

Guia modulo WEB Defense Middlewares e Centrais

Sumário

1	Introdução	3
2	Instalador	4
2.1	Configurações do MYSQL.....	4
2.2	Configurações da MQTT	6
2.3	Configurações do Defense	7
3	Licença.....	10
4	Interface web	12
4.1	Login	12
4.2	Bridge	13
4.3	Cadastro de centrais.....	17
4.3.1	Central de incêndio	17
4.3.2	Central de alarme	19
5	Configuração do Gateway (GW 521).....	21
6	Configuração da central de alarme.....	22
7	Criando um evento no Defense IA Client.....	24

1 Introdução

O módulo Defense Middlewares e Centrais integra com o Defense IA Client para recebimento de eventos das centrais de alarme e incêndio e oferece uma interface web intuitiva para adicionar, editar e excluir centrais, além de ativar bridges.

Neste guia, você encontrará instruções detalhadas sobre a instalação do módulo. Será um passo a passo para garantir que você possa instalar e configurar as informações de instalação com eficiência.

Ao longo deste manual, também abordaremos o procedimento para ativar uma Bridge, além de demonstrar como realizar as seguintes ações: adicionar, editar e excluir uma central de alarme e incêndio. Além disso, será explicada a configuração de zonas e partições de uma central de alarme, e como configurar um evento através do Defense IA Client.

2 Instalador

Nesta seção será abordada de forma clara quais são os passos para a instalação do módulo.

Requisitos:

- Ter um servidor com o Defense Server instalado
- 1 Licença de Bridge ativada no servidor

Para iniciar o processo de instalação, siga as etapas abaixo:

Passo 1: Acesso ao Instalador

Primeiro, navegue até a pasta onde você salvou o arquivo de instalação e encontre o arquivo chamado "instalador-licenca.exe".

Passo 2: Executar como Administrador

Clique com o botão direito do mouse no arquivo "instalador-licenca.exe" e escolha a opção "Executar como administrador". Isso é importante para garantir que a instalação seja feita com os privilégios necessários.

Passo 3: Menu de Opções

Após executar o arquivo como administrador, um menu será exibido, apresentando duas opções: "Instalador" e "Licença". O próximo passo depende das suas necessidades de licenciamento:

Passo 4: Escolher a Opção Certa

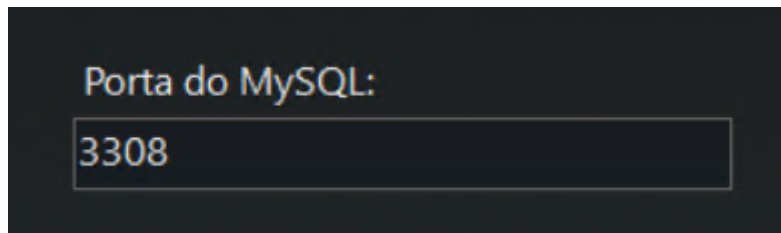
Instalação sem Licença Adicional (Até 5 Centrais): Se você planeja utilizar até 5 centrais, não é necessário gerar uma licença adicional. Nesse caso, clique na opção "Instalador" para prosseguir com a instalação do módulo.

Licenciamento para mais de 5 Centrais: Se você pretende utilizar mais de 5 centrais, será necessário gerar uma licença adicional. Para isso, clique na opção "Licença" e siga as instruções que estão descritas no sumário "3 Licença".

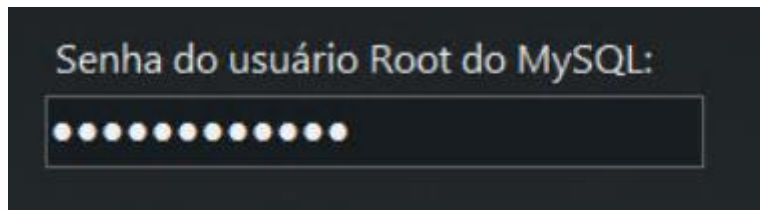
Passo 5: Realizar a instalação conforme as orientações abaixo:

2.1 Configurações do MYSQL

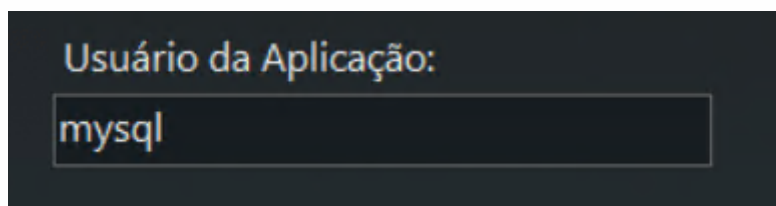
Porta do MYSQL: A porta MYSQL, pode ser escolhida e a mesma não poderá ser a mesma que a já utilizada no Defense. Aconselhamos usar o padrão já preenchido no instalador.



Senha do usuário ROOT do mysql: Esta senha é alterável conforme a necessidade do cliente, visando a privacidade. Aconselhamos usar o padrão já preenchido no instalador.



Usuário Aplicação: Identificador do usuário para o banco MYSQL. Aconselhamos usar o padrão já preenchido no instalador.



Porta Redis: Porta padrão banco de dados REDIS. Aconselhamos usar o padrão já preenchido no instalador.

Ao verificar se todos os dados estão preenchidos corretamente e ter a certeza de que não será necessário alterar nenhum dado, clique em **"próximo"**.

2.2 Configurações da MQTT

MQTT Port: Deve ser a mesma porta usada pelo Defense IA Server.

Service	Service Category	Port	Status	Exception Info	Operation
Defense_NGINX	Basic Service	HTTP:80 HTTPS:443(Login Port)	Running		
Defense_SMC	Basic Service	HTTP:8000 HTTPS:8443 CMS:9000 SHUTDOWN:8006 REDIRECT:9005 SUBCMS:9080	Running		
Defense_HRS	Basic Service	N/A	Running		
Defense_REDIS	Basic Service	6379	Running		
MySQL(Database)	Basic Service	3306	Running		
Defense_MQ	Basic Service	OPENWIRE:61616 MQTT:1883 AMQP:5672 STOMP:61613 JETTY:8161	Running		
Defense_CFGS	Basic Service	HTTP:19801 HTTPS:19443	Running		
Defense_ADS	Basic Service	9600	Running		
Defense_MTS	Basic Service	RTSP:9100 RTSPS:9102	Running		

Download Defense Client

2.3 Configurações do Defense

Defense IP: Endereço IP da máquina que o Defense está instalado. Sempre usar o IP de rede da máquina

Nome do usuário do Defense: Username do superadmin do Defense. Recomendamos usar o System

Senha do Defense: Senha do usuário digitado acima.

Defense HTTP Port: Deve ser utilizada a mesma porta do Defense IA Server.

Service	Service Category	Port	Status	Exception Info	Operation
Defense_NGINX	Basic Service	HTTP:80 HTTPS:443(Login Port)	Running		
Defense_SMC	Basic Service	HTTP:8000 HTTPS:8443 CMS:9000 SHUTDOWN:8006 REDIRECT:9005 SUBCMS:9080	Running		
Defense_HRS	Basic Service	N/A	Running		
Defense_REDIS	Basic Service	6379	Running		
MySQL(Database)	Basic Service	3306	Running		
Defense_MQ	Basic Service	OPENWIRE:61616 MQTT:1883 AMQP:5672 STOMP:61613 JETTY:8161	Running		
Defense_CFGS	Basic Service	HTTP:19801 HTTPS:19443	Running		
Defense_ADS	Basic Service	9600	Running		
Defense_MTS	Basic Service	RTSP:9100 RTSPS:9102	Running		

Porta do Bridge: Deve ser a mesma porta do Defense Server "Defense_SMC: HTTP"

Service	Service Category	Port	Status	Exception Info	Operation
Defense_NGINX	Basic Service	HTTP:80 HTTPS:443(Login Port)	Running		
Defense_SMC	Basic Service	HTTP:8000 HTTPS:8443 CMS:9000 SHUTDOWN:8006 REDIRECT:9005 SUBCMS:9080	Running		
Defense_HRS	Basic Service	N/A	Running		
Defense_REDIS	Basic Service	6379	Running		
MySQL(Database)	Basic Service	3306	Running		
Defense_MQ	Basic Service	OPENWIRE:61616 MQTT:1883 AMQP:5672 STOMP:61613 JETTY:8161	Running		
Defense_CFGS	Basic Service	HTTP:19801 HTTPS:19443	Running		
Defense_ADS	Basic Service	9600	Running		
Defense_MTS	Basic Service	RTSP:9100 RTSPS:9102	Running		

IP da aplicação: IP da máquina a qual está sendo instalado a aplicação. Para evitar problemas de firewall e/ou bloqueios deixar o padrão já preenchido

IP da Aplicação:

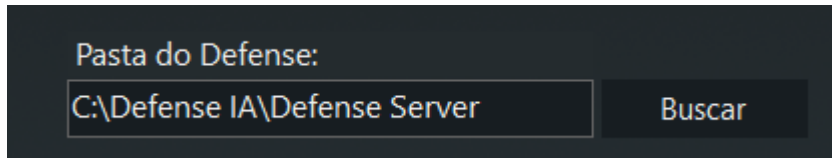
Porta da aplicação: Porta do serviço back-end. Aconselhamos usar o padrão já preenchido no instalador.

Porta da Aplicação:

Porta do Webhook: Porta do serviço webhook. Aconselhamos usar o padrão já preenchido no instalador.

Porta do Webhook:

Pasta do Defense Server: Pasta onde o Defense Server está localizado



Pasta do Defense:

C:\Defense IA\Defense Server

Buscar

Ao terminar de verificar se todos os dados estão digitados e em seus devidos locais, clique em "instalar".

Ao final da instalação você será reencaminhado para a tela inicial.

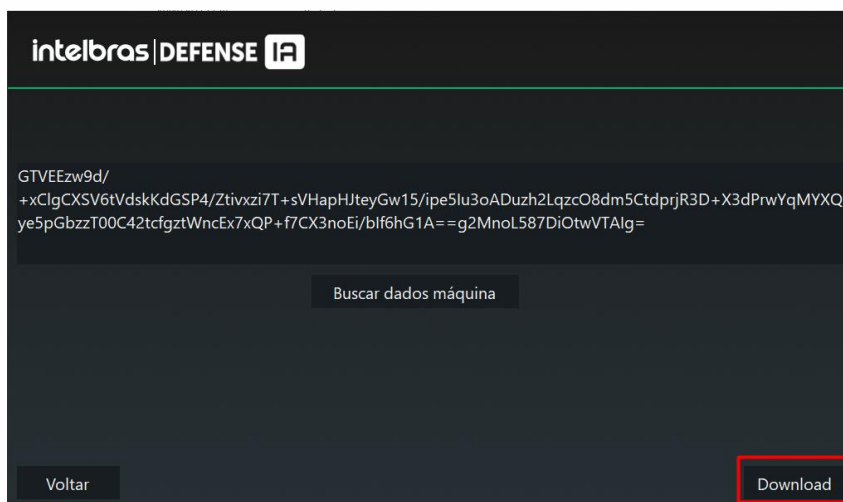
3 Licença

Este menu "Licença" deve ser acessado quando você pretende adicionar mais de 5 centrais ao software. Cada central requer uma licença dedicada, e essas licenças precisam ser adquiridas previamente por meio da equipe de vendas. Para adquirir as licenças necessárias, entre em contato com seu representante.

Após adquirir as licenças, siga o passo a passo abaixo para concluir o processo de adição de ativação da licença:

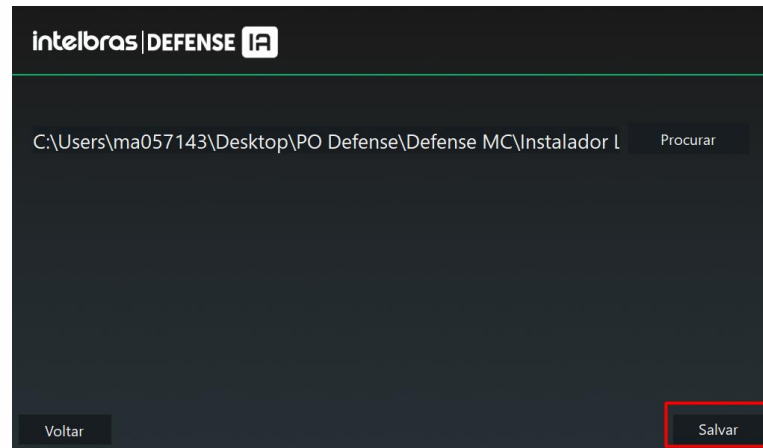
Passo 1: Buscar dados da máquina

Clique no botão "Buscar dados da máquina" momentos após a busca de dados estará completa, clique no botão "download" salve o arquivo "frist.key" e envie para a o representante comercial.



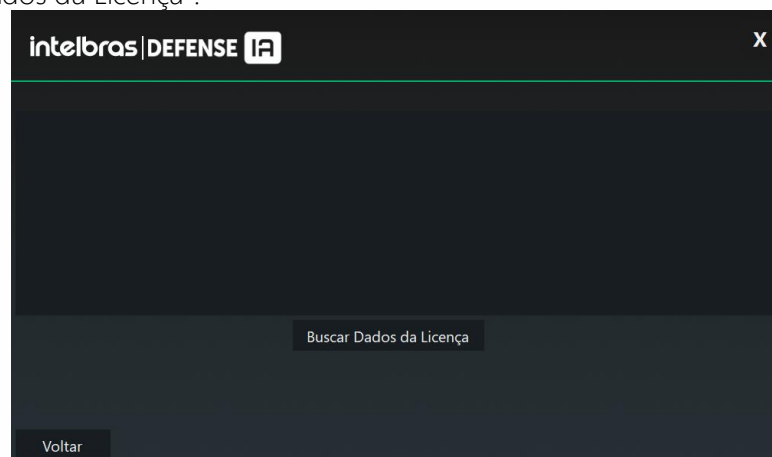
Passo 2: Registrar Licença

A Intelbras irá enviar o arquivo "license.bin" essa licença irá conter a quantidade de dispositivos que você adquiriu. Coloque o arquivo nesse campo e clique em "salvar" para registrar a licença.



Passo 3: Consultar Licença

Nesse menu você conseguirá consultar quantas licenças estão ativas, no botão "Buscar Dados da Licença".

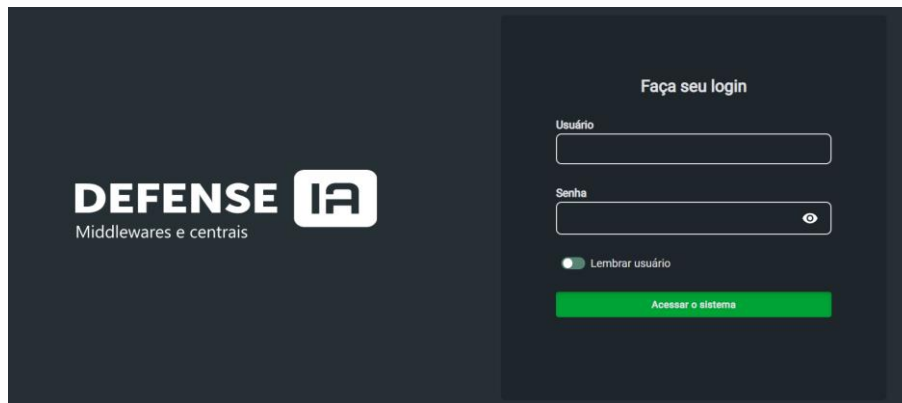


4 Interface web

Nesta seção será apresentado a interface web do módulo e instruções de como realizar as ações necessárias para o funcionamento.

4.1 Login

Interface de login



Para realizar login no módulo o usuário deve acessar a url: **IpServidor:3001**.

IpServidor: Ip em que o servidor do Defense está instalado.

Porta padrão: 3001.


informar o usuário e a senha.

Usuário padrão **system**, senha padrão **mesma senha do Defense IA**

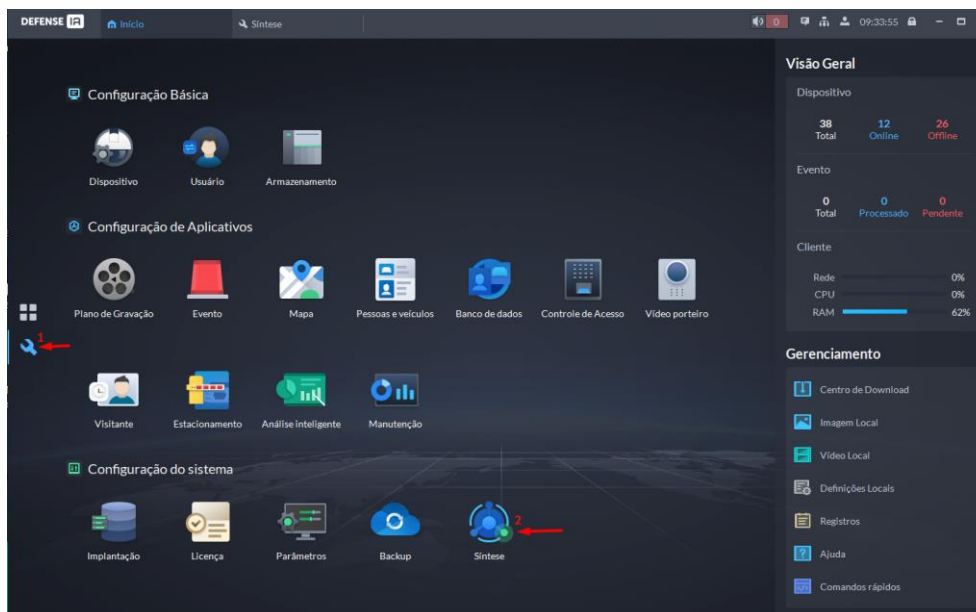
4.2 Bridge

Após realizar o login o usuário deverá ativar o bridge para garantir a integração com o Defense IA Client. Para ativar siga os passos a seguir:

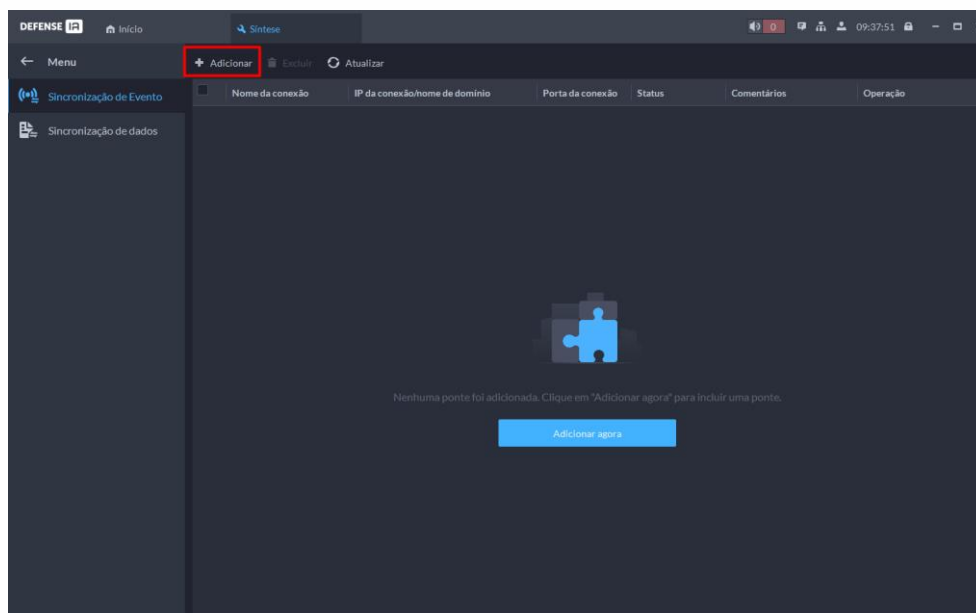
a) Acessando Síntese no Defense IA Client

Acesse o client do Defense IA clique na engrenagem “”, acesse o menu “**Síntese**” e clique em “**+ Adicionar**” no canto superior esquerdo da tela.

Acessando “” e “**Síntese**”



Acessando “**+ Adicionar**”



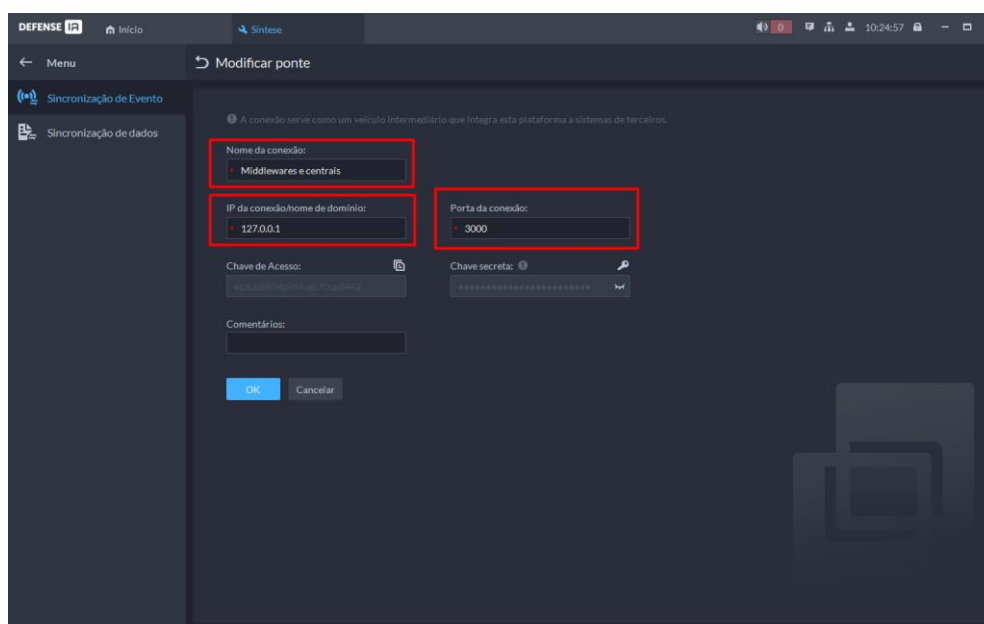
b) Adicionando Bridge no Defense IA

Defina o nome, IP e porta do Bridge.

Nome da conexão: Escolha um nome para o seu Bridge, que seja significativo e facilite sua identificação. O nome pode ser personalizado de acordo com a sua preferência e necessidade.

IP da conexão: certifique-se de colocar o IP em que o módulo web foi instalado.

Porta da conexão: certifique-se de configurar a mesma porta em que o módulo foi instalado.

Exemplo de um Bridge

A captura de tela mostra a interface de usuário do sistema de configuração de uma ponte (bridge) no Defense IA. O formulário "Modificar ponte" contém os seguintes campos:

- Nome da conexão:** Middlewares e centrais
- IP da conexão/home de domínio:** 127.0.0.1
- Porta da conexão:** 3000
- Chave de Acesso:** [campo oculto]
- Chave secreta:** [campo oculto]
- Comentários:** [campo oculto]

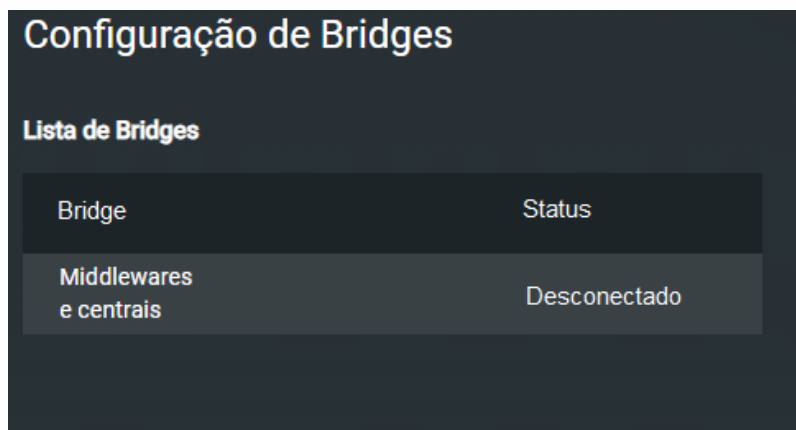
Os campos "Nome da conexão", "IP da conexão/home de domínio" e "Porta da conexão" estão destacados com retângulos vermelhos. O formulário também possui botões "OK" e "Cancelar" na base.

Após realizar os passos acima clique em "OK" para adicionar o Bridge.

c) Ativando o Bridge no módulo WEB Defense Middlewares e Centrais

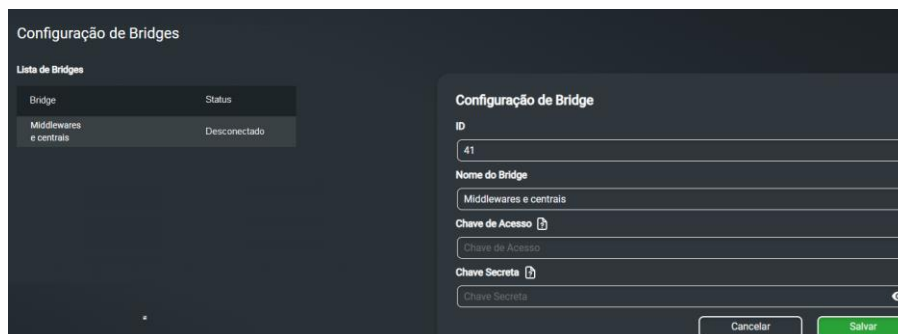
Para ativar o Bridge que foi adicionado no passo “b” você deve acessar o módulo WEB, acessar o menu “Bridges”. Os bridges que foram adicionados no Client, estarão listados nesse menu.

Lista dos Bridges adicionados





Clique na linha do Bridge para adicionar a chave de acesso e a chave secreta.

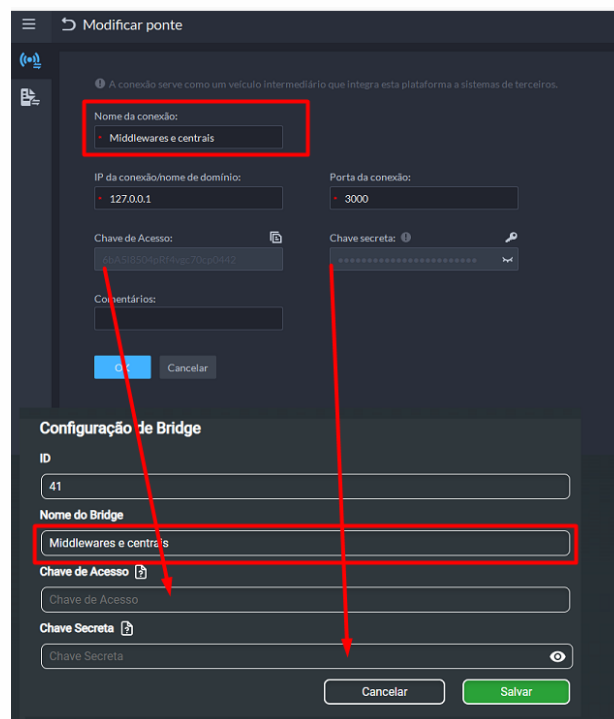
Adicionando a chave de acesso e a chave secreta



Para adicionar as chaves siga os passos abaixo:

- I. Logue no Defense IA Client
- II. Clique em 
- III. Entre no menu "Síntese"
- IV. Clique no botão 
- V. Copie o a chave de acesso e a chave secreta no client e cole na interface web. Certifique-se de que você está copiando as chaves certas, e de que é o mesmo Bridge.

Copiando e colando as chaves



VI. Após copiar as chaves e colar, clique em salvar.

Salvar as alterações

VII. Aparecerá uma mensagem de sucesso na tela e seu Bridge foi ativado.

VIII. Certifique-se de que o status atualize para “conectado”

4.3 Cadastro de centrais

4.3.1 Central de incêndio

Cadastro de centrais de Incêndio

Para realizar o cadastro de uma nova central de incêndio, é fundamental fornecer algumas informações. Ao adicionar uma central ao sistema, o usuário deve preencher os seguintes campos obrigatórios:

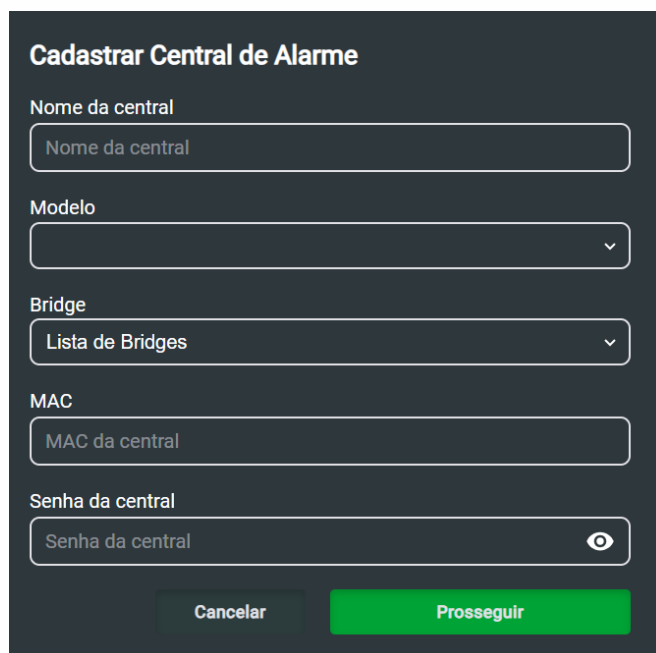
Modelo da Central de Incêndio: Indique o modelo específico da central de incêndio que será cadastrada.

Bridge de Conexão: Selecione o bridge no qual a central de incêndio será adicionada. O bridge é responsável por permitir a conexão e comunicação entre os dispositivos e o Defense IA, garantindo uma integração eficiente.

Endereço MAC Gateway: Informe o endereço MAC do Gateway GW521, que é o dispositivo que possibilita a conexão da central com o Defense. O MAC é um identificador único atribuído a cada dispositivo de rede, permitindo sua identificação no sistema.

4.3.2 Central de alarme

Cadastro de centrais de alarme



O formulário, intitulado "Cadastrar Central de Alarme", possui um fundo escuro e campos de entrada em tons mais claros. Os campos são: "Nome da central" (campo de texto), "Modelo" (menu suspenso), "Bridge" (menu suspenso com a opção "Lista de Bridges" visível), "MAC" (campo de texto) e "Senha da central" (campo de texto com ícone de olho para alternar visibilidade). Na base do formulário, há dois botões: "Cancelar" em cinza e "Prosseguir" em verde.

Para realizar o cadastro de uma nova central de alarme, é fundamental fornecer algumas informações. Ao adicionar uma central ao sistema, o usuário deve preencher os seguintes campos obrigatórios:

Modelo da Central de Alarme: Indique o modelo específico da central de incêndio que será cadastrada. Essa informação é importante para identificar o tipo de dispositivo e suas características.

Bridge de Conexão: Selecione o bridge no qual a central de incêndio será adicionada. O bridge é responsável por permitir a conexão e comunicação entre os dispositivos e o Defense IA, garantindo uma integração eficiente.

Endereço MAC: Informe o endereço MAC da central de alarme. O MAC é um identificador único atribuído a cada dispositivo de rede, permitindo sua identificação no sistema.

Senha da central: O campo senha é referente a senha de "acesso remoto" da central.

Para finalizar o cadastro da central de alarme é necessário cadastrar as zonas que estão relacionadas a elas

Cadastro dos nomes das zonas e seus respectivos IDS.

Cadastro do nome e ID das zonas

Cadastrar Central de Alarme

Ativar partições da central

Zonas da central

Nome da Zona Id da Zona +

Voltar Salvar

5 Configuração do Gateway (GW 521)

Para recebimento de eventos da Central de Incêndio no Defense IA deve ser configurado o Gateway de integração com a central de incêndio GW 521 no Programador CIE.

Siga os passos abaixo:

1. Certifique-se de que o Programador CIE esteja instalado na sua última versão.
2. Conecte via cabo USB no GW 521
3. Clique no menu **"Sistema"**
4. Clique no menu **"Configurações"**
5. Habilite a função **"Webhook"**.
6. Configure no campo **"Endereço do Webhook"** a seguinte rota:
IpServidor/api/gw521/events. Aonde IpServidor é o ip do servidor em que o plug-in foi instalado.
7. Configure no campo **"Porta"** o valor **6000**.

Segue print abaixo da configuração.

Programador CIE "Sistema" → "Configurações"

Configurações

Modo: Integração desabilitada
 Modbus TCP
 Situador
 Webhook

Endereço do Webhook:
Campo obrigatório 27 / 100
Porta:

Autenticação: HMAC HTTPS

Chave privada:
0 / 88 ?

Intervalo Heartbeat: (min:seg) ?
Intervalo entre eventos: (ms)
Código do Equipamento: (opcional)

6 Configuração da central de alarme

Para recebimento de eventos da central de alarme no Defense IA deve ser realizada as configurações de conexão da central no AMT Remoto.

Siga os passos abaixo:

1. Certifique-se de que o AMT Remoto esteja instalado na última versão
2. Conecte na central.
3. No menu "Monitoramento IP" aponte a central para o IP do servidor na porta 9009. Pode ser utilizado a função duplo IP ou regular IP. Certifique-se de habilitar a função "Habilitar transmissão de eventos".

Menu Monitoramento IP

4. No menu "Comunicação" certifique-se de habilitar a função "reportagem em tempo real", setar o "Modo de reportagem" em "Regular IP/Telefone" ou "duplo IP" de acordo com a aplicação.

Menu Comunicação

intelbras

AMT 4010 MAC 0030
AMT 4010 Smart

Online

Configurações

Geral

Usuários

Setores

Comunicação

PGM

Mensagem

Monitoramento IP

Ethernet

GPRS

Temporizações

Dispositivos sem fio

Código de Evento Programável

Eventos

Sair

Central Online: Desconectar

Salvar Salvar e enviar

Comunicação

GERAL
ACESSO REMOTO
TELEFONES
CONTAS MONITORAMENTO
TESTE PERIÓDICO

Reportagem em tempo real

Reportar tensão da bateria

Não reportar falha ao comunicar evento

Não reportar senha incorreta

Amplitude do sinal DTMF enviado

Número de tentativas de discagem

Tempo para reportar falha de AC

Modo de reportagem Regular IP/telefone ▾

Protocolo monitoramento #1 Contact ID ▾

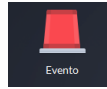
Protocolo monitoramento #2 Contact ID ▾

7 Criando um evento no Defense IA Client

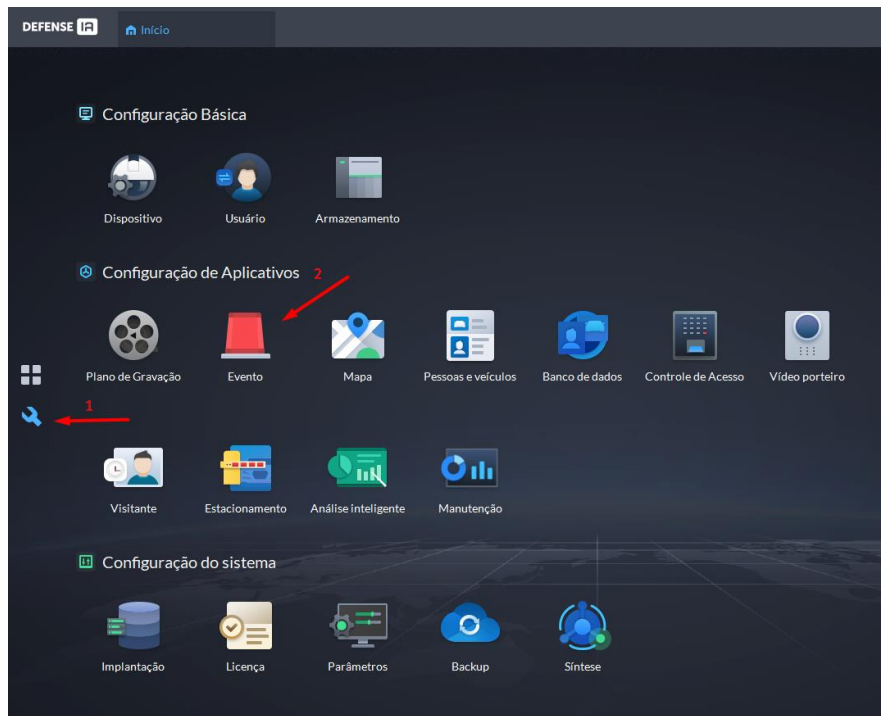
Para criar um novo evento acesse o Client e siga os passos a seguir:

I. Logue no Defense IA Client

II. Clique em  e logo após abra

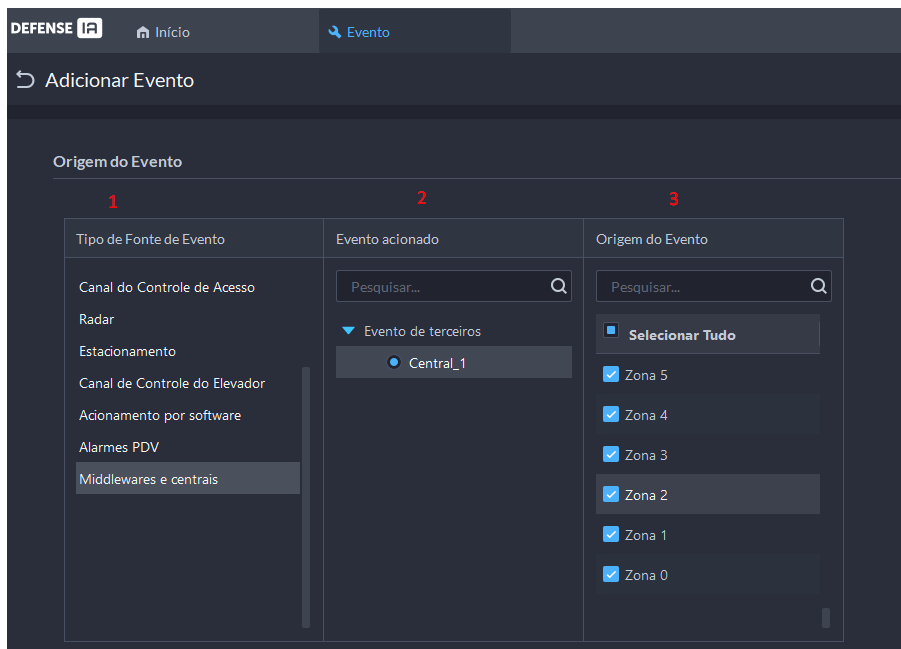


Acessando aba "Evento"



- III. Clique em **+ Adicionar**, em seguida selecione o nome do Bridge na coluna “Tipo de fonte de Evento”, após selecione o nome da central na coluna “Evento acionado”, e por fim selecione as zonas na coluna “Origem do Evento”.

Criando evento



Eventos criados

