

intelbras

Middleware de Centrais

Manual de instalação e configuração

Defense IA 3.2

Sumário

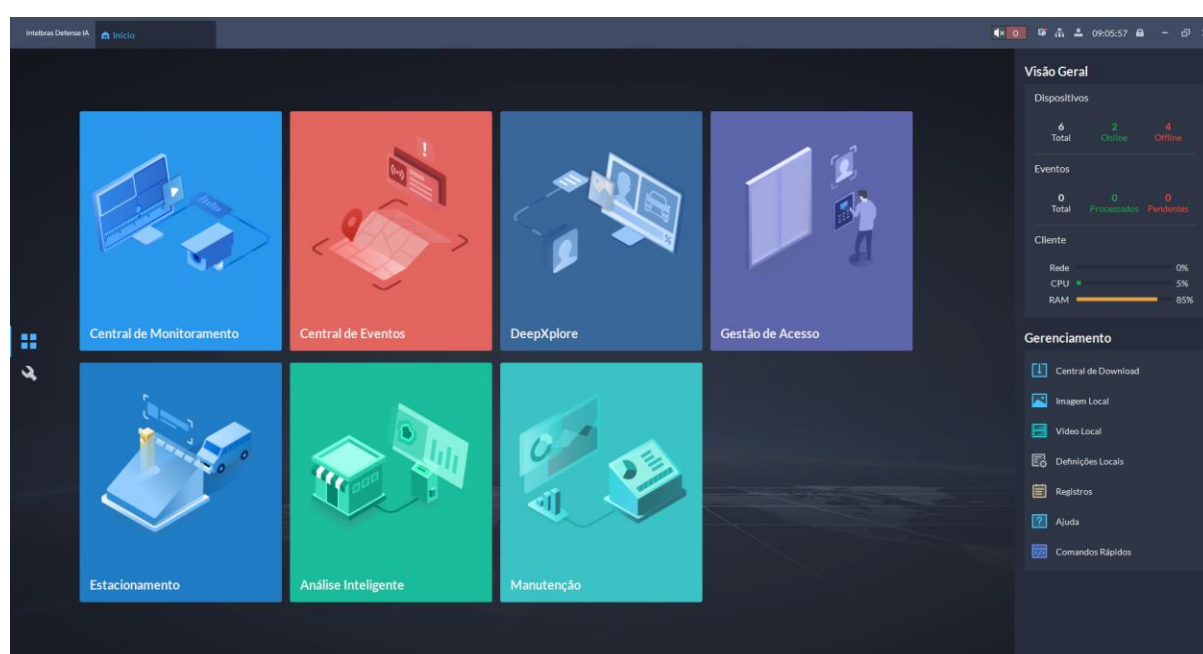
1. Defesa IA	3
2. Instalação do Middleware de Centrais	3
3. Como verificar as portas do firewall	8
4. Como realizar o primeiro acesso.....	11
5. Centrais de Alarme.....	12
5.1. Configuração prévia de uma central de alarme.....	13
5.2. Como adicionar uma central de alarme através do Web Client	17
5.3. Como sincronizar uma central de alarmes	22
5.4. Configurando partições e zonas via Web Client	24
5.5. Como operar uma central de alarme.....	27
5.6. Anulação de Zona (Bypass)	30
5.7. Como configurar e visualizar os eventos das centrais	32
6. Centrais de Incêndio	34
6.1. Configuração prévia de uma central de incêndio	34
6.2. Como adicionar uma central de incêndio através do Web Client	38
6.3. Como configurar e visualizar os eventos das centrais de incêndio	41

1. Defense IA

O Defense IA tem como foco gerir a inteligência artificial dos equipamentos e realizar o videomonitoramento do sistema de forma ágil. Monitore toda a solução em um único software, compatível com CFTV, controle de acesso, detectores de metais, vídeo wall, protocolo Onvif e centrais de alarmes e incêndio.

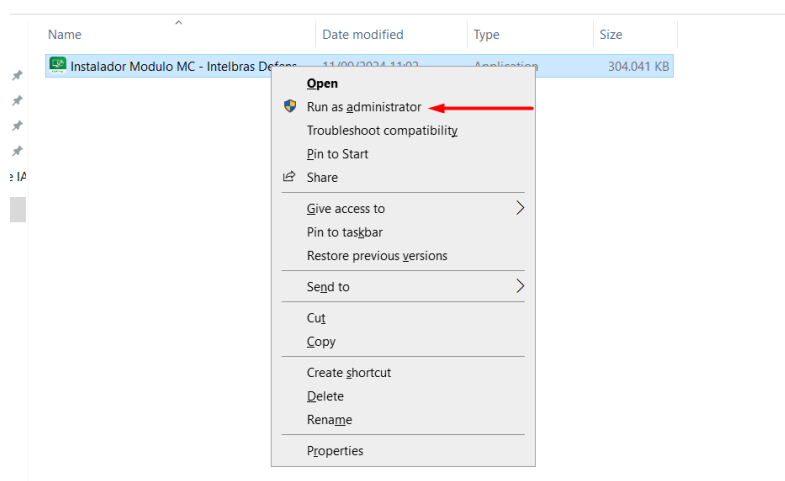
Tenha informações em tempo real sobre a saúde do sistema e monitore os principais eventos por meio de dashboards, tornando o monitoramento mais eficiente. Crie e acompanhe casos e operações a partir de imagens e gravações com registros de incidentes, gerando relatórios com informações detalhadas das ocorrências.

Interligue os sistemas da matriz, filiais e outras plantas de uma empresa, proporcionando uma gestão unificada e inteligente do monitoramento.



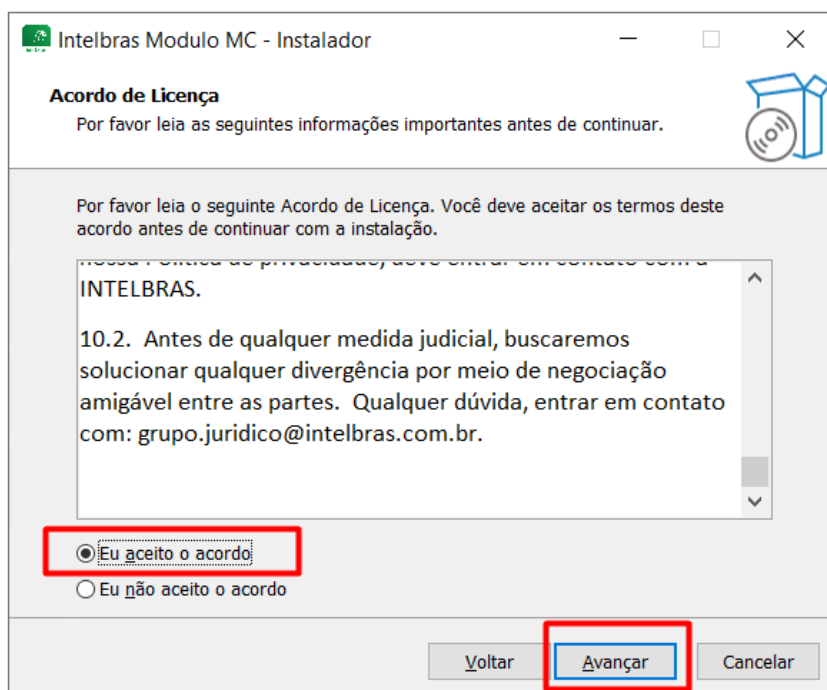
2. Instalação do Middleware de Centrais

Após realizar o download, clique no instalador com o botão direito e o **execute como administrador**.

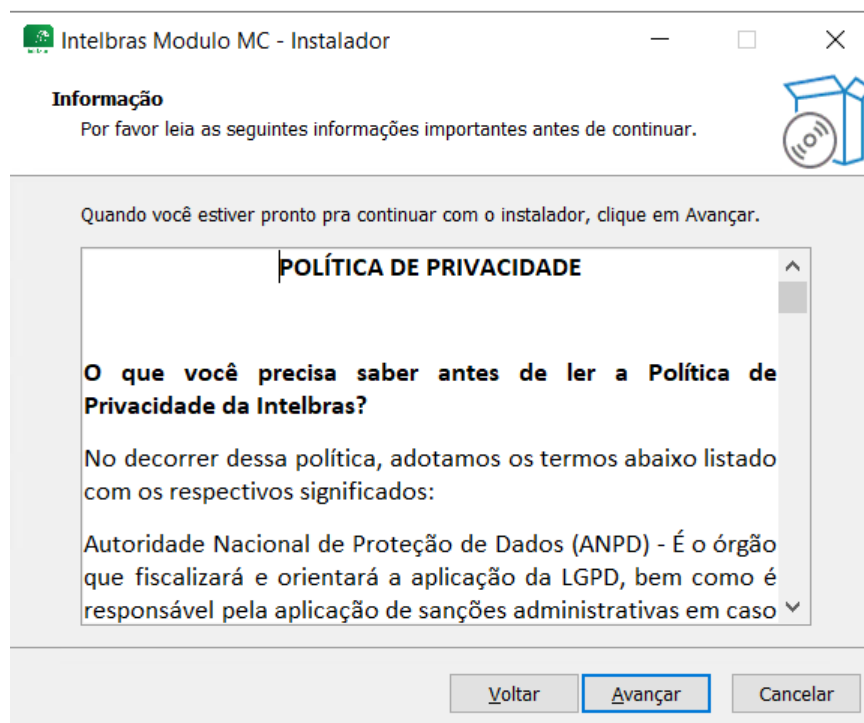


Configurando o instalador:

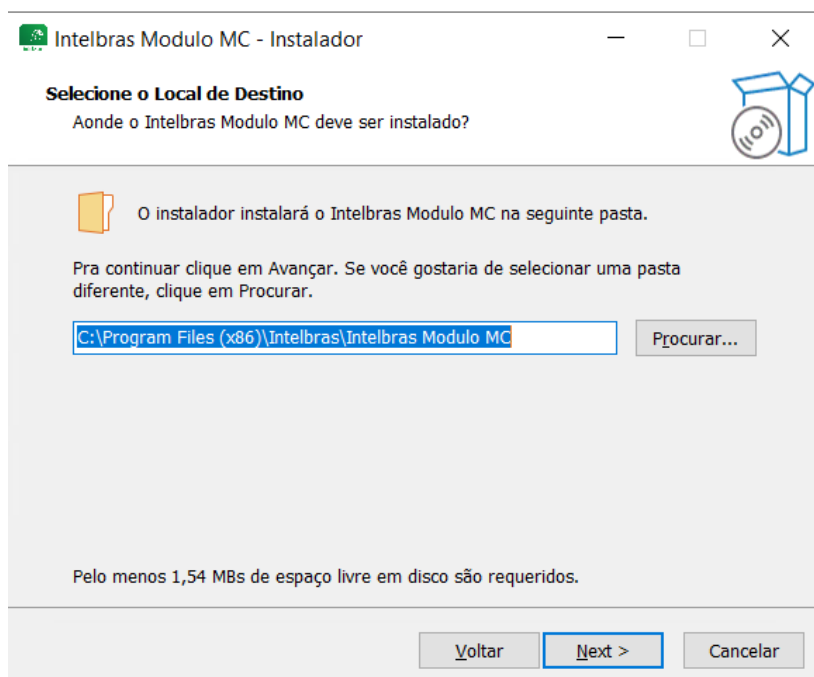
Após executar o instalador como administrador, abrirá uma página do instalador, clique em avançar e aceite os termos clicando em “Eu aceito o acordo”. Em seguida clique em avançar.



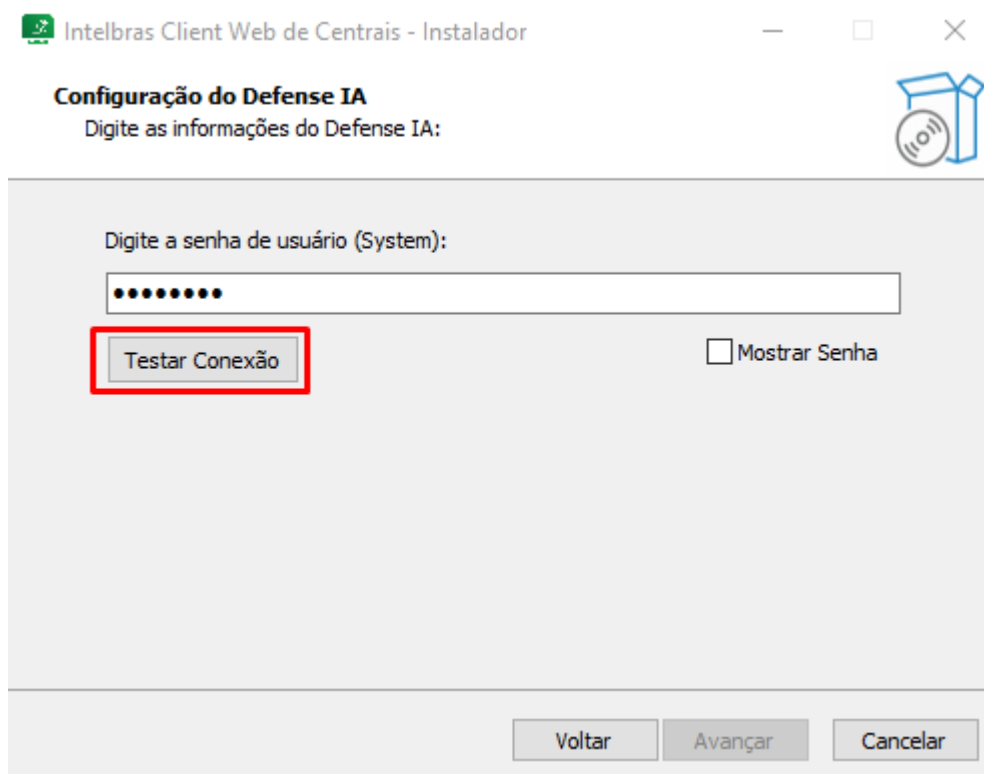
Clique em avançar novamente.



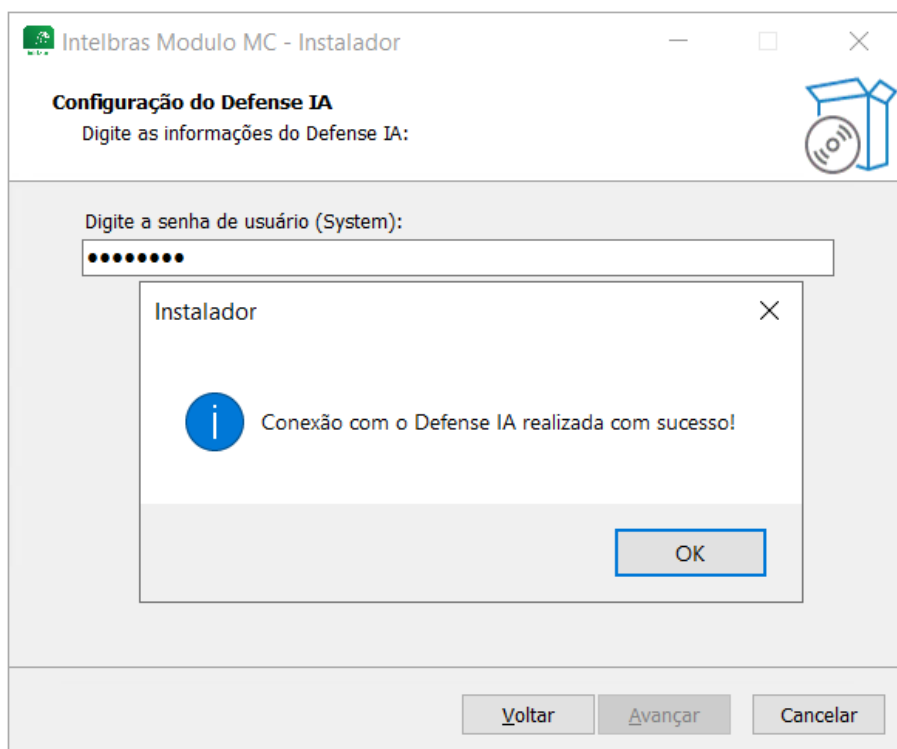
Agora escolha a pasta de instalação e avance novamente



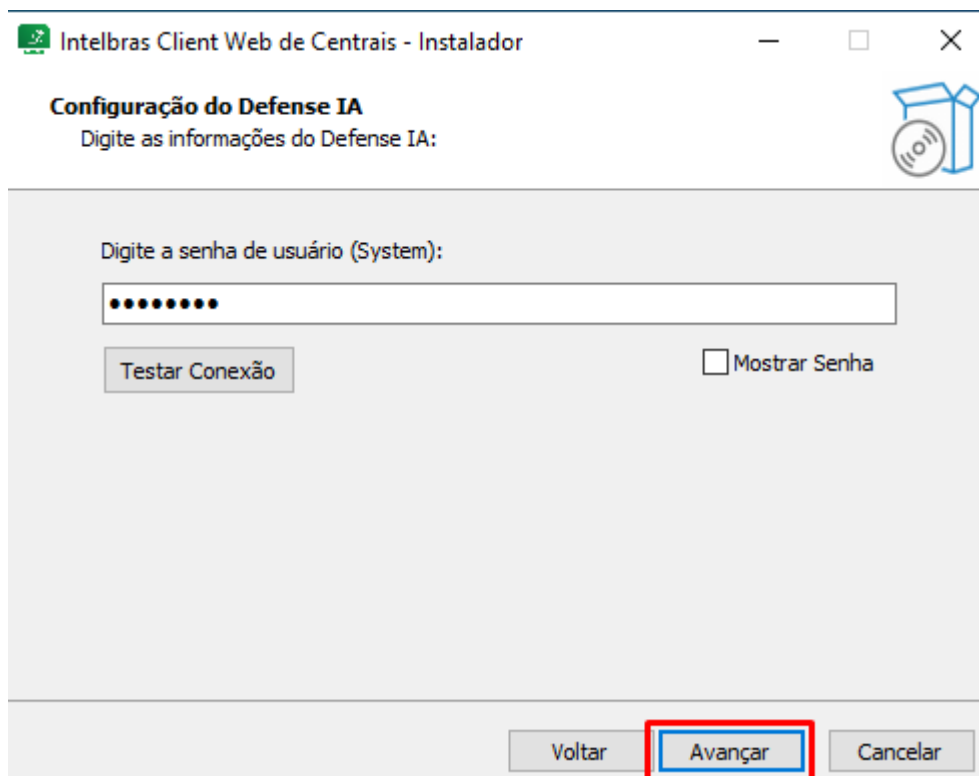
Digite a senha na qual você escolheu na instalação do Defense IA e clique em Testar Conexão.



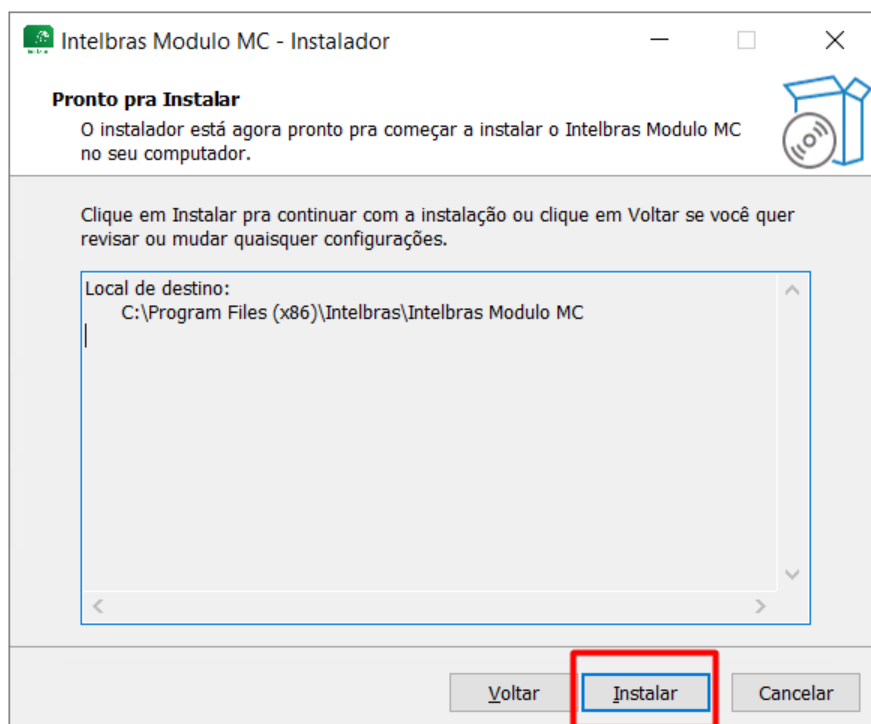
Validado, clique em ok.



Clique em avançar.



Clique em instalar.

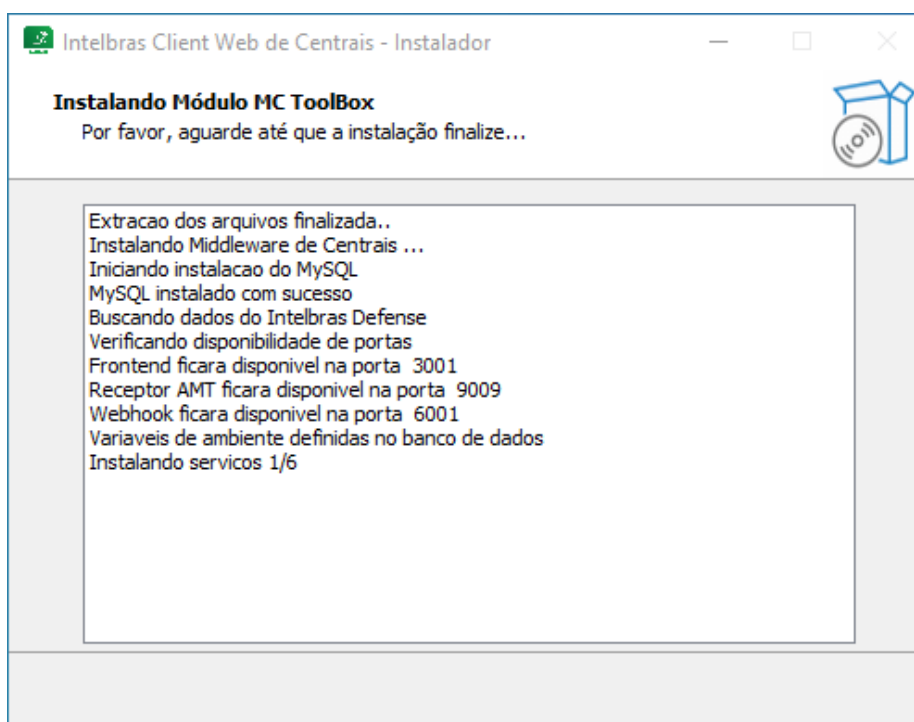


Note que durante a instalação será exibida quais portas de serviço foram escolhidas pelo sistema.

Porta frontend: Utilizada para realizar o acesso ao Client Web através de um navegador (padrão 3001)

Porta Receptor AMT: Porta utilizada para recebimento de eventos das centrais de alarme (padrão 9009)

Porta Webhook: Porta utilizada para recebimento de eventos das centrais de incêndio (padrão 6001)



Após instalar com sucesso, clique em Concluir e o seu módulo já está pronto para uso.

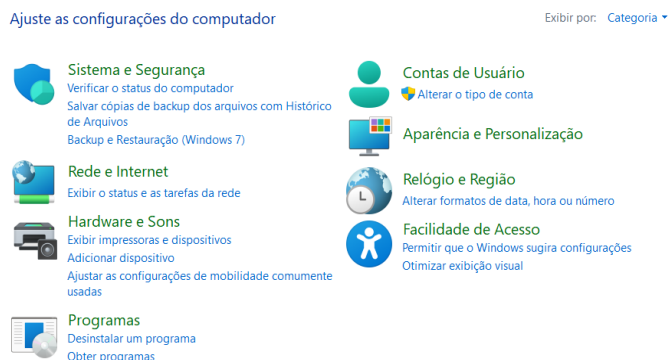


3. Como verificar as portas do firewall

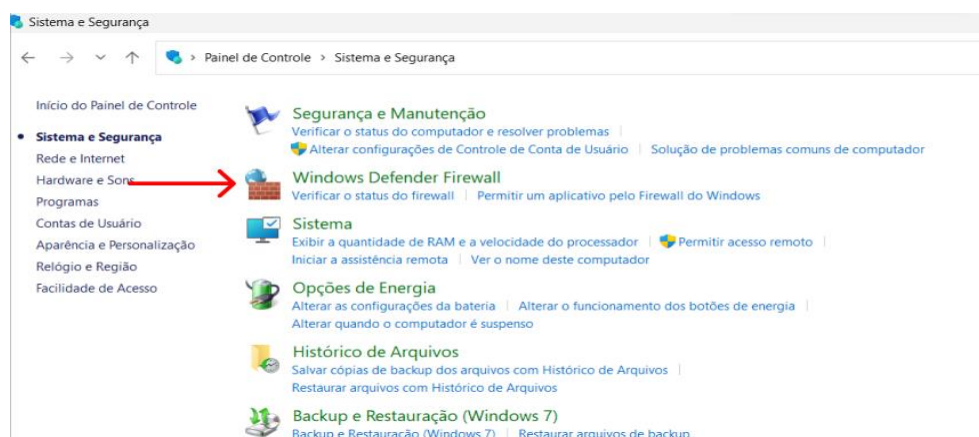
Durante a instalação, o próprio sistema faz a liberação das portas conforme necessário. Como boa prática, recomenda-se verificar se estas portas foram de fato liberadas no firewall. Para isto, acesse o painel de controle do seu computador.



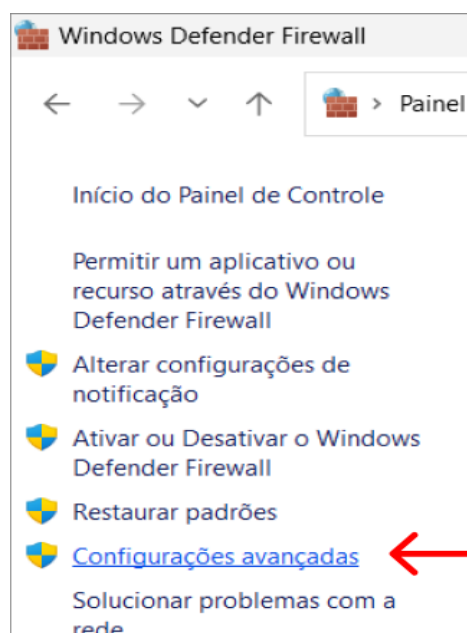
Acesse “**Sistema e Segurança**”.



Clique em “**Windows Defender Firewall**”.



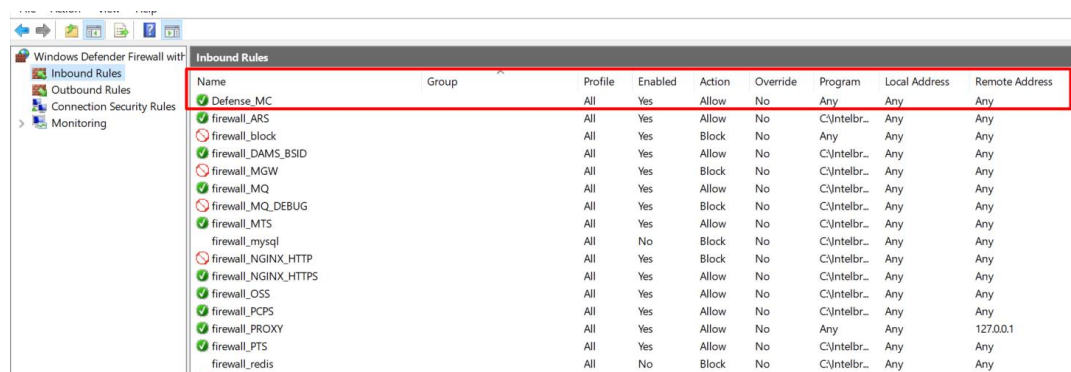
Clique em “**Configurações Avançadas**”.



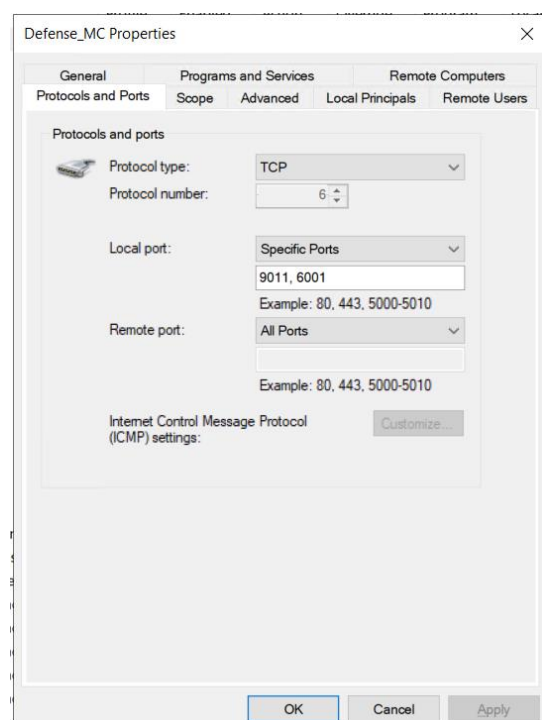
Clique em “Regra de entrada”.



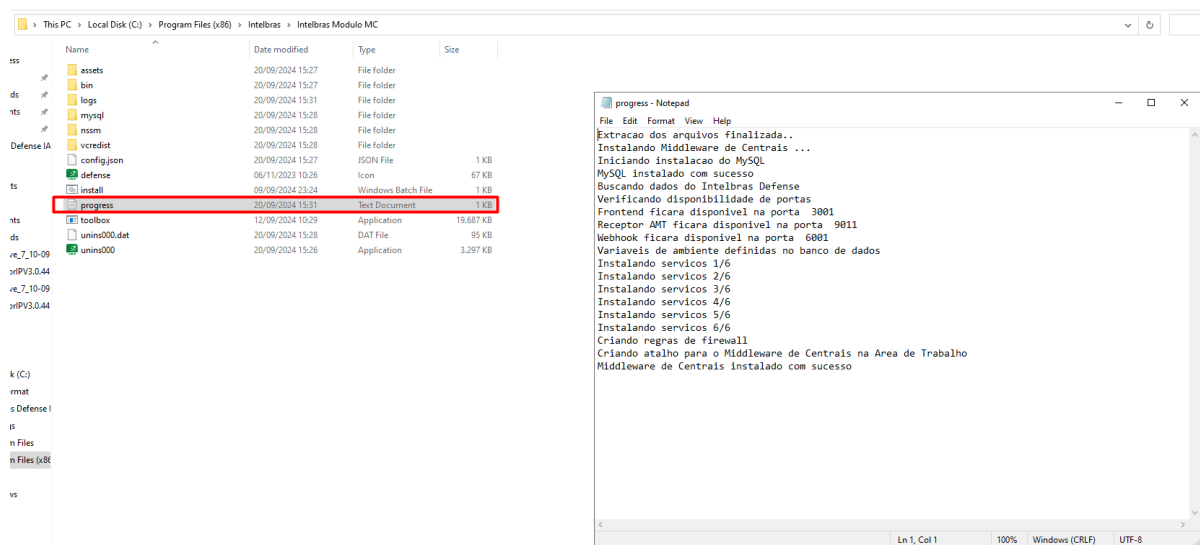
Agora verifique se foi criada a regra “Defense_MC”.



Clique duas vezes na regra e acesse o menu superior nomeado “Protocolos and Portas”. Verifique se as portas liberadas dentro da regra correspondem as portas escolhidas durante a instalação.



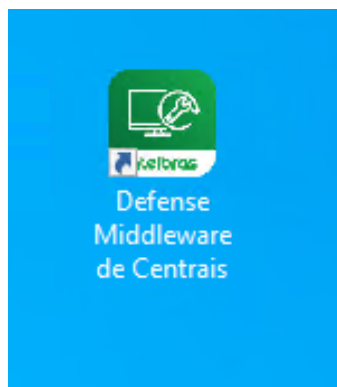
Caso não seja anotado quais portas foram escolhidas durante a instalação. É possível fazer a verificação em outro momento, acessando o arquivo **progress.txt** dentro do caminho onde foi instalado o middleware de centrais.



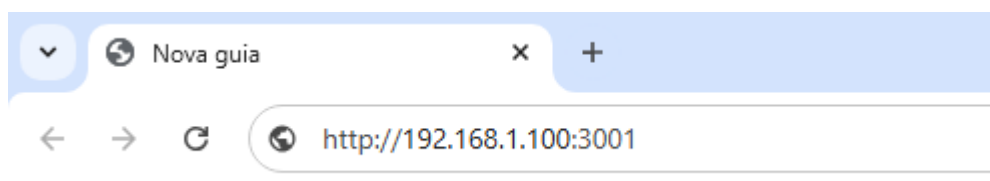
4. Como realizar o primeiro acesso

Para realizar o primeiro acesso, caso esteja na máquina onde o sistema foi instalado, basta clicar no ícone criado na sua área de trabalho ou acessar via navegador <http://localhost:3001/login>.

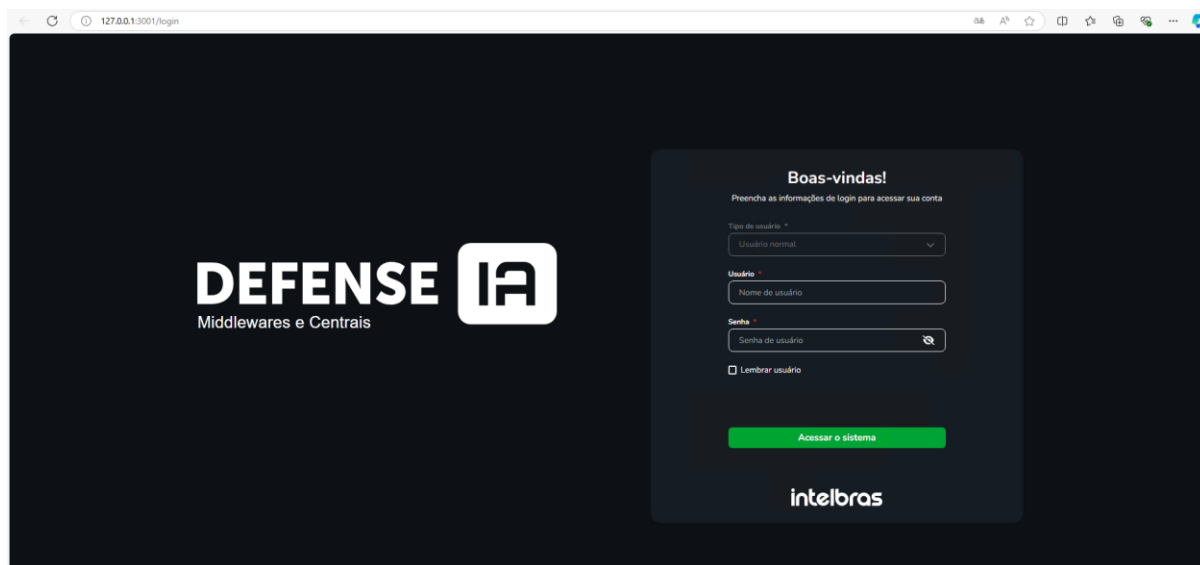
Atenção: Verifique se 3001 é realmente a porta de frontend. Caso seja um número diferente, insira o valor corretor no lugar de 3001.



Caso esteja acessando o sistema de outra máquina, acesse via navegador, inserindo o IP do servidor onde o middleware foi instalado. Ex: Middleware e Defense IA instalados em servidor de IP 192.168.1.100. Nesse caso acesse via navegador utilizando o link <http://192.168.1.100:3001>.



Após acessar você será redirecionado para a página inicial do Web Client e poderá realizar seu login com as credenciais do Defense IA. O Middleware de Centrais permite o acesso de qualquer usuário Admin ou Super Admin existente no Defense IA.



5. Centrais de Alarme

O Middleware de Centrais permite comunicação com as centrais de Alarme Intelbras modelos AMT 1000 SMART, AMT 1016 NET, AMT 2018 E SMART, AMT 2018 E/EG, AMT 4010 SMART e AMT 8000.

As funcionalidades disponíveis são: Adicionar e visualizar status das centrais (online/offline), configuração de partições e zonas, operação da central (arme/desarme e bypass) e recebimento de eventos no Defense IA.



Figura 1. AMT 4010 SMART

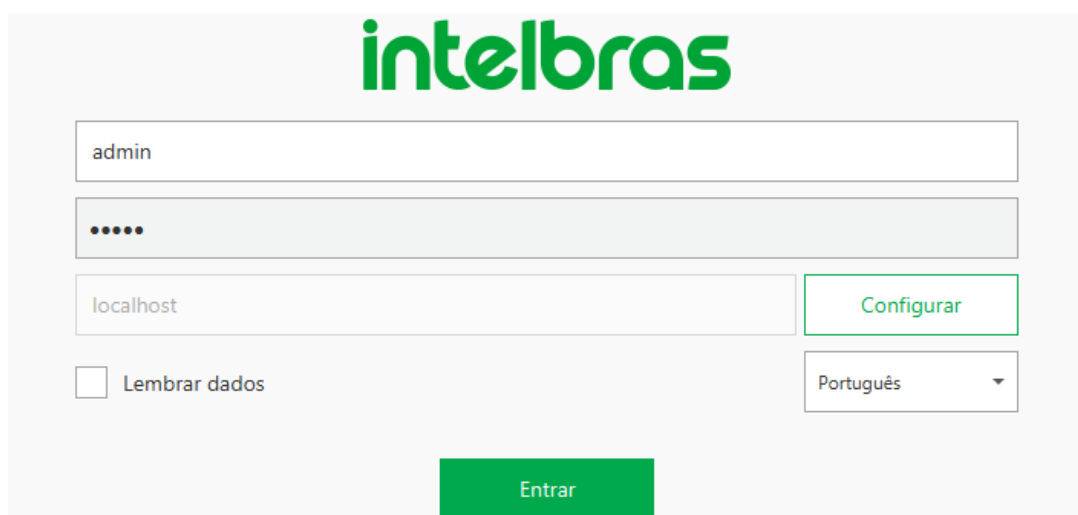
5.1. Configuração prévia de uma central de alarme

Para correta comunicação da central de alarme Intelbras com o Defense IA, é necessário que se faça certas configurações na central de alarme. Estas configurações podem ser feitas tanto via teclado quando via algum software programador. Será explicado como realizar estas configurações utilizando o software Intelbras AMT Remoto. Certifique-se que o seu computador está na mesma rede que as centrais de alarme, dessa forma será possível configura-las utilizando o software Intelbras AMT Remoto. Caso o computador não esteja na mesma rede, é possível conectar na central através do MAC Address via Intelbras Cloud. **O software está disponível no site da Intelbras.**

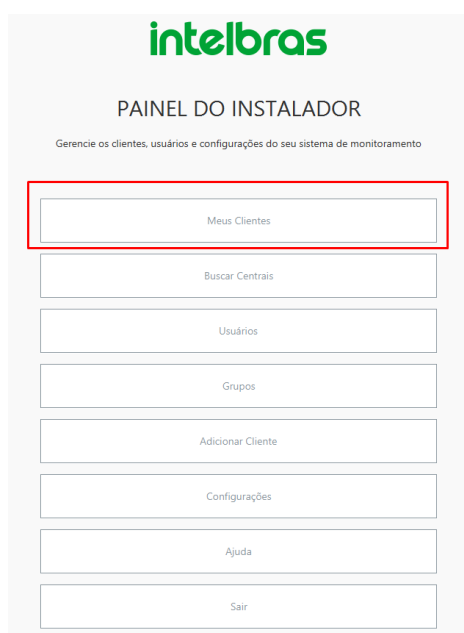
Após instalar e abrir o software, a tela de login será exibida, na qual é possível acessar com a credencial padrão.

Usuário: admin

Senha: admin



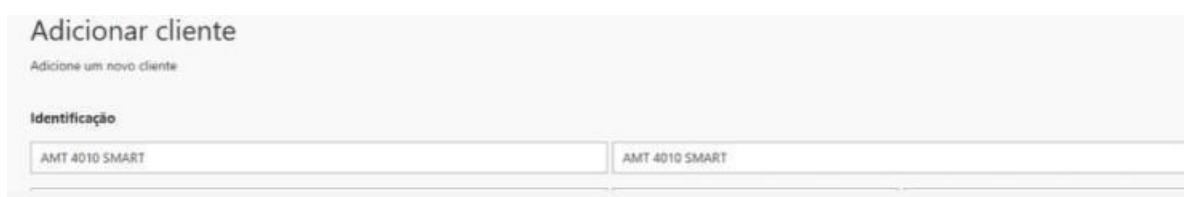
No Painel do Instalador, clique em “Meus Clientes”:



Após abrir o menu central de meus clientes **clique em “Adicionar cliente”**:



Abrindo a página de clientes, o primeiro passo será **identificar a sua central**:

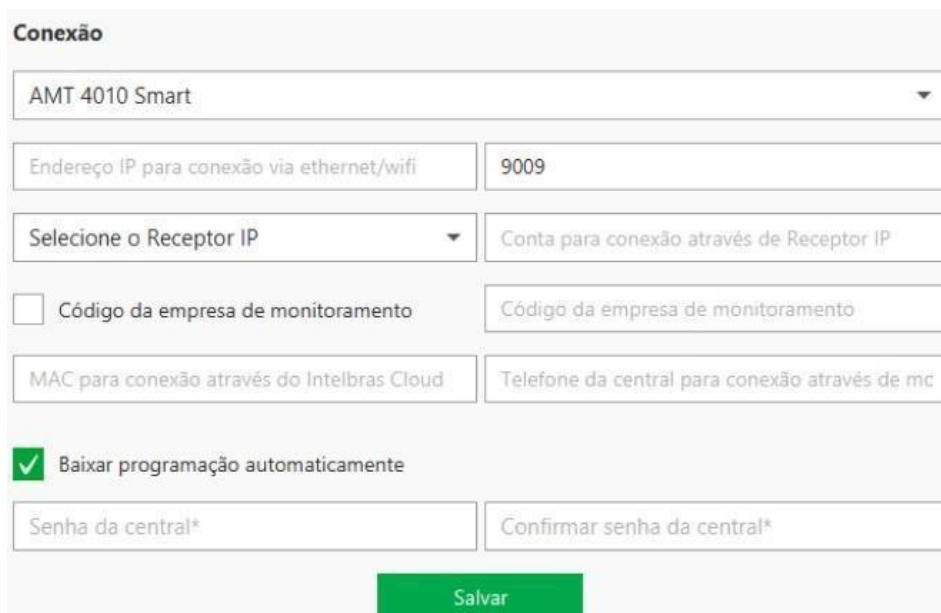


Na seção de conexão, insira as suas informações correspondentes:

Endereço IP: **Coloque o IP na qual sua central está conectada**

Endereço MAC da sua central: Localizado na tampa da sua central

Senha da Central: **Localizado na tampa da sua central (senha de acesso remoto)**



Após configurar sua central e retornar ao menu principal, clique em “Conectar” e selecione a opção para realizar conexão através de Ethernet, assim conseguiremos configurar nossa central de forma remota.

Conectar ao cliente

- ☒ Baixar programação automaticamente
- ☐ Realizar a conexão através de ethernet
- ☐ Realizar a conexão através de conta em Receptor IP
- ☐ Realizar a conexão através do Intelbras Cloud
- ☐ Realizar a conexão através de porta serial
- ☐ Não conectar, apenas ver configuração salva

Conectar

Cancelar

Após conectado com sucesso na central de alarme, clique em configurações e depois em comunicação e marque a opção reportagem em tempo real. Também de preferência para o modo de reportagem Duplo IP, evitando assim configurações erradas no menu de monitoramento IP.

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

Configurações

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 0

Número de tentativas de discagem 9

Tempo para reportar falha de AC 1

Modo de reportagem Duplo IP

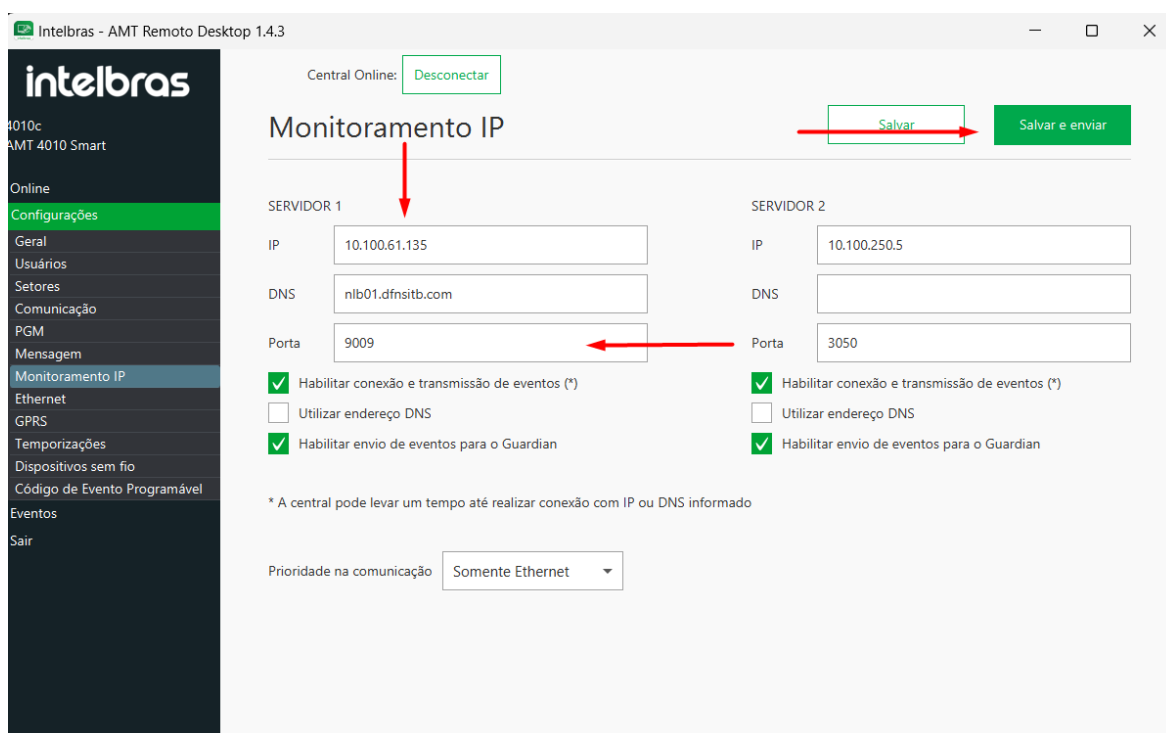
Protocolo monitoramento #1 Contact ID

Protocolo monitoramento #2 Contact ID

Depois clique em configurações novamente e depois em Monitoramento IP:

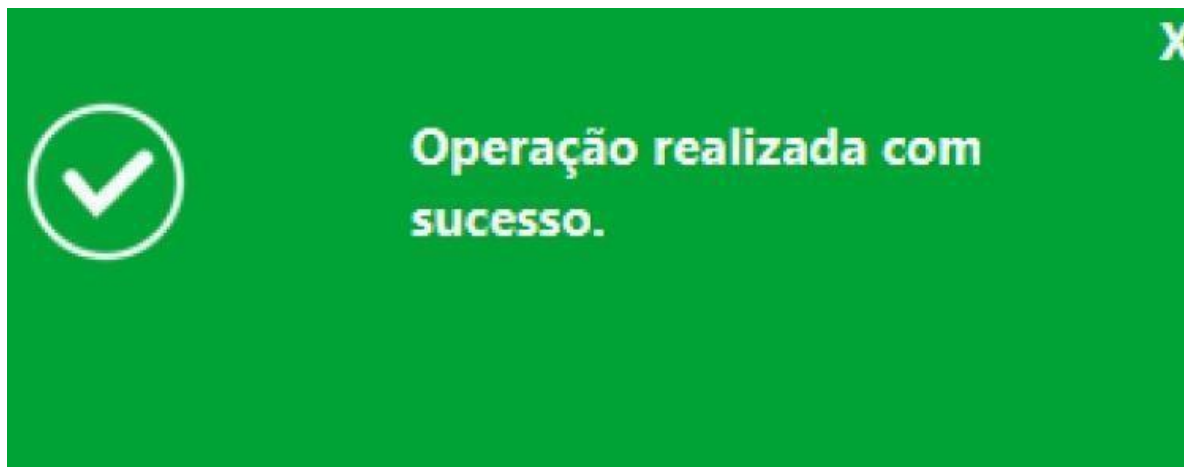


Na configuração do Servidor 1 em Monitoramento IP, **defina o endereço IP correspondente ao seu servidor do Defense IA** e insira a **porta que foi escolhida durante a instalação para o serviço do Receptor AMT (padrão 9009)**. Mantenha os 2 checkbox mostrados da imagem como marcados. Clique em salvar e enviar.



Após isso sua central de alarme estará configurada:

Atenção: Lembre-se de desconectar o AMT Remoto da central de alarme para que você consiga adicionar a central no middleware de centrais.



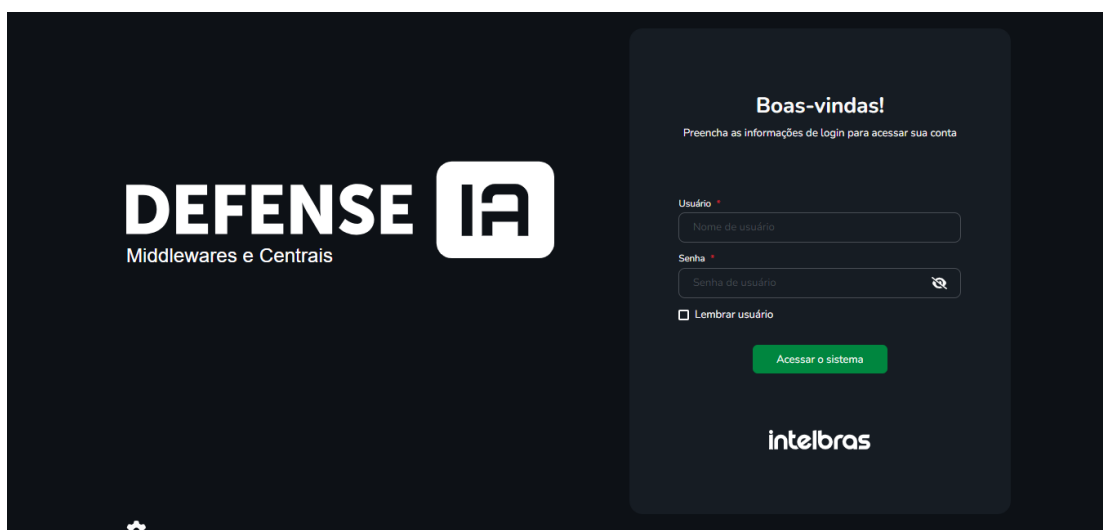
5.2. Como adicionar uma central de alarme através do Web Client

O Web Client é projetado para proporcionar uma experiência intuitiva e eficiente para os operadores. Este sistema se destaca como uma solução para gerenciar as centrais de alarmes e de incêndio.

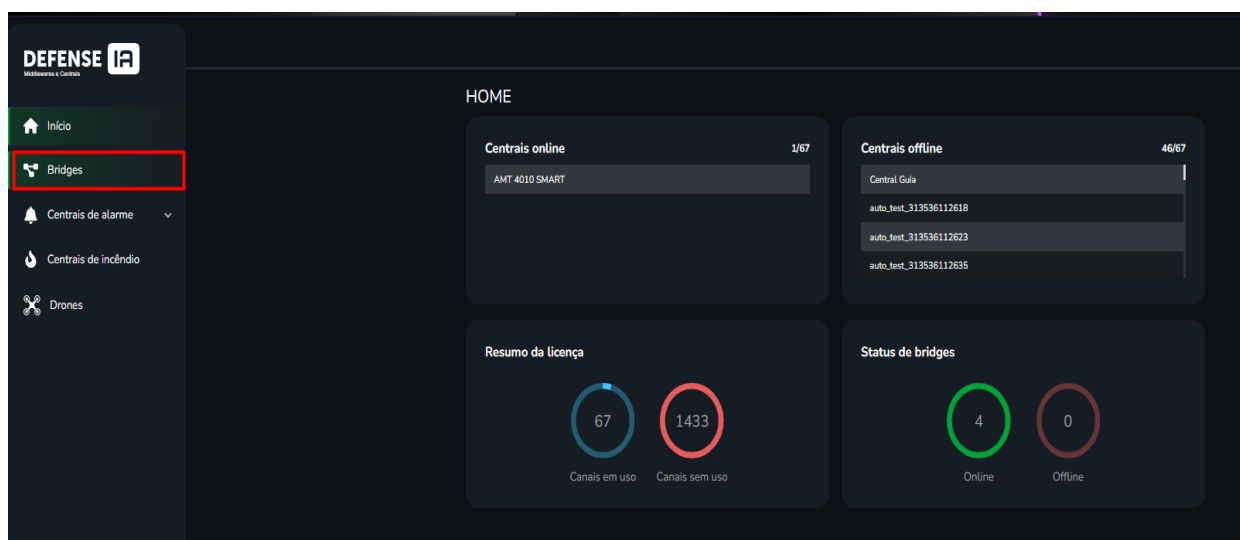
Para ter acesso ao Web Client, no seu navegador digite:

http://(IP do seu servidor do defense):3001.

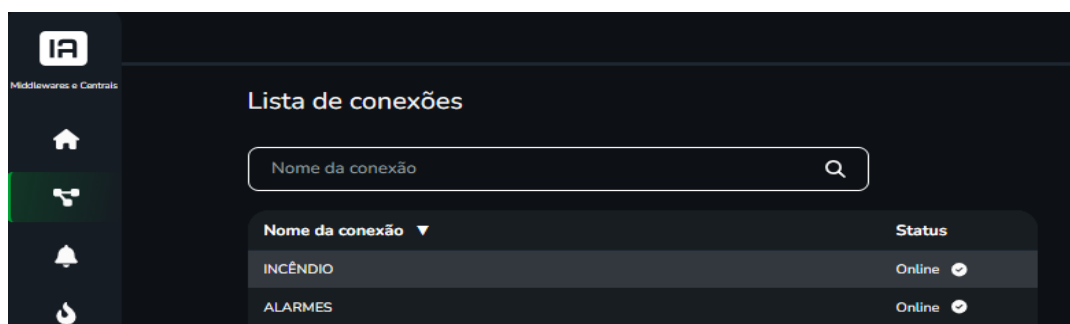
Feito isso faça o login utilizando a credencial de algum usuario Admin ou Super Admin do Defense IA.



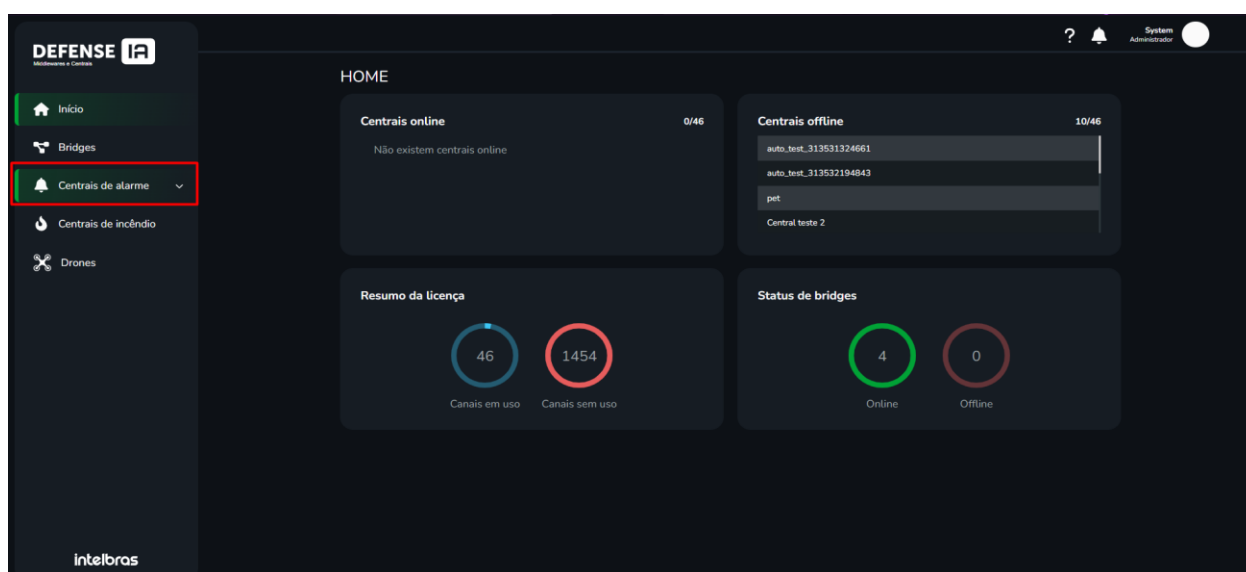
Após conseguir logar, o primeiro passo é verificar se os bridges estão online, o bridge é necessário para que o evento da central de alarme chegue até o cliend desktop do Defense IA. Acesse o menu Bridges no menu lateral esquerdo.



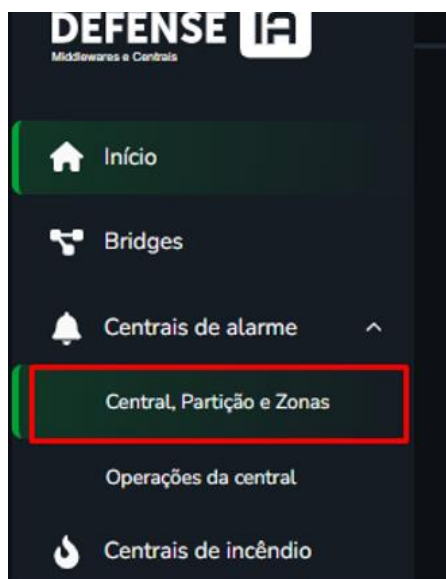
Caso o bridge esteja offline, verifique se os serviços do Defense IA Server estão online. Se todos estiverem online e mesmo assim os bridges estão offline, entre em contato com o suporte.



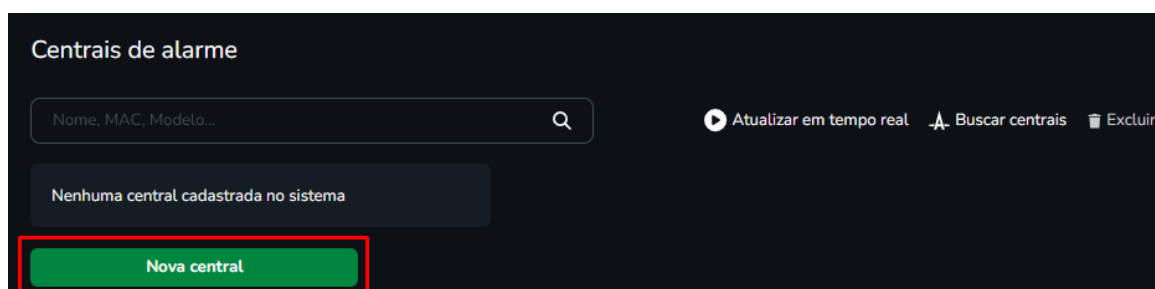
Após conseguir logar, retorne ao início e na barra lateral, clique em central de alarmes na barra lateral.



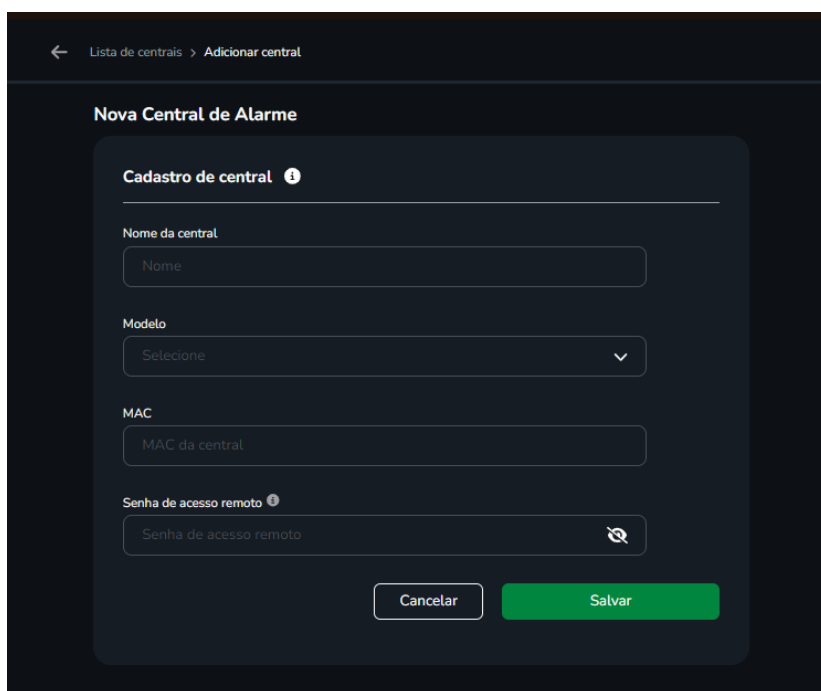
Depois em Central, Partição e Zonas.



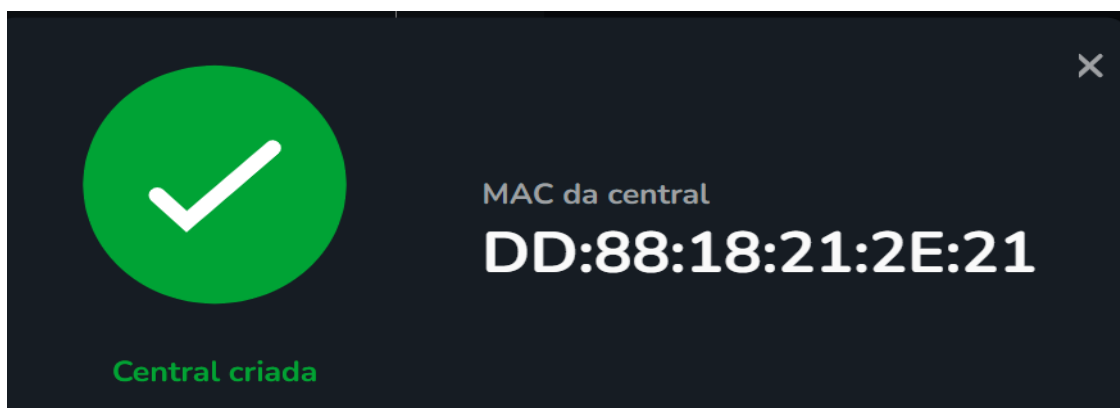
Para adicionar uma central de alarme, clique em nova central.



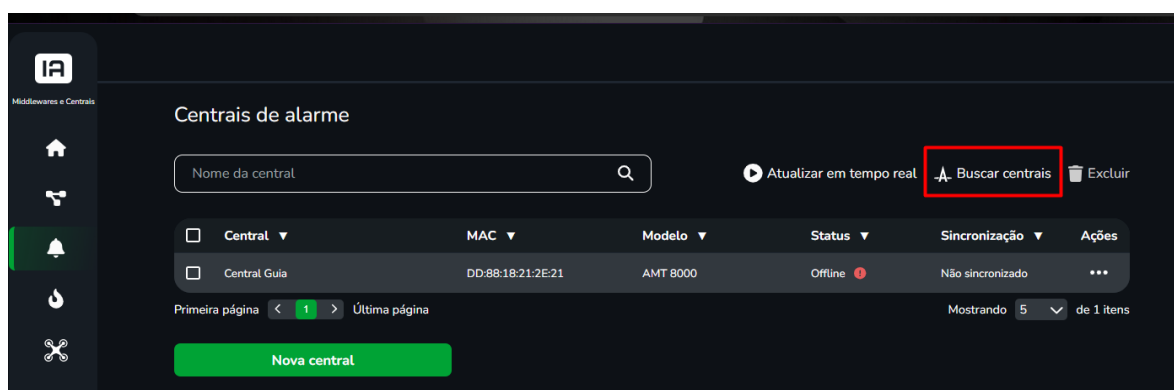
Preencha com as informações corretas e clique em salvar.



Após isso sua central estará cadastrada.



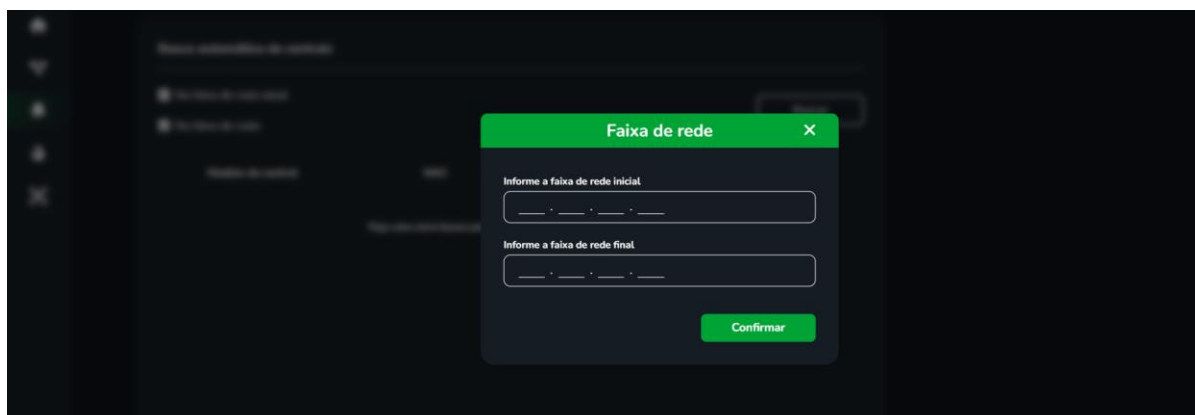
Outra forma de adicionar centrais de alarme é pela faixa de rede. Para isso é preciso acessar o menu de centrais de alarmes novamente, mas dessa vez clicar em buscar centrais.



Feito isso você pode adicionar utilizando a faixa de rede atual do servidor, ou uma faixa de rede distinta. Lembre que a sua rede deve estar configurada de forma correta para que o servidor encontre centrais em faixas diferentes.



Clicando em “Na faixa de rede” você consegue acessar por alguma faixa específica.



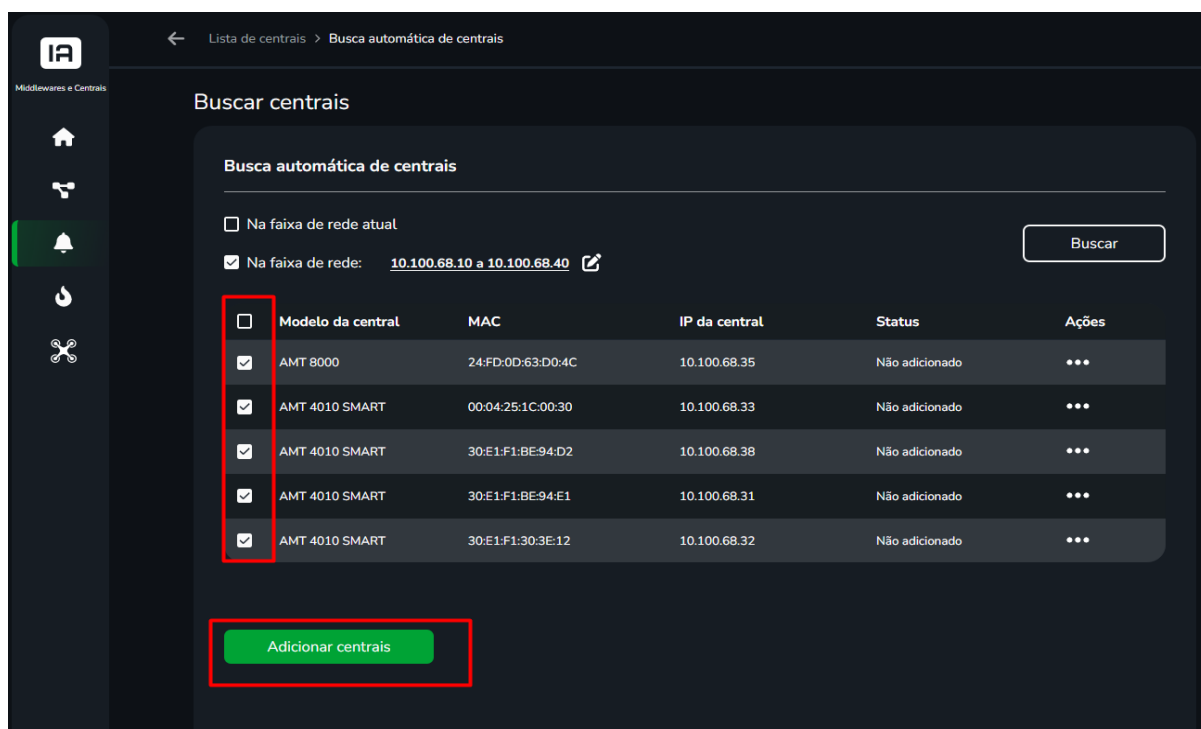
Por exemplo, após selecionar a rede, clique em confirmar.



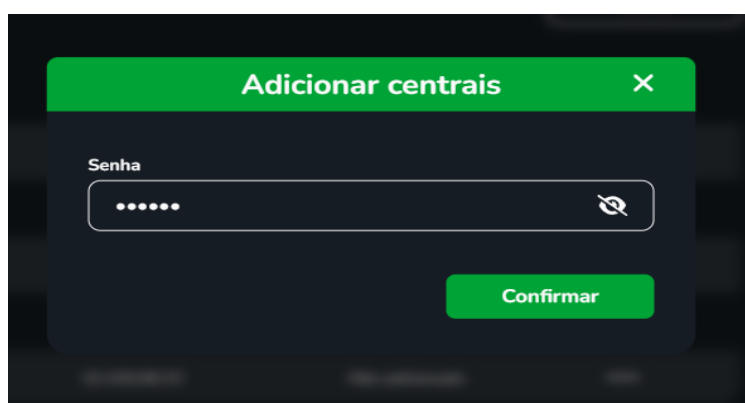
E depois em buscar.



Selecione as centrais na qual deseja cadastrar.



Após isso irá pedir a senha das centrais, coloque a senha e confirme. **Só é possível adicionar centrais em lote se todas possuírem a mesma senha de acesso remoto.**



Pronto, suas centrais já estarão adicionadas.

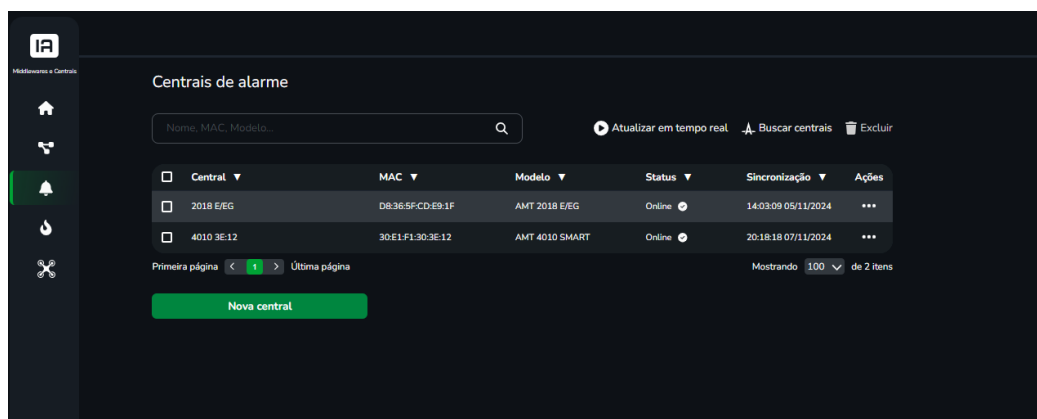
☐	AMT 4010 SMART	30:E1:F1:BE:94:E1	10.100.68.31	Adicionado	...
☐	AMT 4010 SMART	30:E1:F1:30:3E:12	10.100.68.32	Adicionado	...

5.3. Como sincronizar uma central de alarmes

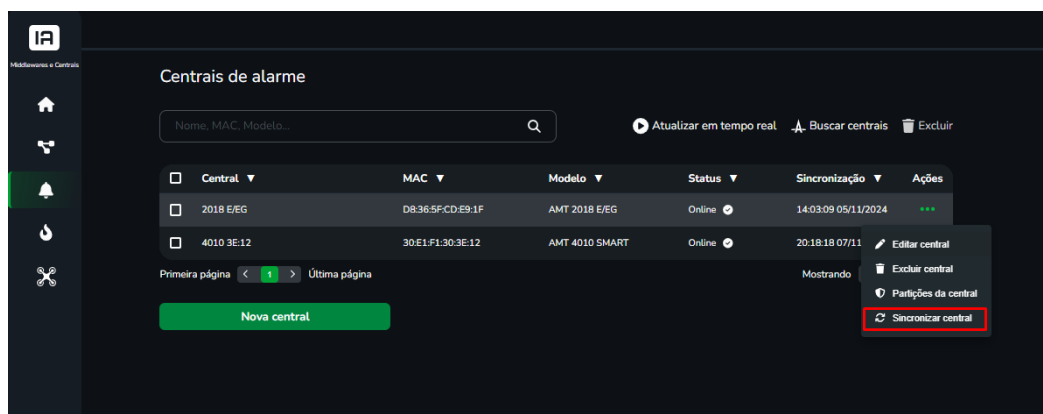
A sincronização serve para trazer para o middleware de centrais as configurações de particionamento e zonas presentes na central de alarme. Assim que você adiciona uma central (se a comunicação estiver disponível) ela é sincronizada automaticamente. No entanto, caso ocorra alguma falha, é

possível realizar a sincronização manualmente. Caso alguma alteração de particionamento e/ou zona seja feito diretamente na central de alarme, é possível voltar nesse menu e fazer a sincronização novamente. Essa funcionalidade está disponível por enquanto apenas para os modelos: **AMT 4010 SMART e AMT 2018 E/EG**.

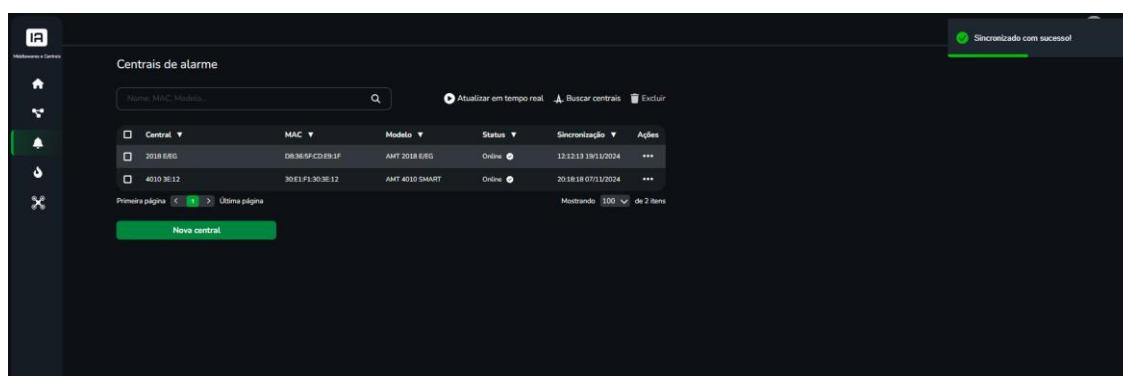
Para sincronizar, abra a pagina das centrais de alarmes.



Após adicionar vai até Ações e pode já selecionar sincronizar central.

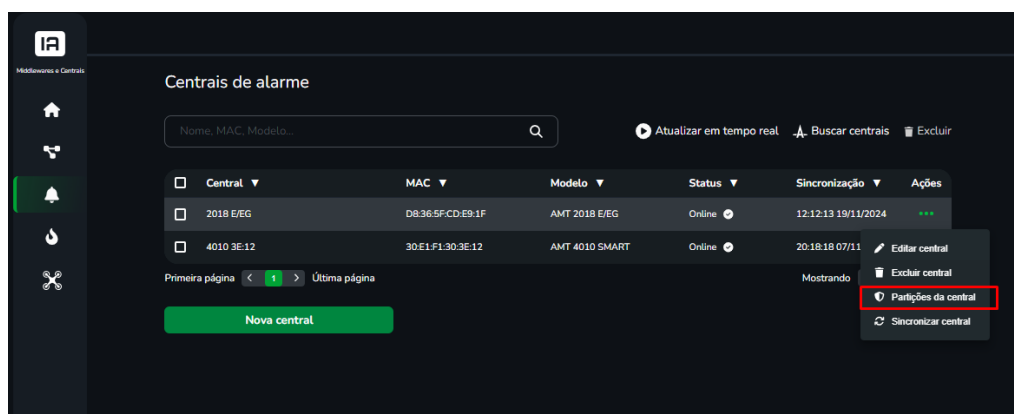


Após isso, sua central estará sincronizada.

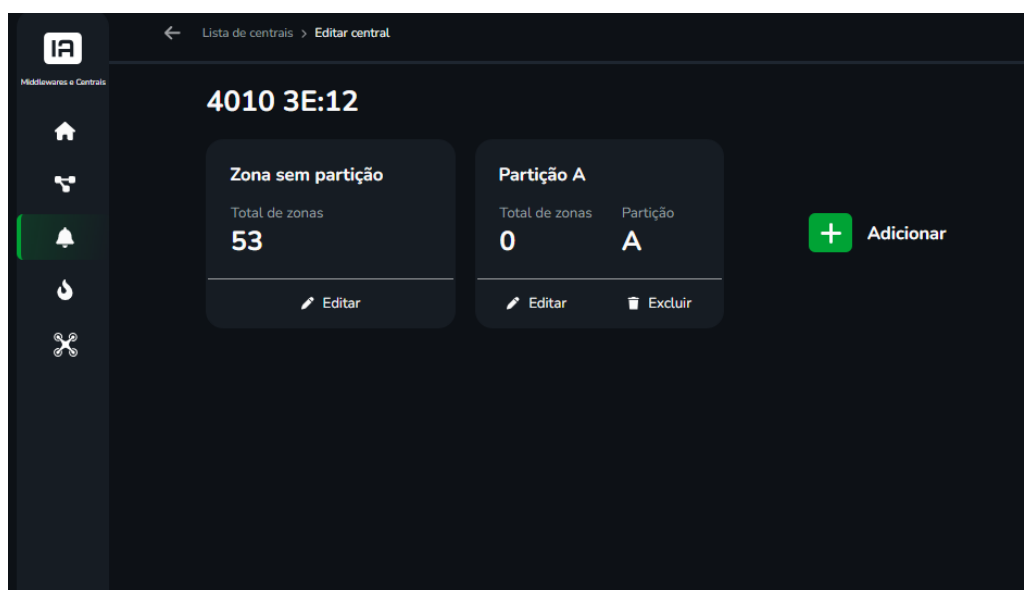


5.4. Configurando partições e zonas via Web Client

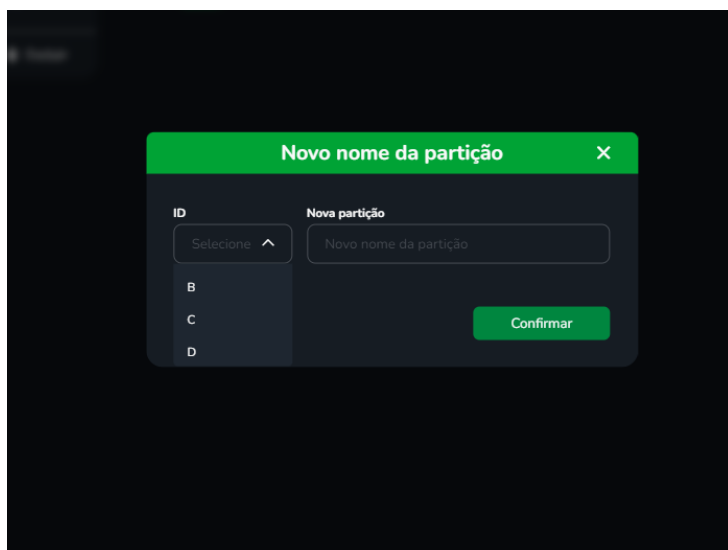
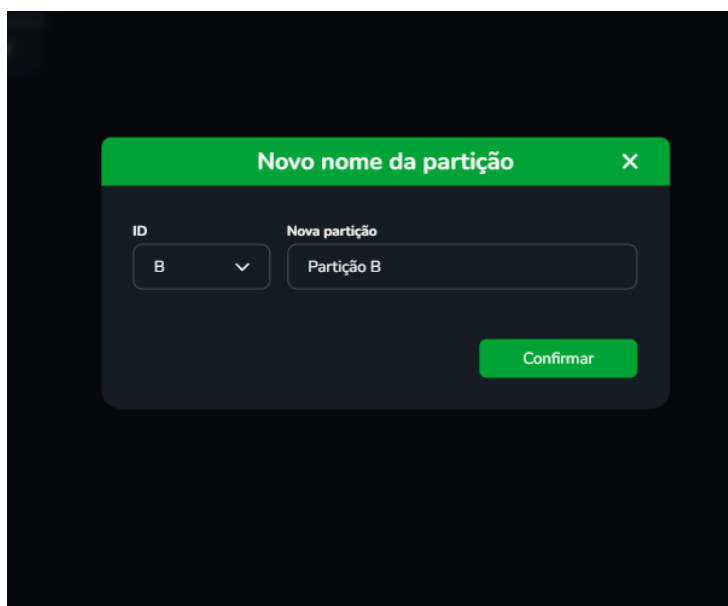
O Middleware de centrais também permite configurar o particionamento e distribuição de zonas das centrais de alarme. É possível fazer alguma alteração de zona e/ou configurar uma zona de alarme nova. Para realizar esta operação, acesse **“Partições da central”**.



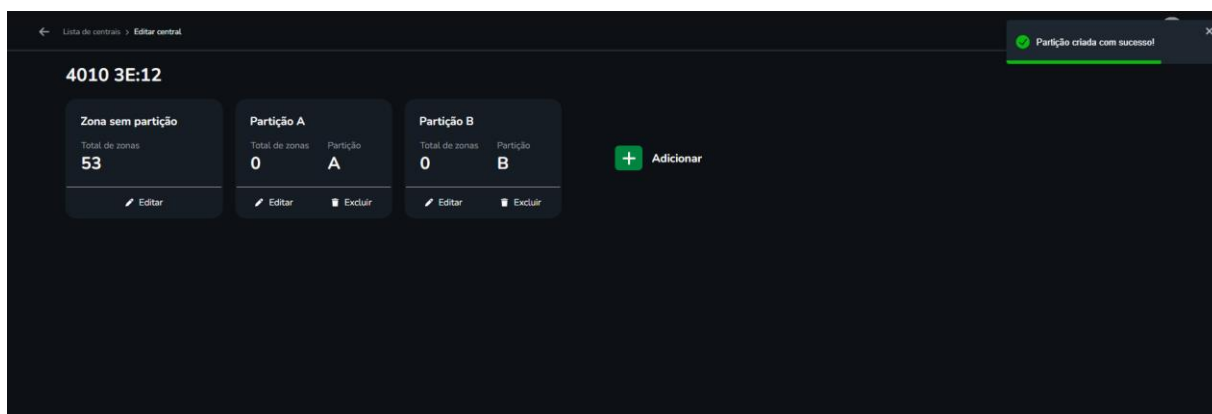
Para adicionar uma partição clique em + Adicionar.



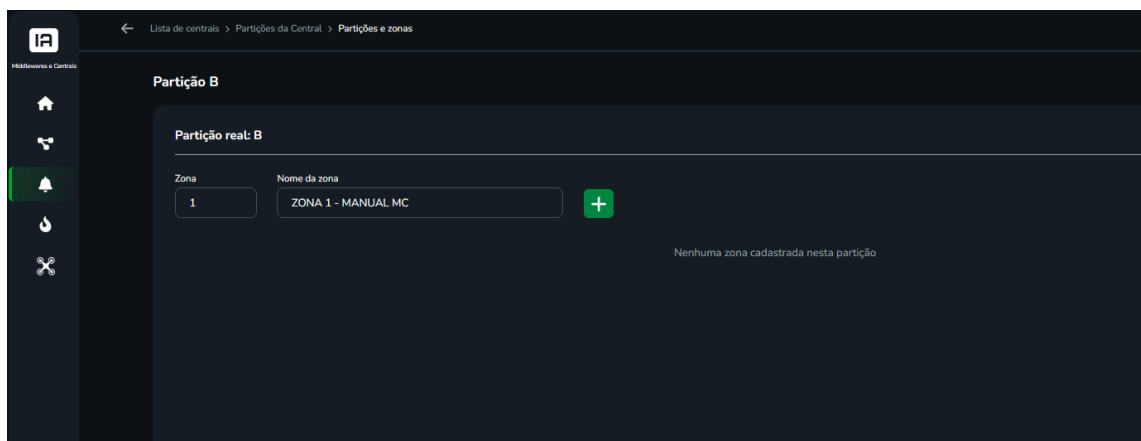
Após isso selecione o ID (que representa qual partição é a que esta sendo criada), nomeie a partição e depois clique em confirmar.

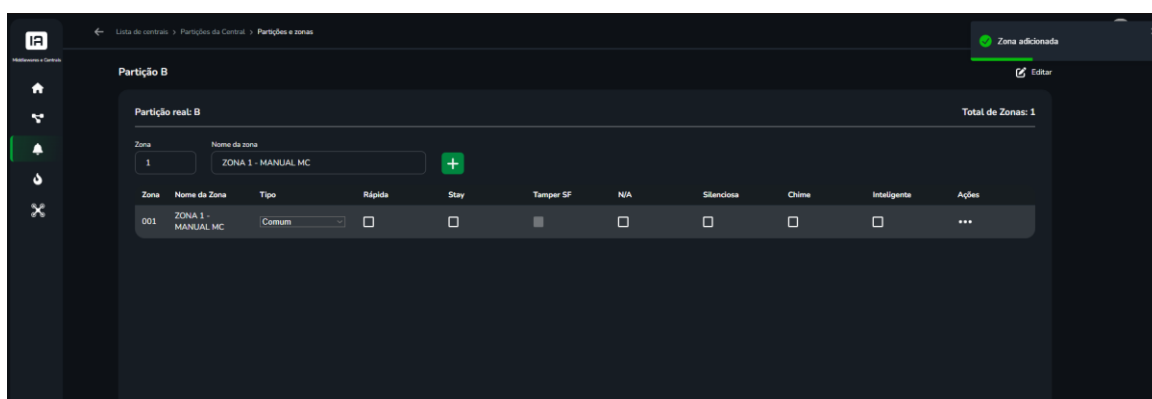
Agora para adicionar as zonas clique em **editar** na sua partição desejada.



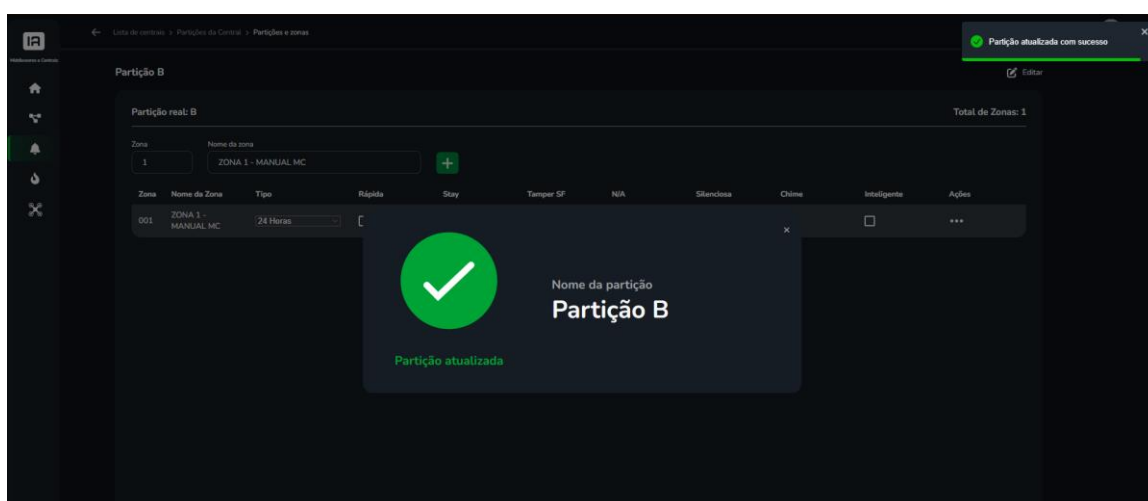
Após isso escolha a zona e nomeie ela, para confirmar clique em no botão +



Agora defina as configurações de cada zona adicionada e clique em salvar. O nome dado a zona neste momento permitirá identificá-la em operações futuras (operação de bypass e recebimento de eventos).



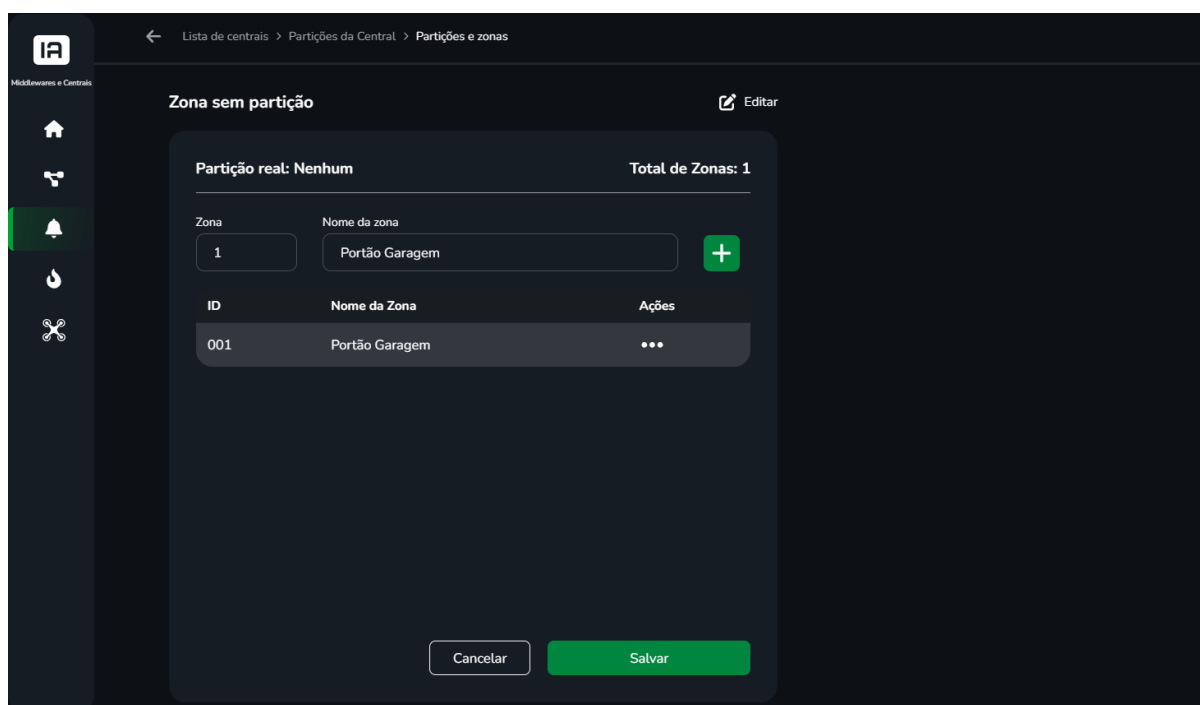
Ao realizar esta operação, as configurações serão enviadas para a central de alarme. Caso alguma outra alteração seja feita na central posteriormente, basta voltar a lista das centrais e clicar em sincronizar.



Esta configuração completa de zonas, onde quando configurado as informações são enviadas para a central **só está disponível para os modelos AMT 4010 SMART, AMT 2018 E/EG e AMT 2018 E SMART.**

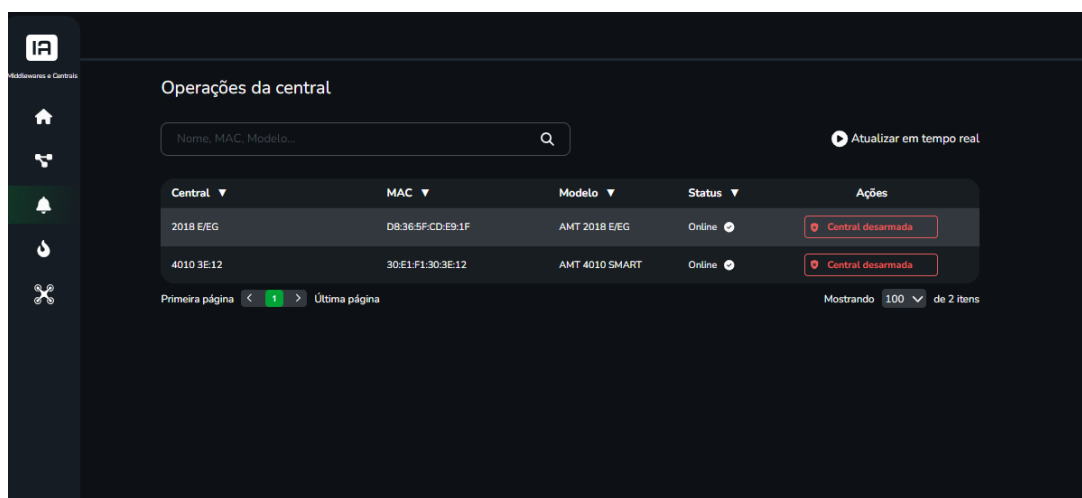
Para os demais modelos (AMT 8000, AMT 1000 SMART, AMT 1016 NET) o sincronismo não está disponível e a configuração da central de alarme deverá ser replicada no middleware de centrais manualmente. A configuração feita no middleware para estas centrais não será enviado para a central de alarme, e servirá apenas para possibilitar operar a central posteriormente (bypass nas zonas, arme/desarme de partições).

Note que ao adicionar uma central não é solicitado as configurações específicas de cada zona, uma vez que adicionar a zona para estes modelos serve apenas para operar a central posteriormente.

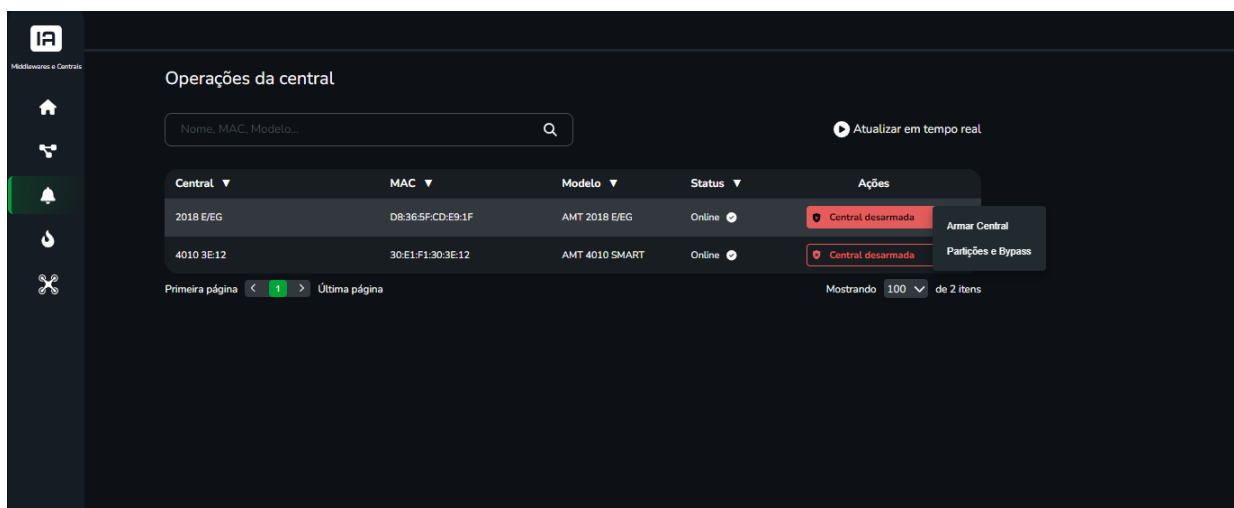


5.5. Como operar uma central de alarme

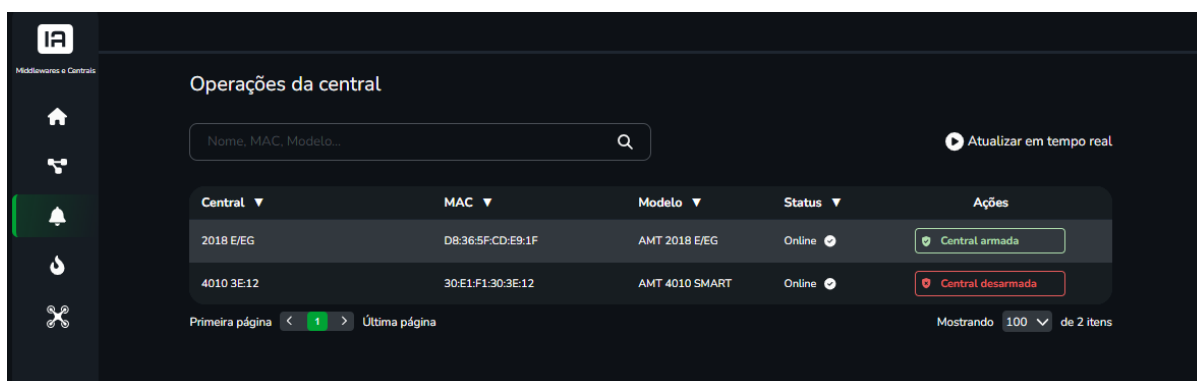
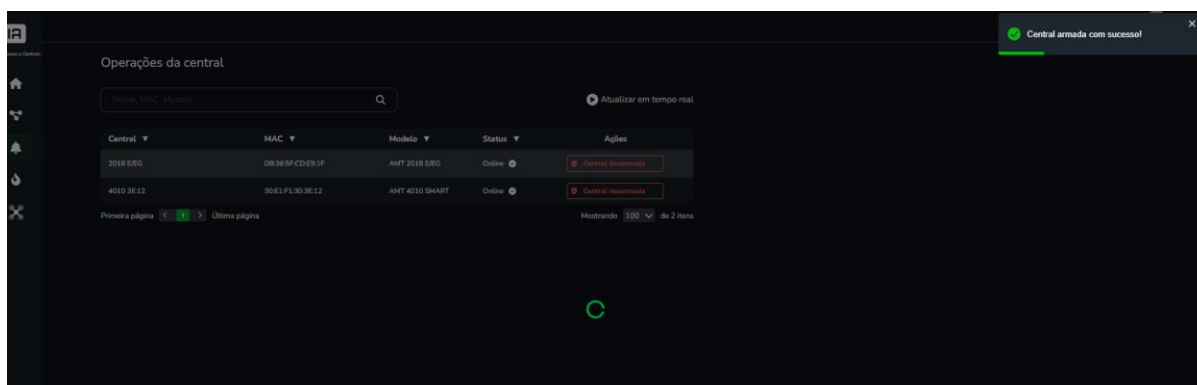
Para armar e desarmar uma central é necessário ir até a página “Operações da central”.



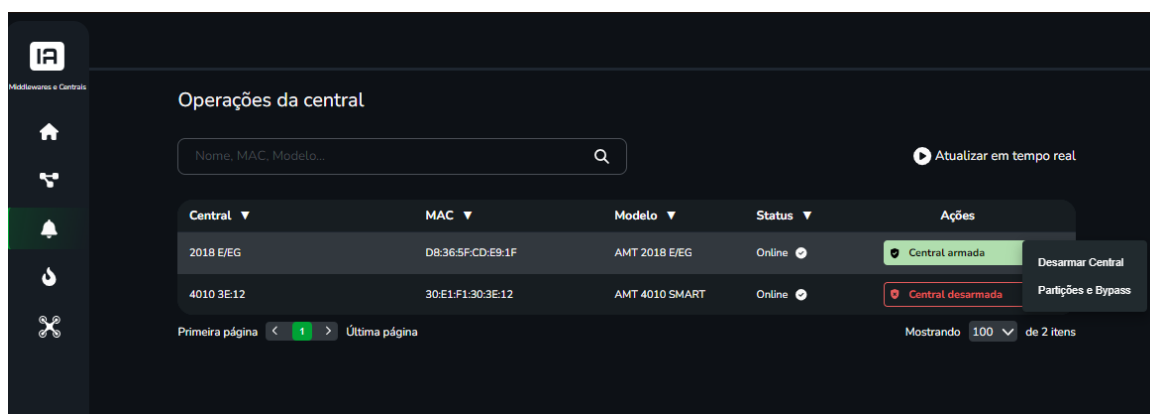
Após isso você pode clicar no botão de **Ações** e selecionar **Armar central** (é necessário que a central esteja online).



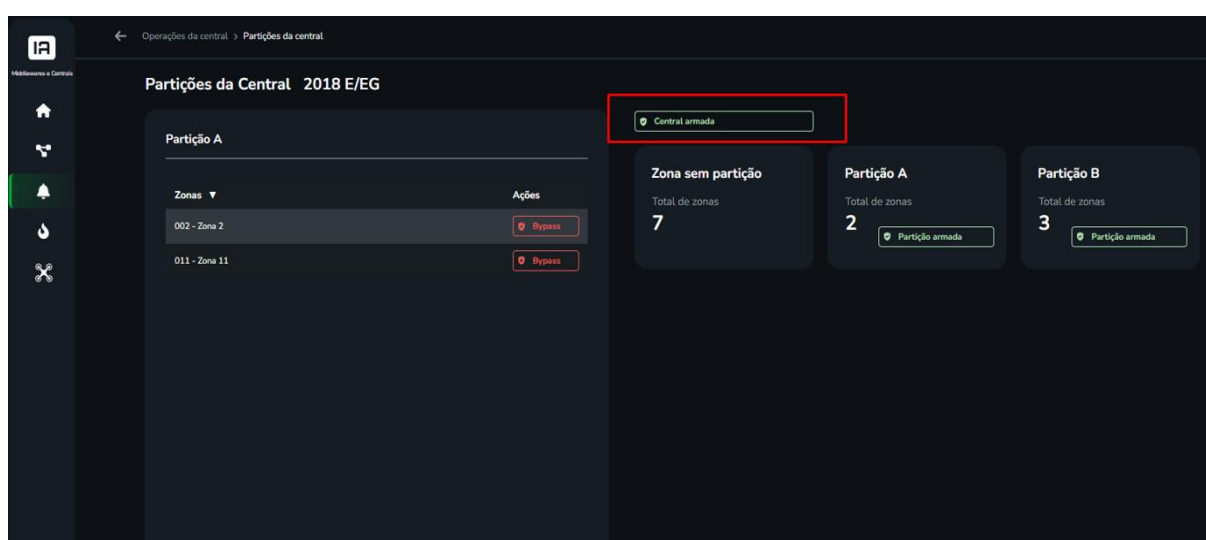
Será exibido uma mensagem de “Central armada com sucesso”.



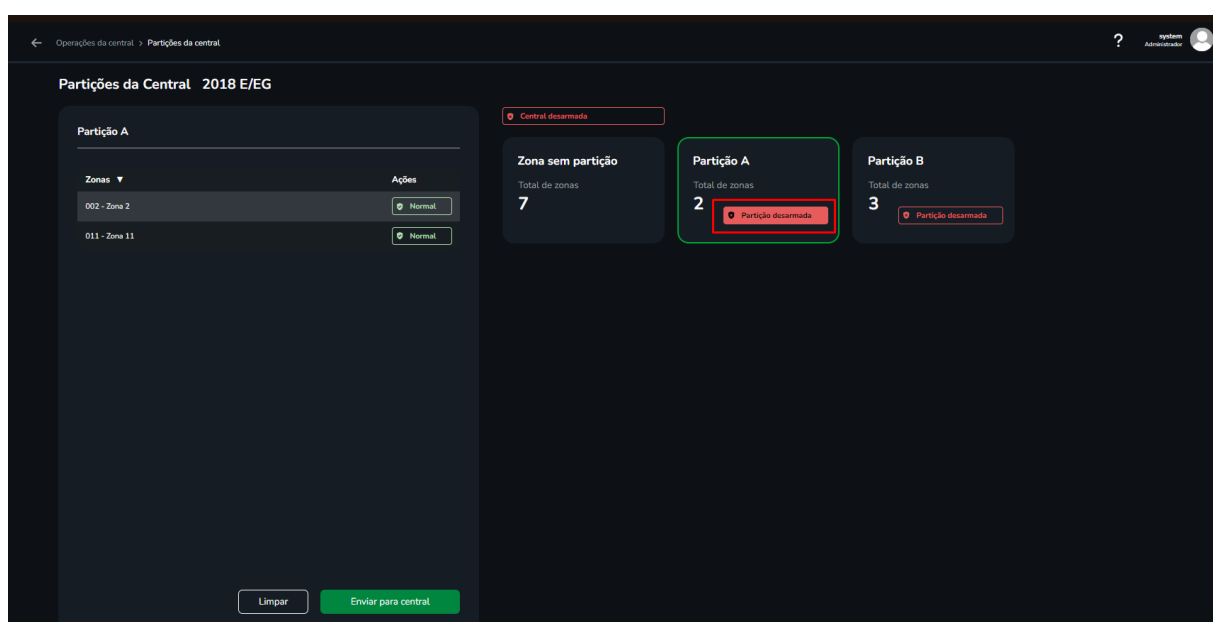
Também é possível armar e desarmar pela tela de partição e bypass, para isso volte a tela de Operações da central e clique em partições e Bypass.



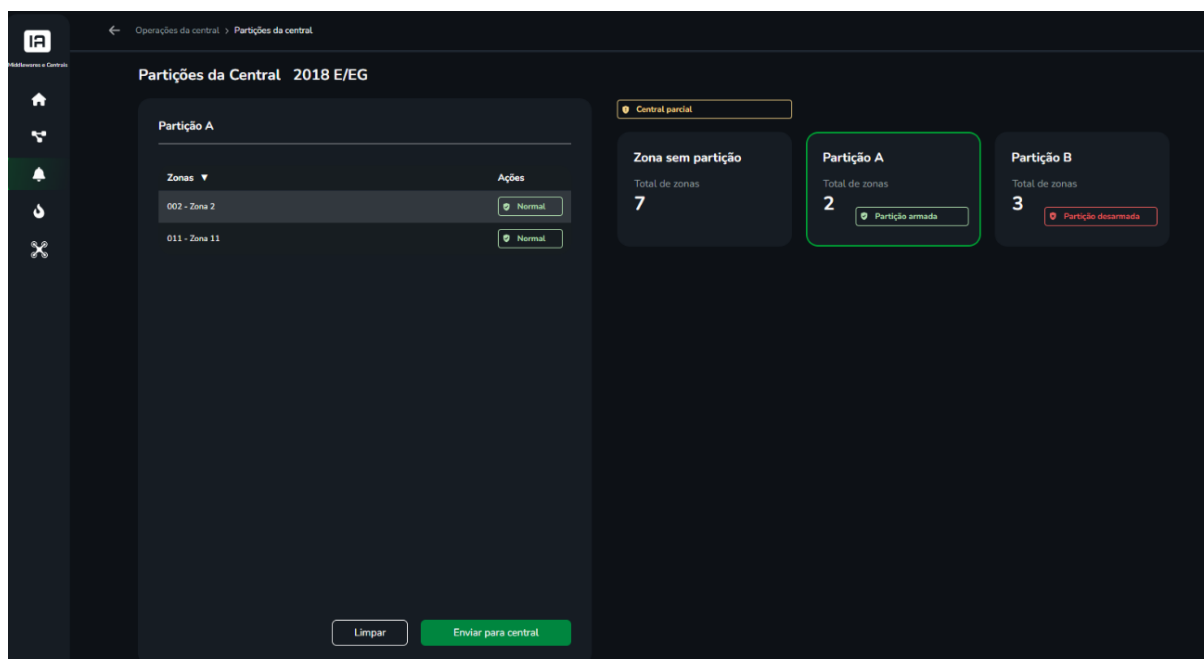
Agora clique em central armada/desarmada na parte superior.



Também é possível armar e desarmar uma partição específica, para isso clique na operação na janela que representa a partição que se deseja operar.

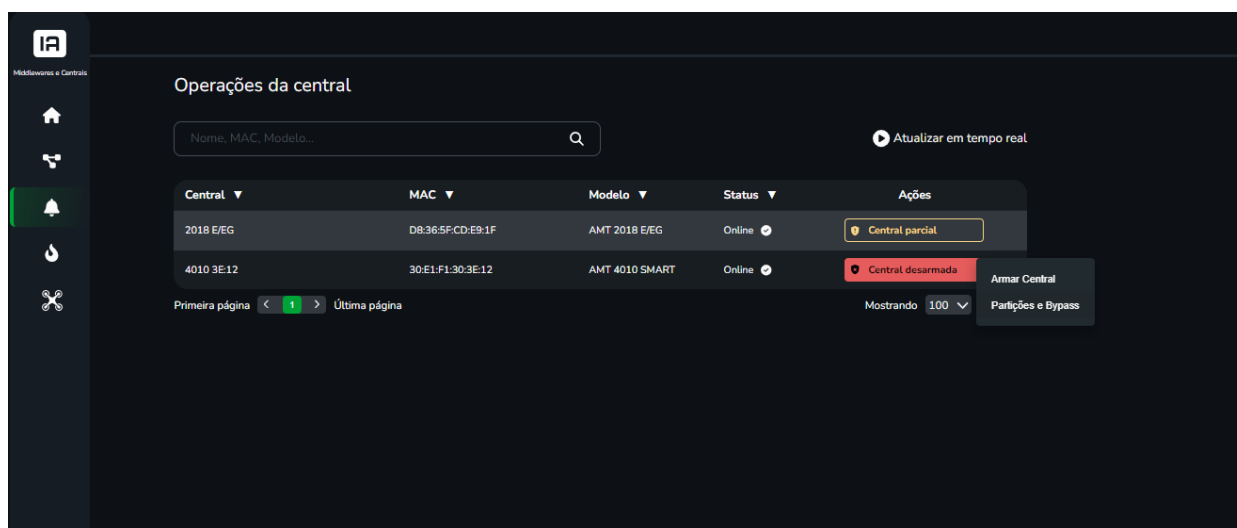


Pronto, estado da partição alterado com sucesso.

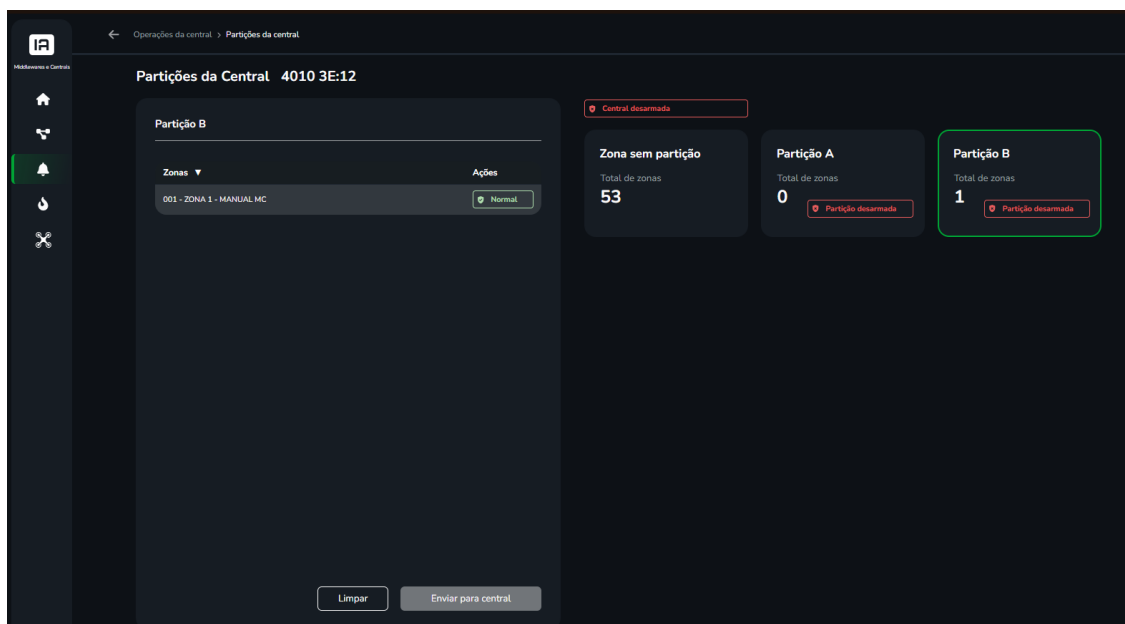


5.6. Anulação de Zona (Bypass)

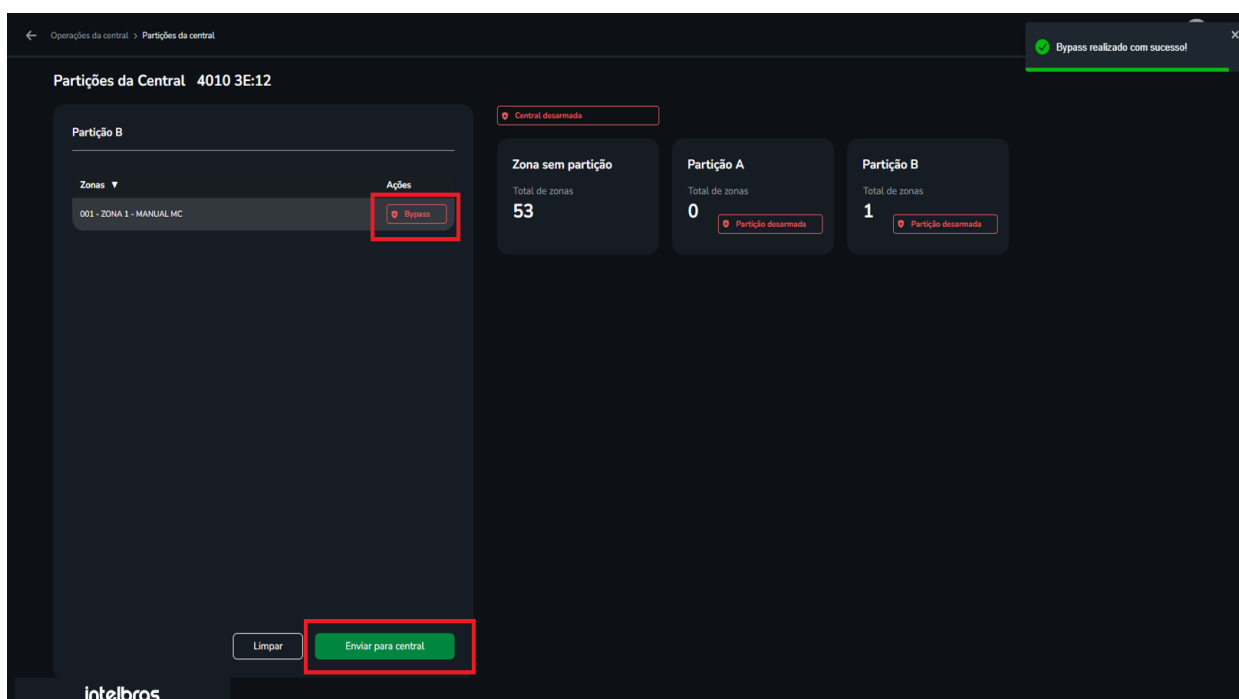
Lembre-se que para armar uma partição é necessário que todos os sensores relacionados a esta partição estejam fechados. Caso não seja possível fechar um sensor, ou caso o sensor esteja com falha, é possível realizar um bypass (anulação de zona) temporário para que o arme seja possível. Para realizar o bypass, acesse o menu de “**Partições e Bypass**” presente na tela de “**Operações da Central**”.



Agora clique na partição na qual está a zona desejada.



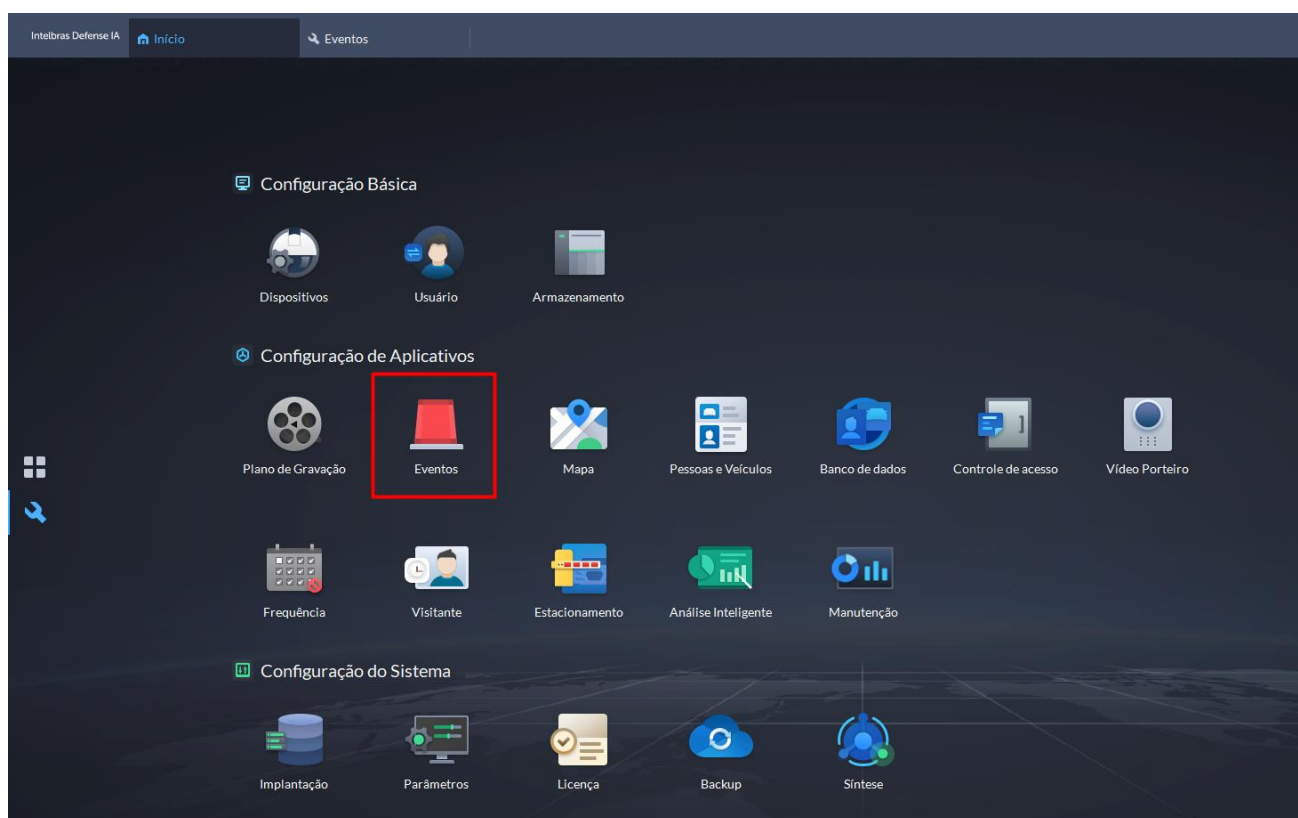
Após isso clique no botão presente na coluna ações na listagem das centrais, deixe a zona na situação desejada (bypass ou normal) e clique em enviar para a central. Após realizar o bypass nas zonas corretas, será possível realizar o arme da central ou partição.



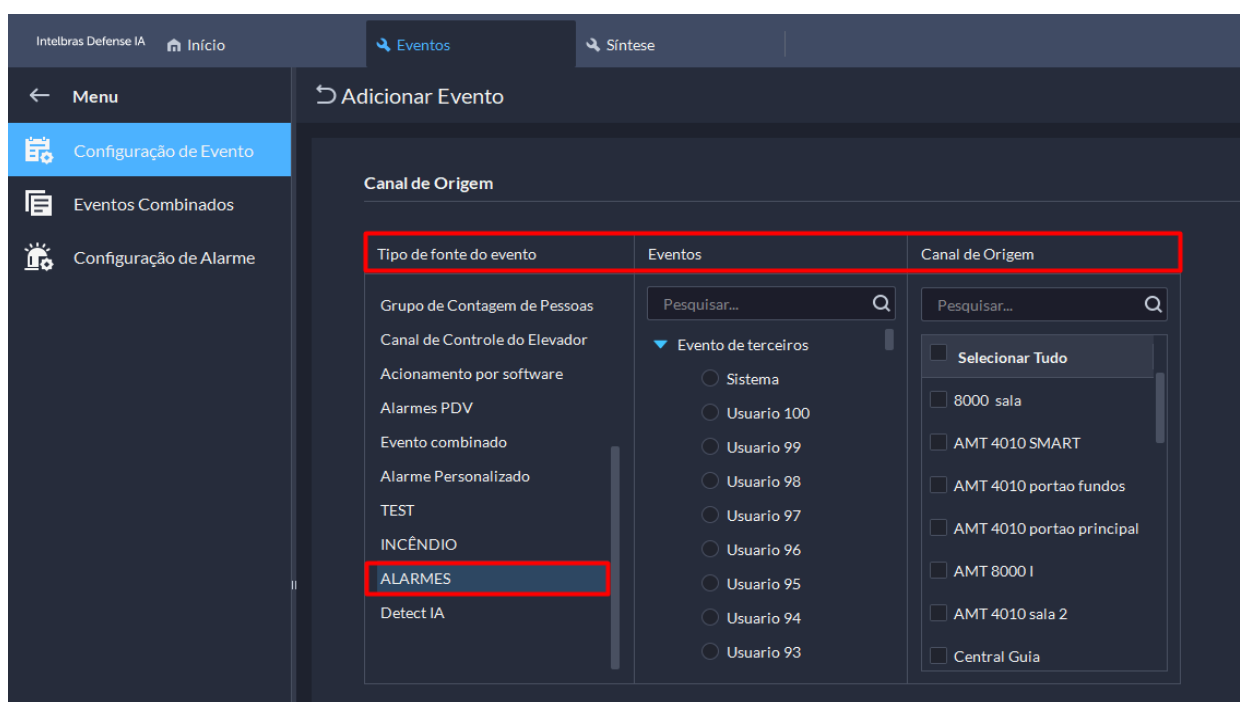
O botão “Limpar” retira o Bypass de todas as zonas das partições desarmadas.

5.7. Como configurar e visualizar os eventos das centrais

Para realizar a configuração, no menu inicial do Defense, clique em Eventos.



Após isso, em fontes de evento desça até “ALARMES” e a selecione, em eventos coloque sua zona desejada e em canal de origem sua central.



Feito isso pode descer a página, nomear o esquema, definir sua prioridade e selecionar os usuários, após tudo isso só clicar em OK.

Atributos do Evento

Nome do Esquema: Prioridade:

Modelo de Tempo: Tabela de Feriados:

Comentários:

ⓘ Durante os feriados, será executado de acordo com o plano de feriados, e fora dos feriados, será executado de acordo com o modelo de horário.

Vincular Ação ☐

Protocolo de Alarme ☐

Notificar Usuário

Selecionar Usuário

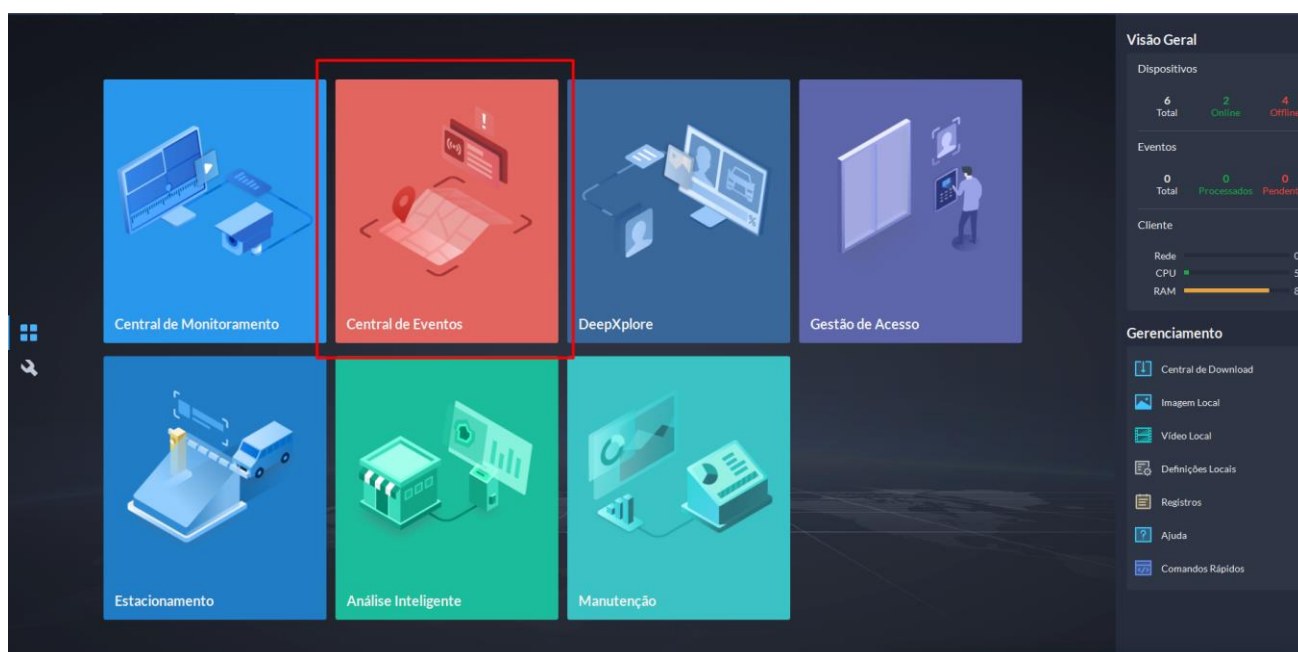
Pesquisar...

- ☒ Superadministrador
- ☒ system
- ☒ Administrador
- ☒ Usuário Normal

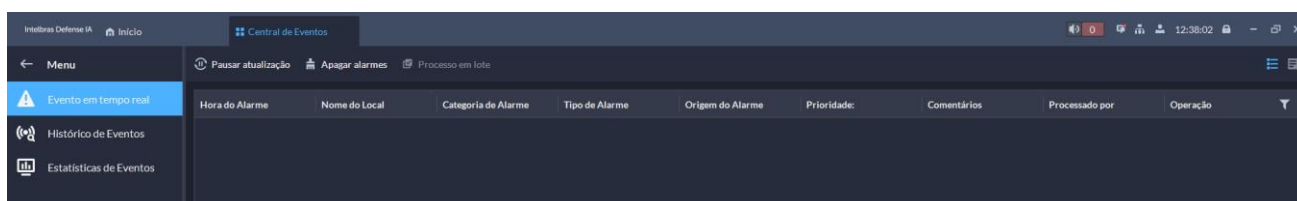
Selecionado(1)	Usuário	Tipo de Usuário	Operação
	system	Superadministrador	⊖

OK Cancelar

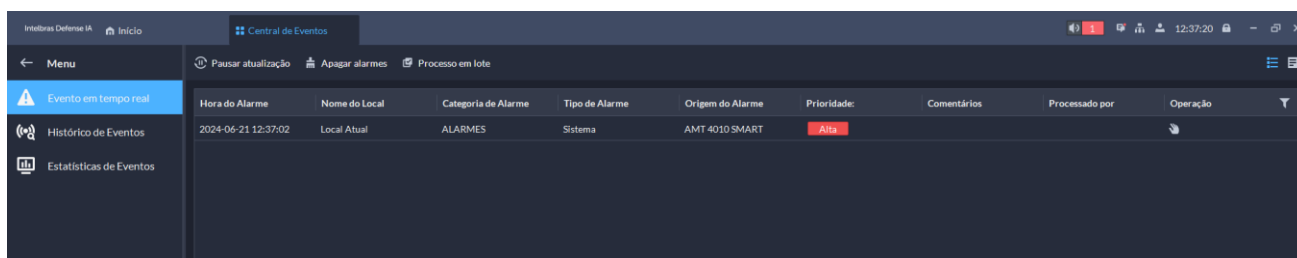
Agora para visualizar os eventos, retorne até o menu do Defense e clique em central de eventos.



Sem eventos assim será a página:



E assim que você receber o evento ele irá notificar da seguinte forma



6. Centrais de Incêndio

O Middleware de Centrais permite comunicação com as centrais de incêndio Intelbras modelos CIE 1125, CIE 1250 e CIE 2500.

As funcionalidades disponíveis são: Adicionar e visualizar centrais disponíveis, recebimento de eventos no Defense IA.

Diferente das centrais de alarme, não é possível realizar configuração de zonas e laços pelo Web Client.

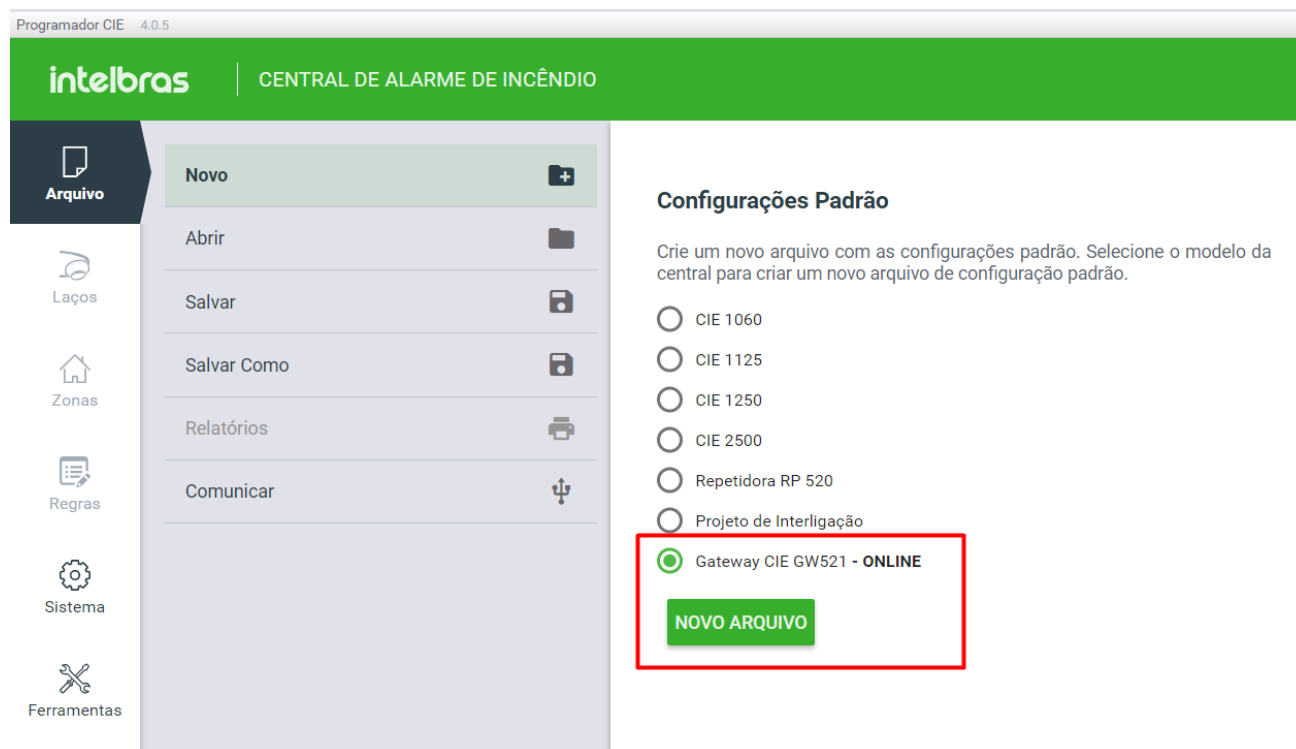


Figura 2. CIE 1125

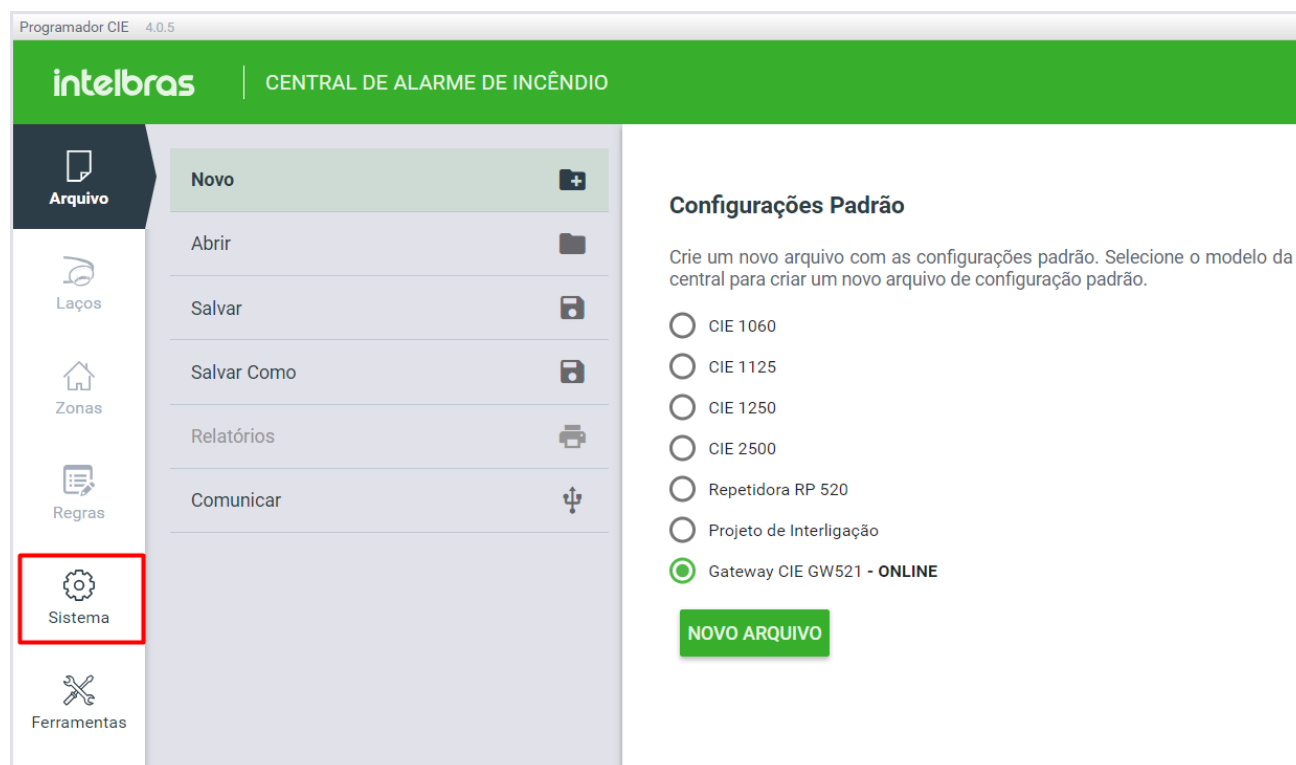
6.1. Configuração prévia de uma central de incêndio

Antes de adicionar a central de incêndio ao middleware de centrais, é necessário realizar algumas configurações na CIE. Para realizar estas configurações é possível utilizar o software **Programador CIE**

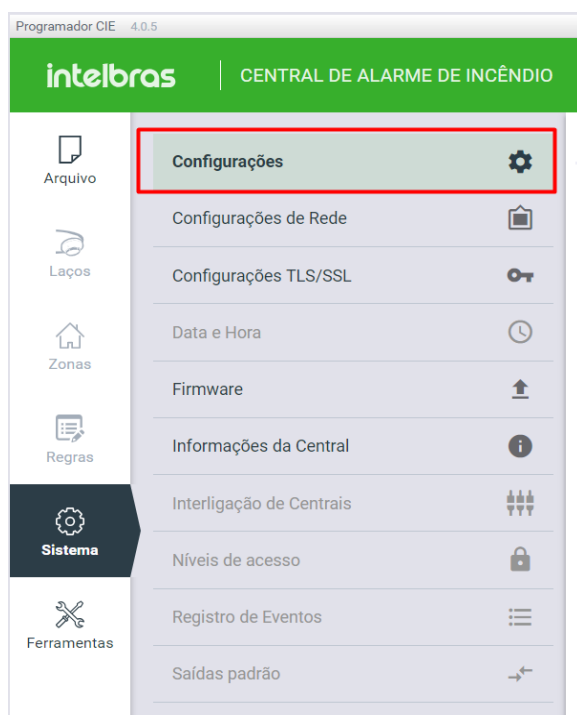
(disponível no site da Intelbras). Conecte via cabo USB no GW 521 e após ficar ONLINE, crie um novo arquivo.



Clique em sistema.



Depois em configurações.



Agora habilite a função webhook.



Após feito isso configure da seguinte maneira:

Endereço do Webhook: IpServidor/api/gw521/events

Porta: Verifique a porta escolhida pelo middleware de incêndio durante a instalação. Caso não lembre, acesso o arquivo progress.txt disponível no caminho onde o middleware de incendio foi instalado.

Porta padrão do webhook: **6001**

Endereço do Webhook: IpServidor/api/gw521/events

27 / 100

Porta: 6001

Atente-se de verificar se a porta 6001 está aberta, conforme explicamos anteriormente na liberação do firewall no tópico 3.

Gere e anote o HMAC, ele será utilizado posteriormente para comunicação entre GW521 e Defense IA. O uso do HMAC não é obrigatório, porém deixará a comunicação entre GW521 e Defense IA sem criptografias.

Autenticação: ☒ HMAC ☐ HTTPS

R08abaXA529RGhPTtp3P4eZq2ZivRsH3HvSWi2Tqd2qbsi4

Chave privada: hYlm0j3szpOACzuMA0dB9pcbnlpg36Tnm7uaTew== 88 / 88

GERAR

Agora por último, deixe o heartbeat em 01:00 e clique em APLICAR.

Idioma: ☐ Português ☐ Espanhol

Intervalo Heartbeat: 01:00 (min:seg) ?

Intervalo entre eventos: 500 (ms)

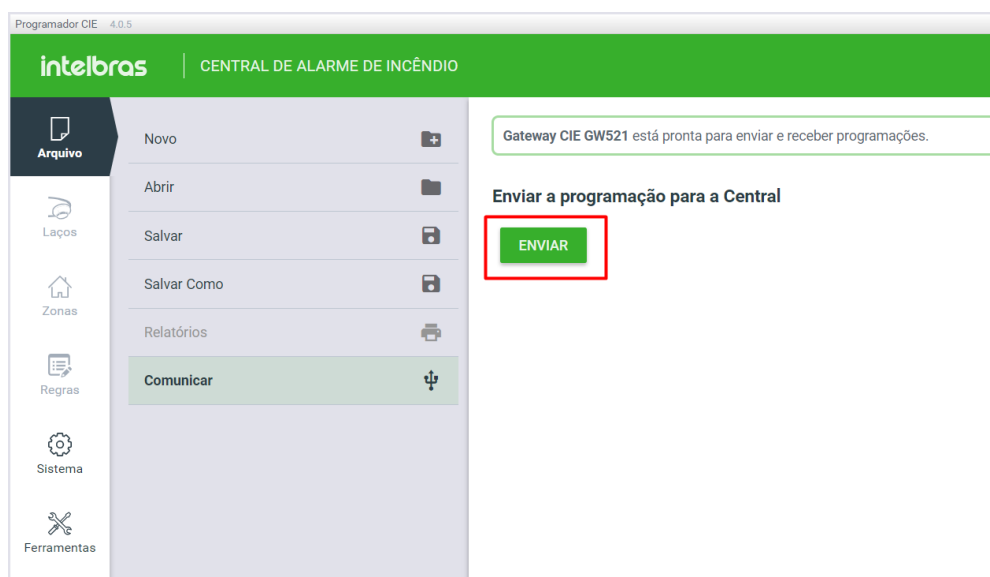
Código do Equipamento: 0 (opcional)

CANCELAR APLICAR

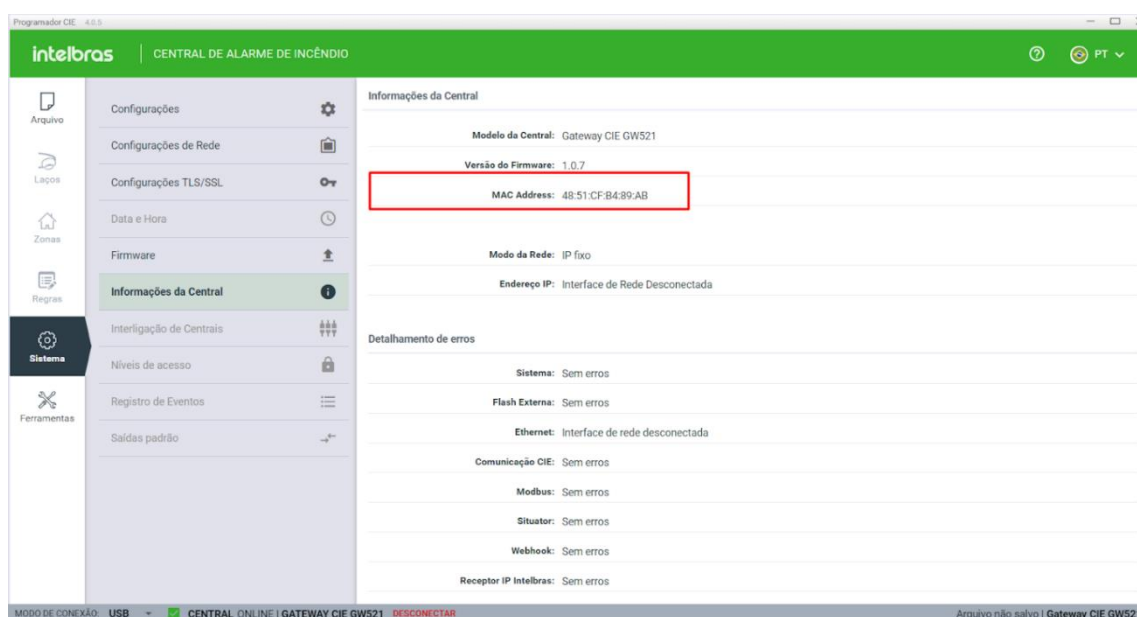
Após aplicar volte para arquivo.



Após voltar para arquivo clique em enviar para enviar as configurações realizadas.

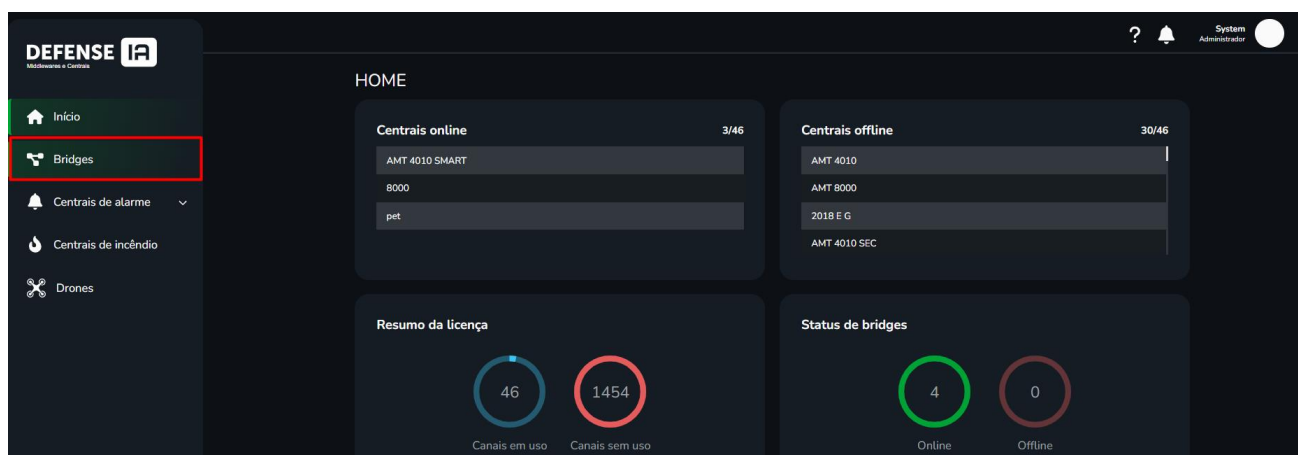


Acesse o menu de “**Informações da Central**” e colete o MAC Address do GW521 para utilização posterior.

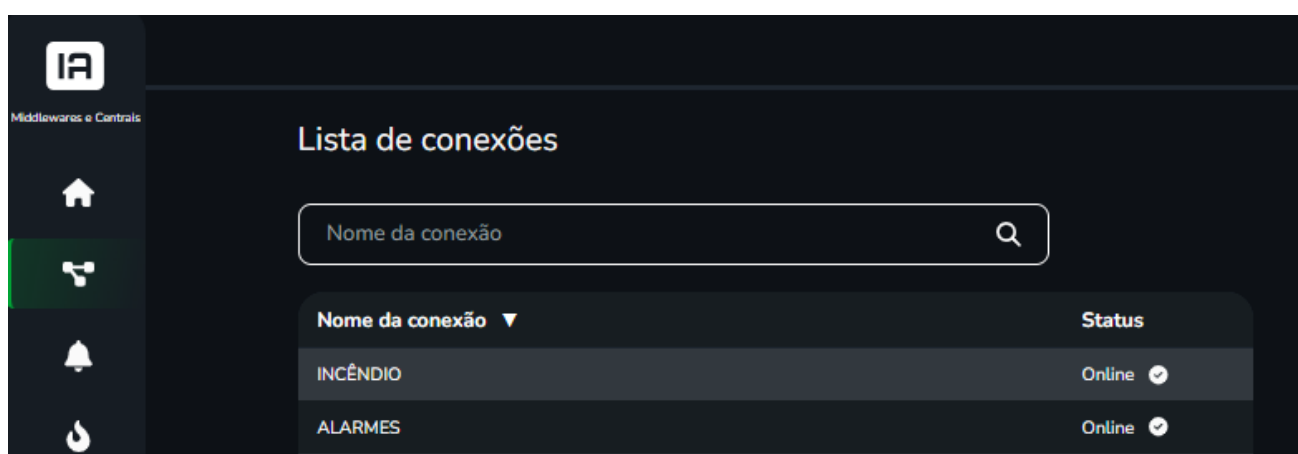


6.2. Como adicionar uma central de incêndio através do Web Client

Antes de adicionar a central de incêndio, certifique-se que o bridge responsável pela comunicação dos eventos com o Defense IA está online. Para confirmar esta informação, vá até o menu Bridges na barra lateral esquerda.

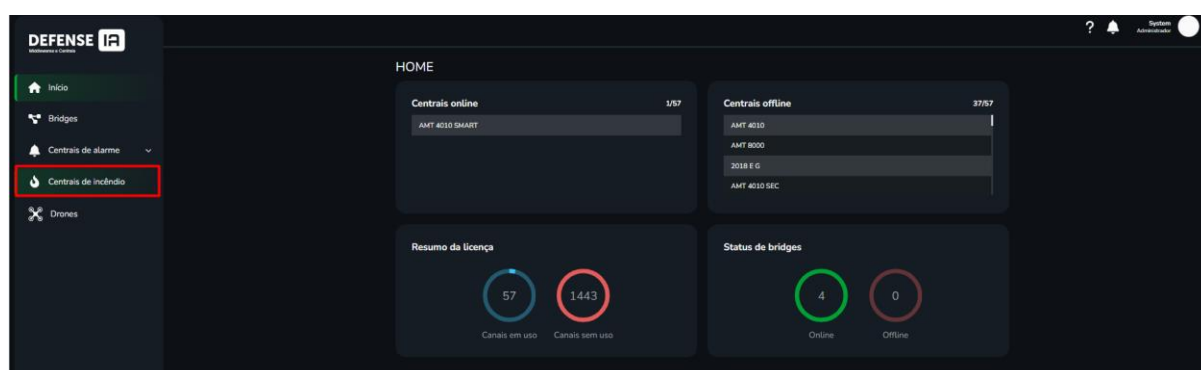


Verifique se o bridge “INCÊNDIO” está online.



Caso o bridge esteja offline, verifique se os serviços do Defense IA Server estão online. Se todos estiverem online e mesmo assim os bridges estão offline, entre em contato com o suporte.

Após confirmação, para adicionar uma nova central de incêndio, clique no menu “Centrais de Incêndio”.



Clique em “Nova Central”.



Agora preencha com as informações corretas.

The screenshot shows the 'Nova Central de Incêndio' form. It includes the following fields:

- Nome da central:** Incendio
- Modelo:** CIE 1125 (selected from a dropdown menu)
- MAC:** 48:51:CF:B4:89:AB
- HMAC da central:** Ki0tPmB69Gr6sD5Y0AJ+JQqx8pttROc32D7wjLS29o2/5tom/SygRSrwfLz

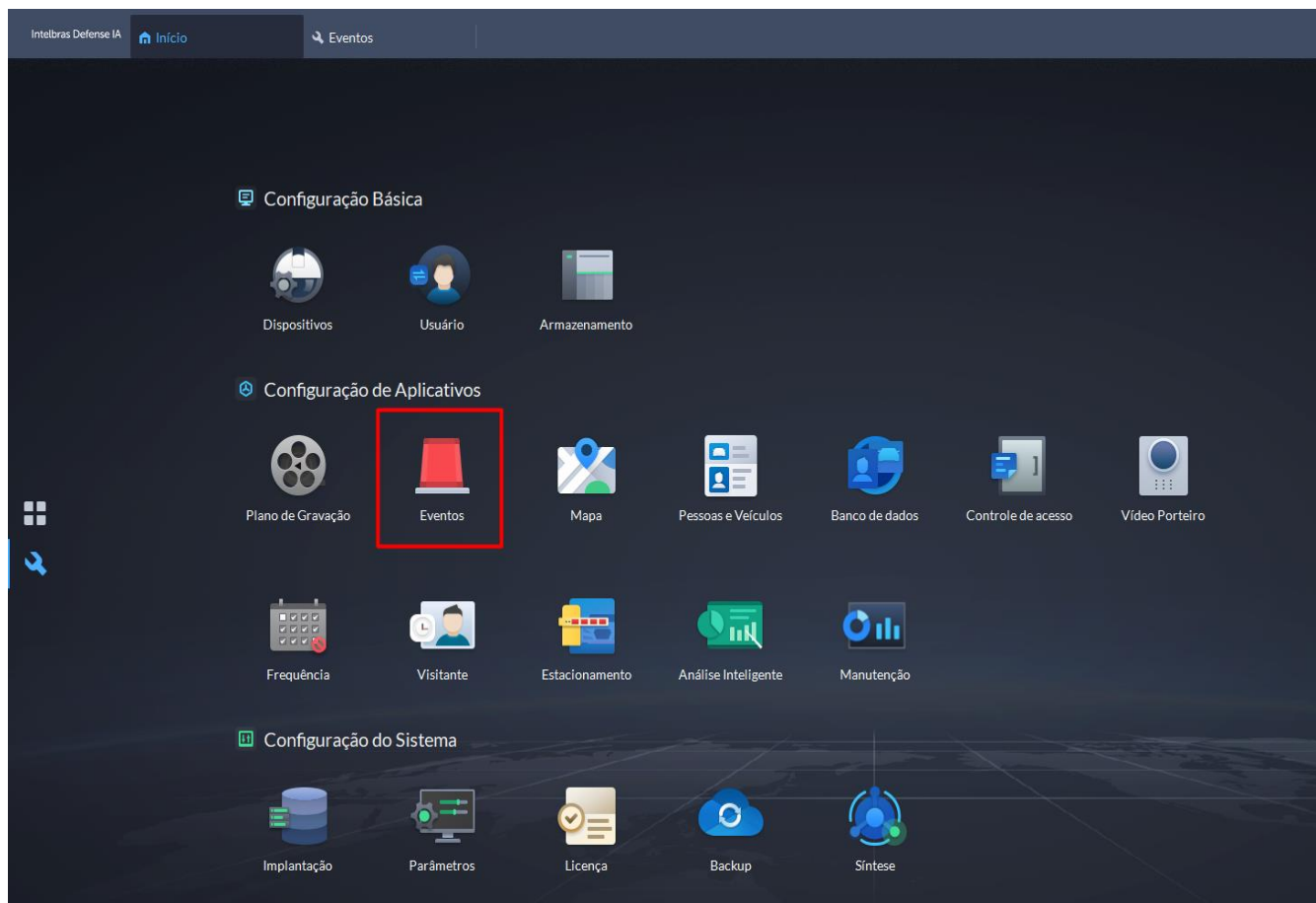
 At the bottom, there are 'Cancelar' and 'Salvar' buttons.

Pronto, central de incêndio cadastrada no Web Client.

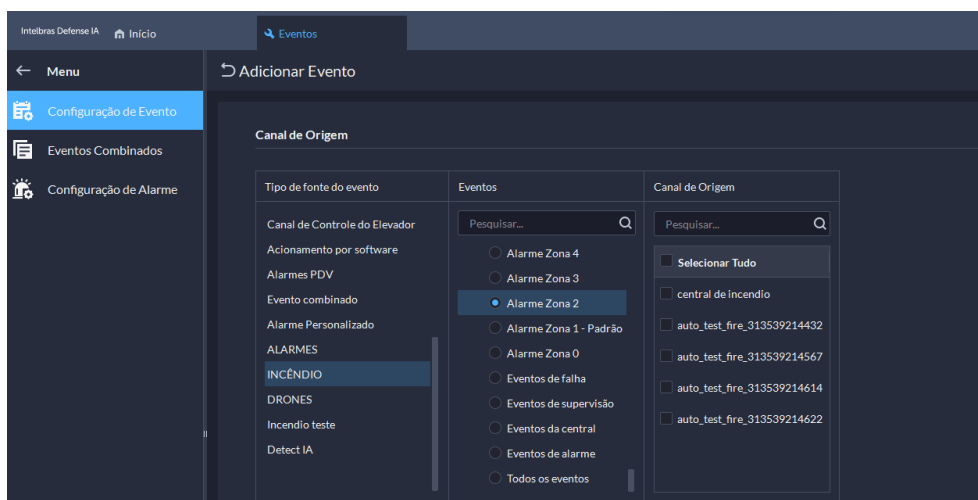


6.3. Como configurar e visualizar os eventos das centrais de incêndio

Para realizar a configuração, no menu inicial do Defense, clique em Eventos.



Após isso, em fontes de evento desça até “INCÊNDIO” e a selecione, em eventos coloque sua zona desejada e em canal de origem sua central.



Todos os eventos: Todo e qualquer evento identificado pela central de incêndio;

Eventos de Alarme: Todos os eventos de alarme da central de incêndio;

Eventos da central: Eventos da central de incêndio;

Eventos de supervisão: Eventos de supervisão de dispositivo;

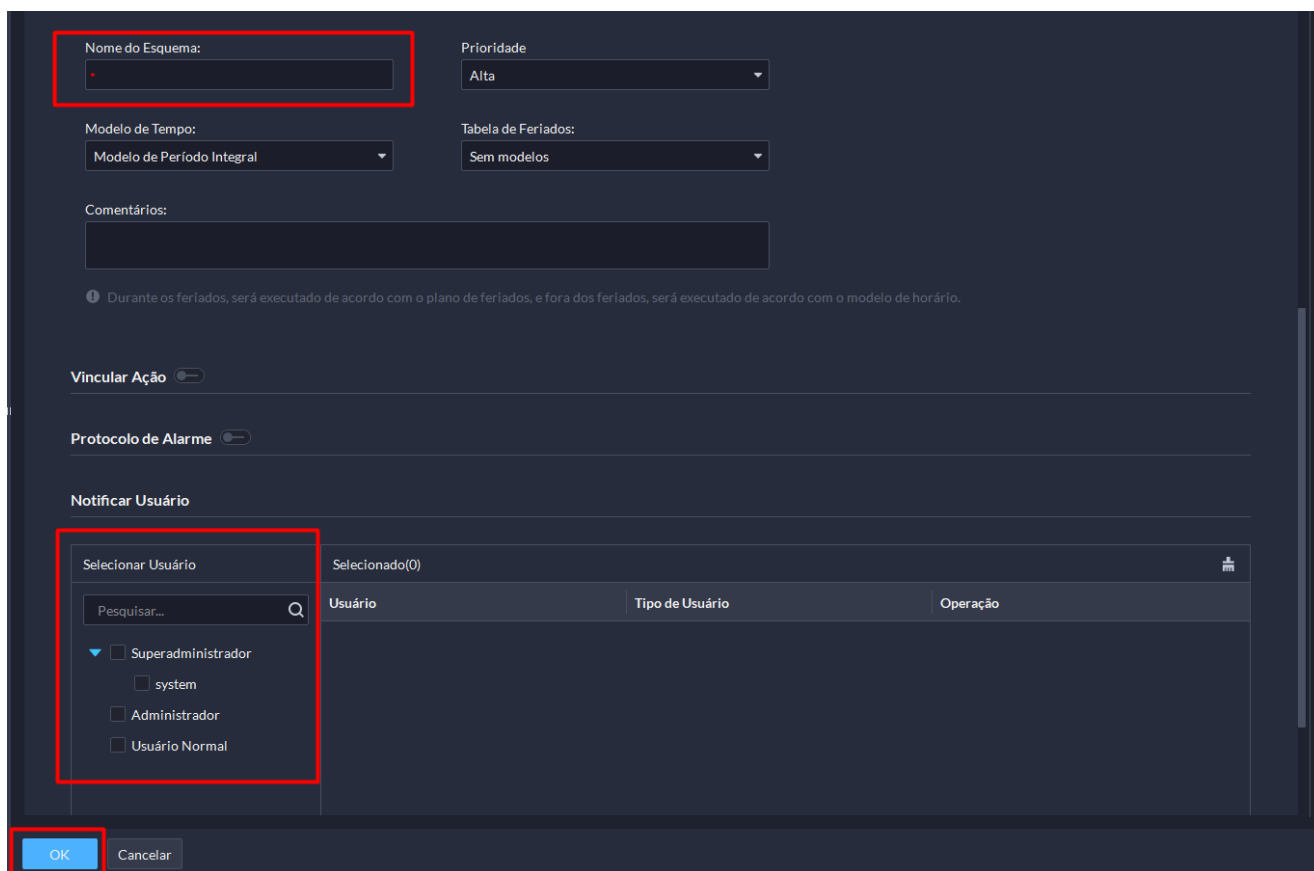
Eventos de falha: Todos e qualquer evento de falha;

Alarme de Zona 0: Evento de alarme da central;

Alarme de Zona 1: Evento de alarme da zona padrão;

Alarme de Zona 2-100: Evento de alarme das zonas da central;

Feito isso pode descer a página, nomear o esquema, definir sua prioridade e selecionar os usuários, após tudo isso só clicar em OK.



Nome do Esquema:

Prioridade: Alta

Modelo de Tempo: Modelo de Período Integral

Tabela de Feriados: Sem modelos

Comentários:

ⓘ Durante os feriados, será executado de acordo com o plano de feriados, e fora dos feriados, será executado de acordo com o modelo de horário.

Vincular Ação

Protocolo de Alarme

Notificar Usuário

Selecionar Usuário

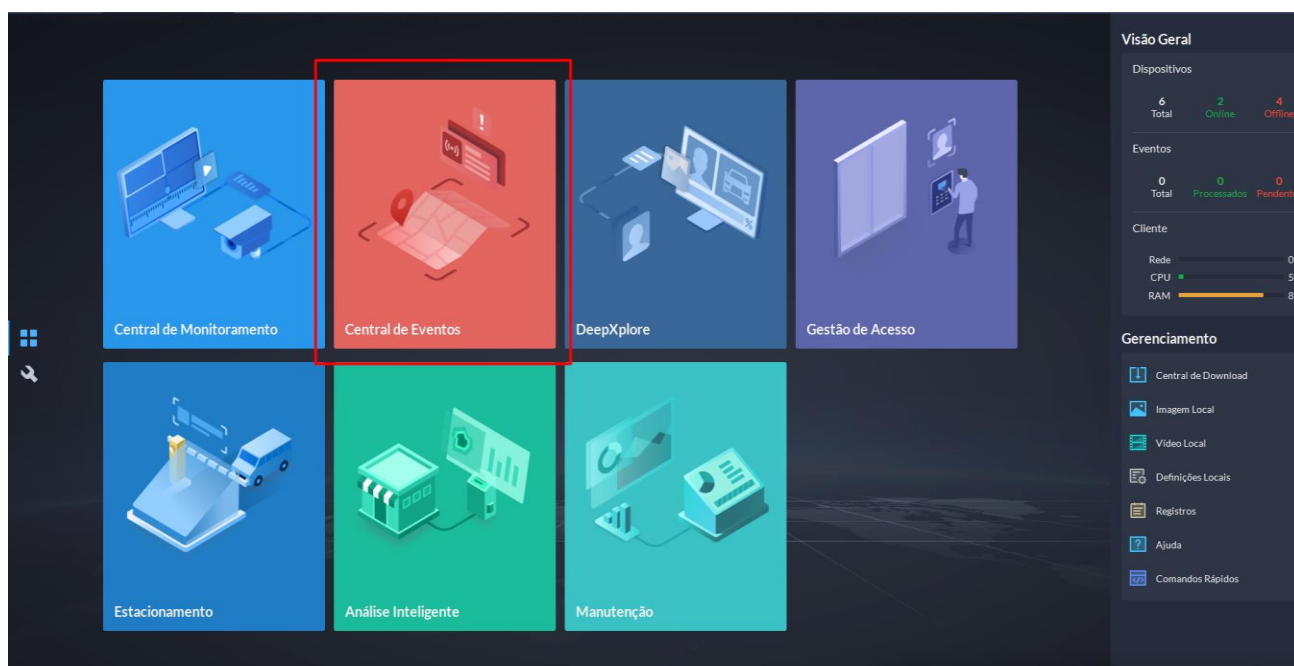
Pesquisar...

- ☒ Superadministrador
- ☐ system
- ☐ Administrador
- ☐ Usuário Normal

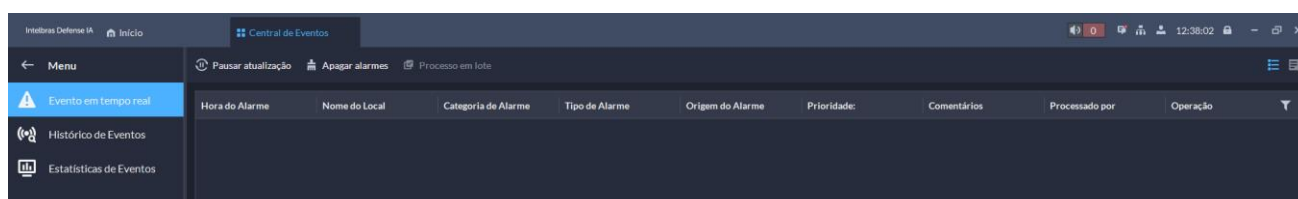
Selecionado(0)	Usuário	Tipo de Usuário	Operação

OK Cancelar

Agora para visualizar os eventos, retorne até o menu do Defense e clique em Central de eventos.



Sem eventos assim será a página.



E assim que você receber o evento ele irá notificar da seguinte forma.

