Middleware de Centrais

Manual de instalação e configuração

Intelbras Defense IA 3.2.3

Matriz: Rodovia BR 101, km 210 – Área Industrial – São José/SC – 88.104-800 – Fone: (48) 3281.9500 – Fax: (48) 3281.9505 **Filial SC**: Rodovia SC 281, Km 4,5 – Sertao do Maruim – São José/SC – 88.122-001 **Filial MG**: Rodovia BR 459, 1325, km 124 – Distrito Industrial – Santa Rita do Sapucaí/MG – 37.540-000 – Fone/Fax: (35) 3471.9840 **Filial AM**: Av. Tefé, 3105 – Japiim – Manaus/AM – 69.078-000

intelbras.com.br

Sumário

1. Intelbras Defense IA

O Intelbras 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.

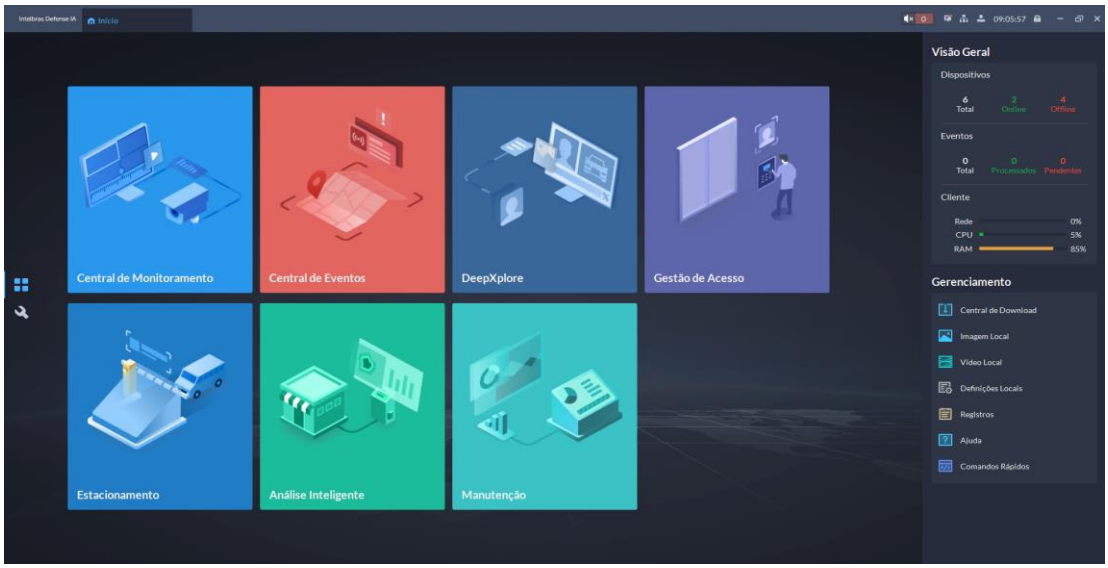


Figura 1. Intelbras Defense IA

2. Instalação do Middleware de Centrais

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

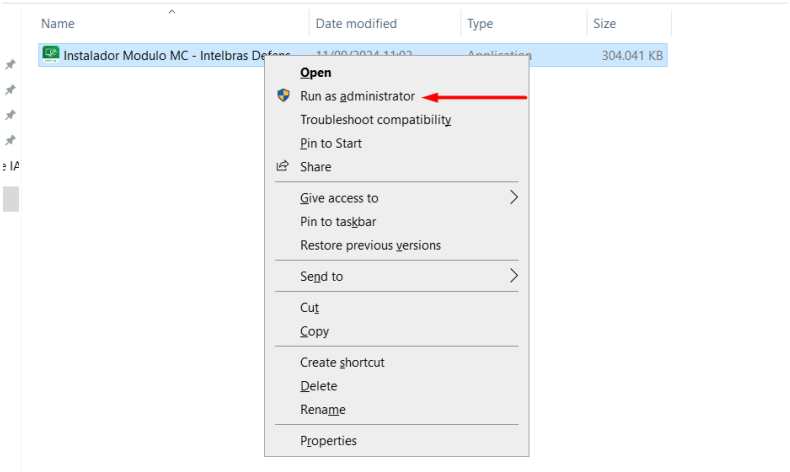


Figura 2. Executar como Administrador

Configurando o instalador:
Após executar o instalador como administrador, clique em avançar e aceite os termos de uso gerais de uso do software e nossa política de privacidade e clique em avançar.

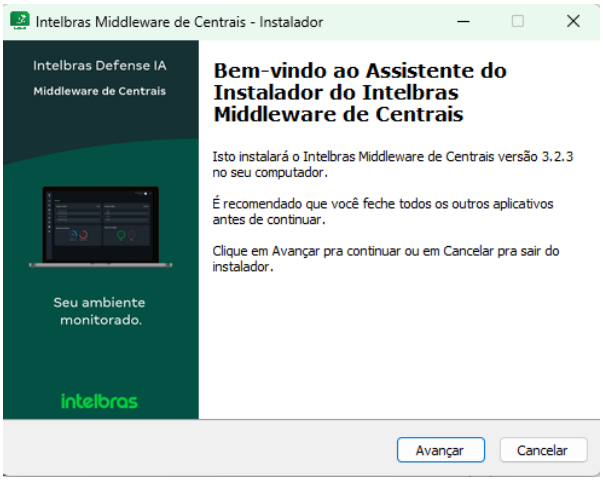


Figura 3. Assistente de Instalação do MC

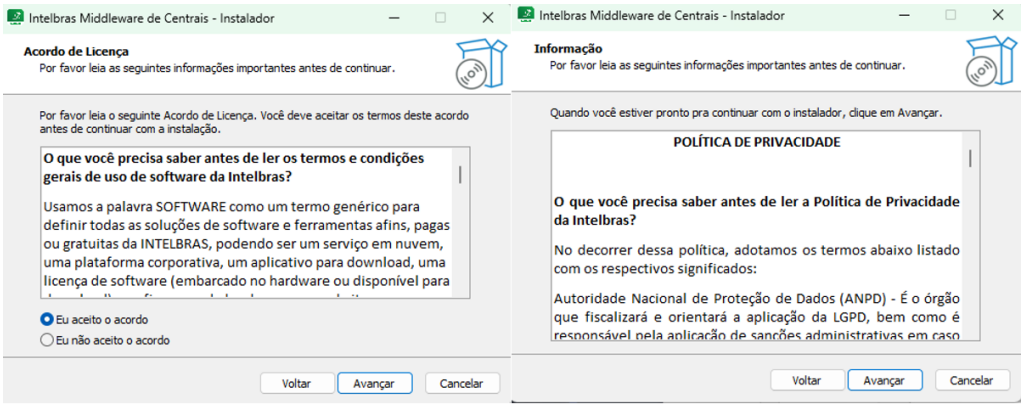


Figura 4. Termos e condições de uso

Agora escolha a pasta de instalação e avance novamente

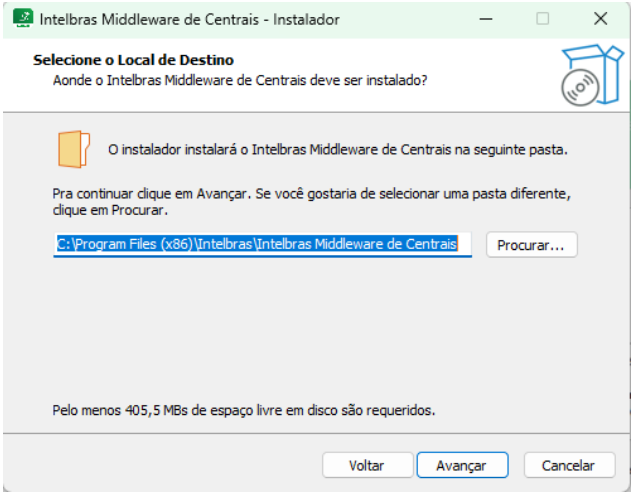


Figura 5. Caminho de instalação

Digite a senha do usuario system a qual você definiu no primeiro acesso ao client Desktop do Intelbras Defense IA e clique em Testar Conexão.

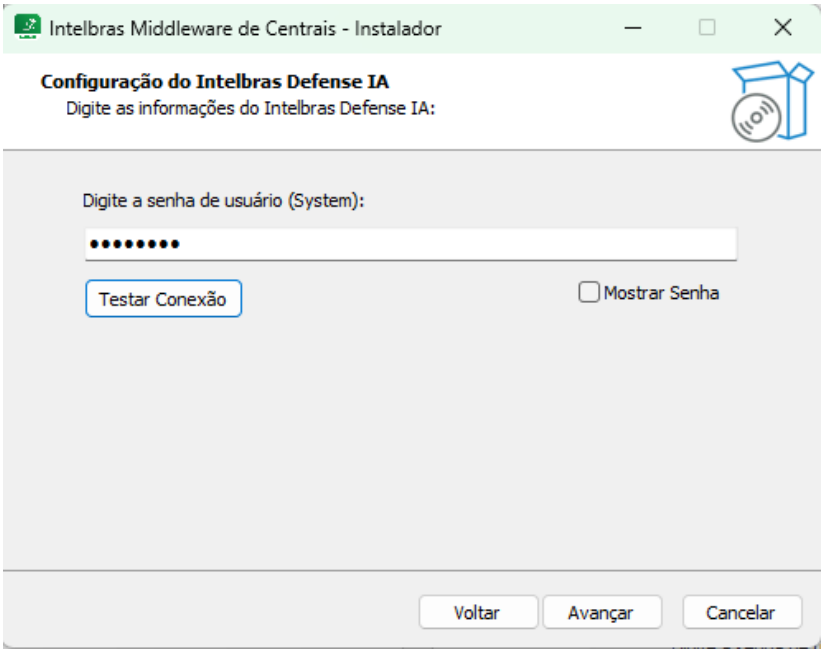


Figura 6. Senha de conexão com o Intelbras Defense IA

Só será possível avançar caso a senha esteja correta. Após validado, clique em ok e em avançar.

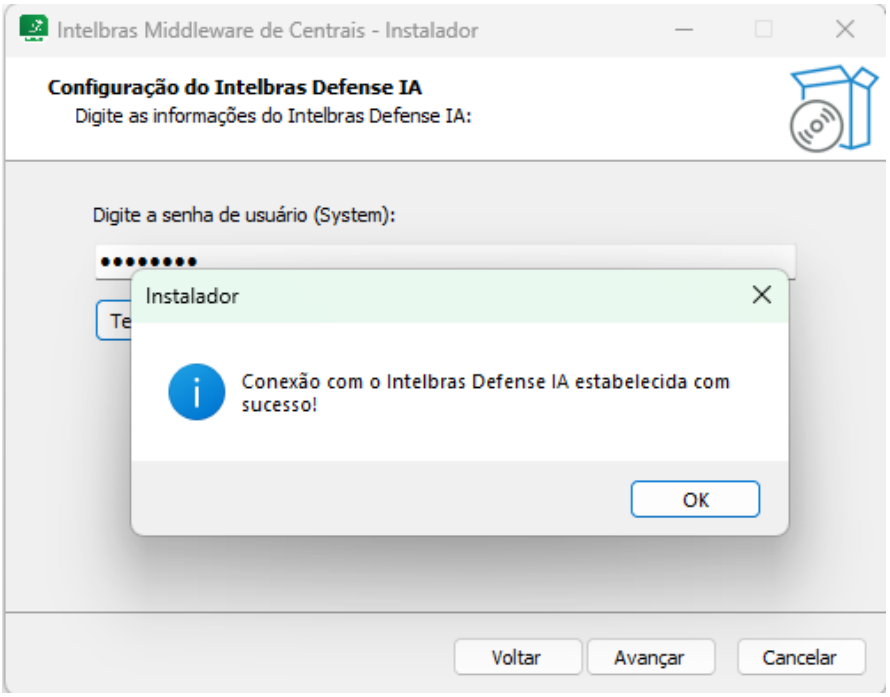


Figura 7. Conexão bem sucedida

Clique em instalar.

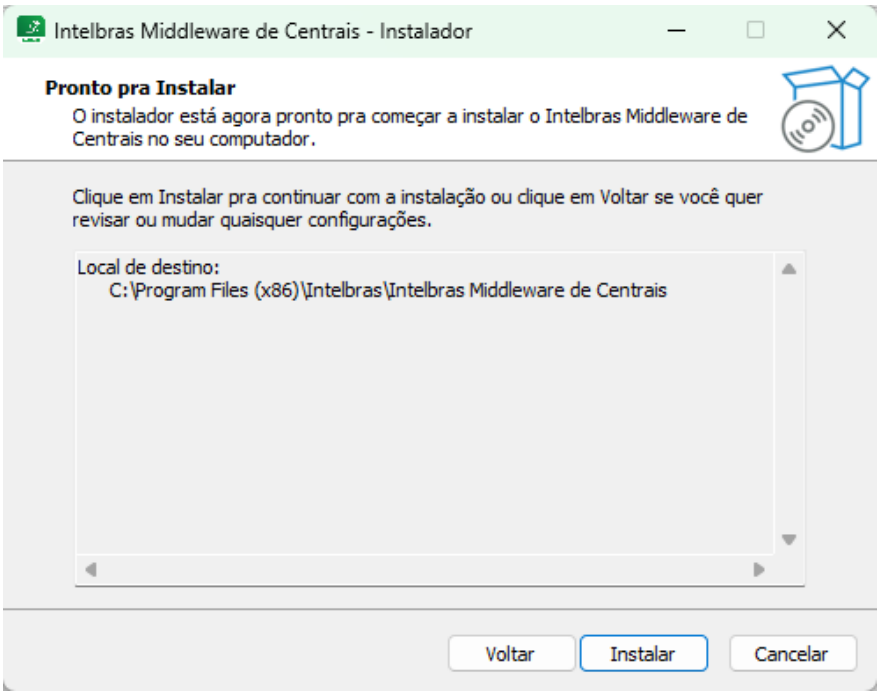


Figura 8. Iniciar instalação

A instalação será iniciada.

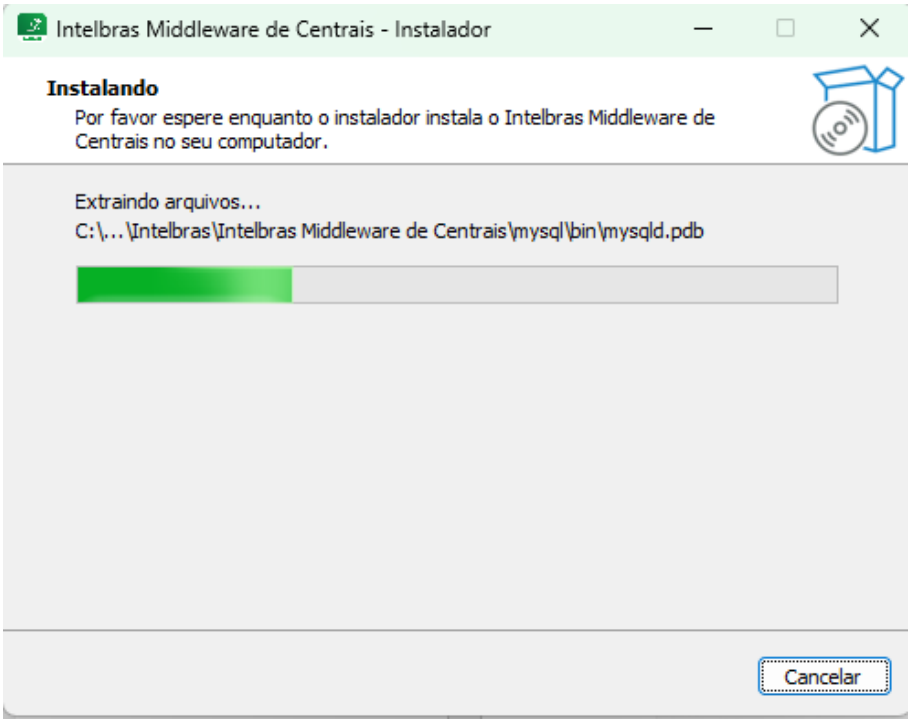


Figura 9. Progresso da instalação

Ao finalizar a instalação, será exibida as portas que serão utilizadas pelo Middleware de Centrais.

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

Caso alguma dessas portas padrão não estiverem disponíveis no servidor. O instalador tentará porta padrão + 1 até encontrar uma porta disponível.

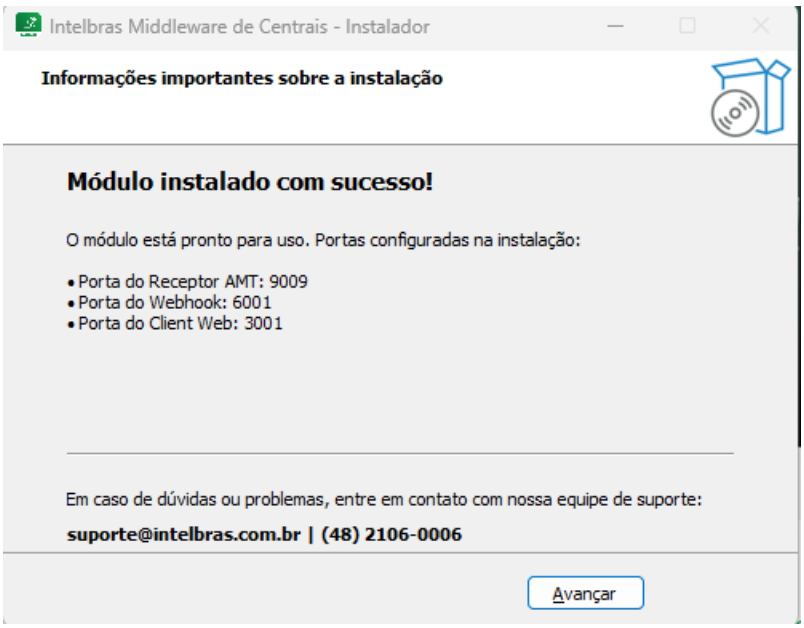


Figura 10. Informações da instalação

Após instalar com sucesso, clique em avançar e concluir e o seu Middleware de Centrais estará pronto para uso.

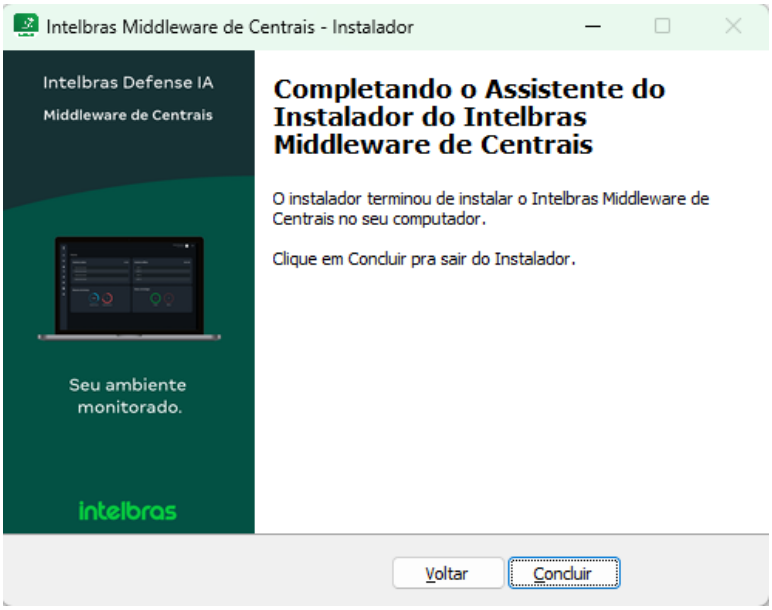


Figura 11. Concluir instalação

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 peinel de controle do seu computador.

Acesse “**Sistema e Segurança”**.

Figura 12. Painel de controle

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

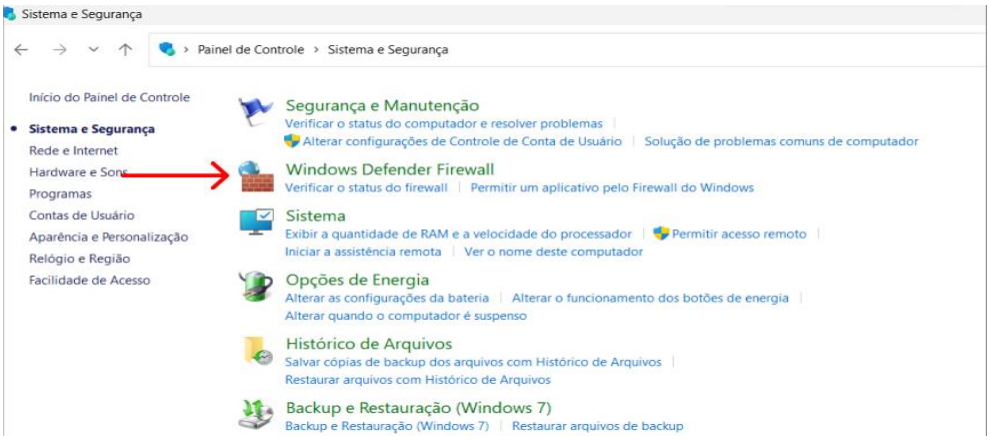


Figura 13. Windows Defender Firewall

Clique em **“Configurações Avançadas”**.

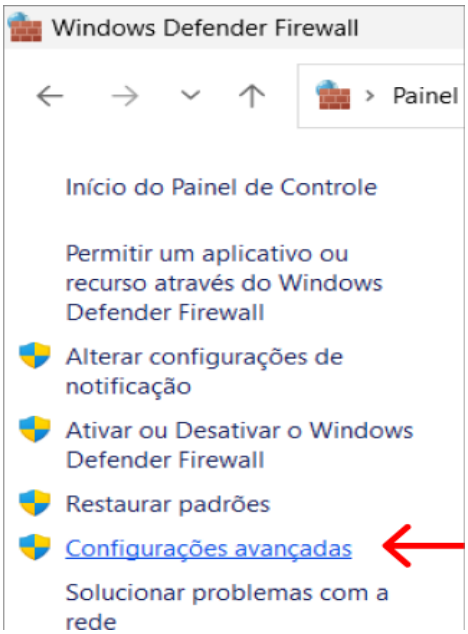


Figura 14. Configurações avançadas

Clique em **"Regra de entrada"**.

Figura 15. Regras de Entrada

Agora verifique se foi criada a regra **"Defense_MC"**.

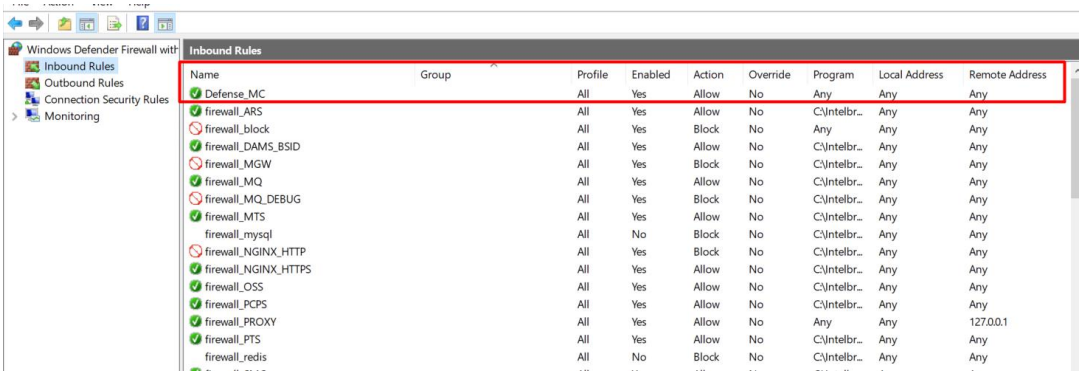


Figura 16. Regra de entrada Defense_MC

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

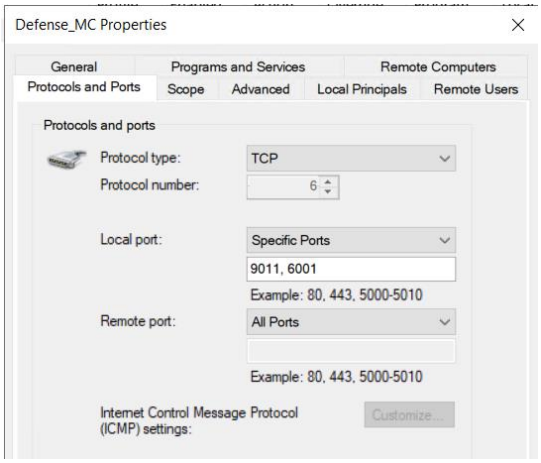


Figura 17. Portas liberadas

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.

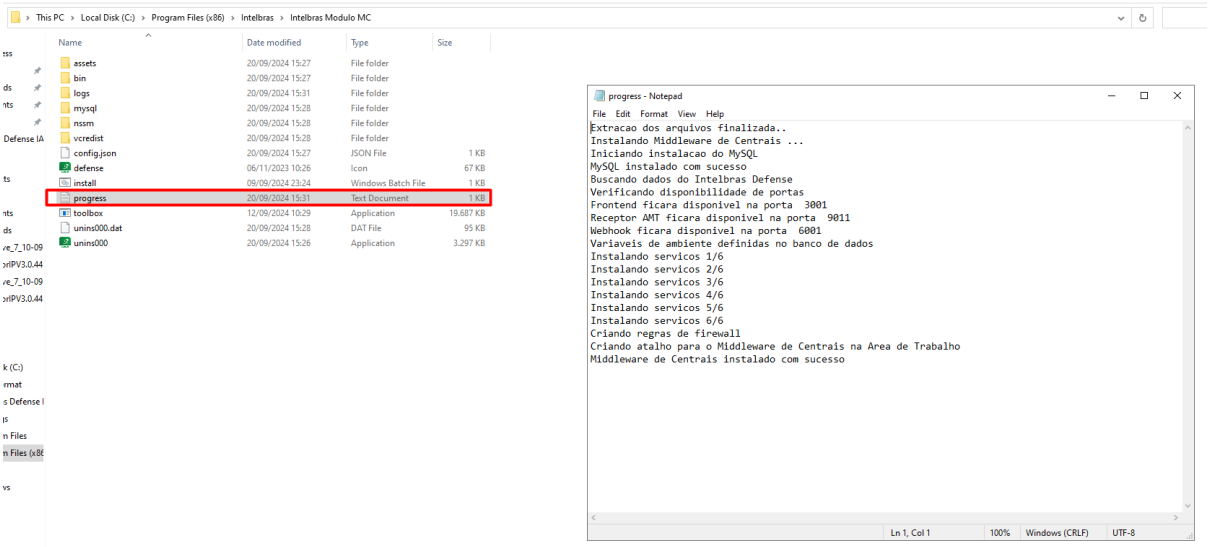
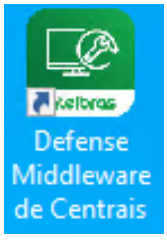


Figura 18. Consulta de portas de comunicação

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.



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

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

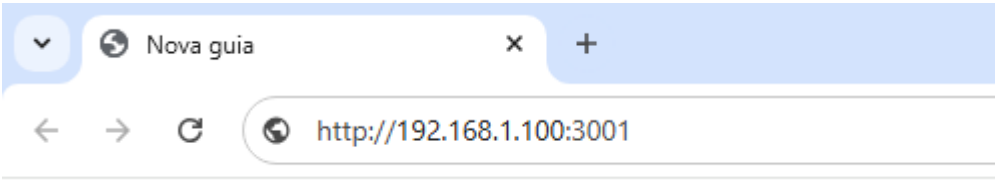


Figura 19. Exemplo de link para acesso ao web client

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

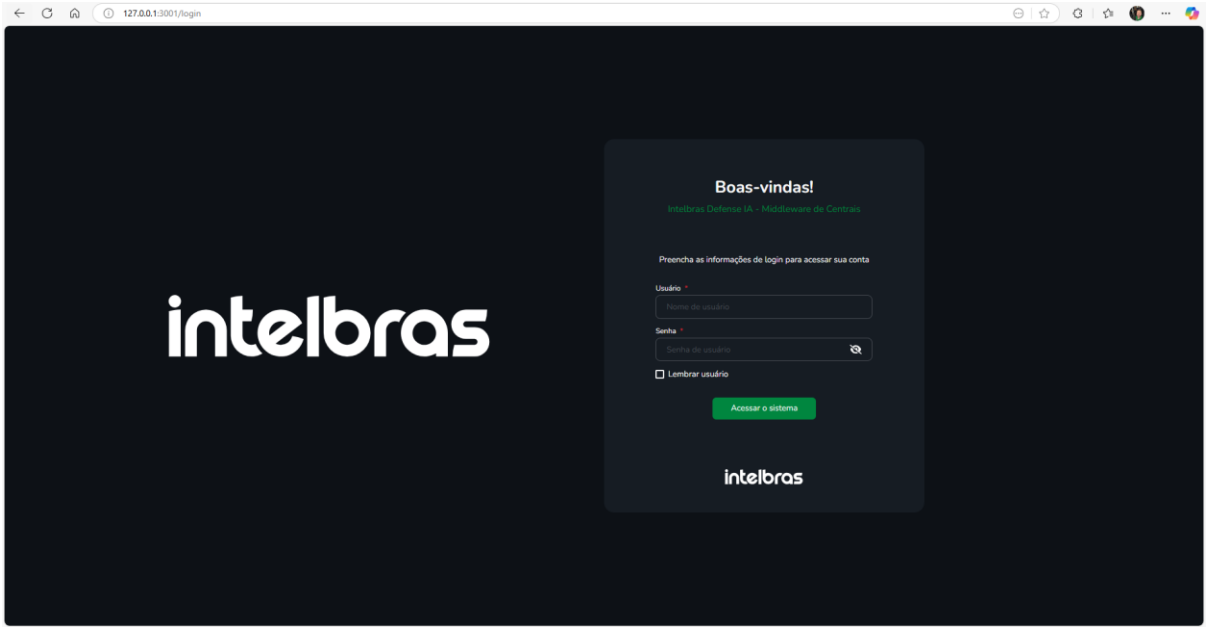


Figura 20. Login Middleware de Centrais

5. Menu Início

A tela inicial do Middleware de Centrais exibe um resumo de algumas informações importantes do sistema.

O primeiro quadrante exibe a lista das centrais de alarme de intrusão e alarme de incêndio online. O segundo quadrante a lista das centrais offline. O terceiro quadrante informa o consumo de licença disponíveis. E o último quadrante exibe o status de online/offline dos Bridges.

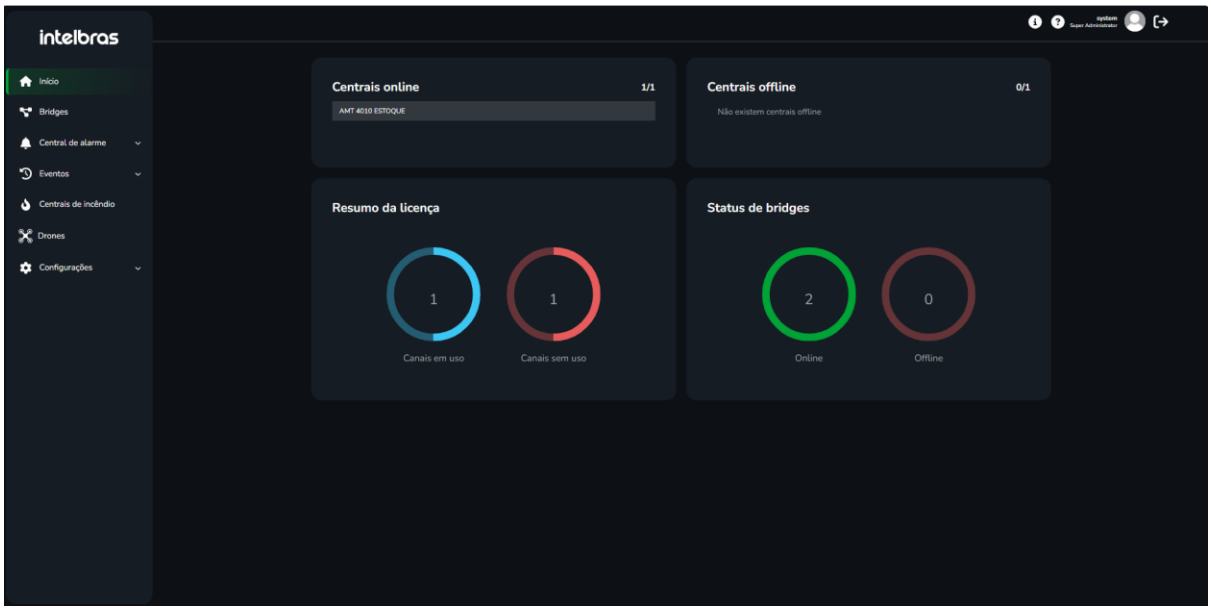


Figura 21. Menu Início

Na barra de ações superior, há o botão onde é possível consultar tanto a versão do Intelbras Defense IA a qual o Middleware de Centrais está conectado quanto a versão do Middleware de Centrais.

No botão o usuário será redirecionado à página do Intelbras Defense IA onde poderá consultar diversas informações inclusives manuais de usuário de todas as ferramentas.

Há também a exibição de qual usuário está logado naquele momento com uma descrição de sua permissão dentro do sistema (Super Administrador, Administrador ou Operador).

Por fim, o botão de logout .

Para acessar as outras funções do sistema, utilize a barra lateral esquerda.

6. Centrais de Alarme de Intrusão

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 Intelbras Defense IA.

Figura 22. AMT 4010 SMART

6.1. Configuração prévia de uma central de alarme

Para correta comunicação da central de alarme de intrusão Intelbras com o software Intelbras 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 Addres 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

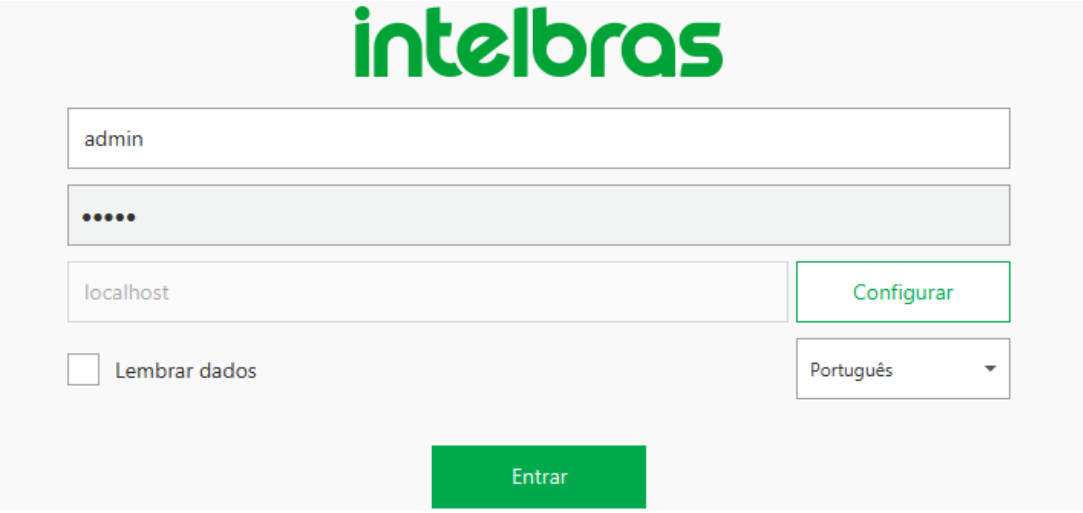


Figura 23. Login AMT Remoto

No Painel do Instalador, **clique em ‘’Meus Clientes’’:**

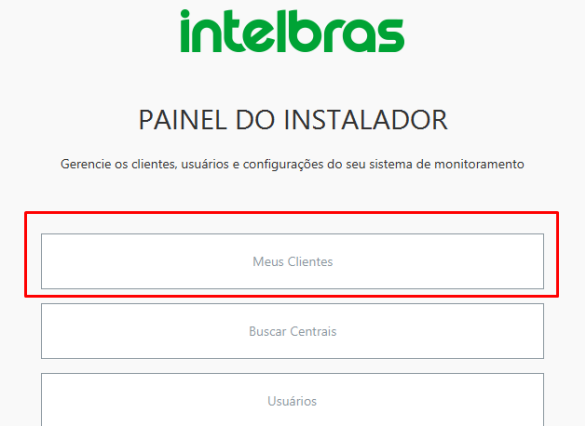


Figura 24. Acesso aos Meus Clientes

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

Figura 25. Adicionar Cliente

Abrindo a página de clientes, o primeiro passo será **identificar a sua central** com um nome amigavel**:**
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);**

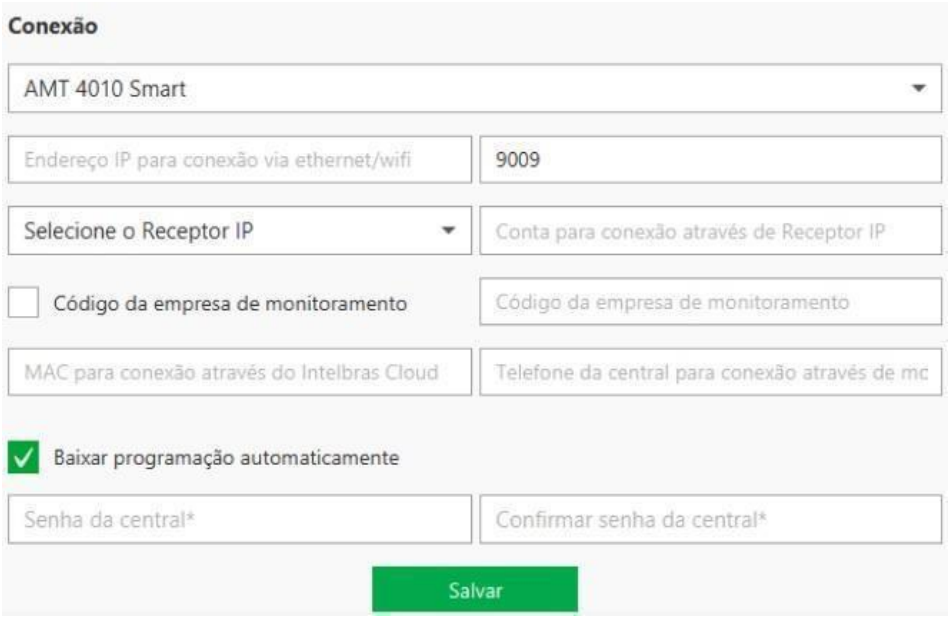


Figura 26. Configurações de conexão

Após configurar sua central e retornar ao menu principal, clique em **''Conectar''** e selecione a opção para realizar conexão através de Ethernet (caso a central esteja na mesma rede), assim será possível configurar a central de forma remota.

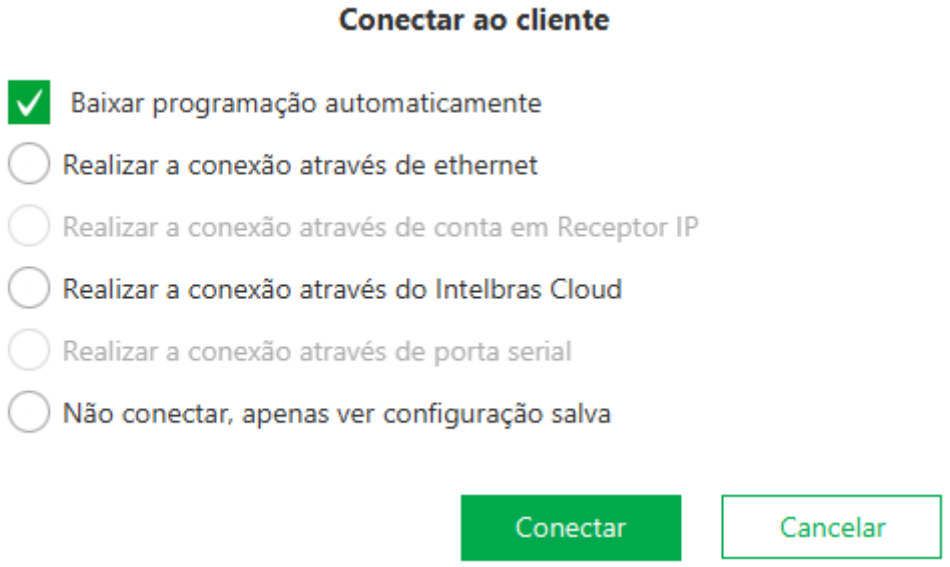


Figura 27. Conectar à AMT

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.

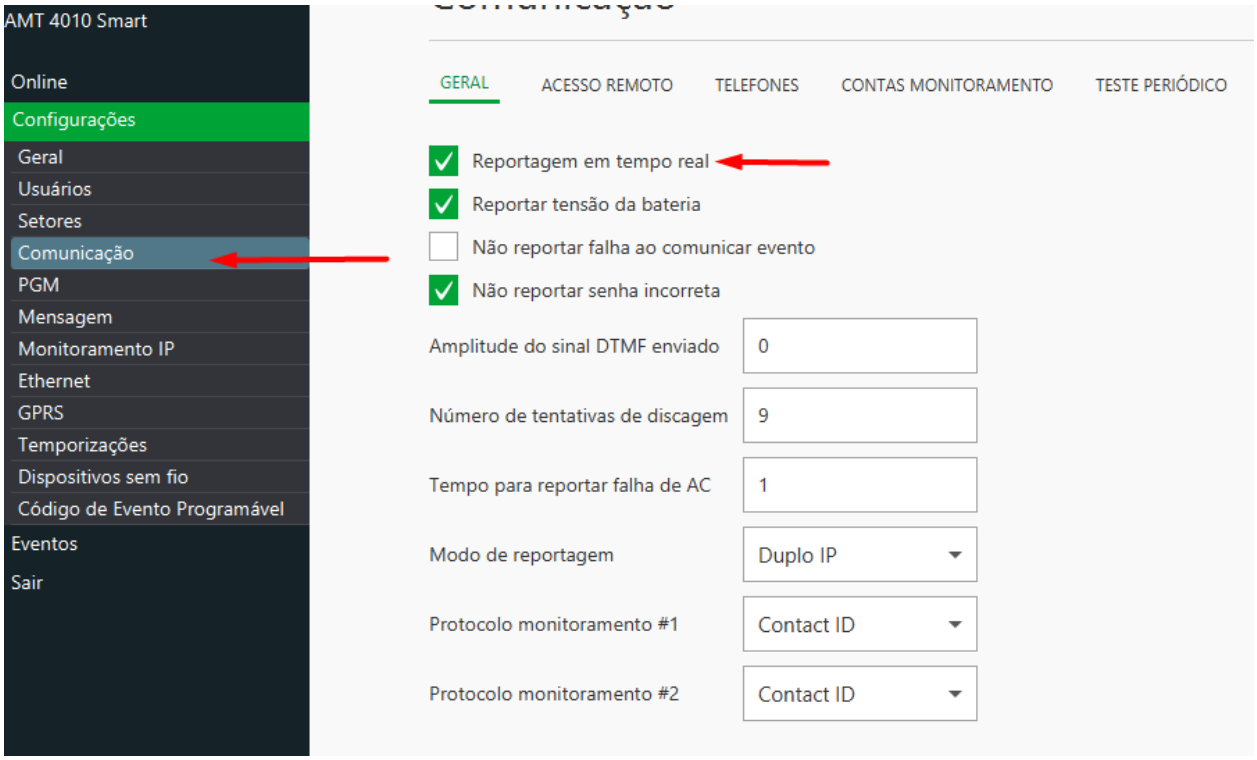


Figura 28. Aba comunicação

Depois, acesse as configurações disponíveis em **Monitoramento IP**:

Na configuração do Servidor 1 em Monitoramento IP, **defina o endereço IP correspondente ao seu servidor do Intelbras 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.

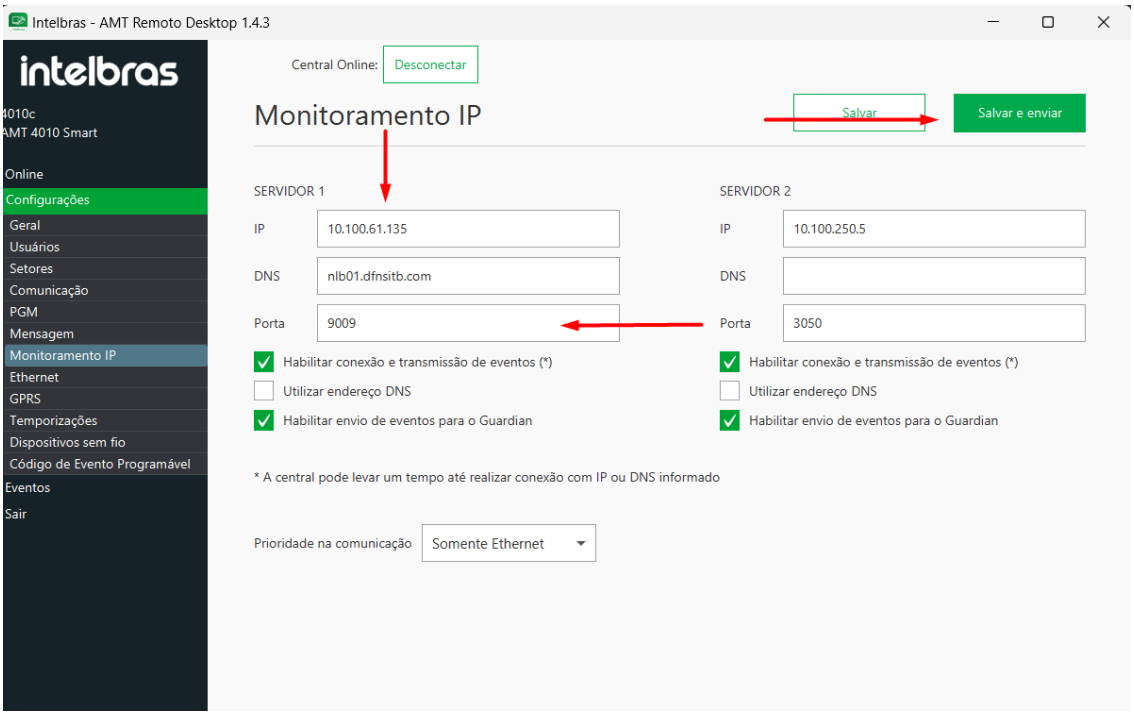


Figura 29. Monitoramento IP

Por último, na aba Ethernet, altere o tempo de keepalive da central para **1** minuto.

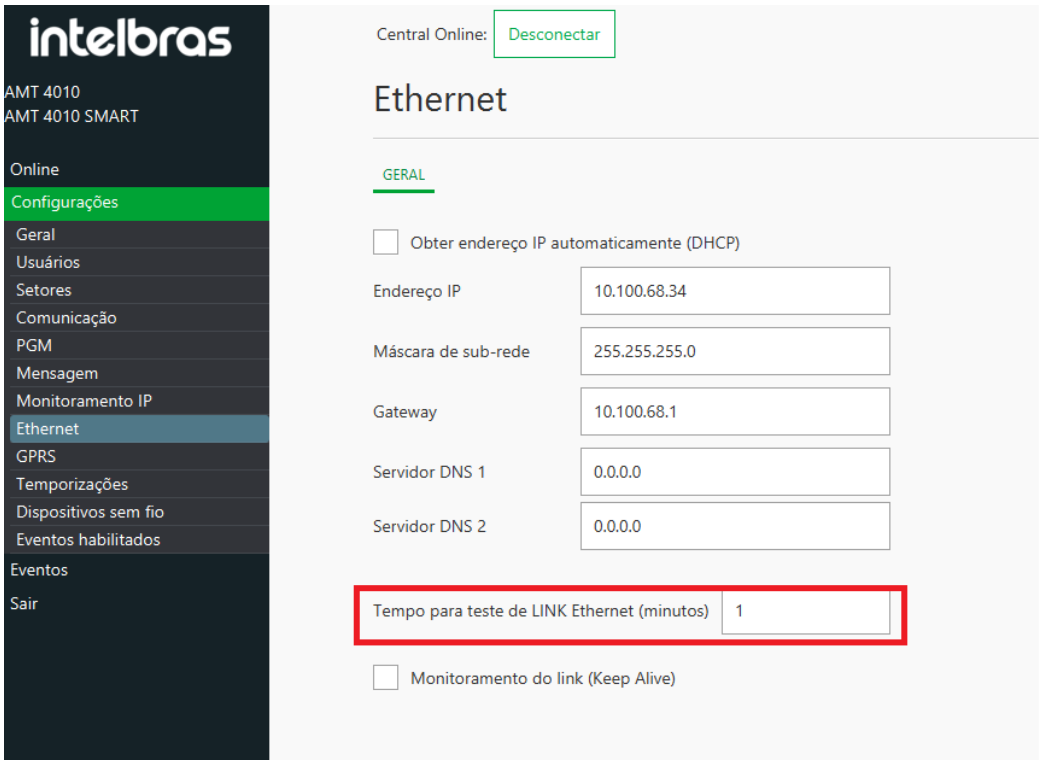


Figura 30. Configuração do keepalive

Após isso sua central de alarme estará configurada.

Lembre-se de desconectar o AMT Remoto da central de alarme para que você consiga adicionar a central ao middleware de centrais.

Não é possível receber eventos no Intelbras Defense IA utilizando a comunicação GPRS disponível nas centrais de alarme de intrusão.

6.2. 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 de intrusão 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 Intelbras Defense IA.

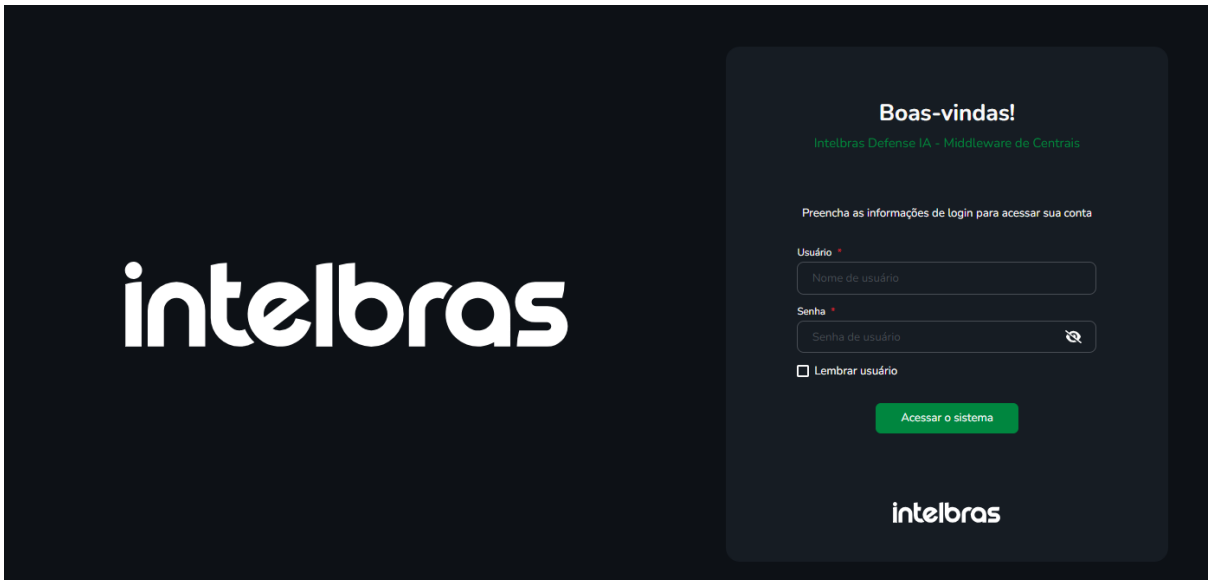


Figura 31. Tela de login

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 desktop client do Intelbras Defense IA. Acesse o menu "**Bridges**" no menu lateral esquerdo.

Figura 32. Lista de conexões Bridges

Caso o bridge esteja **offline**, verifique se os serviços do Intelbras Defense IA Server estão em execução. Se algum serviço estiver parado, tente inicialo. Se não for possível iniciar o serviço ou todos já estiverem em execução e mesmo assim os bridges estão offline, entre em contato com o suporte.

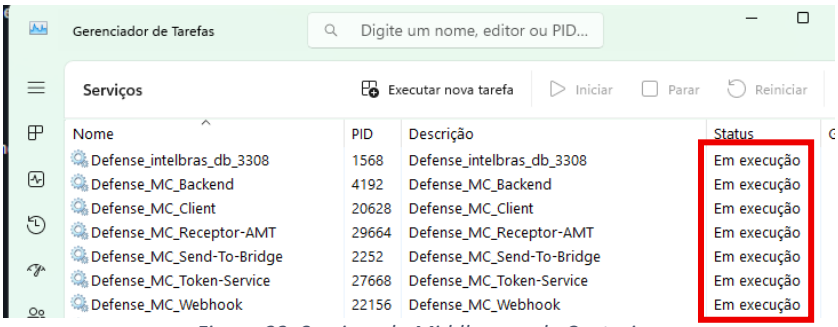


Figura 33. Serviços do Middleware de Centrais

Após realizar a verificação, prossiga para o cadastro da central de alarme de intrusão. Clique em "**Central de alarmes**" na barra lateral e em "**Central, Partição e Zonas**" e clique em "**Nova Central**".

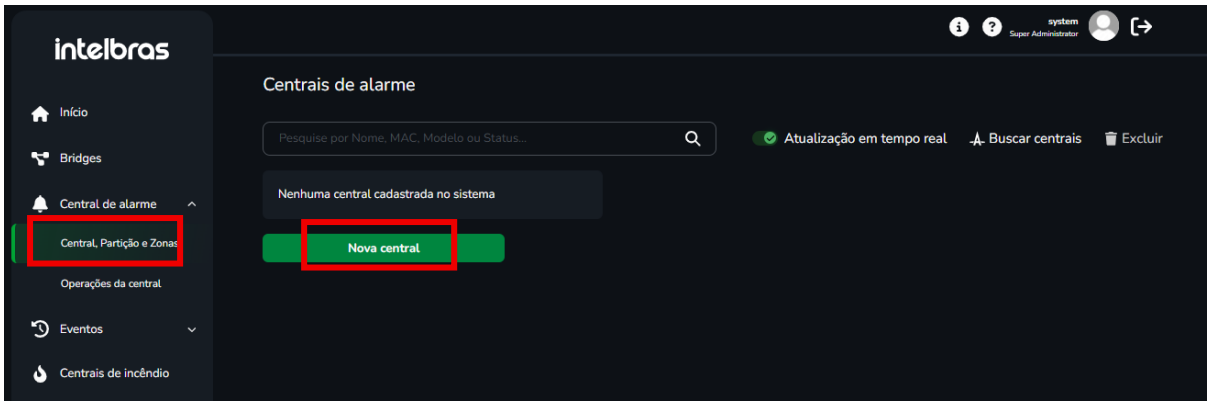


Figura 34. Nova central de alarme de intrusão

Preencha com as informações corretas e clique em salvar.

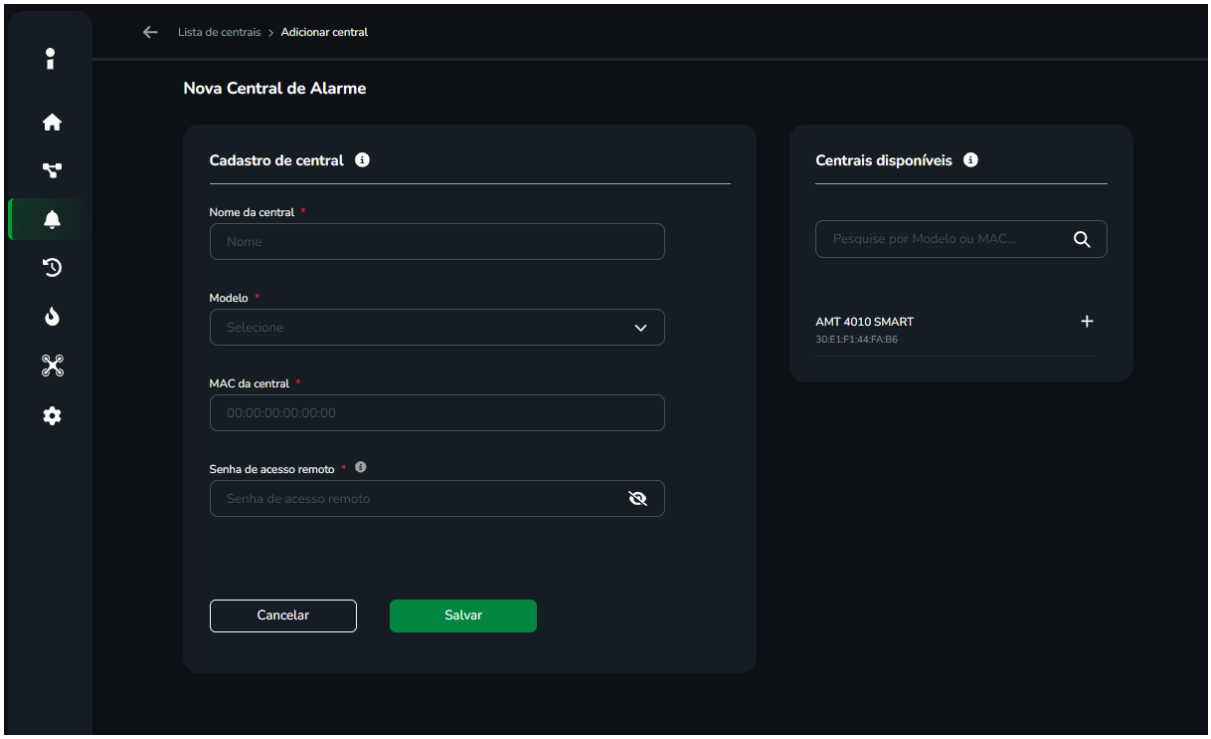


Figura 35. Adicionando central de alarme de intrusão

Note que caso alguma central de alarme de intrusão já tenha sido configurada préviamente de maneira correta (reportando eventos para o servidor do Intelbras Defense IA) ela irá aparecer na janela a direita como uma central disponível. Nesse caso, é possível apenas clicar no botão + que as informações desta central serão preenchidas na janela de cadastro de central a esquerda.

Ao adicionar a central de alarme de intrusão, ela tentará fazer o sincronismo das partições e zonas e manterá o status "**Registrando**" até que uma comunicação seja totalmente estabelecida. Caso não seja possível, a central irá informar uma falha de sincronismo e poderá ficar offline. Caso a conexão seja estabelecida, a central ficará online de forma automática. Com a central online é possível refazer o sincronismo a qualquer momento.

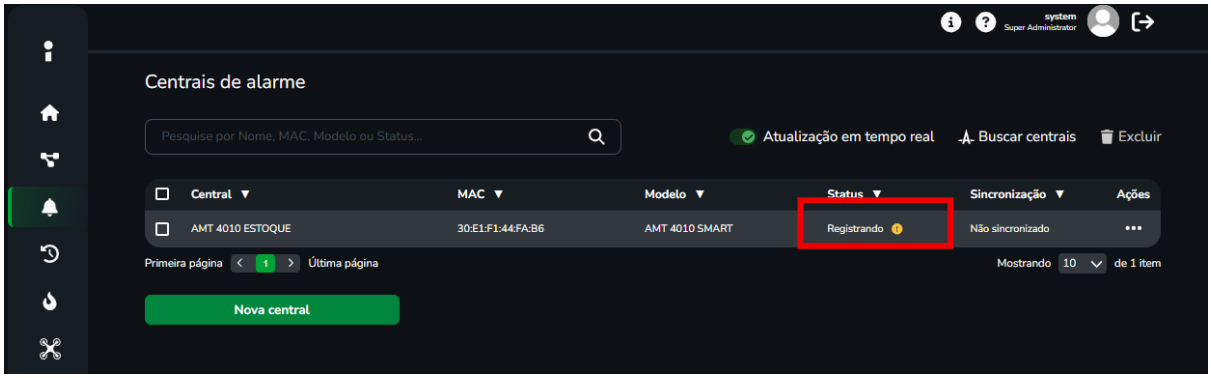


Figura 36. Status Registrando

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.

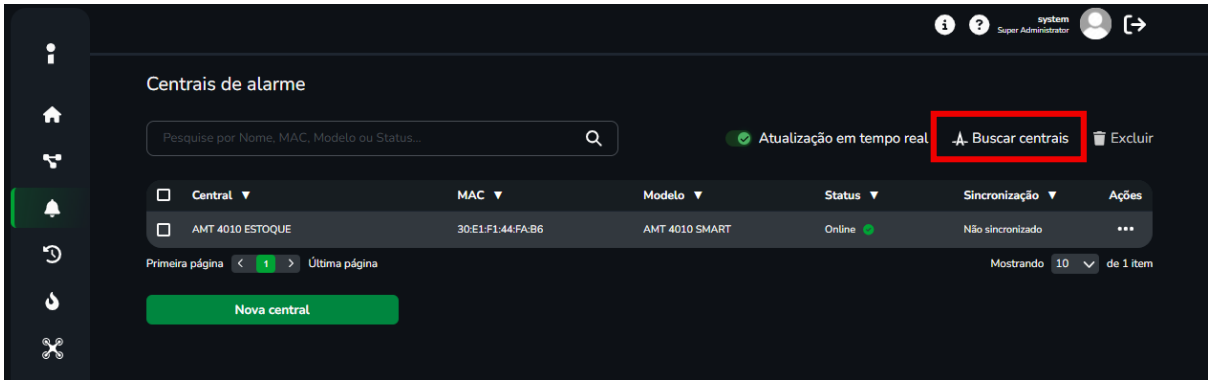


Figura 37.Acesso a função Buscar centrais

Na tela de buscar centrais de alarme de intrusão, escolha as opções de faixa de rede que se deseja realizar a busca. É possível realizar a busca por centrais na mesma faixa de rede do próprio servidor ou em uma faixa de rede /24 desejada.

Figura 38. Buscar centrais

Após escolher as faixas de rede desejadas, clique em buscar. O sistema irá fazer uma busca na rede e listar as centrais de alarme de intrusão encontradas.

Centrais já adicionadas também serão listadas, bloqueando o recadastro.

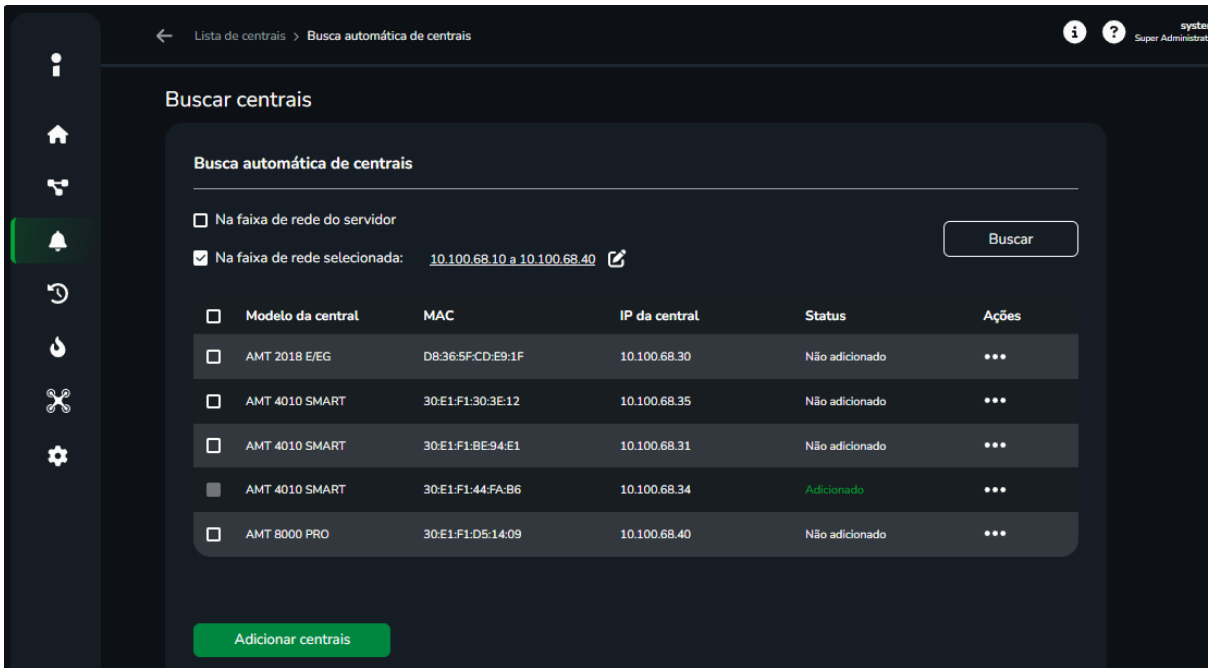


Figura 39. Centrais encontradas

Selecione através dos checkbox quais centrais deseja adicionar e clique em "**Adicionar centrais**" na parte inferior da tela. Será aberta uma janela exigindo a senha de acesso remoto das centrais. A mesma senha será aplicada para **todas** as centrais. Então só adicione em lote centrais de alarme de intrusão que possuam a mesma senha de acesso remoto.

6.3. Como sincronizar uma central de alarme de intrusão

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

particionamento e/ou zona seja feito diretamente na central de alarme, é necessário voltar nesse menu e fazer a sincronização novamente.

Para sincronizar, abra a pagina das centrais de alarmes. Clique no botão ações, e seleciona a opção de **“Sincronizar central”.**

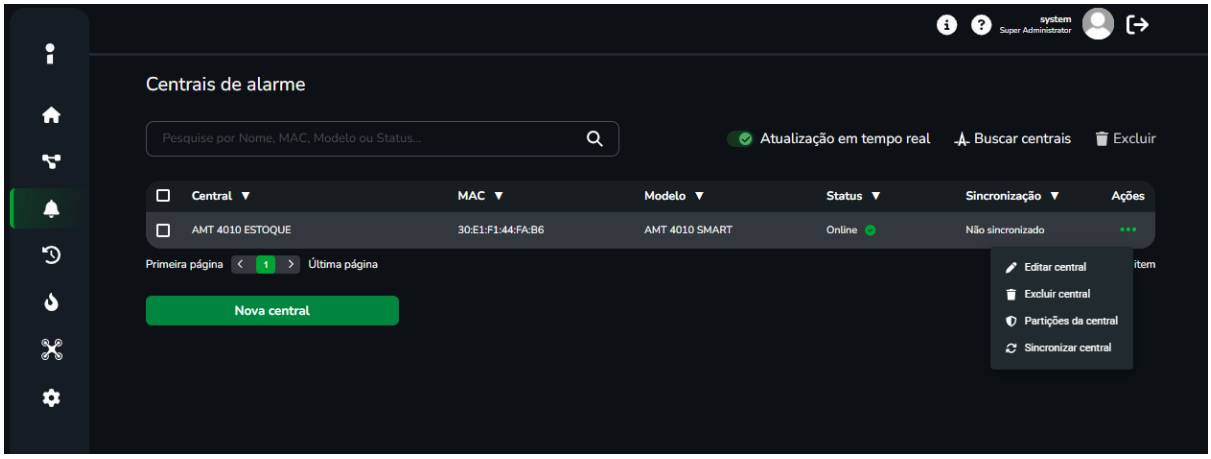


Figura 40. Sincronizar central AMT

Uma mensagem de confirmação será exibida caso a operação tenha sucesso. Só é possível realizar o sincronismo caso a central esteja online.

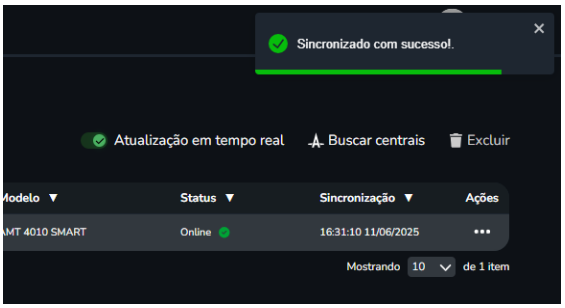


Figura 41. Central AMT sincronizada

6.4. Configurando partições e zonas via Web Client

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

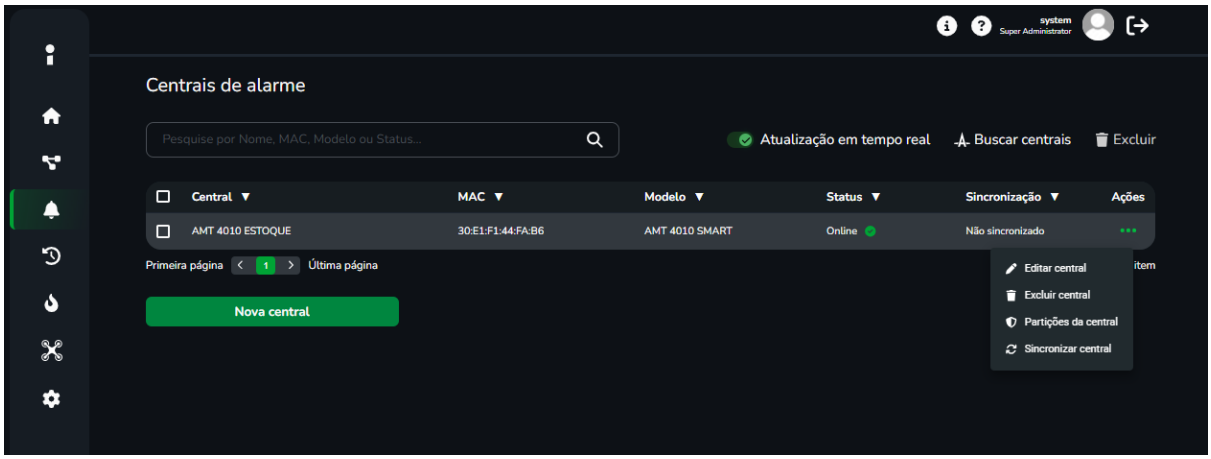


Figura 42. Acessando Partições da central

Para adicionar uma partição clique em + Adicionar.

Figura 43. Lista de partições

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

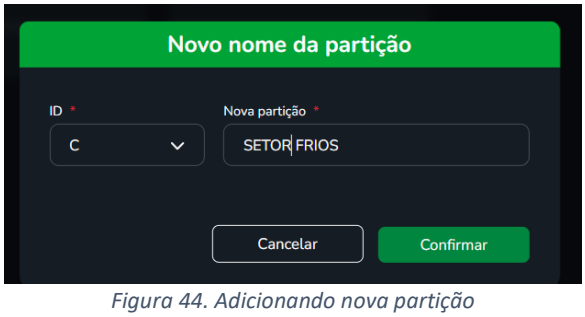


Figura 44. Adicionando nova partição

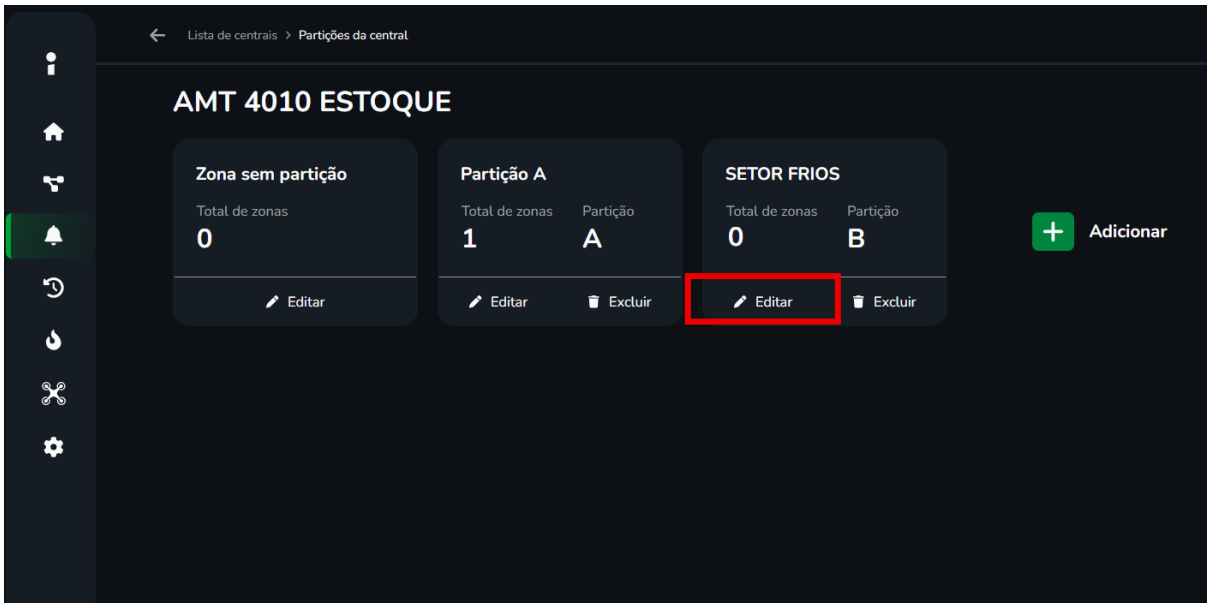


Figura 45. Configurando partição

Ao abrir uma partição é possível editar o seu nome caso necessário.

Figura 46. Editar nome da partição.

Agora para adicionar zonas a uma partição, de volta a listagem de partições, clique em **editar** na partição desejada. Será aberta a tela de configuração de zonas da partição escolhida.

Para adicionar uma nova zona, escolha qual o número da zona e dê um nome amigavel. Para confirmar clique em no botão +.

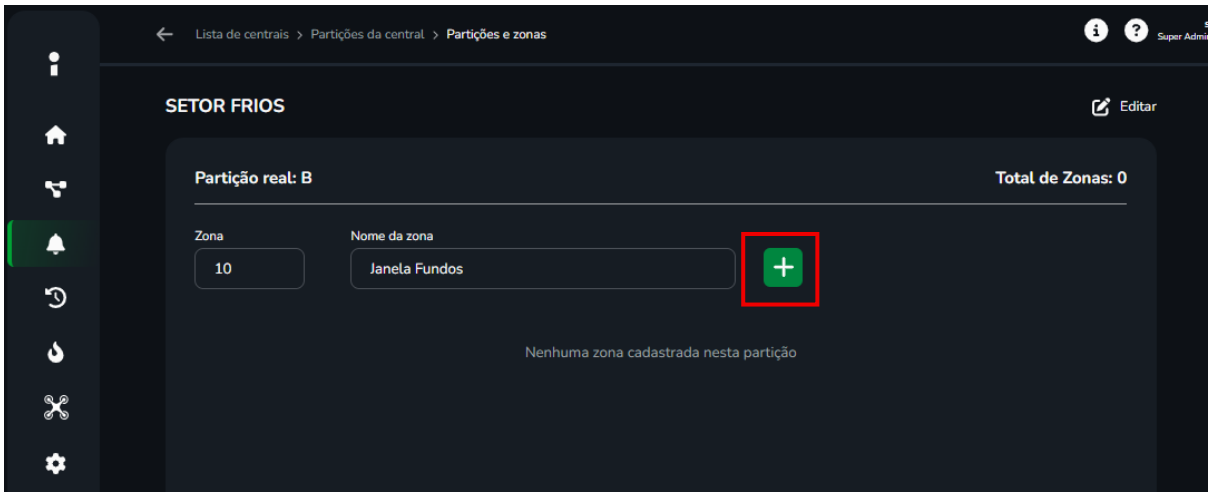


Figura 47. Nomeando nova zona

Após adicionar a zona, é possível fazer configurações pertinentes ao comportamento desta zona.

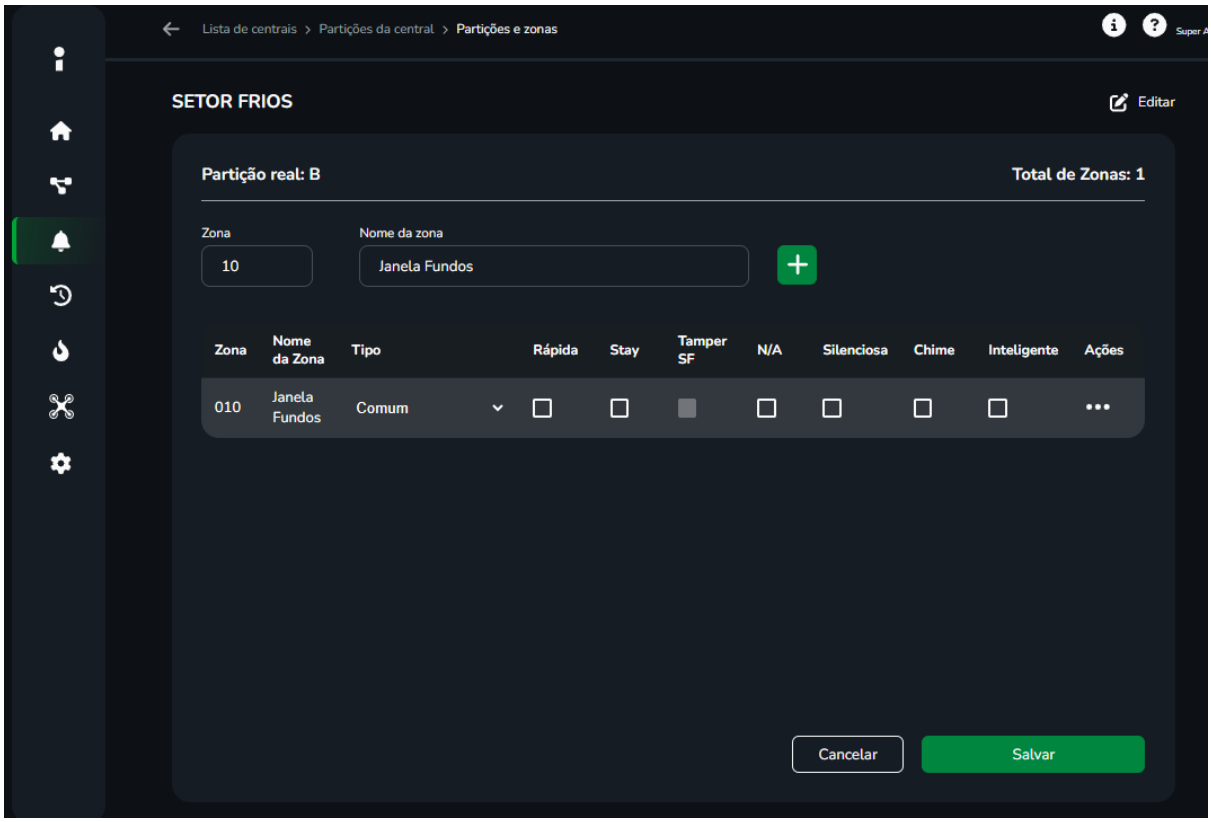


Figura 48. Configurando nova zona

Ao finalizar as configurações de cada zona adicionada, clique em salvar. Zona adicionadas serão habilitadas na central de alarme. O nome dado a zona neste momento permitirá identifica-la em operações futuras (operação de bypass e recebimento de eventos).

No botão ••• na coluna ações é possível editar o nome de uma zona ou excluí-la desta partição. Ao excluir uma zona ela é **desabilitada** e pode ser adicionada novamente em outra partição.

Ao salvar as configurações, estas 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.

6.5. Como operar uma central de alarme

Para armar e desarmar uma central é necessário ir até a página **"Operações da central"**.

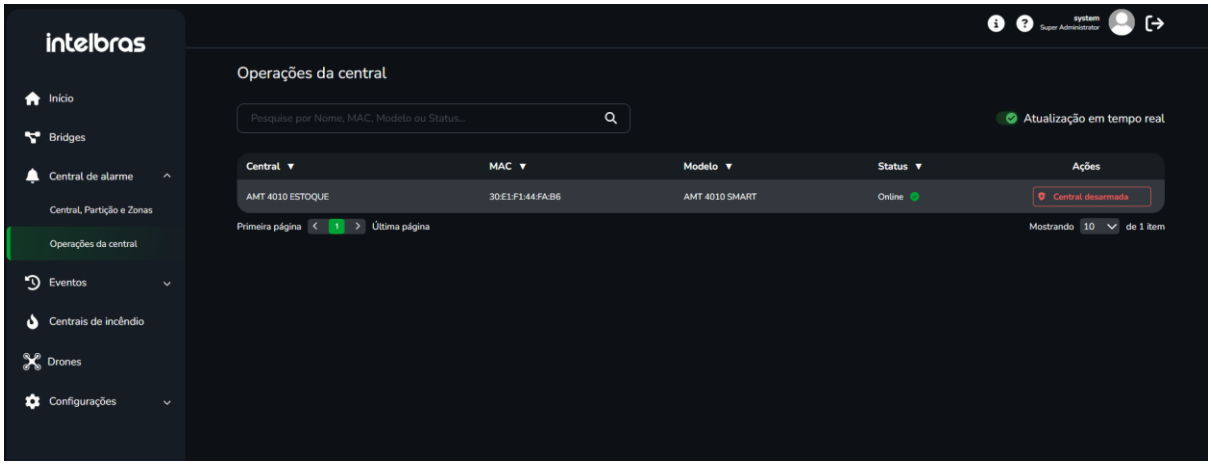


Figura 49. Operações da central

Neste menu será possível operar a central ao clicar no botão de **Ações** e selecionar **Armar central** (é necessário que a central esteja online).

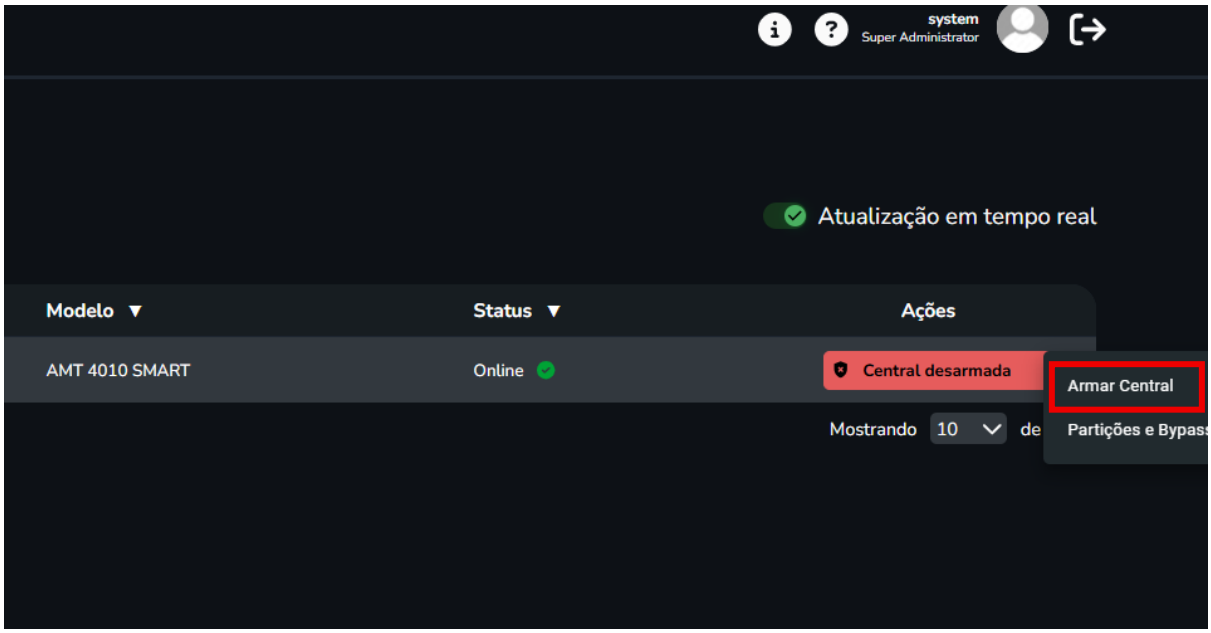


Figura 50. Armar central por completo

Será exibido uma mensagem de **"Central armada com sucesso"**.

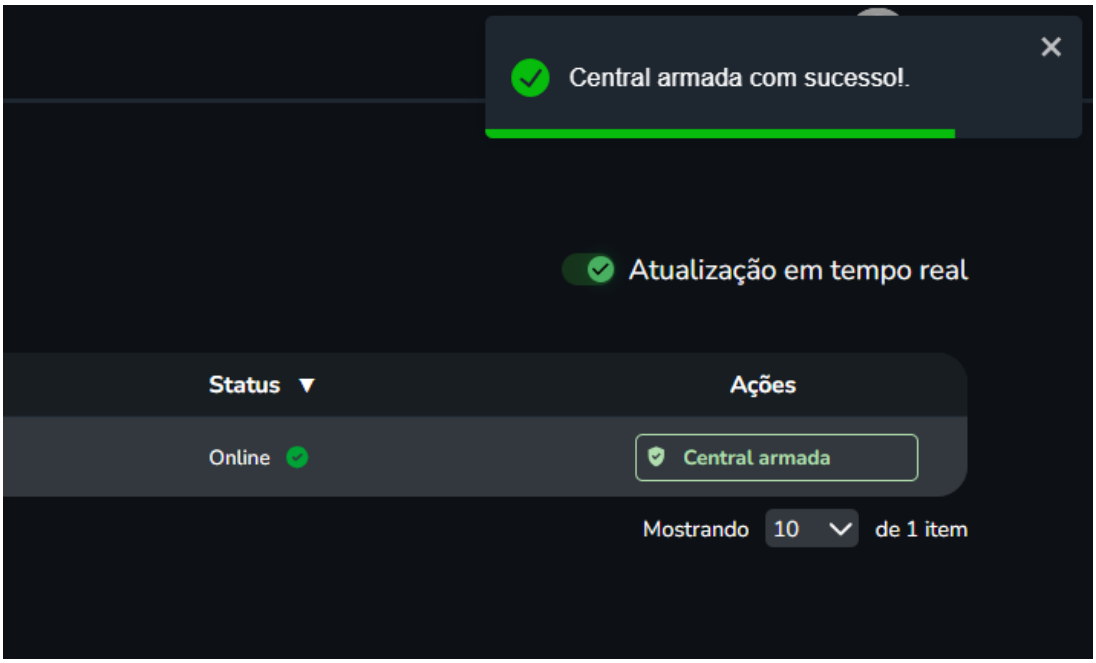


Figura 51. Central armada com sucesso

Caso não seja possível armar a central, um erro será retornado exibindo o motivo do porque não foi possível realizar a operação. Segue abaixo dois exemplos.

Figura 52. Falhas ao armar uma central

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.

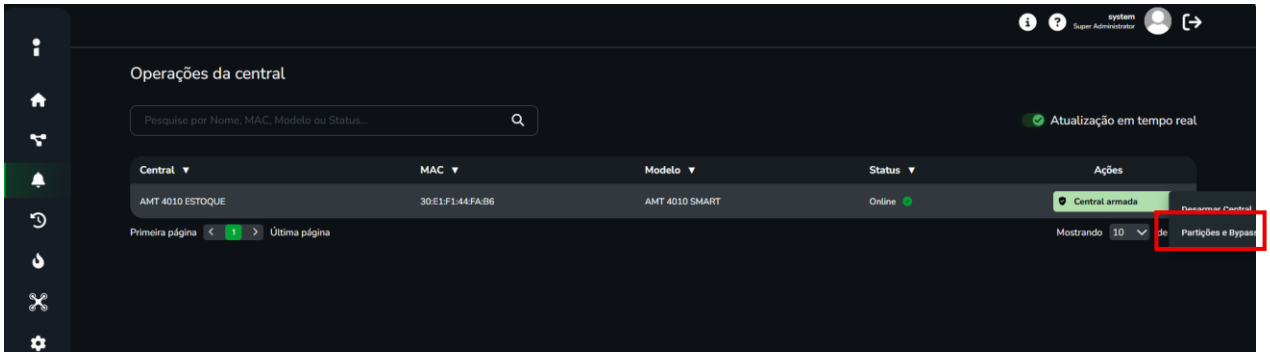


Figura 53. Partições em bypass

Agora clique em central armada/desarmada na parte superior.

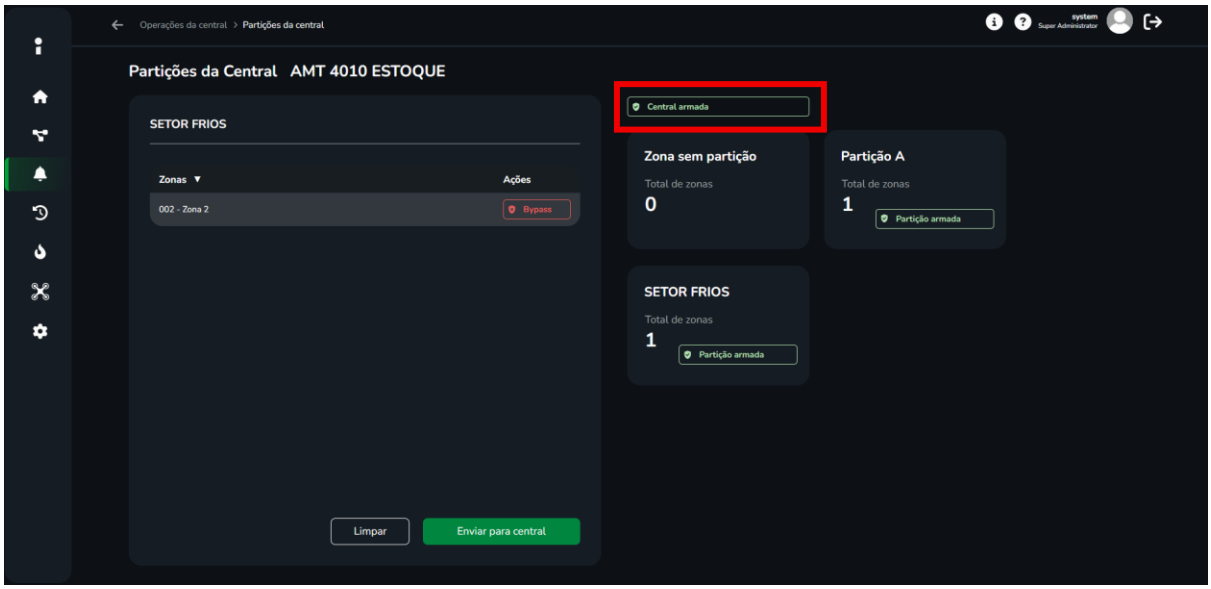


Figura 54. Armar central pela tela de partições e bypass

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

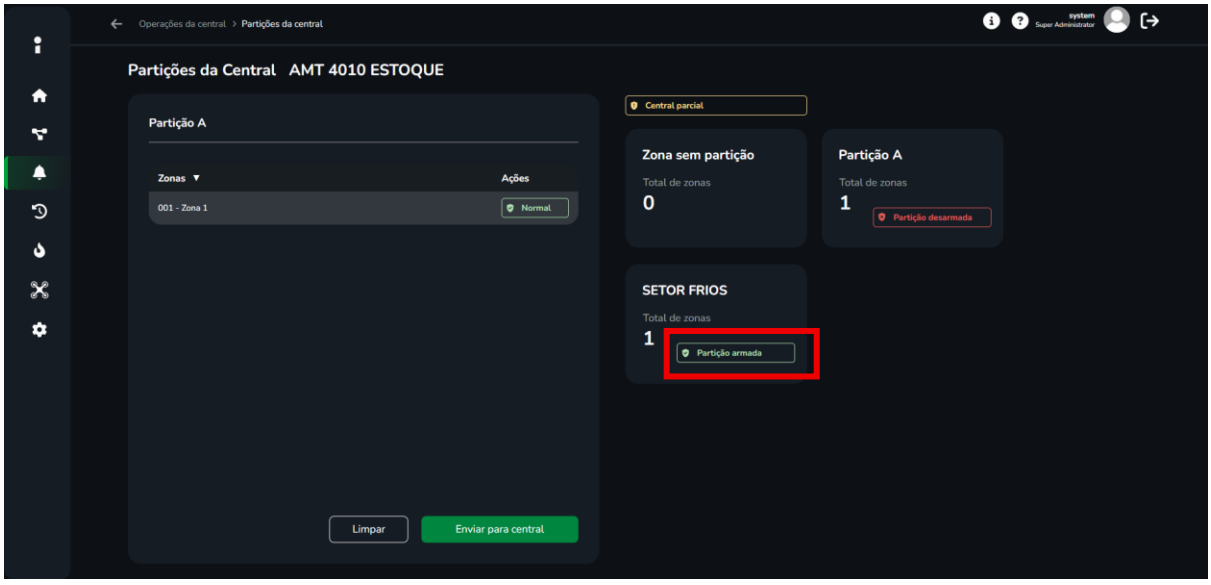


Figura 55. Armar partição individual

Note que caso apenas alguma partição esteja armada, a central exibirá o estado de **“Central parcial”**. Este estado poderá ser visualizado também na lista de operação das centrais de alarme de intrusão.

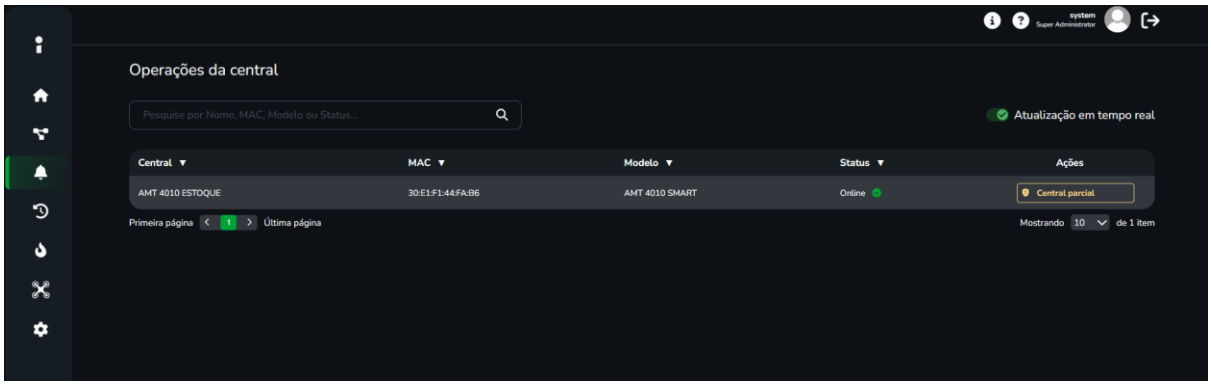
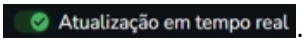


Figura 56. Indicação de arme parcial

Na parte superior há o botão 

. Ao ativa-lo, será possível acompanhar em tempo real a mudança de estado das centrais. Caso no campo, alguma pessoa faça o arme da central via teclado, este refletirá automaticamente à página.

6.6. 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"**.

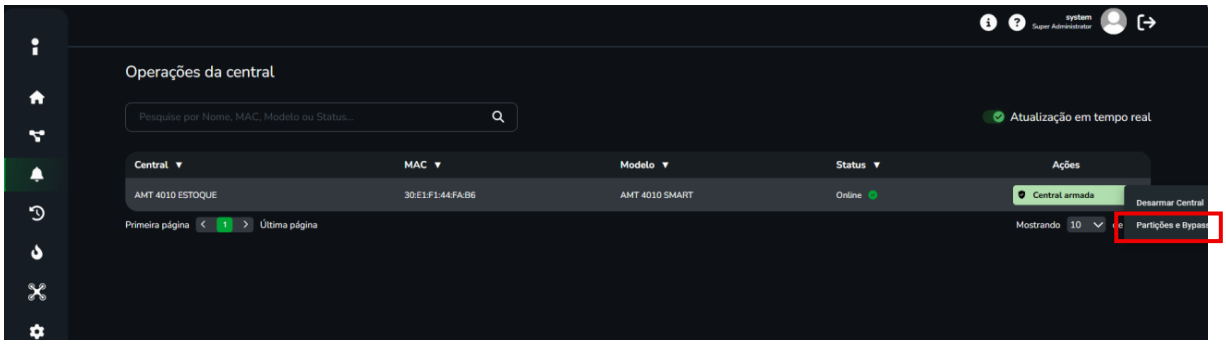


Figura 57. Partições e Bypass

Selecione a partição onde está alocada a zona que se deseja realizar o bypass.

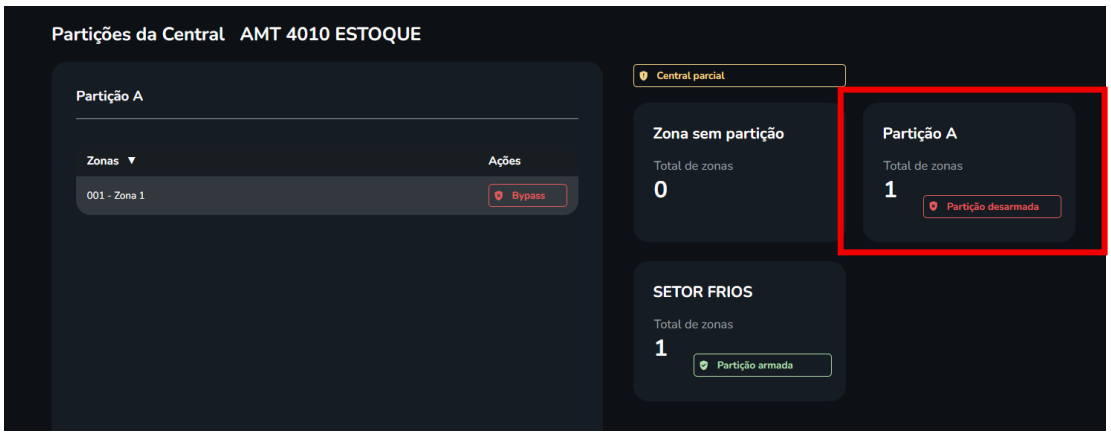


Figura 58. Selecionando Partição

Após isso clique no botão presente na coluna ações na listagem das centrais, deixe a zona na situação desjada (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.

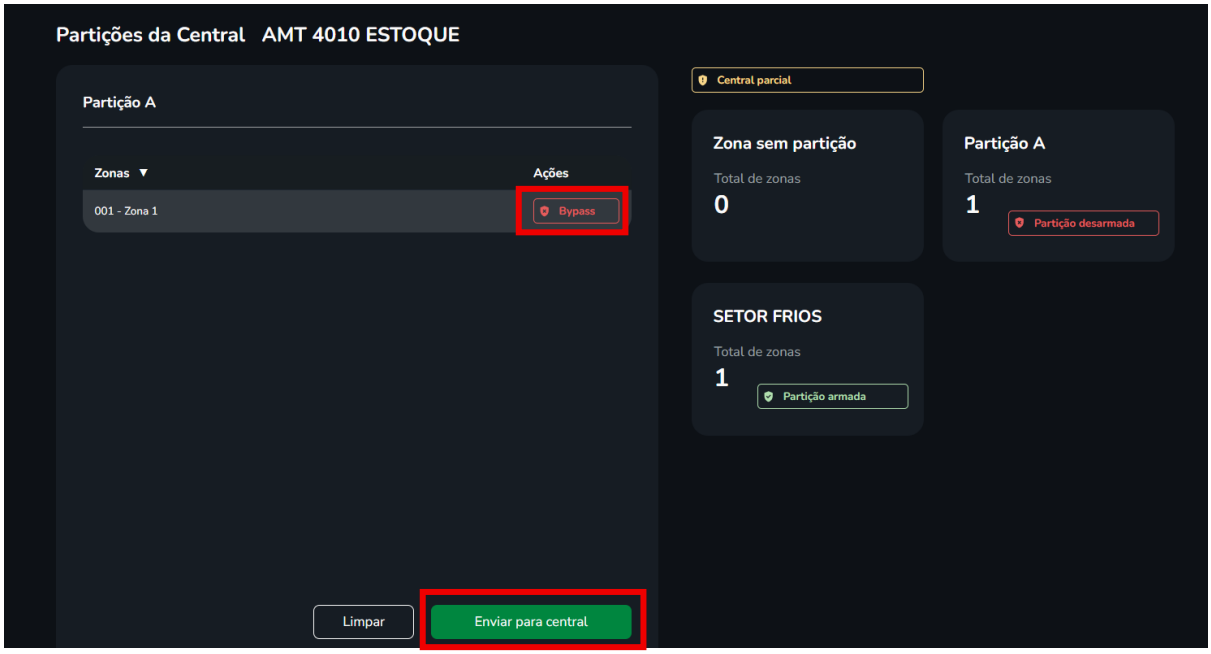


Figura 59. Alterar estado da zona e enviar para a central

O botão "**Limpar**" retira o Bypass de todas as zonas das partições desarmadas.

7. Eventos AMT

A versão 3.2.3. do Middleware de Centrais traz uma nova forma de criar eventos para as centrais de alarme de intrusão. É possível agora criar template de eventos personalizados, onde o usuário consegue escolher apenas eventos específicos de zonas, usuários ou sistema. Desta forma, o operador irá receber apenas os exatos eventos que se deseja, evitando falsos positivos e tendo a segurança de que ações vinculadas aos eventos só serão acionadas no momento correto.

A criação de eventos se dá agora em dois passos. O primeiro é a criação do template de evento, e o segundo é a configuração do evento em si que utiliza templates préviamente criados.

7.1. Template de eventos

Para acessar a página de template de eventos acesse o menu de "**Eventos AMT**" e selecione "**Template de Eventos**".

Nesta página, será listado os templates de eventos já criados, exibindo o nome escolhido no momento da criação e um resumo de quantos eventos de cada tipo aquele template possuí vinculação. Para criar um novo template, clique em "**Novo template**".

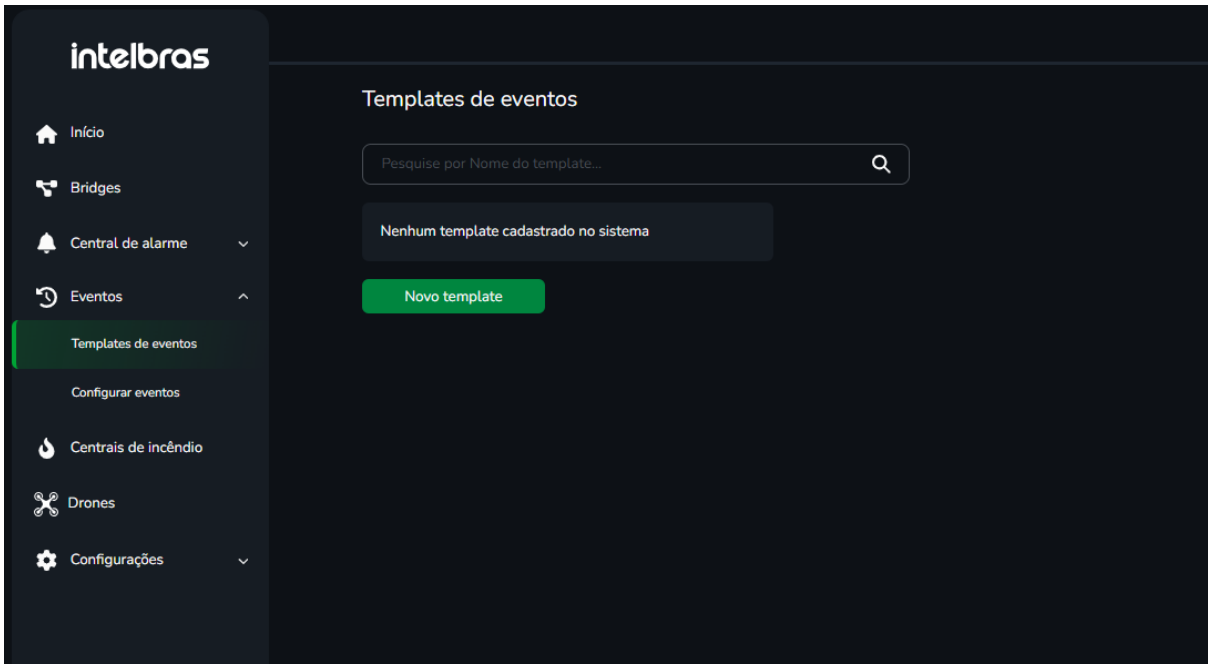


Figura 60. Lista de templates criados

Ao abrir a janela de criação de template de eventos, será possível escolher a composição de eventos que este template representará. É necessário aplicar um nome amigavel ao template de eventos que será criado.

Os eventos são divididos em: eventos de Zona, eventos de Usuário e Usuário de pertição e eventos de Sistema.

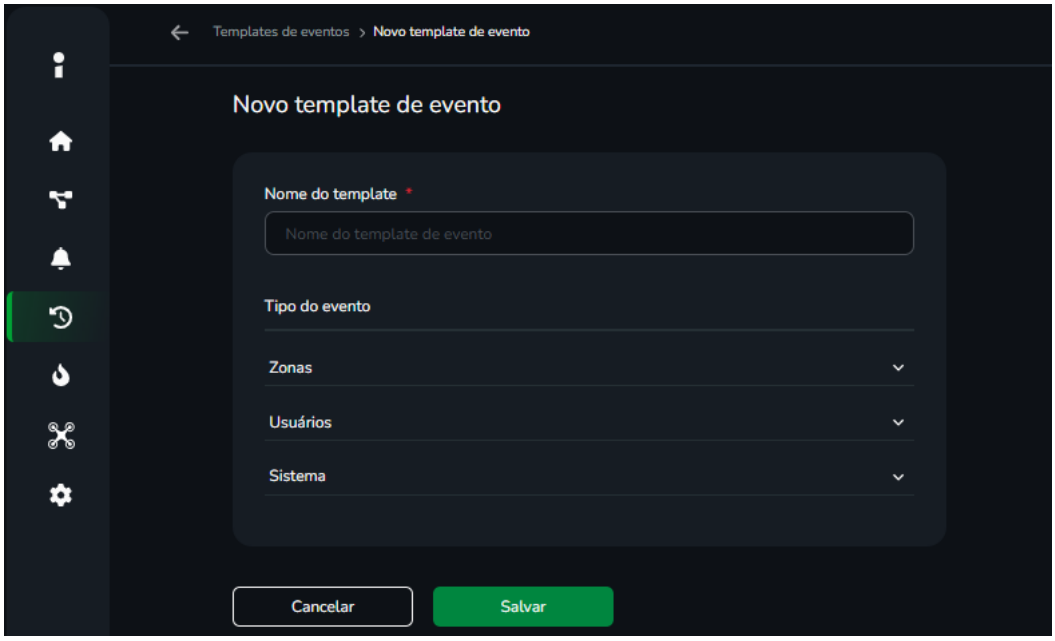


Figura 61. Novo template de evento

Para eventos de zona, é necessário escolher a qual zona o evento selecionado irá corresponder. Ex: Evento de **disparo de zona** para **zona 1**, **3** e **5**. Ao selecionar o tipo de evento, uma janela irá se abrir para que se selecione a quais zonas aquele evento irá corresponder.

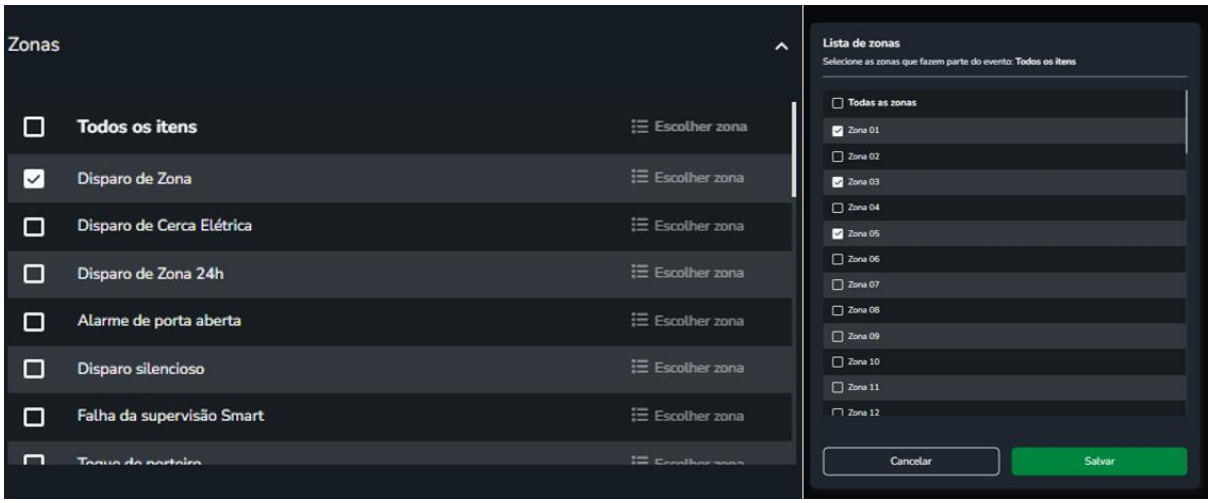


Figura 62. Eventos de Zona

Eventos de usuário se dividem em dois tipos. Eventos de usuário de partição e eventos de usuários. Eventos de usuário de partição é necessário escolher a partição e usuário que serão vinculados ao evento seleciono. Ex: Evento de **Arme de partição** da **partição B** do **usuário 8**.

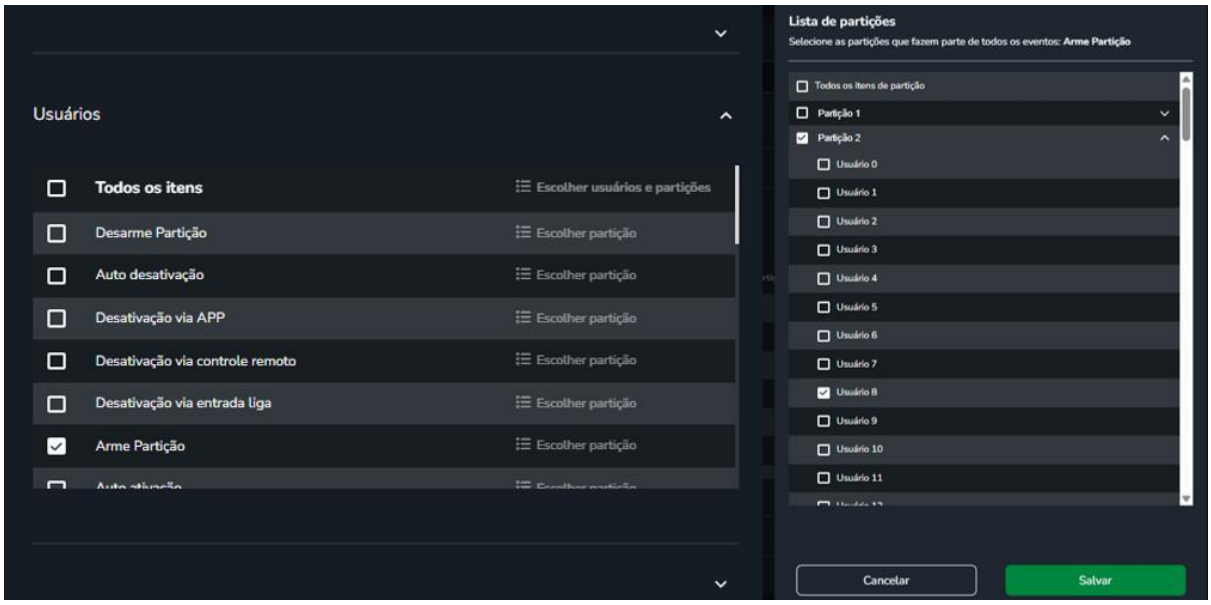


Figura 63. Eventos de usuário de partição

Para Eventos de usuário, é necessário escolher apenas o usuário vinculado ao evento. Ex: Evento de **pânico audível** para **usuário 6**.

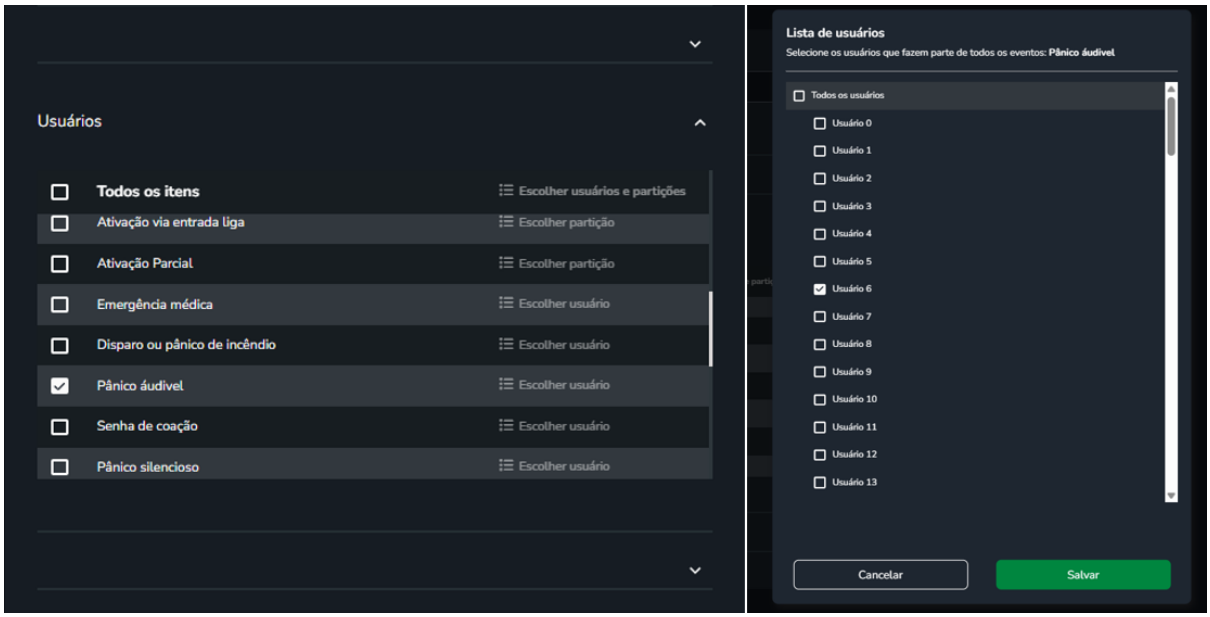


Figura 64. Eventos de usuário

Para eventos de sistema, basta selecionar qual evento deseja adicionar ao templa. Ex: Evento de **Falha de rede elétrica**.

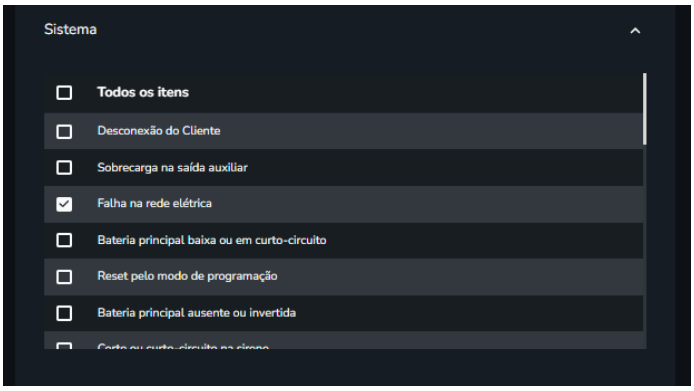


Figura 65. Eventos de sistema

É importante saber que é possível montar qualquer composição que se deseja dentro de um template de eventos, combinando vários eventos diferentes para atender a uma certa necessidade. É possível criar um template que contenha ao mesmo tempo eventos de zona, usuario e sistema. Também é possível ser específico criando um template com apenas um único evento e uma única zona/usuário vinculados para que não se receba eventos não desejados no desktop client.

Apenas criar o template de eventos não fará com que os eventos cheguem no Intelbras Defense IA. É necessário finalizar a criação do evento em si, que será explicado na sessão "*7.2. Configurar eventos*".

7.2. Configurar eventos

Após criar o(s) template(s) de evento desejado(s), entre no menu de configurar eventos e clique em **“Adicionar Evento”.**

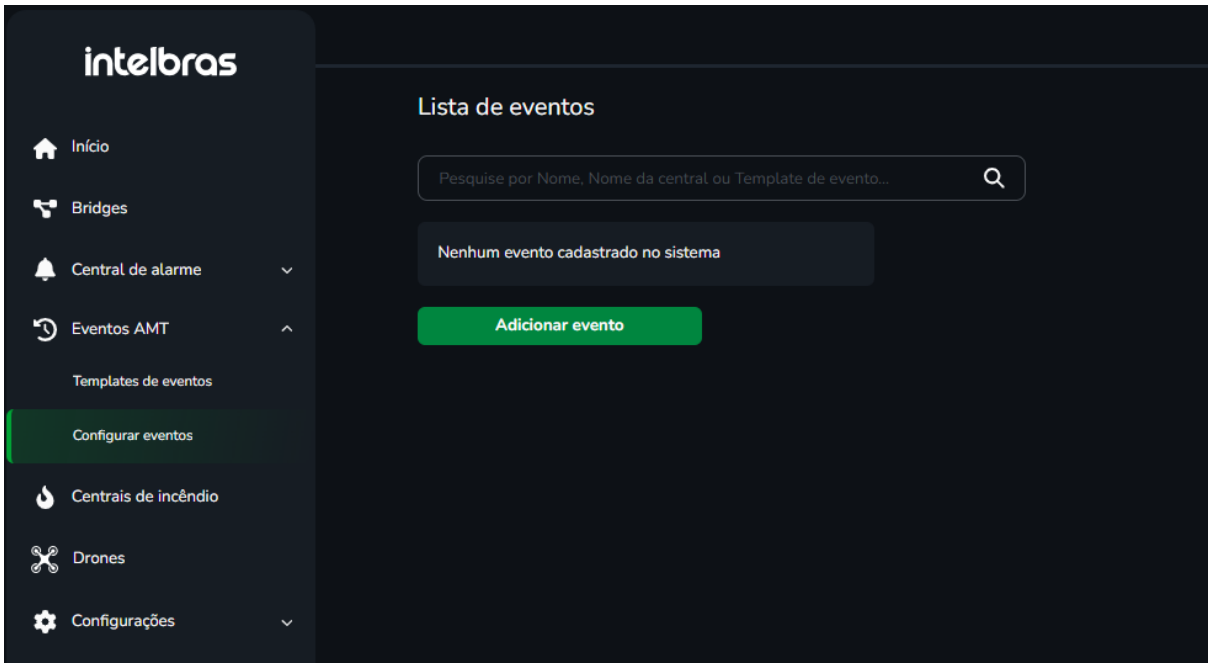


Figura 66. Configurar eventos

Será necessário realizar algumas configurações para criar o novo evento. A primeira aba se refere às informações do evento, um nome para o evento, uma descrição dando mais detalhes, a prioridade do evento (altera o destaque do evento no dektop client) e o modelo de tempo (evento que funciona 24/7, apenas dias de semana, apenas finais de semana...).

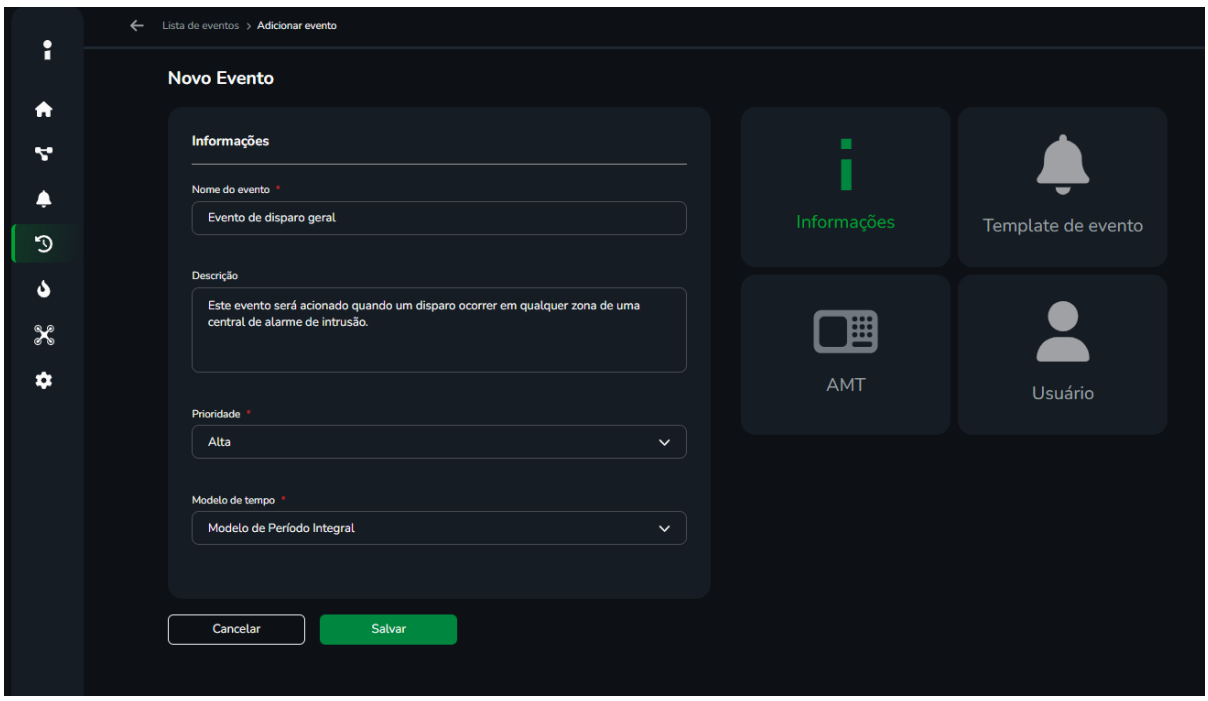


Figura 67. Informações do evento

Na segunda aba é necessário selecionar um template de evento que irá **“filtrar”** os eventos enviados pelas centrais AMT. Só serão encaminhados para o Intelbras Defense IA eventos que foram vinculados dentro do template selecionado.

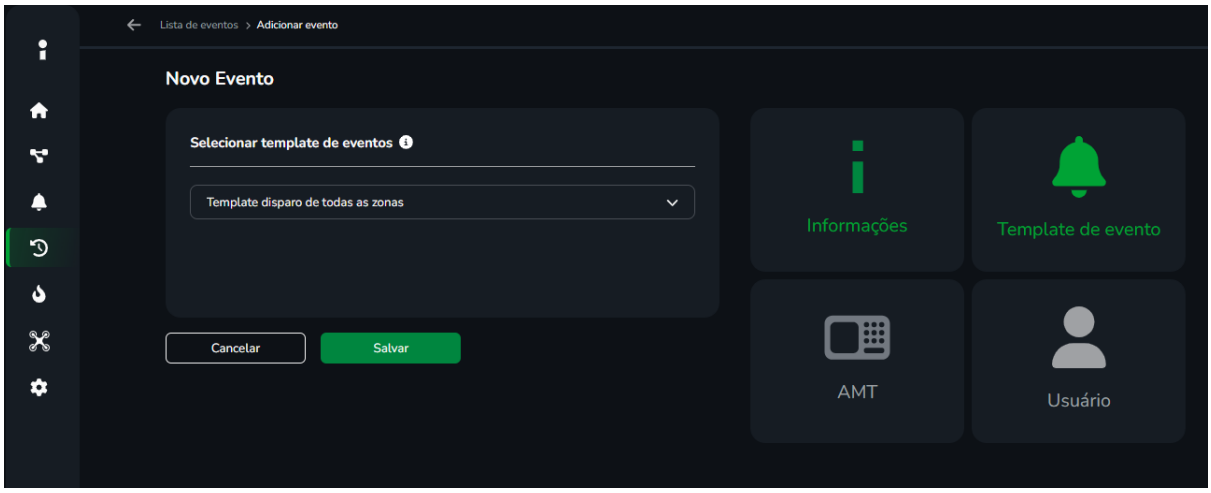


Figura 68. Seleção do template de eventos

Na terceira aba é necessário selecionar as centrais de alarme que serão vinculadas a este evento. Apenas os eventos gerados pelas centrais AMT selecionadas serão encaminhados para o Intelbras Defense IA (apenas eventos que estão incluídos no template de eventos selecionado anteriormente).

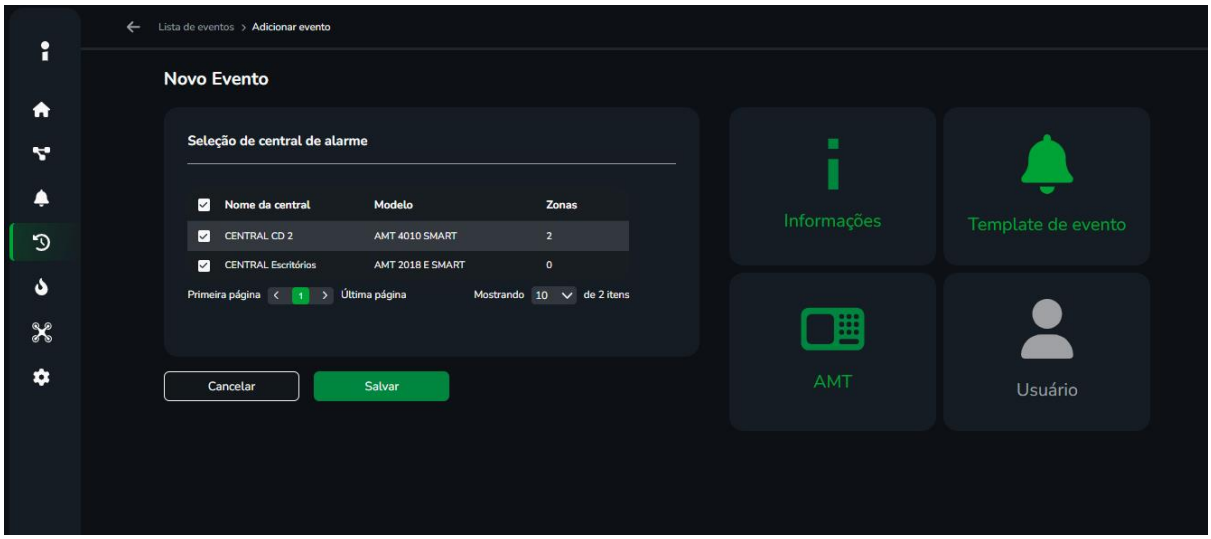


Figura 69. Vinculação de central AMT ao evento

Por último, selecione os usuários operadores do Intelbras Defense IA que serão notificados quando estes eventos forem gerados.

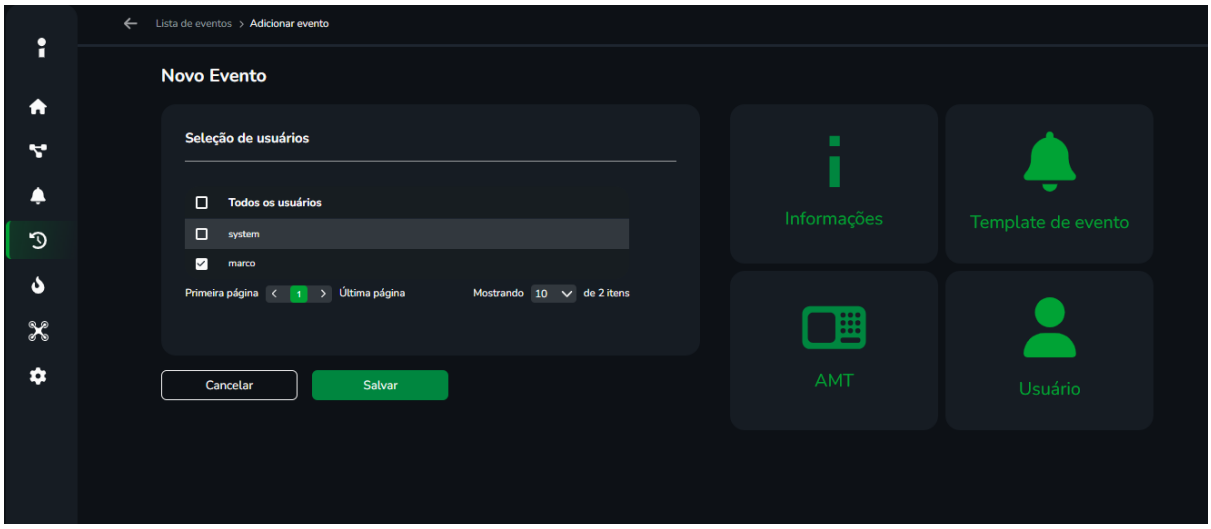


Figura 70. Vinculação de usuário operador notificado

Por fim. Crie o evento. Este, será replicado no Intelbras Defense IA e poderá ser acessado através do desktop client.

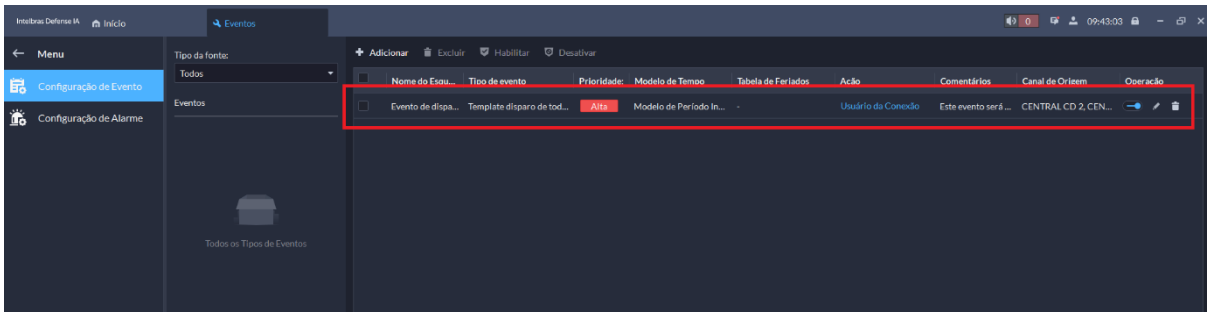


Figura 71. Evento listado no desktop client

7.3. Vinculando ações aos eventos AMT

O Intelbras Defense IA consegue realizar diversas ações após o recebimento de um evento. Essa função ressalta a integração que o sistema possuí entre diferentes módulos. É possível por exemplo, a partir de um evento de alarme, abrir o pop-up de uma câmera e acionar a saída de alarme ou áudio de uma câmera.

Para vincular uma ação a um evento, acesse o desktop client do Intelbras Defense IA e acesse as configurações de eventos.

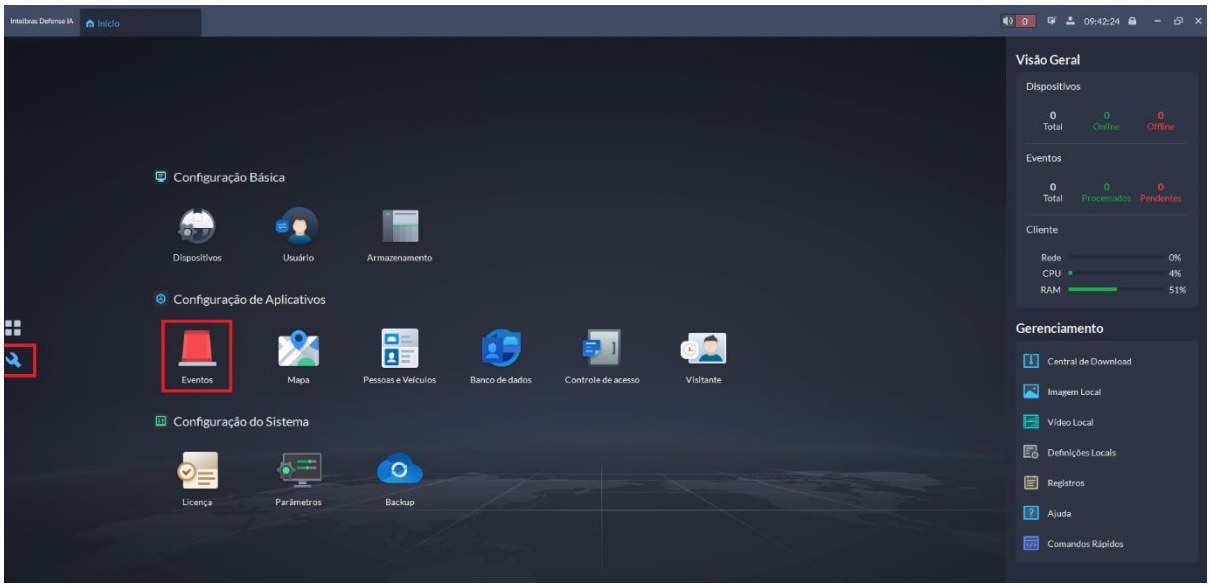


Figura 72. Acesso às configurações de eventos

O evento de central AMT criado através do web client será exibido também aqui. Clique para editar o evento.

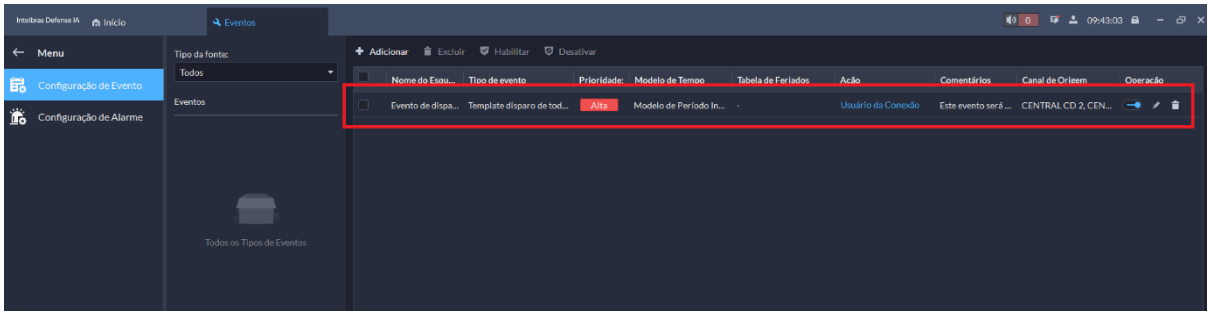


Figura 73. Evento listado no desktop client

Após abrir as configurações de um evento, desça até que seja listado as ações vinculadas a este evento. Realizer a configuração de ações conforme o que deseja que seja realizado assim que o evento for recebido.

Figura 74. Ações disponíveis para vinculação a um evento

Não crie ou realize outras edições nos eventos de alarme de intrusão através do desktop client, pois eles não serão replicados no client web do middleware de centrais. Se limite a apenas vincular e desvincular ações nestes eventos através do desktop client.

7.4. Visualizar eventos de centrais AMT

Para visualizar os eventos, retorne até o menu de aplicativos do Intelbras Defense IA e clique em central de eventos.

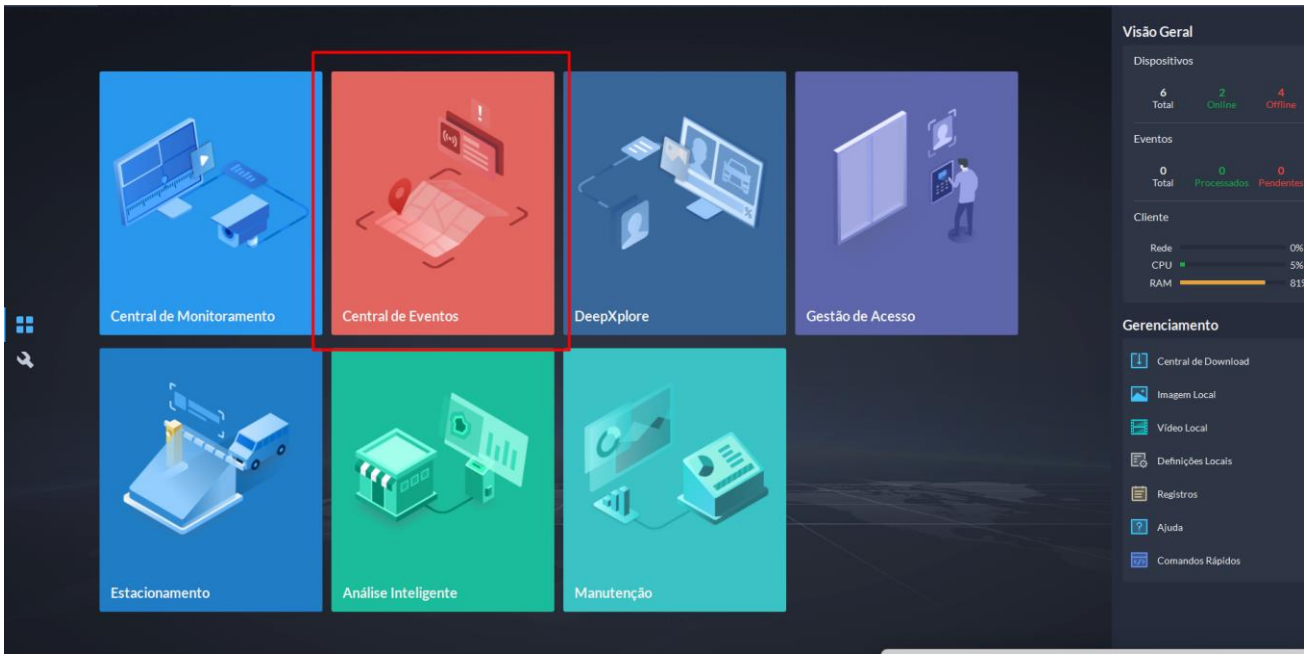


Figura 75. Acesso a central de eventos

Assim que o evento for recebido será notificado da seguinte forma:

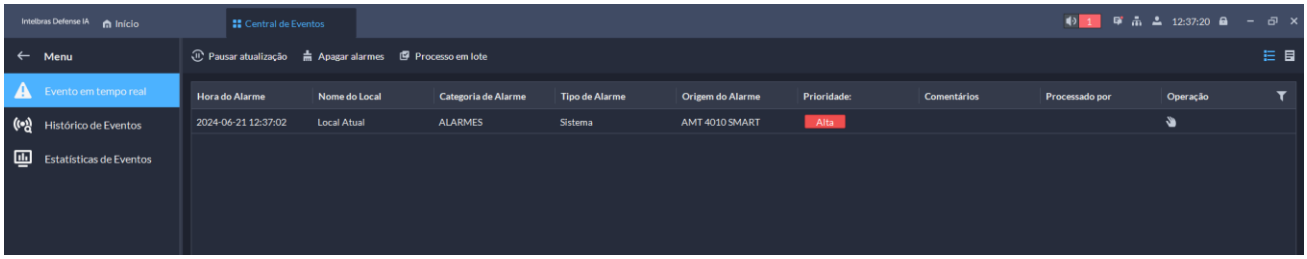


Figura 76. Evento notificado

Se uma ação foi vinculada a este evento, ela será executada assim que o evento for recebido.

8. 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 (online/offline) e recebimento de eventos no Intelbras Defense IA.

Diferente das centrais de alarme de intrusão, não é possível realizar configuração de zonas e laços pelo web client.

Figura 77. CIE 1125

8.1. 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 e novo arquivo.

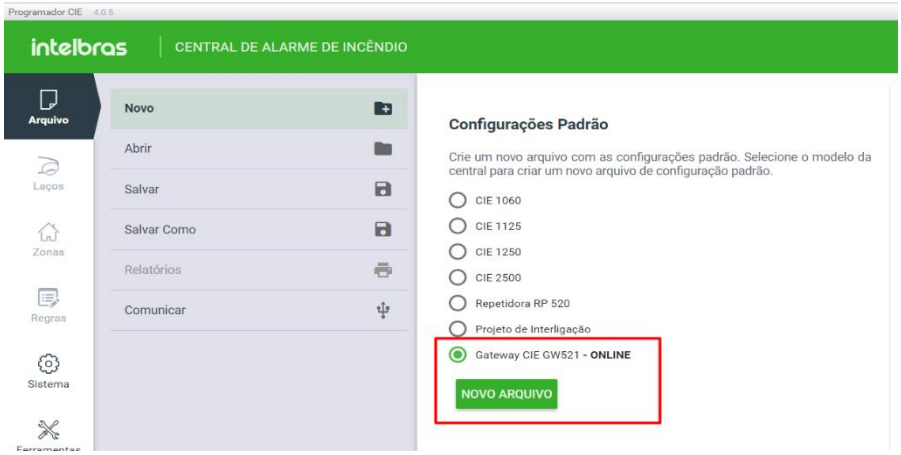


Figura 78. Novo arquivo de configuração

Depois em configurações.

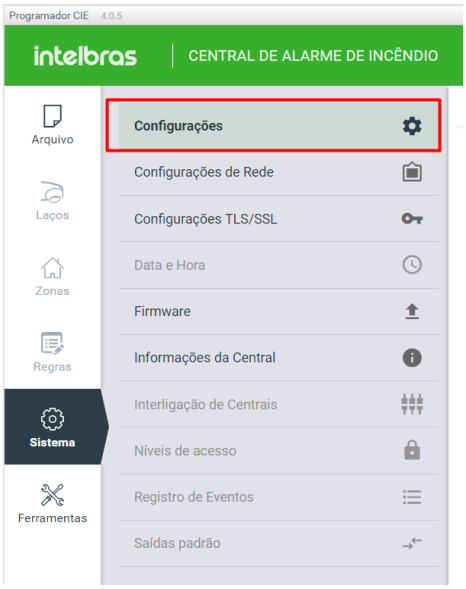


Figura 79. Configurações da CIE

Agora habilite a função webhook.

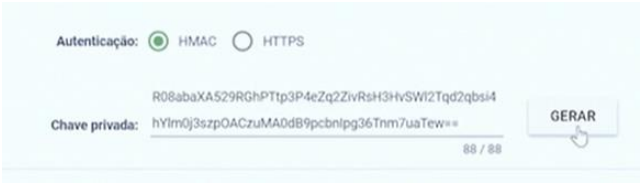
Figura 80. Habilitando modo webhook

Após habilitado, 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**

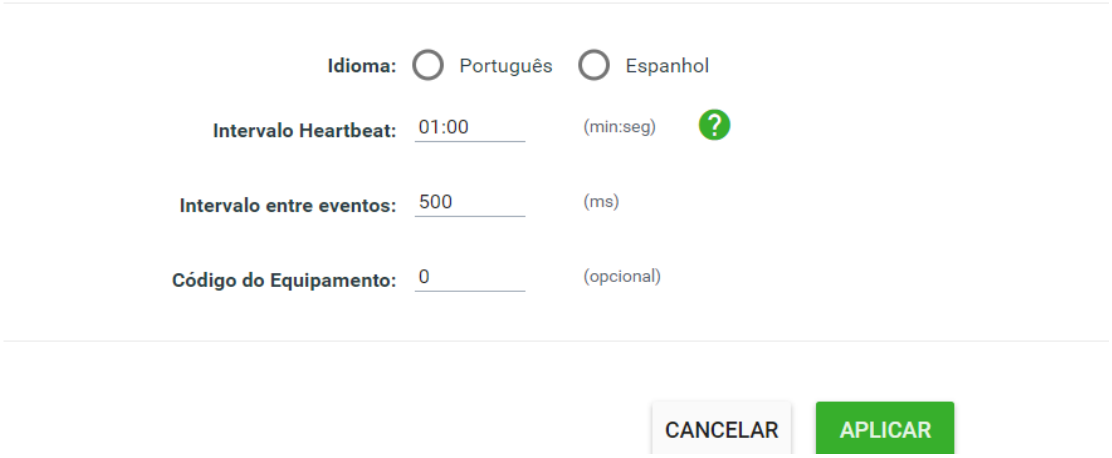
*IpServidor = IP da máquina do Intelbras Defense IA

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 Middleware de centrais. O uso do HMAC não é obrigatório, porém deixará a comunicação entre GW521 e Middleware de centrais sem criptografias.



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



Após aplicar, acesse a aba **“arquivo”**, **“comunicar”** e clique em enviar para enviar as configurações realizadas.

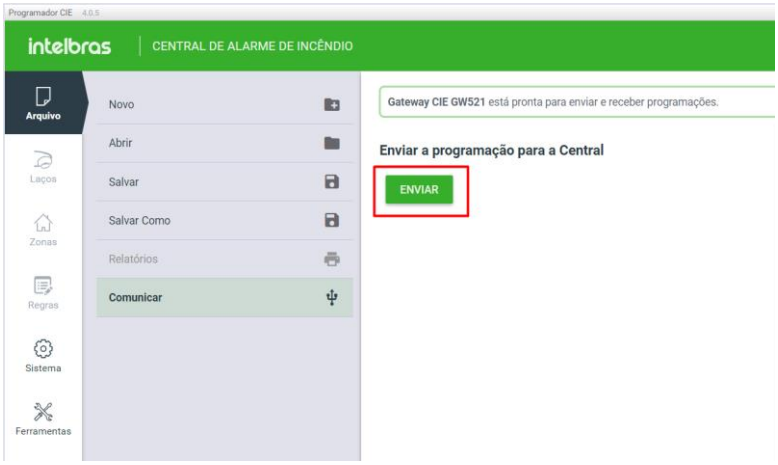


Figura 81. Envio de configurações para central CIE

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

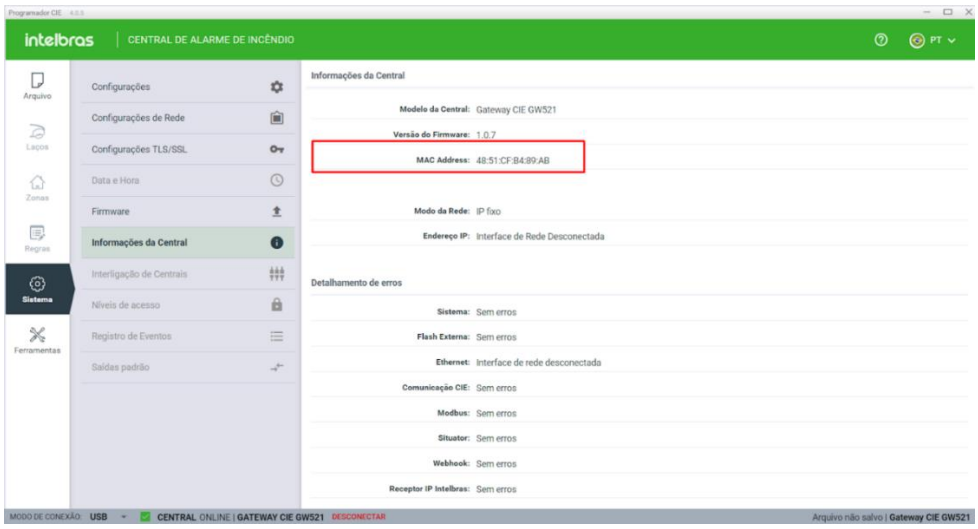
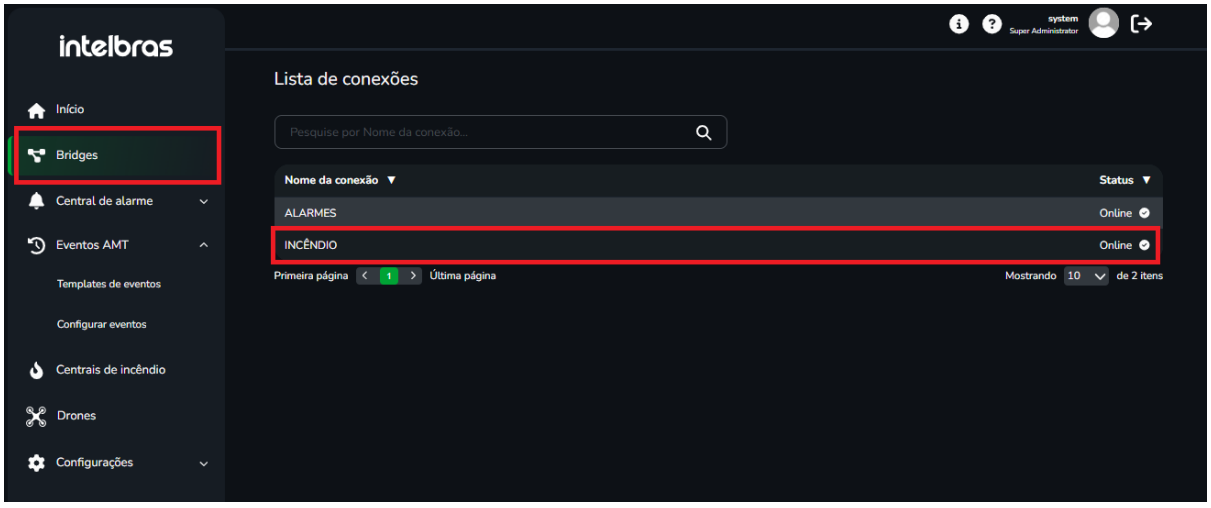


Figura 82. MAC Address GW521

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

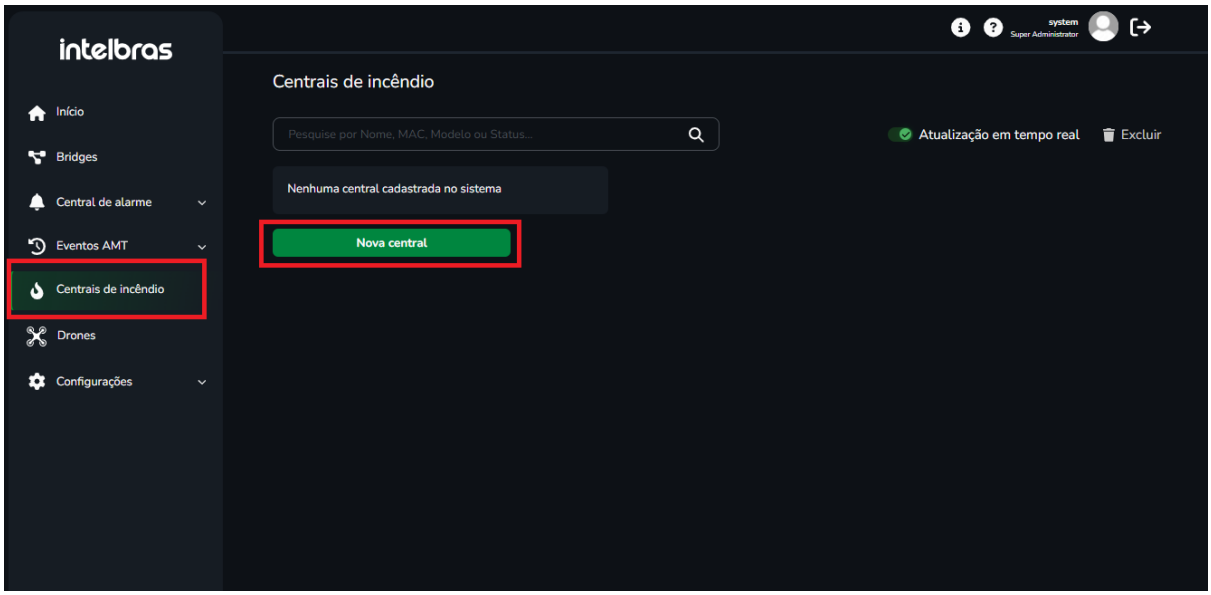
Antes de adicionar a central de incêndio, certifique-se que o bridge responsável pela comunicação dos eventos com o Intelbras Defense IA está online. Para confirmar esta informação, vá até o menu Bridges na barra lateral esquerda.

Verifique se o bridge **"INCÊNDIO"** está online.

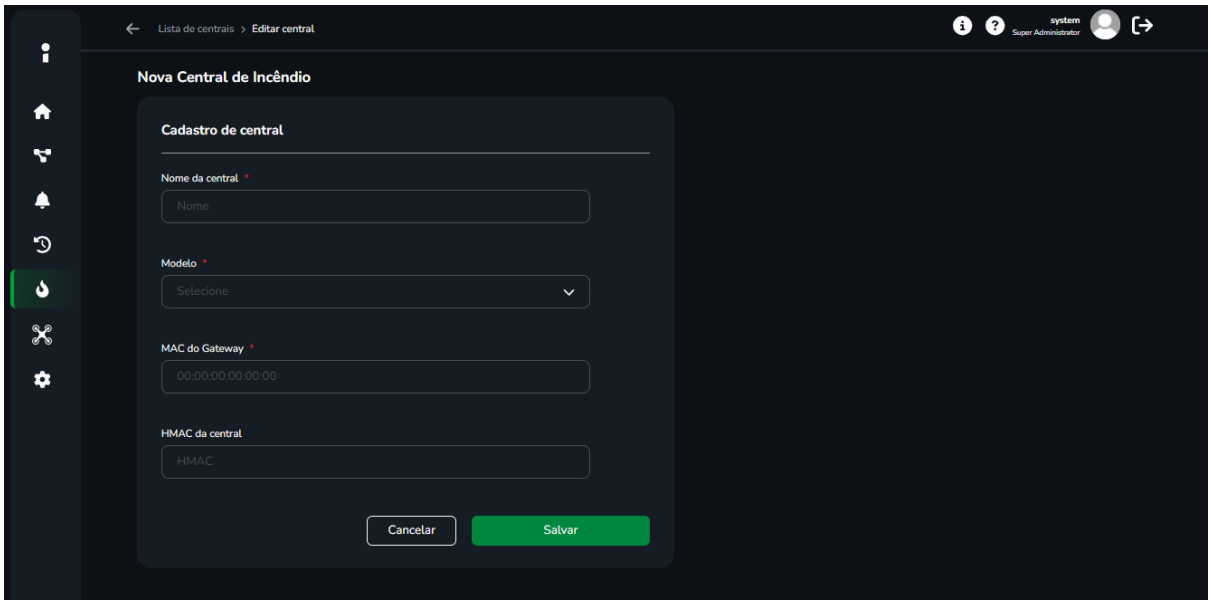


Caso o bridge esteja offline, verifique se os serviços do Intelbras Defense IA Server estão sendo executados. Se algum estiver parado, tente inicialo. Se todos estiverem sendo executados e mesmo assim os bridges estão offline, entre em contato com o suporte.

Após confirmação, para adicionar uma nova central de incêndio, clique no menu **"Centrais de Incêndio"** e em **"Nova Central"**.



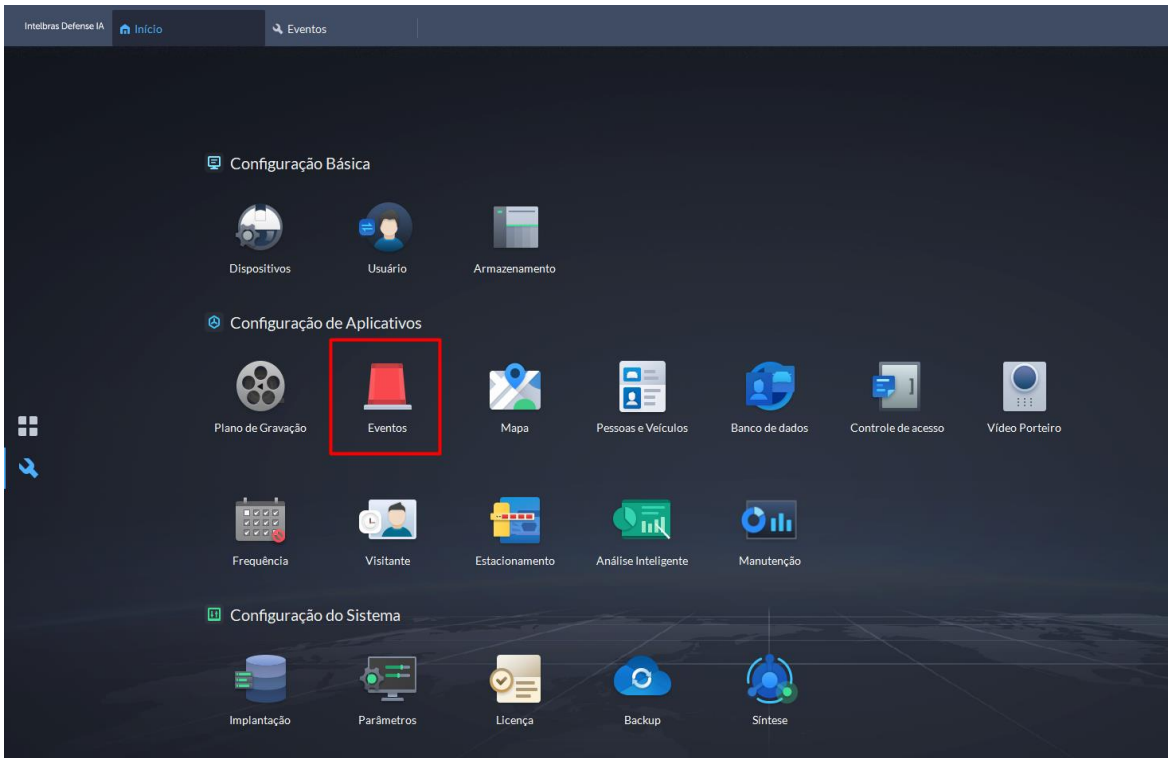
Preencha com as informações corretas e clique em **"Salvar"**.



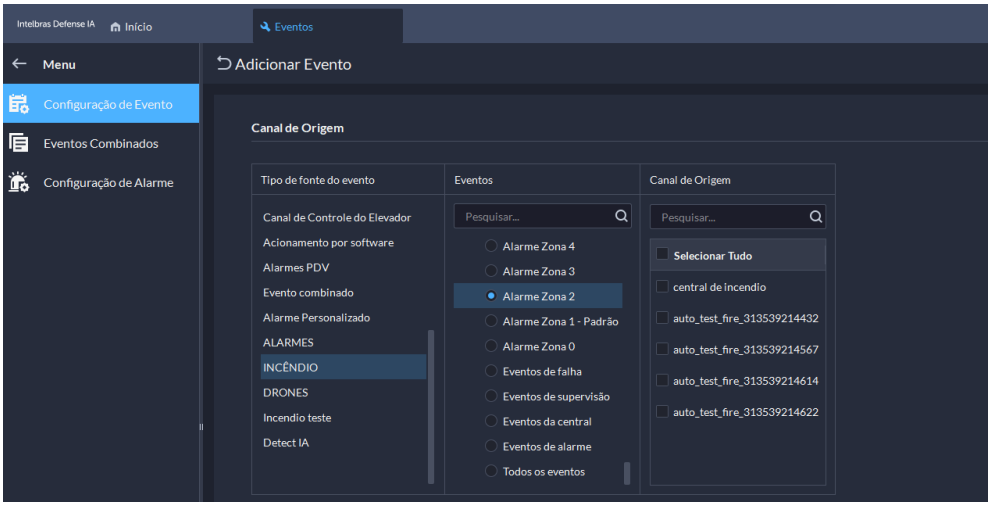
O HMAC deve ser coletado enquanto estiver configurando a central CIE através do programador.

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

Diferente dos eventos das centrais de alarme de intrusão, os eventos das centrais CIE são criados e geridos totalmente no desktop client. Para realizar a configuração, no menu inicial do Intelbras Defense IA, clique em Eventos.



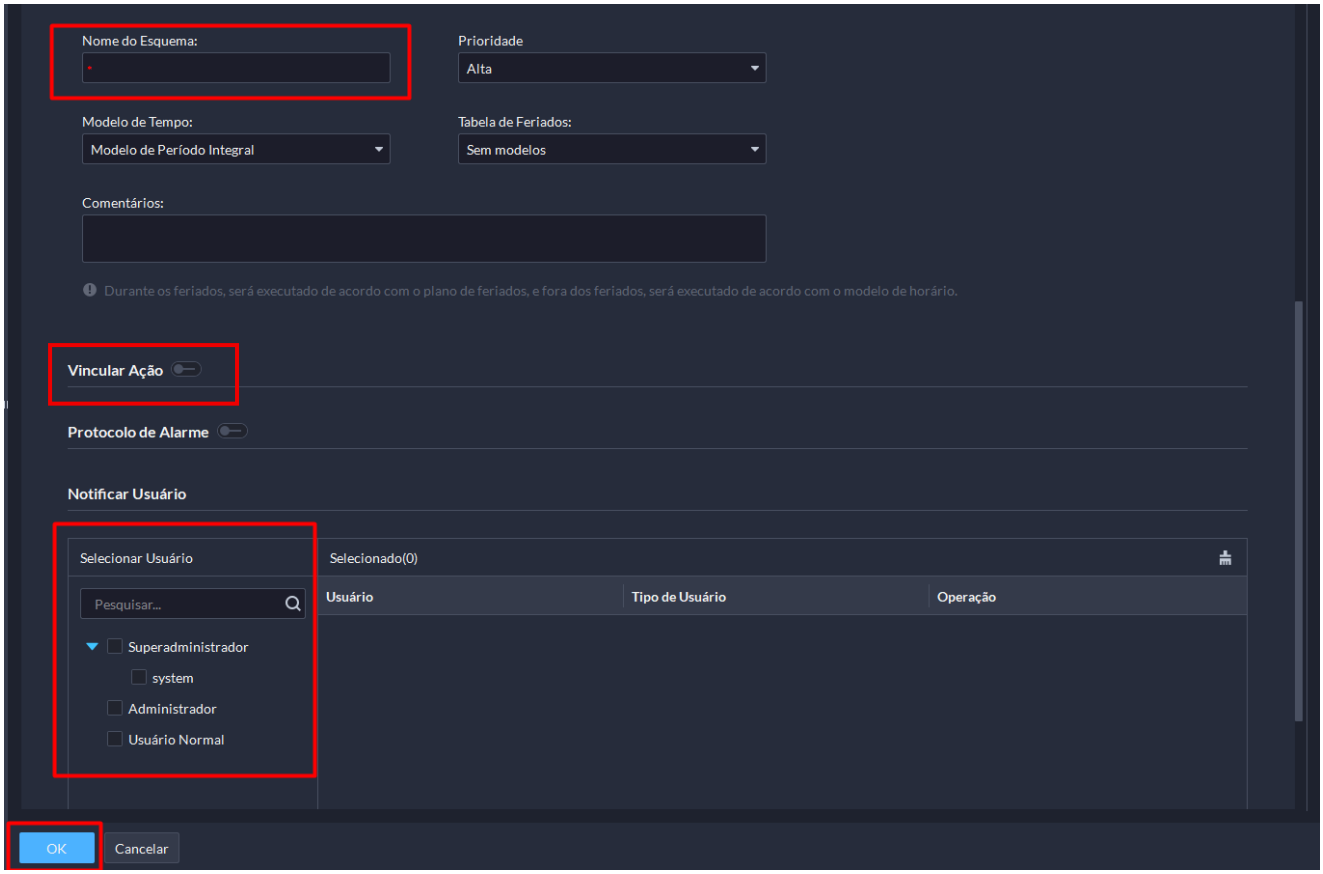
Após isso, em fontes de evento desça até **"INCÊNDIO"** e a selecione, em eventos coloque sua zona desejada e em canal de origem sua central.



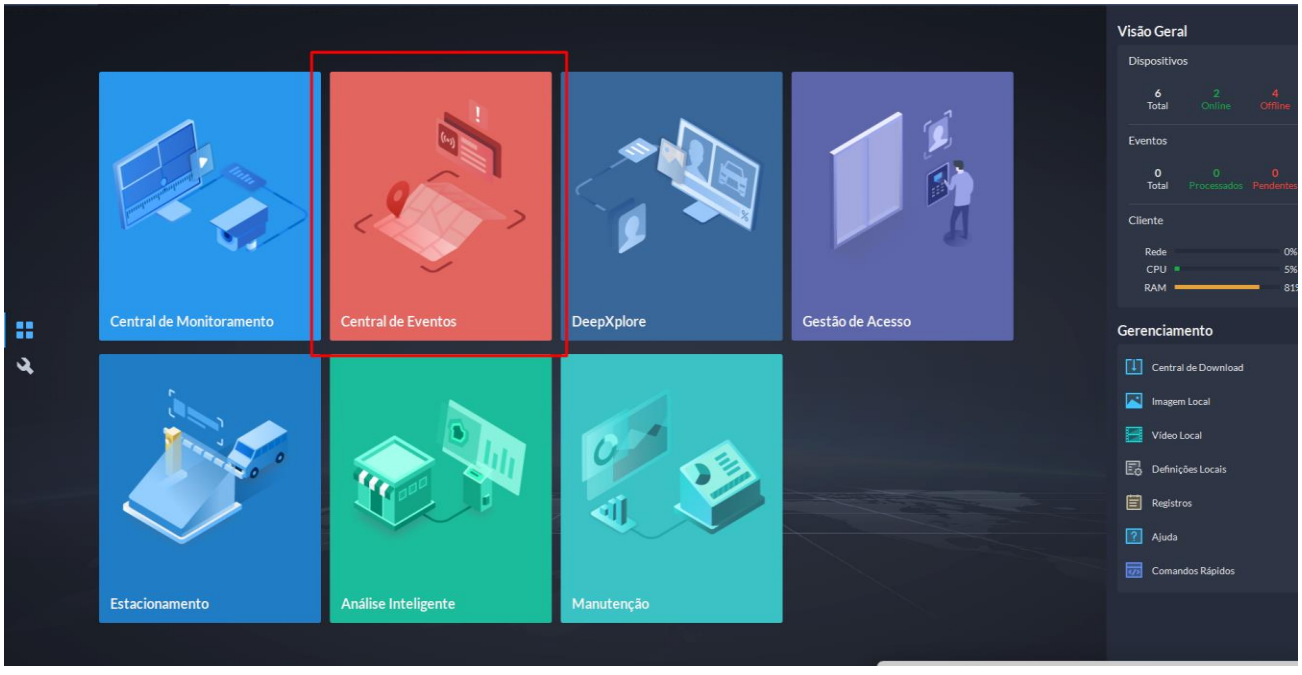
Os tipos de eventos para centrais de incêndio CIE são:

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 ed 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 da zonas da central;

Feito isso, desça a página, nomeie o esquema, defina sua prioridade, vincule ações e selecione os usuários operadores a serem notificados. Por fim, clique em OK.



Para visualizar os eventos, retorne até o menu de aplicativos do Intelbras Defense IA e clique em Central de eventos.



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

Se uma ação foi vinculada a este evento, ela será executada assim que o evento for recebido.

9. Migração de Eventos AMT

Na versão 3.2.3 do middleware de centrais, como apresentado anteriormente, houve uma mudança na estrutura de eventos para centrais de alarme de intrusão.

Nas versões anteriores, os eventos AMT eram criados através do desktop client. O usuário selecionava um tipo de evento listado e então selecionava as centrais que iriam reportar aquele evento. Dentre as opções disponiveis de tipo de evento haviam Sistema, Usuario 0-99 e Zona 1-100.

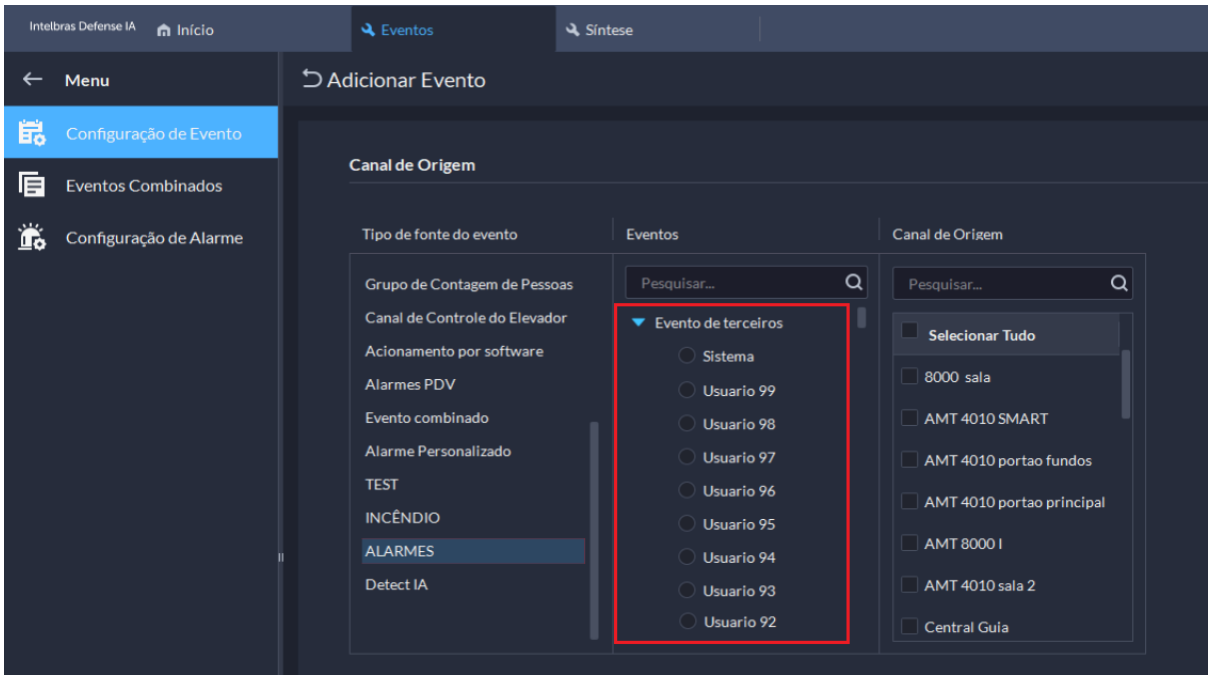


Figura 83. Tipos de eventos MC 3.2.2 ou anterior

O principal problema dessa abordagem e que não era possível escolher qual evento receber entre os eventos de sistema, usuario ou zona. Uma vez que criado o evento de Zona 1 por exemplo, todo evento de zona 1 seria recebido pelo Intelbras Defense IA. Nesse caso o operador poderia estar interessado apenas no evento de intrusão mas receberia diversos eventos de zonas não desejados.

A migração de eventos só ocorrerá entre as versões 3.2 (3.2.0, 3.2.1, 3.2.2 e 3.2.3) do Intelbras Defense IA e MC. Versões anteriores não será possível realizar a migração e o antigo Middleware de Centrais deve ser desinstalado para que o novo seja instalado.

9.1. Migrando tipos de eventos para templates de eventos

A migração de eventos é feito de forma automática durante a instalação da versão 3.2.3 do Middleware de centrais. O instalador irá identificar que há uma versão prévia instalada e irá migrar os eventos de forma automatizada.

Há uma lógica para transferência dos eventos. Os antigos tipos de evento (sistema, usuario 0-99 e zona 1-100) serão apagados e em seu lugar serão criados templates de eventos que representam os antigos tipos de evento em uso. Neste caso, não será criado um template de eventos para cada antigo tipo evento, mas sim um template apenas para cada tipo de evento que estava vinculado a um evento de AMT.

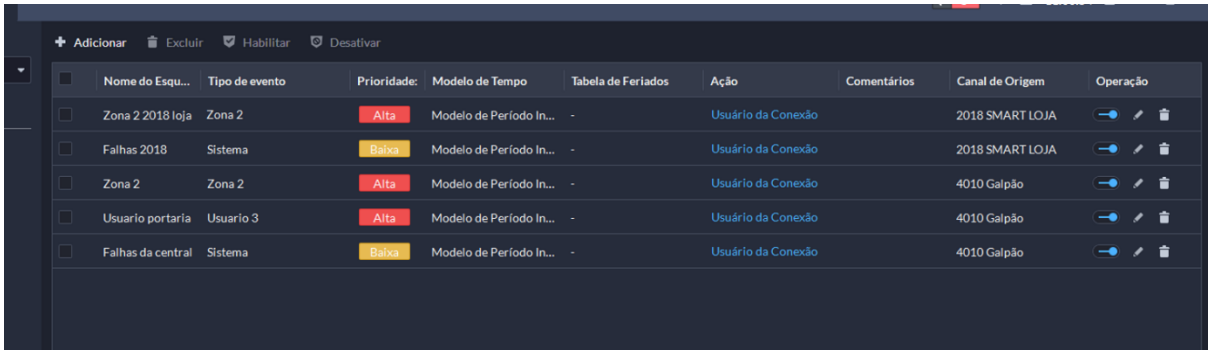


Figura 84. Eventos criados na versão 3.2.2 ou anterior

No caso da *Figura 84*, há **cinco** eventos criados. Estes utilizam apenas **três** tipos de evento: Sistema, Zona 2 e Usuario 3. Ao migrar para a versão 3.2.3, será criado apenas **três** template de eventos, representando apenas os tipos de evento em uso anteriormente. Apesar dos tipos de evento Sistema e Zona 2 serem utilizados mais de uma vez, eles serão **recriados como templates** apenas **uma vez**.

Como os eventos de Zona e Usuário nas versões 3.2.2 e anteriores englobavam todos os eventos deste tipo, ao migrar, isso será mantido no novo template. Ou seja, um tipo de evento Usuário 3 será recriado como um template selecionando todos os eventos de usuário para o usuário 3.

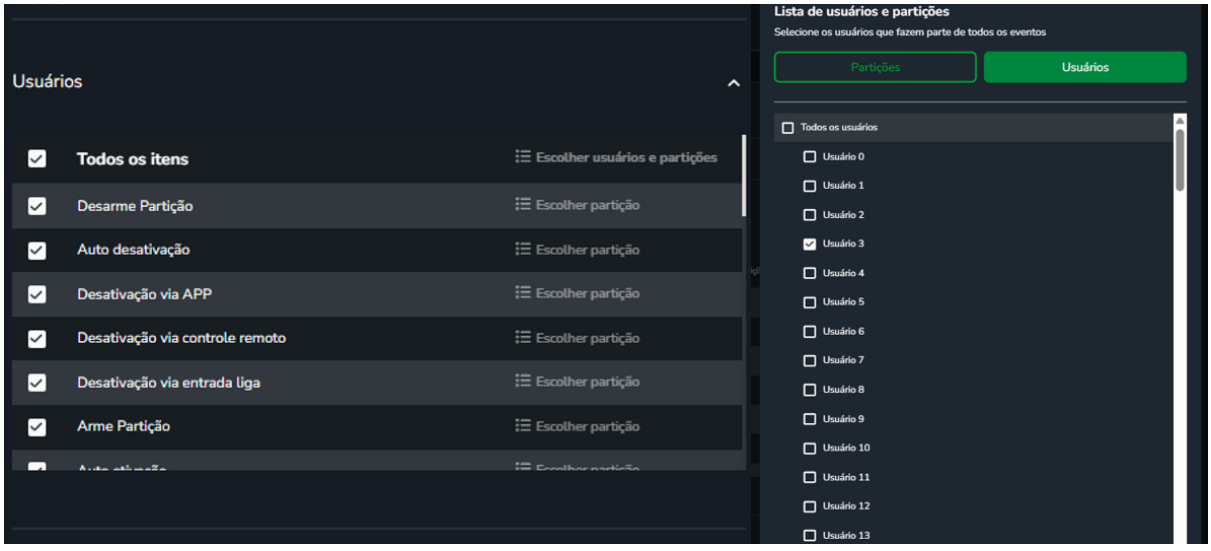


Figura 85. Tipo de evento usuario 3 migrado para Template de eventos

O template que representa o antigo tipo de evento Usuário 3 agora foi criado com o nome de “Usuário 3 – Migrado”. Todos os tipos de eventos migrados seguirão essa lógica.

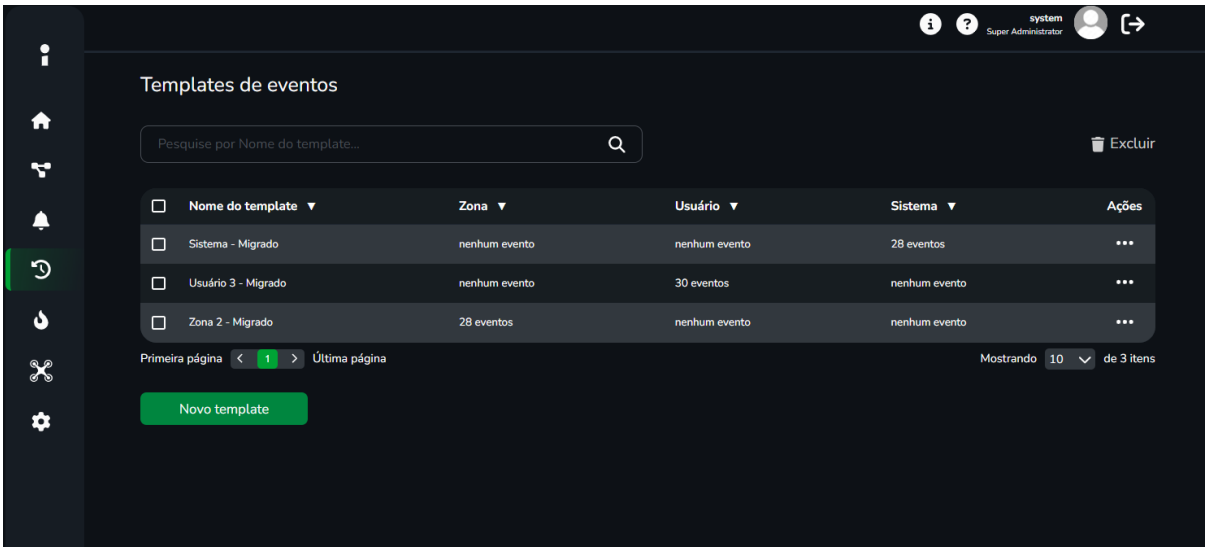


Figura 86. Templates de evento substitutos dos antigo tipos de eventos deste exemplo

9.2. Migrando eventos do desktop client para os eventos do web client

Ainda durante a instalação, após ter todos os templates de eventos criados representando os antigos tipos de eventos em uso, o instalador irá agora migrar os eventos em si.

A migração dos eventos é sempre de 1 para 1. Para cada evento AMT antes criado no desktop client será criado um mesmo evento no web client que o representa, vinculando ao evento o template de evento que representa o antigo tipo de evento que ele substituiu. Este novo evento **manterá todas as ações vinculadas** e os mesmos **usuários notificados**, **além de outras configurações** como prioridade, modelo de tempo, tabela de feriados, comentário do evento etc.

Abaixo, na *Figura 87*, um exemplo de eventos criados ainda na versão 3.2.2 ou anterior.

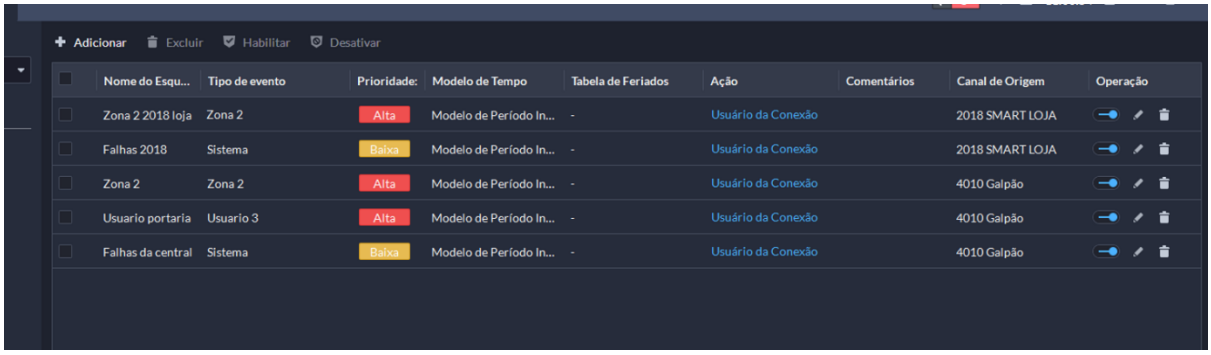


Figura 87. Eventos criados na versão 3.2.2 ou anterior

Durante a instalação, após criar os template, a migração dos eventos irá inciar. Neste exemplo de migração, os eventos ficarão da seguinte forma no web client.

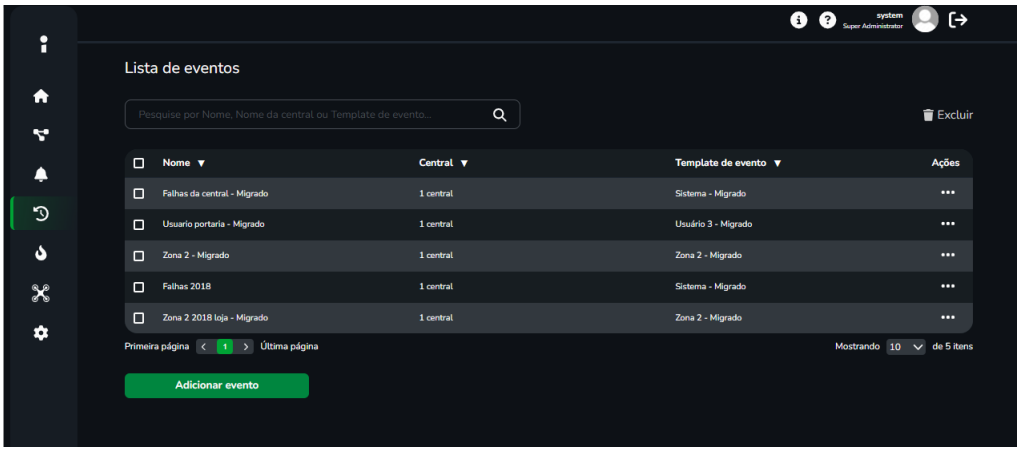


Figura 88. Eventos migrados para versão 3.2.3

Note que os antigos eventos serão deletados do desktop client, e os eventos criados no web client serão também replicados no desktop client novamente.

Figura 89. Eventos migrados para versão 3.2.3 no desktop client

Não crie ou realize outras edições nos eventos de alarme de intrusão através do desktop client, pois eles não serão replicados no client web do middleware de centrais. Se limite a apenas vincular e desvincular ações nestes eventos através do desktop client.