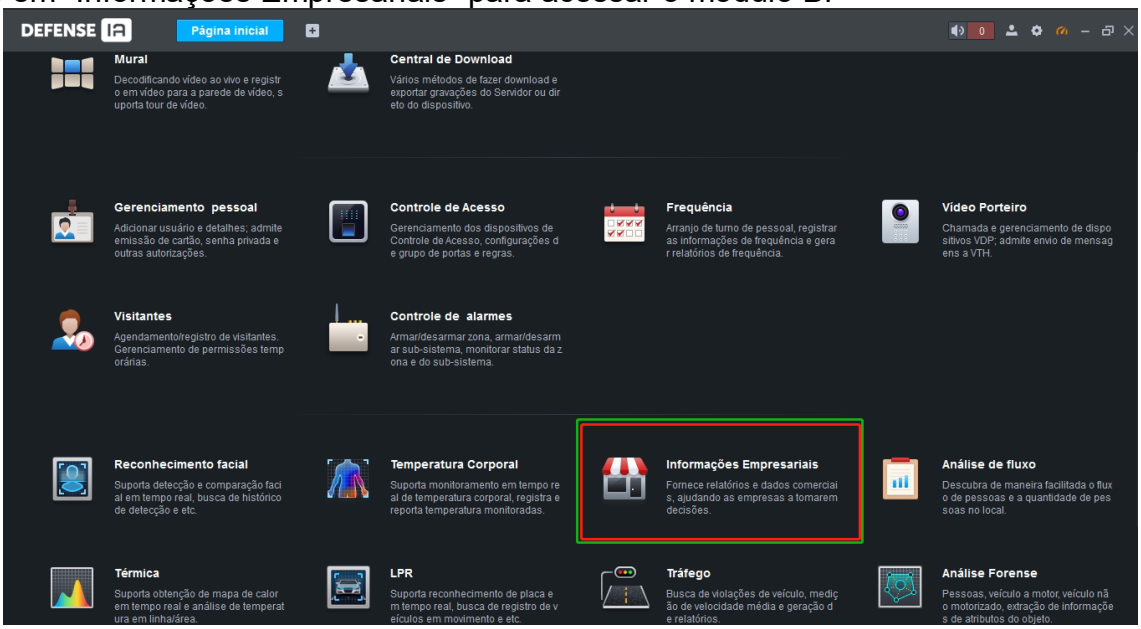


VI. Após realizar esses passos de configuração, a câmera já estará pronta para gerar os relatórios no Defense Client.

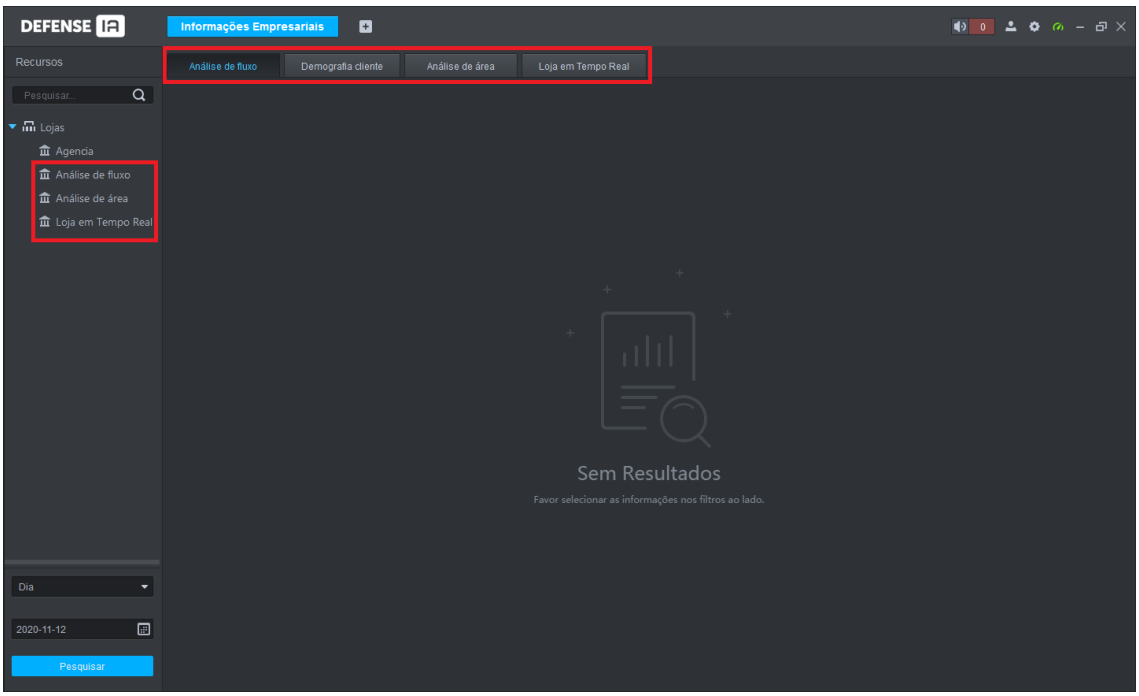
3.7.4 Utilização do Defense Client com B.I.

I. Acesse o Defense Client com o usuário e senha do seu sistema.

II. Clique em “Informações Empresariais” para acessar o módulo BI

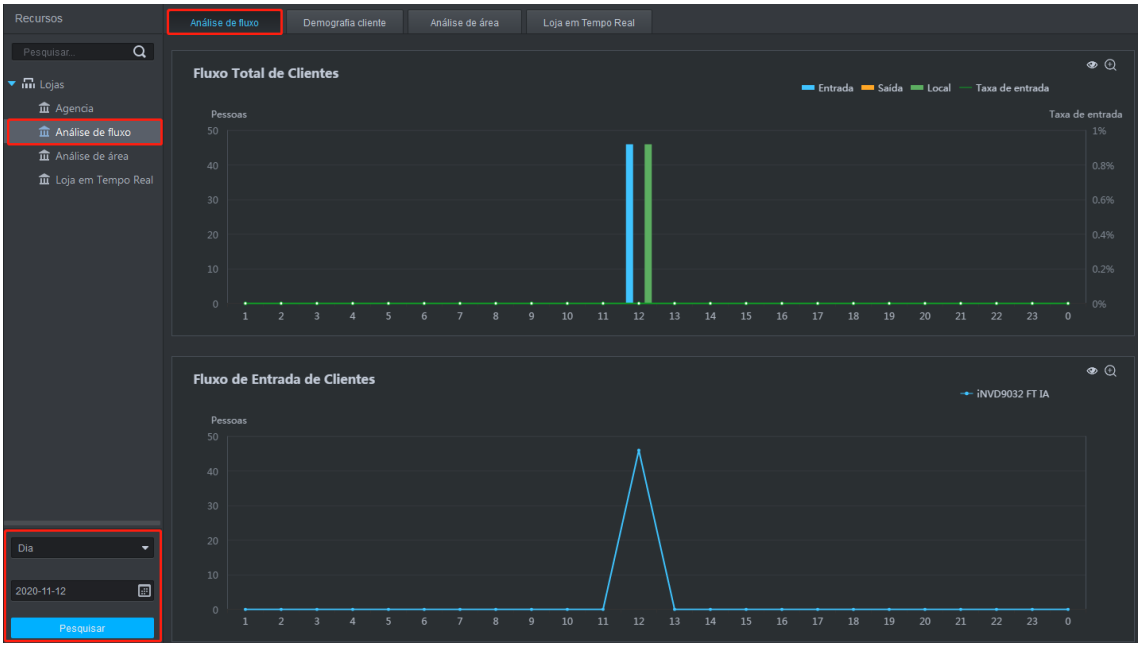


III. O módulo de Informações Empresariais abrirá com as informações configuradas na página Web do servidor



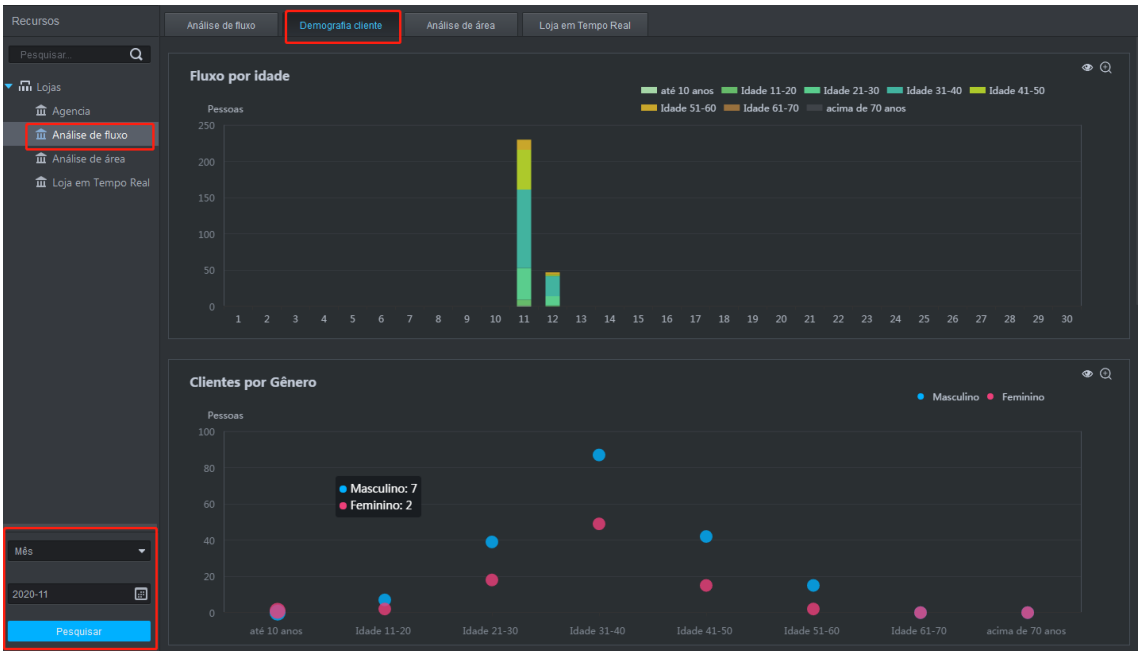
3.7.4.1 Análise de fluxo

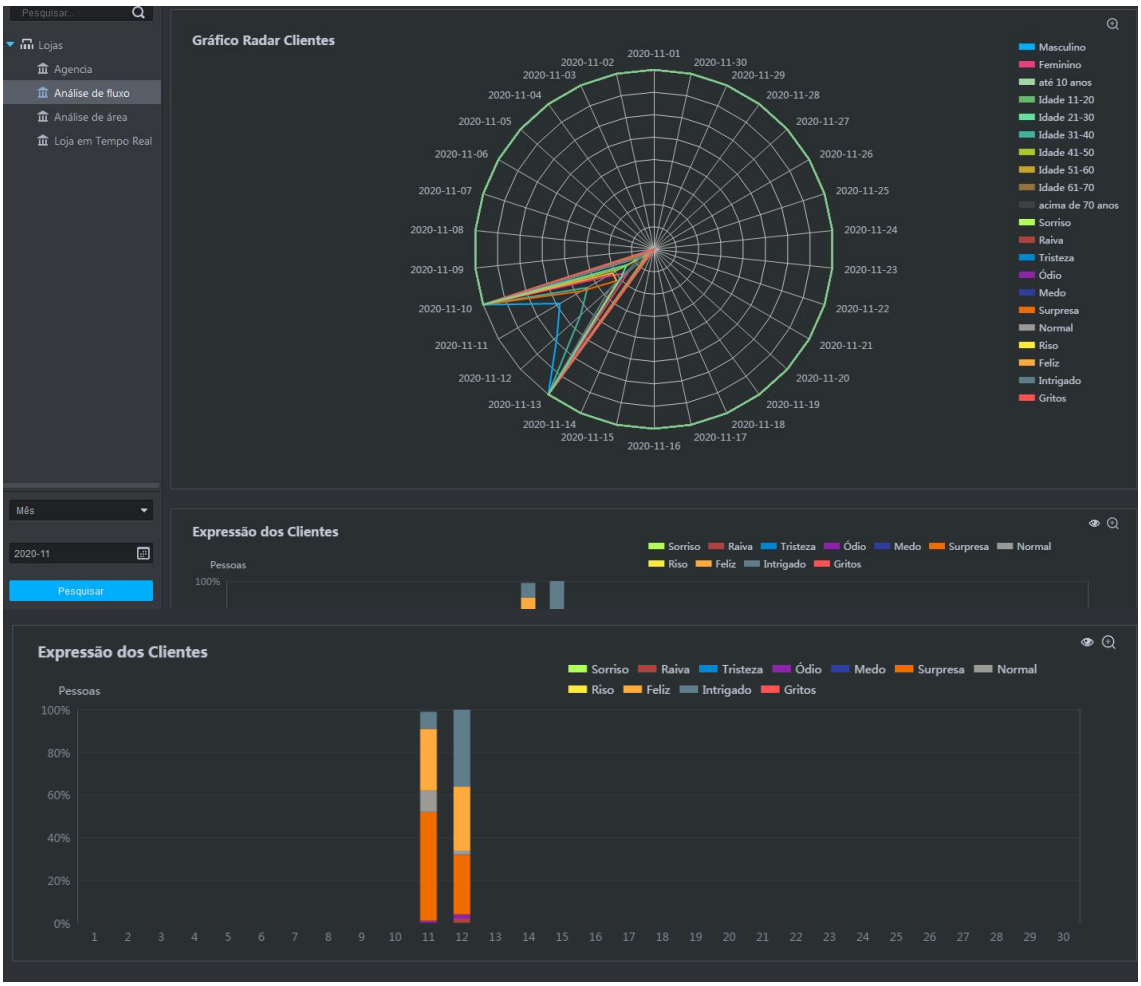
Em “Lojas” selecionamos Análise de fluxo, selecionamos o período desejado e buscamos os relatórios.



3.7.4.2 Demografia de clientes

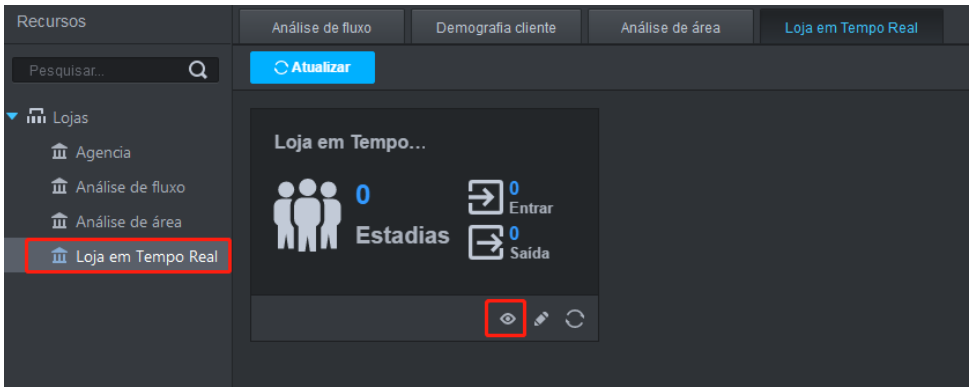
Em “Lojas” selecionamos Demografia cliente, selecionamos o período desejado e buscamos os relatórios.





3.7.4.3 Loja em tempo real

Em “Lojas” selecionamos Loja em tempo real, selecionamos a loja desejada e clique no ícone do Olho para visualizar a ocupação.



Livre

Atenção

Pare

3.8 CONFIGURANDO N + M

Para configurar N + M, ative os sub-servidores no servidor principal e confirme a relação entre os sub-servidores e os servidores sobressalentes. Essa solução garante que quando um Servidor Auxiliar tenha problemas, um outro servidor sobressalente atue no local do servidor auxiliar com problemas, de maneira a não afetar o funcionamento do sistema em casos de problemas.

Certifique-se de que todos os servidores estejam bem instalados antes de iniciar a configuração do N + M.

Passo 1. Faça login na interface Web do servidor principal.

Passo 2. Clique + e selecione **Gerenciamento do servidor> Configuração do servidor**. Os sub-servidores estão desabilitados por padrão.

Passo 3. Clique em OFF próximo a cada sub-servidor para habilitar todos os sub-servidores.

Quando desativado, o status do servidor é mostrado como **Offline**; quando habilitado e se o servidor funcionar normalmente, seu status é mostrado como **Running**.

Passo 4. Defina servidores específicos como servidores sobressalentes.

1. Clique ⚙ de cada sub-servidor.
2. Selecione o **Servidor sobressalente** na lista suspensa Tipo de servidor. Clique em **OK**.

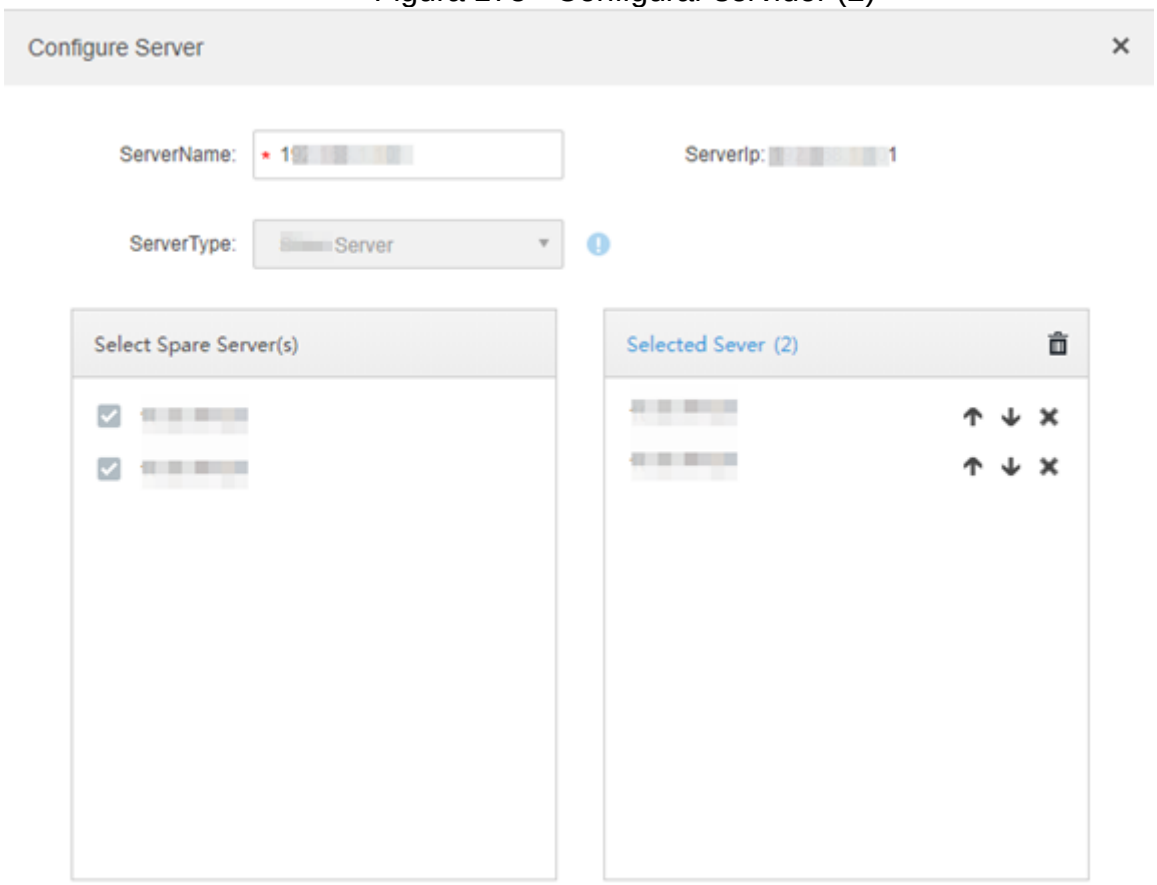
Passo 5. Configure o relacionamento entre sub-servidores e servidores sobressalentes.

Aceite os dois métodos a seguir para configurar.

- Vá para a interface **Configurar Servidor** do sub-servidor e, em seguida, selecione servidores sobressalentes. Cheque as instruções abaixo.
    1) Clique do sub servidor.
    A interface **Configuração de Servidor** é exibida.
    2) Selecione um ou mais servidores sobressalentes na lista **Selecionar servidor (es) sobressalentes.**

Os servidores selecionados estão listados à direita. Clique para ajustar a prioridade.

Figura 175 - Configurar servidor (2)



3) Clique **OK.**
Ir para a interface de **Configuração do Servidor** do servidor sobressalente e, em seguida, selecione os sub-servidores. Olhe instruções abaixo.

4) Clique do servidor sobressalente.
A interface de **Configuração do Servidor** é exibida.

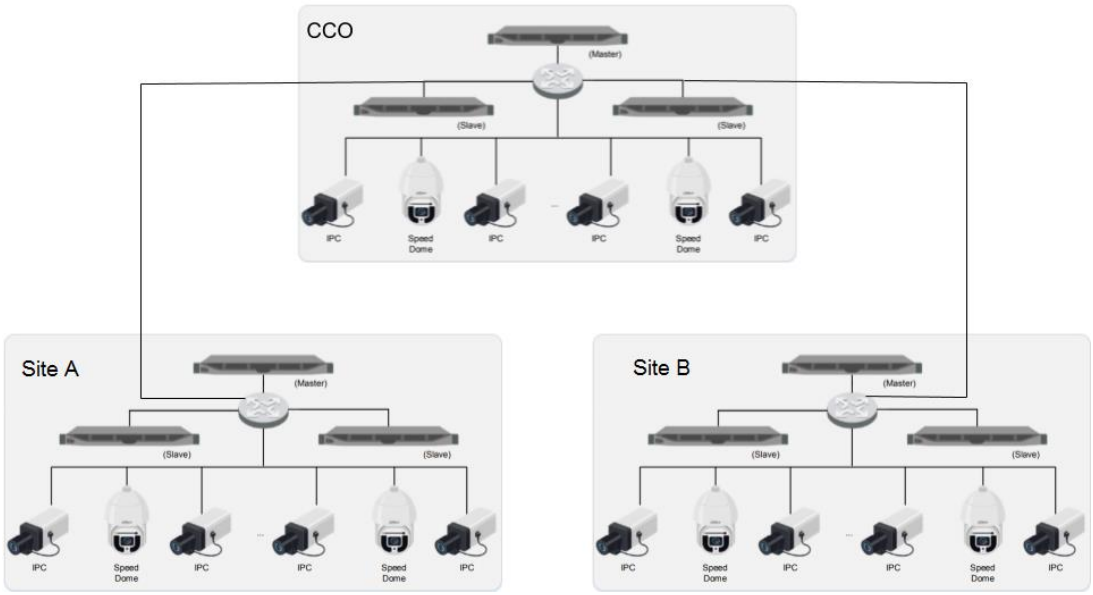
5) Selecione um ou mais sub-servidores da lista **Selecionar Sub-servidor (es).**
Os servidores selecionados são listados à esquerda. Clique para ajustar a prioridade.

6) Clique **OK.**

3.9 CASCATA

Arquitetura cascateada:

Figura 176 - Ilustração de arquitetura cascateada.



O Defense IA possui a topologia cascateada, no qual permite que Servidores de Níveis Superiores (no exemplo, o CCO) possam visualizar Visualizações ao Vivo (Live-Stream) e gravações de vídeo dos servidores de níveis inferiores. Para licenciar e configurar o sistema cascateado, deve-se adicionar licenças de Domínio nos Servidores de Níveis mais altos, permitindo então que os mesmos possam enxergar os Servidores de níveis inferiores. O sistema hoje suporta até 3 níveis de cascateamento com limite de 20 servidores master para esse tipo de arquitetura.

A arquitetura cascateada é mais utilizada em sistemas de múltiplos sites (localizações) e que possuem a necessidade de uma central de monitoramento unificada (ou acesso as câmeras de níveis inferiores de uma central principal). Nessa arquitetura, não são necessárias conexões em rede local entre servidores master, porém é recomendado uma conexão estável, de baixa latência e com boas velocidades de upload e download (condizente com o *throughput* necessário para a operação).

Os únicos eventos que são possíveis de serem encaminhados dos Servidores em Níveis inferiores para os de Nível Superior são os dos menus de Canais de Vídeo e Canais Inteligente.

Cada Servidor Master em cenário cascateado é considerado um sistema a parte, ou seja, se a conexão entre um servidor Master e o servidor Master do nível superior cair, ambos os sistemas se mantem operáveis.

É possível fazer a utilização da arquitetura distribuída e cascateada ao mesmo tempo. Dessa forma, se possuí a possibilidade de expansão de cada um dos servidores cascateados, aumentando a performance/capacidade de cada um dos sistemas individuais.

1ª observação: O Defense IA não possuí suporte nativo a aplicações em nuvem.

2ª observação: Para o dimensionamento do sistema, deve-se atender as especificações de hardware (Ex: velocidade de escrita e leitura dos discos de armazenamento devem atender throughput requerido para armazenamento das gravações em cada cenário).

3ª observação: Limites de cada uma das arquiteturas descritos no Datasheet e na seção Capacidades do Sistema.

3.9.1 Instalação do Defense IA

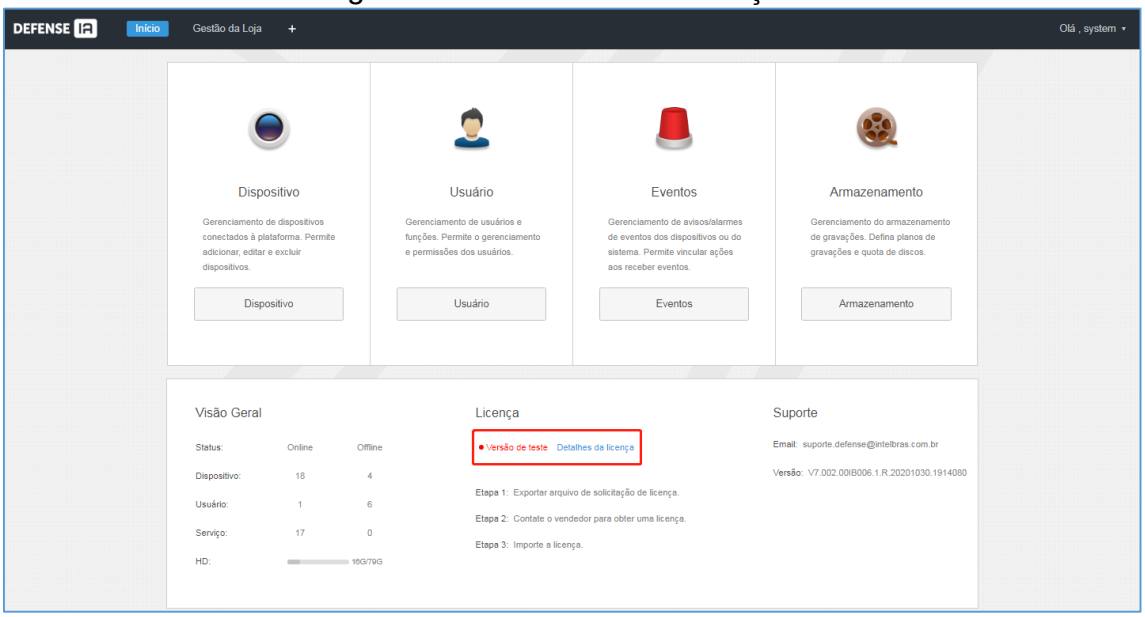
Como primeiro passo, deve-se instalar o Defense IA (Master) em todos os PC's/Servidores que irão utilizar a arquitetura cascateada. Feito isso, pode-se adotar ambas as estratégias a seguir: Adicionar as câmeras pertencentes de cada um dos servidores e depois configurar o Domínio; configurar o domínio e depois configurar as câmeras em cada um dos servidores.

Garanta que a versão do Defense IA é V7.002.00IB006.1.R.20200807 ou superior.

3.9.2 Licenciamento

Confirme se a versão do Defense IA possuí licenças de Domínio, clique em "Detalhes da licença" e confirme se o Módulo BI está ativo, conforme imagens abaixo.

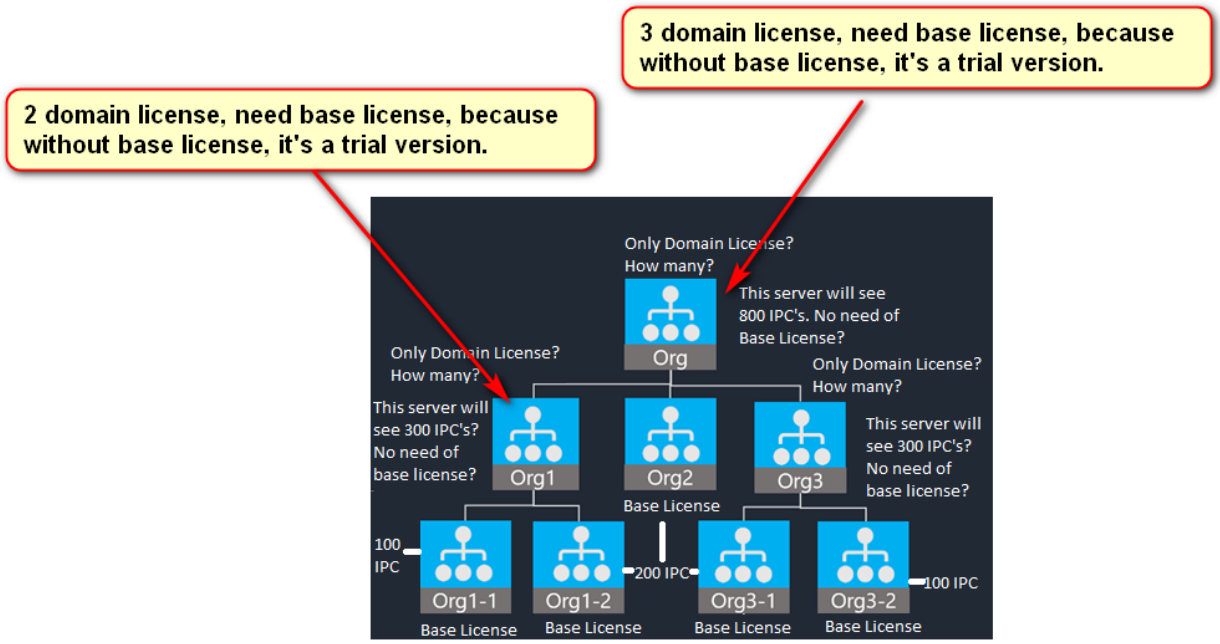
Figura 177 - Detalhes da licença



Para cada servidor que estiver conectado em níveis abaixo e que desejam ser enxergados na estrutura pelo Servidor em nível superior, deve-se possuir uma licença de domínio. Usando o exemplo da imagem 3, seriam necessárias ao menos 2 licenças de Domínio para poder adicionar os 2 servidores (Site A e Site B) que estão abaixo do mesmo (CCO). Lembrando que como são sistemas independentes, cada um dos sistemas também depende de ter ao menos uma licença Master (licença base).

Imagem de referência para casos de 3 níveis (número máximo de níveis):

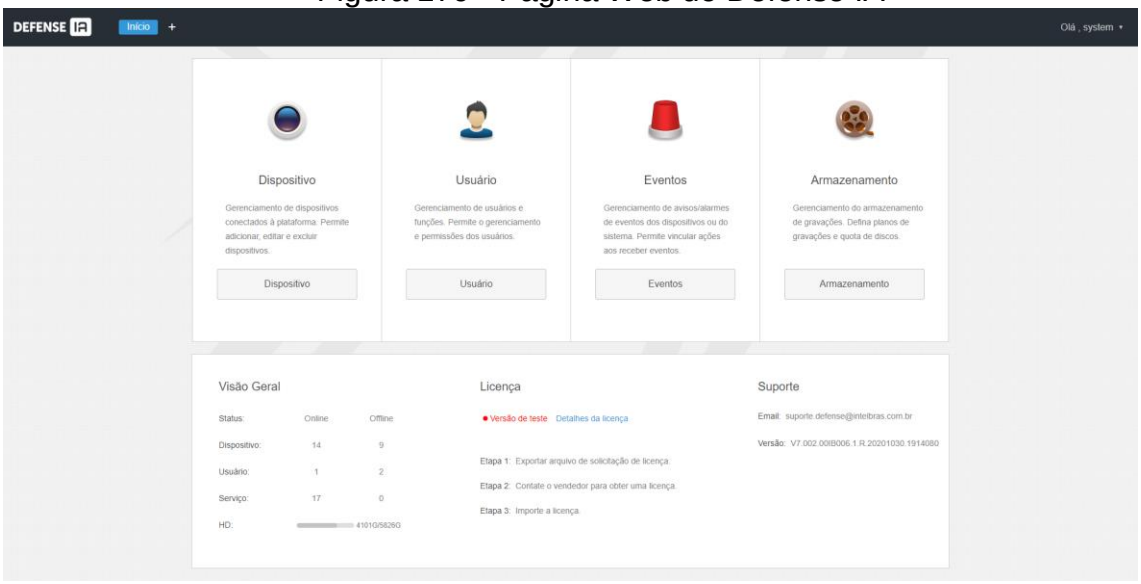
Figura 178 - Cascateamento e licenças requisitadas.



3.9.3 Configuração de Domínio

I. Abra a página web do(s) Servidor(es) que ficarão no topo da arquitetura cascateada. Tomando a Imagem 3 como referência, entraremos na página web do servidor CCO.

Figura 179 - Página Web do Defense IA

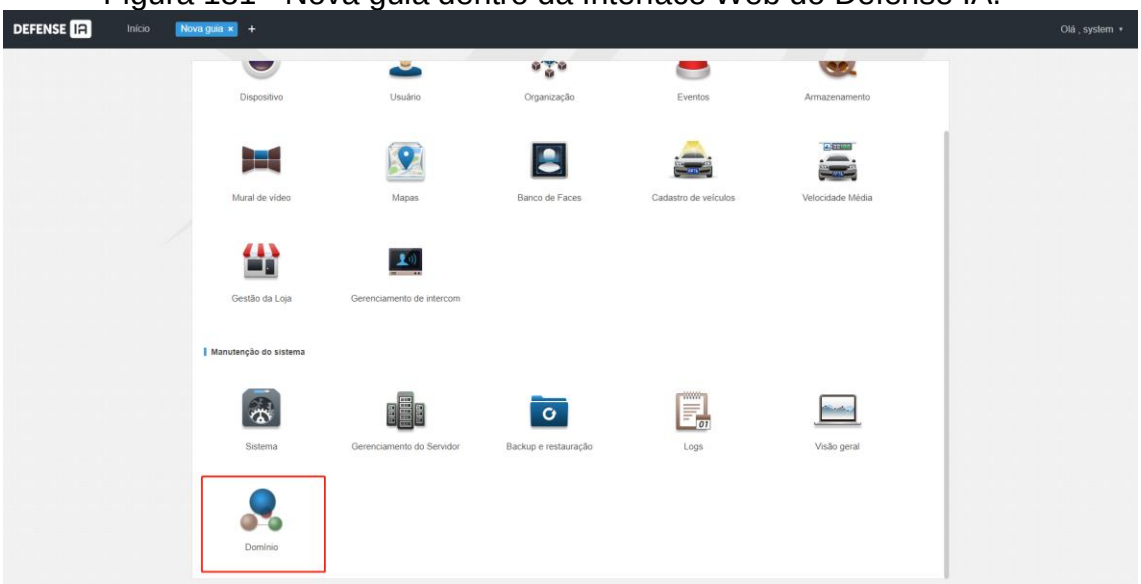


II. Clique no “+”.

Figura 180 - Página Web do Defense IA.

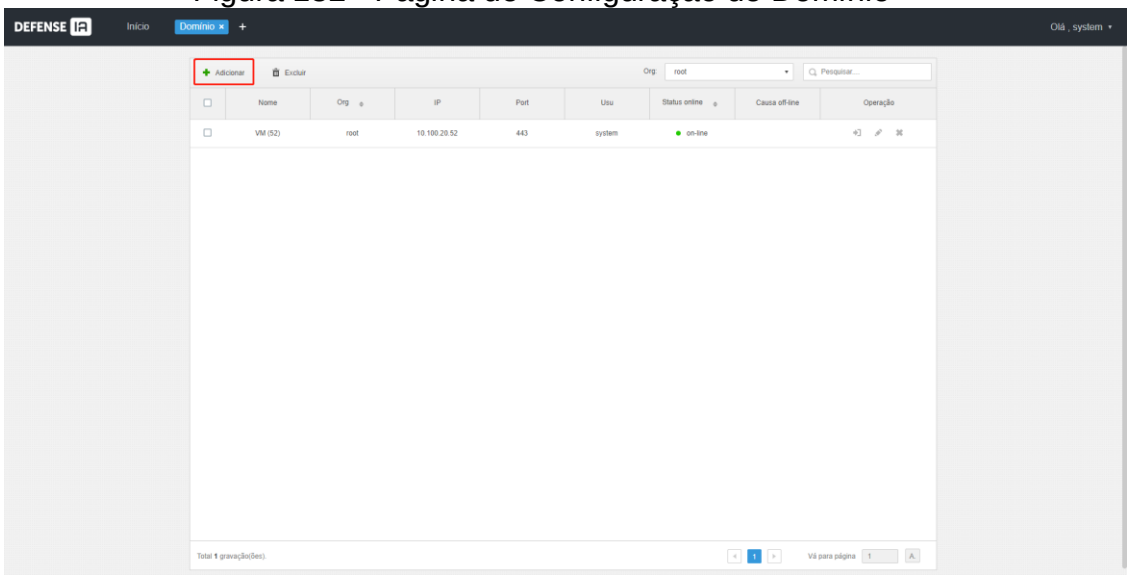
III. Role a página e clique na opção do menu “Domínio”.

Figura 181 - Nova guia dentro da Interface Web do Defense IA.



IV. Clique no botão “Adicionar”.

Figura 182 - Página de Configuração de Domínio



I. Digite um Nome para o Servidor adicionado.

II. Escolha uma Organização a qual o servidor será pertencente.

III. Mantenha o Protocolo de Domínio padrão (Intelbras).

IV. Insira o Endereço IP referente ao Servidor que estará abaixo do servidor em que se está sendo adicionado. Pensando na “Imagem 3”, IP do Site A (primeiramente).

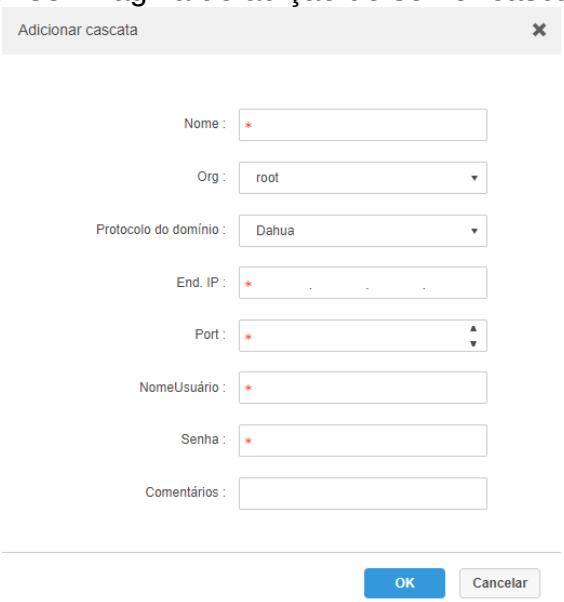
V. Informe em “Porta: ” a porta HTTPs do Servidor Master que está sendo adicionado ao cascateamento (Porta HTTPs do Site A – usando “Imagem 3” como referência).

VI. Informe em “Nome do Usuário” e “Senha” as credenciais do sistema. De preferência, utilizar o usuário “system” e a senha referente a esse usuário.

VII. Caso tenha interesse, no campo “Comentários”, você pode inserir uma descrição do Servidor sendo adicionado.

VIII. Clique em “OK”.

Figura 183 - Página de adição de server cascata.



I. Espere de 1 a 2 minutos até o “Status Online” aparecer “Online” em verde.

Figura 184 - Servidor adicionado e Online. Estrutura cascateada iniciada.

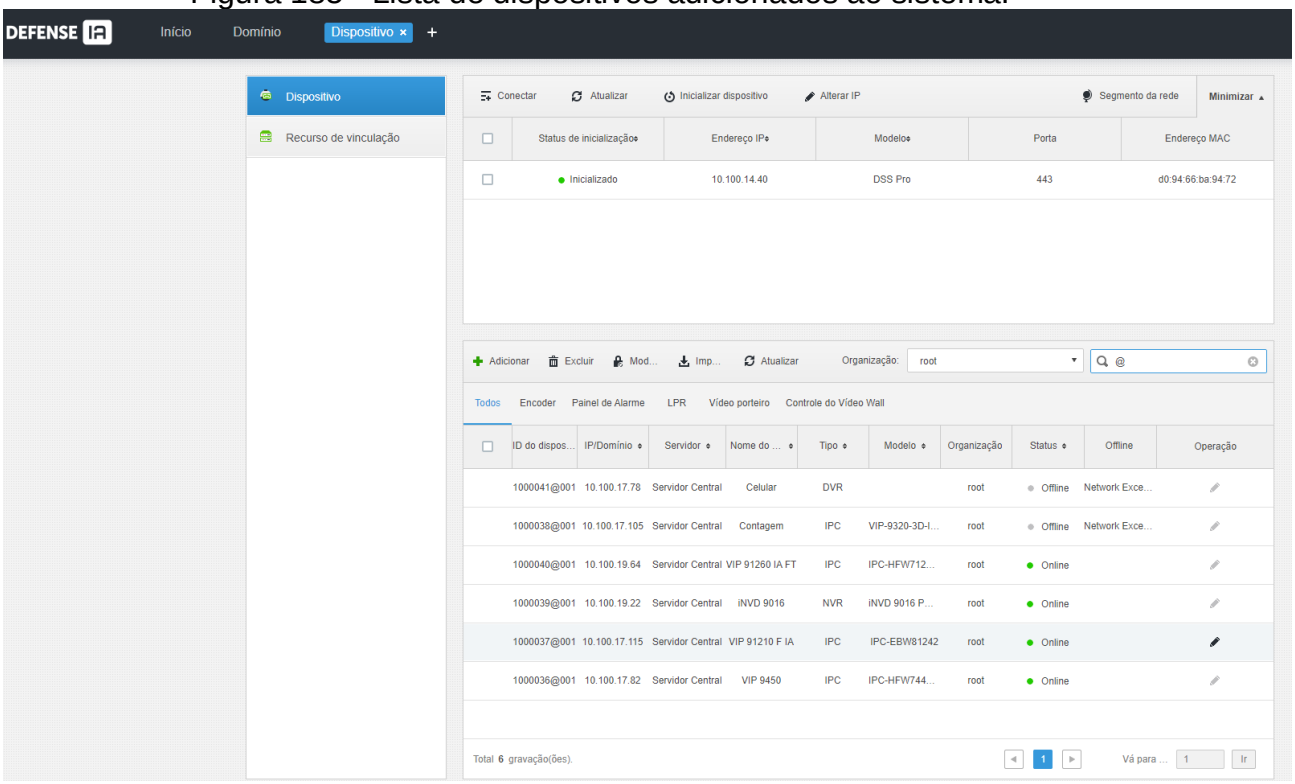
II. Servidor foi adicionado com sucesso. Agora repita as etapas 4 até 14 para todos os servidores de nível inferior ao Servidor em questão.

III. Repita as etapas 1 até 14 para servidores que estejam abaixo dos servidores no segundo nível (lembrando que a arquitetura cascateada tem limite de 3 níveis).

3.9.4 Usabilidade do domínio

I. Na aba dispositivos, todos os dispositivos adicionados em servidores que estão em níveis mais baixos do Cascateamento, devem aparecer na lista de dispositivos, além dos dispositivos que foram adicionados diretamente ao Servidor sendo acessado em página Web. Os dispositivos que são visualizados de outros servidores, devem vir com o símbolo @ no ID do dispositivo. O número antes do @ é o ID do dispositivo e após o @ é o ID do Servidor no qual o dispositivo foi adicionado originalmente. Dessa forma, pode-se identificar quais câmeras pertencem a quais servidores.

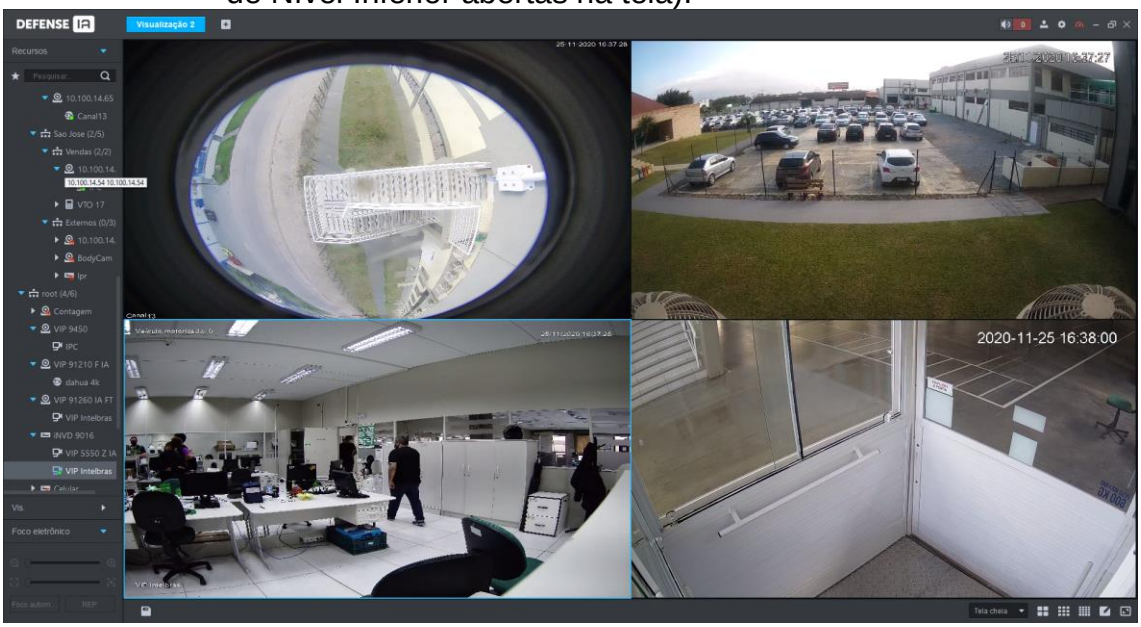
Figura 185 - Lista de dispositivos adicionados ao sistema.



Para receber eventos (com as limitações informadas no “Capítulo 1”), deve-se configurar os eventos em ambos os servidores – no de nível inferior e superior – se configurado apenas em um deles, o evento não será recebido nos níveis superiores.

II. Quando logado no Defense IA Client (nos servidores os quais possuem servidores adicionados em níveis inferiores), será possível ter acesso a todos os dispositivos adicionados em servidores de níveis inferiores ao atual nas páginas de Visualização e Reprodução. Além disso, o usuário terá acesso completo a todos os outros dispositivos adicionados no servidor que está sendo acessado de maneira direta.

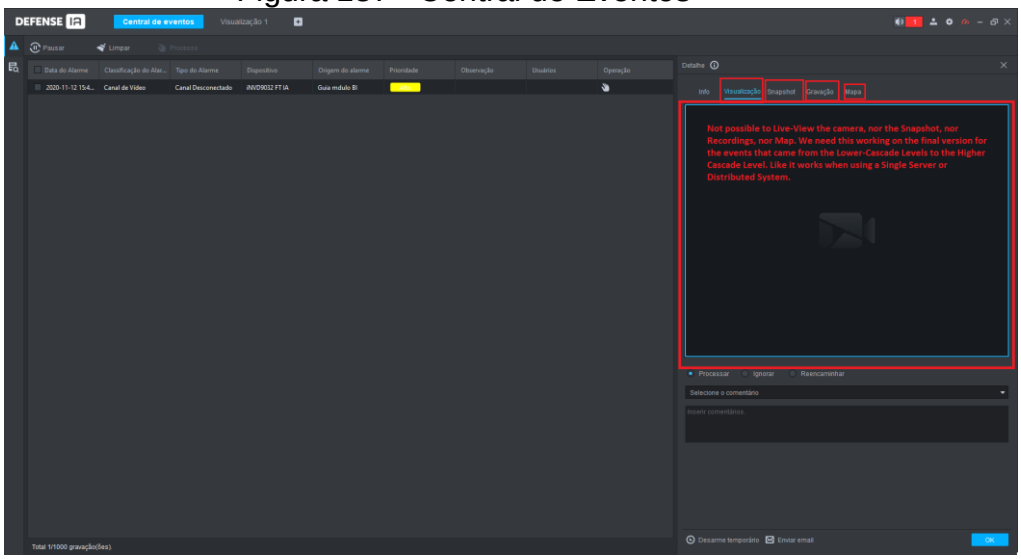
Figura 186 - Client rodando com Câmeras adicionadas do Modo Cascata (Câmeras de Nível Inferior abertas na tela).



Importante lembrar: Os únicos eventos que são possíveis de serem encaminhados dos Servidores em Níveis inferiores para os de Nível Superior são os dos menus de Canais de Vídeo e Canais Inteligente.

O Defense IA recebe os eventos no modo cascateado, porém os eventos de dispositivos adicionados em servidores de nível inferior não trazem Vídeo ao Vivo, Snapshots, Gravação ou Mapa **na Central de Eventos**. Isso significa que na Central de Eventos só se recebe a informação de que os Eventos ocorreram (assim como “Origem do Alarme”, “Horário”, Tipo do “Alarme”, “Status do Alarme” e etc.).

Figura 187 - Central de Eventos



3.10 GRAVAÇÃO E REPRODUÇÃO

Você pode pesquisar e reproduzir os registros armazenados no dispositivo ou no servidor.

3.10.1 Preparativos

- Dispositivos como câmeras e NVRs ou DVRs devem estar configurados.
- O Defense IA estar configurado.
- Os dispositivos ou Defense IA gravando vídeos.

3.10.2 Reprodução

Reprodução de gravações de vídeos

3.10.2.1 Reproduzindo Vídeos Gravados

Passo 1. Faça login no Defense Client e selecione a aba Reprodução de gravação.

Figura 188 - Reprodução de gravação

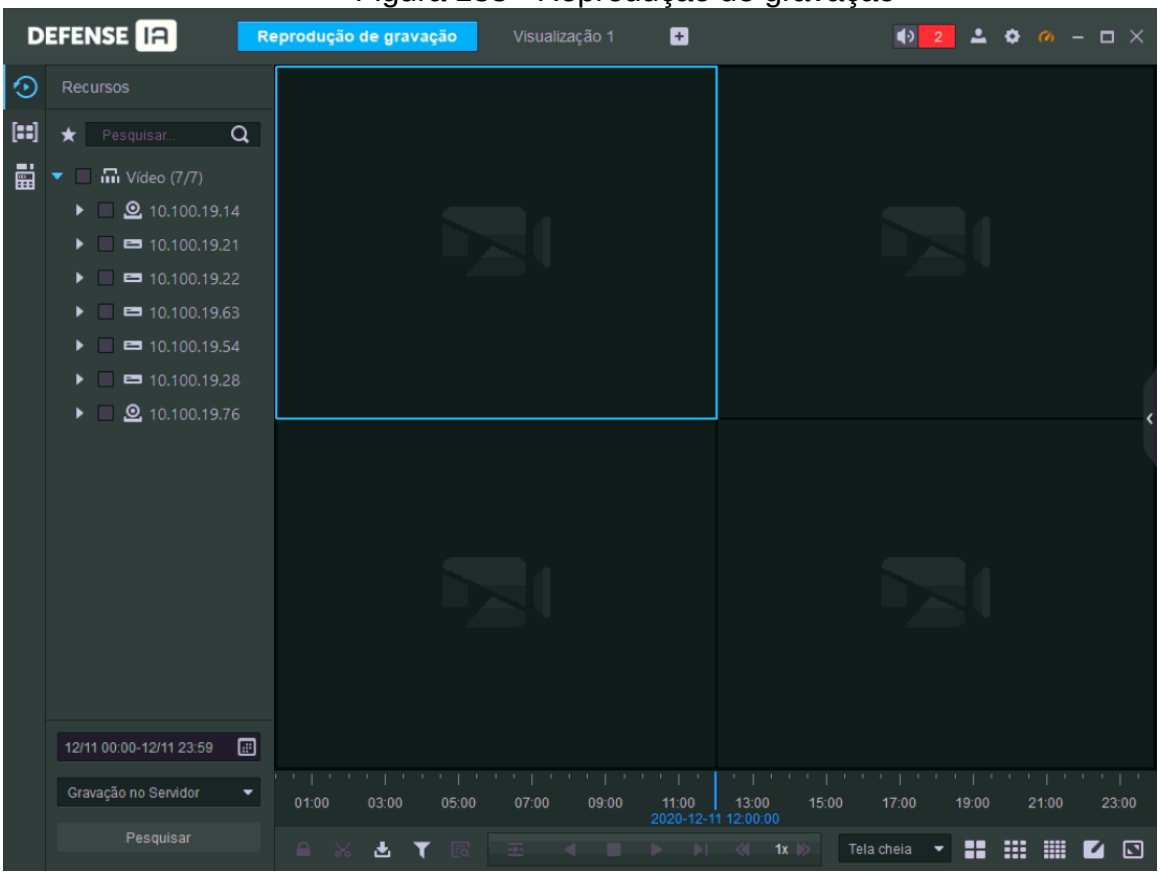


Tabela 28 - Parâmetros reprodução de gravação

Ícone	Descrição
	Trave o vídeo armazenado no servidor dentro de algum período do canal designado. O vídeo bloqueado não será substituído quando o disco estiver cheio.
	Cortar vídeo
	Download do vídeo
	Filtro de vídeo de acordo com o tipo de gravação.
	Faça uma análise de detecção dinâmica em alguma área da imagem gravada, apenas reproduz o vídeo com a imagem dinâmica na área de detecção.
	Arquivos de gravação de reprodução do mesmo período de canais diferentes em janelas selecionadas.
	Parar/pausar a reprodução
	Reprodução quadro a quadro/retrocesso quadro a quadro.
1x	Reprodução rápida/lenta. Máx. suporta 64X ou 1/64X.
10:00 12:00 14:00 16:00 2018-07-18 12:16:09	Durante a reprodução, você pode arrastar a barra de progresso de tempo para reproduzir a gravação em um momento específico.

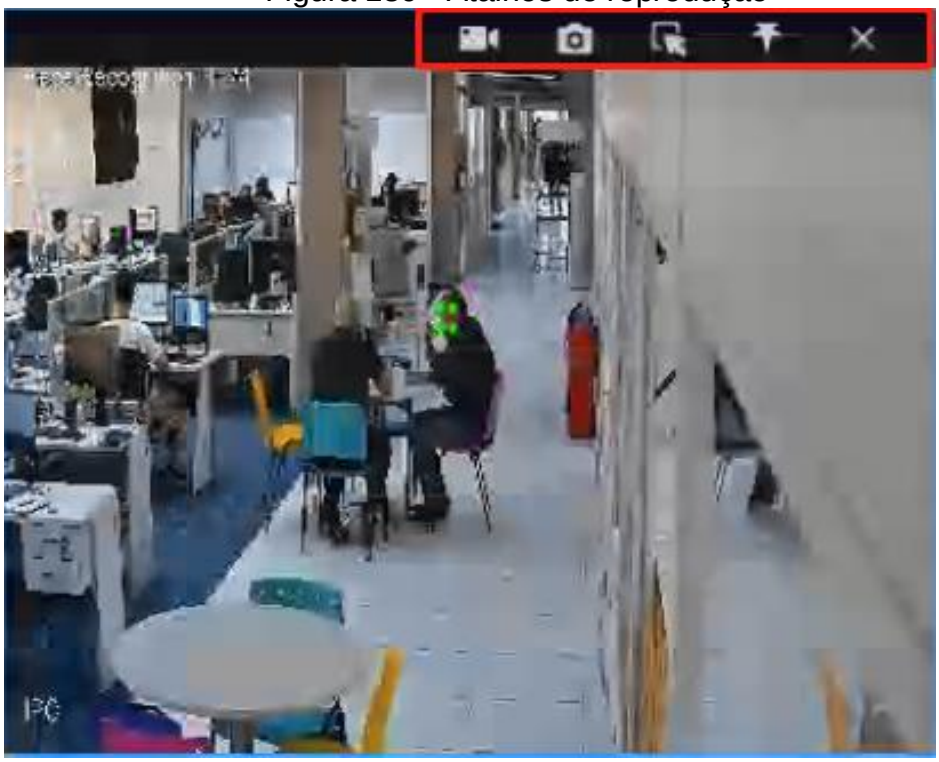
Passo 2. Selecione um canal na árvore de dispositivos.

Passo 3. Selecione a data e a posição de armazenamento do registro. Clique em Pesquisar. Pontos azuis no calendário indicam que existe arquivos de vídeo.

Passo 4. Selecione uma janela que contenha vídeo e clique para reproduzir.

Passo 5. Passe o mouse sobre o vídeo e os ícones aparecem. Você pode realizar as seguintes ações.

Figura 189 - Atalhos de reprodução



-

Tabela 29 - Parâmetros de atalhos de reprodução

Ícone	Nome	Descrição
	Gravar etiquetagem	Marque os vídeos de interesse para facilitar a pesquisa no futuro.
	Gravação Local	Clique neste ícone para iniciar a gravação. O vídeo gravado é armazenado localmente. O caminho para salvar é " C:\Defense IA\Client\Record" por padrão.
	Snapshot	Clique neste ícone para tirar uma foto. A foto é armazenada localmente. O caminho para salvar é " C:\Defense IA\Client\Picture" por padrão.
	Zoom in	Selecione uma seção para ampliar e ver os detalhes.
	Fechar	Fecha a janela

- Clique com o botão direito do mouse no vídeo e execute as seguintes ações.

O menu de atalho varia dependendo da funcionalidade da câmera. O real deve prevalecer.

Figura 190 - Menu de atalho

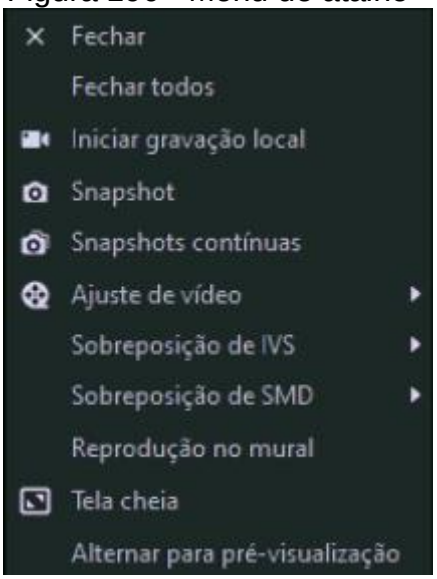


Tabela 30 - Parâmetros de menu de atalhos

Nome	Descrição
Fechar	Fecha a janela atual
Fechar todos	Fecha todas as janelas de reprodução
Iniciar gravação local	Grava áudio e vídeo da janela de vídeo atual e salve-os localmente.
Entrada de áudio	Se a câmera tiver mais de um canal de entrada de áudio, você pode selecionar um ou selecionar o áudio mixado. Esta configuração é eficaz tanto com visualização ao vivo quanto com reprodução.
Snapshot	Clique neste ícone para tirar uma foto. A foto é armazenada localmente. O caminho para salvar é " C:\Defense IA\Client\Picture" por padrão.
Snapshots contínuas	Tire um instantâneo da imagem atual (três instantâneos de cada vez por padrão).
Ajuste de vídeo	Faça o ajuste e o aprimoramento do vídeo.

Nome	Descrição
Sobreposição de IVS	O Defense client não mostra linhas de sobreposição sobre o vídeo ao vivo por padrão. Quando necessário, você pode clicar em Sobreposição de AI e ativar Sobreposição de regra e Sobreposição de objeto e, em seguida, o vídeo ao vivo mostra linhas de sobreposição se as regras de detecção de IA estiverem habilitadas no dispositivo. Esta configuração é efetiva com o canal selecionado atualmente tanto na exibição ao vivo quanto na reprodução.
Sobreposição de SMD	Habilite a sobreposição de SMD para mostrar o quadro alvo sobre o vídeo ao vivo. Quando SMD está habilitado no dispositivo, você pode habilitar sobreposição de SMD para o canal do dispositivo, e então o vídeo ao vivo exibirá quadros de destino dinâmicos. Esta configuração é efetiva com o canal selecionado atualmente tanto na exibição ao vivo quanto na reprodução.
Desativar máscara de privacidade	Para uma câmera que oferece suporte ao mascaramento de privacidade de rosto humano, você pode desativar o mascaramento aqui para visualizar a imagem do rosto.
Reprodução no mural	Reproduza o canal atual no vídeo wall.
Tela cheia	Mude a janela de vídeo para o modo de tela inteira. Para sair da tela inteira, clique duas vezes na janela do vídeo ou clique com o botão direito para selecionar sair da tela inteira.
Alternar para pré-visualização	Vai para tela de Visualização ao vivo desse mesmo canal.

3.10.2.2 Filtro de tipo de gravação

Faça filtros para o vídeo de acordo com o tipo de gravação, o tipo de gravação inclui gravação programada; registro de alarme e registro de detecção de movimento.

Passo 1. Faça login no Defense Client e selecione a aba Reprodução de gravação.

Passo 2. Na janela de reprodução de gravação, defina as condições de pesquisa para pesquisar vídeos. Selecione uma janela que contenha vídeos e clique em .

Figura 191 - Interface reprodução de gravação

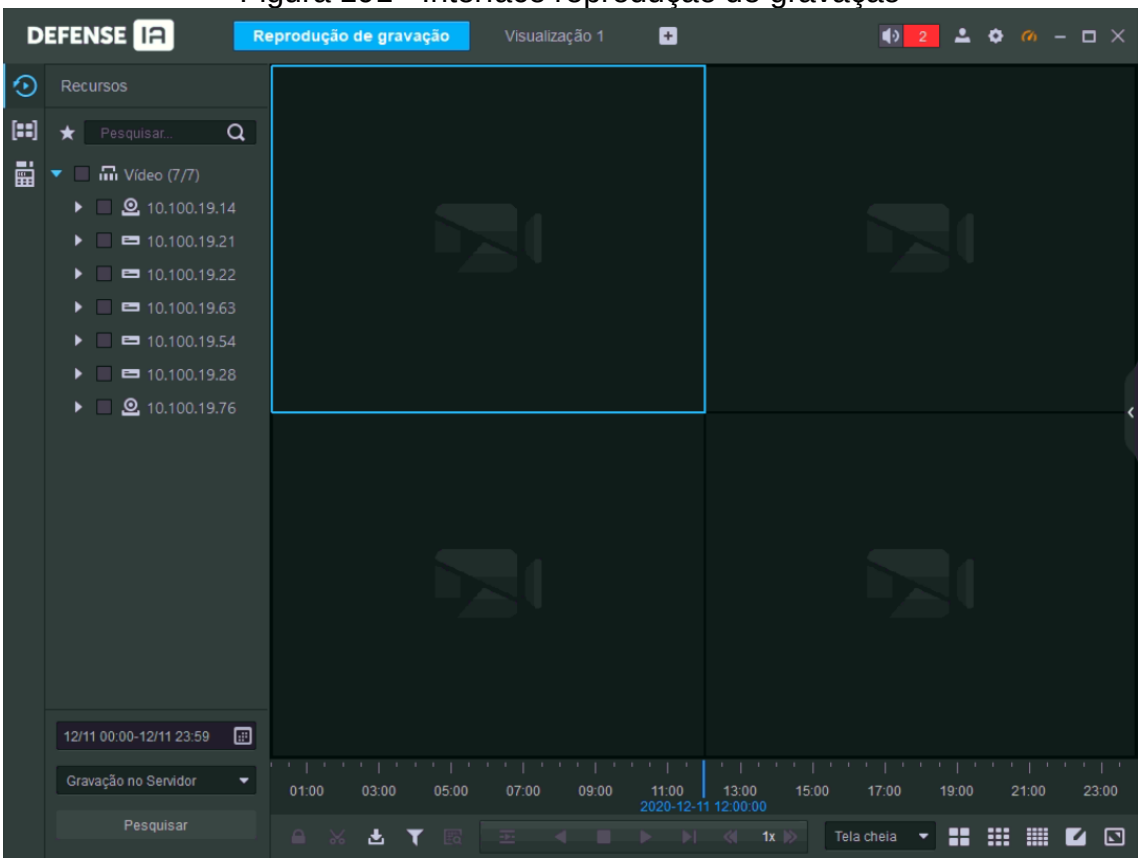
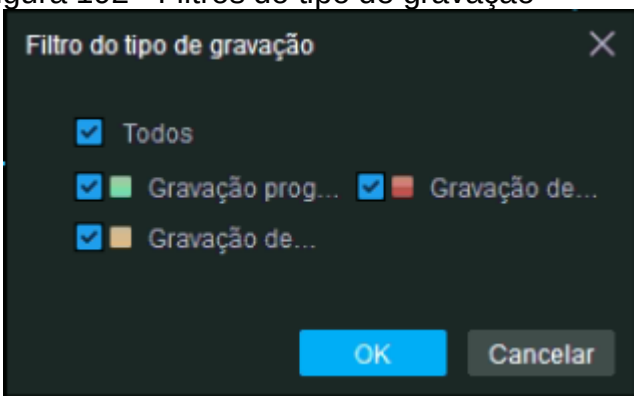


Figura 192 - Filtros do tipo de gravação



Passo 3. Selecione um tipo (ou tipos) de registro e clique em **OK**.
Passo 4. O sistema exibe apenas o vídeo do tipo selecionado.

3.10.2.3 Pesquisa Inteligente

Com a função Pesquisa Inteligente, você pode selecionar uma zona de interesse na imagem de vídeo para visualizar os registros de movimento nesta seção. A câmera

relevante é necessária para suportar a Pesquisa Inteligente; caso contrário, o resultado da pesquisa será nulo.

Passo 1. Faça login no Defense Client e selecione a aba Reprodução de gravação.

Passo 2. Na interface de reprodução de gravação, defina as condições de pesquisa para pesquisar vídeos. Selecione uma janela que contenha vídeos. Clique em e selecione um tipo.

A interface de pesquisa inteligente é exibida. Quadrados 22×18 são exibidos na janela.

III.

Figura 193 - Pesquisa inteligente

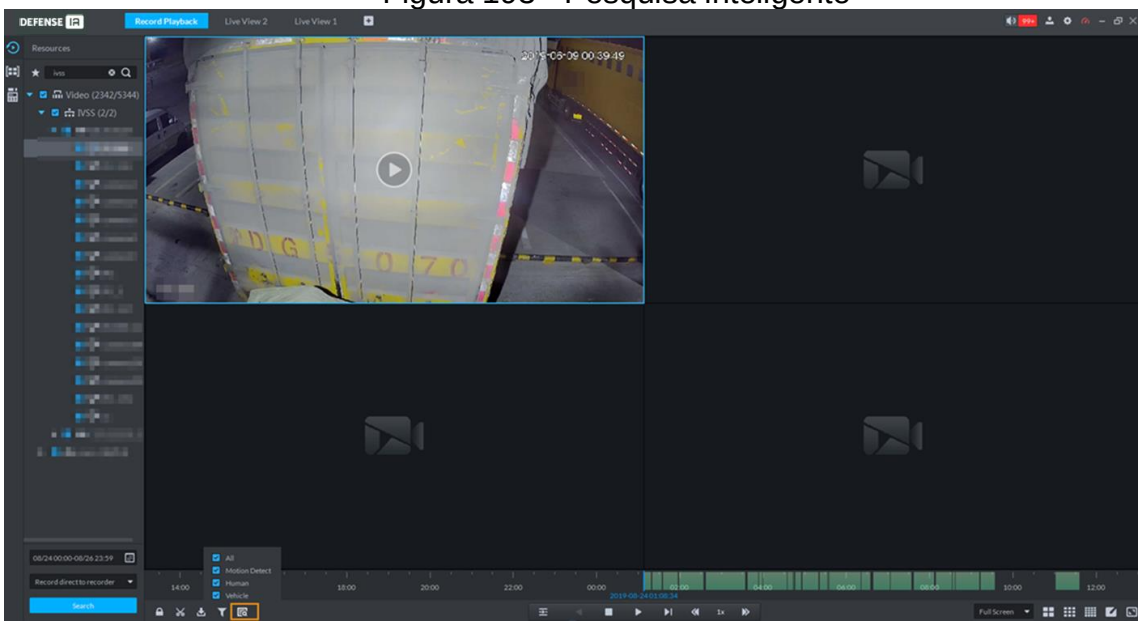
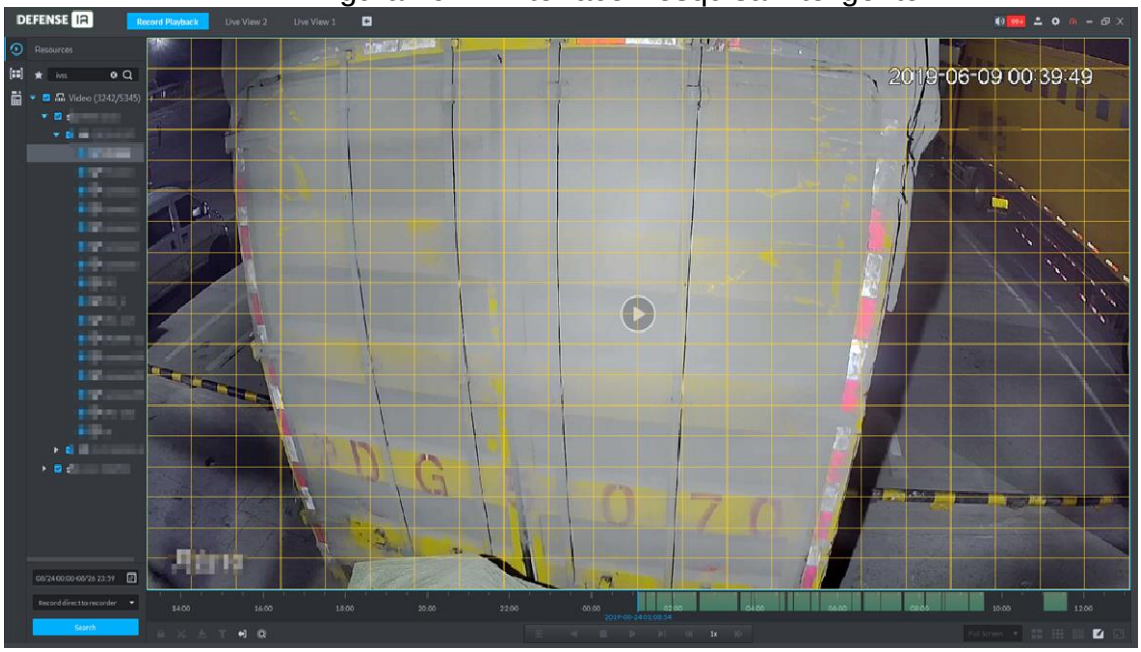


Figura 194 – Interface Pesquisa inteligente



Passo 3. Clique nos quadrados e selecione as áreas de detecção.

IV.

- Selecione a área de detecção; Mova o ponteiro do mouse para a imagem, pressione o botão esquerdo do mouse e arraste o mouse para selecionar o quadrado.
- Para a área selecionada, clique novamente ou selecione o quadrado para cancelá-la.

Passo 4. Clique  e começar a análise de pesquisa inteligente.

- Se houver resultado da pesquisa, a barra de progresso de tempo ficará roxa e exibirá um quadro dinâmico.
- Se não houver nenhum resultado da pesquisa ou se o dispositivo de reprodução selecionado não for compatível com a pesquisa inteligente, ele informará que o resultado da pesquisa inteligente é nulo.

Clique  e você pode selecionar novamente a área de detecção.

Passo 5. Clique no botão play na imagem ou barra de controle.
O sistema reproduz os resultados da pesquisa. Os resultados da pesquisa são marcados em roxo na linha do tempo.

Passo 6. Clique  para sair da Pesquisa Inteligente.

3.10.2.4 Bloqueio de Gravações

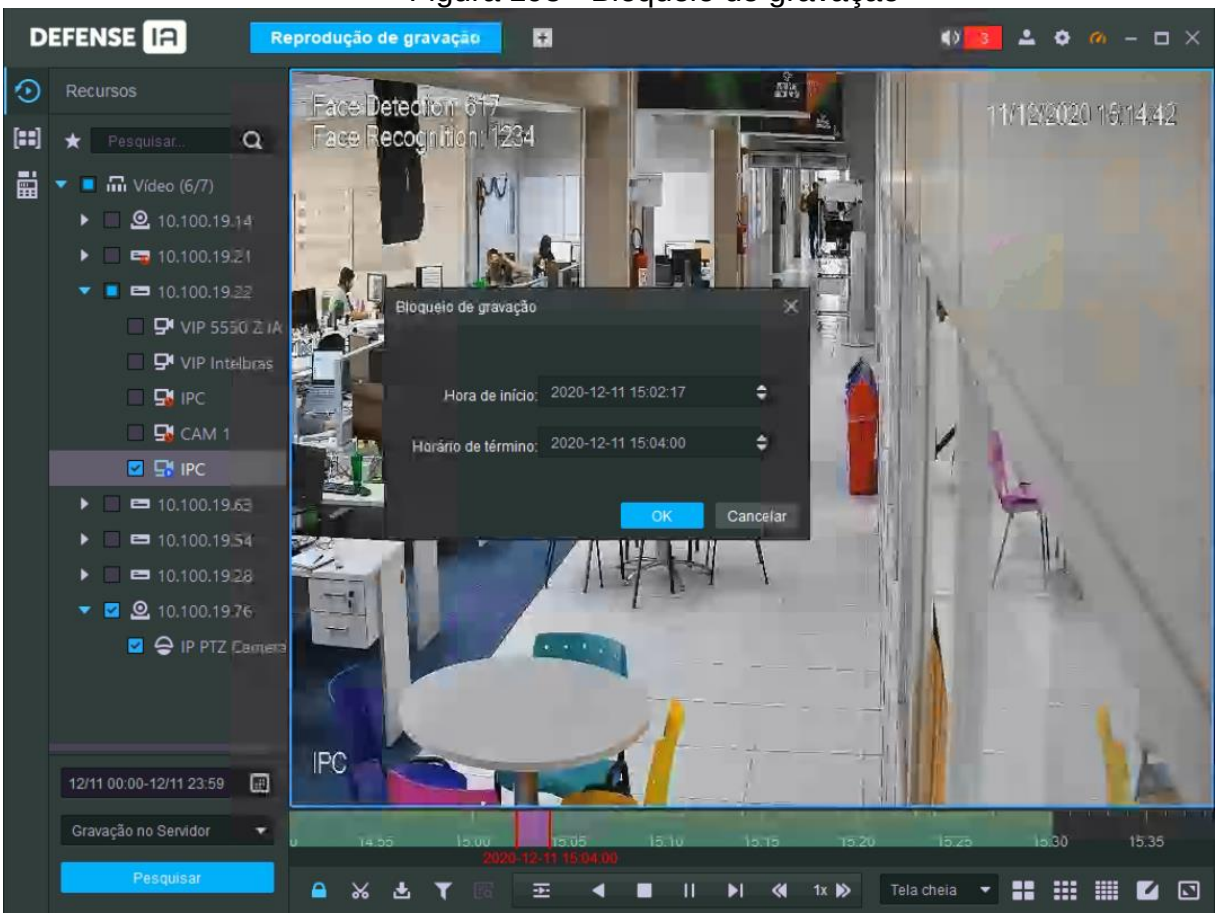
Trave o vídeo armazenado no servidor dentro de algum período de canal específico. O vídeo bloqueado não será substituído quando o disco estiver cheio.

Você só pode bloquear o vídeo central armazenado no servidor.

Passo 1. Faça login no Defense Client e selecione a aba **Reprodução de gravação**.

Passo 2. Defina as condições de pesquisa e clique em pesquisar. Selecione uma janela que tenha o vídeo gravado e clique em  na parte inferior da interface Gravar Reprodução e, a seguir, clique na linha do tempo para marcar o ponto inicial e final do videoclipe de que você precisa.

Figura 195 - Bloqueio de gravação



Passo 3. Confirme a hora de início e de término e clique em **OK**.

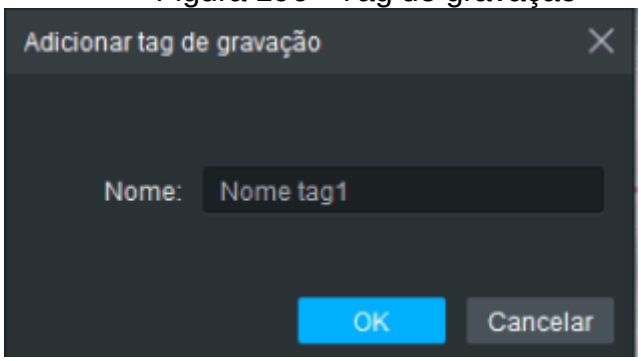
3.10.2.5 Tag de gravação

Você pode marcar registros de interesse para uma pesquisa rápida.

Passo 1. Faça login no Defense Client e selecione a aba **Reprodução de gravação**.

Passo 2. Na interface de reprodução de gravação, mova o ponteiro do mouse para a janela que está reproduzindo a gravação. Clique em no canto superior esquerdo.

Figura 196 - Tag de gravação



Passo 3. Nomeie a tag e clique em **OK**.

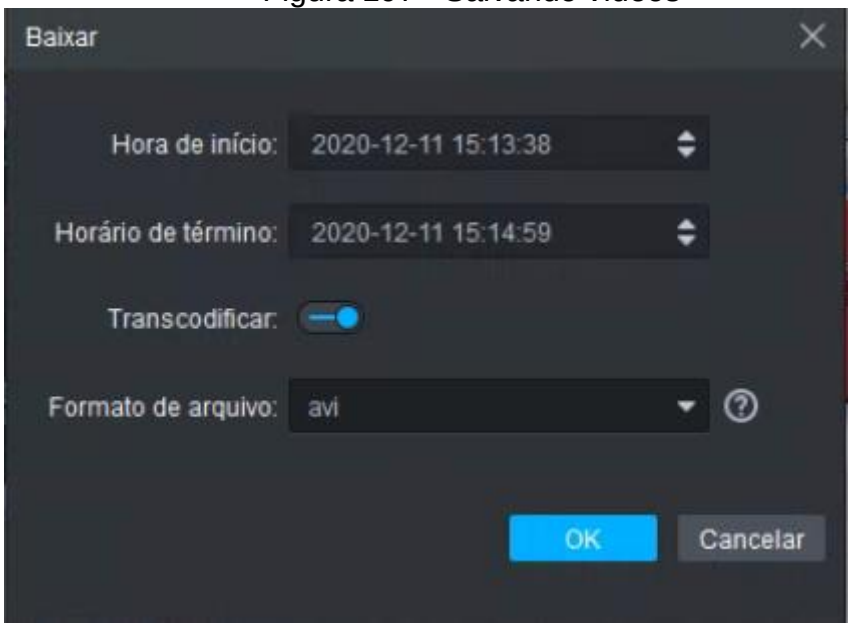
3.10.2.6 Cortando vídeos

Passo 1. Faça login no Defense Client e selecione a aba **Reprodução de gravação**.

Passo 2. Clique em na parte inferior da interface de reprodução de gravação (certifique-se de que haja gravação na janela).

Passo 3. Na linha do tempo, clique para selecionar o horário de início e término.

Figura 197 - Salvando vídeos



Passo 4. Defina o formato do arquivo e clique em **OK.**

3.10.2.7 Central de downloads

Você pode baixar os vídeos de interesse armazenados no servidor ou no dispositivo. Os vídeos baixados estão no formato .avi, mp4 ou .asf.

Existem três maneiras de baixar vídeos:

Baixe vídeos recortados da linha do tempo.

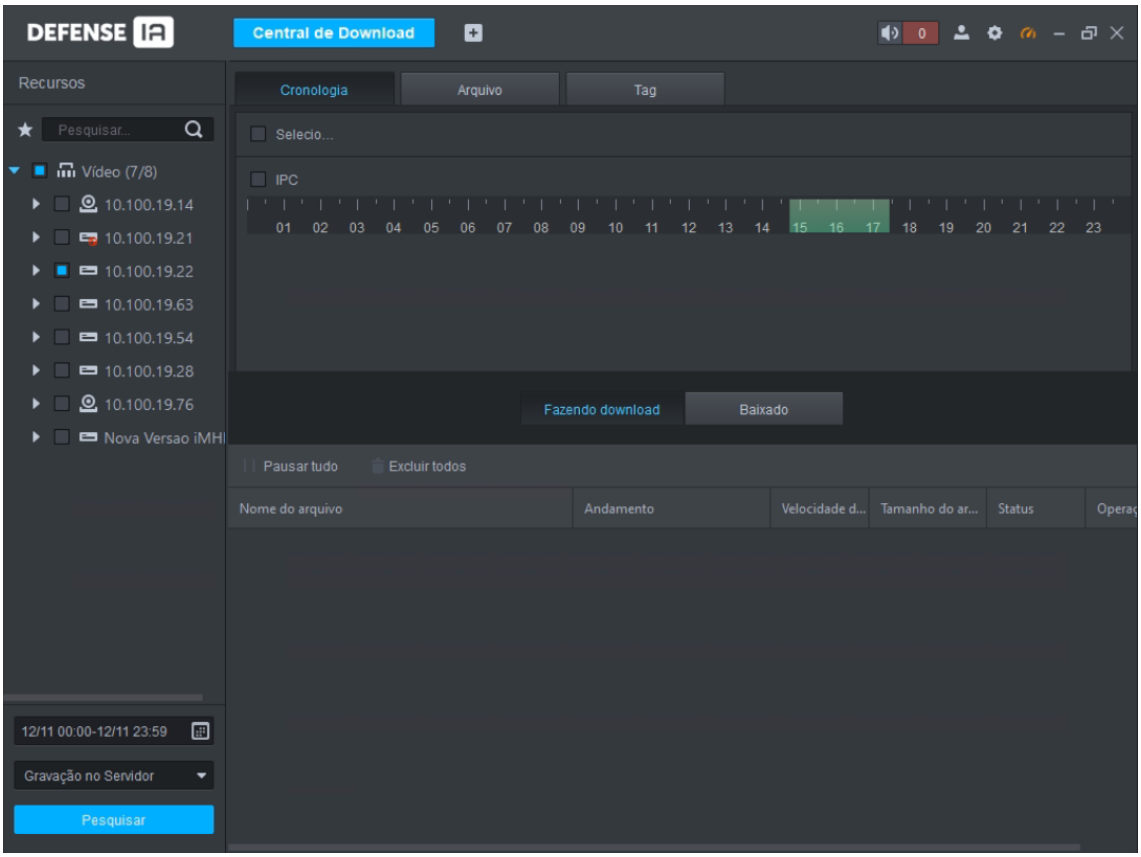
Baixe os arquivos de vídeo da central de downloads.

Baixe vídeos procurando tags de vídeo.

Passo 1. Clique em na aba de **Reprodução de gravação**, ou clique em e selecione o menu **Central de Download**.

Passo 2. Defina as condições de pesquisa e clique em **Pesquisar**.

Figura 198 - Central de download



Passo 3. Selecione os vídeos para download.

- Para baixar vídeos recortando a linha do tempo, clique na guia Linha do tempo e selecione a hora de início e término do videoclipe clicando na linha do tempo.
- Para baixar vídeos selecionando os arquivos de vídeo pesquisados, clique na guia Arquivo e, em seguida, clique em .
- Para baixar vídeos marcados com **Tag**, clique na guia **Tag** e, em seguida, clique em Baixar arquivo.

Passo 4. Caso apareça uma caixa de diálogo de verificação de senha que aparece, digite a senha e clique em **OK**.

Passo 5. Na caixa de diálogo Download de registro, confirme o intervalo de tempo e, se necessário, clique em para selecionar o formato do arquivo de vídeo e clique em **OK**.

O progresso do download é exibido. Durante o processo de download, você pode pausar, parar e cancelar a tarefa de download clicando nos ícones correspondentes.

3.10.3 Buscando por miniaturas

Você pode dividir o vídeo pesquisado em níveis e exiba na forma de miniatura, que é o ROI selecionado. Você pode visualizar o vídeo pesquisado e a mudança de imagem do ROI em diferentes momentos e realizar uma pesquisa rápida.

Passo 1. Faça login no Defense Client e selecione a aba **Reprodução de gravação**.

Passo 2. No menu de Reprodução de gravação, clique em  .

Figura 199 - Miniaturas

Passo 3. Na guia lateral de dispositivos, selecione um canal de vídeo e defina o período de pesquisa e a posição de registro. Clique  .

Há um ponto azul no canto superior esquerdo da data se o canal tiver arquivos de gravação.

Figura 200 - Selecione o período

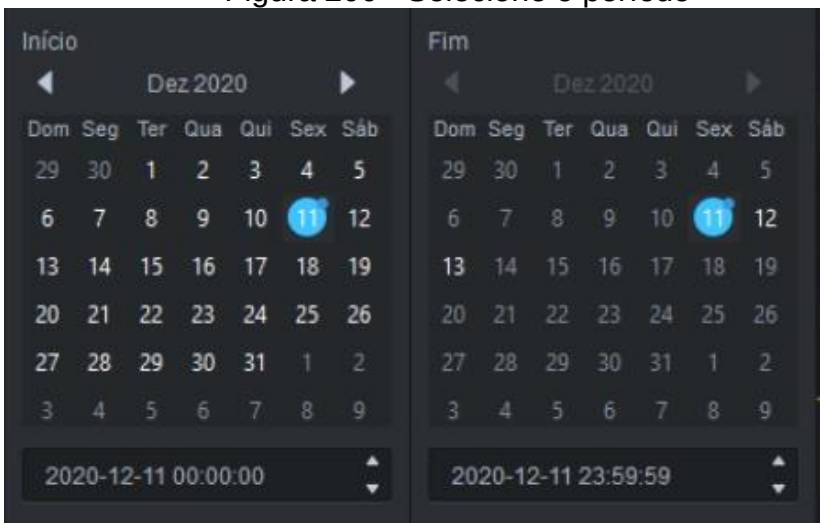
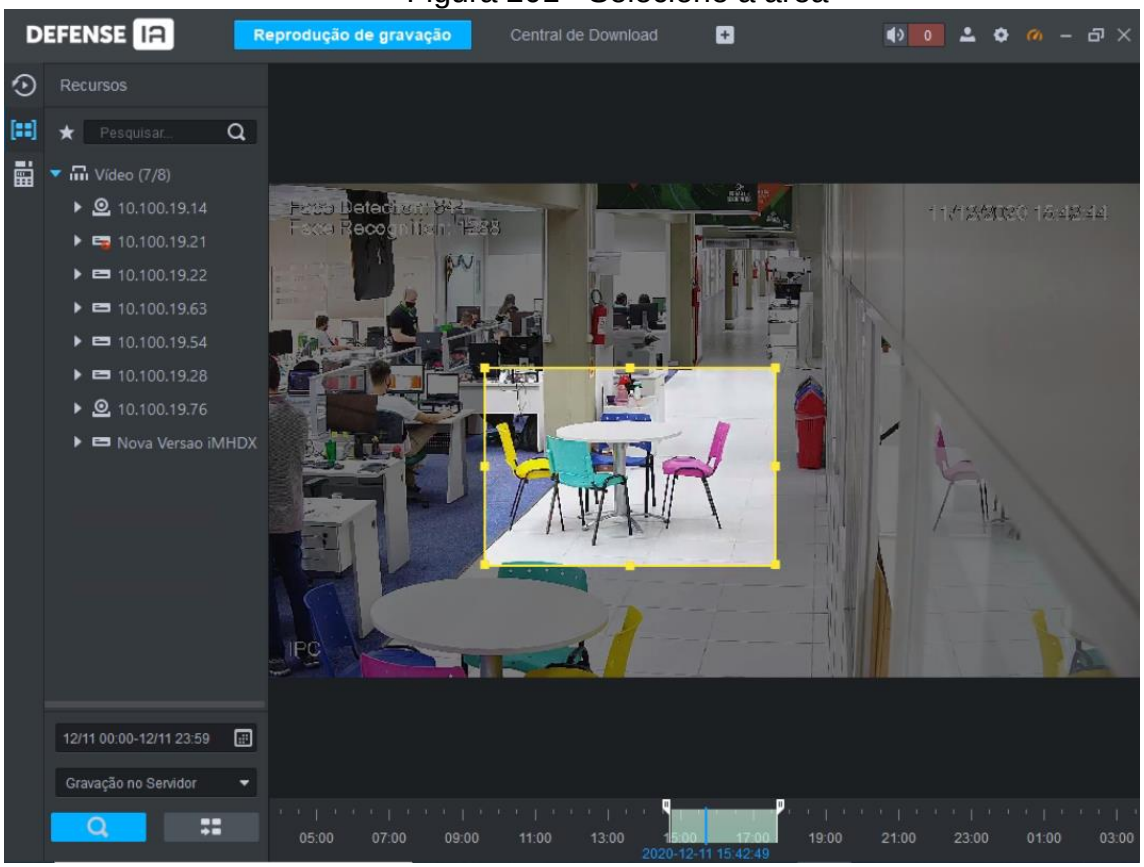
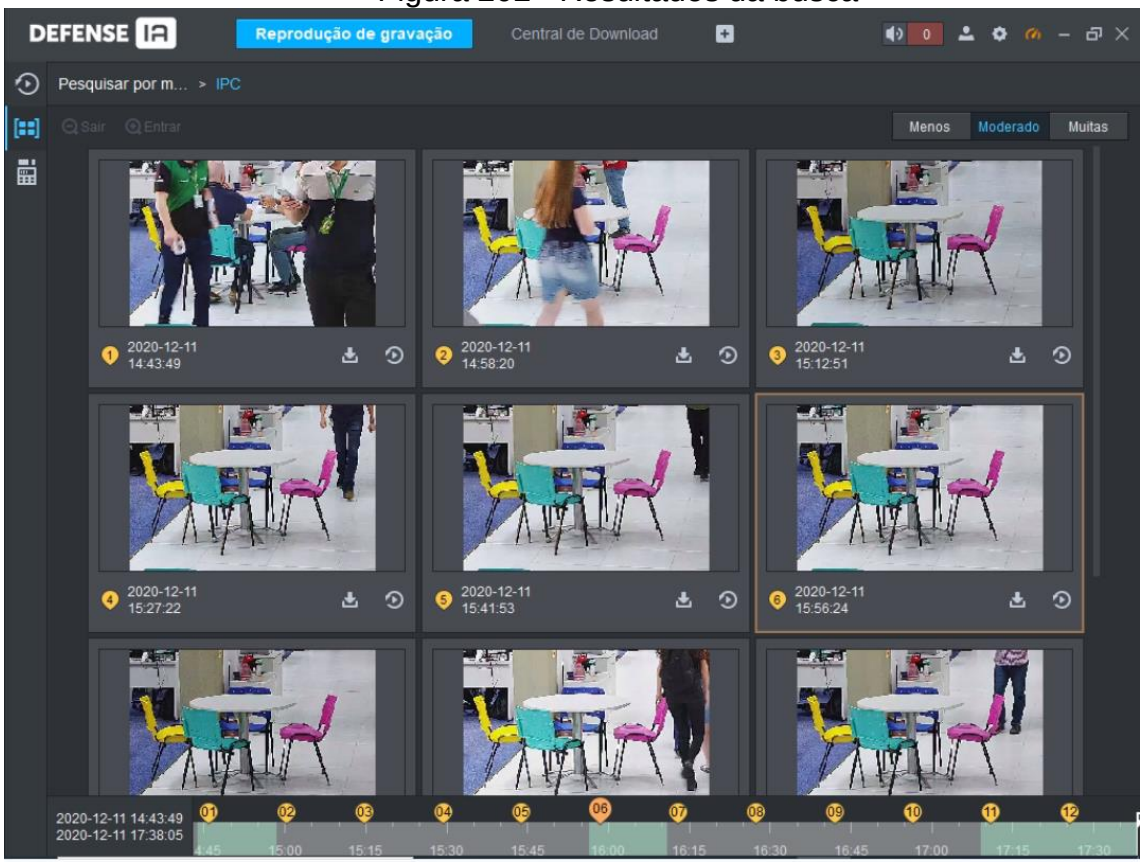


Figura 201 - Selecione a área



Passo 4. Arraste a moldura amarela para definir o intervalo de miniaturas. Clique em  .

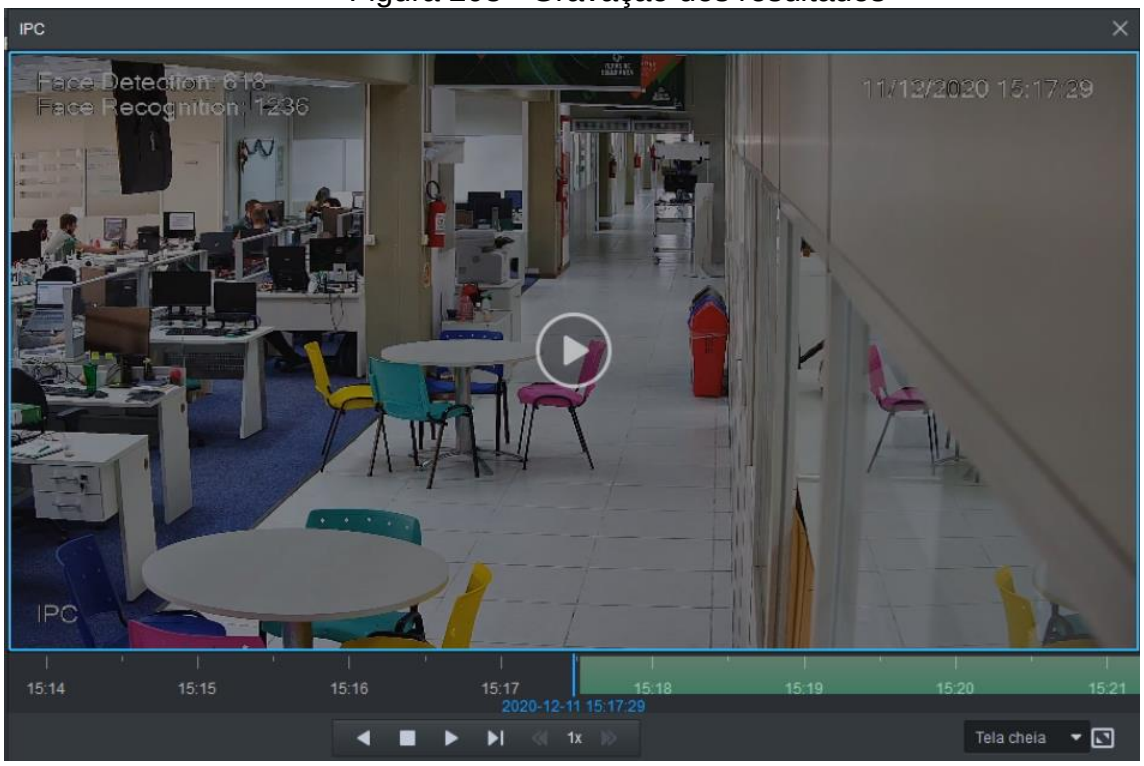
Figura 202 - Resultados da busca



- O sistema exibe os resultados da pesquisa no modo Moderado por padrão. Clique em Menos, Moderado, Muitas para ver o modo adequado.
- Dê um clique duplo na miniatura, o sistema busca novamente pelo registro entre a imagem atual e a próxima imagem.

Passo 5. Clique em no canto inferior direito da miniatura, você pode ver o vídeo correspondente relacionado à miniatura.

Figura 203 - Gravação dos resultados

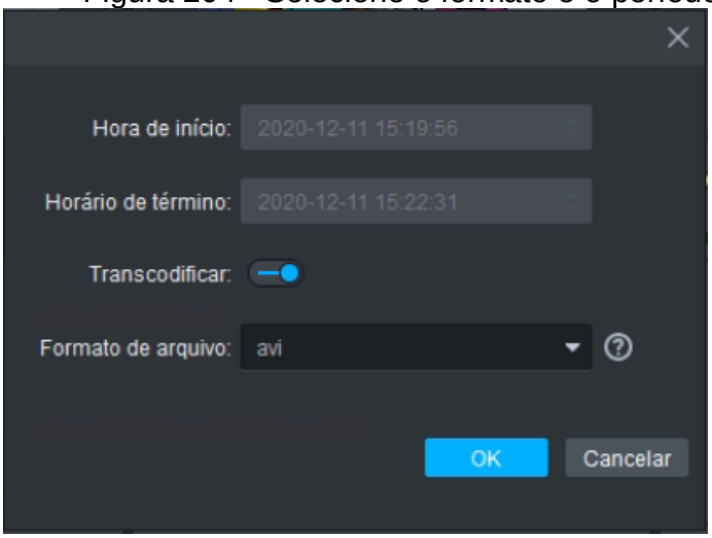


Passo 6. Download de gravação

Se houver vídeos de diferentes tipos de transmissão no período de download, eles só podem ser salvos como .dav.

1) Clique em no canto direito da miniatura, e então o sistema baixa o registro entre a imagem atual e a próxima imagem.

Figura 204 - Selecione o formato e o período



2) Selecione o formato de vídeo e então clique em **OK**.

3) Vá para a **Central de Downloads** para visualizar os detalhes do download.

3.11 CONFIGURAÇÃO DO SISTEMA

Defina as configurações do sistema, como e-mail e modo de login do dispositivo.

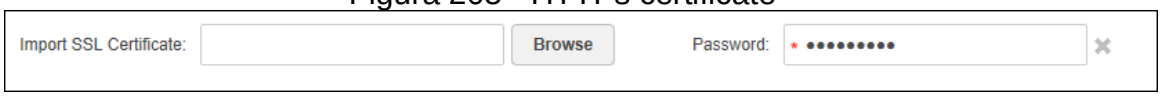
3.11.1 Certificado HTTPs

HTTPS (Hyper Text Transfer Protocol sobre Secure Socket Layer) é um protocolo de transmissão HTTP seguro. Ele fornece garantia segura e estável de informações do usuário e segurança do dispositivo. Quando o certificado HTTPS é configurado, você pode fazer login na plataforma por meio do protocolo HTTPS para garantir a segurança da transmissão.

- O certificado SSL foi criado ou adquirido e você obteve a senha.

Passo 1. Faça login no Gerenciador Web, clique em + e selecione Sistema .
Passo 2. Clique na guia HTTPS.

Figura 205 - HTTPs certificate

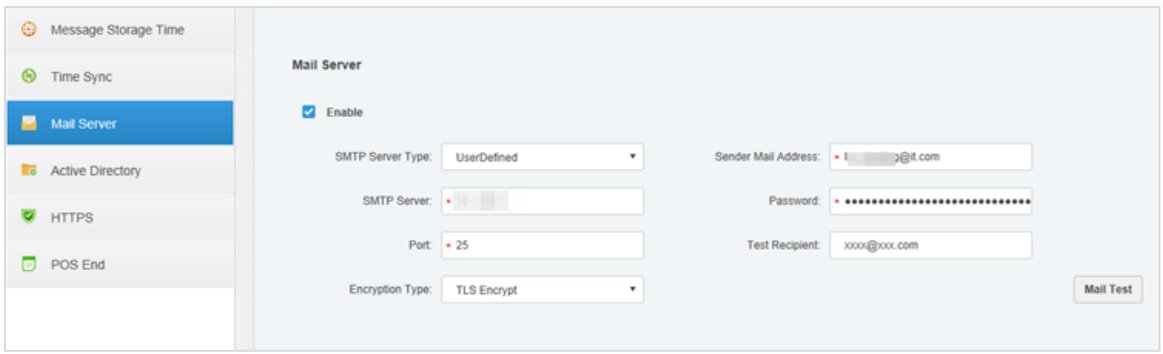


Passo 3. Clique em Procurar, importe o certificado SSL e digite a senha.
Passo 4. Clique em Salvar.

3.11.2 Configuração do servidor de correio

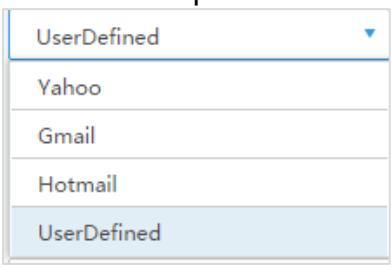
Passo 1. Clique em + no Gerenciador Web e selecione **Sistema** .
Passo 2. Selecione a guia **Servidor de e-mail** , marque **Habilitar** para habilitar a configuração de e- mail

Figura 206 - Definir o servidor de E-mail



Passo 3. Selecione o tipo de servidor de e-mail na caixa suspensa..

Figura 207 - Selecione o tipo de servidor de e-mail



Passo 4. Defina o IP do servidor de e-mail, porta, tipo de criptografia, nome de usuário / senha, remetente e destinatário de teste, etc.

Passo 5. Clique em **Teste de e-mail** para testar se a configuração do servidor de e-mail é válida. O prompt de teste será recebido se o teste for bem-sucedido, e a conta de teste receberá o e-mail correspondente.

Passo 6. Clique em Save após o teste ser bem-sucedido para salvar as informações de configuração.

3.12 GERENCIAMENTO DE SERVIDOR

O gerenciamento de servidor suporta o gerenciamento de informações do servidor, ajustando o servidor ou servidor superior do dispositivo.

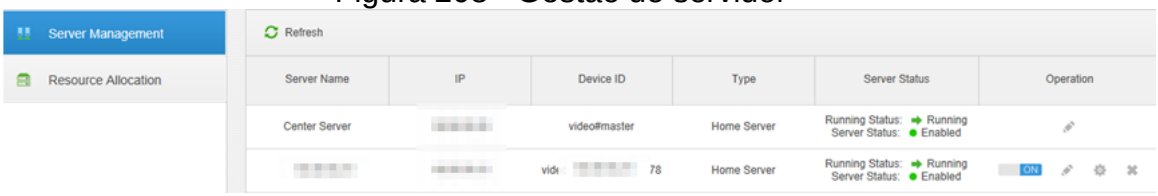
3.12.1 Gerenciamento de Servidor

O gerenciamento de servidor oferece suporte a uma série de operações, como alternar entre modo principal / sobressalente do servidor, modificação do nome do servidor, ativação ou desativação do serviço, etc.

Passo 1. Clique em + e selecione **Gerenciamento do servidor** na interface da **Nova guia**

Passo 2. Clique na guia Gerenciamento do servidor.

Figura 208 - Gestão de servidor



Passo 3. O servidor de gerenciamento suporta as seguintes operações:

- Cliquem em e edite as informações do servidor.
- OFF significa que o servidor não está habilitado; Clique no ícone e ele se torna ON, isso significa que o servidor já está habilitado.
- Clique e aloque o tipo de servidor.
- Clique e exclua as informações do servidor.

3.12.2 Configuração de recursos

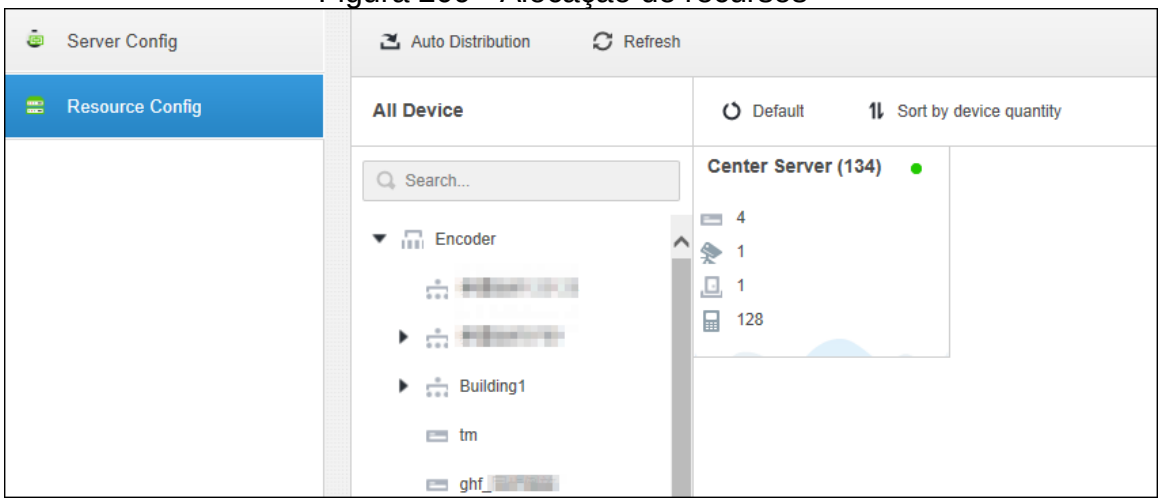
Ajuste o servidor do dispositivo durante a implantação distribuída.

Passo 1. Clique em + e selecione **Gerenciamento de servidor**.

Passo 2. Clique na guia Configuração de recursos.

- Clique em **Padrão** e os servidores serão classificados de acordo com a hora em que forem adicionados
- Clique em **Classificar por quantidade de dispositivos** e os servidores serão classificados de acordo com a quantidade de dispositivos conectados a eles.

Figura 209 - Alocação de recursos



Passo 3. Ajuste o servidor conectado.

- Ajuste manual

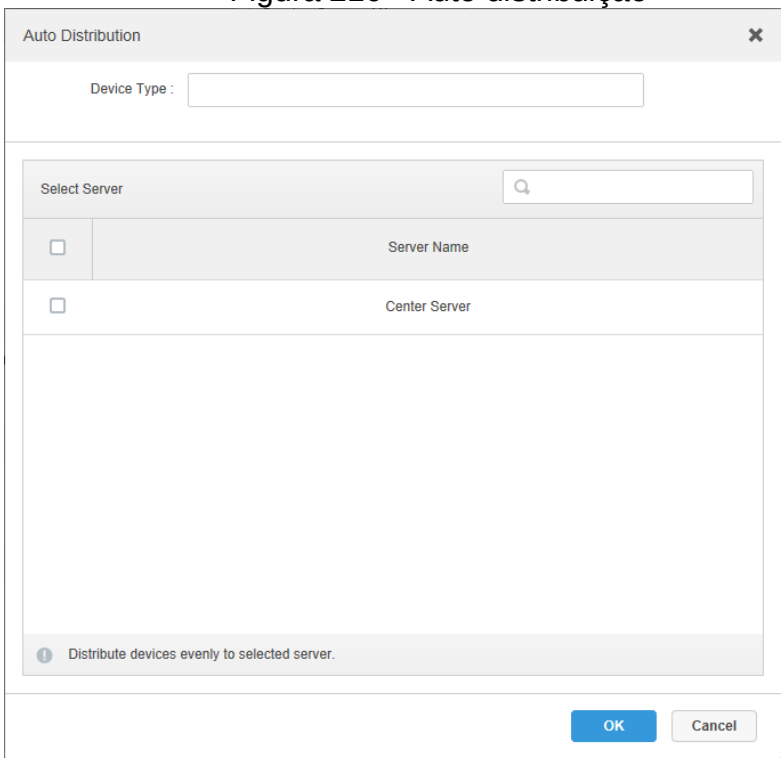
  Selecione o dispositivo à esquerda e arraste-o para o servidor à direita. A quantidade de dispositivos do servidor conectado aumentará, enquanto a quantidade de dispositivos do servidor original diminuirá.

- Distribuição Automática

  Distribua de forma média o mesmo tipo de dispositivo para o servidor que é implantado por distribuição.

I. Clique em Distribuição automática.

Figura 210 - Auto distribuição



II. Selecione os tipos de dispositivos.

III. Selecione um servidor para onde os dispositivos serão distribuídos.

IV. Clique em **OK**.

3.13 MANUTENÇÃO DE SENHA

A plataforma suporta a modificação da senha do usuário e a redefinição da senha do usuário do sistema quando ela é esquecida. Apenas o usuário do sistema pode redefinir a senha. Outros usuários, quando suas senhas são esquecidas, podem pedir ao usuário do sistema para modificar as senhas.

3.13.1 Modificando senha

Aconselhamos você a modificar sua senha regularmente para a segurança da conta.

Passo 1. Efetue login no Control Client, clique em no canto superior direito e selecione **Alterar senha** . Você também pode ir para o Web Manager, passar o mouse sobre **Olá, sistema** e selecionar **Alterar senha**

Passo 2. Insira a senha antiga, a nova senha e confirme a nova senha. Clique **OK**.

3.13.2 Redefinindo senha

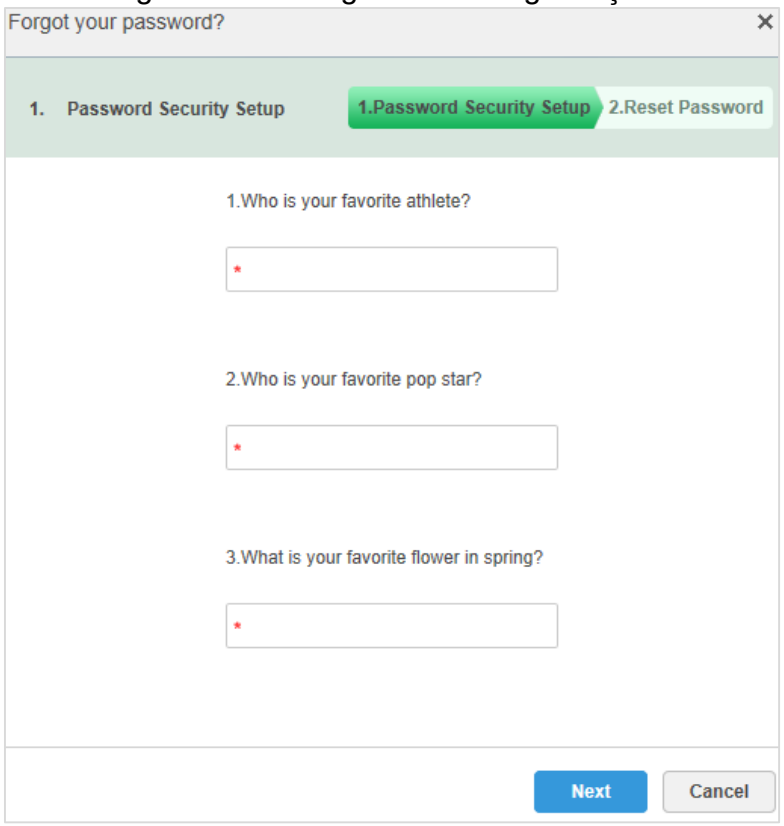
3.13.2.1 Redefinindo a senha do usuário do sistema

Quando a senha do usuário do sistema é esquecida, você pode redefinir a senha respondendo às perguntas de segurança.

Passo 1. Ao fazer login no Web Manager, digite system e uma senha aleatória e clique em Login.

Passo 2. Clique em Esqueceu sua senha?

Figura 211 - Perguntas de segurança



Passo 3. Digite as respostas das perguntas e clique em Avançar.

Passo 4. Digite a nova senha e clique em **OK.**

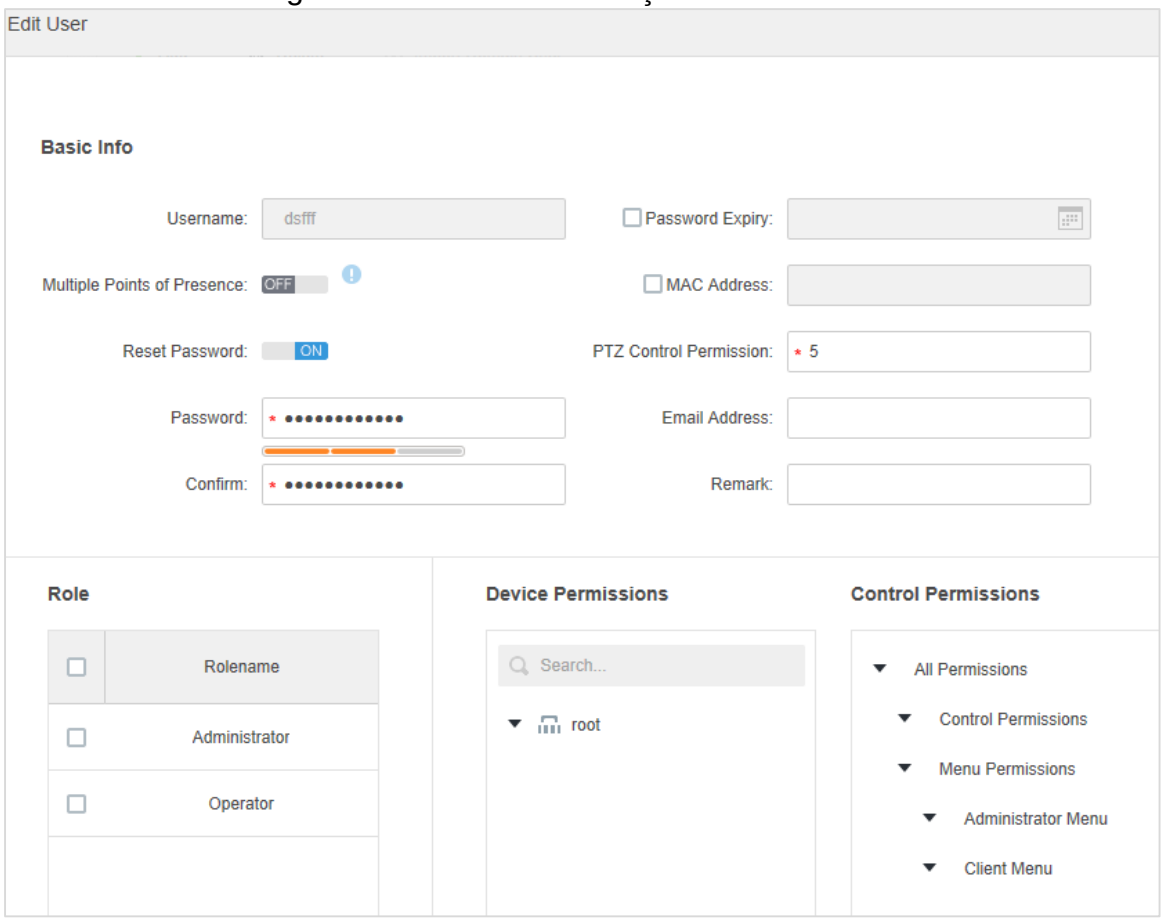
3.13.2.2 Redefinindo a senha do usuário geral

Apenas o usuário do sistema pode redefinir a senha. Outros usuários, quando suas senhas são esquecidas, podem pedir ao usuário do sistema para redefinir as senhas.

Passo 1. Faça login no Web Manager usando o nome de usuário e a senha do sistema e clique em **Usuário.** .

Passo 2. Clique na guia **Usuário** , selecione o usuário cuja senha deve ser redefinida e clique em .

Figura 212 - Editar informações do usuário



Passo 3. Ative **Redefinir senha** , insira a nova senha e confirme-a. Clique **O**

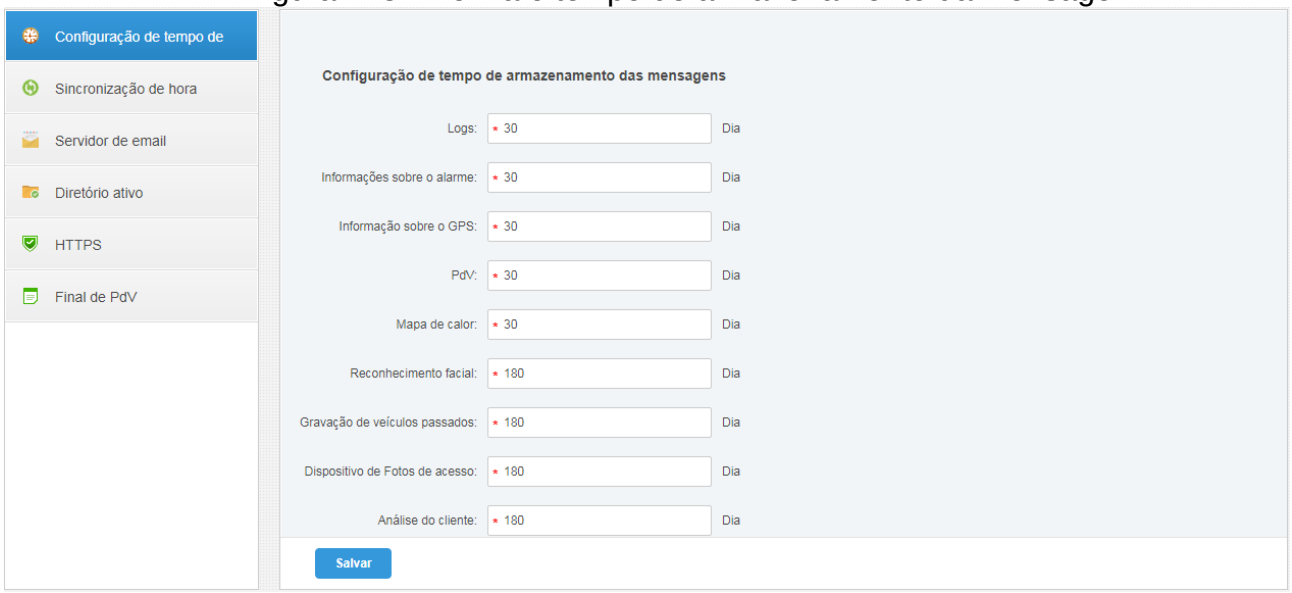
4 MANUTENÇÃO

4.1 CONFIGURANDO O PERÍODO DE ARMAZENAMENTO DE DADOS NO SISTEMA.

Defina os períodos de retenção para registros, mensagens de alarme, informações de GPS, registros de veículos, dados de mapa de calor, registros de reconhecimento de rosto e registros de fotos de acesso.

Passo 1. Clique +, selecione **Sistema** na interface da **Nova Guia**.
Passo 2. Configure os parâmetros correspondentes.

Figura 213 - Defina o tempo de armazenamento da mensagem



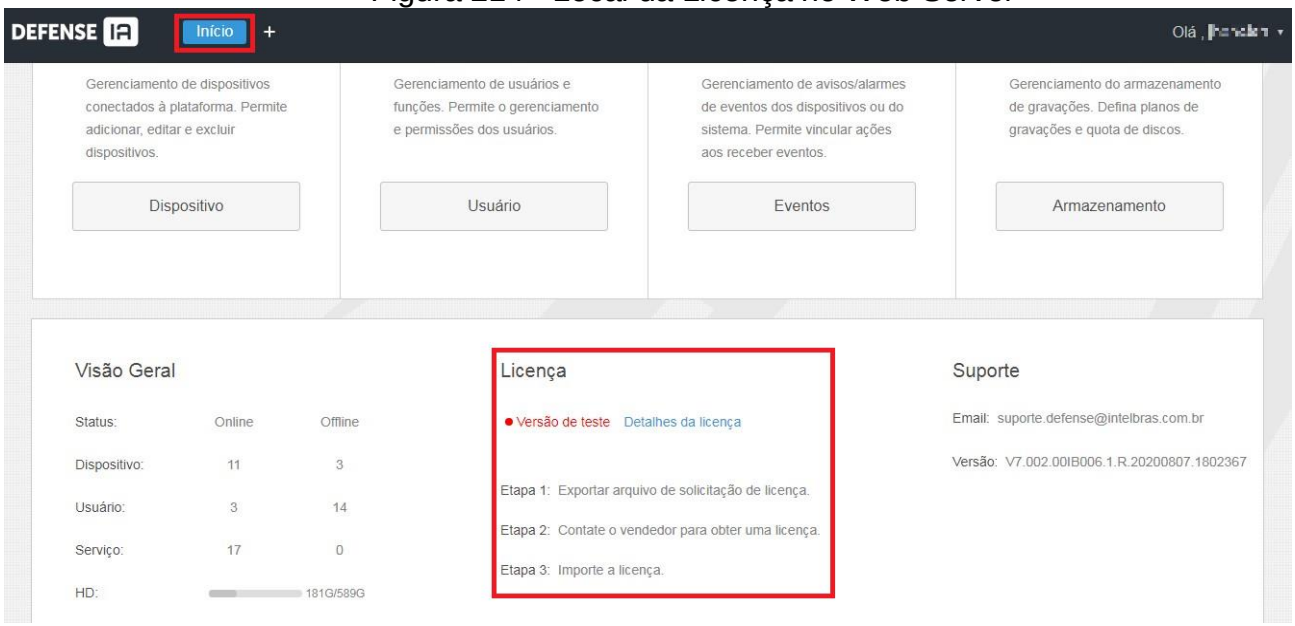
Passo 3. Clique em Salvar.

4.2 ATUALIZANDO CERTIFICADO DO SOFTWARE

Atualizar o certificado do software quando ele expira. Mesmo método para Defense IA Mobile.

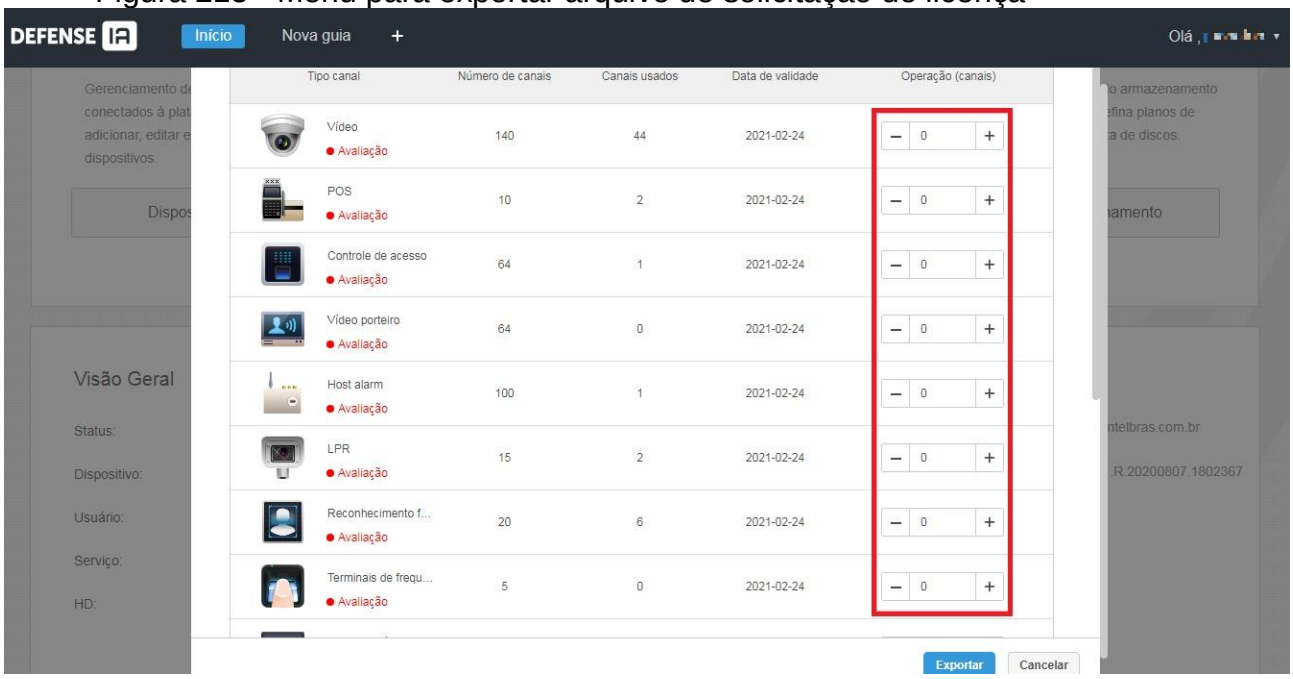
Passo 4. Acesse a interface **Web Server** e clique em **Início** na aba superior.

Figura 214 - Local da Licença no Web Server



Passo 5. Clique em “Exportar arquivo de solicitação de licença. ”.

Figura 215 - Menu para exportar arquivo de solicitação de licença



Passo 6. Adicione os tipos de canais e módulos, caso necessário, e exporte o arquivo de licença. Um arquivo “LicenseInfo.zip” será baixado para a pasta de downloads padrão do seu navegador.

Passo 7. Envie esse arquivo “LicenseInfo.zip” ao e-mail suporte.defense@intelbras.com.br para obter um novo certificado.

Passo 8. Após receber o e-mail do suporte com o arquivo “License.dat”, clique em “Importe a licença” para importar o novo certificado.

Passo 9. Insira o arquivo “.dat” e clique em “Importar”.

4.3 LOG REMOTO

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

Passo 1. Clique em , selecione **Sistema** na interface da **Nova Guia**.
Passo 2. Clique na guia Log remoto.
Passo 3. Marque a caixa de seleção Ativar e defina os parâmetros conforme necessário.

V. O número da plataforma deve ser o mesmo no servidor remoto e na plataforma.

Figura 216 - Habilitar registro remoto

Passo 4. Clique em Salvar.

4.4 SINCRONIZAÇÃO DE HORÁRIO

Sincronize a hora do sistema de todos os dispositivos conectados com a da plataforma; caso contrário, o sistema pode funcionar mal. Por exemplo, a pesquisa de vídeo pode falhar. A plataforma suporta sincronização de tempo de dispositivos conectados através do protocolo Intelbras e ONVIF. Você pode sincronizar manualmente ou automaticamente.

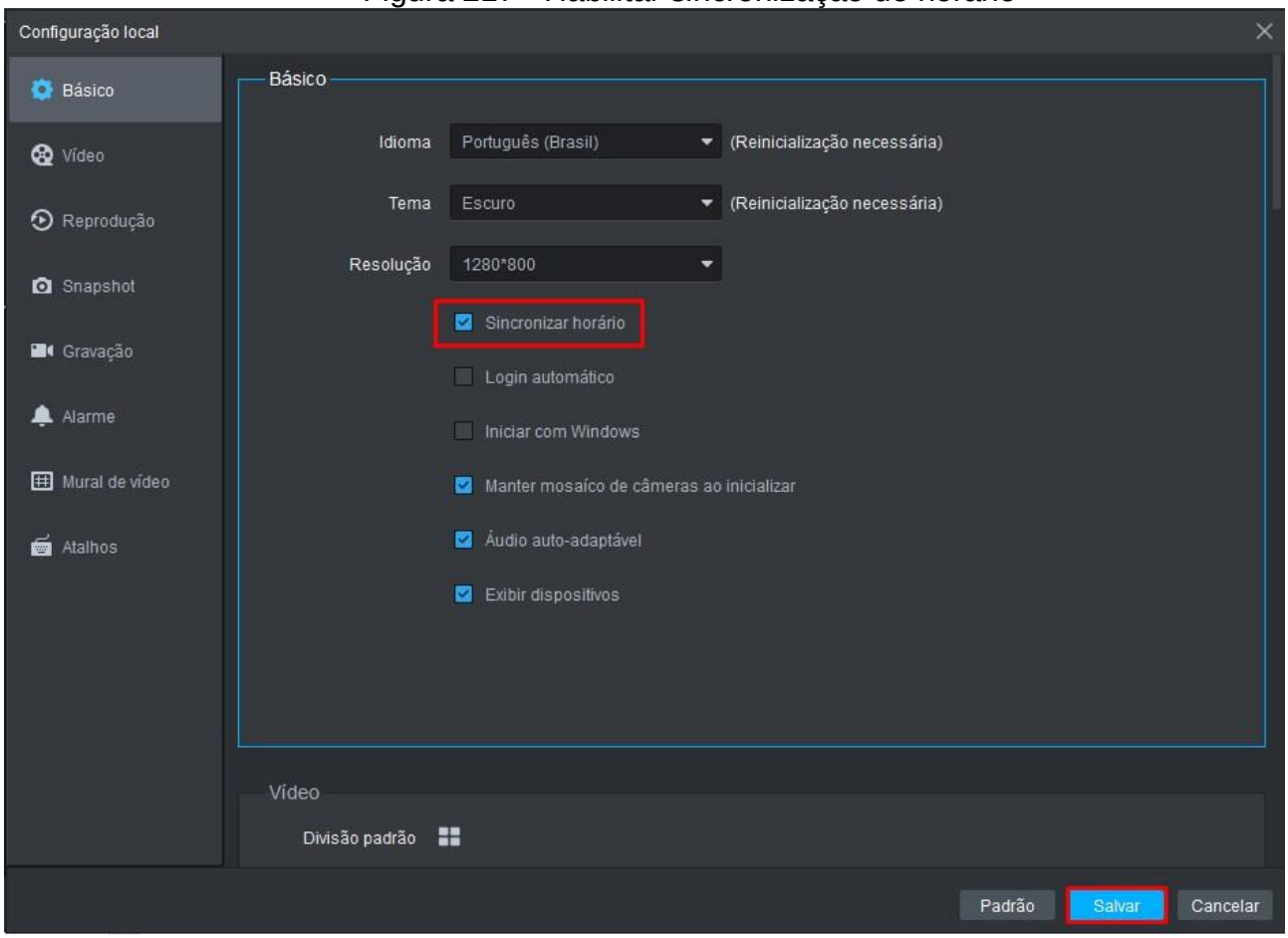
4.4.1 Sincronização Agendada de Horário

Configure a sincronização automática de tempo.

Passo 1. (Opcional) Habilite a sincronização de tempo no **Defense IA Client**.
7) Faça login no **Defense IA Client** e clique em para acessar a **Configuração Local**.
8) Clique em **Básico**, marque a caixa de seleção ao lado de **"Sincronizar horário"** e clique em **Salvar**.

➢ O sistema sincroniza imediatamente a hora após a ativação da função.

Figura 217 - Habilitar sincronização de horário



Passo 2. Clique + na **interface Web do Defense IA Server** e, em seguida, selecione **Sistema**.

Passo 3. Clique na guia Sincronização de hora e marque a caixa de seleção para ativar a função. Defina os parâmetros de sincronização de tempo.

Figura 218 - Habilitar sincronização de hora

Passo 4. Clique em Salvar.

4.4.2 Sincronização de Horário Manual

Sincronize manualmente a hora do sistema.

Passo 1. (Opcional) Habilite a sincronização de tempo no Control Client. Para obter detalhes, consulte "4.4.1 Sincronização Agendada de Horário. "

Passo 2. Clique + na interface Web do Defense IA Server e selecione Sistema.

Passo 3. Clique na guia **Sincronização de hora** e, em seguida, clique em Sincronizar.

Figura 219 - Sincronização imediata

4.5 BACKUP E RESTAURAÇÃO

O Defense IA suporta backup de configuração e armazena isso na máquina local, para que você possa usar o arquivo de backup para restaurar as configurações.

Apenas as contas com função *Administrador* podem realizar o backup e restauração.

4.5.1 Backup do sistema

Para garantir a segurança dos dados do usuário, o sistema Defense IA fornece a função de backup de dados. O backup inclui backup manual e backup automático.

Backup Manual

Passo 1. Clique + na interface Web do Defense IA Server e selecione Backup e restauração.

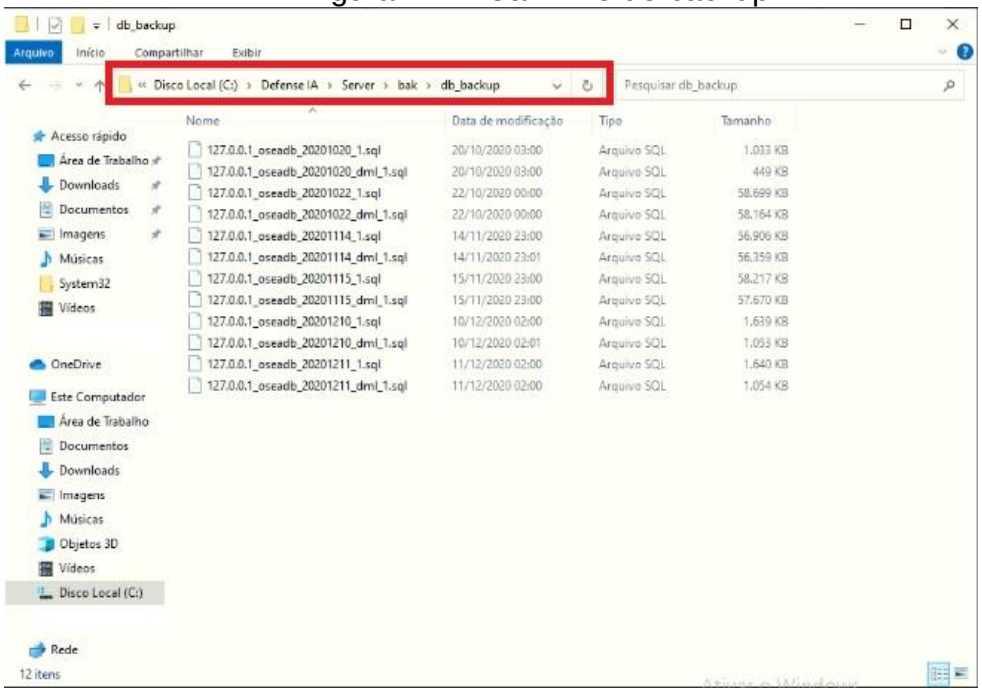
Figura 220 - Backup

Passo 2. Clique em Backup manual.
Passo 3. Digite a senha criptografada e clique em OK.

Backup Automático

Passo 1. Clique + na interface Web do Defense IA Server e, em seguida, selecione Backup e restauração.
Passo 2. Clique em Backup automático.
Passo 3. Selecione um período de backup e clique em OK.
Passo 4. Verifique o arquivo de backup automático no servidor. Caminho padrão: C:\Defense IA\Server\bak\db_backup

Figura 221 - Caminho de backup



4.5.2 Restauração do sistema

Armazene os dados do último backup quando o banco de dados do usuário responder de forma anormal. Ele pode restaurar rapidamente o sistema Defense IA do usuário e reduzir a perda de eventuais informações.

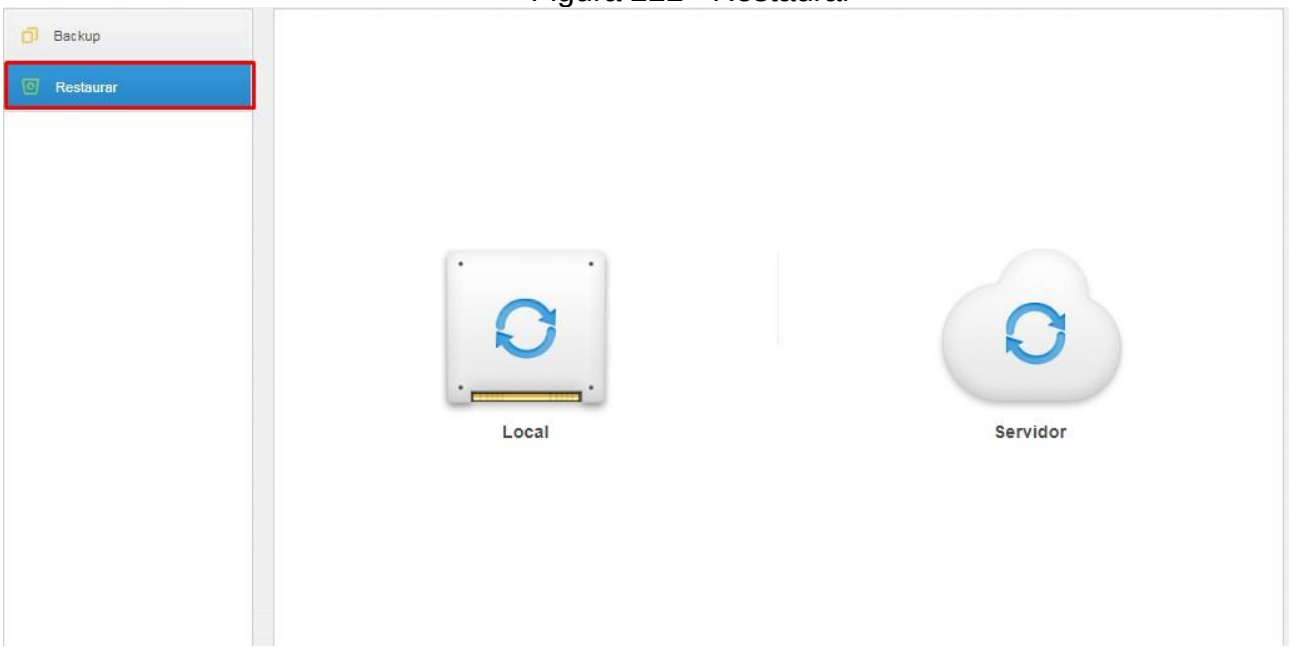
Interrompa outros usuários usando o sistema Defense IA ao implementar a restauração do sistema. Tenha cuidado ao usar a função porque ela pode alterar as informações dos dados.

Local

Passo 1. Clique na interface Web do Defense IA Server e, em seguida, selecione Backup e restauração.

Passo 2. Selecione a guia **Restaurar**.

Figura 222 - Restaurar



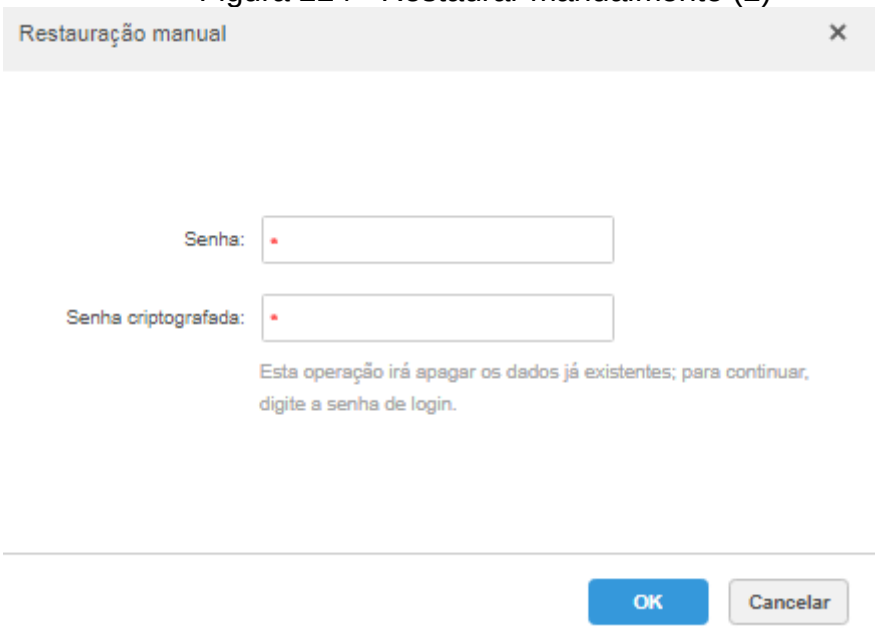
Passo 3. Clique em Local.

Figura 223 - Restaurar manualmente (1)

Passo 4. Clique em **Pesquisar**, selecione o arquivo com extensão “.dbk” e clique em OK.

Passo 5. Digite a senha de login do administrador e a senha criptografada do arquivo de backup.

Figura 224 - Restaurar manualmente (2)



Passo 6. Clique OK.

Os dados estão sendo restaurados; ele exibirá a porcentagem de restauração através da barra de progresso. O sistema será reiniciado depois de concluído.

Servidor

Ele seleciona restaurar os dados do arquivo de backup no lado do servidor. A pré-condição é que ele precisa habilitar a função de backup automático, o servidor faz o backup do banco de dados de acordo com o período definido e o arquivo de backup do formulário.

Passo 1. Selecione a guia **Restaurar**.

Figura 225 - Restaurar

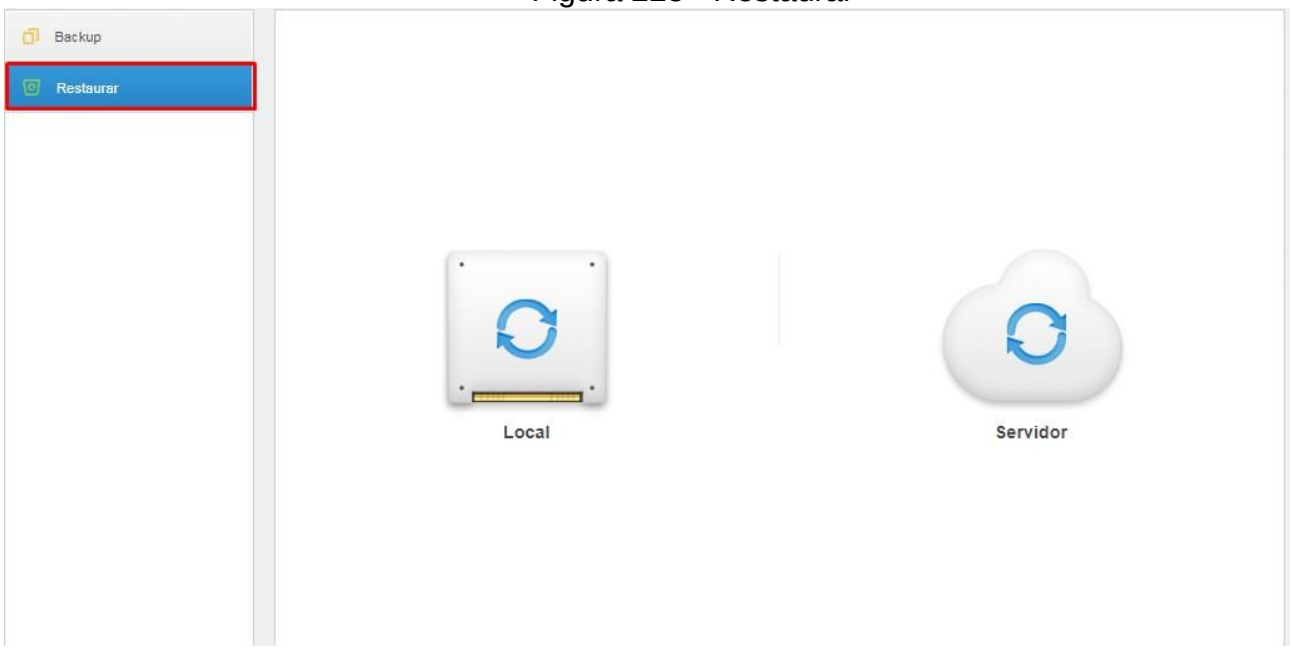
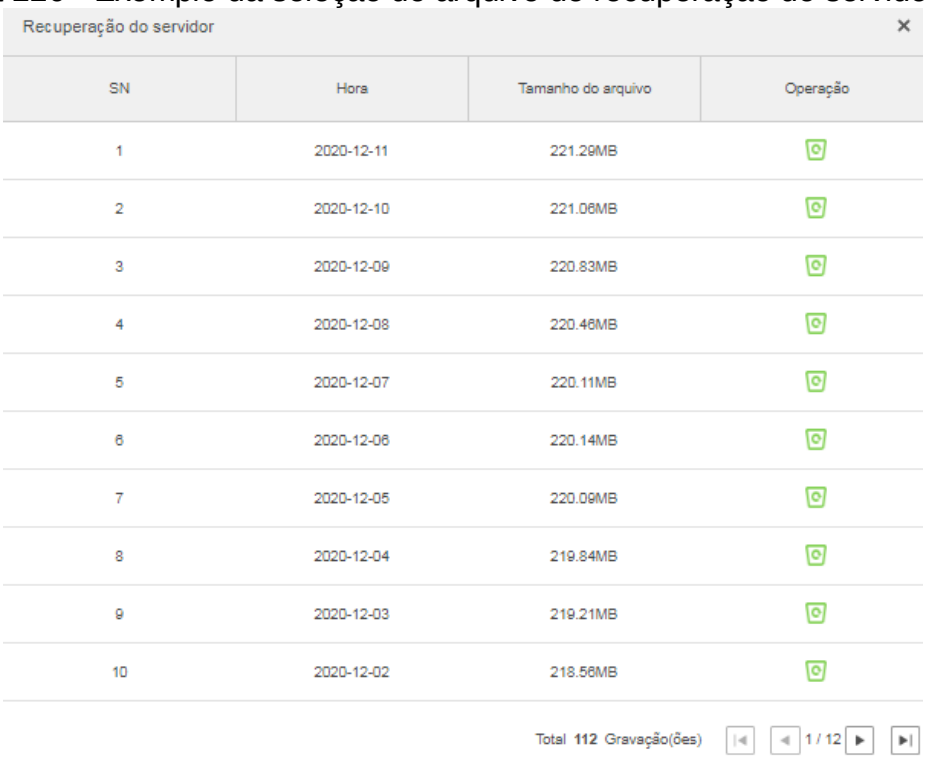
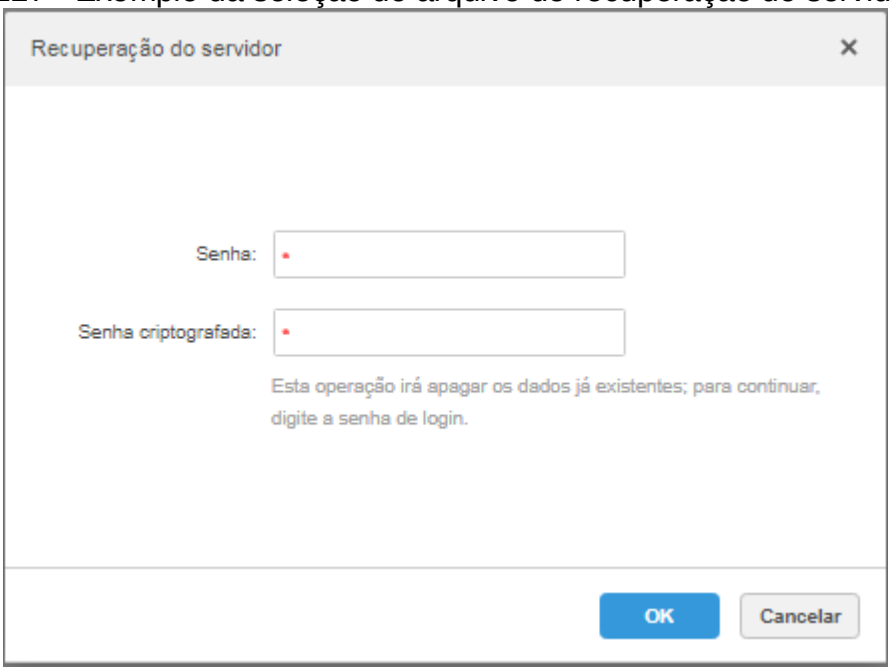


Figura 226 - Exemplo da seleção do arquivo de recuperação do servidor



Passo 2. Clique em **Servidor** e clique em na lista e selecione o arquivo que precisa ser restaurado.

Figura 227 - Exemplo da seleção do arquivo de recuperação do servidor



Passo 3. Digite a senha de administrador, a senha criptografada, clique em OK e restaure.

O sistema será reiniciado depois que os dados forem restaurados com sucesso.

4.6 REGISTRO

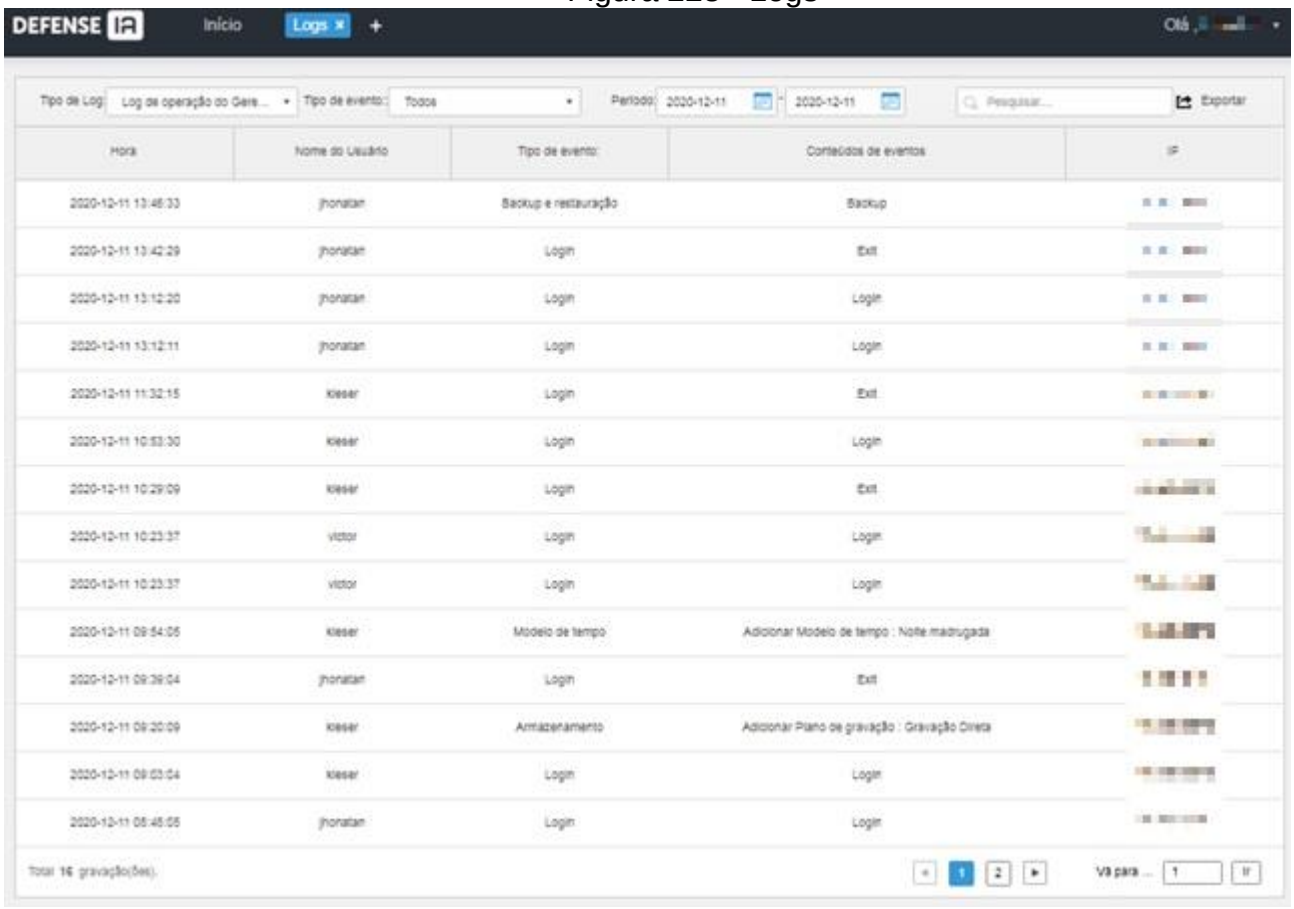
Visualize os registros de operação do administrador e do operador. Você pode filtrar por evento e hora.

Tome como exemplo o Log de Operação de Gerenciamento.

Passo 1. Clique + e selecione **Logs** na interface da **Nova Guia**.

Passo 2. Selecione o tipo de registro, tipo de evento ou tempo de consulta.

Figura 228 - Logs



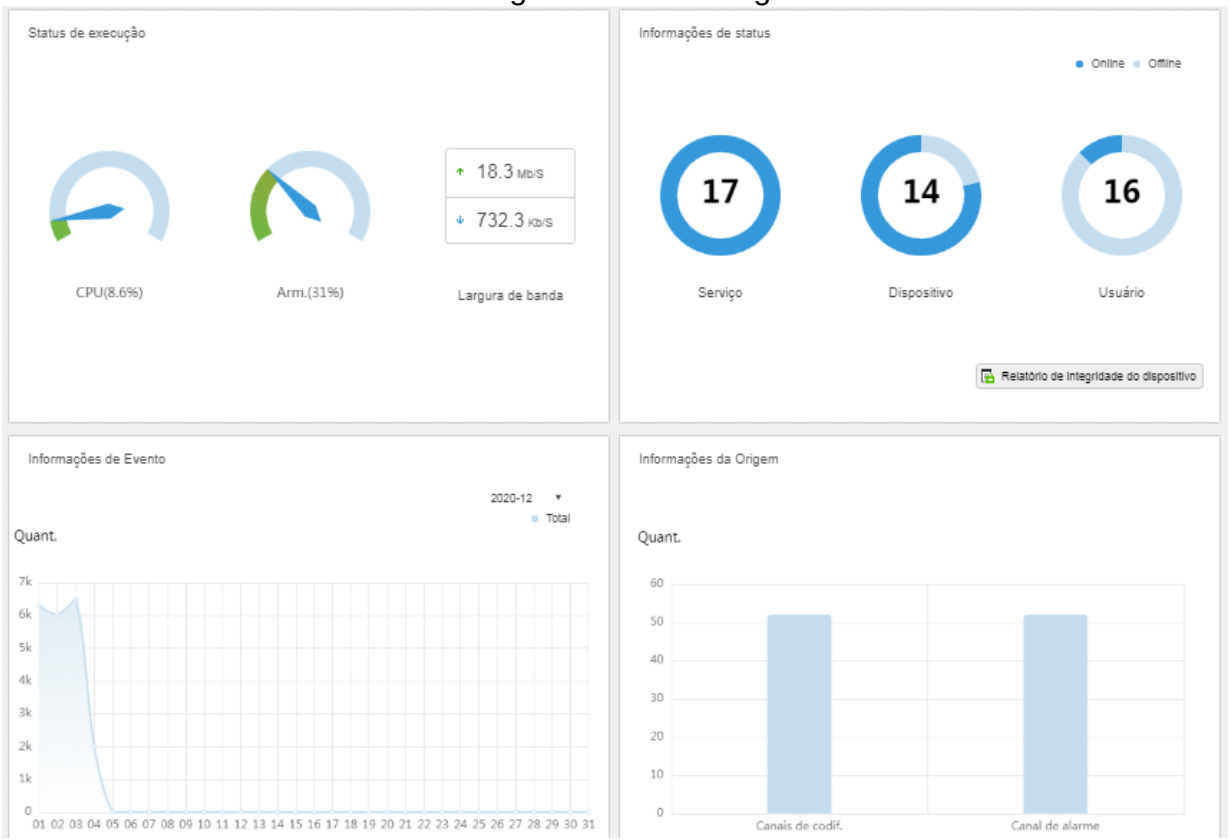
4.7 MANUTENÇÃO DE SISTEMA

Visão estatística de operação e manutenção do sistema para saber a situação de funcionamento do sistema.

4.7.1 Visão global

Clique + na interface Web do Defense IA Server e selecione Visão geral.

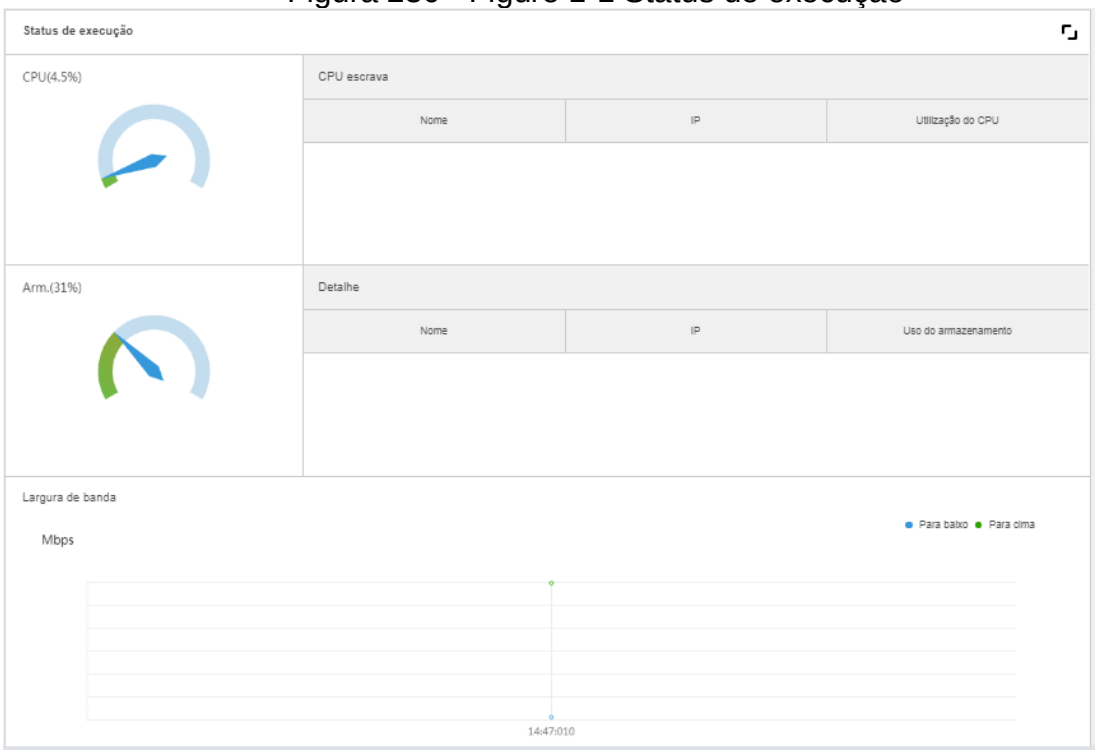
Figura 229 - Visão global



4.7.2 Status de execução

Clique em Status de execução para ver o estado da CPU, armazenamento e largura de banda.

Figura 230 - Figure 1-1 Status de execução



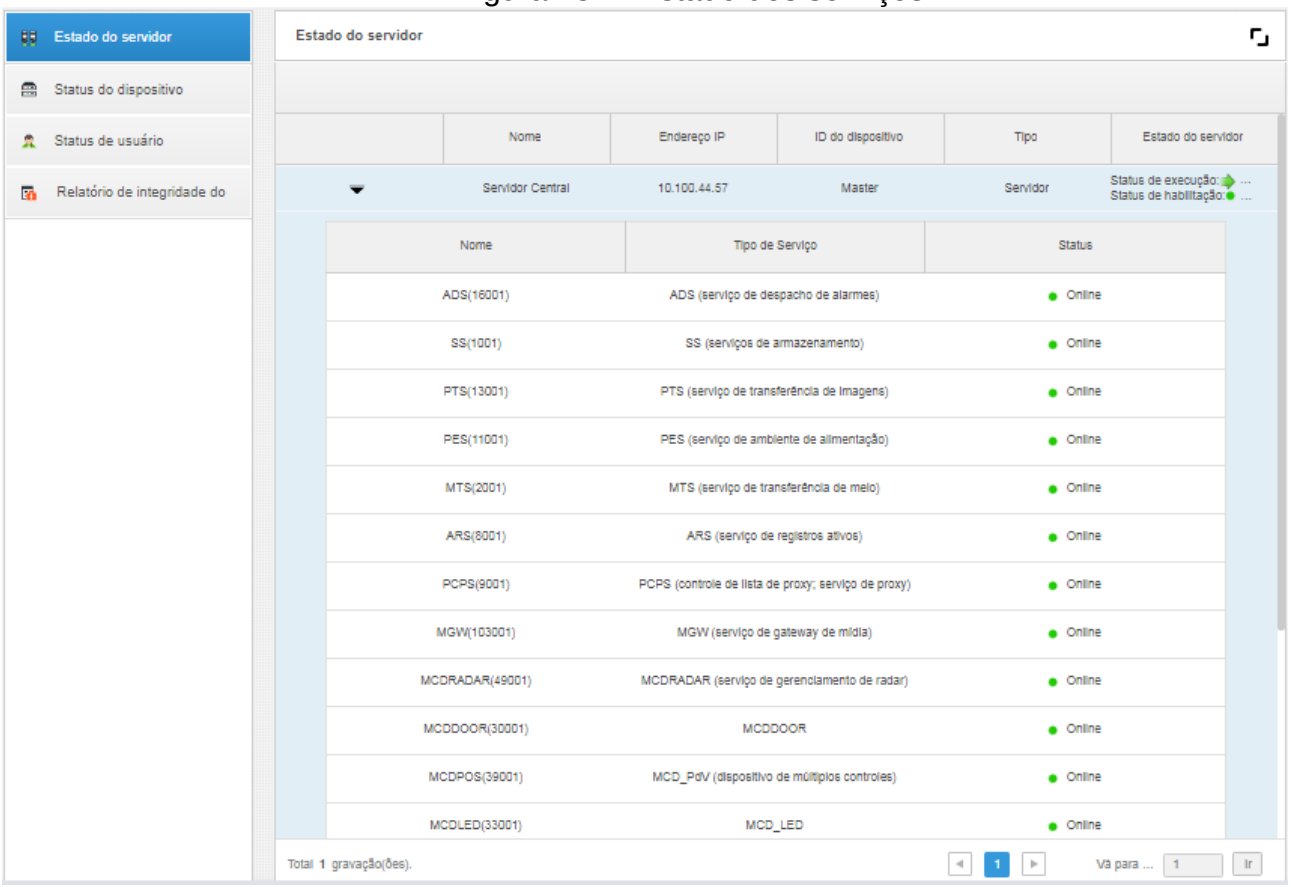
4.7.3 Estado do servidor

Ver o estado do servidor, dispositivos, e dos usuários.

Informações do estado dos serviços

Clique na interface de Estado do servidor e, em seguida, a interface exibe os detalhes dos serviços.

Figura 231 - Estado dos serviços

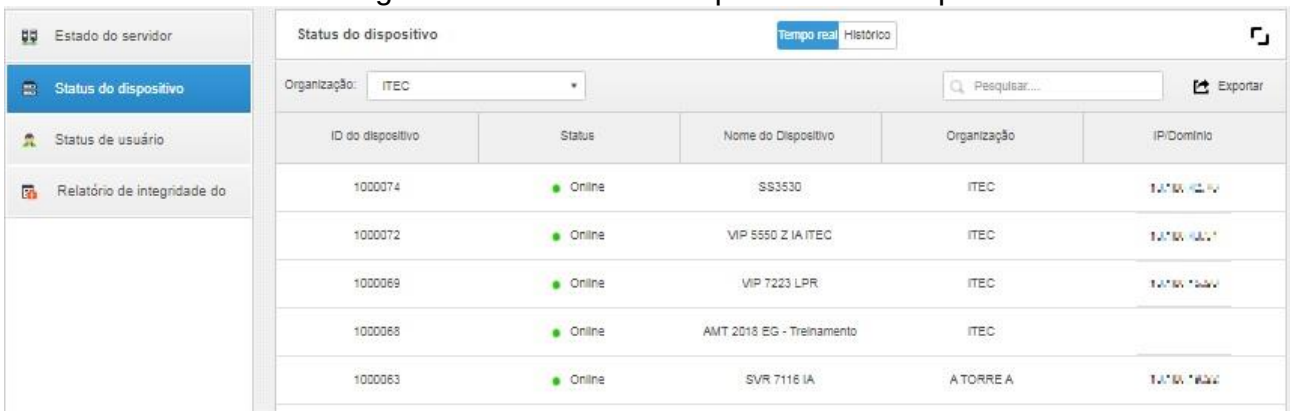


Informações de status dos dispositivos

Passo 1. Clique na interface Web do Defense IA Server e selecione Visão geral.

Passo 2. Clique em Status do dispositivo.

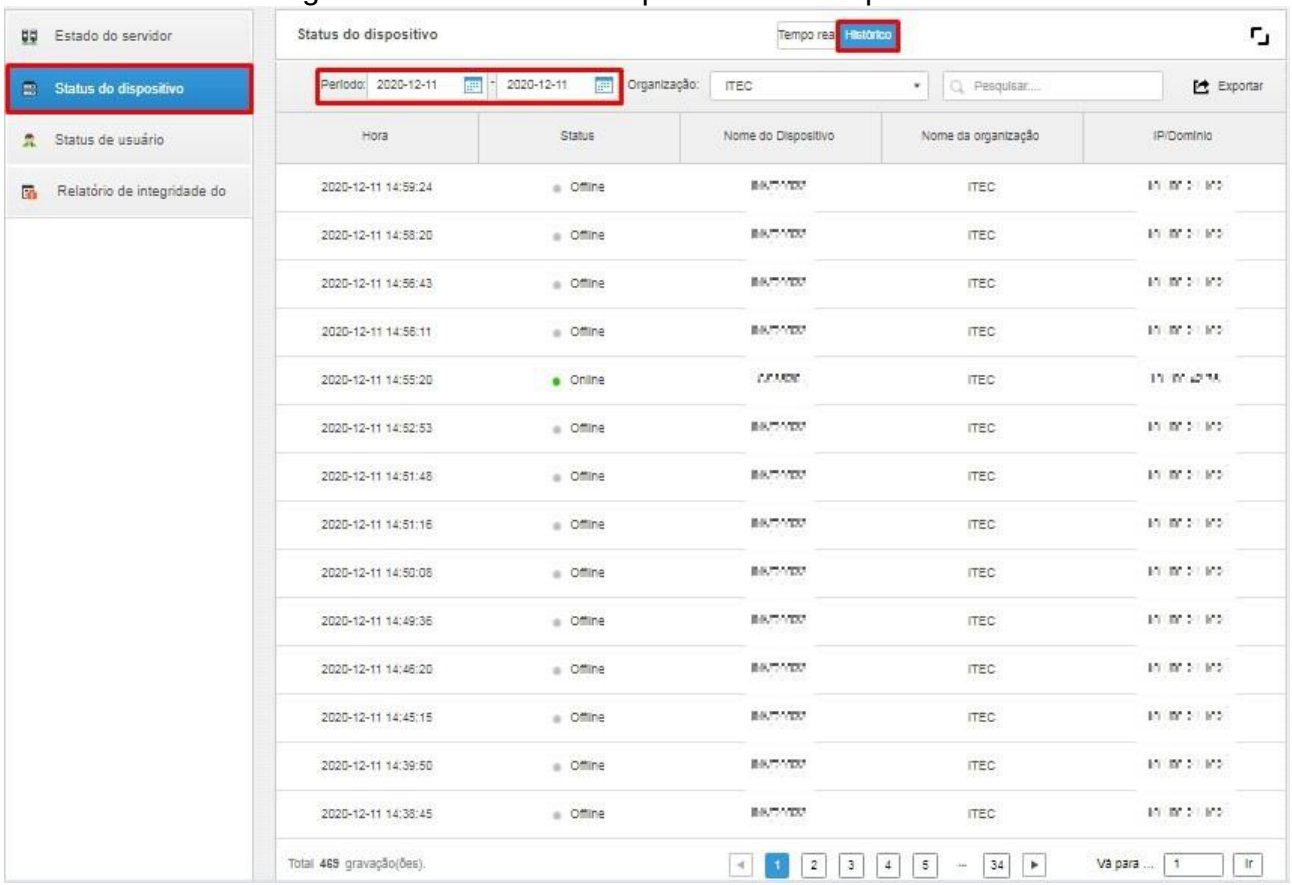
Figura 232 - Status do dispositivo em tempo real



Passo 3. Verifique o status do dispositivo.

1. Clique na aba **Tempo Real** na interface de informações de status do dispositivo para ver o estado do dispositivo em tempo real.
2. Clique na aba **Histórico** na interface de informações de status do dispositivo para ver o histórico de estado do dispositivo.

Figura 233 - Status do dispositivo em tempo real / histórico



Passo 4. Clique em **Exportar** para exportar informações de status do dispositivo em tempo real (formato PDF).

Passo 5. Clique em Status de usuário e em Relatório de integridade do dispositivo para ver mais detalhes.

4.7.4 Informação de Evento

Visão do número total de eventos de alarme e eventos processados por mês.

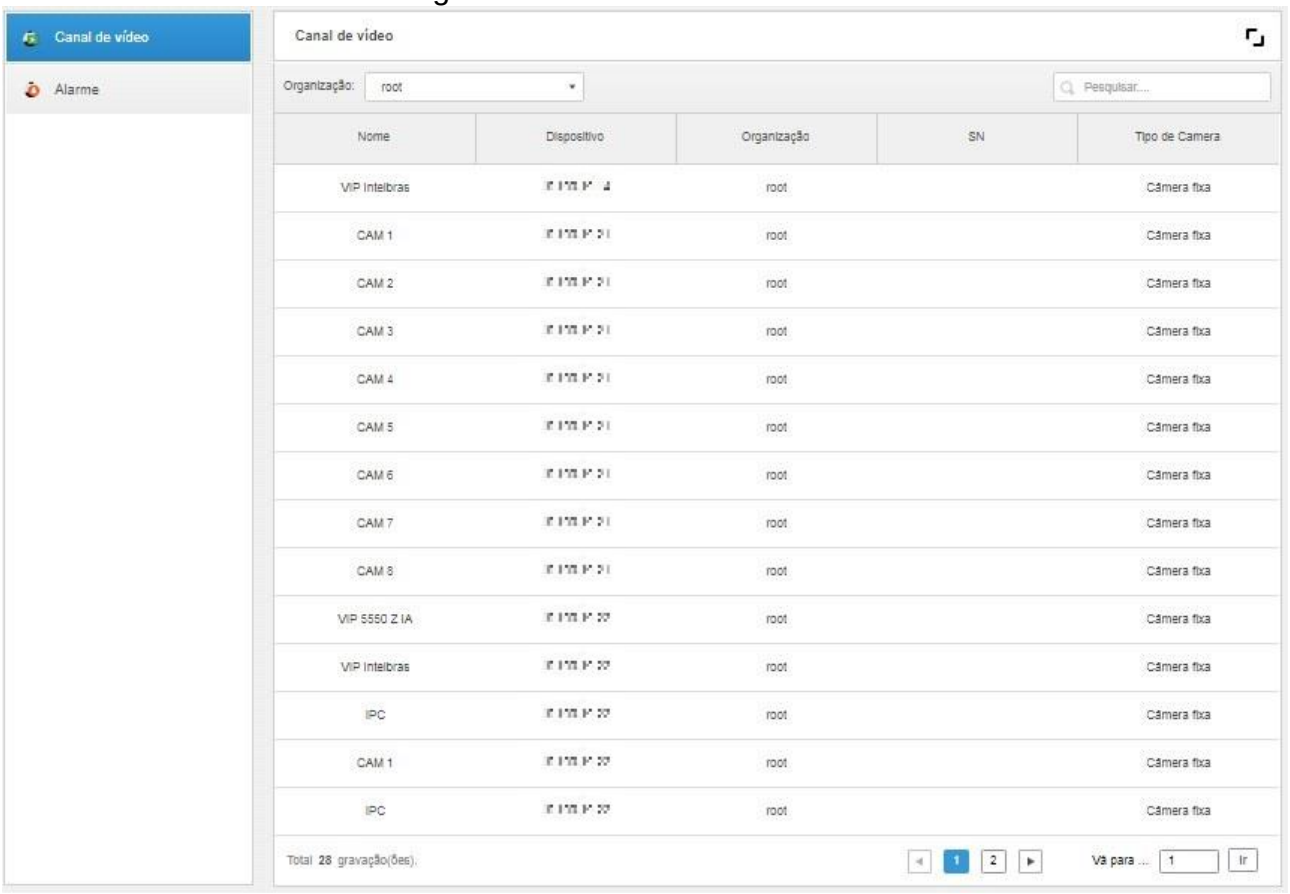
Figura 234 - Informação do evento

4.7.5 Informação da Origem

Visão das estatísticas dos canais de vídeo e dos canais de alarmes. Clique em **Informações da Origem** para visualizar a interface detalhada.

Visão dos detalhes do canal de vídeo.

Figura 235 - Detalhes do canal de vídeo



Clique na guia Alarme para ver em detalhes o canal de alarmes.

Apêndice 1 - Anexo I

I. TIPOS DE AUTENTICAÇÃO E CRIPTOGRAFIAS

O Defense IA possui os seguintes tipos de autenticações, certificados e criptografias principais:

HTTP/HTTPS (TLS 1.0/1.1/1.2 - a escolha do usuário) para comunicações via página Web e Client.

Cifras TLS: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA.

Para acesso ao banco de dados MySQL, é utilizado método “Secure Password Authentication”, criptografia AES256 [ECB].

Para interações com os serviços do Defense, são utilizadas criptografias AES256/SHA256.

Para acesso aos Storage iSCSi é utilizado encriptação CHAP.

Comunicação com as câmeras Intelbras encriptadas por Digest.

O sistema possuí aceitação para importação de Certificados Digitais SSL.

O Defense IA tem compatibilidade com o Microsoft Active Directory (AD).

II. LOGS E RELATÓRIOS DO SISTEMA

Existe a possibilidade de averiguação dos seguintes Logs na Página WEB do Servidor:

1. Logs de Operações na interface Web do Servidor. Logs dos tipos usuários, configurações, dispositivo, organização, função, eventos, armazenamento, modelo de tempo, mural de vídeo, lista negra de veículos, backup e restauração, login, E-Map, gerenciamento de pessoal, gerenciamento de controle de acesso, gerenciamento de frequência e gerenciamento de visitantes. Estes logs possuem o conteúdo dos eventos e o IP do operador.
2. Logs de operações no client. Logs dos tipos: login, visualização, controle de PTZ, gravação de vídeo, fala áudio, abrir a barreira, gerenciamento de estacionamento e radar smart track. Estes logs possuem o conteúdo dos eventos e o IP do operador.

3. Logs do sistema. Logs dos tipos reiniciar, mudança de horário do sistema, CPU anormal, largura de banda anormal, login anormal, excluir arquivo do sistema, gravação programada, foto agendada, log hot spare, log do servidor, log do usuário, atualização do sistema. Estes logs possuem o conteúdo do evento.
4. Relatórios de integridade dos dispositivos
5. Status de conexão dos usuários em tempo real e históricos passados.
6. Status de conexão com dispositivos em tempo real e históricos passados.
7. Status dos servidores e serviços.
8. Gráficos de quantidades de alarmes em cada mês e por tipo de dispositivos.

Na interface do Client, pode-se visualizar todos os eventos gerados por todos os dispositivos atrelados ao sistema pela Central de Eventos (com limites de histórico baseado no armazenamento ou nos dias configurados de retenção das informações - o que acontecer antes). Além disso, na pasta de instalação do Client existem logs para checar possíveis problemas com requisições/bugs do sistema.

Existem Logs de todos os serviços do Defense IA Server na pasta de instalação do software, o qual permite-se checar eventuais problemas com os serviços/requisições/bugs do sistema.

III. BACKUP

O Defense IA possui função de Backup configurável na sua interface WEB, tendo a possibilidade de configurar um arquivo de backup para ser criado de acordo com um agendamento diário/semanal/mensal. As variáveis que são armazenadas no backup são descritas abaixo:

Variáveis de Backup	Descrição
adm_devices:DEVICES:180	Dispositivos adicionados e configurações dos dispositivos
adm_general_system:SYSTEM:180	Configurações gerais do sistema
adm_users:USERS:180	Usuários Criados e grupos
adm_organization:ORG:180	Organizações criadas
adm_log_alarm:ALARM_DATE:180	Log de Eventos
adm_log_adm:CREATE_DATE:180	Log de Gerenciamento
adm_log_opt:CREATE_DATE:180	Log de Operação

bd_facial_DATA:180	Banco de Dados Facial
od_objectiondetection_DB:180	Dados de Análise Forense
pc_peoplecounting_data:180	Dados de Contagem de Pessoas
hm_heatmap_data:180	Dados de Mapa de Calor
pos_receipt_item:RECEIPT_TIME:180	Recibos de POS
pos_receipt:RECEIPT_TIME:180	Detalhes de Recibo de POS
ac_door_access_record:SWIPE_TIME:180	Registros de Controle de Acesso
adm_gps_info_[0-9]{8}	Dados do GPS/GIS (tabela de tempo)

IV. ARQUITETURAS DO DEFENSE IA

O Defense IA pode trabalhar com 3 tipos de arquitetura. Para projetos de pequena escala, geralmente se utiliza da Arquitetura de Servidor Único. Para atender aos requisitos de projetos de grande e média escala, utiliza-se as arquiteturas Cascateadas e Distribuídas (ou ambas).

Arquitetura de Servidor Único:

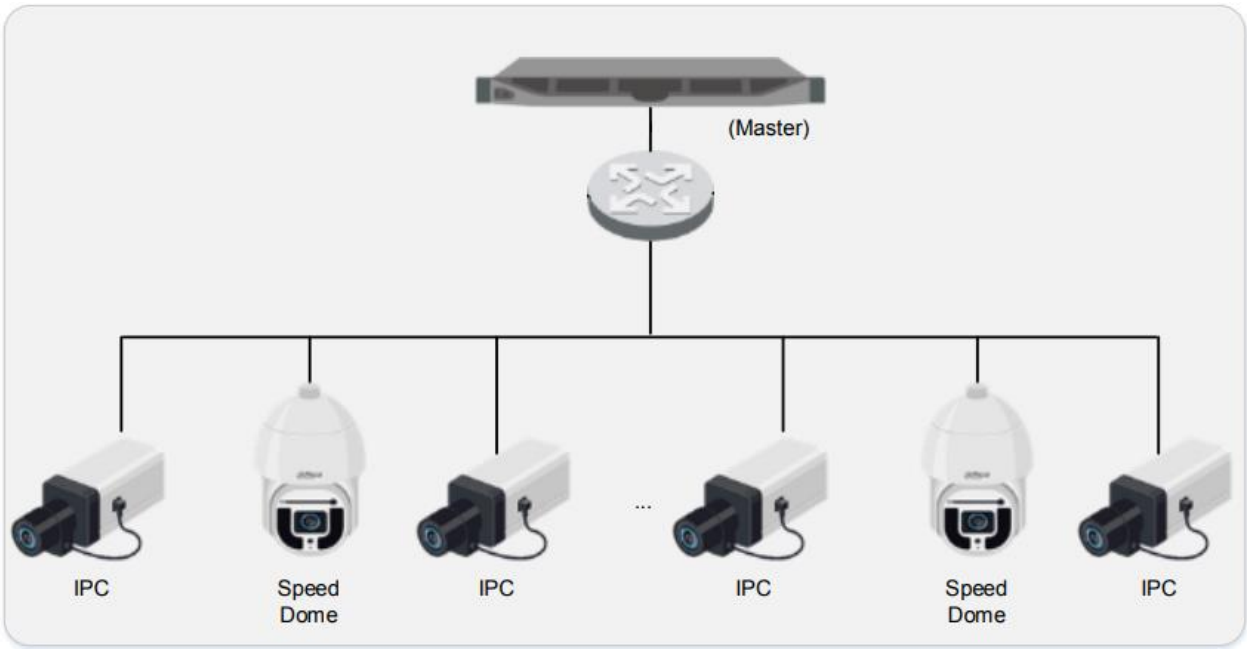


Imagem 1 – Ilustração de arquitetura de Servidor Único

É o modo mais comum de se utilizar em cenários menores ou em cenários que possuam gravações sendo feitas em gravadores/diretamente nos dispositivos.

Esta é a topologia usual para cenários que não ultrapassem as características de quantidade de dispositivos, throughput, quantidade de eventos e armazenamento descritas para um único servidor no datasheet do Defense IA.

Para o funcionamento da arquitetura de servidor único, o cliente precisa ter no mínimo uma licença base e no caso de quantidades de dispositivos excederem o limite da licença base, os adicionais de canais para cada um dos dispositivos excedentes. Além disso, também é comercializado também as licenças de modo separado para os módulos de Tráfego e BI.

Arquitetura Distribuída:

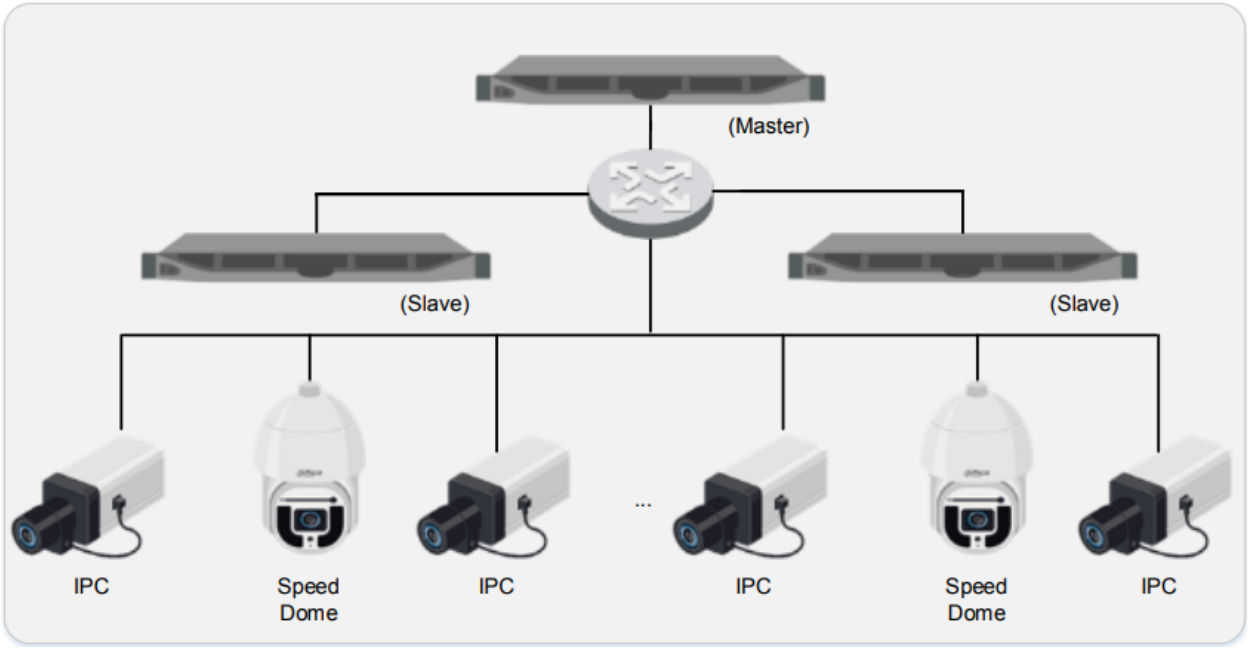


Imagem 2 - Ilustração de arquitetura Distribuída.

Esta topologia é recomendada para cenários maiores do que os comportados por um único servidor. Os servidores *slaves* que se conectam no master servem para distribuição de carga tanto de processamento quanto de armazenamento, dessa forma aumentando a capacidade e performance do sistema.

Os servidores *slaves* não possuem interface *WEB*, o sistema é visto como um só e toda configuração é feita pela interface *WEB* do master. Este tipo de arquitetura pode ter apenas um servidor master e consome apenas uma licença base (licenciamento idêntico à arquitetura de servidor único). Dessa forma, quando se quer expandir a capacidade do sistema usando arquitetura distribuída, não são necessárias licenças adicionais no sistema (apenas a licença base e os adicionais de licença para os canais ou módulos extras).

Esta arquitetura deve ser implementada apenas em redes locais. Para aplicações em de múltiplas localidades deve ser utilizada a topologia de cascata.

Arquitetura Cascateada:

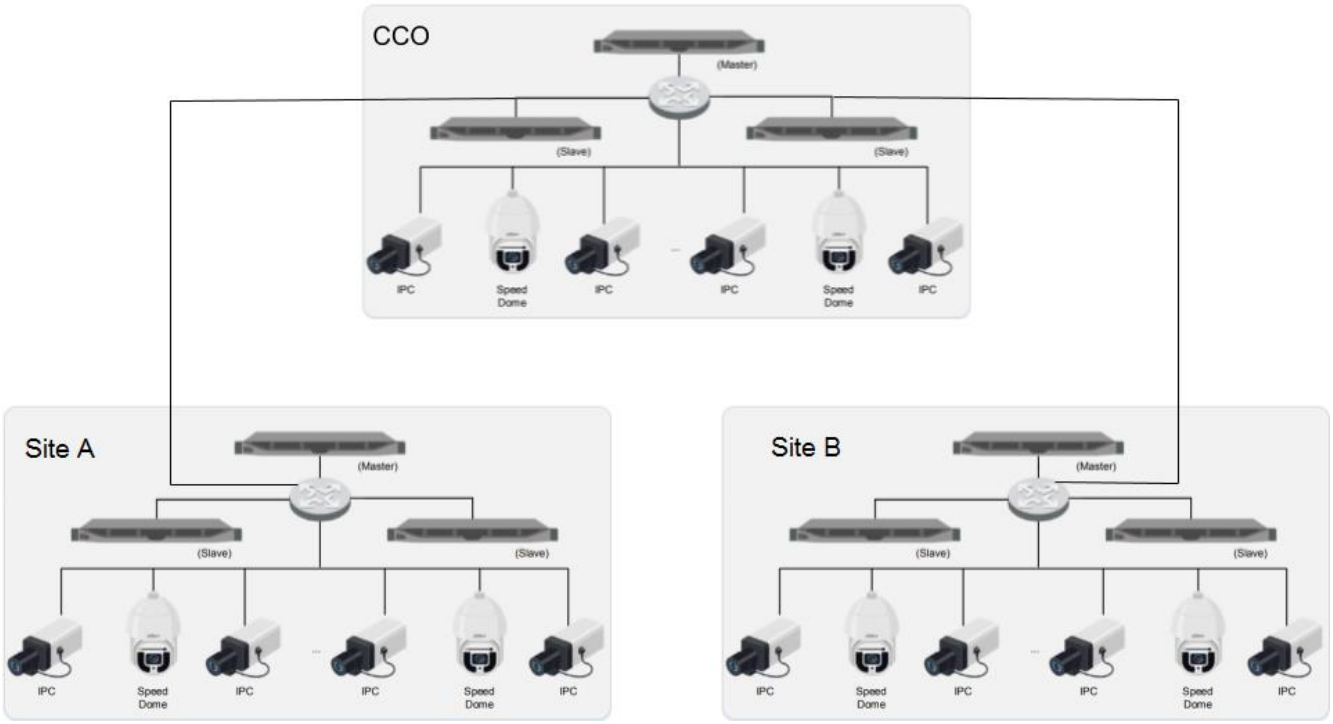


Imagem 3 – Ilustração de arquitetura cascateada.

O Defense IA possui a topologia cascateada, no qual permite que Servidores de Níveis Superiores (no exemplo, o CCO) possam visualizar Visualizações ao Vivo (Live-Stream) e gravações de vídeo dos servidores de níveis inferiores. Para licenciar e configurar o sistema cascateado, deve-se adicionar licenças de Domínio nos Servidores de Níveis mais altos, permitindo então que os mesmos possam enxergar os Servidores de níveis inferiores. O sistema hoje suporta até 3 níveis de cascateamento com limite de 20 servidores master para esse tipo de arquitetura.

A arquitetura cascateada é mais utilizada em sistemas de múltiplos sites (localizações) e que possuem a necessidade de uma central de monitoramento unificada (ou acesso as câmeras de níveis inferiores de uma central principal). Nessa arquitetura, não são necessárias conexões em rede local entre servidores master, porém é recomendado uma conexão estável, de baixa latência e com boas velocidades de upload e download (condizente com o *throughput* necessário para a operação).

Os únicos eventos que são possíveis de serem encaminhados dos Servidores em Níveis inferiores para os de Nível Superior são os dos menus de Canais de Vídeo e Canais Inteligente.

Cada Servidor Master em cenário cascateado é considerado um sistema a parte, ou seja, se a conexão entre um servidor Master e o servidor Master do nível superior cair, ambos os sistemas se mantem operáveis.

É possível fazer a utilização da arquitetura distribuída e cascateada ao mesmo tempo. Dessa forma, se possuí a possibilidade de expansão de cada um dos servidores cascateados, aumentando a performance/capacidade de cada um dos sistemas individuais.

1ª observação: O Defense IA não possuí suporte nativo a aplicações em nuvem.

2ª observação: Para o dimensionamento do sistema, deve-se atender as especificações de hardware (Ex: velocidade de escrita e leitura dos discos de armazenamento devem atender throughput requerido para armazenamento das gravações em cada cenário).

3ª observação: Limites de cada uma das arquiteturas descritos no Datasheet e na seção Capacidades do Sistema.

V. PORTAS E SERVIÇOS

Segue abaixo a relação de portas e serviços utilizados pelo Defense IA:

Serviço	Nome do Serviço	Descrição	Porta	Tipo de Protocolo
Center Management Service (CMS)	Defense_Web	O serviço de gerenciamento central gerencia os outros serviços e provê as portas de acesso.	HTTPS : 443 HTTP : 80 CMS : 9000 SHUTDOWN : 8005 REDIRECT : 9005	TCP
Message Queue Service (MQ)	Defense_MQ	O Serviço de Fila de Mensagens transfere menssagens entre serviços.	61616	TCP

Device Management Service (DMS)	Defense_DMS	O Serviço de Gerenciamento de Dispositivos é responsável por registrar o codificador front-end, receber o alarme, transferir o alarme e enviar o comando de tempo de sincronização.	9200	TCP
Media Transmission Service (MTS)	Defense_MTS	O Serviço de Transmissão de Mídia consiste em obter o fluxo de áudio / vídeo do dispositivo front-end e transferir esses dados para o Serviço de armazenamento Defense_SS, plataforma client e decodificador.	9100	TCP
Storage Service (SS)	Defense_SS	O Serviço de Armazenamento serve para armazenar, pesquisar e reproduzir gravações.	9320	TCP
Video Matrix Service (VMS)	Defense_VMS	O Serviço de Matriz de Vídeo Wall serve para fazer login no decodificador e enviar para o decodificador as tarefas do vídeo wall.	N/A	-
Media Gateway Service (MGW)	Defense_MGW	O Serviço de Gateway de Mídia serve para fazer a ponte entre as instâncias do serviço MTS e o decodificador.	9090	TCP
Auto Register Service (ARS)	Defense_ARS	O Serviço de Registro Automático serve para escutar os dispositivos que são adicionados ao Defense via auto-registro. Este serviço	9500	TCP

		executa o login e envia o fluxo de dados para o serviço MTS.		
ProxyList Control Proxy Service (PCPS)	Defense_PCPS	O Serviço de Controle de Proxy serve para fazer login nos dispositivos ONVIF S/G e em seguida, obter o fluxo e transferir os dados para o MTS.	REGISTER : 9550 SIP : 5060	UDP/TCP
Alarm Dispatch Service (ADS)	Defense_ADS	O Serviço de Despacho de Alarme consiste em enviar informações de alarme a diferentes objetos de acordo com os planos.	9600	TCP
Multi-Control Device (MCD)	Defense_MCD	O serviço de Multi-Controle de Dispositivos lida com acesso de dispositivos de alarme. Este serviço simula dispositivos e lida com acesso de SDK de controladores de alarme, dispositivos de controle de acesso e dispositivos de monitoramento de ambiente dinâmico.	30001	TCP
Power Environment Server (PES)	Defense_PES	O Serviço é responsável pelo monitoramento/acesso dos dispositivos em ambiente dinâmico.	9400	TCP
Switch Center (SC)	Defense_SC	O Serviço lida com os logins de SIP referentes as conexões de PC Clients e Aplicativos. O serviço também é responsável por	SIP : 5080 RTP : 554	TCP/UDP

		encaminhar streams de conversa/aúdio.		
Object Storage Service (OSS)	Defense_OSS	O Serviço lida com o armazenamento de snapshots de face e imagens obtidas nos eventos de alarme inteligente.	HTTP : 9900 HTTPS : 9901	TCP
Picture Transfer Service (PTS)	Defense_PTS	O Serviço de Transferencia de Fotos	LISTEN : 9115 PICTURE : 8081 RTP : 40000-49999	UDP/TCP
Radar	Defense_RADAR	Serviço de gerenciamento de radar.	N/A	-
MCD-POS	Defense_MCDPOS	Serviço de gerenciamento de PdV (POS). Esse serviço se comunica com o serviço MCD.	8080	UDP/TCP
MCD-LED	Defense_MCDLed	Serviço de gerenciamento de painéis LED. Esse serviço se comunica com o serviço MCD.	N/A	-
MCD-Door	Defense_MCDDoor	Serviço de gerenciamento de Vídeo Porteiros/Controle de Acesso. Esse serviço se comunica com o serviço MCD.	N/A	-
MCD-Alarms	Defense_MCDAlarm	Serviço de gerenciamento de Painéis de Alarme. Esse serviço se comunica com o serviço MCD.	N/A	-
HRS	Defense_HRS	Serviço HRS.	N/A	-
Enhanced Analysis Service (EAS)	Defense_EAS	Serviço de análise aprimorada	N/A	-
MySQL	Defense_MySQL	Serviço referente ao banco de dados do sistema. Necessário	3306	UDP/TCP

		para a maioria das operações do sistema, armazenando principais informações inseridas no servidor.		
SOSO	Defense_SOSO	Serviço SOSO.	12366	UDP/TCP
Remote Dictionary Server (REDIS)	Defense_REDIS	Base de dados REDIS.	6379	UDP/TCP

As portas apresentadas acima são padrões de quando o sistema é instalado. Todavia, todas estas portas podem ser alteradas manualmente pelo usuário.

VI. LICENCIAMENTO E ATUALIZAÇÕES

O Licenciamento é feito por meio de arquivo de validação de licença. O mesmo deve ser exportado de cada um dos servidores Master rodando o sistema.

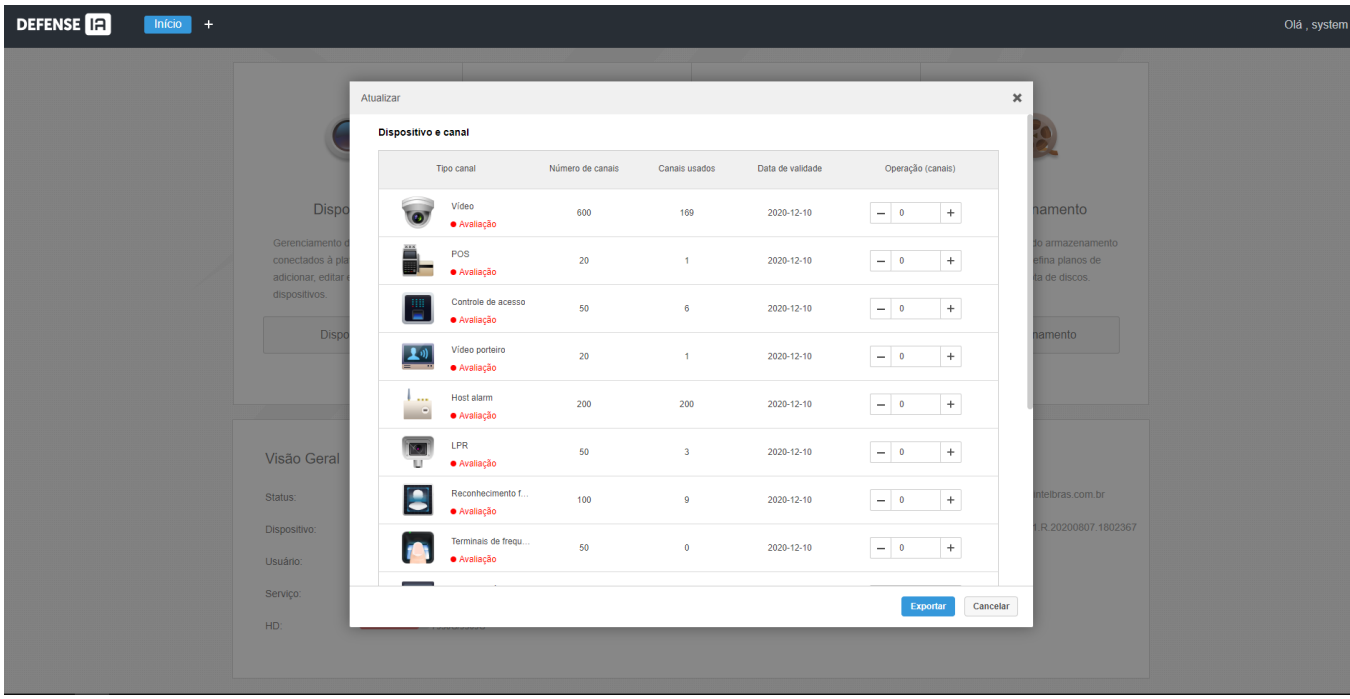


Imagem 4 - Menu de exportação da Licença

O usuário selecionará as quantidades necessárias de canais/licenças e módulos necessários em seu cenário e exportá o arquivo de licença. O mesmo deve ser encaminhado ao representante responsável pelo projeto da Intelbras, o qual entregará pelo setor responsável com a validação das licenças. Após licença validada, um arquivo

License.dat será enviado ao cliente, o qual deve ser importado no menu de importação de licença na página WEB do servidor.

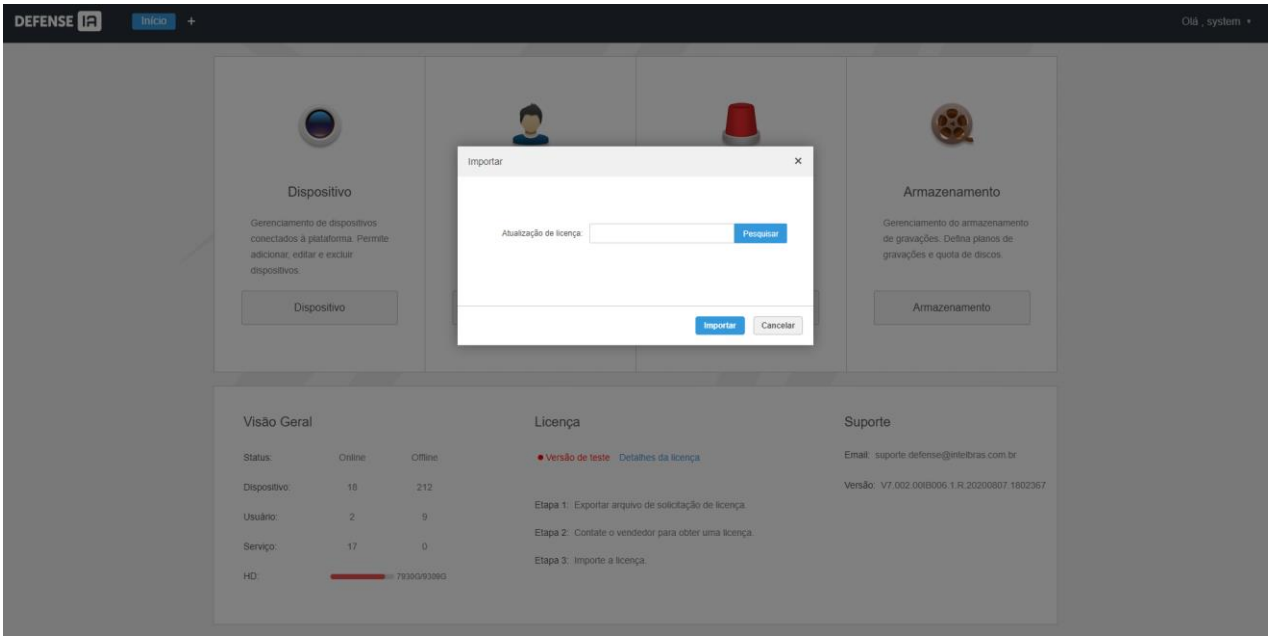


Imagem 5 - Menu de importação de Licença

O mesmo arquivo de licença pode ser utilizado, utilizado ao fazer downgrade ou upgrade de versão, desde que essa seja pertencente a mesma baseline (Ex: V1.0 para V1.x). Possibilidade de upgrade por instalação em cima da versão anterior já instalada no sistema ou desinstalação e reinstalação do sistema (possibilidade de fazer procedimento de Backup manual para retenção das informações do sistema).

A licença do Software é disponibilizada de forma vitalícia ao USUÁRIO, no entanto, a garantia de suporte e correção de bugs são de responsabilidade da Intelbras por vício do software pelo prazo de 1(um) ano a contar da compra da licença, sendo que após este período, a Intelbras poderá vir a cobrar pela prestação de serviços de manutenção, atualização, suporte técnico e demais serviços. A Intelbras fornece a atualização, dentro da mesma versão base do software (Ex: V1.0 para V1.x. Não incluí atualização de base de software, como 1.X para 2.X ou superiores), dentro de um prazo de 1(um) ano.

Além do mais, a partir do período de 5(cinco) anos a contar da compra da licença do Software pelo USUÁRIO, a INTELBRAS poderá modificar ou descontinuar (temporária ou permanentemente) a distribuição ou a atualização desse serviço e não é obrigada a fornecer nenhum tipo de suporte.

A partir do prazo de 1(um) ano, a INTELBRAS e seus fornecedores isentam-se de quaisquer garantias e condições expressas ou implícitas incluindo, sem limitação, garantias de comercialização, adequação, titularidade e não violação no que diz respeito ao serviço e a qualquer um de seus componentes ou ainda à prestação ou não de serviços de suporte.

A INTELBRAS não garante que a operação desse serviço seja contínua e sem defeitos. Com exceção do estabelecido neste documento, não há outras garantias, condições ou promessas vinculadas ao serviço, expressas ou implícitas, e todas essas garantias, condições e promessas podem ser excluídas de acordo com o que é permitido por lei sem prejuízo à Intelbras e a seus colaboradores.

I. A INTELBRAS não garante, declara nem assegura que esse serviço esteja livre de perda, interrupção, ataque, vírus, interferência, pirataria ou outra ameaça à segurança e isenta-se de qualquer responsabilidade em relação a essas questões. Você é responsável pelo backup dos arquivos armazenados em seu dispositivo.

II. A INTELBRAS se isenta de responsabilidade quanto à funcionalidade do SOFTWARE e à prestação de suporte técnico/pós-venda, inclusive no período de garantia de 1 (um) ano, caso a instalação, manutenção, configuração, operação do SOFTWARE tenha sido realizada por profissional não qualificado e que não possua a Certificação ITEC Software Defense IA.

III. Em hipótese alguma a INTELBRAS, bem como seus diretores, executivos, funcionários, afiliadas, agentes, contratados o responsabilizar-se-ão por perdas ou danos causados pelo mau uso do software.
O Kit de Licença Defense IA Master (9940176), também conhecida como base, inclui as seguintes licenças:

-Licença para 64 câmeras;

-Licença para 2 canais de reconhecimento facial;

-Licença para 2 canais para leitura de placa (LPR);

-Licença para 64 portas de controle de acesso;

-Licença para 2 painéis de alarme.

VII. CAPACIDADE DO SISTEMA

Organização	
Organização	10 hierarquias, 999 organizações por hierarquia
Grupos de usuários	100
Usuários	200 simultâneos, 2500 no total
Dispositivos totais	
Dispositivos totais	2000 dispositivos
Dispositivos de vídeo e canais	
Total de dispositivos de vídeo e canais	1000 dispositivos, 2000 canais
ONVIF	200 dispositivos, 800 canais
Dispositivos de LPR	64 canais
Canais de reconhecimento facial	100 canais

Canais de detecção de objeto	20 canais
Canais de mapa de calor	64 canais
Canais de contagem de pessoas	100 canais
Canais de imagem térmica	20 canais
Dispositivos de Controle de Acesso	200 IPs, 1024 Portas
Dispositivos de Painel de Alarme	50 dispositivos
Transmissão de mídia por servidor	
Input de vídeo por servidor	600 Mbps
Output de vídeo por servidor	600 Mbps
Reprodução, armazenamento e download	
Largura de banda da reprodução por servidor	100 Mbps
Capacidade máxima de armazenamento no servidor	200 TB
Tarefas de download	5
Máximo de planos de gravação	100
Alarme	
Regras de alarmes	200
Mapa	
Hierarquia	8 hierarquias
Submapa	32 por hierarquia
Tamanho do mapa de bits	14,7 MB
Pontos por mapa (entrada de alarme da câmera e etc.)	Até 300 (GIS e Raster)
LPR	
Blacklist de veículos	100
Número de seções	100
Informações de registro	
Registros de alarme	5.000.000*
Registros de imagens de faces capturadas	5.000.000*
Registros de placas lidas (LPR)	5.000.000*
Registros de violação	5.000.000*
Registros de velocidade média	5.000.000*
Registros de contagem de pessoas	5.000.000*
Registros de mapa de calor	5.000.000*
Logs	5.000.000*

Eventos	
Eventos totais	300/s**
Eventos de LPR com foto	15/s**
Alarmes com foto	50/s**
Capturas de face com foto	150/s**
Detecções de objeto com foto	50/s**
Eventos de Controle de Acesso	20/s**
Eventos de Painel de Alarme	2/s**
Sistema distribuído	
Número de servidores	
Número de servidores escravos	Até 20
Canais e dispositivos	
Dispositivos totais	5000 dispositivos
Canais e dispositivos de vídeo	
Canais e dispositivos de vídeo totais	5000 dispositivos, 20000 canais
ONVIF	500 dispositivos, 2000 canais
Canais de LPR	320 canais
Canais de reconhecimento facial	500 canais
Canais de detecção de objetos	100 canais
Canais de mapa de calor	320 canais
Canais de contagem de pessoas	500 canais
Canais de imagem térmica	100 canais
Dispositivos de Controle de Acesso	600 IP, 3072 portas
Dispositivos de Painel de Alarme	50 dispositivos
Eventos	
Eventos totais	600/s**
Eventos de LPR com foto	150/s**
Alarmes com foto	150/s**
Capturas de face com foto	350/s**
Detecções de objeto com foto	100/s**
Eventos de Controle de Acesso sem foto	120/s**
Eventos de Painel de Alarme	5/s**
Sistema em cascata	
Número de cascateamento	
Níveis de cascateamento	3
Número de servidores cascateados	20
Canais e dispositivos	

Canais e dispositivos de vídeo totais em cascata	5000 dispositivos, 20000 canais
ONVIF	500 dispositivos, 2000 canais
***O número de registros depende da capacidade do disco.** ****A soma de cada um dos tipos de evento não pode exceder o número total de eventos. Os eventos de alarme com foto assim como os eventos de detecção de objeto equivalem à três eventos de detecção facial.**	

A Intelbras e o Defense IA atendem as seguintes normas:

LGPD Lei nº 13.853, de 2019; GDPR (EU) 2016/679; ISO 9001.

VIII. INTEGRAÇÕES E HOMOLOGAÇÕES COM TERCEIROS

O Defense IA é um software de desenvolvimento próprio da Intelbras. Dessa maneira, deve-se checar com a Intelbras a possibilidade de desenvolvimento de integrações e homologações de software/hardware/protocolos de terceiros com a solução do Defense IA.

Até o presente momento, o Defense IA funciona de forma autônoma e é independente de aplicações de terceiros. Com relação a compatibilidade com hardware de terceiros de CFTV IP, o Defense tem compatibilidade com protocolo ONVIF.

Apêndice 2 - Recomendações de cibersegurança

A cibersegurança é mais do que apenas uma palavra da moda: é algo que se aplica a todos os dispositivos conectados à Internet. A vigilância por vídeo IP não é imune a riscos cibernéticos, mas tomar medidas básicas para proteger e fortalecer redes e dispositivos em rede os tornará menos suscetíveis a ataques. Abaixo estão algumas dicas e recomendações sobre como criar um sistema de segurança mais seguro.

Ações obrigatórias a serem tomadas para segurança de rede de equipamentos básicos:

1. **Use senhas fortes**

   Siga as seguintes sugestões para definir senhas:
   - O tamanho não deve ser inferior a 8 caracteres;
   - Inclua pelo menos dois tipos de caracteres; letras maiúsculas e minúsculas, números e símbolos;
   - Não conter o nome da conta ou o nome da conta na ordem inversa;
   - Não use caracteres contínuos, como 123, abc, etc .;
   - Não use caracteres sobrepostos, como 111, aaa, etc .;
2. **Manter os softwares atualizados (Server, Client e firmware dos dispositivos)**
   - De acordo com o procedimento padrão na indústria de tecnologia, recomendamos manter o firmware do seu equipamento (como NVR, DVR, câmera IP, etc.) atualizado para garantir que o sistema esteja com as correções de segurança mais recentes. Quando o equipamento estiver conectado à rede pública, é recomendável habilitar a função “verificação automática de atualizações” para obter informações oportunas das atualizações de firmware divulgadas pelo fabricante.
   - Sugerimos que você baixe e use a versão mais recente do software.

Boas práticas para melhorar a segurança da rede do seu equipamento:

1. **Proteção Física**

   Sugerimos que você execute proteção física aos equipamentos, principalmente dispositivos de armazenamento. Por exemplo, coloque o equipamento em uma sala e gabinete de computador especial e implemente uma permissão de controle de acesso e gerenciamento de chaves para evitar que pessoas não autorizadas realizem contatos físicos, como hardware danificado, conexão não autorizada de equipamento removível (como disco flash USB , porta serial), etc.
2. **Alterar senhas regularmente**

   Sugerimos que você altere as senhas regularmente para reduzir o risco de ser adivinhado ou quebrado.
3. **Definir e atualizar as informações de redefinição de senhas em tempo hábil**

   O equipamento suporta a função de redefinição de senha. Configure as informações relacionadas para redefinição de senha a tempo, incluindo a caixa de correio do usuário final e perguntas sobre proteção de senha. Se as informações mudarem, modifique-as a tempo. Ao definir questões de proteção de senha, sugere-se não usar aquelas que podem ser adivinhadas facilmente.
4. **Habilitar bloqueio de conta**

   O recurso de bloqueio de conta é habilitado por padrão e recomendamos que você o mantenha para garantir a segurança da conta. Se um invasor tentar fazer login com a senha errada várias vezes, a conta correspondente e o endereço IP de origem serão bloqueados.
5. **Alterar HTTP padrão e outras portas de serviço**

   Sugerimos que você altere o HTTP padrão e outras portas de serviço para qualquer conjunto de números entre 1024 ~ 65535, reduzindo o risco de intrusos serem capazes de adivinhar quais portas você está usando.
6. **Habilitar HTTPS**

   Sugerimos que você habilite o HTTPS, para que você visite o serviço da Web por meio de um canal de comunicação seguro.

7. **Habilitar lista de permissões**
   Sugerimos que você habilite a função de lista de permissões para evitar que todos, exceto aqueles com endereços IP especificados, acessem o sistema. Portanto, certifique-se de adicionar o endereço IP do seu computador e o endereço IP do equipamento que o acompanha à lista de permissões.
8. **Ligação de endereço MAC**
   Recomendamos que você vincule o endereço IP e MAC do gateway ao equipamento, reduzindo assim o risco de spoofing de ARP.
9. **Atribuir contas e privilégios de maneira razoável**
   De acordo com os requisitos de negócios e gerenciamento, adicione usuários de maneira razoável e atribua um conjunto mínimo de permissões a eles.
10. **Desative serviços desnecessários e escolha modos seguros**
    Se não for necessário, é recomendado desligar alguns serviços, como SNMP, SMTP, UPnP, etc., para reduzir os riscos.
    Se necessário, é altamente recomendável que você use modos de segurança, incluindo, mas não se limitando aos seguintes serviços:
    - SNMP: Escolha SNMP v3 e configure senhas de criptografia e senhas de autenticação fortes.
    - SMTP: Escolha TLS para acessar o servidor de caixa de correio.
    - FTP: escolha SFTP e configure senhas fortes.
    - Ponto de acesso AP: escolha o modo de criptografia WPA2-PSK e configure senhas fortes.
11. **Transmissão criptografada de áudio e vídeo**
    Se o conteúdo dos seus dados de áudio e vídeo for muito importante ou sensível, recomendamos que você use a função de transmissão criptografada, para reduzir o risco de roubo de dados de áudio e vídeo durante a transmissão.
    Lembrete: a transmissão criptografada causará alguma perda na eficiência da transmissão.
12. **Auditoria Segura**
    - Verifique os usuários online: sugerimos que você verifique os usuários online regularmente para ver se o dispositivo está conectado sem autorização.
    - Verifique o registro do equipamento: Ao visualizar os registros, você pode saber os endereços IP que foram usados para fazer login em seus dispositivos e suas principais operações.
13. **Log de rede**
    Devido à capacidade limitada de armazenamento do equipamento, o registro armazenado é limitado. Se você precisar salvar o log por um longo período, é recomendável habilitar a função de log da rede para garantir que os logs críticos sejam sincronizados com o servidor de log da rede para rastreamento.
14. **Construir um ambiente de rede seguro**
    Para melhor garantir a segurança do equipamento e reduzir potenciais riscos cibernéticos, recomendamos:
    - Desative a função de mapeamento de porta do roteador para evitar o acesso direto aos dispositivos da intranet da rede externa.
    - A rede deve ser particionada e isolada de acordo com as necessidades reais da rede. Se não houver requisitos de comunicação entre duas sub-redes, sugere-se o uso de VLAN, GAP de rede e outras tecnologias para particionar a rede, de modo a obter o efeito de isolamento da rede.
    - Estabeleça o sistema de autenticação de acesso 802.1x para reduzir o risco de acesso não autorizado a redes privadas.
    - É recomendável que você habilite o firewall ou a lista de bloqueio do seu dispositivo e o recurso de lista de permissões para reduzir o risco de que o seu dispositivo seja atacado

Apêndice 3 – API e SDK da aplicação

O software Defense IA conta com API e SDK para integração. Tal documentação só pode ser adquirida após o firmamento de um contrato de confidencialidade (NDA) com a Intelbras.

Para realizar o NDA entre em contato com o suporte da Intelbras.