

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
	Indica um perigo potencial alto que, se não for evitado, resultará em problemas graves no sistema.
	Indica um perigo potencial médio ou baixo que, se não for evitado, pode resultar em problemas leves ou moderados.
	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.
	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

PREFÁCIO
1 INSTALAÇÃO E IMPLANTAÇÃO8
1.1 REQUISITOS DO SERVIDOR
1.2 INSTALANDO O SERVIDOR PRINCIPAL
1.3 INSTALANDO SUB SERVER 12
1.4 GERENCIANDO SERVIÇOS DE PLATAFORMA
1.5 CONFIGURANDO LAN OU WAN 16
1.5.1 Configurando o roteador 16
1.5.2 Configurando a plataforma Defense IA16
1.6 DESINSTALANDO A PLATAFORMA 17
2 CONFIGURAÇÕES BÁSICAS 18
2.1 LOGIN NO GERENCIADOR WEB 18
2.2 ATIVANDO A PLATAFORMA 19
2.2.1 Capacidade de licença 19
2.2.2 Solicitando uma licença 20
2.2.3 Ativando ou Atualizando Licença 20
2.3 ADICIONANDO ORGANIZAÇÃO 20
2.4 GERENCIANDO DISPOSITIVOS
2.4.1 Procurando Dispositivos Online 22
2.4.2 Inicializando dispositivos 23
2.4.3 Modificando o endereço IP do dispositivo
2.4.4 Adicionando Dispositivos26
2.4.5 Dispositivos de edição 32
2.4.6 Recursos de vinculação 36
2.5 ADICIONANDO FUNÇÃO E USUÁRIO 38
2.5.1 Adicionando função de usuário 38
2.5.2 Adicionando usuário

2.5.3	(Opcional) Configurando o usuário do domínio41
2.6 (CONFIGURANDO A GRAVAÇÃO DOS DISPOSITIVOS
2.6.1	Configurando o Plano de Gravação 43
2.6.2	Adicionando Modelo de Tempo 45
2.6.3	Configurando o backup de armazenamento 47
2.6.4	Configurando os Discos de Armazenamento 49
2.6.5	Configurando a cota de grupos dos discos 53
2.7	EVENTO E ALARME
2.7.1	Configurando Eventos 55
2.7.2	Configurar atributo de alarme64
3 Fl	JNÇÕES 66
3.1 F	PREPARATIVOS
3.1.1	Instalando o Cliente 66
3.1.2	Login no cliente70
3.1.3	Página inicial do cliente de controle72
3.1.4	Configuração Local73
3.2 \	/ISUALIZAÇÃO
3.2.1	Visualizando Vídeo ao Vivo82
3.2.5	Tour
3.2.6	Visualização 90
3.2.7	Favoritos
3.2.8	Região de Interesse
3.2.9	Foco eletrônico
3.3 /	ANÁLISE INTELIGENTE 100
3.3.1	Topologia Típica 100
3.3.2	Configurando Análise Inteligente 101
3.4 /	ANÁLISE DE FLUXO 126
3.4.1	Topologia Típica 127
3.4.2	Fluxo de Negócios128

3.4.3	Configurando a Análise de Fluxo128		
3.4.4	Aplicativos de análise de fluxo141		
3.5 F	RECONHECIMENTO FACIAL		
3.5.1	Topologia Típica 145		
3.5.2	Fluxo de Negócios147		
3.5.3	Configurando o reconhecimento facial147		
3.5.4	Aplicativos de reconhecimento facial156		
3.6 A	ANÁLISE FORENSE		
3.6.1	Topologia Típica 165		
3.6.2	Fluxo de Negócios165		
3.6.3	Aplicação de Análise Forense 166		
3.7 N	MÓDULO BI (BUSINESS INTELLIGENCE) 172		
3.7.1	Análise de Fluxo e Demografia do Cliente 172		
3.7.2	Análise de área 178		
3.7.3	Loja em tempo real184		
3.7.4	Utilização do Defense Client com B.I 191		
3.8 0	CONFIGURANDO N + M 195		
3.9 (CASCATA		
3.9.1	Instalação do Defense IA 198		
3.9.2	Licenciamento198		
3.9.3	Configuração de Domínio 199		
3.9.4	Usabilidade do domínio 202		
3.10 0	GRAVAÇÃO E REPRODUÇÃO 204		
3.10.1	Preparativos		
3.10.2	204 2Reprodução		
3.10.3	Buscando por miniaturas		
3.11 CONFIGURAÇÃO DO SISTEMA			
3.11.1 Certificado HTTPs 219			
3.11.2Configuração do servidor de correio			

3.12 GERENCIAMENTO DE SERVIDOR	220
3.12.1 Gerenciamento de Servidor	220
3.12.2Configuração de recursos	221
3.13 MANUTENÇÃO DE SENHA	222
3.13.1 Modificando senha	222
3.13.2Redefinindo senha	223
4 MANUTENÇÃO	225
4.1 CONFIGURANDO O PERÍODO DE ARMAZENAMENTO DE DADOS	NO
SISTEMA.	225
4.2 ATUALIZANDO CERTIFICADO DO SOFTWARE	225
4.3 LOG REMOTO	227
4.4 SINCRONIZAÇÃO DE HORÁRIO	227
4.4.1 Sincronização Agendada de Horário	227
4.4.2 Sincronização de Horário Manual	228
4.5 BACKUP E RESTAURAÇÃO	229
4.5.1 Backup do sistema	229
4.5.2 Restauração do sistema	231
4.6 REGISTRO	234
4.7 MANUTENÇÃO DE SISTEMA	235
4.7.1 Visão global	235
4.7.2 Status de execução	236
4.7.3 Estado do servidor	237
4.7.4 Informação de Evento	239
4.7.5 Informação da Origem	239
APÊNDICE 1 - ANEXO I	044
	241



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

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

Tabela 1 - Requisito de hardware

1.2 INSTALANDO O SERVIDOR PRINCIPAL

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

Geral Compa	tibilidade Archive Segurança Detalhes Versões Anteriores		
F	ermica_Win32_IS_V7.002.0000003.0.T.20200501		
Tipo de arquivo:	Aplicativo (.exe)		
Descrição	Cópia de 1099363_Defense_Termica_Win32_IS_V7		
Local	C:\Users\ualac\Downloads		
Tamanho:	1,32 GB (1.418.143.426 bytes)		
Tamanhoem disco:	1,32 GB (1.418.149.888 bytes)		
Criado em:	quarta-feira, 1 de julho de 2020, 14:00:52		
Modificado em:	quarta-feira, 1 de julho de 2020, 14:03:07		
Acessado em:	quarta-feira, 1 de julho de 2020, 14:03:07		
Atributos:	Somente leitura Dculto Avançados		
Segurança:	Este arquivo veio de outro computador, e pode ser bloqueado para ajudar a proteger este computador.		

Figura 1 - Desbloqueio o arquivo ".zip"

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

 \square 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.





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.

 \square

- 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"

Geral Compa	tibilidade Archive Segurança Detalhes Versões Anteriores		
LA.	emica_Win32_IS_V7.002.0000003.0.T.20200501		
Tipo de arquivo:	Aplicativo (.exe)		
Descrição:	Cópia de 1099363_Defense_Termica_Win32_IS_Vi		
Local	C:\Users\ualac\Downloads		
Tamanho:	1,32 GB (1.418.143.426 bytes)		
Tamanhoem disco:	1,32 GB (1.418.149.888 bytes)		
Criado em:	quarta-feira, 1 de julho de 2020, 14:00:52		
Modificado em:	quarta-feira, 1 de julho de 2020, 14:03:07		
Acessado em:	quarta-feira, 1 de julho de 2020, 14:03:07		
Atributos:	Somente leitura Oculto Avançados		
Segurança:	Este arquivo veio de outro computador, e pode ser bloqueado para ajudar a proteger este computador.		

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

 \square

- 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 On 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 🚇.

1				2345678
				8 8 9 0 - ×
Reiniciar todos os serviços	🛿 Para todos 🖸 Atualizar]		9 💿 Executando
Serviço 🗘	Porta	Status do servidor	Informação de exceção	Operação
Defense_OSS	HTTP:9900 HTTPS:9901			,
MySQL				,
Defense_MTS				1
Defense_MQ	OPENWIRE:61616 MQTT:1883 JETTY:8161			1
Defense_MGW	9090			1
Defense_MCDRadar		Online		
Defense_MCDPos				1
Defense_MCDLed		Online		
Defense_MCDDoor				
Defense_MCDAlarm				
Defense_HRS				
Defense_EAS				
Defense_DMS		Online		1
Defense_ARS		Online		1
Defense_ADS				/
& Abrir Interface web 11				10

Figura 9 - Interface de gerenciamento de serviço



Nº.	Função	Descrição
		Gerenciamento de serviços, ele suporta os
4	Gestão	seguintes três tipos de operação:
1	de Serviços	Clique em "Reiniciar todos os serviços" para reiniciar todos os servicos.
		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.
	Abrir	
11	Administrador	Vai para o Gerenciador Web que é usado pelos administradores do sistema
	Cliente	

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

DEFENSE IA				∎∎•••••-×
Reiniciar todos os serviços	II Para todos 🖸 Atualizar			Executando
Serviço 🛟	Porta	Status do servidor	Informação de exceção	Operação
Defense_OSS	HTTP:9900 HTTPS 9901			1
MySQL				1
Defense_MTS				1
Defense_M0	OPENWIRE 61616 MQTT:1683 JETTY:0161	Online		,
Defense_MGW	9090			1
Defense_MCDRadar		Online		
Defense_MCDPos		Online		1
Defanse_MCDLed		Online		
Defanse_MCDDoor				
Defense_MCDAlarm		Online		
Defense_HRS				
Defense_EAS		Online		
Defense_DMS		Online		1
Defense_ARS		Online		1
Defense_ADS				1
🌆 Abrir Interface web				

Passo 2. Clique na 🔯 no canto superior direito.

Figura 11 - Configuração

Configurar rede de mapear	nento LANAVAN	
IP CMS:		
IP de mapeamento:		
	ок	Cancelar

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.

 \square

- 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

DEFENSE IA Inicio +							Olá , syster
		۲		2		۲	
	Gerencia conectar adiciona dispositi	Dispositivo mento de dispositivos los à plataforma. Permite r, editar e excluir ros.		Usuário Gerenciamento de usuários e funções. Permite o gerenciamento e permissões dos usuários.	Eventos Gerenciamento de avisositaliarmes de eventos dos dispositivas ou do salemar. Parente vincular ações aos receber eventos.	Armazenamento de gravações. Detina planos de gravações e quata de discos.	
	Visão	Seral		Licenca		Suporte	
	Status	Online	Offline	Versilo de teste De	talhes da licença	Email: suporte.defense@intelbras.com.br	
	Dispositivo	C (11)	3	Etapa 1: Exportar arqui	No de solicitação de licença.	Versão: V7.002.00(B006.1.R.20200807.1802367	
	Usuário: Servico:	1	16 D	Etapa 2. Contate o ven	idedor para obter uma licença.		
	HD:		= 1800/5890	Etapa 3: Importe a licer	nça.		

- 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 ana 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.

DEFENSE IA	Início +						Olá , system •
		Dispositivo dispositivo adicionar, editar e excluir dispositivos. Dispositivo	25 mite	Usuário Usuário Gerenciamento de usuários e trunções. Permite o gerenciamento e permissões dos usuários.	Eventos Gerenciamento de avisoratarmes de eventos dos dispositivos ou do sasterna. Permite vincular ações aos receber eventos	Contraction de arrangemento de gravações. Defina planos de gravações e quota de dacos. Armazenamento	
		Visão Geral Status: Online Dispositivo: 11 Usuano: 1 Serviço: 17 HD:	Offline 3 16 0 1800/5890	Licença • Versão de teste D Elapa 1. Exportar arqu Elapa 2. Contate o ve Elapa 3. Importe a lice	etañtes da Icença uivo de solicitação de licença. Indedor para otder uma licença. exça	Suporte Email: suporte defense@intelbras.com.br Versão: V7.002.0018006.1.R.20200807.1802367	

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 te selecione Organização na interface da nova guia.

Organização × +									Olá , system ▪
+ Adicionar 📋 Excluir	÷ 14	lover para					Q, Pesquisa	K	
Q. Pesquisar		Nome do Dispos +	ID do dispositivo	Endereço IP +	Tipo e	Servidor +	Porta	Status #	
★ III (TEC) ∴ ITEC	0	VIP 5550 Z IA ITEC	1000072	10.100.43.54	IPC Dimenitive LPR	Servidor Central	37777	Online	
 Portaria 1 injetoras 		AMT 2018 EG - Treina	1000068	10,100,13,20	Painel de Alarme	Servidor Central	37777	Online	
 Portaria 2 Fábrica 	0	VIP-3240-IA VIP 5550 Z IA	1000048	10.100.15.53	IPC	Servidor Central Servidor Central	37777	Online Online	
 Recebimento Area interna 		VIP 7223 SD R	1000015	10.100.15.19	IPC	Servidor Central	42719	Online	
Alarmes Alarmes Alarmes ATORRE A		MHDX 3132	1000071	10.100.21.142	DVR	Servidor Central	37777	 Offline 	
슈 ATORRE B 슈 ATORRE C 슈 ATORRE D									

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

+ Adicionar 💼 Excluir
Q Pesquisar
▼ III ITEC
itec
Portaria 1
Injetoras
📩 Portaria 2
🕨 📩 Fábrica
📩 Recebimento
🕨 💼 Area interna
📩 Alarmes
÷ Intercom
📩 A TORRE A
📩 A TORRE B
📩 A TORRE C
📩 A TORRE D
hova organização1





Operações

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

Ш

- 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

DEFENSE	nização Dispositivo × +							Olá , sys	tem +
4	Dispositivo	⇒ Conectar	Ø Atualizar	() Inicializar dispositivo	🖋 Alterar IP	👂 Segmento da rede	Minimizar 🔺		
1	Recurso de vinculação	C Sta	tus de inicialização+	Endereço IP+	Modeloe	Insira e IP Inicial.	MAC		
			 Inicializado 	10.0.0.45	VIP-5500-F	- Insira o IP final	27:25		
			• Inicializado	10.1.19.70	A\$17223X-A-T1	Pesquisar	b0.06		
			 Inicializado 	10.1.53.123	VIP-E6400-G2		186.86		
			Inicializado	10.100.44.54	VIP-3212-SD-IR	37777 58.10.8c	97.25.b1		

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.

- <u>___</u>
 - Você pode selecionar vários dispositivos para inicializá-los em lotes. Certifiquese de que os dispositivos selecionados tenham o mesmo nome de usuário, senha e informações de e-mail.
 - Clique

 ou

 coluna de status e, em seguida, você pode ver todos os dispositivos não inicializados.

Initialize Device			×
1.Set Password		1.Set Password 2.Password Secur	e 3.Change IP
Username:	admin		
New Password:	*		
Confirm:	*		
		Password Secure →	Cancel

Figura 18 - Configurar senha

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

Initialize Device				×
2.Password Secure		1.Set Password	2.Password Secure	3.Change IP
Bind Email Address:	•			
		Back	Change IP →	Cancel

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

Initialize Device			×
3.Change IP	1.Set Password	2.Password Secure	3.Change IP
New IP-			
Subnet Mask			
Default Gateway:			
	Back	ОК	Cancel

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.

Modify Device IP						×
1.Validate				1.V	alidate	2.Change IP
	Username:	*				
	Password:					
			CI	hange IP	-+	Cancel

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

Modify Device IP		×
2.Change IP	1	.Validate 2.Change IP
New IP:	*	
Subnet Mask:	*	
Default Gateway:	*	
	Back OK	Cancel

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

26

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

Cevice	<u>5</u> ∓ Co	nnect 🕻	Refresh	() Initialize Device	🖋 Chan	ge IP			Network Segment	Config	Pack Up	
Bind Resource		Ir	iit Status	IP Add	ress +	Type	•	Port		MAC A	ddress	
	•	•	Initialized			Unknown	n	37777				Ĥ
		•	Initialized			NVR		37777				
		•	Initialized			NVR		37117				
		•	Initialized			IPC		37755				
	+ ^	8 8 0	elete 🔒 N	lod 🛓 im	ıp	Org:	root		• ٩			
	AI	Encoder	Decoder Video	Wall ANPR I	Matrix Access	Control Led Devi	ce Video Interco	om Emergency				
		Device ID	IP/Domain •	Home Server •	Device Name	• Type •	Org	Status •	Offline Cause	c	peration	
		1001885		Center Server	1.0000	Access Snapsho	root	 Offline 	Network anomaly	y. ,	/ ×	
		1001880		Center Server		EVS	root	 Offline 	Network anomaly	y. ,	r ×	
		1001878		Center Server		VTH	root	 Offline 	Network anomaly	y. ,	/ ×	
		1001875		Center Server		Access Snapsho.	. root	 Offline 	Network anomaly	y. ,	/ ×	
		1001874		Center Server	1.00	NVR	root	 Offline 	Network anomaly	y. ,	×	
		1001873		Center Server		Unit VTO	COMPANY.	• Offine	Network anomaly	y. ,	/ ×	
		1001872		Center Server		VTH	constant and	i o Offine	Network anomal)	y. ,	×	

Figura 23 - Dispositivo

Passo 2. Clique em Adicionar.

Add All	×
1. Login Information.	1.Login Information 2.Device Information
Protocol:	Tables •
Manufacturer:	Total •
Add Type:	IP Address •
Device Category:	Encoder •
IP Address:	•
Device Port:	• 37777
User:	◆ admin
Password:	•••••
Org:	PTZ •
Video Server:	Center Server •
	Add Cancel

Figura 24 - Adicionar um dispositivo (1)

Passo 3. Defina os parâmetros.



 \square

- 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.

Add All	×
2. Device Information.	1.Login Information 2.Device Information
Device Name:	*
Туре:	DVR •
Device SN:	
Role:	Administrator, Operator
Video Channel:	
Alarm Input Channel:	
Alarm Output Channel:	
	Back Continue to add OK

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.

Batch Add		×
Org:	root 💌	
Video Server:	Center Server 🔹	
User:	* admin	
Password:	•••••	
	OK Cancel	

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 interco	omunicação	o de vídeo ((1)
						· · /

Import Interc	om Device	×
Import	Download Intercom Device Template	
	No Import file	
	ОК	

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.

 \square

 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.



2)

Import Inte	Import Intercom Device				
Import	Download Intercom Device Template				
	Prompt	×			
	import Successfully 1 Record(s). Import Failed 0 Record(s).				
		ОК			

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 ^C da lista de dispositivos.

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

Edit Device					×
Basic Info	Input Info				
Video Channel	Protocol:		Manufacturer:		Ψ
Decode Channel	IP Address:	• 2010 10 m	User:	• 80001	
	Device Port:	• 37777	Password:		
	Video Server:	Center Server *	Org:	root	•
	Device Details	5			
	Device Name:	•	Device SN:		
	Type:	NVD *			
Get Info				ОК Са	ancel

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.



Edit Device		×
Basic Info	Channel Amount: • 1 Stream Type: Main Stream •	
Video Channel	Name Camera Type Features SN	KeyBoard Code
Alarm Input Channel	Channel0 Fixed Camera Intelligent Alarm,Elec	
Alarm Output Channel		
	Total 1 record(s)	I≪ 1/1 ► ►I
Get Info	(OK Cancel

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.

 \square

- 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.

Edit Device		×
Basic Info	Channel Amount: 2	
Video Channel	Name	AlarmType
Alarm Input Channel	* 86_1	External Alarm 🔹
		External Alarm
Alarm Output Channel	* 86_2	Infrared Detect
		Zone Disarm
		PIR
		Gas Sensor
		Smoke Sensor
		Glasses Sensor
		Emergency Button
		Stolen Alarm
		Perimeter
		Preventer Move
		Total 2 record(s)
Get Info		OK Cancel

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.

Edit Device	×
Basic Info	Channel Amount: 2
Video Channel	Name
Alarm Input Channel	* 86_1
Alarm Output Channel	* 86_2
	Total 2 record(s)
Get Info	OK Cancel

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.

Dispositivo	+ Adicion	ar 💼 Excluir Tipo d	e can Todos	Dispositivo: iTEC	▼ Q,	Pesquisar
Recurso de vinculação		Organização	Canal do dispositivo.	Tipo canal	Canais associados	Operação
		ITEC	VIP 5550 Z IA iTEC_1	Canal vídeo	VIP 5550 Z IA ITEC_1	e x
		ITEC	POS1	Canal POS	mm	e x
		ITEC	CAM 32	Canal vídeo	CAM 32	e x
		ITEC	CAM 31	Canal vídeo	CAM 31	/ X
		ITEC	CAM 30	Canal vídeo	CAM 30	× ×
		ITEC	CAM 29	Canal vídeo	CAM 29	/ ×
		ITEC	CAM 28	Canal vídeo	CAM 28	/ ×
		ITEC	CAM 27	Canal vídeo	CAM 27	/ ×
		ITEC	CAM 26	Canal vídeo	CAM 26	/ ×
		ITEC	CAM 25	Canal vídeo	CAM 25	/ ×
		ITEC	CAM 24	Canal vídeo	CAM 24	/ ×
		ITEC	CAM 23	Canal vídeo	CAM 23	/ ×
		ITEC	CAM 22	Canal vídeo	CAM 22	/ ×
		ITEC	CAM 2	Canal vídeo	CAM 2	/ X
		ITEC	CAM 2	Canal vídeo	CAM 2	/ X
	Total 54 gra	vação(ões).		٩ 1	2 3 4 🕨	Vá para 1 Ir

Figura 34 - Recurso de vinculação

Passo 3. Clique em Adicionar.

Figura 35 - Adicionar recurso para vincular

Adicionar vinculação de recursos	×
Tipo de canal de origem	Canal de vídeo
Todos	Q Pesquisar
Q. Pesquisar	▼ L
	🗌 🌧 Nova organização0
▼ III ITEC	Recebimento
▼ m ITEC	Area interna
▼ .	Alarmes
10.100.44.55_1	🗆 📩 Intercom
10.100.44.55_2	A TORRE A
10.100.44.55_3	► 🗌 📼 SVR 7116 IA
▶ 📼 iNVD9032	🗆 🌧 A TORRE B
Controle de acesso Facial	A TORRE C
Portaria 1	🗆 🏥 A TORRE D



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 te 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.

Adicionar Função			×
Informações básicas Nome: • Comentário:	Copiar de:	×	
Perm. disp. e loja	Controle de Permissões	Usuário Nome do Usuário	
árvore de dispositivos	Permissões de controle Menu de Permissões	system	
árvore de Loja	Menu do administrador Menu do cliente	kieser ualace	
		victor benaia	

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.

8 Role	🕇 Add	💼 Delete 🛃 Imp	ort Domain User		Q	Search
🔹 User		Username	Role	Status	User Type	Operation
		ym	Administrator	Online	Normal User	≙ ∕ ×
		asd		Offline	Normal User	🔒 🖉 🗙
		778888111	Administrator	Offline	Normal User	🔒 🖉 🗙
		778888	Administrator	Offline	Normal User	≙ ∕ ×
		1		Offline	Normal User	≙ ∕ ×
		Ш	Administrator,II	Offline	Normal User	🔒 🖉 🗶
		zhhq	Administrator	Offline	Normal User	🔒 🖉 🗶
		testfx	Administrator,Operator,II	 Offline 	Normal User	🔒 🖉 🗶
		А	A-role	Offline	Normal User	🔒 🖉 🗶
		chenjie	Administrator	Offline	Normal User	🔒 🖉 🗶
		21396	Administrator	Offline	Domain User	🔒 🖉 🗶
		Imx	Ш	Online	Normal User	🔒 🖉 🗶
		system	Administrator,99,100,120,121	Online	Normal User	P
	Total 13 reco	rd(s).			◀ 1 ▶	Go to page 1 Go

Figura 37 - Adicionar um usuário (1)

III. Clique em Adicionar.

Figura	38 -	Adicionar	um	usuário	(2)
iguiu	00	/ Glorial	um	usuuno	(~)

Basic Info								
	Usemame:	* mike			Password Expiry:	2020	-03-31	
Multiple Points	of Presence:				MAC Address:			
	Password:	*	•		PTZ Control Permission:	* 5		
	Confirm:	* •••••	••		Email Address:			
					Remark:			
Role				Device P	ermissions		Control Permissions	
	Rolena	me		Q, Sea	arch		 All Permissions 	^
	Administ	rator		▼ □	root		Control Permissions	- 11
	Operat	or		•	□ 10.33.68.8		Record	
	role1				Shannel0 €		Record Lock	
0	10101						PTZ	
							Audio Talk	~
							<	>

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 X 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.

- L. 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.

Active Directory				
Enable	SSL Encrypt			
Domain Name:	3000X.3000C.COM	Username:	X000X	
IP Address:		Password:		Test
Port:	389	Base DN:	DC=xxx,DC=xxx	Get DN

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	- L	.ogin	do	usuário	de	domínio
--	-----------	-----	-------	----	---------	----	---------

DEFENSE IA				×
	Usuário de domínio:	•		
	: 443	•	•	
	よ jhoantan	8		
I WW	٩			
	Lembrar I	Login auto		
		-		

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

DEFENSE IA Inicio	+				Olå , jhonatan 🔸
	۲	٥		۲	
	Dispositivo Geranciamento de dispositivos conectados à plataforma. Permite adicionar, editar e excluir dispositivos.	Usuário Ocrensismento de usuários e funções. Permite o generalismento o permiseões dos usuários.	Eventos Corenciamento de avisociólismes de eventos dos dispositivos ou do astorno. Permito vincular ações aso inceber eventos.	Armazenamento Orrenciamento do armazenamento de gravações. Defina planos de gravações o quota de discos.	
	Dispositivo	Usuário	Eventos	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.

DE	FENSE IA Início	Z	Armazen	amento × Dispositivo	· +			Olá , system ∙
	Plano de gravação		+ Ac	dicionar 💼 Excluir			Q.I	Pesquisar
	Plano de gravação backup			Nome do Plano	Modelo de tempo	Posição	Status	Operação
	Quota de grupos			gravação no storage	All-Period Template	Armazenamento no gravador	Ativado	on / x
	Configuração de Disco			Teste	All-Period Template	Armazenamento no servidor	Ativado	

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, significa que o plano foi habilitado, clique no ícone e ele se torna , 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.
- Clique no botão adicionar e o seguinte menu, Adicionar Plano de gravação, será aberto na tela.

Canais de vídeo disponíveis Plano de gravação	
Q Pesquisar	
Nome do Plano:	
▶ 🗋 📩 Portaria 1 Tipo transm: Stream Principal 🔻	
▶ 🗋 💼 Injetoras Modelo de tempo: All-Period Template 🔻	
Portaria 2	
Fábrica	
Comentário:	
Area interna Ativado	
Alarmes	
Intercom	
VIP 7223 SD R	

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 do stream que será gravado. Tendo como opções stream principal e
Tipo transmissão	stream extra.
	No caso do stream extra, o mesmo deve estar habilitado na câmera.
	Agendamento da gravação. O campo possui alguns modelos pré-
Modelo de tempo	configurados e também a possibilidade de criar planos personalizados.
	Verifique a parte do manual Adicionando Modelo de Tempo.
	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
Posição	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.
Ativada	Assim como o botão on/off do menu acima este check box habilita ou
Alivado	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

New	v Time Tem	plate																				×
Ten	nplate Name:	*					opy:					Ŧ										
Θ	0	1 2	3	4 4	56	7	8	9 1	10 1	1 1 - 1 -	12 1	3 1.	4 1: 	5 16	5 17	18	19	20	21	22	23 2	4
E	Mon																					牵
E	Tue																					¢
E	Wed																					¢
Ð	Thu																					÷
E	Fri																					中
E	Sat																					臣
E	Sun																					中
																			0	к	Cano	el

- 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.

Name: •																				
				(Copy:						Ψ									
0 1 . . . n	2	34	5	6	7 8	9	10) 1	1 1	2	13 1	4 1 :	5 16	17	18	19	20	21 2	2 23	24
9																				ф
d																				φ
L																				ф
																				ф
t																				¢
ı																				\$

Figura 45 - Defina o período de tempo por desenho

Clique no ^{an} do dia correspondente, defina o período de tempo na interface de configuração do período. Vejo0.

Period S	etup				×
Period1	02:00:00	÷	04:30:00	: •	• ×
Period2	06:00:00	* •	08:30:00	÷ •	- ×
Period3	12:00:00	÷	14:00:00	: •	• ×
Period4	17:30:00	-	20:15:00	: •	• ×
Mon	🗌 Tue	Wed	Thu 🗌 Fri	Sat [Sun
			o	K Ca	ancel

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.

EFENSE IA Início	Armazena	mento × +			Olá , system
🕴 Plano de gravação	🕂 Adi	cionar 💼 Excluir			Q, Pesquisar
Plano de gravação backup		Nome do Plano	Tamanho da grav. backup	Condição	Operação
Quota de grupos		backup SD cameras	12	00:00 - 23:59	CN / X
Configuração de Disco					

Figura 47 - Plano Backup

Operações

- Ativar / desativar plano de registro de backup.
- Na coluna de operação, significa que o plano foi ativado; clique no ícone e ele se tornará^{OFE}, 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 ^{m Delete} para excluir o plano em lotes.

Clique no correspondente ³⁴ 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.

Adicionar Plano de gravação backup				×
Canais de vídeo disponíveis	Parâmetro do plano de	e gravação de backup		
Q, Pesquisar				
	Nerre de Plane:			
ITEC	Nome do Plano.	*		
🕨 🗔 📩 Portaria 1	Condição:	Hora 🔻		
Injetoras			_	
🗌 💼 Portaria 2		00:00	3:59	
🕨 🗔 💼 Fábrica		0 12	24 12	24
Recebimento				
Area interna	Tamanho da grav. backup:	*	Hora	
Alarmes				
🗆 📩 Intercom	O plano de gravação de b	ackup realiza o backup da gravação arma	azenada em IPCs e NVRs de acord	o com a
VIP 7223 SD R	condição definida no Defe tempo de execução do pla	nse. Para a condição de tempo, pode-se ano de composição. Para Wi-Fi, pode faze	fazer gravação dentro de 1-24h ant er gravação de três dias antes.	tes do
			ОК Са	incelar

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 gravaçã 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.

 \square

- 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

Record Plan					Net	Disk Local Disk						
Backup Record Plan	🔶 Ad	id 💉 Format	0						All			
Group Quota	0	Server Name	IP	Volume Name	Capacity(GB)	Free Capacity(GB)	Disk Type	Disk status		Oper	ation	
Storage Config		Center Server	10.1.3.141	sjo-tedef-01-defe	100.00	0.00	Video	Normal	\$	÷		3
	0	Center Server	10.1.3.141	sjo-tedef-01-defe	95.00	0	Not set	Abnormal		4	×	

Ш

- 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^{III}.



• 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.

D	EFENSE	IA Início	Gerenci	iamento do Servidor	Armazenamento ×	+				Ol	á, system ▼
	E Plar	no de gravação		Adicionar Disco de Rede				×			
	🛗 Plar	no de gravação backup	+ /						[[Todos	•
	🎒 Quo	ota de grupos		Nome do	Servidor Central	•			Status do disco	Operação	
	🚦 Con	ifiguração de Disco		Servidor: Endereço IP:	•						
				Nome de Usuário:							
				Senha:							
							ov	Cancolar			
							UN	Cancelar			

- IV. Selecione o disco, clique em Formatar ou clique no victor próximo às informações do disco para formatar o disco correspondente.
- V. Selecione o tipo de disco de formato e clique em OK.

Format					×
	Disk Type:	Video		•	
				ок	Cancel
			_		

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
--------	----	----------------------------	--------

Plano de gravação		Disco de Rede <mark>Disco Local</mark>								
Plano de gravação backup	💰 Fo	♦ Formatar								
Quota de grupos		Nome do Servidor	Nome do disco	Capacidade (GB)	Capacidade tot	Tipo de disco	Status de integri	Status do disco	Qtde vagas	Operação
Configuração de Disco		Servidor Central	\\.\PhysicalDrive1	74.53	0.00	Vídeo		Normal	-1	φ.
		Servidor Central	\\.\PhysicalDrive2	149.05	137.38	Imagem de LPR		Normal	-1	\$
		Servidor Central	C:/	366.00	271.00	Imagem geral	ок	Normal	0	<i>ф</i>

- Passo 1. Clique te 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.
- •



Face / Alarm and Other Pictures
Not Configured
Video
ANPR Picture
Face / Alarm and Other Pictures

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

 \square

 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 Name Status Record Plan Operation Backup Record Plan 172.22.151.19 Online ø 10.35.92.65 Offline 10.35.92.19 Offline 🔒 Storage Config Center Server Online

Passo 3. Clique ✓ próximo ao online / offline do servidor de status. Figura 55 - Editar grupo de disco

Edit Di	sk Group							×
1.	Set Group.						1.Set Group	2.Allocate Channel
Not	Allocated				Gro	up List		
	Disk Name	Total Capacity(GB)	Used capacity (GB)			Group Name	Total Capacity(GB)	Contain
	\\.\PhysicalDrive6	150	150					
	\\.\PhysicalDrive16	500	500					
				\sum				
				$\overline{\langle}$				
							Ne	xt Cancel

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

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

Edit Disk Group		×
2. Allocate Channel.		1.Set Group 2.Allocate Channel
Not Allocated	Group List	
▼ □ III root	Disk Group 1	~
▶ □ 📩 ipc		
► 🗆 📩 ANPR		
TV WALL		
🗆 📩 pt		
nvif		
□ .m. NVR		
▶ 🔲 📩 alarm		
ARS		
D 📩 POS		
GDPR		
🗆 🏥 hik		
	Baci	Cancel

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.

•

 \square

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.

Edit Device				
Basic Info	Channel Amount: • 1	Stream	Type: Main Stream 🔻	
Video Channel	Name	Camera Type	Features	SN
Alarm Input	Channel0	Fixed Camera	Intelligent Alarm	
Alarm Output			Intelligent Alarm Fisheye	^
POS Channel			Master Slave Track	
			Electric Focus	
			IR Temperature Measure	surem
			People Counting	
			Heat Map Statistics	
			Face Detection	~
			Face Recognition	>

Figura 57 - Editar recursos (1)

2.7.1.2 Configurando Eventos

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

Add Alarm Scheme		×
1. Select Alarm Source		1. Alarm Source 2. Alarm Linkage 3. Alarm Attribute
Alarm Type 🌘		Alarm Source
Device	🔨 🗹 Disk Full	Q. Search
EVS NVR Device	Disk Error	
Video Channel	Device Offline	▼ ■ III root
Audio Detection	No Disk	Building99
Alarm Input Channel		► □
Intelligent Channel		
Thermal		
MCS Device		
Traffic Blocklist		0 🖴 111
Traffic Violation		0 📼 98
Access Control Normal		🗆 📼 acs
Access Control Abnormal		
Access Control/VDP Alarm	~	Selected(0)
The remaining 2 steps		Alarm Linkage Cancel

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.

Edit Alarm Scheme		×
2. Select Linkage		1. Alarm Source 2. Alarm Linkage 3. Alarm Attribute
Link Actions		
	There is nothing here. Try to add on	el
The remaining 1 steps		Back Alarm Attribute Cancel

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.

Edit Alarm Scheme					×
2. Select Linkage		1	. AlarmSource 2.	Alarm Linkage 3. Al	larm Attribute
Link Cameras					
Link Bind Camera Select Camera					
Link bind camera prompt	Position:	Store on Server	,	•	
All video channels bind themselves, you can configure the source binding on the	Stream Type:	Main Stream		·	
device config page.	Record Time:			\$	
	Prerecord Time:			s	
		Capture a pictur	e of camera when a	larm is triggered.	
		Open camera vi	deo on client when a	alarm is triggered.	
The remaining 1 steps			Back	Alarm Attribute	Cancel

Figura 61 - Vincular câmera

Parâmetro	Descrição
 Link Bind Camera Select Camera () 	 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.

Edit Alarm Scheme				×
2. Select Linkage			1. Alarm Source 2.	Alarm Linkage 3. Alarm Attribute
Link Cameras Link PTZ	+			
Q. Search		Channel(s)	Preset	Operate 💼
▼ □ 🗔 root	^			
	~		Total 0	record(s)
The remaining 1 steps			Back	Alarm Attribute Cancel

Figura 62 - Link PTZ

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

Edit Alarm Scheme			×
2. Select Linkage		1. Alarm Source 2.	Alarm Linkage 3. Alarm Attribute
Link Cameras Link PTZ	Alarm Output		
Q, Search	Output	Duration	Operate 💼
▼ □ 🔐 root	^		
• 🗆 🧟 🚃			
• 🗆 🧕			
• 🗆 🧕 🖬 🖬			
• • • • • • • • •	~	Total 0	record(s)
< >>			
The remaining 1 steps		Back	Alarm Attribute Cancel

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))
--------	------	------	-------	--------	-----	---

Edit Alarm Scheme		×
2. Select Linkage		1. Alarm Source 2. Alarm Linkage 3. Alarm Attribute
Link Cameras Link PTZ	Alarm Output Link Video Wall	٠
 Link Bind Camera Select Camera 	Video Wall: rf	Video Wall Alarm Window Setup
Link bind camera prompt All video channels bind themselves, you can configure the source binding on the device config page.	Ba.	
The remaining 1 steps		Back Alarm Attribute Cancel

Edit Video	Wall Alarm Window Setup		×
Video Wall:	1-4	▼ Duration: - 30	(30-3600)s
		Screen0	
			OK Cancel

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.

Edit Alarm Scheme	×
2. Select Linka	ge 1. Alarm Source 2. Alarm Linkage 3. Alarm Attribute
Link Cameras	Link PTZ Alarm Output Link Video Wall Link Email
Email Template:	Default •
Address:	•
Subject:	Event time Event type
	Send event image
	Please pay attention, there is alarm. The following is the details Time: Event time
	Location: Org name
	Event Source: Event source
The remaining 1 steps	Back Alarm Attribute Cancel

Figura 67 - Definir modelo de e-mail

Add Alarm Scheme		×
Template Name	Mail Content:	
Default	Template Name:	
12 / X	Event time Org name Event source Event type	
4 New Template	Mail Content:	
	ОК Сало	el

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

Figura 68 - Link de usuário

Edit Alarm Scheme								×
2. Select Link	age				1. AlarmSource	2. Alarm Linka	00) 3. Alarn	Attribute
Link Cameras	Link PTZ	Alarm Output	Link Video Wall	Link Email	Link User	+		
Q. Search			User			Operate	â	
🔻 🗌 🚨 Administrate	ar							
🗆 💄 system								
🗌 🔔 gs0706								
🗌 🚢 pel_yant	lei							
🔻 🗌 🚨 Operator								
0.4.885								
A. 1980 A. 198 A. 198								
🔻 🗌 🚢 test3								
. 20					Tot	al 0 record(s)	(a (a 1)	
The remaining 1 steps					Back	Alarm At	tribute	Cancel

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

Edit Alarm Scheme								×
2. Select Linkag	e				1. Alarm Source	2. Alarm Link	age 3. Ala	rm Attribute
Link Cameras L	ink PTZ.	Alarm Output	Link Video Wall	Link Email	Link User	Link Door		
Q Search			Door	F	Reaction		Operate	ō
 in root in 10.35.93.18 in mer in AE86 in 10.35.93.18 in 10.35.93.18 in 123 	8							
<	>				To	tal 0 record(s)		1/1 🕨 📄
The remaining 1 steps					Back	Alarm	Attribute	Cancel

Figura 69 - Porta de ligação

Passo 2. Clique em atributo de alarme.

2.7.2 Configurar atributo de alarme

Edit Alarm Scheme	×
3. Alarm Info	1. Alarm Source 2. Alarm Linkage 3. Alarm Attribute
Name:	• fx
Time Template:	All-Period Template
Priority:	High 👻
Remark	
The remaining 0 steps	Back OK Cancel

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 para habilitar o esquema.

Quando o ícone muda para 🔲 🔤 , significa que o esquema foi habilitado.

Operações

• Editar

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

Excluir



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.



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.

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

Tabela 3 - Requisitos de hardware

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.

Defense IA	× +			- d	n x
$\boldsymbol{\epsilon} \rightarrow \boldsymbol{c} \ \boldsymbol{\nabla}$	▲ Não seguro 10.100.14.69/admin/login_login.action		Q,	\$ 🔒 Anônim	a) :
독관		DEFENSE IA			
		Usuário normal 👻			
		Norre de Utudro Senta			

Figura 71 - Faça login no gerenciador da web

Passo 2. Clique em \blacksquare 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 **Defense** 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.

DEFENSE IA		×
	Usuário Normal	
	= 10.100.14.69 : 443	• @
	🛓 system	
	Login	

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

	1				<u></u>		3
DEFENSE IA	Página inicial			2			● ● ▲ ● ● → ● ×
۲	Visualização Extinção de vídeo ao vivo. Compativel com pré-visualização em múltiplas ja nelas, snapshot, PTZ. etc.	8	Reprodução de gravação Reprodução de gravações no Servid or ou diretamente dos dispositivos.	Å	EMapa Exibição visual da área de instalação do dispositivo, admite pré-visualizaçã o do mapa, reprodução, alarme etc.	٤	Central de eventos Listando eventos por nivel de evento, você pode processar alarmes e busc ar histórico de alarmes.
)=(Murai Decodificando vídeo ao vivo e registr o em vídeo para a parede de vídeo, s uporta tour de vídeo.	<u> </u>	Central de Download Vários métodos de faser download e exportar pravações do Servidor ou dir eto do dispositivo.				
	Gerenciamento pessoal Adicionar usuário e detalhes: admite emissão de catão, senha privada e outras autorizações.		Controle de Acesso Gerenciamento dos dispositivos de Controle de Acesos, configurações d e grupo de portas e regras.		Frequência Arranjo de turmo de pessoal, registrar as informações de frequência e pera r relatórios de frequência.	0	Video Porteiro Chamada e gerenciamento de dispo añivos VDP; admite envio de mensag ens a VTH.
20	Visitantes Apendamientoriegistro de visitantes. Gerenciamiento de permissões temp oráritas.		Controle de alarmes Armardosarmar zona, armaridesarm ar sub-sistema, monitorar status da z ona e do sub-sistema.				
	Reconhecimento facial Suporta detecção e comparação faci al em tempo real, busca de histórico de detecção e etc		Temperatura Corporal Suporta monitoramento em tempo re al de temperatura corporal, registra e reporta temperatura monitoradas.		Informações Empresariais Fornece relatórios e dados comerciai s, ajudando as empresas a tomarem decisões.	at	Anàlise de fluxo Descubra de maneira facilitada o flux o de pessoaa e a quantidade de pes soas no local.

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. Configurações do usuário: você pode definir as configurações gerais, configurações de vídeo, configurações de reprodução, 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.

Configuração local			3		×
🧔 Básico	Básico ———				
🚱 Vídeo	ldioma	Português (Brasil) 🔹 🔻	(Reinicialização necessária)		
🕑 Reprodução	Tema	Escuro 👻	(Reinicialização necessária)		
Snapshot	Resolução	1440*900 🗸			
Gravação		Sincronizar horário			
		Login automático			
🐥 Alarme		Iniciar com Windows			
🖽 Mural de vídeo		Manter mosaíco de câmeras ao	inicializar		
🚽 Atalhos		🖌 Áudio auto-adaptável			
		Exibir dispositivos			
	Video				
	Divisão padrão				
				Padrão Salvar	Cancelar

Clique Sono canto superior direito da página inicial. Passo 1. Figura 78 - Configurações locais

Passo 2. Clique em Básico para definir os parâmetros.

Tabela 5 - Parametros de video				
Parâmetros Descrição				
Idioma	Modifique o idioma exibido no cliente; reinicie o cliente para torná-lo válido após a configuração.			

~ 1. 71

intelbras.com.br

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 S no canto superior direito da página inicial.

Passo 2. Clique em Video para definir os parâmetros.



Configuração local	Ū.		X
🛱 Básico	Vídeo		
😵 Vídeo	Divisão padrão	=	
Reprodução	Selecionar Stream	9 -	Após este limite, todos canais em stream extra
~ occursts	Fluência do vídeo	Prioridade de equilíbrio	
O Snapsnot	Tempo de buffer		0-1500 ms
Gravação	Tempo da gravação	30s •	
🜲 Alarme			Segundo V 10s-24h
🖽 Mural de vídeo		Ativar aceleração de hardware	(efetivo após reabrir vídeo)
🝯 Atalhos		Clicar duas vezes em vídeo pa	ra maximizar a janela e trocar para a fluxo pri
		Fechar vídeo em silêncio	
	Horário de silêncio		(1 a 30 min)
	Reprodução		
	Divisão padrão	=	
	Eluvo	Tranemieeão Comolata	
			Padrão <mark>Salvar</mark> Cancelar

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.

	i iguia ou	Domini do coningulações de repredação
Configuração local		×
😫 Básico	Reprodução	
🔂 Vídeo	Divisão padrão	
 Reprodução 	Fluxo Tra	nsmissão Completa 🔹
🖸 Snapshot		Ativar ajuste de alta definição
🖼 Gravação		

Figura 80 - Definir as configurações de reprodução

Parâmetros		Descrição		
	Divisão Padrão	Definir divisão padrão da janela de reprodução		

Parâmetros	Descrição				
	Selecione um tipo de stream padrão para reprodução de				
Fluxo	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.				
	Se habilitado, quando o fluxo de reprodução é grande				
Ativar ajuste de alta	devido à alta definição, o sistema reserva quadros I para				
definição	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 S no canto superior direito da página inicial.

Passo 2. Clique em Snapshot para definir os parâmetros.

Configuração local			Ū			×
🖨 Básico	Snapshot					
🤁 Vídeo	Formato	JPEG	•			
Reprodução	Caminho da imagem	C:\Defense IA\Client\Picture\			Pesquisar	
Snapshot	Nome da imagem	CanalNome_Hora	•			
Gravação	Intervalo entre fotos		\$ (Não menos do que 1 s)		
🐥 Alarme	Quantidade contínua		(2-10)		

Figura 81 - Definir configurações de snapshot

Parâmetro	Descrição		
Formato	Escolhe o formato de imagem instantânea. Suporta		
	BMP e JPEG.		
Caminho	Configura o caminho de armazenamento de		
da imagem	snapshot.	Snapshot	
Nome da	da a r		ere
imagem	Configura a regra de nomenciatura das imagens	à função	de
Intervalo	Configura o intervalo e número de snapshots. Por	Snapshot	
entre fotos	exemplo, se o intervalo de snapshot for 10 e a	durante	а
	Quantidade contínua for 4, quando você clicar com	exibição	ao
Quantidad	o botão direito na Vídeo ao vivo ou na Reprodução	vivo	ou
	e seleciona Snapshot no menu, 4 fotos serão	reprodução	0.
e Continua	capturadas de uma vez e o intervalo de tempo entre		
	elas é de 10 segundos.		

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 S no canto superior direito da página inicial.

Passo 2. Clique em Gravação para definir os parâmetros.

	0	0,	0 3		
Configuração local					×
Básico	Gravação ———				
🔂 Vídeo	Diretório	C:\Defense IA\Client\Record\		Pesquisar	
🕑 Reprodução	Nome da gravação	CanalNome_Hora 🗸			
O Snapshot	Tamanho máximo	1024	(10-1500M)		
Gravação	Alarme				

Figura 82 - Definir as configurações de gravação

Parâmetros	Descrição				
Configura o caminho do armazenamento dos a					
Diretório	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.				

Tabela 9 - Parâmetros

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.

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

	Figura		niiguraço	es de alarme	5
Configuração local					×
O Básico	Alarme				
🛛 Vídeo	•	2 Tocar som de Alarme	Loop		
🕑 Reprodução	Tipo de Alarme Diretório som	Perda de Video	et way	ana Reporter	
O Snapshot					
🗃 Gravação	Tipo do Alarme	Piscar mapa ao ocorrer ala Perda de Vídeo	rme. -		
🔺 Alarme					
🖽 Mural de vídeo	Abertura como:	Pop Up Em prévia			
着 Atalhos					

Figura 83 - Dofinir configuraçãos do alarmo

Tabela 10 - Parâmetros

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

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.

Clique em Salvar. Passo 3.

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.

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

Passo 2.

Figura 84 - Definir configurações de vídeo wall

Configuração local				×
🖨 Básico	Mural de vídeo			
🔂 Video	Tipo de fluxo Padrão	Fluxo Primário 🗸		
Reprodução	Tempo de permanência (s)	15	(15 - 65535 s)	
Snapshot	Selecionar Stream	9 -	Após este limite, todos canais em stream extra	
Gravação	Modo vinculativo	💿 Ronda 🛛 🔿 Lado a lado	Investigação	
🌲 Alarme		Clicar duas vezes em video par	a maximizar a janela e trocar para a fluxo primário	
🖽 Mural de vídeo	Atalhos			

Tabela 11 - Parâmetros	
	-

Parâmetro	Descrição			
	Selecione Fluxo primário, Fluxo secundário ou Local			
Tipo de fluxo padrão	Sinal como o tipo de transmissão padrão para exibição			
	de vídeo wall.			
	Defina o intervalo de tempo padrão entre os canais para			
	o tour exibição. Por exemplo, se o tempo de			
Tempo (s) de estadia	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			
	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			
lipo de fluxo	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	Duplo clique em o vídeo para maximizar a janela, e			
janela e trocar para a	entretanto, o tipo de stream mudará para stream			
transmissão principal	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 S 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.

Configuração local	i igure			×
🖨 Básico	- Atalhos			
🚱 Vídeo	Tipo de teclado 🔷 Joy	stick USB	Teclado PC	
Reprodução	Função	Tecla de atalho	Função	Tecla de atalho
C	Mover a janela para cima			Ctrl+L
Snapshot	Mover a janela para baixo		Ajustar janela única	Р
Compaña	Mover a janela para a esquerda	Left	Atalho de Snapshot	Ctrl+P
Gravação	Mover a janela para a direita	Right	Gravação local	Ctrl+R
🜲 Alarme	Abertura-	Insert	Predefinição 1	1
_	Abertura+	Delete	Predefinição 2	2
🜐 Mural de vídeo		Home	Predefinição 3	3
🧧 Atalhos			Predefinição 4	4
		PgUp	Predefinição 5	
		PgDn	Predefinição 6	
	Abrir janela única	Enter	Predefinição 7	
	Fechar a janela única	Enter	Predefinição 8	
	Abrir tela cheia	Ctrl+F	Predefinição 9	
	Sair da tela cheia		Predefinição 10	
				Padrão Salvar Cancelar

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
0	Gravação	Abre / fecha a reprodução instantânea. Vá para Configuração local> Geral para definir o tempo de reprodução instantânea. Certifique-se
	instantanea	de que haja um registro na plataforma ou no dispositivo.
¥	Áudio	Habilita/Desabilita o áudio
ᢀ	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.
0	Snapshot	Clique para tirar um print da tela
L¥.	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.

×	Fechar	
	Fechar todos	
∢ ×	Ativar áudio	
٠	Ativar conversas	
-	Iniciar gravação local	
	Iniciar gravação remota	
ø	Snapshot	
ø	Snapshots contínuas	
۰	Definir janela de alarme	
	Selecionar Stream	٠
	Fluência do vídeo	۲
•	Ajuste de vídeo	٠
	Sobreposição de IVS	٠
	Sobreposição de SMD	۲
	Modo de janela	٠
	Controle de saída alarme	
*	Adicionar a favorito	
	Tela cheia	
۲	Troca para reprodução	
,91	Localização no mana	

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.



N⁰.	Nome	Função
1	Recursos	 Você pode pesquisar um dispositivo ou canal por nome em search. Q. 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	Мара	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 exibila 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 Dara 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	
DEFENSE IA	Visualização 1 🕂	
Recursos 🔹		
★ Pesquisar Q		
▼ 🖬 Vídeo (6/6)		
▶ <u></u> 10.100 19 14		
▶ 📼 10. Conf.dian	10s	
▶ 10.100.19.22	sus 1min	
▶ 📼 10.100.19.63	2min	
▶ 🖴 10.100.19.54	5min	
▶ 🛤 10.100.19.28	iumin	
Mapa		

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 📩



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



- 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.

 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 Recursos

Resquisar.
Q

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









Parâmetros	Descrição
2	 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.
0	O tempo padrao para desbloquear PTZ automaticamente e 30 segundos.
U	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.
LŔ	Esta função só pode ser controlada com o mouse.
4	Ajuste a velocidade de rotação do PTZ de cima para baixo. Defina o tamanho do passo de 1 a 8.
Θ	Zoom + e Zoom -
\odot \odot	Ajuste de foco
0 0	Ajuste de Íris
►, ⊵, ⊡, …	Definir preset, Tour, padrão, scan, rotação, limpador, luz, e iluminação de IR.

Tabela 12 - Parâmetros foco eletrônico

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 **Z**.
- Passo 4. Insira o número do Preset e clique em M.

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 .

Definir tour	×
No: 1	Nome: Preset 1
Ponto de Preset	Operação
	+ ×
	+×
	+ ×
	+ ×
	+ ×
	+ ×
	+ ×
	+ ×
	+ ×
	+ ×
	+ ×
	and the second s
	OK Cancelar

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 D, 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 5

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 ke 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 死 para ativar o limpador. Clique em 쭏 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



Tabela 13 - Parâmetros botões

Parâmetros	Descrição
\sim	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 e para fechar a função do menu PTZ.
ОК	 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



- 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 Ma 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



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.

 \square

• 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 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 de 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.
- 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 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
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.	área de detecção deve ser o mais simples possível.

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	Empreendimento zonas, salões e muito mais.
	alarme.	

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. Considerational 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

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

I. Clique em Configuração e defina os parâmetros.

Figura 105 - Definir parâmetros

Configure			
Parameters	Arming schedule	Alarm	
Object Type:			
🔽 Human 🛛	Vehicle		
Direction:	A<>B		

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 Configure Parameters Arming schedule Alarm 📕 Alarm Output Alarm Latch Seconds (10-300) Set \sim 10 🔳 Record Set \sim Record Delay 10 Seconds (10-300) 🛃 Snapshot Set \sim 📕 Send Email Cancel Save

Table 1-1 Parâmetros

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

Parâmetro	Descrição		
	Quando um alarme acontece, ele aciona a gravação de vídeo imediatamente.		
Registro	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.	Clique em Definir próximo a Snapshot para	
	Requer que o dispositivo já tenha programações de instantâneos. Consulte o manual do dispositivo para obter instruções detalhadas.	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.
- Clique em Adicionar regra. Passo 2.
- Passo 3. Habilite a regra e modifique o nome e o tipo.
- Ativar regra. **Constituta de la regra está habilitada**. Ι.
- П. 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.



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. "



Configure			
Parameters	Arming schedule	Alarm	
Object Type:			
🔲 Human 🕅	Vehicle		
Action List:			
Appears	7 Cross		
Direction:	Bidirection		

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. III 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

Configure			×
Parameters Armin	g schedule	Alarm	
Min Duration:	10	Second (s) (6-3600)	

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.

 \square

- 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

Configure			
Parameters Arming	gschedule Als	12°M	
Object Type: Human 🔲 Vehio	cle		
Min Duration:	1	Second (s) (1-60)	
Sensitivity:	Low 🔴	Hi gh	

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. I 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

Configure			
Parameters Arming	schedule Ala	rm	
Min Duration:	6	Second (s) (6-300)	

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.



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

Configure			
Parameters Armin	ng schedule	Alarm	
Min Duration:	10	Second (s) (10-300)	
Report Interval:	10	Second(s)(10-300)	
Sensitivity:	Low	Hi gh	

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. Considerational 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

Configure			
Parameters	Arming schedule	Alarm	
Min Durstion:	10	Second (s) (6-3600)	

Tabela 21 - Parâmetros

	Parâmetro	Descrição
	Duração mínima	O tempo mínimo de duração desde o desaparecimento do objeto até o disparo do alarme.
P	asso 6. Clique e	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. Constitutada 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.

	F	igura 121 - Dete	ecção de vadia	agem	
IVS Setting					×
	1	Smart Flan	2	IVS	
Detect Region	Rule config	Parameters			
		e Prave Complete di	201.9-07-17 08-50.25	Rule Details Add rule Enable Rule name Delete Rule1 × Re-draw Clear Rule name: Rule1 Rule type: Loitering Detect + Config Target Filter	
Back	Apply	Save Cancel			

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

Configure			
Parameters Arming	schedule	Alarm	
Min Duration:	5	Second (s) (1-600)	
Report Interval:	1	Second (s) (1-600)	

Tabela 22 - Parâmetros

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

IVS Setting						×
		Smart Plan		(2)	IVS	
Detect Region	Rule config P	arameters				•
- n ² · · · 1	 .					•
💟 Disturban	ice filter					
Sensitivity:	Low	Hi gh				
Back	Apply	Save	Cancel			

Figura	123 -	Parâmetros
--------	-------	------------

Parâmetro	Descrição
	Filtre alvos falsos, incluindo plantas ondulantes e ondas de água.
Filtro de Perturbação	Esta função pode causar omissões de alvo, pois algumas partes
T Churbação	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



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

No adicionar uma camera ou NVR na interface de Dispositivos na interface Web do Servidor, selecione Encoder para a categoria de dispositivo.



1. Login Information.	1.Login Information 2.Device Information
Protocol:	V
Manufacturer:	•
Add Type:	IP Address •
Device Category:	Encoder
IP Address:	* 10 ** 01 000
Device Port:	• 37777
User:	• admin
Password:	•••••
Org:	root •
Home Server:	Center Server •

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 d	lo canal	de	vídeo
iguiu		Lana	10001000 0		ac	VIGCO

Edit Device					×
Basic Info	Channel Amount: 1	Stream	Type: Sub Strea 🔻		
Video Channel	Name	Camera Type	Features	SN	KeyBoard Code
Alarm Input	 IP PTZ Camera 	Dome Camera	People Counting		
			Intelligent Alarm	~	
Alarm Output			Fisheye		
			Master Slave Track	c .	
			Electric Focus		
			IR Temperature Me	easurem	
			People Counting		
			Heat Map Statistics	;	
			Face Detection	<u> </u>	
			Face Recognition	>	
				Total 1 record(s)	
Get Info					OK Cancel



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.

Configure Arming schedule Alarm 🔘 Sunday 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 🔘 Monday 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 🔘 Tuesday 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 🔘 Wednesday 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 🔘 Thursday 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 🔘 Friday 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 🔘 Saturday 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 End 23:59:59 Begin 0:00:00 Begin 0:00:00 23:59:59 🗍 End \checkmark End 23:59:59 🗍 Begin 0:00:00 Begin 0:00:00 End 23:59:59 [Begin 0:00:00 End 23:59:59 🗍 Begin 0:00:00 End 23:59:59 Save Cancel

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.

Conf	igure					
Armi	ng schedule	Alarm				
•	Alarm Output					
	Alarm Latch	10	Seconds	(10-300)		Set \sim
	Record					
	Record Delay	10	Seconds	(10-300)		Set \sim
	Snapshot					Set \sim
	PTZ Activation					Set \sim
	Send Email					
					Save	Cancel

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
Trava de alarme	A ação de saída de alarme atrasará a parada após o término do evento de alarme.	canal de saída de alarme.

Parâmetro	Descrição	
Gravação	Quando um alarme acontece, ele aciona a gravação automática de vídeo imediatamente.	Clique em Definir (Set)
	programações de gravação. Consulte o manual do dispositivo para obter instruções detalhadas.	proximo 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.	Clique em Definir (Set) próximo a Snapshot para selecionar o canal de instantâneo.
Enviar email	instruções detalhadas. O sistema enviará um e-mail para o endereço de e-mail relacionado quando ocorrer um alarme.	Nenhum
	Requer que o dispositivo já tenha o e-mail configurado. Consulte o manual do dispositivo para obter instruções detalhadas.	

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.

	rigara ree	I lane meeng	onto	
IVS Setting				×
	Smart Plan	(2)	IVS	
<u>^</u>				
Neut				
Lancel				

Figura 133 - Plano inteligente

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

IVS Setting (1)Smart Plan (2) Rule Details Add rule Enable Rule name Delete StereoNumb 🛛 🗙 Re-draw Clear Rule name: StereoNumberStat Rule type: People Counting R Config Back Apply Save Cancel

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. **L** 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.

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

Figura	135 - Definir pa	arâmetros (contagei	m de pessoas) ×
contiguie				
Parameters Arm	ning schedule	Alarm		
Min Height:	50	cm (0-200)		
Max Height:	220	cm (0-300)		
Enter No.:	0			
Exit No. :	0			
Remaining No.:	0			
Sensitivity:	Low	Hi gh		
			Some	Concel
			Dave	Califer

ofinir parâmotros (oc 201



Configure				×						
Parameters Arming	schedule Alar	'n								
Min Height:	50	cm (0-200)								
Max Height:	220	cm (0-300)								
Sensitivity:	Low Contraction	Hi gh								
🗾 Man Num Alarm Ens	able									
Man Num Threshold:	30									
Detect Mode:	Alarm when greate									
Stay Detect Enabl	le									
Stay Min Duration:	30	Second(s)(1-1800)								
			Sava	Cancel						
			Dave	Calicer						

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

Co	nfi	jure					Ū					U															×
	Par	ameters	Ą	t rmi	ng	sch	edul	le		LA	arı	n															
	0	Sunday	(D 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	۲	Monday	() 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	۲	Tuesday	(J 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	۲	Wednesda	y (J 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	•	Thursday	(D 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
		Friday	(J 1	2	3	4	5	6	7	8	9	10	11	12	13	14 1	15	16	17	18	19	20	21	22	23	24
		Saturday	(J 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
		Begin (00:00	:00]	End	23	8:59	9:59			•	Ве	≥gin	. 0	: 00	:00	-		End	1	23:5	59:5	59	▲ ▼	
	•	Begin ():00	:00]	End	23	8:59	9:59			•	Be	≥gin	0	: 00	:00	-		End	L :	23:5	59:5	59	▲ ▼	
	•	Begin (00:00	:00]	End	23	8:59	9:59			•	Be	≥gin	. 0	: 00	:00	•		End	. :	23:5	59:5	59	÷	
																				2011	•			с	a	۵٦_	
																				Jav	-			- U	anc	eT.	

Figura 137 - Agenda de Funcionamento

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

Figura 138 - Alarme

Configure					
Parameters Arming schedule Alarm					
Alarm Output					
Alarm Latch 10 Seconds (10-300)	Set \sim				
Record					
Record Delay 10 Seconds (10-300)	Set \sim				
🗾 Snapshot	Set \sim				
Send Email					
Save	Cancel				

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
Trava de alarme	A ação de saída de alarme atrasará a parada após o término do evento de alarme.	canal de saída de alarme.

Parâmetro	Descrição				
Gravação	Quando um alarme acontece, ele aciona a gravação automática de vídeo imediatamente.	Clique em Definir (Set) próximo a Gravar (Record) para selecionar o canal de gravação.			
	programações de gravação. Consulte o manual do dispositivo para obter instruções detalhadas.				
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			



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 <u>Ina p</u>ágina 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.





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 🚵

D	EFENSE	a) _	ladar Smart Track	Flow Analysis	0		·		() [0] 3	: • <u>•</u> - # ×
۵		14	Daily Report							👌 Epot
*	Inarih	۹								
P ₂	+ Addise		Exit/Entry People					Entry 0 Person	s(a) 🚃 Exit O Person(a)	
		1.0								
					and a star was					
			Slay People							Stay People
	Ow.									
	2012-12-02									
			1 3 3 00		a Section and a	10 11 11	CARLER B	an annaithe	# 3.80 B	e enven

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

ad 🖌 🖃

\square

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


D	EFENSE IA 🔹	dar Smart Track Flow Analysis	0	00 ± 0 A - 8×
۵	Resources Rule	Daily Report 2019-12-02		👌 Export
* 5	Search	Exit/Entry People		💴 Entry 8068 Person(s) 📟 Exit 7562 Person(s)
	• • • • • • • • • • • • • • • • • • •			
	Constanting			
	· · ····			
		Stay People		
				Stay People
			5 • Stay People : 0	
	Day •			
	Search			15 16 17 18 19 20 21 22 23 0

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 🗟

D	efense IA	Análise de fluxo	Visualização 1	÷			••••) – – – ×
٨								
Å		Q						
E ₂	☐ 🖬 Vídeo							
					Sem Resulta Favor selecionar as informações r	ados nos filtros ao Iado.		
	Dia							
	2020-12-10							
	Tempo de espera 5s							

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



- 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





- 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.





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.



rigura	
1. Login Information.	1.Login Information 2.Device Information
Protocol:	
Manufacturer:	P
Add Type:	IP Address
Device Category:	Encoder
IP Address:	• 10 per our and
Device Port:	• 37777
User:	• admin
Password:	••••
Org:	root •
Home Server:	Center Server 🔹

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.

Edit Disp.				×
Informações	Quantidade de ca.	* 5	Tipo transm: Str	ream Ext 🔻 🇹 Código de canal zero
Canal de vídeo	Canal SN	Nome	Tipo de Camera	Características SN Cód. do teclado
Entrada de	* 0	* VIP 5550 Z IA	Câmera fixa 🔻	Foco elétrico
Saída alarme	* 1	* VIP Intelbras	Câmera fixa 🔻	Foco elétrico
Canal EdV	* 2	* IPC	Câmera fixa 🔻	Reconheciment
Canarray	* 3	* CAM 1	Câmera fixa 🔻	Estatística de mapa termico Estatística de linhas cruzada:
Canal de alarme	* 4	* IPC	Câmera fixa 🔻	Contagem de pessoas em m
				Estatísticas de área
				Detecção facial
				Reconhecimento facial
				Detecção de alvos
				Foto de acesso
Obter informações			9	Smart Track (Radar + PTZ)

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.

	1 '9			.00 (_)	
Basic Info	Channel Amount: • 1	Stream	Type: Sub Strea •		
Video Channel	Name	Camera Type	Features	SN	KeyBoard Code
Alarm Input	• IDD12588874873775	Fixed Camera •	Face Recognition		
Alarm Output			IR Temperature Me	easurem	
			People Counting		
POS Channel			Heat Map Statistics	3	
			Face Detection		
			Face Recognition		
			Target Detection		
			Smart Track (Rada	r + PTZ)	
			Privacy Mask	~	
			<	>	

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	e rosto
---	---------

24	Plano de gravação			Disc	co de Rec <mark>e</mark> Disco Local			
	Plano de gravação backup	🖋 F	ormatar				Todos	
4	Quota de grupos		Nome do Servidor Nome do dis	co Capacidade (GB) Capacidade tot	Tipo de disco Status de integri	Status do disco	Qtde vagas	Operaçã
	Configuração de Disco		Alocação tipo			×	-1	φ
						ormal	-1	φ
					_	ormal	0	¢
			Tipo de disco:	Imagem geral	_	ormal	0	¢
			Capacidade (GB):	Vídeo		ormal	1	
				Imagem de LPR Imagem geral	1			
					OK	elar		

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 t na Interface Web do Defense IA e, em seguida, selecione Banco de Faces.

Passo 2. Clique em Adicionar.

Figura 150 - Adicionar um banco de dados de rosto	
Adicionar banco de dados de faces	×
Nome do Banco de Dados : *	
Banco de dados de cores : Cinza 🔹	
Comentários :	
ок	ancelar

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 ^{IIII} para adicionar informações de identificação Facial.

- 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

Configu	urar tipo de pessoa	×
🕇 Adi	icionar 🗰 Excluir	
	Tipo de pessoa	Operação
	* Funcionario	ж
Total 1 gr	ravação(ões).	
		Fecha

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 X 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

Face Library Manage	Face Library > 11test	🏘 Person Type Config 📑 🗄
Sec Device Config	💠 Add 🗰 Delete 🛃 DownLoad Template 🛃 Import	Q, Search

• Clique 🌡 no cartão pessoal.

Figura 153 - Defina os detalhes da pessoa

Sace Library Manage	Face Library	
B Face Device Config	+ Add	Q. Search
Pace Device Coming	Total 1000 Person	
	Total 5 record(s).	() Go to page 1 Go

- 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

B .	1				
🖺 Face.jpg	195,094	194,877	JPEG	2018/7/16 10	5C085341
國 face-EN.xls	154,112	10,904	Microsoft Excel	2018/8/23 15	ABEE3C

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)						
Importar pessoa			×			
Importação da pe		lm. arq.				
	 Faça upload de arquivo .zip, .rar ou .7z. 					
	 Não altere o sufixo de arquivos de fotos locais. 					
			Cancelar			

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 ^Q.
- 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 ⁴ para começar a configuração de envio das faces.

Configurar disp. de rostos	100 0010		anai	×
Biblioteca de Rostos: Intelbras				
Q Pesquisar	Selecionado(1)			
▼ ■ III root	Nome canal	Similaridade	Operação	曲
10.100.19.22	IPC	∗ 70 ▲	×	
	Total 1 gravação(ões).	He de	1/1	м
			OK Ca	ncelar

Figura 156 - Selecione um canal

Passo 4. Selecione os canais de destino e defina o nível de similaridade desejado.

Passo 5. Clique em OK.

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 ¹ 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.

- Clique em 🖿 no Cliente de Controle e selecione Reconhecimento Passo 1. Facial.
- Clique em 睯 Passo 2.



N٥	Nome	Descrição						
		Exibe os dispositivos que possuem as						
1	Árvore de Dispositivos	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. 						
2		Ouando este ícone está na interface, o nainel de						

de rosto humano.

Figura 157 - Vídeo ao vivo

exibição de instantâneo atualiza a imagem com snapshots de rostos humanos. Clique no ícone, e o sistema pausará o exibir as imagens/snapshots

N°	Nome		Descrição
3	Registros reconhecim	de ento facial	Exibe os reconhecimentos faciais obtidos nos canais de vídeo abertos.
4	Janela de M	lonitoramento	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.
	Full Screen 🔻	Proporção de visualização	Existem dois modos: tela inteira, e escala original. A tela inteira refere-se a uma janela em tela inteira.
5	:: ::: : : [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.

 \square

- A pesquisa por imagem está disponível apenas com IVSS e alguns NVR's.
- Passo 1. Clique em to 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.

D		onhecimento facial 🕒			·	4)	9 2	• 🗛 –	- 🗆 ×
80) 270	Pesquisar em Biblioteca Gravação	Lista				llimitado		llimitado	-
98	Intelbras -	Selec tudo							
	Para Imagem Caracteristicas Tipo de pessoa Todos Nome da Pessoa Insira o nome	Nome: MARCIO AL Nº do certifica:d2390 Tipo de pesso #uncionario Género: Masculino Aniversàrio: Região: Brazil Comentários:	DOR	Nome: DAVID BRES D 4º do certifica (32930 Tipo de pesso Funcionario Gênero: Masculino Aniversário: Região: Brazil Comentários:	00	Nome: FERNANDO PE Nº do certificard22900 Tipo de pesso-Funcionario Género: Masculino Aniversário: Região: Brazil Comentários:	D		
	Nº do certificado		:đ		ରେ 🗆		īđ		
	Idade Todos • Gênero Todos • Pesquisar	Nome: Nº do certifica Tipo de pesso Genero: Masculino Aniversáno: Região: Brazil Comentários;		Nome: MARI LUCE Co 4º do certificat 02820 Tipo de pesso :Funcionario Gênero: Feminino Aniversário: Região: Brazil Comentários:	DE	Nome: I ^a do certificad Tipo de pessot Gênero: Feminino Aniversário: Região: Brazil Comentários:			
			2đ		5đ 🗆		īđ		
		Nome: No		Nome: ISABELA FERM ^{‡7} do certifica:(32430 Tipo de pesso: Funcionario Gênero: Ferninino Aniversário: Reglão: Brazil Comentários:	NA	Nome: Nº do certifici Tipo de pess Gênero : Masculino Aniversário : Região : Brazil Comentários ;			
			[ď		Ia 🗆		īđ		

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.

 \square

- 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 Gravações	de	Clique para salvar o arquivo rar no caminho especificado. O arquiv .rar contém as imagens /snapshots de rosto humano e imagens d contexto.				
Registro reprodução	de	Clique 🔄 para reproduzir a gravação de vídeo de 15 segundos antes e depois do instantâneo.				
Adicionar pessoa		 Adicione a pessoa do snapshot ao banco de dados. Clique . Clique . Defina as informações da pessoa e clique em OK. 				
Pesquisa Gravações	de	 Você pode fazer upload de uma imagem de rosto para pesquisar nas gravações. 1. Clique a, 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

D	efense Ia	Recon	ihecimento fac	ial 🛨								🐠 🧕 🔺 🗘	<u> </u>	⊐ ×
8 2	Canal IPC		Lista 🔄								Similaridade 🖷			96%
23	Data 12/08 00:00-12/08 23:59		Selec tudo											
Ē	Tipo de pessoa Todos		LEANDRO E 53163	EUSTA Fun	53163	DRO EUSTA	Fun	LEANDRO 53163	DEUSTA I	Fun				
	Nome da Pessoa Insira o nome Nº do certificado Insira o n.º do certificado		Ø.	96%	×		97%							
	Idade	_ 1	IPC	2020-12-08 18:45:27	IPC	2020-12-0	08 18:42:12	IPC	2020-12-08 18	:02:00				
	Todos			@ .t.			@ .*.		ര					
	Todos Pesquisar													
		10	0 🔻 Por Página											

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



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.

Figura 164 - Descrição de funções

3.5.4.4 Relatórios Faciais

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

Passo 1. Clique To Cliente do Defense IA e selecione Reconhecimento Facial.

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.

Passo 2. Na interface de Reconhecimento Facial, clique em



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.



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.

Ш

 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.

1. Login Information.	1.Login Information 2.Devi	ce Inform
Protocol:	•	
Manufacturer:	-	
Add Type:	IP Address •	
Device Category:	Encoder	
IP Address:	* gran an ann	
Device Port:	* 37777	
User:	* admin	
Password:	•••••	
Org:	root •	
Home Server:	Center Server	

Figura 169 - Adicionar Dispositivo

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

Edit Disp.		×
Informações	Quantidade de ca * 8	Tipo transm: Stream Ext 🔻 🗹 Código de canal zero
Canal de vídeo	Canal SN Nome	e Tipo de Camera Características SN Cód. do teclado
Entrada de	* 0 * CAM	1 Câmera fixa 🔻 Detecção de alvos
Saída alarme	* 1 * CAM	2 Câmera fixa Estatística de mapa térmico
	* 2 * CAM	3 Câmera fixa 🔻 🗌 Estatística de linhas cruzada:
Canal PdV	* 3 * CAM	4 Câmera fixa 🔻
Canal de alarme	★ 4 ★ CAM	5 Câmera fixa Deteccão facial
	* 5 * CAM	6 Câmera fixa 🔻 🗌 Reconhecimento facial
	* 6 * CAM	7 Câmera fixa 🔻
		Smart Track (Radar + PTZ)
		Total 8 Gravação(ões)
Obter informações		OK Cancelar

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 a Iniciar atua	atualização / alização	 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 monitoram	de iento	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	Full Screen 🔹	Proporção de exibição da imagem Número de janelas	Existem dois modos: tela inteira, e escala original. A tela inteira refere-se a uma janela em tela inteira. 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 ^{III} e salve os arquivos .rar no caminho especificado.
 - Clique en 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

D	SFENGE IA	The put Detraction	•					0	1 • • - 0 ×
٠	-								
6	Channel PC-PC-Artic SEE SELEV. Trans Extension Extension Film Film Paint Namber Net Control on any other multiple for Weathington Add	 Sector Sector					Allocate 2019 20, 57		
	weischeisege Al Al Al Al Mete Celor Al Cean N	• • • •		C M Marine o Carlo a Marine C A A A		e Ref Manda a da far far far Ref & A & A		C Managa ang ang ang ang ang ang ang ang an	
		11 × 100			1				

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 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

 Visualizar X 🗆 Disp. Rem 	×												Configurações
> Dispositivos	Dispositiv	ros	Atualiza	ar câmera									
Parâmetros Encoder	End. IP			10.100.1	4.70		Buscar					Não Inicializad	Inicializar
				Monitor	Status	End. IP		Porta	Nome	Protocolo	Tipo	MAC	Serial
Nome do canal													
Status dos canais													
	Buscar	Adici	onar A	d.Manual	Modificar	IP						Fitros Nenhur	

II. Configure todas as informações da câmera:

Ad.Manual		×
Canal	2 .	
Protocolo	Intelbras-1	•
End. IP	10.100.14.70	
Porta de Serviço	37777	(1~85535)
Usuário	admin	
Senha		
Número do Canal	1	Conectar
Canal remoto	1	Ajustar
Buffer	Default	·
		Salvar Cancelar

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.

	Channel	Edit	Delete	Status	IP Address	Port	Device Na	Remote C	Manufactu	CAM Nam	WEB	Туре	Serial No.
	1	ø	Ť.	•	10.100.17.80	37777	83XH	1	Intelbr	CAM 1	e	VIP-5	83XH
	2	ø	Ē		10.100.14.70	37777			Intelbr	PeD F	e		5L087
Ара	gar	Importar	Exp	portar	Atualizar	Jsuário/Senha	Padrão	Mudança aut	omática de c	ompressão de	vídeo		

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

Edit Disp.				×
Informaçõ e s	Inserir informa	ıções		
Canal de vídeo	Protocolo:	Intelbras-1 *	Fabricante:	Intelbras v
Entrada de	Endereço IP:	• 10.100.21.139	Usuário:	• admin
Saída alarme	Porta:	• 12234	Senha:	
Canal Pd∨	Servidor:	Servidor Central 🔻	Organização:	root •
Canal de alarme	Informações s	obre o dispositivo		
	Nome do	• iNVD9032 FT IA	SN:	3NFI6101401LK
	Dispositivo: Tipo:	NVR *	Modelo:	iNVD 9032 PE FTU
Obter informações				OK Cancelar

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

informações	Quantic	sade de ci	ай <u>–</u> 1	2	Tipo transm:	Stream Ext	• 🗹 Có	digo de canal ze	ro
Canal de vídeo	Can	el SN		Nome	Tipo de Camera	Caracteri	stoas	SN	Cód. do teclado
Entrada de	•	1	• 0	Juia mdulo Bl	Câmera fixa	Alarme int	eligen samento de e	scravo/mx	
Saída alarme	•	2		CAMIS	Câmera fixa	Foco	elétrico		
Canal PdV						Medig Estati	ão de temper stica de mapi	a térmico	
Canal de alarme						Estati	stica de linha	s cruzada:	
						Conta	igem de pess sticas de árei	oasemm	
						Deteo	ção facial		
						Recor	nhecimento fa	icial	
						Tot	al 2 Gravaçã	io(ões) [4	41/100

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"

۲				
Dispositivo	Usuário	0	Eventos	Armazenamento
Gerenciamento de dispositivos conectados à plataforma. Permite adicionar, editar e excluir dispositivos.	Gerenciamento de us funções. Permite o ge e permissões dos usu	suários e C srenciamento d Jários. s a	Gerenciamento de avisos/alarmes le eventos dos dispositivos ou do istema. Permite vincular ações los receber eventos.	Gerenciamento do armazename de gravações. Defina planos de gravações e quota de discos.
Dispositivo	Usuário		Eventos	Armazenamento
Configurações Empresariais		9 ⁶ 9		
Dispositivo	Usuário	Organização	Eventos	Armazenamento
Mural de vídeo	Mapas	Banco de Faces	Cadastro de veículos	Velocidade Média

II. Clique em Adicionar para incluir uma loja

Q Pesquisar	+ Adici	ionar 🛱 Excluir 🎌 Mover para	Q, Pesquisar	
▼ iiii root		Nome da loja	Limite de número de pessoas	Operação
		Agencia	12	/ x =

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:

Adicione armaz			×
Inf básica	1F 🔶		
Iome compra: 1	💠 Mova disp. 🕂 Adicionar zona	Q Dispositivo/Áre	
 Análise de fluxo]		
Configuração de tempo livre:			
• 00:00:00			
imite de número de pessoas:	_		
Valor de aviso:			
Organização:			
Disp.	3		
Q. Pesquisar			
▼ 📅 root		viar mapa 2	
▶ (Q) iNVD9032 FT IA			
O 10.100.17.80			
O iMHDX Face			

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

Dispositivo	Usuário
conectados à plataforma. Permite adicionar, editar e excluir dispositivos.	funções. Permite o gerenciamento e permissões dos usuários.
Dispositivo	


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

Conectar 🕻 Atualizar	🕐 Inicializar dispositivo 🖉	Alterar IP	🗭 S	egmento da rede Minin
] Status de inicialização#	Endereço IP\$	Modelo#	Porta	Endereço MAC
] Inicializado	10.100.17.115	IPC-EBW81242	37777	a0:bd:1d:54:d2:66
dicionar lote				×
Organizaçã	o: root	•		
Servido	Servidor Central	•		
Usuári	o: • admin			
Senh	B: •••••			

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

Todos	Encoder P	ainel de Alarme								
	ID do dispos	IP/Domínio +	Servidor +	Nome do +	Tipa +	Modelo +	Organização	Status +	Offline	Operação
	1000022	10.100.19.63	Servidor Central	12M	IPC		root	Offline	Network Exce	≠ ×
	1000027	10.100.17. 1 15	Servidor Central	10.100.17.115	IPC	IPC-EBW81242	root	• Online		¢ 🖊 ×

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

Edit Disp.				:	×
Informações	Inserir informa	ações			
Canal de vídeo	2° Protocolo:	Intelbras-1 *	Fabricante:	Intelbras v	
Entrada de	Endereço IP:	• 10.100.17.115	Usuário:	• admin	
Saída alarme	Porta:	• 37777	Senha:		
	Servidor:	Servidor Central	Organização:	root 🔻	
	Informações s	obre o dispositivo			
	Nome do	• 10.100.17.115	SN:	5G04AE7PAG2AAEC	
	Dispositivo: Tipo:	IPC *	Modelo:	IPC-EBW81242	
Obter informações	1°			OK Cancelar	r

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".

Edit Disp.					×
Informações	Quantidade de ca	• 1 Tipo	transm: Stream Ext	•	
Canal de vídeo	Nome	Tipo de Camera	Características	SN	Cód. do teclado
Entrada de	Fisheye 2	Câmera fixa 🔻	Alarme inteligente, Le		
Saída alarme			 Alarme inteligente Lente fisheye Rastreamento de es Foco elétrico Medição de tempera Estatística de mapa Estatística de linhas Contagem de pesso Estatísticas de área 	cravo/me tura térmico cruzada: as em m	[4] € 1/1 ▶ ▶]
Obter informações					OK Cancelar

3.7.2.3 Configurando o módulo Gestão de Loja

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

DEFENSE IA	I 🕂			
	۲	2		(3)
	Dispositivo	Usuário	Eventos	Armazenamento
	Gerenciamento de dispositivos conectados à plataforma. Permite adicionar, editar e excluir dispositivos.	Gerenciamento de usuários e funções. Permite o gerenciamento e permissões dos usuários.	Gerenciamento de avisos/alarmes de eventos dos dispositivos ou do sistema. Permite vincular ações aos receber eventos.	Gerenciamento do armazenamento de gravações. Defina planos de gravações e quota de discos.
	Dispositivo	Usuário	Eventos	Armazenamento
DEFENSE IA Início	Nova guia × +			
	Configurações Empresariais			
	۲	2		
	Dispositivo	Usuário Organizaçã	ão Eventos	Armazenamento
	×			
	Mural de vídeo	Mapas Banco de Fa	ces Cadastro de veículos	Velocidade Média
	#			
	Gestão da Loja Gereno	ciamento de intercom		

II. Clique em Adicionar para incluir uma loja

Q. Pesquisar	+ Adi	cionar 📋 Excluir 🛟 Mover para		Q. Pesquisar
▼ root		Nome da loja	Limite de número de pessoas	Operação
		Agencia	12	∕ × ≘

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:

Adicione armaz	×
Inf básica	1F + 3
Nome compra: 2	💠 Mova disp. 💠 Adicionar zona 🔍 Dispositivo/Àre 😭 Modificar mapa
 Analise de area Configuração de tempo livre: 	
 00:00:00 Limite de número de pessoas: 	
Valor de aviso:	
Organização: root • Disp.	
Q. Pesquisar	
▼ III root	
INVD9032 FT IA	
O 10.100.17.80 O	
MHDX Face	
▶ @ 10.100.17.115 1	

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

- Co			×
	Nome da zona:	Àrea 1	
	Câmera associada:	Fisheye 2 🔹	
	Zonas de câmera:	•	
Sale		Tempo 2	
-		Áres 1	
		Áres 2	
		Cit Caller	
			Configurando Área 1
r			Configuration Area 1
Fisheye 2	OK Excluir	×	
Tipo câm.:			
Estat. área	•		

			×	
	Nome da zona:	Àrea 2		
	Câmera associada:	Fisheye 2	•	
	Zapas da aŝenera:	Área 2	_	
	Zonas de camera:	Area 2	*	
- Bailt				
E				
		ок	Cancelar	
- Birdh		1.00		
and and a second	H - H - H - H			
	8 88 88 88	0.0.0		
muranette				
				-
	Fisheye 2		e - 9	
	9.8 8 8	H H H	A 1	
			-	

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".

intelbras Acesso Web				
Config. Câmara	Plano Intelig.			
Def. de Rede				
🔻 Gestão de Eventos				
> Deteção de Video				
> Deteção de Áudio	•			
> Plano Intelig.				
> Análise IVS				
> Deteção Facial				
> Contagem de Pessoas				
> Def. Alarme	Atualizar Guardar			
> Anormalidade				
Gostão de Armar				

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.

Config. Câmara Def. de Rede	Contagem de Pessoas Ajuste da calibração	ColocarFila Reis	atório		_
Gestão de Eventos > Deteção de Video > Deteção de Audio		2020-11-12 (4/27/22	Ø 1 PC-1	Contagem de Pessi	
> Plano intelig. > Análise IVS > Deteção Facial Contagem de Pessoan > Det. Alarme > Anormalidade			Def. Parâmetro Ativar Sobreposição Pierlodo de Function	Limpar	
Gestão de Armaz. Sistema Inform. do Sistema	V1*Teselbras		Alarme Débitofluxo Intr. Número Déticar Número	0	
	Desenhar LL.	Remover	Agend. Gravação Atraso de Gravação	10 s (10-300)	
			Retardar Atarme	10 s (10~300)	
			Config. Global Sensibilidade Altura máxima		s 300)
			Altura minima Padrão At	0 Centimetro (0 ualtzar Guardar	~200)

3.7.3.2 Adicionando a câmera no Defense

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

• +	
Dispositivo	
Gerenciamento de dispositivos conectados à plataforma. Permite adicionar, editar e excluir dispositivos.	Gerenciamento de usuários e funções. Permite o gerenciamento e permissões dos usuários.
Dispositivo	Usuário

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

🛱 Conectar 🛛 🕄 Atualizar 🖉	👌 Inicializar dispositivo	Alterar IP	🌻 Segn	nento da rede Minimizar 🔺
Status de inicialização‡	Endereço IP\$	Modelo‡	Porta	Endereço MAC
Inicializado	10.100.17.111	VIP-9320-3D-IA-FT	37777	bc:32:5f:23:9b:4d
Adicionar lote				×
Organização	o: root	•		
Servido	r: Servidor Central	•		
Usuário	• admin			
Senhs	a:			
			ок	Cancelar

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

🕇 Adic	ionar 🛅 Ex	cluir 🔒 Moo	i 🛃 Imp	G Atualiza	r Orgar	nização: root		•	Q111	8
Todos	Encoder P	ainel de Alarme								
	ID do dispos	IP/Domínio +	Servidor +	Nome do 🕈	Tipo +	Modelo +	Organização	Status +	Offline	Operação
	1000030	10.100.17.111	Servidor Central	10.100.17.111	IPC	VIP-9320-3D-I	root	Online		⊕ 🖉 ×

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

Edit Disp.				×
Informações	Inserir informa	ações		
Canal de vídeo	2° Protocolo:	Intelbras-1 *	Fabricante:	Intelbras v
Entrada de	Endereço IP:	• 10.100.17.111	Usuário:	• sdmin
Saída alarme	Porta:	• 37777	Senha:	
	Servidor:	Servidor Central 🔹	Organização:	root *
	Informações s	obre o dispositivo		
	Nome do	• 10.100.17.111	SN:	6G04852PAG2333B
	Dispositivo: Tipo:	IPC *	Modelo:	VIP-9320-3D-IA-FT
	D			or Orman
Obter Informações				Cancelar

 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".

Edit Disp.					×
Informações	Quantidade de ca	1 Tipo	transm: Stream Ext	•	
Canal de vídeo	Nome	Tipo de Camera	Características	SN	Cód. do teclado
Entrada de	VIP Intelbras	Câmera fixa 🔻	Alarme inteligente,C		
Saída alarme			 Alarme inteligente Lente fisheye Rastreamento de e Foco elétrico Medição de tempei Estatística de mapi Estatística de linha Contagem de pess Estatísticas de árei 	escravo/me ratura a térmico as cruzada: soas em m a	
			Tot	tal 1 Gravação(ões)	
Obter informações					OK Cancelar

- 3.7.3.3 Configurando o módulo Gestão de Loja
 - I. Clique no símbolo de "+" para encontrar o módulo "Gestão de Loja"

•			
	2		
Dispositivo Gerenciamento de dispositivos conectados à plataforma. Permite adicionar, editar e excluir dispositivos.	Usuário Gerenciamento de usuários e funções. Permite o gerenciamento e permissões dos usuários.	Eventos Gerenciamento de avisos/alarmes de eventos dos dispositivos ou do sistema. Permite vincular ações aos receber eventos.	Armazenamento Gerenciamento do armazenamento de gravações. Defina planos de gravações e quota de discos.
Dispositivo	Usuário	Eventos	Armazenamento

Início	Nova guia × +				
	Configurações Empresariais				
	۲	2	9 9 9 9 9 9 9		3
	Dispositivo	Usuário	Organização	Eventos	Armazenamento
	Mural de vídeo	Mapas	Banco de Faces	Cadastro de veículos	Velocidade Média
	Gestão da Loja	Gerenciamento de intercom			

II. Clique em Adicionar para incluir uma loja

Q. Pesquisar	+ Adicionar	I Adicionar 🛱 Excluir ↔ Mover para				
▼ III root		Nome da loja	Limite de número de pessoas	Operação		
		Agencia	12	/ × =		
		Análise de fluxo		/ x =		
		Análise de área		/ x =		

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:

			×
0	Nome da zona:	Loja	
- []	Câmera associada:	VIP Intelbras	*
	Zonas de câmera:	PC-1	•
		ок са	ancelar
VIP Intelbr	аз ок	Excluir	
VIP Intelbr Tipo câm.:	as OK	Excluir	

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.

DEFENSE IA			×
	Usuário Normal	•	
	10.100.20.52 : 443	- 0	
	L system		
	••••••		
	🗹 Lembrar	Login auto	
	Login		

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

DEFENSE IA	Informações Empre	esariais 🔹 🔹				● ○ △ ◆	<u>м</u> – в×
Recursos	Análise de fluxo	Demografia cliente	Análise de área	Loja em Tempo Real			
Pesquisar Q							
▼ 🖬 Lojas							
🏛 Agencia							
Análise de fluxo							
血 Analise de area 俞 Loja em Tempo Real							
				Sem Res	ultados		
Dia 👻							
2020-11-12							
Pesquisar							

3.7.4.1 Análise de fluxo

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

Recursos	Análise de fluxo	Demografia cliente	Análise de área	Loja em Tempo Real				
Pesquisar Q ▼ 급 Lojas	Fluxo Total de	Clientes				💳 Entrada 💻 Saída ≔ Loca	🔹 🕢	
â Agencia								
Análise de fluxo								
 Análise de área Loja em Tempo Real 								
				9 10 11 12	13 14 15 16	5 17 18 19 20		
	Fluxo de Entra	da de Clientes						
				\wedge				
				/ \				
				/ `	\			
Dia 👻								
2020-11-12					\			
Pesquisar								



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.



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 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)	
on	figure Server		×
	ServerName: * 1	Serverlp: 1	
	ServerType: Server *	0	
	Select Spare Server(s)	Selected Sever (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



2021-02-11



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).

1

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

3

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.

II. Clique no "+".



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



IV. Clique no botão "Adicionar".

DEFENSE IA	Início Do	mínio × +									
		+ Adicionar	📋 Excluir				Or	g: root	• 9	Posquisar	
			Nome	Org o	IP	Port	Usu	Status online $_{\oplus}$	Causa off-line	Operação	
		0	VM (52)	root	10.100.20.52	443	system	on-line		+1 <i>P</i> 14	
		Total 1 gravação(d	ies).					4	1 > Vá	para página 1 A.	

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.

Adicionar cascata		×
Nome :	*	
Org :	root 👻	
Protocolo do dominio :	Dahua 🔻	
End. IP :	*	
Port :	* 4	
NomeUsuário :	*	
Senha :	*	
Comentários :		
	OK Cancela	r

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



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

🕂 Ac	licionar 🛱 Excluir				C	Org: root	• Q	Pesquisar
	Nome	Org 🔶	IP	Port	Usu	Status online 🝦	Causa off-line	Operação
	VM (52)	root	10.100.20.52	443	system	on-line		*] & #

- 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

ENCE IO

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.

Dispositivo	<u>∓</u> Co	nectar 🖸 Atualizar	Inicializar dispositivo	🖋 Alterar IP			🍨 Segmento da r	ede Minimiza
🚍 Recurso de vinculação		Status de inicialização	Endereço IPo	Modelo	90	Porta		Endereço MAC
		 Inicializado 	10.100.14.40	DSS P	ro	443	d	10:94:66:ba:94:72
	+ Adici	onar 💼 Excluir 🔒 Moc	d 🛃 Imp 🗘 Atualiza	r Organização:	root	-	Q @	
	Todos	Encoder Painel de Alarme	LPR Vídeo porteiro Cr	ntrole do Vídeo Wall				
		ID do dispos IP/Domínio 🔹	Servidor Nome do	Tipo ♦ Mod	elo • Organização	Status •	Offline	Operação
		ID do dispos IP/Domínio • 1000041@001 10.100.17.78	Servidor • Nome do • Servidor Central Celular	Tipo • Mod DVR	elo + Organização root	Status •Offline	Offline Network Exce	Operação
		D do dispos IP/Dominio • 1000041@001 10.100.17.78 1000038@001 10.100.17.105	Servidor • Nome do • Servidor Central Celular Servidor Central Contagem	Tipo • Mod DVR IPC VIP-932	elo • Organização root 0-3D-1 root	Status Offline Offline	Offline Network Exce	Operação III IIII
		D do dispos IP/Dominio • 1000041@001 10.100.17.78 1000038@001 10.100.17.105 1000040@001 10.100.19.64	Servidor • Nome do • Servidor Central Celular Servidor Central Contagem Servidor Central VIP 91260 IA FT	Tipo • Mod DVR IPC VIP-932 IPC IPC-HFI	elo e Organização root 0-3D-1 root N712 root	Status Offline Offline Online	Offline Network Exce Network Exce	Operação //
		D do dispos IP/Dominio 1000041@001 10.100.17.78 1000038@001 10.100.17.105 1000040@001 10.100.19.64 1000039@001 10.100.19.22	Servidor • Nome do • Servidor Central Celular Servidor Central Contagem Servidor Central VIP 91260 IA FT Servidor Central INVD 9016	Tipo • Mod DVR IPC VIP-932 IPC IPC-HFT NVR INVD 90	Organização 0-3D-1 root N712 root 16 P root	Status • • Offline • Offline • Online • Online	Offline Network Exce Network Exce	Operação // //
		D do dispos IP/Domínio • 1000041@001 10.100.17.78 1000038@001 10.100.17.105 1000039@001 10.100.19.64 1000039@001 10.100.19.22 1000037@001 10.100.17.115	Servidor e Nome do e Servidor Central Celular Servidor Central Contagem Servidor Central VIP 91260 IA FT Servidor Central INVD 9016 Servidor Central VIP 91210 F IA	Tipo • Mod DVR IPC VIP-932 IPC IPC-HPC NVR INVD 90 IPC IPC-EB	organização 0rganização -root 0-3D-1 0-3D-1 root N712 root 116 P root W81242	Status Offline Offline Offline Onfline Online Online	Offline Network Exce	Operação // // //

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 18	8 - Reprodu	ção de gravaçã	io	
D	EFENSE 🖪 📃 🧖	eprodução de gravação	Visualização 1	Ð	4) 2 🚨 🗘	<i>₀</i> – □ ×
\odot						
[::]	★ Pesquisar Q					
	▼ 🔲 🖬 Vídeo (7/7)					
	▶ 10.100.19.14					
	 IO.100.19.21 IO.100.19.23 					
	 Image: 10.100.19.22 Image: 10.100.19.63 					
	▶ 🗖 🗖 10.100.19.54					
	▶ 🔲 🛤 10.100.19.28					
	▶ 🔲 🙆 10.100.19.76					<
	12/11 00:00-12/11 23:59					
	Gravação no Servidor 🔹	01:00 03:00 05:00	07:00 09:00	11:00 13:00 15:00 020-12-11 12:00:00	17:00 19:00 2	1:00 23:00
	Pesquisar	● × Ł ▼ ₪		► ► ► ► ► ► ► ► ► ► ► ► ► ► ► ► ► ► ►	cheia 🔻 🚼 🎫	III 🔽 🖾

Tabela 28 - Parâmetros reprodução de gravação

Ícone Descrição				
A	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			
T	Filtro de vídeo de acordo com o tipo de gravação.			
國	Faça uma análise de detecção dinâmica em alguma área da imagem gravada, apenas reproduz o vídeo com a imagem dinâmica na área de detecção.			
I÷I	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 **D** 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
Ŧ	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.
٥	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.
Ģ	Zoom in	Selecione uma seção para ampliar e ver os detalhes.
\times	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.



Tabela 30 - Parâmetros de menu de atalhos

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

Nome	Descrição
	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
Sobreposição de	e Sobreposição de objeto e, em seguida, o vídeo ao vivo
IVS	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.
	Habilite a sobreposição de SMD para mostrar o quadro alvo
	sobre o vídeo ao vivo. Quando SMD está habilitado no
Sobreposição de	dispositivo, você pode habilitar sobreposição de SMD para o
SMD	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	Para uma câmera que oferece suporte ao mascaramento de
máscara de	privacidade de rosto humano, você pode desativar o
privacidade	mascaramento aqui para visualizar a imagem do rosto.
Reprodução no	Poproduza o capal atual no vídeo wall
mural	Reproduza o canaratuarno video waii.
	Mude a janela de vídeo para o modo de tela inteira. Para sair
Tela cheia	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.







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







- 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 Q 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 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 Opara 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 a 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.

IV.



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 **Solution** no canto superior esquerdo.

Adicionar tag de	gravação		×
Nome:	Nome tag1		
	-OF	Ca	ancelar

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 a 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

Baixar			×
Hora de início:	2020-12-11 15:13:38	÷	
Horário de término:	2020-12-11 15:14:59	÷	
Transcodificar.			
Formato de arquivo:	avi	•	
	ОК	Cancela	ir



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 in aba de Reprodução de gravação, ou clique em in e selecione o menu Central de Download.

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

DEFENSE IA	Central de Download	0	● > 0 ▲	• • - • ×
Recursos				
★ Pesquisar Q				
 Vídeo (7/8) 10.100.19.14 10.100.19.21 10.100.19.22 10.100.19.63 10.100.19.54 	☐ IPC ' ' ' ' ' ' ' 01 02 03 04 05		' ' ' ' ' ' ' ' ' '	' ' ' ' 20 21 22 23
 ► 10.100.19.28 ► 2 10.100.19.76 ► Nova Versao iMHI 	Pausar tudo 📄 Excluir todi	Fazendo download	Baixado	
12/11 00:00-12/11 23:59 Gravação no Servidor ▼ 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 **De** 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.
4		De	7 205	0		•								
1		0.0	202	.0		r.,								
Dom	Seg	Ter	Qua	Qui	Sex	Sáb	Do	m	Seg	Ter	Qua	Qui	Sex	Sáb
29	30	1	2	3	4	5	2							5
6	7	8	9	10	0	12							1	12
13	14	15	16	17	18	19	1	3	14	15	16	17	18	19
20	21	22	23	24	25	26	2		21	22	23	24	25	26
27	28	29	30	31					28	29	30	31		
		5								5				
20	20-12	2-11	00.00	-00		•		20:	20-12	2-11	23.50	-59		

Figura 200 - Selecione o período





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



- 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 <u>at</u>ual e a próxima imagem.
- **Passo 5.** Clique em o 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 te selecione Sistema.
Passo 2. Clique na guia HTTPS.

		Figura 205	- HTTPs	certificate		
Import SSL Certi	ficate:		Browse	Password:	* ******	×
Passo 3.	Clique	em Procurar, impo	orte o cer	tificado SS	SL e digite a se	enha.

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

🕒 Message Stor	age Time					
S Time Sync		Mail Server				
Server		C Enable				
Active Directo	у	SMTP Server Type:	UserDefined •	Sender Mail Address:	• Competition	
U HTTPS		SMTP Server:	• 10.1 0.07	Password:	• • • • • • • • • • • • • • • • • • • •	
POS End		Port.	• 25	Test Recipient:	xxxx@xxx.com	
		Encryption Type:	TLS Encrypt			Mail Test





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

UserDefined 🔹
Yahoo
Gmail
Hotmail
UserDefined

- **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.

	Figu	ira 208 - C	Jestao de s	servidor		
U Server Management	C Refresh					
Resource Allocation	Server Name	IP	Device ID	Type	Server Status	Operation
	Center Server		video#master	Home Server	Running Status: Running Server Status: Enabled	đ
			vide 78	Home Server	Running Status: Running Server Status: Enabled	ON / 🗘 🛪

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

- Image: significa que o servidor não está habilitado; Clique no ícone e ele se torna
 Image: 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.

Server Config	🖀 Auto Distribution 🛛 💭 Refresh							
📰 Resource Config	All Device	O Default 11 Sort by device quantity						
	Search	Center Server (134) ● ■ 4 ◆ 1 □ 1 □ 1 □ 128						
	n ghf_							

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.

Dev	vice Type :				
Select Serv	er			Q	
			Server Name		
			Center Server		
Distribution	ute devices evenly to	selected server.			

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?

Forgot your passwor	d?			×
1. Password Secu	rity Setup	1.Password Security Security	etup 2.Res	et Password
	1.Who is y	our favorite athlete?		
	*			
	2.Who is y	our favorite pop star?		
	•			
	3.What is y	our favorite flower in spring?		
	*			
			Next	Cancel

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 .



Edit User				
Basic Info				
Username:	dsfff		Password Expiry:	
Multiple Points of Presence:	OFF I		MAC Address:	
Reset Password:	ON		PTZ Control Permission:	* 5
Password:	* ••••••		Email Address:	
Confirm:	* ********		Remark:	
Role		Device F	ermissions	Control Permissions
Rolena	ame	Q Sea	arch	 All Permissions
Adminis	trator	▼	root	Control Permissions
C Opera	tor			Menu Permissions Administrator Menu
				 Client Menu

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.

	FI	gura 213 - Defi	na o tempo de a	irmazenamento da mensagem
۲	Configuração de tempo de			
6	Sincronização de hora	Configuração de tempo	de armazenamento das mensage	ns
2	Servidor de email	Logs:	* 30	Dia
6	Diretório ativo	Informações sobre o alarme:	* 30	Dia
	HTTPS	Informação sobre o GPS:	* 30	Dia
	Final de PdV	PdV:	* 30	Dia
		Mapa de calor:	* 30	Dia
		Reconhecimento facial:	* 180	Dia
		Gravação de veículos passados:	* 180	Dia
		Dispositivo de Fotos de acesso:	* 180	Dia
		Análise do cliente:	* 180	Dia
		Salvar		

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 DEFENSE IA Olá , handka y Início + Gerenciamento do armazenamento Gerenciamento de dispositivos Gerenciamento de usuários e Gerenciamento de avisos/alarmes funções. Permite o gerenciamento de gravações. Defina planos de conectados à plataforma. Permite de eventos dos dispositivos ou do e permissões dos usuários. sistema. Permite vincular ações gravações e quota de discos. adicionar, editar e excluir aos receber eventos. dispositivos. Dispositivo Usuário **Eventos** Armazenamento Visão Geral Licença Suporte Email: suporte.defense@intelbras.com.br Versão de teste Detalhes da licenca Online Offline Status: Versão: V7.002.00/B006.1.R.20200807.1802367 Dispositivo: 11 3 Etapa 1: Exportar arquivo de solicitação de licença. Usuário 3 14 Etapa 2: Contate o vendedor para obter uma licença. 17 Servico: 0 Etapa 3: Importe a licença. HD: 181G/589G

Passo 5. Clique em "Exportar arquivo de solicitação de licença.".

Figura 215 - Menu para exportar arquivo de solicitação de licença

conectados à plát adicionar, editar e dispositivos.	Vídeo • Avaliação POS • Avaliação	140	44	2021-02-24	- 0 +	afina planos de
Dispos	POS • Avaliação					a de discos.
		10	2	2021-02-24	- 0 +	namento
	Controle de acesso • Avaliação	64	1	2021-02-24	- 0 +	
2	Vídeo porteiro • Avaliação	64	0	2021-02-24	- 0 +	
Visão Geral	Host alarm Avaliação	100	1	2021-02-24	- 0 +	
Status Dispositivo:	LPR • Avaliação	15	2	2021-02-24	- 0 +	.R.20200807.1802367
Usuário:	Reconhecimento f • Avaliação	20	6	2021-02-24	- 0 +	
Serviço:	Terminais de frequ • Avaliação	5	0	2021-02-24	- 0 +	

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 <u>suporte.defense@intelbras.com.br</u> 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

Remote Log :			
Enable			
IP Address:	* 127.0.0.1	Platform Number:	* 22
Port:	* 514		

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.

- 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**.
- Ш
- > O sistema sincroniza imediatamente a hora após a ativação da função.



Configuração local					×
🜻 Básico	Básico				
🔂 Vídeo	Idioma	Português (Brasil)	 (Reinicialização necessária) 		
Reprodução	Tema	Escuro	 (Reinicialização necessária) 		
Snapshot	Resolução	1280*800	•		
🖴 Gravação		Sincronizar horário			
🜲 Alarme		Iniciar com Windows			
🖽 Mural de vídeo		Manter mosaíco de câm	eras ao inicializar		
🗃 Atalhos		Áudio auto-adaptável			
		Z Exibir dispositivos			
	Video				
	Divisão padrão				
				Padrão Salvar Can	celar

Figura 217 - Habilitar sincronização de horário

- Clique 🛨 na interface Web do Defense IA Server e, em seguida, Passo 2. selecione Sistema.
- Clique na guia Sincronização de hora e marque a caixa de seleção para Passo 3. ativar a função. Defina os parâmetros de sincronização de tempo.

1 igura 210 - Habilitar Sincronização de nora	1
ema × +	Olá , , se i :
Sincronização de hora	
Sincronização Agendada	
Hora de início: * 00.00.00 Intervalo da sincronização: * 24	Hora Sincronizar
Sincronizar nos dispositivos	
	Intervalo da sincronização: • 24 Sincronizar nos dispositivos

----~ . . 1.1.1.1.114 .

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, <u>consulte</u> "4.4.1 Sincronização Agendada de Horário."

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

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



DEFEN	NSE IA Início	Sistema × +		Olá, NHI LANI 🔹
e	Configuração de tempo de			
Ø	Sincronização de hora	Sincronização de hora		
	Servidor de email	Sincronização Agendada		
	Diretório ativo	Hora de início: + 00:00:00	Intervalo da sincronização: * 24	Hora
	HTTPS	Sincronizar nos dispositivos		
E	Final de PdV			

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 **t** na interface Web do Defense IA Server e selecione Backup e restauração.

Figura 220 - Backup

	r igaia 220	Baenap
Backup Restaurar		
	Backup manual	Backup automático
		Período: Dia Hora: 03:00:00
Passo 2	Clique em Backun manual	
F a 3 3 U Z.	CIIQUE EIII DAUKUD MAHUAI.	

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

Acesso régido Nome Data de modificação Tipo Tamanho Aces de Tabalho 127.0.0.1_oscadb_2020102_1.sql 20/10/2020 03:00 Arquivo SQL 1.033 KB Downhoads 127.0.0.1_oscadb_20201022_1.sql 22/10/2020 00:00 Arquivo SQL 58.699 KB Documentos 127.0.0.1_oscadb_20201022_1.sql 22/10/2020 00:00 Arquivo SQL 58.699 KB Imagens 127.0.0.1_oscadb_20201114_1.sql 22/10/2020 00:00 Arquivo SQL 58.699 KB Músicas 127.0.0.1_oscadb_20201114_1.sql 14/11/2020 23:00 Arquivo SQL 56.906 KB Músicas 127.0.0.1_oscadb_20201114_1.sql 14/11/2020 23:00 Arquivo SQL 58.217 KB Systemi22 127.0.0.1_oscadb_20201115_1.sql 15/11/2020 23:00 Arquivo SQL 58.217 KB Videos 127.0.0.1_oscadb_20201210_fml_1.sql 15/11/2020 23:00 Arquivo SQL 1.639 KB 127.0.0.1_oscadb_20201210_fml_1.sql 10/12/2020 02:00 Arquivo SQL 1.639 KB 127.0.0.1_oscadb_20201210_fml_1.sql 10/12/2020 02:00 Arquivo SQL 1.639 KB 127.0.0.1_oscadb_20201210_fml_1.sql 10/12/2020 02:00 Arquivo SQL 1.640 KB Downhoads </th <th>🚽 Y 🛧 📙 «</th> <th>Disc</th> <th>o Local (C:) → Defense IA → Server → bak →</th> <th>db_backup 🗸</th> <th>Pesquisar d</th> <th>b_backup</th> <th>3</th>	🚽 Y 🛧 📙 «	Disc	o Local (C:) → Defense IA → Server → bak →	db_backup 🗸	Pesquisar d	b_backup	3
Access of spildo 127.0.0.1_oscadb_20201020_1.sql 20/10/2020 03:00 Arquivo SQL 1.033 KB Area de Trabalho 127.0.0.1_oscadb_20201020_1.sql 20/10/2020 03:00 Arquivo SQL 58.699 KB Downloads 127.0.0.1_oscadb_20201022_1.sql 22/10/2020 00:00 Arquivo SQL 58.699 KB Downloads 127.0.0.1_oscadb_20201022_1.sql 22/10/2020 00:00 Arquivo SQL 58.699 KB Imagens 127.0.0.1_oscadb_20201112_1.sql 14/11/2020 23:00 Arquivo SQL 56.906 KB Músicas 127.0.0.1_oscadb_20201114_1.sql 14/11/2020 23:00 Arquivo SQL 56.217 KB System32 127.0.0.1_oscadb_20201115_dnql 15/11/2020 23:00 Arquivo SQL 58.217 KB Videos 127.0.0.1_oscadb_20201115_dnql 15/11/2020 23:00 Arquivo SQL 58.217 KB Videos 127.0.0.1_oscadb_20201210_dnql 10/12/2020 02:00 Arquivo SQL 1.639 KB 127.0.0.1_oscadb_20201210_dnql 10/12/2020 02:00 Arquivo SQL 1.639 KB 127.0.0.1_oscadb_20201210_dnql 10/12/2020 02:00 Arquivo SQL 1.630 KB 127.0.0.1_oscadb_20201210_dnql 11/12/2020 02:00 Arquivo SQL 1.630 KB <t< th=""><th>and the second second second</th><th></th><th>Nome</th><th>Data de modificação</th><th>Tipo</th><th>Tamanho</th><th></th></t<>	and the second second second		Nome	Data de modificação	Tipo	Tamanho	
Area de Trabalho * 127.0.0.1_oseadb_2020102_dmi_1.sqi 20/10/2020 03:00 Arquive SQL 449 K8 Downhoads 127.0.0.1_oseadb_20201022_1.sqi 22/10/2020 00:00 Arquive SQL 58.699 K8 Documentos 127.0.0.1_oseadb_20201022_1.sqi 22/10/2020 00:00 Arquive SQL 58.699 K8 Imagens 127.0.0.1_oseadb_20201114_1.sqi 22/10/2020 00:00 Arquive SQL 56.906 K8 Musicas 127.0.0.1_oseadb_20201114_1.sqi 14/11/2020 23:00 Arquive SQL 56.399 K8 System32 127.0.0.1_oseadb_20201115_1.sqi 15/11/2020 23:00 Arquive SQL 58.217 K8 Videos 127.0.0.1_oseadb_20201115_dml_1.sqi 15/11/2020 23:00 Arquive SQL 58.217 K8 OneDrive 127.0.0.1_oseadb_20201116_dml_1.sqi 15/11/2020 23:00 Arquive SQL 1.639 K8 127.0.0.1_oseadb_20201210_dml_1.sqi 10/12/2020 02:00 Arquive SQL 1.639 K8 127.0.0.1_oseadb_20201210_dml_1.sqi 11/12/2020 02:00 Arquive SQL 1.640 K8 127.0.0.1_oseadb_20201211_sdi 11/12/2020 02:00 Arquive SQL 1.640 K8 Downhoads 127.0.0.1_oseadb_20201211_sdi 11/12/2020 02:00 Arquive SQL 1.654 K8	Acesso rápido		127.0.0.1 oseadb 20201020 1.sql	20/10/2020 03:00	Arquivo SOL	1.033 KB	
Downloads I 127.0.0.1_oseadb_20201022_1.rql 22/10/2020 00:00 Arquive SQL S8.699 K3 Documentos I 127.0.0.1_oseadb_20201022_dml_1.sql 22/10/2020 00:00 Arquive SQL S8.699 K3 Musicas I 127.0.0.1_oseadb_20201114_inql 14/11/2020 23:00 Arquive SQL S6.359 K3 System32 I 127.0.0.1_oseadb_20201114_inql 14/11/2020 23:00 Arquive SQL S6.359 K3 Videos I 127.0.0.1_oseadb_20201114_inql 14/11/2020 23:00 Arquive SQL S6.359 K3 System32 I 127.0.0.1_oseadb_20201115_inql 15/11/2020 23:00 Arquive SQL S6.359 K3 Videos I 127.0.0.1_oseadb_20201115_inql 15/11/2020 23:00 Arquive SQL S8.217 K8 Videos I 127.0.0.1_oseadb_20201210_inn_1.sql 15/11/2020 23:00 Arquive SQL 1.639 K3 OneDrive I 127.0.0.1_oseadb_20201210_inn_1.sql 11/12/2020 02:00 Arquive SQL 1.639 K3 OneDrive I 127.0.0.1_oseadb_20201211_inql 11/12/2020 02:00 Arquive SQL 1.640 K3 Exte Computador I 227.0.0.1_oseadb_20201211_inql 11/12/2020 02:00 Arquive SQL 1.054 K3 Downloads Imsgens I 227.0.0.1_oseadb_20201211	Area de Trabalho	*	127.0.0.1 oseadb 20201020 dml 1.sol	20/10/2020 03:00	Arquive SQL	449 KB	
Documentos # 127.0.0.1_oseadb_20201022_dml_1.sql 22/10/2020 00:00 Arquive SQL 58.164 K3 Imagens # 127.0.0.1_oseadb_20201114_dml_1.sql 14/11/2020 23:00 Arquive SQL 56.96 K3 Musicas 127.0.0.1_oseadb_20201114_dml_1.sql 14/11/2020 23:00 Arquive SQL 56.359 K3 System32 127.0.0.1_oseadb_20201115_1.sql 15/11/2020 23:00 Arquive SQL 58.217 K8 Videos 127.0.0.1_oseadb_20201115_1.sql 10/12/2020 02:00 Arquive SQL 57.670 K8 OneDrive 127.0.0.1_oseadb_20201210_1.sql 10/12/2020 02:00 Arquive SQL 1.638 K8 OneDrive 127.0.0.1_oseadb_20201210_dml_1.sql 10/12/2020 02:00 Arquive SQL 1.640 K3 Area de Trabalho 127.0.0.1_oseadb_20201211_sql 11/12/2020 02:00 Arquive SQL 1.054 K8 Downloads 1127.0.0.1_oseadb_20201211_dml_1.sql 11/12/2020 02:00 Arquive SQL 1.054 K8 Downloads 100.0.1_oseadb_20201211_dml_1.sql 11/12/2020 02:00 Arquive SQL 1.054 K8 Downloads 100.0.1_oseadb_20201211_dml_1.sql 11/12/2020 02:00 Arquive SQL 1.054 K8 Downloads 100.0.1_oseadb_20	👆 Downloads	*	127.0.0.1 oseadb 20201022 1.sql	22/10/2020 00:00	Arguivo SQL	58.699 KB	
Imagens 127.0.0.1_oseadb_20201114_1.aql 14/11/2020 23:00 Arquive SQL 56.359 KB 127.0.0.1_oseadb_20201115_1.aql 14/11/2020 23:00 Arquive SQL 56.359 KB System32 127.0.0.1_oseadb_20201115_1.aql 15/11/2020 23:00 Arquive SQL 58.217 K8 Videos 127.0.0.1_oseadb_20201115_dml 1.aql 15/11/2020 23:00 Arquive SQL 58.217 K8 127.0.0.1_oseadb_20201115_dml 1.aql 15/11/2020 23:00 Arquive SQL 58.217 K8 127.0.0.1_oseadb_20201115_dml 1.aql 15/11/2020 23:00 Arquive SQL 1.639 K8 127.0.0.1_oseadb_20201210_1.sql 10/12/2020 02:00 Arquive SQL 1.639 K8 127.0.0.1_oseadb_20201210_1.sql 10/12/2020 02:00 Arquive SQL 1.639 K8 127.0.0.1_oseadb_20201211_sql 11/12/2020 02:00 Arquive SQL 1.639 K8 127.0.0.1_oseadb_20201211_sql 11/12/2020 02:00 Arquive SQL 1.640 K8 Ta50.0.1_oseadb_20201211_sql 11/12/2020 02:00 Arquive SQL 1.640 K8 Ta50.0.1_oseadb_20201211_dml 1.aql 11/12/2020 02:00 Arquive SQL 1.640 K8 Documentos Documentos Documentos Douvnloads Imagens Mukicas Objetos 3D Videos Docuce Local (Ci) Disco Local (Ci)	🖹 Documentos	1	127.0.0.1_oseadb_20201022_dml_1.sql	22/10/2020 00:00	Arquivo SQL	58.164 KB	
Mušicas 127.0.0.1_oseadb_20201114_dmi_1.sql 14/11/2020 23:01 Arquivo SQL 56.359 KB System32 127.0.0.1_oseadb_20201115_1n.sql 15/11/2020 23:00 Arquivo SQL 58.217 KB Videos 127.0.0.1_oseadb_20201115_dmi_1.sql 15/11/2020 23:00 Arquivo SQL 57.670 KB 127.0.0.1_oseadb_20201210_1.sql 10/12/2020 02:00 Arquivo SQL 1.639 KB 127.0.0.1_oseadb_20201210_1.sql 10/12/2020 02:00 Arquivo SQL 1.640 KB 127.0.0.1_oseadb_20201211_sql 11/12/2020 02:00 Arquivo SQL 1.640 KB ComeDrive 127.0.0.1_oseadb_20201211_sql 11/12/2020 02:00 Arquivo SQL 1.640 KB Este Computador 127.0.0.1_oseadb_20201211_dml_1.sql 11/12/2020 02:00 Arquivo SQL 1.654 KB Documentos Documentos 127.0.0.1_oseadb_20201211_dml_1.sql 11/12/2020 02:00 Arquivo SQL 1.054 KB Mušicas Documentos 127.0.0.1_oseadb_20201211_dml_1.sql 11/12/2020 02:00 Arquivo SQL 1.054 KB Mušicas Documentos 127.0.0.1_oseadb_20201211_dml_1.sql 11/12/2020 02:00 Arquivo SQL 1.054 KB Mušicas Documentos 10/15/15/15/15/15/15/15/15/1	📰 Imagens	*	127.0.0.1_oseadb_20201114_1.sql	14/11/2020 23:00	Arquive SQL	56.906 KB	
System32 127.0.0.1_oseadb_20201115_1.sql 15/11/2020 23:00 Arguivo SQL 58.217 K8 Videos 127.0.0.1_oseadb_20201210_1.sql 15/11/2020 23:00 Arguivo SQL 57.670 K8 127.0.0.1_oseadb_20201210_1.sql 10/12/2020 02:00 Arguivo SQL 1.639 K8 127.0.0.1_oseadb_20201210_dml_1.sql 10/12/2020 02:00 Arguivo SQL 1.639 K8 127.0.0.1_oseadb_20201210_dml_1.sql 10/12/2020 02:00 Arguivo SQL 1.630 K8 127.0.0.1_oseadb_20201210_dml_1.sql 11/12/2020 02:00 Arguivo SQL 1.630 K8 CheDrive 127.0.0.1_oseadb_20201211_sql 11/12/2020 02:00 Arguivo SQL 1.640 K8 Este Computador 127.0.0.1_oseadb_20201211_dml_1.sql 11/12/2020 02:00 Arguivo SQL 1.054 K8 Documentos Documentos Documentos Videos Videos Videos Videos Videos Disco Local (CL) Disco Local (CL) Videos Videos Videos Videos Videos	h Músicas		127.0.0.1_oseadb_20201114_dml_1.sql	14/11/2020 23:01	Arquivo SQL	56.359 KB	
Videos 127.0.0.1_oseadb_20201115_dml_1.sql 15/11/2020 02:00 Arguivo SQL 57.670 KB Videos 127.0.0.1_oseadb_20201210_1sql 10/12/2020 02:00 Arguivo SQL 1.639 KB DoceDrive 127.0.0.1_oseadb_20201210_dml_1.sql 10/12/2020 02:00 Arguivo SQL 1.639 KB Este Computador 127.0.0.1_oseadb_20201211_sql 11/12/2020 02:00 Arguivo SQL 1.640 KB Area de Trabalho 127.0.0.1_oseadb_20201211_dml_1.sql 11/12/2020 02:00 Arguivo SQL 1.054 KB Downloads Imagens Nusicas Doynloads 1 1 Disco Local (C;) Disco Local (C;) 1 1 1 1	System 32		127.0.0.1_oseadb_20201115_1.sql	15/11/2020 23:00	Arquivo SQL	58.217 KB	
integers introductor	Wideos		127.0.0.1_oseadb_20201115_dml_1.sql	15/11/2020 23:00	Arquivo SQL	57.670 KB	
Interpretein 127.0.0.1_oseadb_20201210_dml_1.sql 10/12/2020 02:01 Arquivo SQL 1.033 KB OneDrive I127.0.0.1_oseadb_20201211_1.sql 11/12/2020 02:00 Arquivo SQL 1.640 KB Este Computador I27.0.0.1_oseadb_20201211_dml_1.sql 11/12/2020 02:00 Arquivo SQL 1.054 KB Area de Trabalho Documentos Documentos Inagens Videos Inagens Músicas Dobjetos 3D Videos Insc Local (Ci) Insc Local (Ci) Insc Local (Ci)	Videos		127.0.0.1_oseadb_20201210_1.sql	10/12/2020 02:00	Arquive SQL	1.639 KB	
OneDrive 127.0.0.1_oseadb_20201211_1.sql 11/12/2020 02:00 Arguivo SQL 1.640 XB Este Computador 127.0.0.1_oseadb_20201211_dmL_1.sql 11/12/2020 02:00 Arguivo SQL 1.054 KB Area de Trabalho Documentos Documentos Documentos Documentos Downloads Imagens Músicas Dojutos 3D Este Sub Discos Local (Ci.) Discos Local (Ci.) Discos Local (Ci.) Discos Local (Ci.)			127.0.0.1_oseadb_20201210_dmil_1.sql	10/12/2020 02:01	Arquivo SQL	1.053 KB	
Este Computador 127.0.0.1_oseadb_20201211_dml_1.sql 11/12/2020 02:00 Arquivo SQL 1.054 K8 Area de Trabalho Documentos Documentos Dominoads Imagens Musicas Dipletos 3D Videos Linico Locel (C:)	OneDrive		127.0.0.1_oseadb_20201211_1.sql	11/12/2020 02:00	Arquivo SQL	1.640 KB	
Area de Trabalho Documentos Documentos Downloads Imagens Muisicas Objetos 3D Videos L Disco Local (C:)	Este Computador		127.0.0.1_oseadb_20201211_dml_1.sql	11/12/2020 02:00	Arquive SQL	1.054 KB	
 Documentos Downloads Imagens Músicas Objetos 3D Videos Linso Local (Ci) 	📑 Área de Trabalho	8					
Downloads Imagens Musicas Objetos 3D Videos Disco Locel (C:)	Documentos						
 Imagens Músicas Objetos 3D Wideos Li Disco Local (Ct) 	Downloads						
Músicas ■ Objetos 3D ■ Vídeos … Disco Local (Ct)	El Imagens						
Mojetos 3D Videos Videos Disco Local (C:)	h Músicas						
Uijetes 50 Videos L Disco Local (Ci)	Objetere 2D						
Wideos La Disco Local (C:)	Dijetos 3D						
Disco Local (C:)	Videos						
	Disco Local (C:)						
	1000 C						10-

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 - R	estaurar
Restaurar	Local	Goodeana
Passo 3.	Clique em Local.	

Figura 223 - Restau	urar manualment	e (1)
Restauração manual		×
Selecione o arquivo de	P	esquisar
restauraçao,	ок	Cancelar



- **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.

Figu	ura 224 - Restaurar manualmente (2)	
Restauração manual		×
Senha:	•	
Senha criptografada:	•	
	Esta operação irá apagar os dados já existentes; para continuar,	
	digite a senha de login.	
	OK Cancela	ar

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 précondição 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

	0	
🗗 Backup		
Restaurar		
	0	
	Ð	G
	· · ·	
	Local	Servidor

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

Recuperação do servidor			×
SN	Hora	Tamanho do arquivo	Operação
1	2020-12-11	221.29MB	0
2	2020-12-10	221.06MB	0
3	2020-12-09	220.83MB	0
4	2020-12-08	220.46MB	0
5	2020-12-07	220.11MB	0
6	2020-12-06	220.14MB	0
7	2020-12-05	220.09MB	0
8	2020-12-04	219.84MB	0
9	2020-12-03	219.21MB	0
10	2020-12-02	218.56MB	0
		Total 112 Gravação(ões)	⊲ ⊲ 1/12 ► ►

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



Recuperação do servido	or		×
Senha:	•		
Senha criptografada:	• Este operarão irá epenar os dados iá evi	stentes: nara continuar	
	digite a senha de login.	sientes, para continuar,	
		OK	ır

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.

por evento e nora.

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.

o de Log 🛛 Log de operação do G	ere 🔹 🔹 Tipo de evento: Todos	• Periodo 200	0-12-11 🔽 - 2020-12-11 🔄 🔍 Perganar	Lt top
нога	Nome do Usuário	Tipo de evento:	Contecidos de eventos	P
2020-12-11 13:46:33	ponatan	Sackup e restauração	Backup	**
2020-12-11 13:42:29	poratan	Logm	D.I	
2020-12-11 13:12:20	ponatan	Login	Logie	
2020-12-11 13:12:11	poratan	Login	Lögin	N. 81 (1999)
2020-12-11 11:32:15	Kisser	Login	Ext	
2020-12-11 10:53:30	Keser	Login	Login	
2020-12-11 10:29:09	Kleser	Login	Est.	100.000
2020-12-11 10:23:37	victor	Login	Login	10.0 - 10
2020-12-11 10:23:37	victor	Login	Login	24.64
2020-12-11 09:54:05	Kleser	Modelo de tempo	Adicionar Modelo de tempo : Noñe madrugada	1.4.875
2020-12-11 09:39:04	poratan	Login	Ext	1000
2020-12-11 09:20:09	xeser	Amazenamento	Adicionar Plano de gravação : Gravação Direta	1.10.001
2020-12-11 09:03:04	Neser	Login	Logie	-
2020-12-11 05-45-55	itotalar	Look	Logie	10.00000

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.



4.7.2 Status de execução

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

	J J		<u>2</u>
Status de execução			ت ا
CPU(4.5%)	CPU escrava		
	Nome	q	Utilização do CPU
Arm.(31%)	Detalhe		
	Nome	ιp	Uso do armazenamento
Largura de banda			 Dara haiyo e Dara dima
Mbps			
	¢		
	14:47:0	10	
	1.474710		

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.

		rigula 201		5 301 MQ03		
👯 Estado do servidor	Estado	do servidor				L L
Status do dispositivo						
🙎 Status de usuário		Nome	Endereço IP	ID do dispositivo	Тіро	Estado do servidor
Relatório de integridade do		Servidor Central	10.100.44.57	Master	Servidor	Status de execução: 📦 … Status de habilitação: 🌒 …
		Nome	Tipo de	Serviço	Status	
	ADS(16001)		ADS (serviço de des	pacho de alarmes)	 Online 	
	SS(1001)		SS (serviços de a	SS (serviços de armazenamento)		
		PTS(13001)	PTS (serviço de transferência de imagens)		Online	
		PES(11001)	PES (serviço de amblente de alimentação)		Online	
		MTS(2001)	MTS (serviço de transferência de meio)		Online	
		ARS(8001)	ARS (serviço de registros ativos)		Online	
		PCPS(9001)	PCPS (controle de lista de	a de proxy; serviço de proxy) Online		
		MGW(103001)	MGW (serviço de gateway de midia) MCDRADAR (serviço de gerenclamento de radar)		 Online 	
		MCDRADAR(49001)			Online	
	MCDD		MCDD	OOR	 Online 	
		MCDPOS(39001)	MCD_PdV (dispositivo	de múltiplos controles)	 Online 	
		MCDLED(33001)	MCD_	LED	 Online 	
	Total 1 gra	avação(ões).			I ► V	à para 1 Ir

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.

🛱 Estado do servidor	Status do dispositivo		Tempo real Histórico		ت ا
💼 Status do dispositivo	Organização: ITEC	•		Q. Pesquisar	🛃 Exportar
🙇 Status de usuário	ID do dispositivo	Statue	Nome do Dispositivo	Organização	(P/Dominia
Relatório de integridade do	1000074	Online	SS3530	ITEC	1.010 (2.10
	1000072	Online	VIP 5550 Z IA ITEC	ITEC	10/10/10/2017
	1000069	Online	VIP 7223 LPR	ITEC	13/10/15/20
	1000068	Online	AMT 2018 EG - Treinamento	ITEC	
	1000063	Online	SVR 7116 IA	A TORRE A	1.0100 10.000

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.

Estado do servidor	Status do dispositivo		Tempo real Histò	rico.	r
📰 Status do dispositivo	Periodo: 2020-12-11	- 2020-12-11 📰 Organiz	аção: пес	• C. Pesquisar	🗠 Exporta
🎗 Status de usuário	Hora	Status	Nome do Dispositivo	Nome da organização	(P/Dominia
Relatório de integridade do	2020-12-11 14:59:24	 Offline 	86.77700	ITEC	N . M 2 . NO
	2020-12-11 14:58:20	 Offline 	84.77722	ITEC	10.00.01.000
	2020-12-11 14:56:43	 Offline 	84.774702	ITEC	12 10 2 102
	2020-12-11 14:56:11	 Offline 	84.774702	ITEC	11.00.2.00
	2020-12-11 14:55:20	Online	10.000	ITEC	11 11 21 11
	2020-12-11 14:52:53	 Offline 	0.0.757000	ITEC	11 IN 2 102
	2020-12-11 14:51:48	Offline	0.0.7517000	ITEC	11 IN 2 102
	2020-12-11 14:51:16	Offline	0.0.7517000	пес	11 (M 2) M2
	2020-12-11 14:50:08	Offline	0.0.7517022	пес	10 (M 2) M2
	2020-12-11 14:49:36	Offline	0.0.771702	пес	10.00.01.000
	2020-12-11 14:46:20	Offline	8.6.771722	пес	10.00.01.00
	2020-12-11 14:45:15	Offline	84.77 YEAR	пес	11.00.21.02
	2020-12-11 14:39:50	Offline	84.77 YEAR	пес	10.00.21.02
	2020-12-11 14:38:45	· Offine	00.71722	ITEC	10.00.21.002
	Total 465 gravação(ões).		4 🖬 2 3	[4] [5] [34] [b]	Và para

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

6k

5k

4k

3k

2k

1k

0

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.

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

Visão dos detalhes do canal de vídeo.

Canal de vídeo	Canal de vídeo				
ð Alarme	Organização: root	Organização: root 🔹			
	Nome	Dispositivo	Organização	SN	Tipo de Camera
	VIP Intelbras	C 171 P 2	root		Cámera fixa
	CAM 1	2 PM P 21	root		Cámera fixa
	CAM 2	10 PM (P. 21	root		Cámera fixa
	CAM 3	10 PM (P. 21	root		Cámera fixa
	CAM 4	10 PM (P. 21	root		Cámera fixa
	CAM 5	10 PM (P 21	root		Câmera fixa
	CAM 6	10 PM (P. 21	root		Câmera fixa
	CAM 7	10 PM (P. 21	root		Câmera fixa
	CAM 8	10 PM (P. 21	root		Câmera fixa
	VIP 5550 Z IA	17 F.M. P. 27	root		Câmera fixa
	VIP Intelbras	8 P.M. P. 22	root		Câmera fixa
	IPC	17 F.M. P. 27	root		Câmera fixa
	CAM 1	8 P.M. P. 22	root		Cámera fixa
	IPC	2 PM P 22	root		Cámera fixa
	Total 28 gravação(ões).			< 1 2 F	Vā para 1

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:

- 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.
- 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:18	Configurações gerais do sistema
0	
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

intelbras.com.br



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:	Recibos de POS
180	
pos_receipt:RECEIPT_TIME:180	Detalhes de Recibo de POS
ac_door_access_record:SWIPE_TI	Registros de Controle de Acesso
ME:180	
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.

1^a 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
				Protocol
				0
Center	Defense_Web	O serviço de gerenciamento	HTTPS : 443	ТСР
Management		central gerencia os outros	HTTP : 80	
Service (CMS)		serviços e provê as portas de	CMS : 9000	
		acesso.	SHUTDOWN: 8005	
			REDIRECT : 9005	
Message Queue	Defense_MQ	O Serviço de Fila de Mensagens	61616	ТСР
Service (MQ)		transfere menssagens entre		
		serviços.		

Device	Defense_DMS	O Serviço de Gerenciamento de	9200	ТСР
Management		Dispositivos é responsável por		
Service (DMS)		registrar o codificador front-end,		
		receber o alarme, transferir o		
		alarme e enviar o comando de		
		tempo de sincronização.		
Media	Defense_MTS	O Serviço de Transmissão de	9100	ТСР
Transmission		Mídia consiste em obter o fluxo		
Service (MTS)		de áudio / vídeo do dispositivo		
		front-end e transferir esses		
		dados para o Serviço de		
		armazenamento Defense_SS,		
		plataforma client e		
		decodificador.		
Storage	Defense_SS	O Serviço de Armazenamento	9320	ТСР
Service (SS)		serve para armazenar, pesquisar		
		e reproduzir gravações.		
Video Matrix	Defense_VMS	O Serviço de Matriz de Vídeo	N/A	-
Service (VMS)		Wall serve para fazer login no		
		decodificador e enviar para o		
		decodificador as tarefas do		
		vídeo wall.		
Media Gateway	Defense_MGW	O Serviço de Gateway de Mídia	9090	ТСР
Service (MGW)		serve para fazer a ponte entre as		
		instâncias do serviço MTS e o		
		decodificador.		
Auto Register	Defense_ARS	O Serviço de Registro	9500	ТСР
Service (ARS)		Automático serve para escutar		
		os dispositivos que são		
		adicionados ao Defense via		
		auto-registro. Este serviço		

		executa o login e envia o fluxo de		
		dados para o serviço MTS.		
ProxyList	Defense_PCPS	O Serviço de Controle de Proxy	REGISTER : 9550	UDP/TCP
Control Proxy		serve para fazer login nos	SIP : 5060	
Service (PCPS)		dispositivos ONVIF S/G e em		
		seguida, obter o fluxo e		
		transferir os dados para o MTS.		
Alarm Dispatch	Defense_ADS	O Serviço de Despacho de	9600	ТСР
Service (ADS)		Alarme consiste em enviar		
		informações de alarme a		
		diferentes objetos de acordo		
		com os planos.		
Multi-Control	Defense_MCD	O serviço de Multi-Controle de	30001	ТСР
Device (MCD)		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.		
Power	Defense_PES	O Serviço é responsável pelo	9400	ТСР
Environment		monitoramento/acesso dos		
Server (PES)		dispositivos em ambiente		
		dinâmico.		
Switch Center	Defense_SC	O Serviço lida com os logins de	SIP : 5080	TCP/UDP
(SC)		SIP referentes as conexões de PC	RTP: 554	
		Clients e Aplicativos. O serviço		
		também é responsável por		

		encaminhar streams de		
		conversa/aúdio.		
Object Storage	Defense_OSS	O Serviço lida com o	HTTP : 9900	ТСР
Service (OSS)		armazenamento de snapshots	HTTPS : 9901	
		de face e imagens obtidas nos		
		eventos de alarme inteligente.		
Picture Transfer	Defense_PTS	O Serviço de Transferencia de	LISTEN : 9115	UDP/TCP
Service (PTS)		Fotos	PICTURE : 8081	
			RTP : 40000-	
			49999	
Radar	Defense_RADAR	Serviço de gerenciamento de	N/A	-
		radar.		
MCD-POS	Defense_MCDPOS	Serviço de gerenciamento de	8080	UDP/TCP
		PdV (POS). Esse serviço se		
		comunica com o serviço MCD.		
MCD-LED	Defense_MCDLed	Serviço de gerenciamento de	N/A	-
		painéis LED. Esse serviço se		
		comunica com o serviço MCD.		
MCD-Door	Defense_MCDDoor	Serviço de gerenciamento de	N/A	-
		Vídeo Porteiros/Controle de		
		Acesso. Esse serviço se		
		comunica com o serviço MCD.		
MCD-Alarms	Defense_MCDAlar	Serviço de gerenciamento de	N/A	-
	m	Painéis de Alarme. Esse serviço		
		se comunica com o serviço MCD.		
HRS	Defense_HRS	Serviço HRS.	N/A	-
Enhanced	Defense_EAS	Serviço de análise aprimorada	N/A	-
Analysis Service				
(EAS)				
MySQL	Defense_MySQL	Serviço referente ao banco de	3306	UDP/TCP
		dados do sistema. Necessário		

		para a maioria das operações do		
		sistema, armazenando principais		
		informações inseridas no		
		servidor.		
SOSO	Defense_SOSO	Serviço SOSO.	12366	UDP/TCP
Remote	Defense_REDIS	Base de dados REDIS.	6379	UDP/TCP
Dictionary				
Server (REDIS)				

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.

	Atualizar							×
		Dispositivo	e canal					2
			Tipo canal	Número de canais	Canais usados	Data de validade	Operação (canais)	
	Dispo	07	Video • Avallação	600	169	2020-12-10	- 0 +	namento
	Gerenciamento d conectados à pla adicionar, editar e		POS • Avaliação	20	1	2020-12-10	- 0 +	to armazenamento efina planos de ta de discos.
	dispositivos.		Controle de acesso • Avaliação	50	6	2020-12-10	- 0 +	
	Dispo	1 (1)	Video porteiro • Avaliação	20	1	2020-12-10	- 0 +	
		ł	Host alarm • Avaliação	200	200	2020-12-10	- 0 +	
	Visão Geral		LPR • Avaliação	50	3	2020-12-10	- 0 +	
	Status:		Reconhecimento f Avallação	100	9	2020-12-10	- 0 +	intelbras.com.br
	Dispositivo: Usuário:		Terminais de frequ • Avaliação	50	0	2020-12-10	- 0 +	1.R.20200807.1802367
	Serviço:	_						

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

Olá, syste



License.dat será enviado ao cliente, o qual deve ser importado no menu de importação de licença na página WEB do servidor.

DEFENSE IA Início +							Olá , syster
Dispositivo Oceneratives conectados à patatorna. Permé adicionar, estare executa dispositivos Dispositivo			mportar Atuatzação de licença:	Perquest Perquest Inguestar Cancelar	Correction de arracenamento de gravações: Delina planos de: gravações: de quota de discos. Armazonamento		
	Visão Geral			Licença		Suporte	
	Status:	Online	Offline	Versão de teste Detalhes da licença		Email: suporte defense@intelbras.com.br	
	Dispositivo:	18				Versão: V7.002.00(8006.1.R.20200807.1802367	
	Usuário:		9	Etapa 1. Exportar arguivo de solicitação d	ie licença.		
	Serviço:	-17		Etapa 3: Importe a licenca			
	HD:	-	79306/93096	and a second			

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

10 hierarquias, 999 organizações
por hierarquia
100
200 simultâneos, 2500 no total
2000 dispositivos
1000 dispositivos, 2000 canais
200 dispositivos, 800 canais
64 canais
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	200 IPs, 1024 Portas
Acesso	
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	
	400 M
Largura de banda da reprodução	SAGIM OUL
por servidor	200 TD
Capacidade maxima de	200 TB
	5
	5
Alarmo	100
Regras de alarmes	200
Mana	200
Hierarquia	8 hierarquias
Submapa	32 por hierarquia
Tamanho do mapa de bits	14.7 MB
Pontos por mapa (entrada de	Até 300 (GIS e Raster)
alarme da câmera e etc.)	
LPR	
Blacklist de veículos	100
Número de seções	100
Informações de registro	
Registros de alarme	5.000.000*
Registros de imagens de faces	5.000.000*
capturadas	
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	5.000.000*
pessoas	
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	5000 dispositivos, 20000 canais
totais	
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	600 IP, 3072 portas
Acesso	
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	120/s**
sem foto	
Eventos de Painel de Alarme	5/s**
Sistema em cascata	
Número de cascateamento	
Níveis de cascateamento	3
Número de servidores	20
cascateados	
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.

- 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.