Versão deste manual: 1.00

# Interface Web

A Interface Web é uma plataforma integrada aos dispositivos faciais Intelbras, desenvolvida para simplificar o gerenciamento das configurações dos sistemas de controle de acesso corporativo.

Com uma interface web intuitiva e interativa, os operadores têm acesso a uma ampla gama de opções de configuração, garantindo maior praticidade e eficiência. A versatilidade da plataforma permite que ela seja acessada de qualquer ambiente por meio dos navegadores Google Chrome®, Firefox® ou Safari®, desde que estejam conectados à mesma rede local, otimizando o processo de configuração dos dispositivos.

Para utilizar a Interface Web, é essencial que o dispositivo esteja conectado à mesma rede do computador. O acesso é realizado diretamente pelo endereço IP do dispositivo.

# CHANGELOG

**OBS.: Esse produto não possui Wi-Fi e nem PoE.**

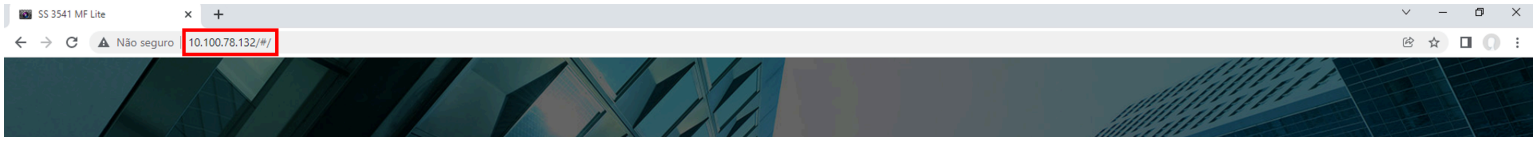
---

# AMBIENTAÇÃO

## Acesso

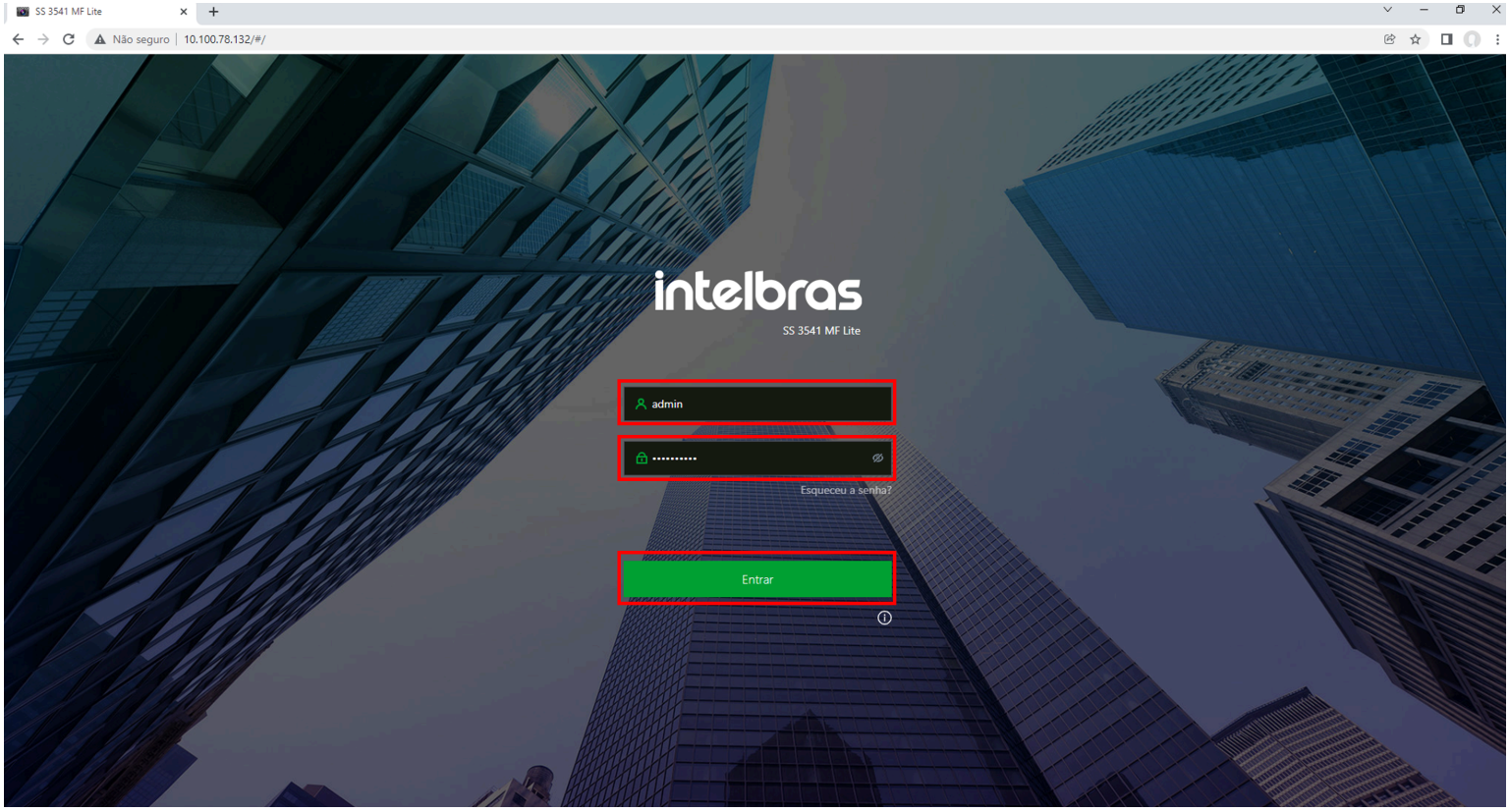
Para acessar o dispositivo, utilize um navegador de internet, como Google Chrome®, Firefox® ou Safari®. Digite na barra de endereço o IP previamente configurado, seja ele atribuído automaticamente por DHCP ou configurado manualmente como IP dinâmico.

**Atenção: O IP exibido em imagens ou exemplos é apenas ilustrativo. Certifique-se de utilizar o IP específico do seu dispositivo.**

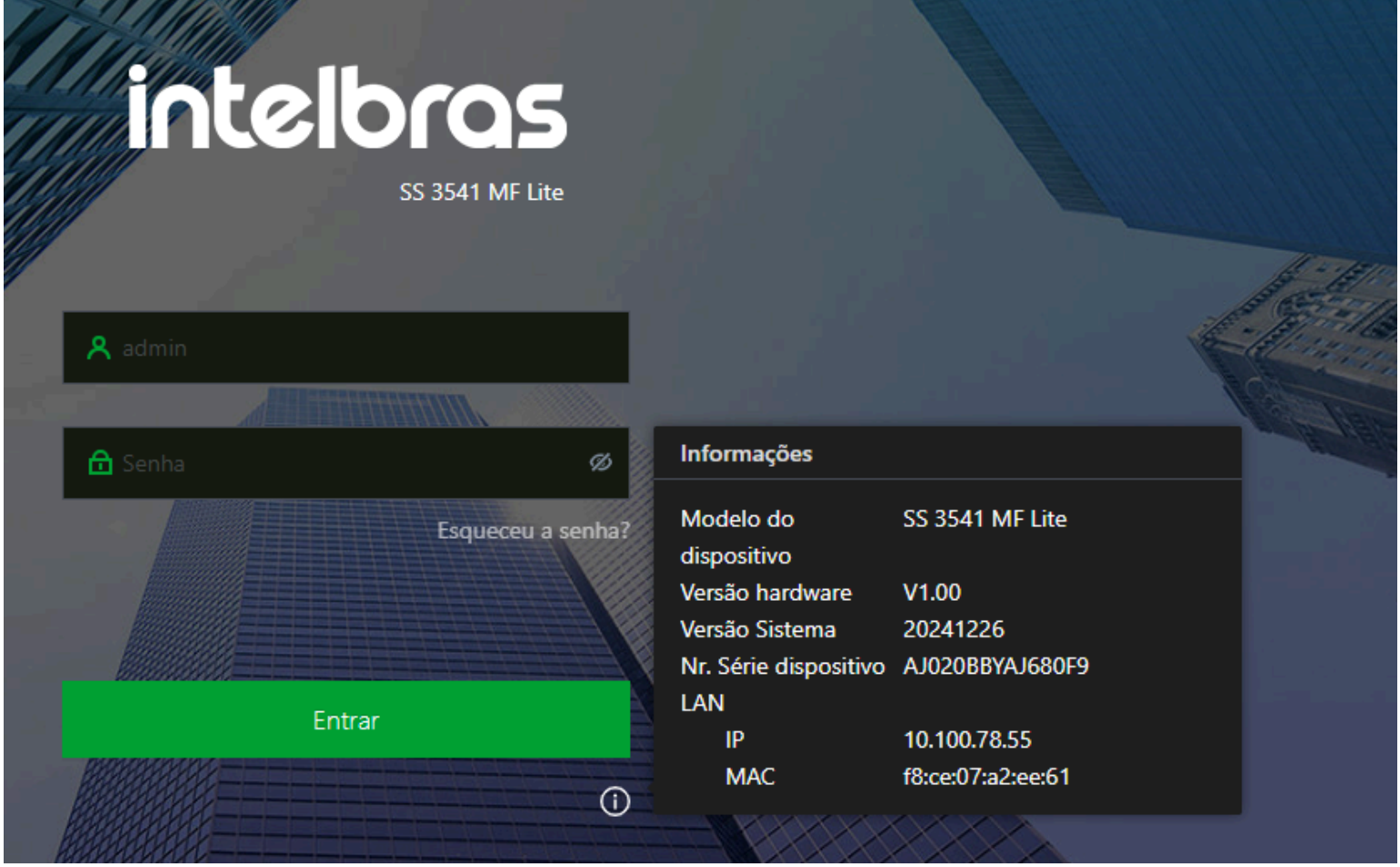



# Login

Após acessar o sistema, realize o login inserindo 'admin' no campo Usuário e a senha de administrador configurada durante a inicialização do dispositivo.



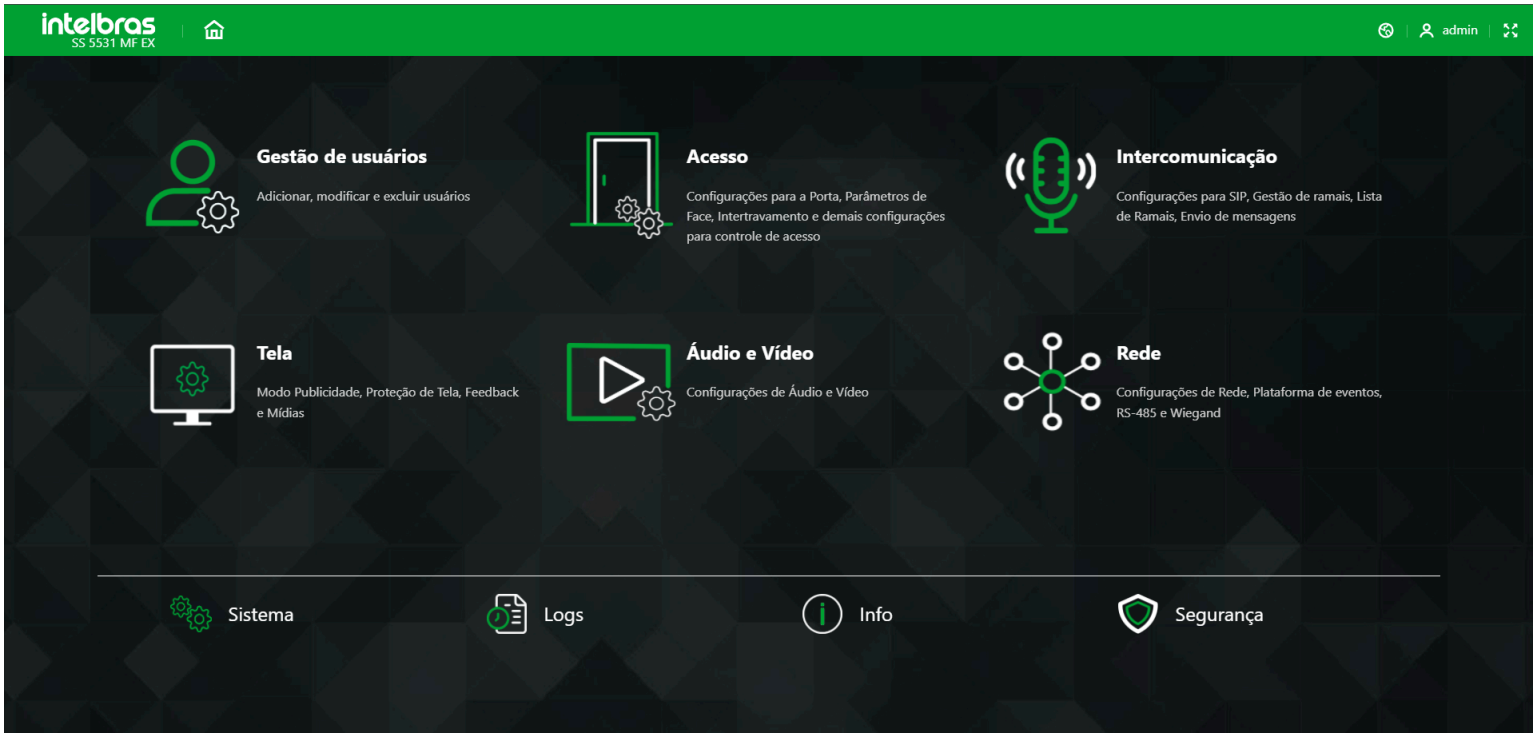

Para visualizar informações do dispositivo, basta clicar no ícone correspondente. 




# Menu Principal

Após realizar o login, a página é redirecionada para a tela do menu principal.

Na tela principal, é possível selecionar as páginas de configurações que deseja visualizar e configurar.

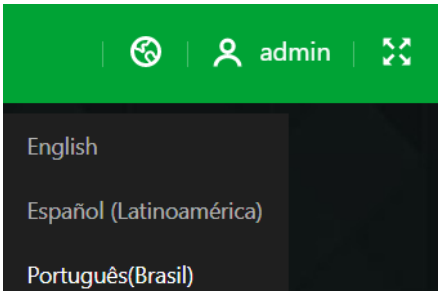



# Menu de informações

No canto superior esquerdo, é exibido o modelo do dispositivo. Na parte central, aparece o título da página atualmente aberta no sistema. O ícone (  ) permite retornar à página inicial a qualquer momento. Já o ícone (  ) possibilita a seleção do idioma da interface web e do produto por meio de um submenu.

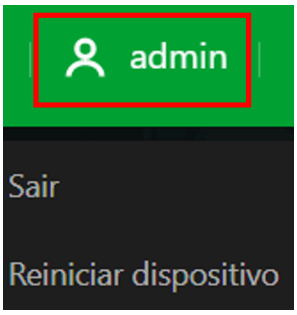

## Idioma

Ao clicar no ícone ( ), é possível escolher entre os idiomas: Inglês, Espanhol e Português. Após selecionar o idioma desejado, o dispositivo será reiniciado para aplicar as alterações.




## Informações usuário

Ao clicar com o mouse sobre o ícone de usuário ou no nome 'admin', é possível encerrar a sessão ou reiniciar o dispositivo. Ao selecionar qualquer uma das opções, uma tela de confirmação será exibida com as opções 'Sim' ou 'Não'.



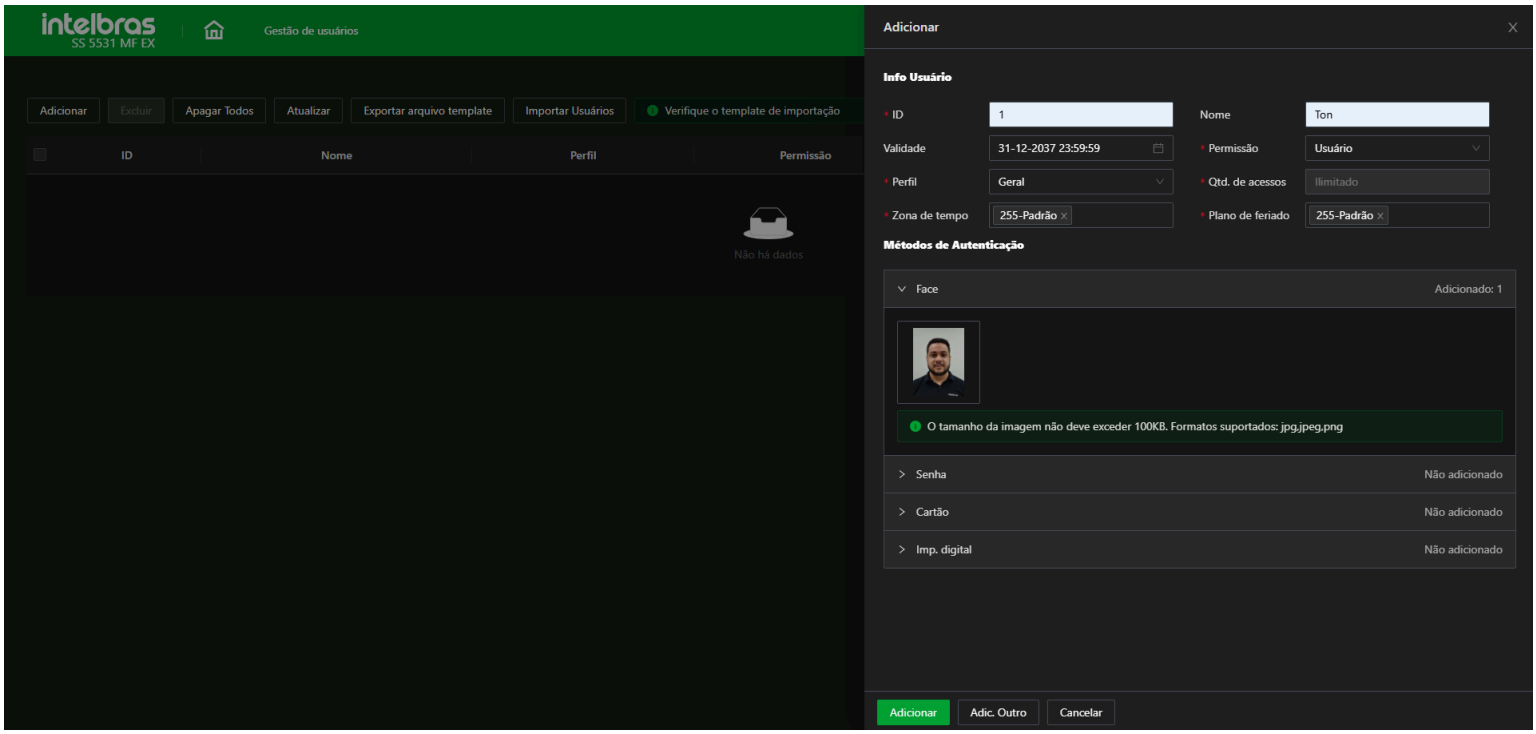

---

# Gestão de usuários

O menu Gestão de usuário oferece opção para cadastro de um novo usuário, visualizar e editar lista de usuários e lista de administradores e excluir usuarios.

## Adicionando usuários

Na página inicial, selecione "Gestão de Usuários" e, em seguida, clique em "Adicionar".




# Info. Usuário

- **ID:** Número que identifica o usuário. Esse número deve ser único, entretanto pode ser personalizado pelo administrador como, por exemplo, a matrícula ou alguma referência ao apartamento, sala etc.
- **Nome:** Nome que será exibido para esse usuário.
- **Validade:** Data limite que esse usuário terá acesso. A partir dessa data o usuário continuará cadastrado no dispositivo, mas seu acesso será negado.
- **Permissão:** Define se esse cadastro será de um usuário comum ou um usuário Admin. Este último com acesso ao menu principal e todas as configurações do dispositivo.
- **Perfil:** Define o perfil que será atribuído ao usuário. Dos quais:
  - **Geral:** Usuários com o perfil Geral podem realizar o acesso normalmente.
  - **VIP:** Libera o acesso independente das configurações de zona de tempo ou regra de anti-passback.
  - **Visitante:** O usuário tem um número limitado de acessos a esse dispositivo.
  - **Ronda:** Apenas registra evento, não faz nenhum acionamento.
  - **Bloqueados:** O usuário inserido desse perfil gera um evento de alarme ao efetuar o acesso.
  - **PcD:** Estende o tempo de acionamento em 5 segundos para pessoa com deficiência.
  - **Usuário 1:** Reservado para customização. Usuários podem realizar o acesso normalmente.
  - **Usuário 2:** Reservado para customização. Usuários podem realizar o acesso normalmente.
- **Qtd. de acessos:** Campo permite selecionar quantos acessos o usuário Visitante (do campo anterior) pode realizar no dispositivo.
- **Zona de tempo:** ID da zona de tempo atribuída ao usuário.
- **Plano feriado:** ID do plano de feriado atribuída ao usuário.

## Métodos de autenticação

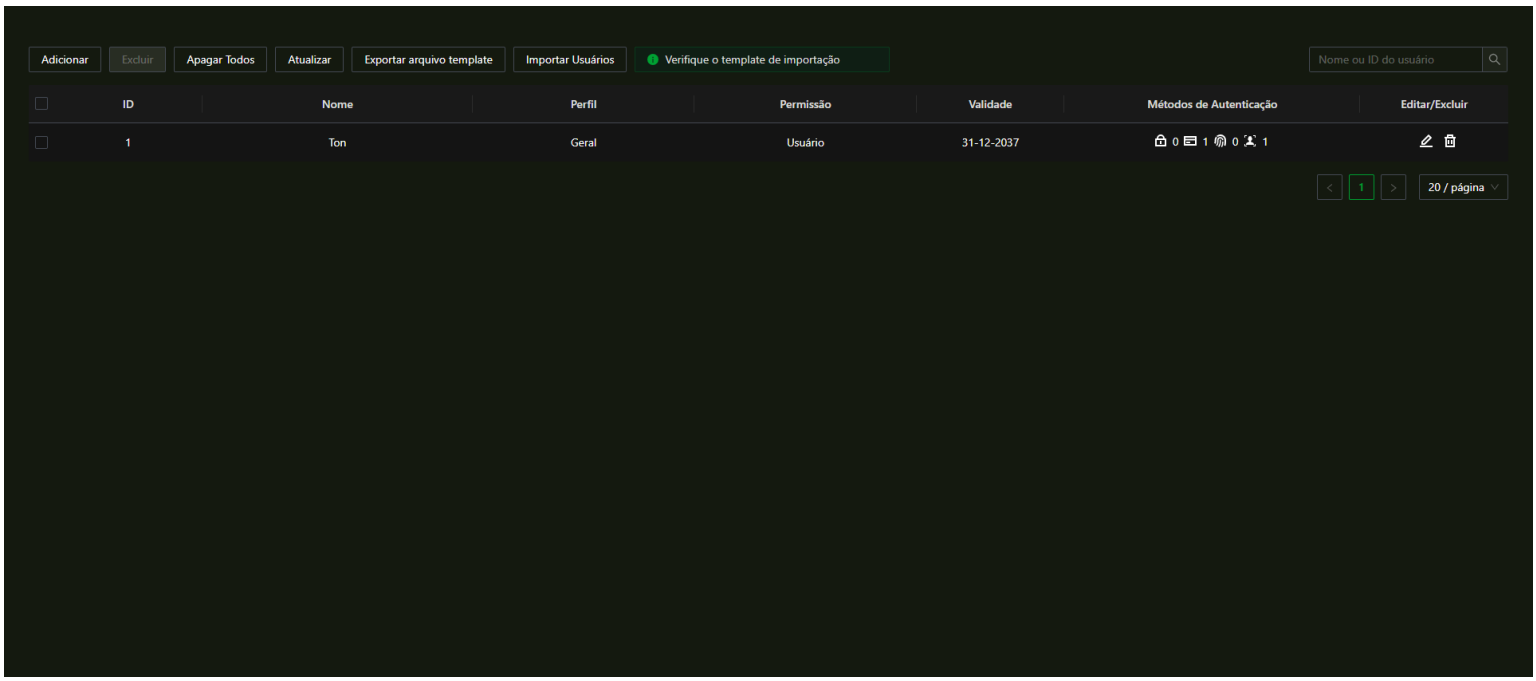
- **Face:** Foto do usuário que será utilizada para identifica-lo através do método de autenticação de reconhecimento facial.
- **Senha:** Permite a criação de uma senha de acesso individual de até 8 dígitos numéricos. Para acessar por esse método de autenticação é necessário que o usuário insira também a ID do usuário.
- **Cartão:** Permite o cadastro de até 5 cartões ou tags RFID por usuários. Nessa opção é permitido habilitar um desses cadastros como coação (emite um alerta para o software de monitoramento e/ou aciona uma saída de alarme).
- **Imp. digitais:** Permite o cadastro de até 3 impressões digitais por usuário. Nessa opção é permitido habilitar um desses cadastros como coação (emite um alerta para o software de monitoramento e/ou aciona uma saída de alarme).

**Função disponível apenas para modelos que possuem leitor de biometria digital.**

- **Ok:** Salva as alterações feitas.
- **Cancelar:** Cancela as configurações realizadas.

## Operações Relacionadas

Na tela principal do menu "Gestão de Usuário", é possível visualizar uma lista com informações detalhadas, incluindo quais credenciais cada usuário possui e a quantidade de credenciais atribuídas. Além disso, por meio do ícone ( ) é possível editar as informações ou excluir informações através do ícone ( ) conforme necessário.



- **Apagar Todos:** Ao selecionar esta opção, será exibida uma tela de confirmação para verificar se você deseja excluir todos os usuários cadastrados.

**Atenção:** A exclusão é permanente e não será possível restaurar os usuários excluídos. A recuperação só será viável se houver um backup previamente realizado.

- **Atualizar:** Atualiza a lista de usuários cadastrados no dispositivo.
- **Exportar arquivo template:** Clique para baixar o modelo e insira as informações dos usuários.

**Obs:** Coloque as fotos para reconhecimento facial e o arquivo no formato .xml no mesmo diretório.

- **Importar Usuários:** Ao clicar abrirá uma janela para importar a pasta com os arquivos de importação.
- **Barra de busca:** Pesquise pelo nome de usuário ou pelo ID do usuário.

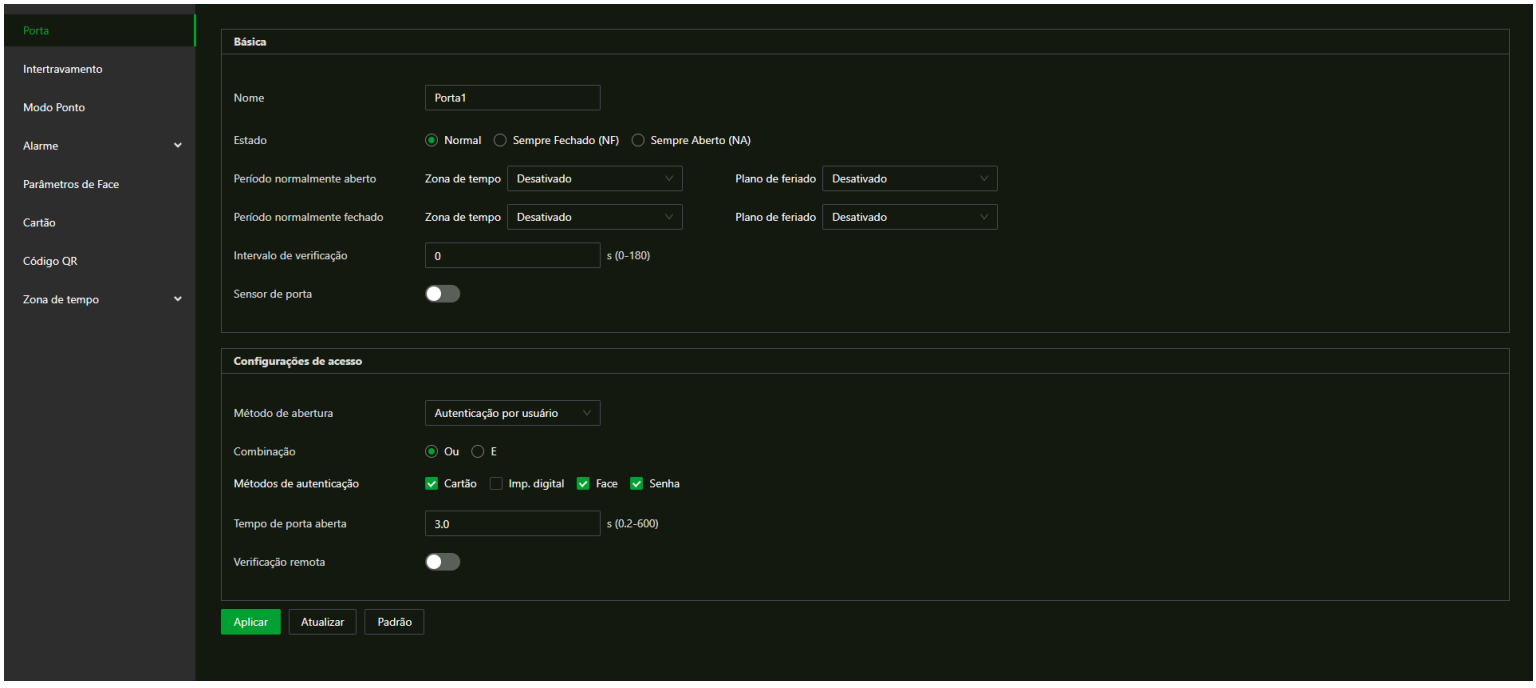
---

# ACESSO

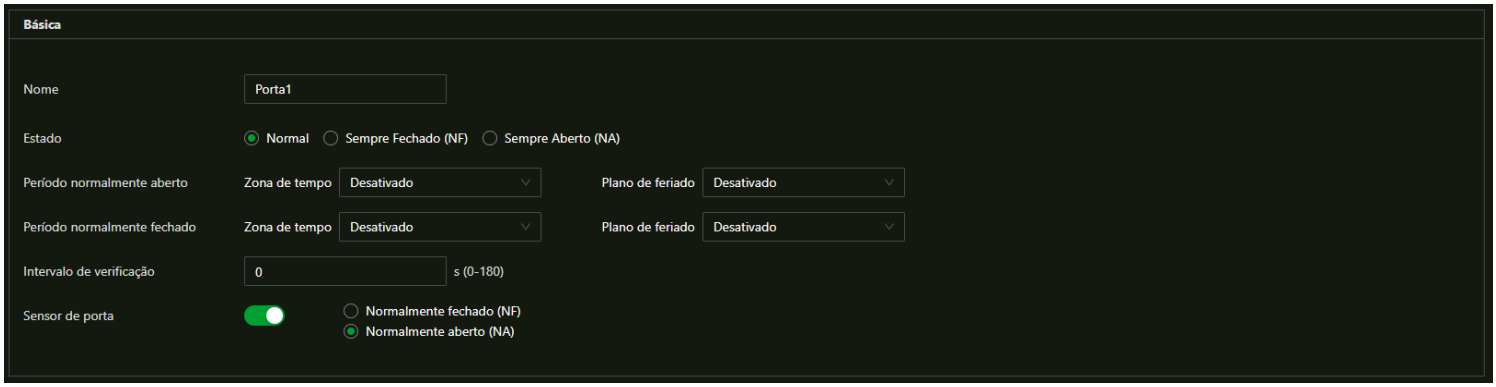
Este é o menu onde você pode configurar a Porta, os Parâmetros de Reconhecimento Facial, o Intertravamento e outras opções para o controle de acesso.

## Porta

O painel de Porta oferece ao usuário as configurações referentes a ativação do relé do dispositivo. Abaixo, os esclarecimentos de cada item.



# Básica




- **Nome:** Define o nome referente ao ponto de acesso em que o dispositivo será vinculado.
- **Estado:** São três opções, que determinam as condições de acionamento do relé de porta.
  - **Normal:** Porta será liberada com uma credencial válida
  - **Sempre fechado (NF):** Define que a porta estará sempre fechada, ou seja, não haverá acionamento mesmo que uma credencial válida seja verificada.
  - **Sempre aberto (NA):** Define que a porta estará sempre aberta, ou seja, relé de acionamento sempre ativo.

- **Período normalmente aberto:** Período pré-determinado em que o dispositivo abre a porta independente da zona de tempo a que pertença. Ao expandir as opções, é possível selecionar qualquer **zona de tempo** já criada para usar como período.
- **Período normalmente fechado:** Período pré-determinado em que o dispositivo mantém a porta fechada independente da zona de tempo a que pertença. Ao expandir as opções, é possível selecionar qualquer **zona de tempo** já criada para usar como período.

**Obs.:** Quando o período normalmente aberto entra em conflito com o período normalmente fechado, o período normalmente aberto tem prioridade sobre o período normalmente fechado.

- **Plano de feriado:** Os períodos com um ID de feriado configurado permitem o acesso liberado(quando atribuído ao periodo normalmente aberto) ou negado(quando atribuído ao periodo normalmente fechado) para um usuario durante o período definido para o feriado previamente configurado.

**Obs.:** Quando o período entra em conflito com o plano de feriado, o plano de feriado têm prioridade sobre os períodos.

- **Intervalo de verificação:** Se o usuário verificar sua identidade várias vezes em um curto período, apenas a primeira verificação será válida, e a porta não abrirá nas tentativas seguintes. A partir do momento em que a porta não abrir, você precisará esperar pelo intervalo de tempo configurado antes de tentar verificar sua identidade novamente.
- **Sensor de porta:** Quando habilitado, um sensor magnético de abertura conectado ao seu dispositivo pode acionar um alarme caso as portas sejam abertas ou fechadas de maneira anormal. O sensor de portas possui dois tipos de

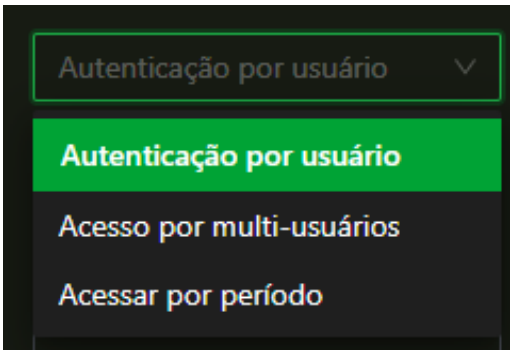
operação:

- **Normalmente fechado (NF):** O sensor permanece em estado de curto-circuito enquanto a porta estiver fechada.
- **Normalmente aberto (NA):** Um circuito aberto é formado quando a porta está realmente fechada.

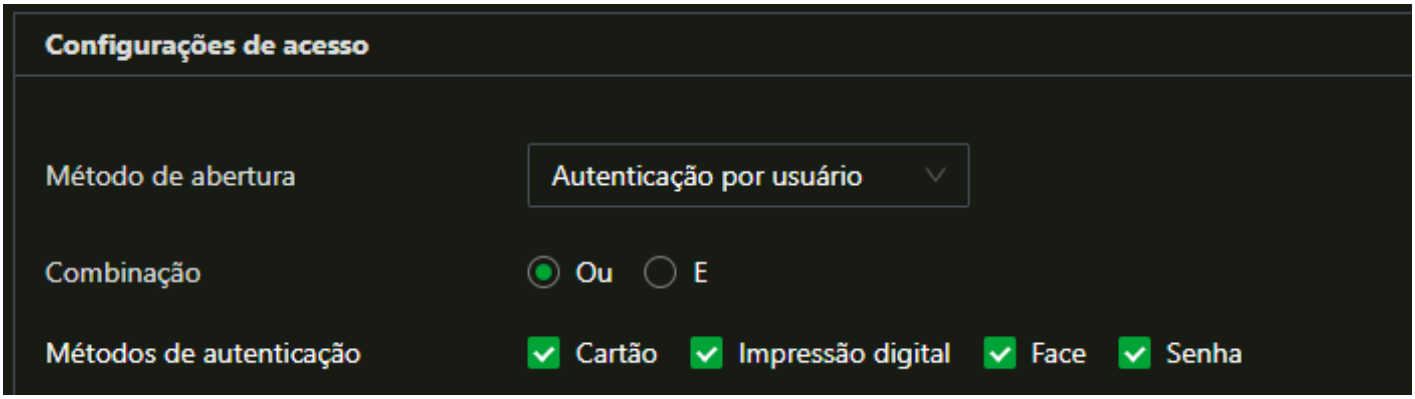
# Configurações de acesso

É possível realizar abertura de porta utilizando diferentes métodos de acesso, como cartão, impressão digital (apenas para o modelo SS 3541 MF Lite), reconhecimento facial ou senha. Além disso, você pode combinar esses métodos para criar um método de desbloqueio personalizado.

- **Método de abertura:** São três opções, que determinam o método de abertura: Autenticação por usuário, acesso por multi-usuários ou acessar por período.




- **Autenticação por usuário:** Habilita a opção de combinação "OU" ou "E" e os checkboxes para selecionar os métodos de autenticação necessários na combinação para a liberação da porta.

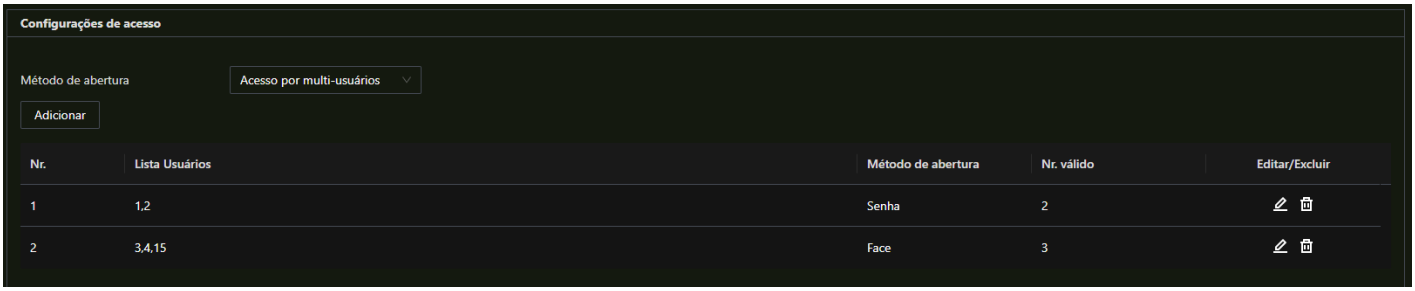



- **Combinação:**
  - **OU:** o usuário utiliza de qualquer um dos métodos selecionado para realização do acesso, ou seja, considerando as opções Cartão e Face selecionadas, o usuário terá seu acesso liberado se fazer a verificação apenas da Face e também terá seu acesso liberado se fizer a liberação apenas através do cartão/tag RFID.
  - **E:** o usuário terá que utilizar todos os métodos selecionados para que o seu acesso seja liberado, ou seja, caso as opções Cartão e Face estejam selecionadas, o usuário terá que passar seu cartão/tag RFID e na sequência realizar a verificação da Face. O acesso é liberado ao verificar ambas as credenciais.

**Obs.:** Ao selecionar a combinação no modo "E", é importante seguir a ordem em que o dispositivo solicitará as credenciais. A sequência respeitará os métodos de autenticação configurados, sendo: cartão, impressão digital (disponível apenas no modelo SS 3541 MF Lite), reconhecimento facial e senha.

- **Métodos autenticação**
  - **Cartão:** Se esta opção for selecionada, exige que seja aproximado do controlador no local indicado (  ) ou de um leitor externo conectado, um cartão RFID cadastrado para realizar uma autenticação válida.
  - **Imp. Digital:** Se esta opção for selecionada, exige que uma biometria digital seja verificada no controlador de acesso ou em um leitor externo para realizar uma autenticação válida. Disponível apenas no modelo SS 3541 MF Lite.
  - **Face:** Se esta opção for selecionada, será necessário verificar uma face previamente cadastrada na câmera do controlador de acesso.
  - **Senha:** Se esta opção for selecionada, exige que seja inserido no controlador de acesso uma ID de usuário e a senha de usuário já cadastrado.

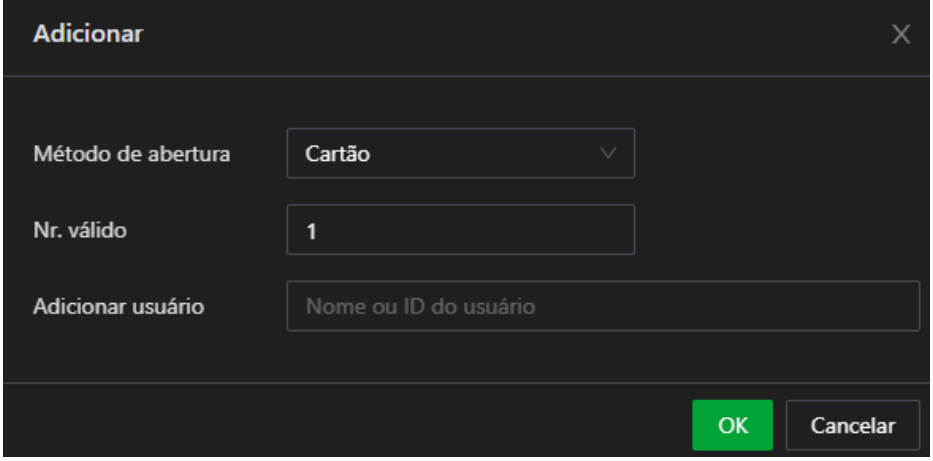
- **Acesso por multi-usuários:** Quando habilitada, Se apenas um grupo for adicionado, a porta será destrancada somente quando o número de pessoas no grupo que concedem acesso atingir o número válido definido.



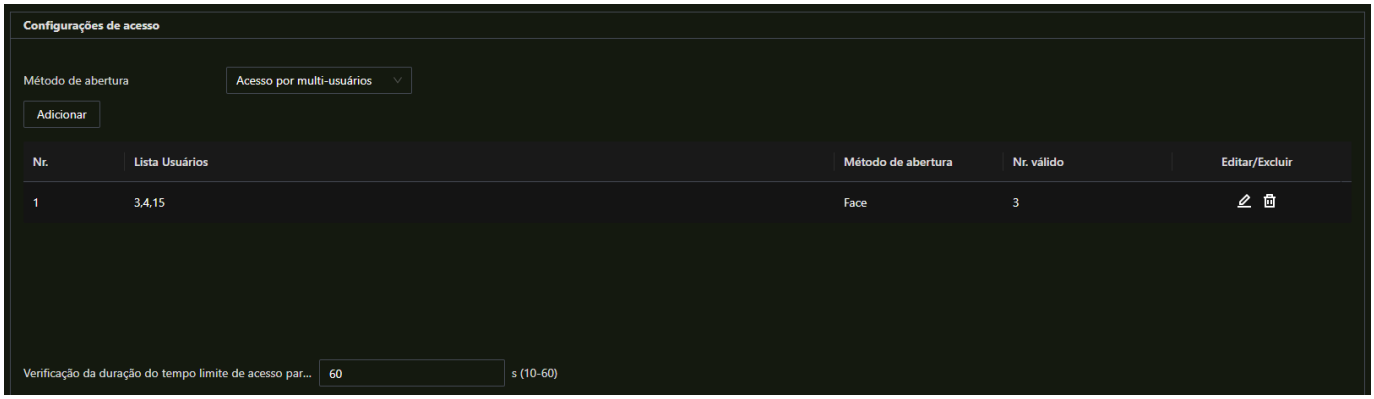

Se mais de um grupo for adicionado, a porta será destrancada apenas quando o número de pessoas em cada grupo que concedem acesso atingir o número válido definido. É possível adicionar até 4 grupos.

- **Tela de combinações:** Nessa tela, é possível visualizar as listas de combinações já existentes, criar novas listas ou editar as listas existentes. Clique no botão de adição ( 

 ) para adicionar uma nova lista de combinação, no ícone de editar (  ) para editar uma combinação já existente ou no ícone de excluir (  ) para excluir uma combinação.

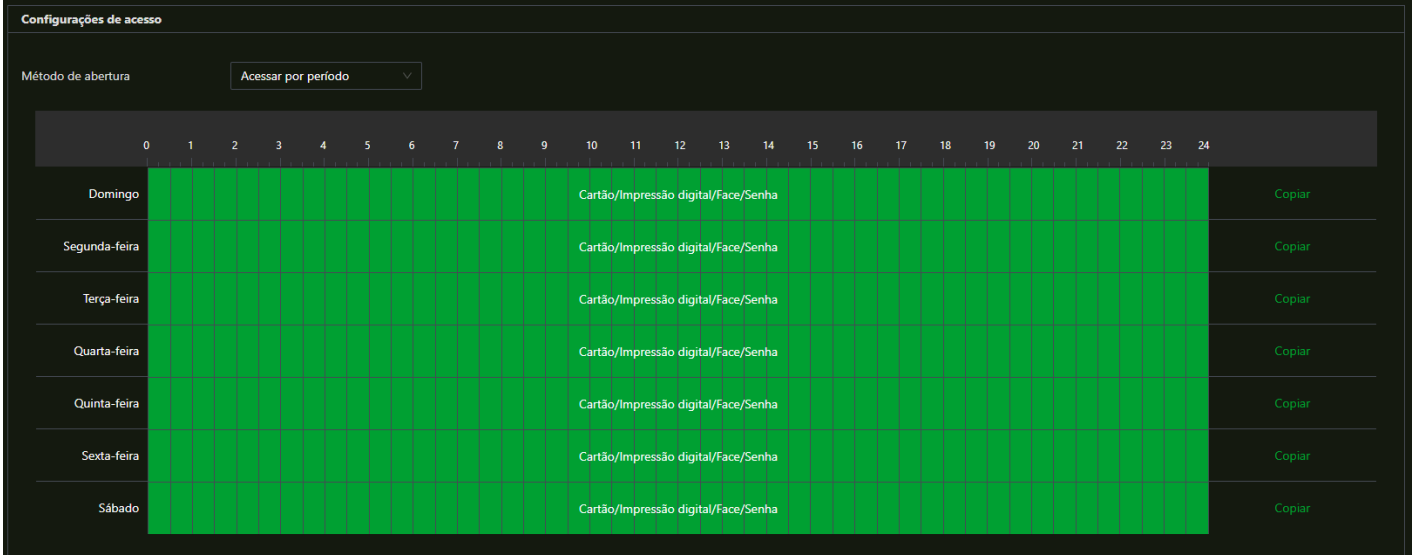



- **Método de abertura:** Seleciona o tipo de credencial que será verificada na combinação. É possível escolher entre Cartão, impressão digital, senha ou face.
- **Nr. válido.:** Indica a quantidade de pessoas em cada grupo que precisam verificar suas identidades no dispositivo antes que a porta seja destrancada.
- **Adicionar usuários:** É necessário inserir o número de ID dos usuários que deverão se autenticar nesta etapa para que ela seja validada. O limite máximo de usuários na lista é 50. Caso seja inserido um usuário que não possui o tipo de credencial selecionada cadastrado, o dispositivo irá negar a autenticação.
  Por fim, ao concluir as definições, clique em OK para salvar ou Cancelar para desfazer as alterações.




- **Exemplo:**
  Por exemplo, se o número válido for configurado como 3 para um grupo, qualquer combinação de 3 pessoas desse grupo deverá verificar suas identidades para destravar a porta.
- **Verificação da duração do tempo limite de acesso para multi-usuários:** Tempo de validade para a realização dos acessos. Após o tempo configurado, o contador é zerado, e será necessário validar novamente as credenciais que foram verificadas anteriormente.

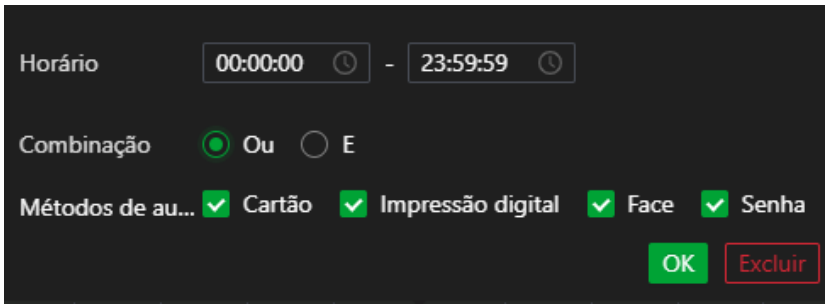
- **Acessar por período:** Permite selecionar os tipos de credenciais que serão aceitas em um período específico do dia.

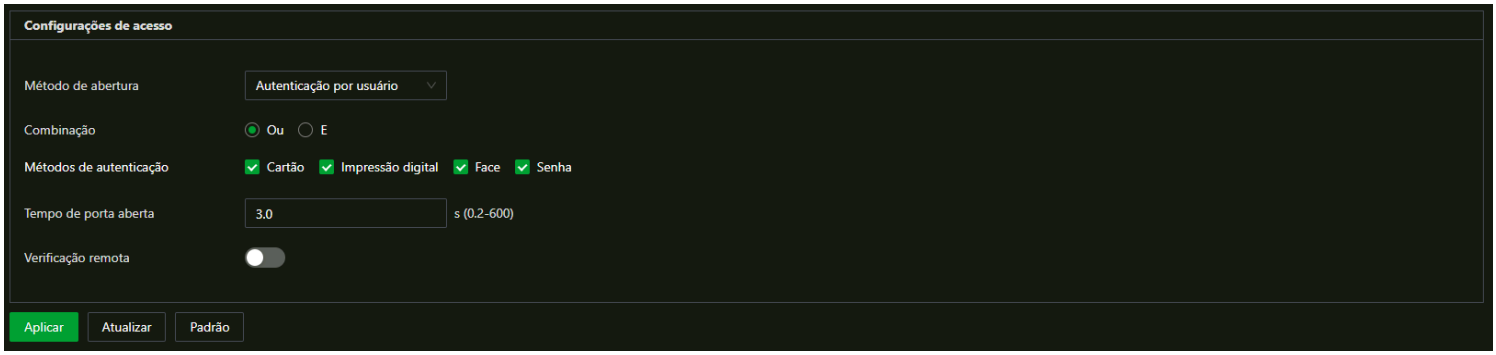



- **Tela de edição:**

  Ao clicar sobre o dia da semana desejado ou arrastar o ponteiro do mouse , é possível ajustar o período de tempo para cada dia, o tipo de combinação "OU" e "E" e o tipo de credencial, há quatro possibilidades: **cartão**, **impressão digital**, **face** e **senha.**

  Por fim, ao concluir as definições, clique em OK para salvar ou Cancelar para desfazer as alterações.




- **Tempo de porta aberta:** Após a autorização de acesso, a porta permanecerá destrancada por um período configurado, permitindo a passagem da pessoa. Esse intervalo pode ser configurado entre 0,2 a 600 segundos.
- **Verificação remota:** Habilita ou desabilita o dispositivo para realizar acessos gerenciados por um operador utilizando o software Defense IA.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.

- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

# Intertravamento

Um intertravamento de portas, é um sistema de segurança que coordena a operação de duas portas, garantindo que elas não possam ser abertas simultaneamente.

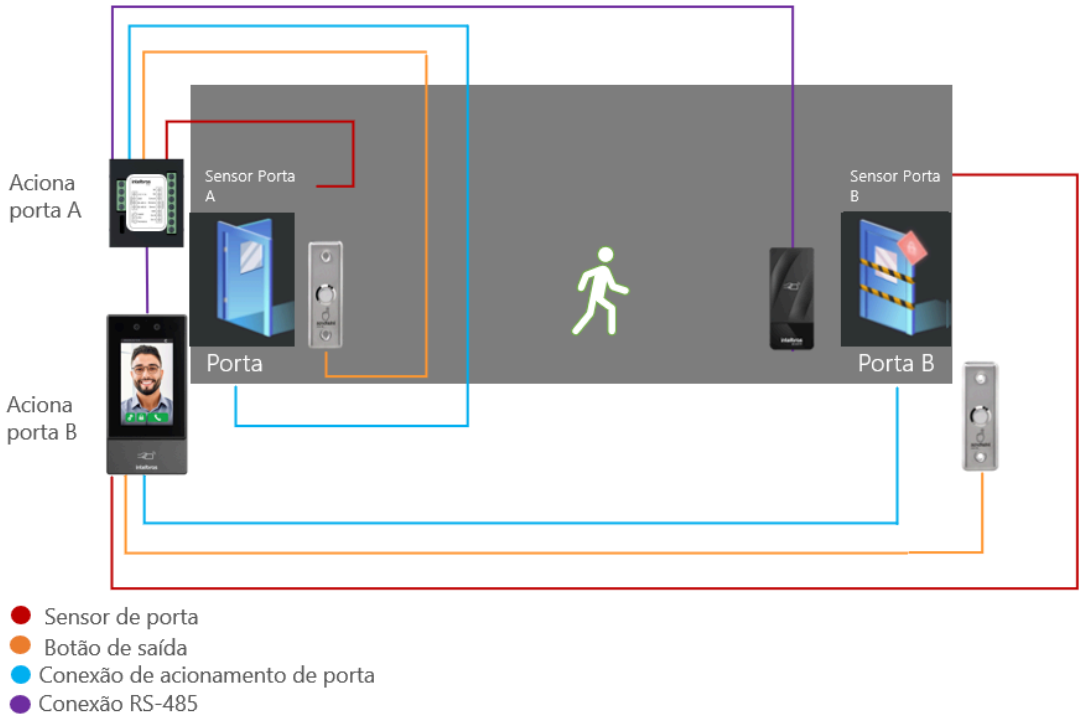
Um exemplo comum de intertravamento de portas é em bancos, onde duas portas são usadas em uma entrada sequencial (uma eclusa). A primeira porta precisa ser fechada antes que a segunda possa ser aberta, aumentando a segurança contra invasões.

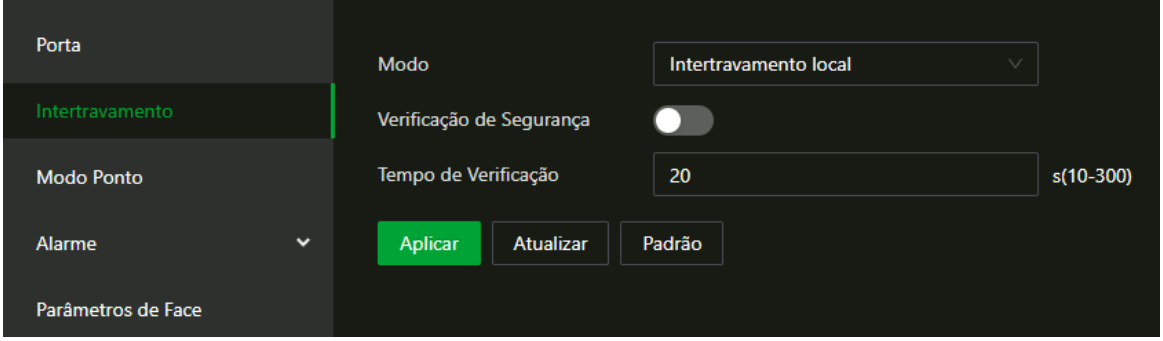
- **Modo Intertravamento local**

  Nesse formato de aplicação, quando habilitado, o XR 2201(módulo de segurança) irá efetuar o monitoramento e controle da porta A. O controlador de acesso, através da interface Wiegand, sensores e botão de saída, irá efetuar o monitoramento e controle da porta B.

  Para o funcionamento correto é necessário habilitar o XR 2201 como módulo de segurança, verificar se o sensor de porta está habilitado e conectar um leitor Wiegand na entrada respectiva do controlador de acesso. Para mais detalhes de configuração do módulo de segurança e leitor Wiegand, acesse o menu Porta Serial

  **Esquema de ligação**






- **Verificação de Segurança:** Quando habilitado, exige que o mesmo usuário realize a entrada pelas portas da eclusa. Caso o usuário autentique na primeira porta e o tempo configurado expire, a passagem pela segunda porta será bloqueada. Para concluir o acesso, será necessário iniciar um novo ciclo de autenticação dentro do tempo definido.
- **Tempo de Verificação:** Tempo limite para que o usuário realize a passagem dentro da eclusa.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.
- **Obs.:** Por padrão de fábrica a função intertravamento vem desabilitada.

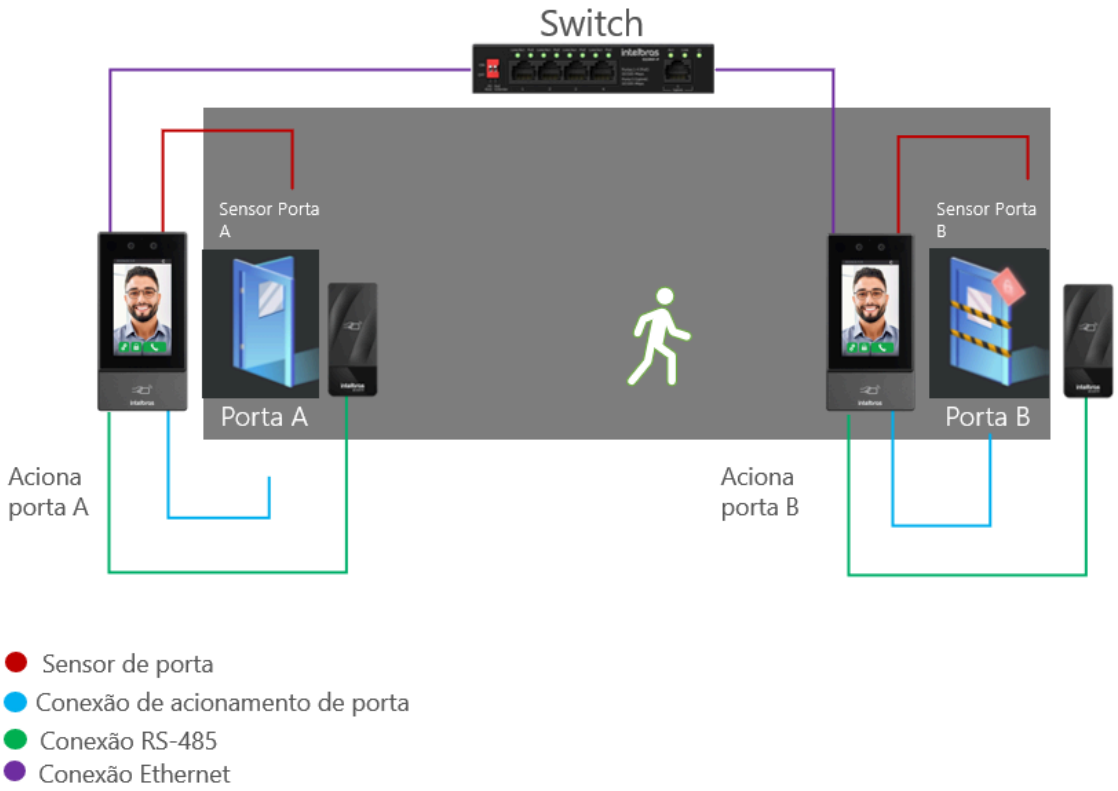
- **Modo Intertravamento inteligente**

O intertravamento inteligente funciona em dois controladores de acesso facial, um como função do principal e o segundo como função secundário.

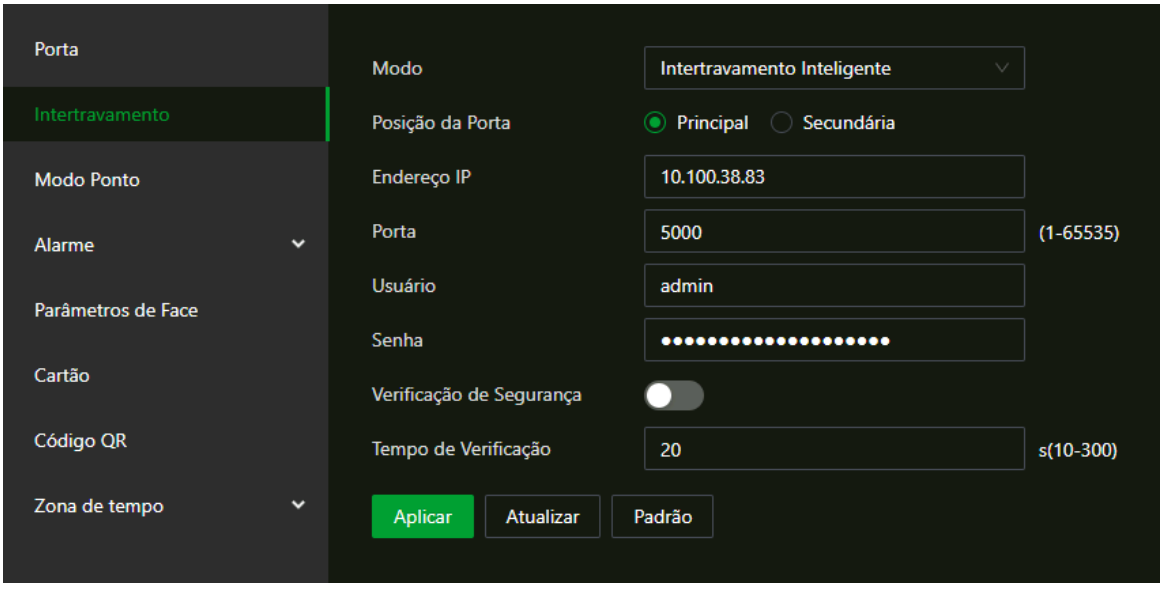
Nesse formato, os controladores deverão está interligados em rede local, preferencialmente via cabo de rede. Pode ser utilizado através de um roteador ou ponto a ponto, desde que tenha um switch para realizar a comunicação.

Para o funcionamento correto é necessário ter conectividade em rede local entre os controladores configurados como IP estático, com a opção de DHCP desabilitado, verificar se o sensor de porta está habilitado, conectar um leitor RS-485 ou Wiegand nas respectivas entradas do controlador de acesso. Para mais detalhes de configuração acesse o menu Porta Serial

**Esquema de ligação - Leitor RS-485**




**Obs:** Para o fluxo de saída e abertura de portas, poderá ser utilizado os leitores ou o botão de saída (botoeira) ligação aos controladores de acesso faciais.

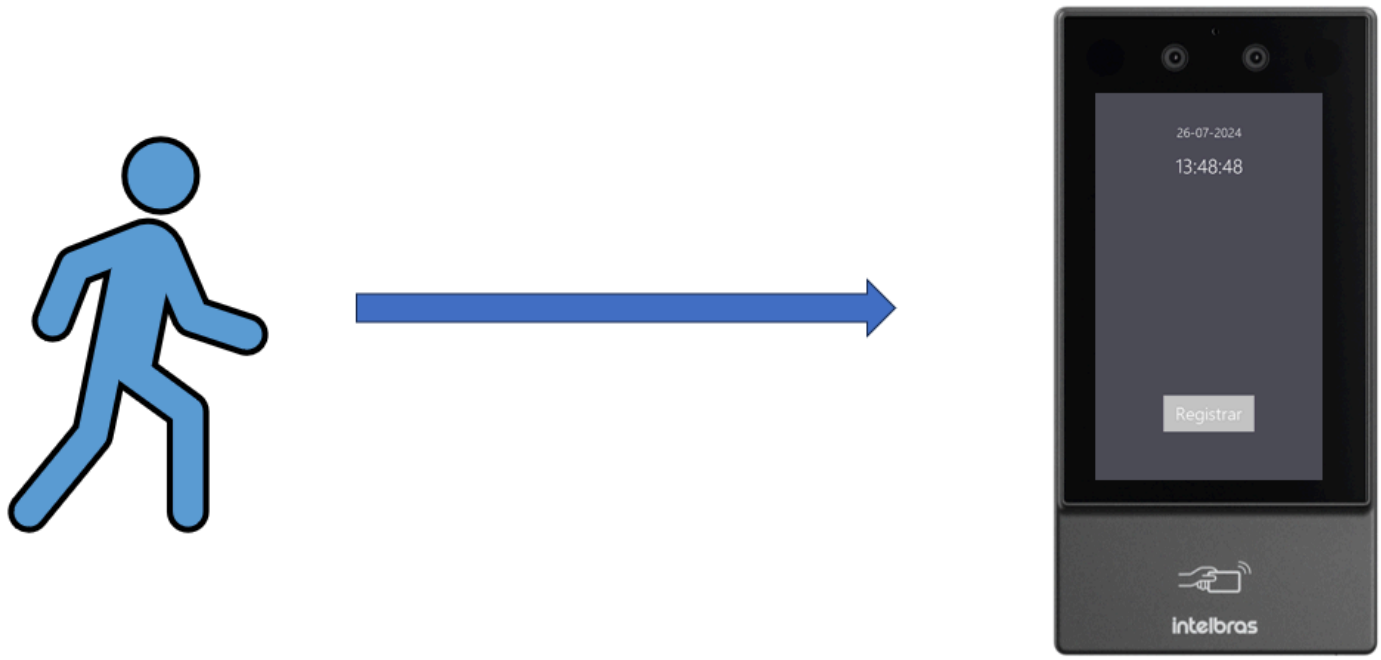



- **Posição da porta:** Define quem será o controlador principal ou secundário.
- **Endereço IP:** Define o IP do controlador secundário, quando definido como secundário o IP a ser configurado é o do controlador primário.
- **Porta:** Padrão 5000. Recomendamos não realizar alteração.
- **Usuário:** admin, mesmo utilizado para acesso ao menu do facial.
- **Senha:** mesma utilizado para acesso ao menu do facial.
- **Verificação de Segurança:** Quando habilitado, exige que o mesmo usuário realize a entrada pelas portas da eclusa. Caso o usuário autentique na primeira porta e o tempo configurado expire, a passagem pela segunda porta será bloqueada. Para concluir o acesso, será necessário iniciar um novo ciclo de autenticação dentro do tempo definido.

- **Tempo de Verificação:** Tempo limite para que o usuário realize a passagem dentro da eclusa.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.
- **Obs.:** Por padrão de fábrica a função intertravamento vem desabilitada.

# Modo Ponto

Essa função, quando habilitada, deixará o dispositivo de controle de acesso facial com uma proteção de tela exibindo continuamente a data no formato DD/MM/AAAA e a hora no formato HH:MM:SS, além de um botão fixo para registro. Isso permite que o usuário realize a marcação do ponto no trabalho de forma fácil e intuitiva.

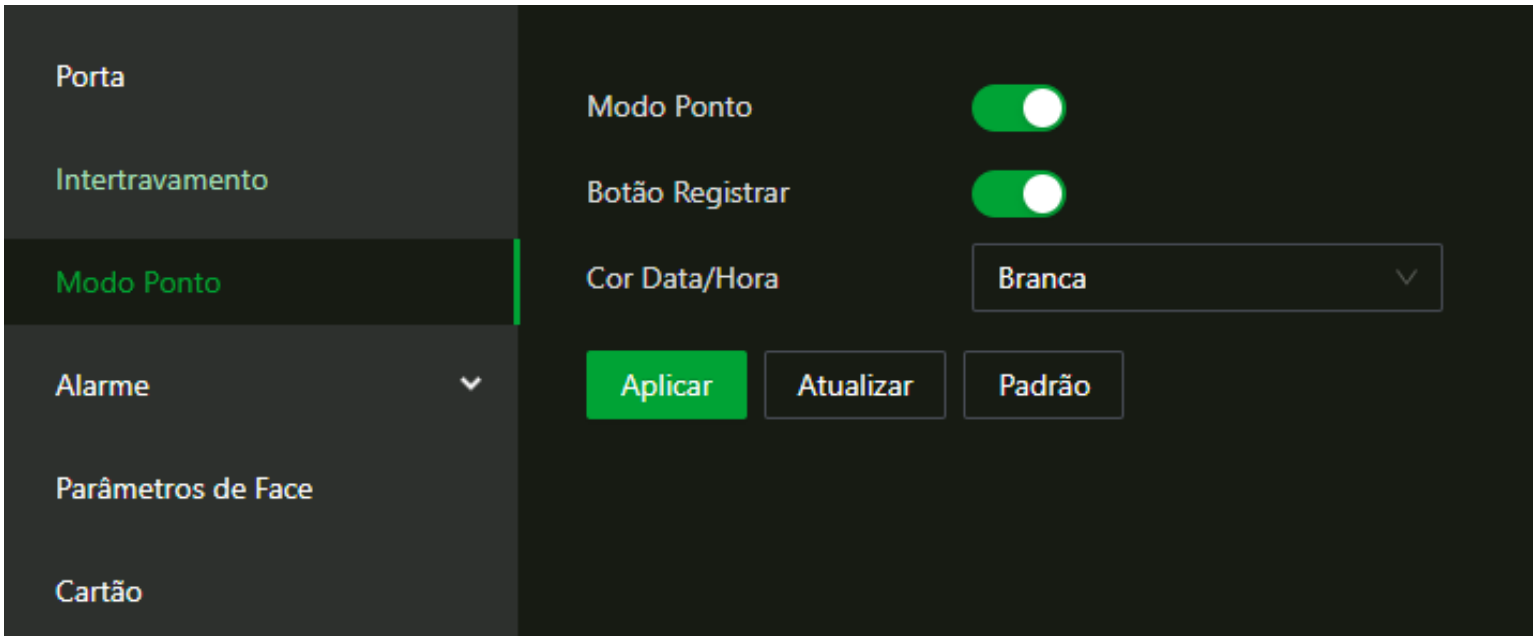



Nesse exemplo, com a função modo ponto ativada, o usuário deve primeiro clicar em "registrar" para utilizar sua credencial e realizar o acesso/registro de ponto.

Com essa função ativa, o dispositivo apresenta comportamento de coletor "REP-P", ou seja, irá coletar o registro de ponto e encaminhar ao software responsável pela gestão do ponto. A integração do dispositivo com o software de gerenciamento do ponto, será através da API Intelbras de integração.

Para mais informações acesse: www.intelbras-caco-api.intelbras.com.br (https://intelbras-caco-api.intelbras.com.br/)

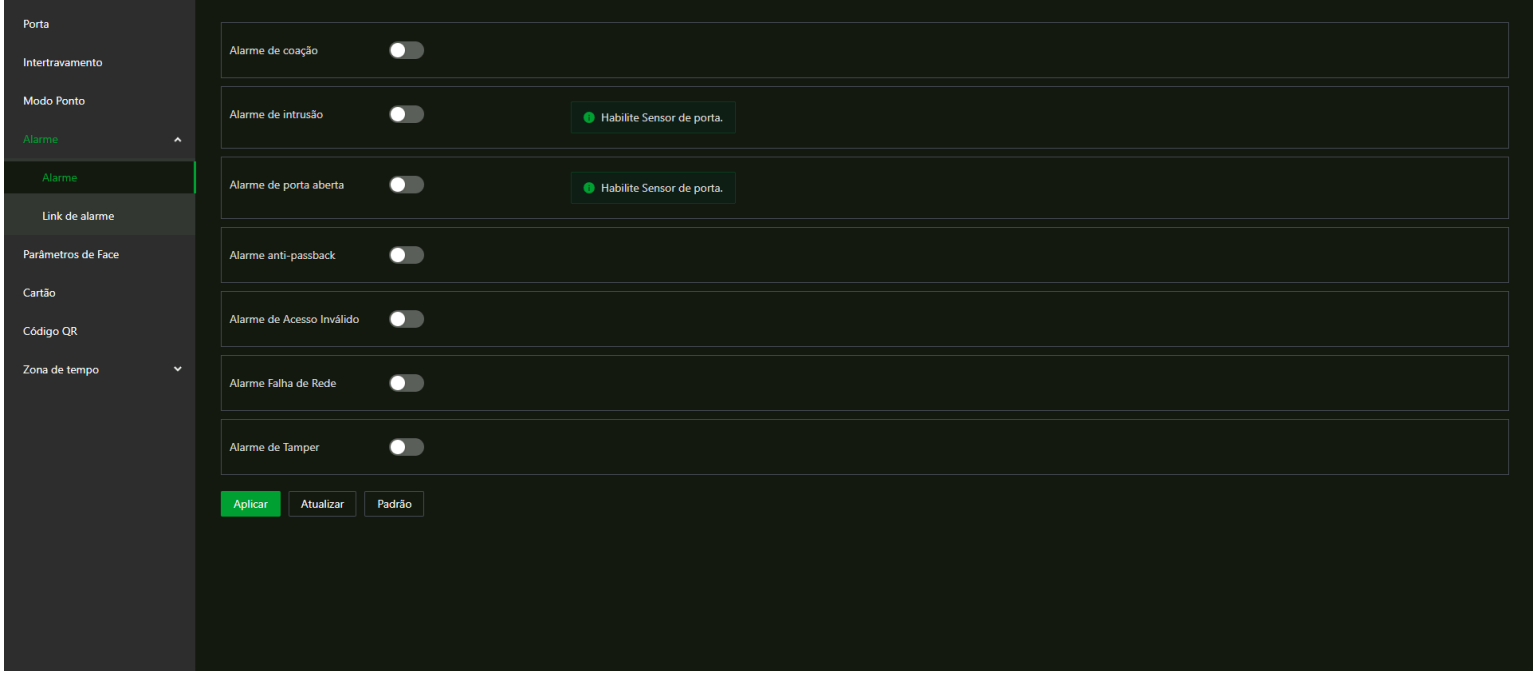
- Habilitando função ponto




- **Modo ponto:** Quando o checkbox estiver verde, a função será habilitada.
- **Botão registrar:** Quando o checkbox estiver verde, a função será habilitada e o botão de registro aparecerá na tela do facial. O acesso será realizado apenas quando o usuário pressionar o botão.
- **Cor Data/Hora:** É possível escolher até trê opções de cores na exibição de data e hora. Pois o plano de fundo da função ponto por padrão é cinza, mas poderá ser alterado na opção de proteção de tela. Para mais detalhes consulte as opções mídias e proteção de tela no menu PERSONALIZAÇÃO.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

# Alarme

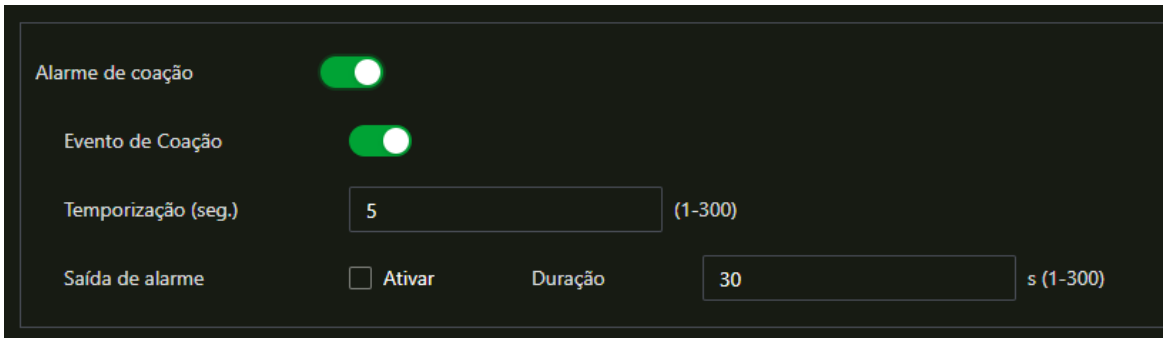
Esse menu é possível configurações vários tipos de alarme disponíveis no dispositivo.




# Alarme

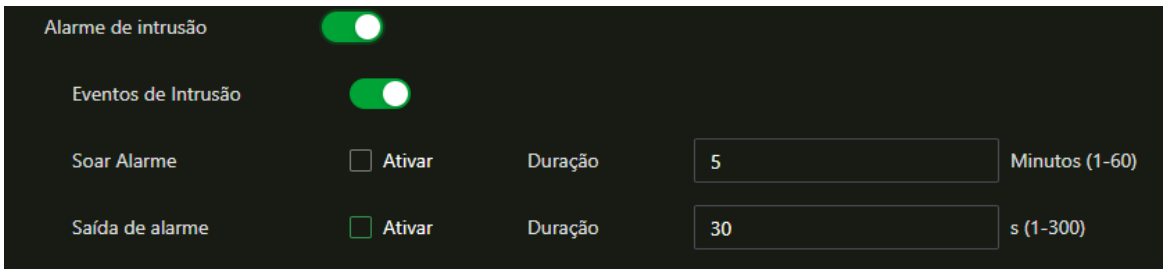
Um ou mais alarmes serão acionados sempre que ocorrer um evento de acesso anormal.

## Alarme de coação



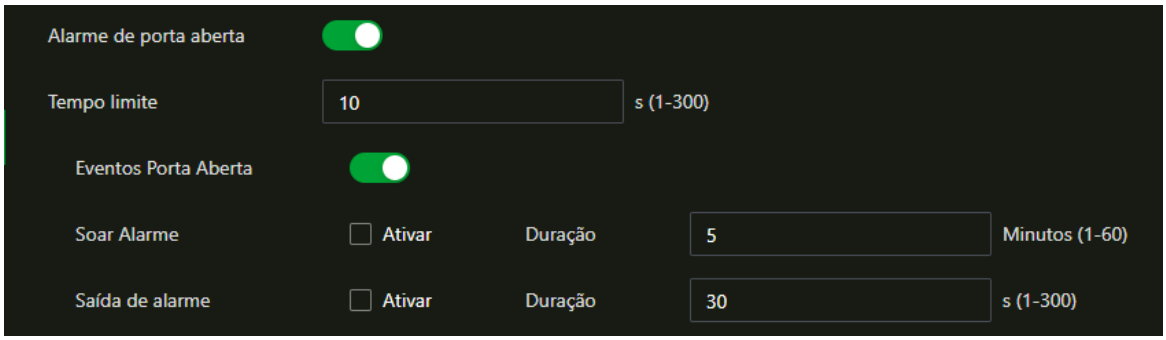

- **Alarme coação:** Quando habilitado, permite que um alarme seja acionado sempre que um cartão de coação, senha de coação ou impressão digital de coação for usado para destrancar a porta.
- **Temporização (seg.):** Define o tempo entre a liberação de acesso com a credencial de coação e a ativação do alarme.
- **Saída de alarme:** Habilita ou desabilita a saída auxiliar de alarme.
- **Duração:** Define o tempo que a saída auxiliar de alarme fica ativa.

## Alarme de intrusão



- **Eventos de intrusão:** Quando habilitado, Se a porta for aberta de forma anormal, um alarme de intrusão será acionado e permanecerá ativo pelo tempo definido.
- **Soar alarme:** Habilita um alarme sonoro no dispositivo.
- **Duração (minutos):** Define o tempo de duração do alarme sonoro do dispositivo.
- **Saída de alarme:** Habilita saída auxiliar de alarme do dispositivo.
- **Duração (seg.):** Define o tempo que a saída auxiliar de alarme fica ativa.

## Alarme de porta aberta

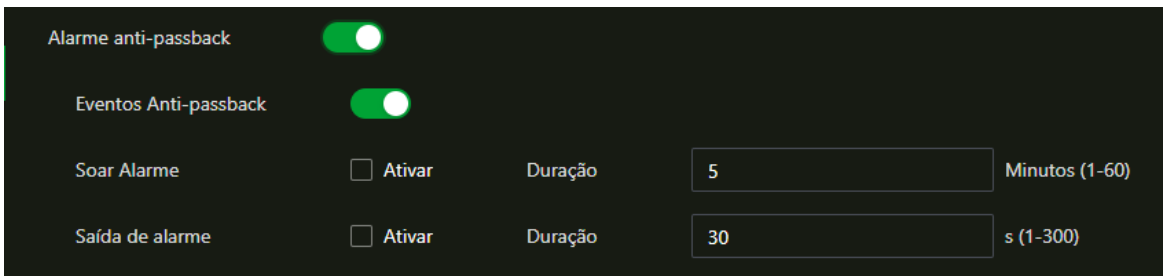



- **Tempo limite:** Quando habilitado, se a porta permanecer destrancada por mais tempo do que a duração do tempo limite configurado, o alarme será acionado e durará pelo tempo definido.

**Obs.:** A função de sensor de porta e o tempo limite da porta precisam estar habilitados ao mesmo tempo.

- **Eventos porta aberta:**Quando habilitado, Se a porta for aberta de forma e não for trancada antes do tempo limite configurado, um alarme será acionado e permanecerá ativo pelo tempo definido.
- **Soar alarme:** Habilita um alarme sonoro no dispositivo.
- **Duração (minutos):** Define o tempo de duração do alarme sonoro do dispositivo.
- **Saída de alarme:** Habilita saída auxiliar de alarme do dispositivo.
- **Duração (seg.):** Define o tempo que a saída auxiliar de alarme fica ativa.

## Alarme anti-passback




- **Eventos anti-passback:** Quando habilitado, os usuários precisam confirmar suas identidades tanto na entrada quanto na saída; caso contrário, um alarme será disparado. Isso evita que alguém use o cartão de acesso para

passar para outra pessoa. Com a função de anti-passback ativada, o usuário precisa sair da área segura usando um leitor de saída para poder entrar novamente.

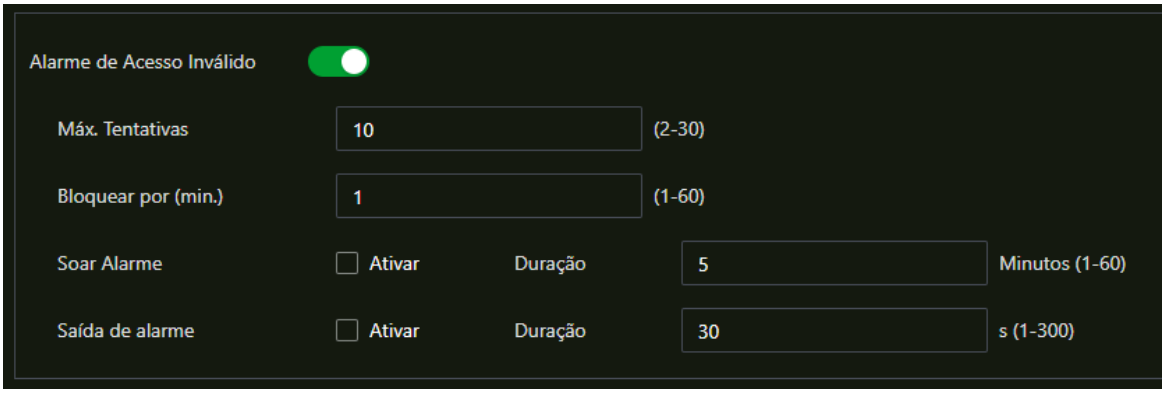
**Obs.[1]:** O acesso será negado e um alarme acionado caso o usuário entre ou saia sem autorização.

**Obs.[2]:** Em dispositivos conectados a uma única fechadura, a verificação no dispositivo indica entrada, e no leitor externo, saída.

Essa configuração pode ser ajustada em configurações de comunicação.

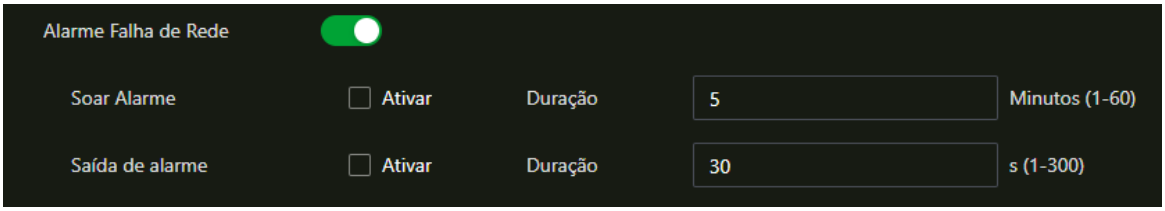
- **Soar alarme:** Habilita um alarme sonoro no dispositivo.
- **Duração (minutos):** Define o tempo de duração do alarme sonoro do dispositivo.
- **Saída de alarme:** Habilita saída auxiliar de alarme do dispositivo.
- **Duração (seg.):** Define o tempo que a saída auxiliar de alarme fica ativa.

# Alarme de Acesso Inválido




- **Alarme de Acesso Inválido:** Quando habilitado, Se uma senha ou cartão incorreto for usado ao número máximo tentativas consecutivas, em um intervalo de 60 segundos, o alarme por uso excessivo de cartão inválido será acionado e o dispositivo permanecerá bloqueado pelo tempo definido.
- **Máx. tentativas:** Define o número máximo de tentativas incorretas permitidas antes que o dispositivo seja bloqueado.
- **Bloquear por (min.):** Define tempo máximo para que o dispositivo seja bloqueado após as tentativas máximas excedidas.
- **Soar alarme:** Habilita um alarme sonoro no dispositivo.
- **Duração (minutos):** Define o tempo de duração do alarme sonoro do dispositivo.
- **Saída de alarme:** Habilita saída auxiliar de alarme do dispositivo.
- **Duração (seg.):** Define o tempo que a saída auxiliar de alarme fica ativa.

# Alarme Falha de Rede




- **Alarme Falha de Rede:** Quando habilitado, se houver desconexão com a rede ethernet o dispositivo irá emitir um alarme.
- **Soar alarme:** Habilita um alarme sonoro no dispositivo.
- **Duração (minutos):** Define o tempo de duração do alarme sonoro do dispositivo.
- **Saída de alarme:** Habilita saída auxiliar de alarme do dispositivo.
- **Duração (seg.):** Define o tempo que a saída auxiliar de alarme fica ativa.

# Alarme de Tamper

- **Alarme de Tamper:** Quando habilitado, se o dispositivo for removido da sua base de fixação irá emitir um alarme.
- **Soar alarme:** Habilita um alarme sonoro no dispositivo.
- **Duração (minutos):** Define o tempo de duração do alarme sonoro do dispositivo.
- **Saída de alarme:** Habilita saída auxiliar de alarme do dispositivo.
- **Duração (seg.):** Define o tempo que a saída auxiliar de alarme fica ativa.

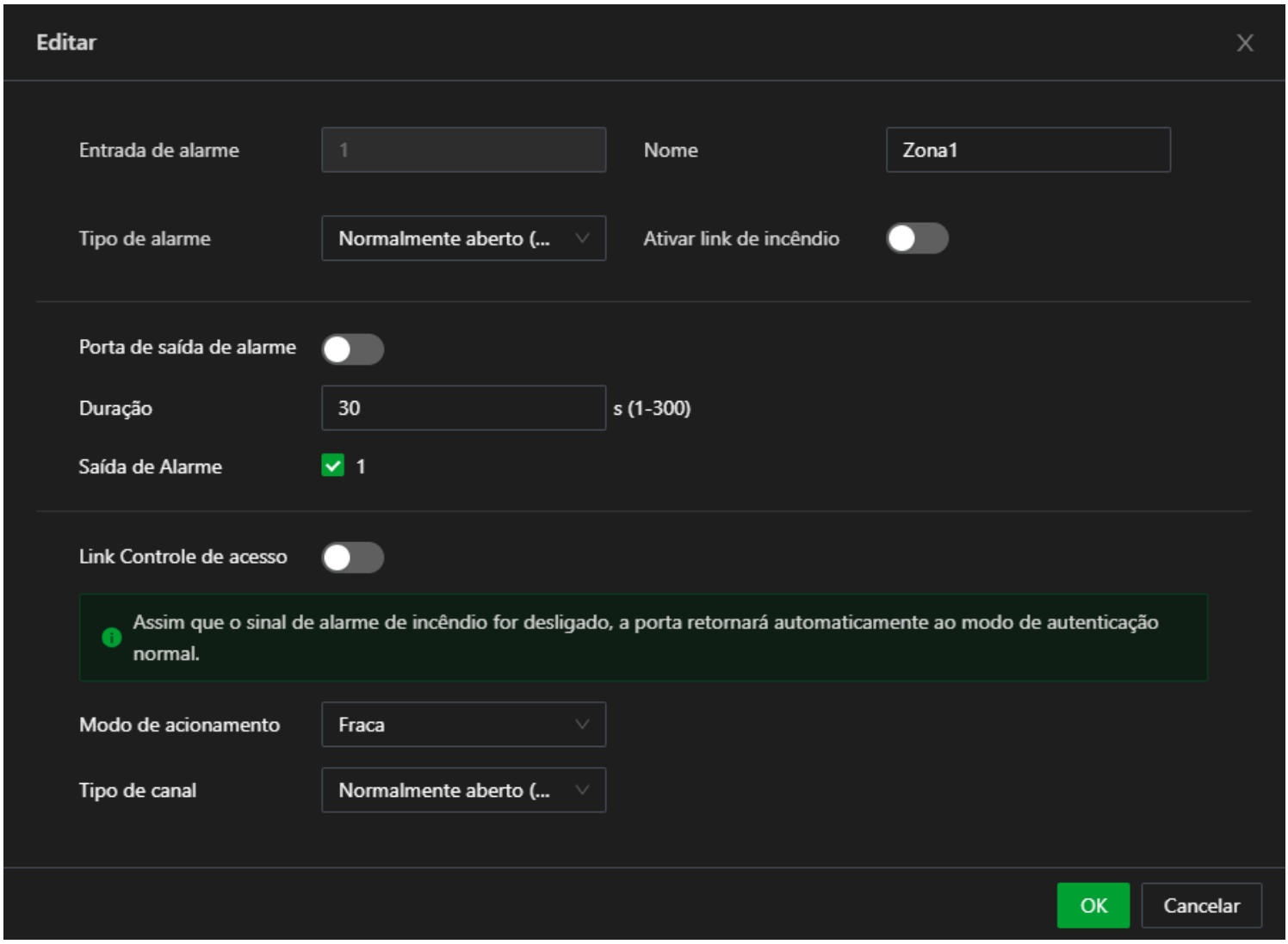
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

# Link de alarme

Dispositivos de alarme podem ser conectados ao controlador de acesso, permitindo configurar as ações que o controlador deve executar ao receber um sinal na entrada de alarme.


# Edição da configuração de vinculação de alarme

Na tela principal do menu configuração de vinculação de alarme, é possível visualizar uma lista com informações. Por meio do ícone (  ) é possível editar as informações.



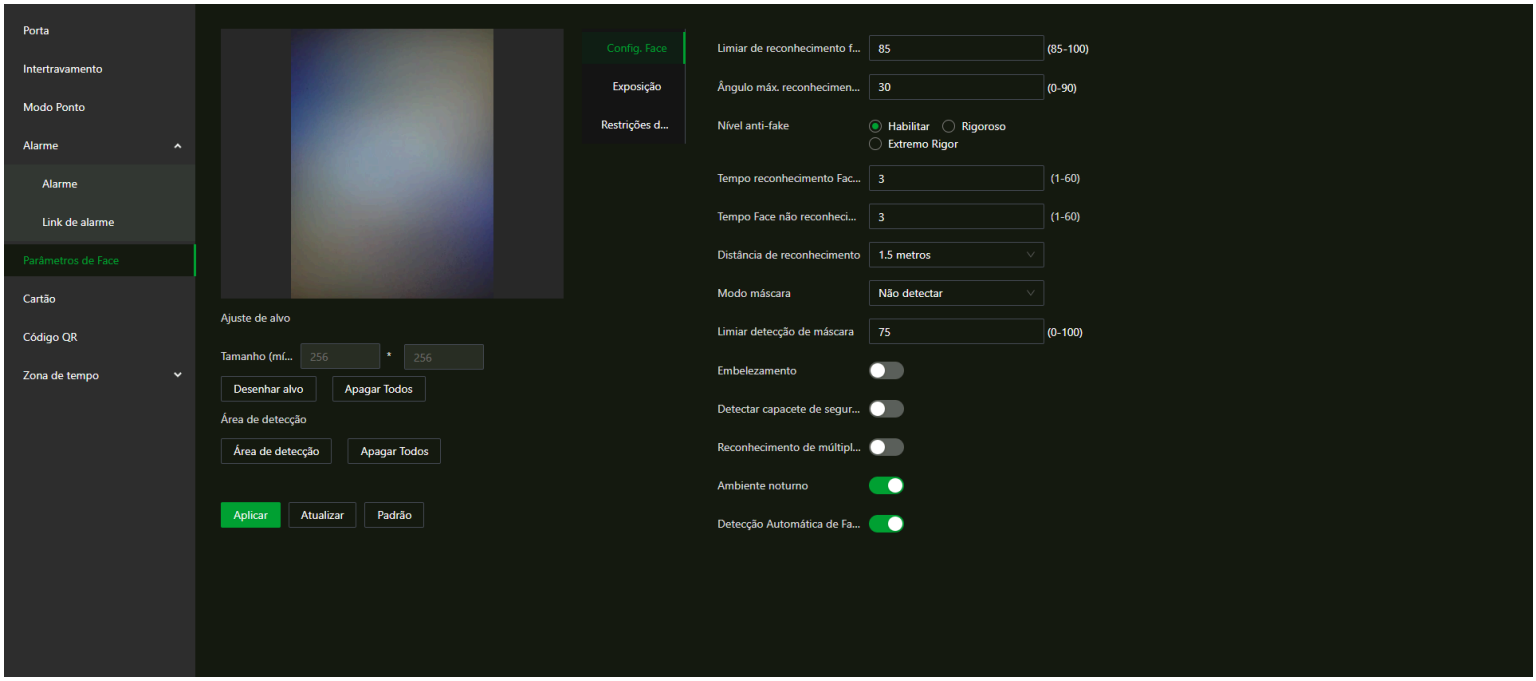

- **Entrada de alarme:** Não é possível alterar. A Entrada 1 está vinculada ao alarme 1 (ALM1_IN) e a Entrada 2 ao alarme 2 (ALM2_IN).
- **Nome:** É possível definir um nome nome para a zona de alarme.
- **Tipo de alarme:** Selecione de acordo com o sistema de alarme:
  - **Ao selecionar NA (Normalmente Aberto)**, o alarme será disparado quando for detectado o fechamento do contato entre o GND e a entrada de alarme.
  - **Ao selecionar NF (Normalmente Fechado)**, o alarme será disparado quando for detectado que a entrada de alarme não está conectada ao GND.
- **Ativar link de incêndio:** Se o link de incêndio estiver ativado, o controlador de acesso acionará a saída de alarme e destravará a porta ao receber um sinal na entrada de alarme. Ao ativar o link de incêndio, a saída de alarme é ativada e a porta configurada como "sempre aberta" será destravada. Certifique-se de revisar as demais configurações para garantir a ação desejada.
- **Porta de saída de alarme:** Habilita ou desabilita o uso da saída de alarme.
- **Duração:** Tempo durante o qual o contato recebido na entrada de alarme permanecerá ativado.
- **Saída de Alarme:** Habilita ou desabilita o acionamento da saída de alarme.
- **Ativar link de incêndio:** Quando habilitado, ativa as funções Porta de saída de alarme e Link Controle de acesso.

- **Link Controle de acesso:** Quando habilitado, vincular o controle de acesso ao acionamento do alarme de incêndio.
- **Modo de acionamento:**
  - **Fraca:** Assim que o sinal de alarme de incêndio for desligado, a porta retornará automaticamente ao modo de autenticação normal.
  - **Forte:** Assim que o sinal de alarme de incêndio for desligado, a porta ficará no status atual. Altere manualmente para o modo de autenticação normal.
- **Tipo de canal:**
  - **Normalmente Fechado (NF):** A entrada de alarme está em um estado de circuito fechado quando o alarme não foi disparado. Abertura do circuito fechado ativa o alarme.
  - **Normalmente Aberto (NA):** O dispositivo de entrada de alarme está em um estado de circuito aberto quando o alarme não foi disparado. Fechamento do circuito ativa o alarme.

    **Obs.:** Se quiser vincular o controle de acesso ao acionamento do alarme de incêndio, ative a opção Vinculação de Controle de Acesso.
- **Ok:** Salva as alterações feitas.
- **Cancelar:** Cancela as configurações realizadas.

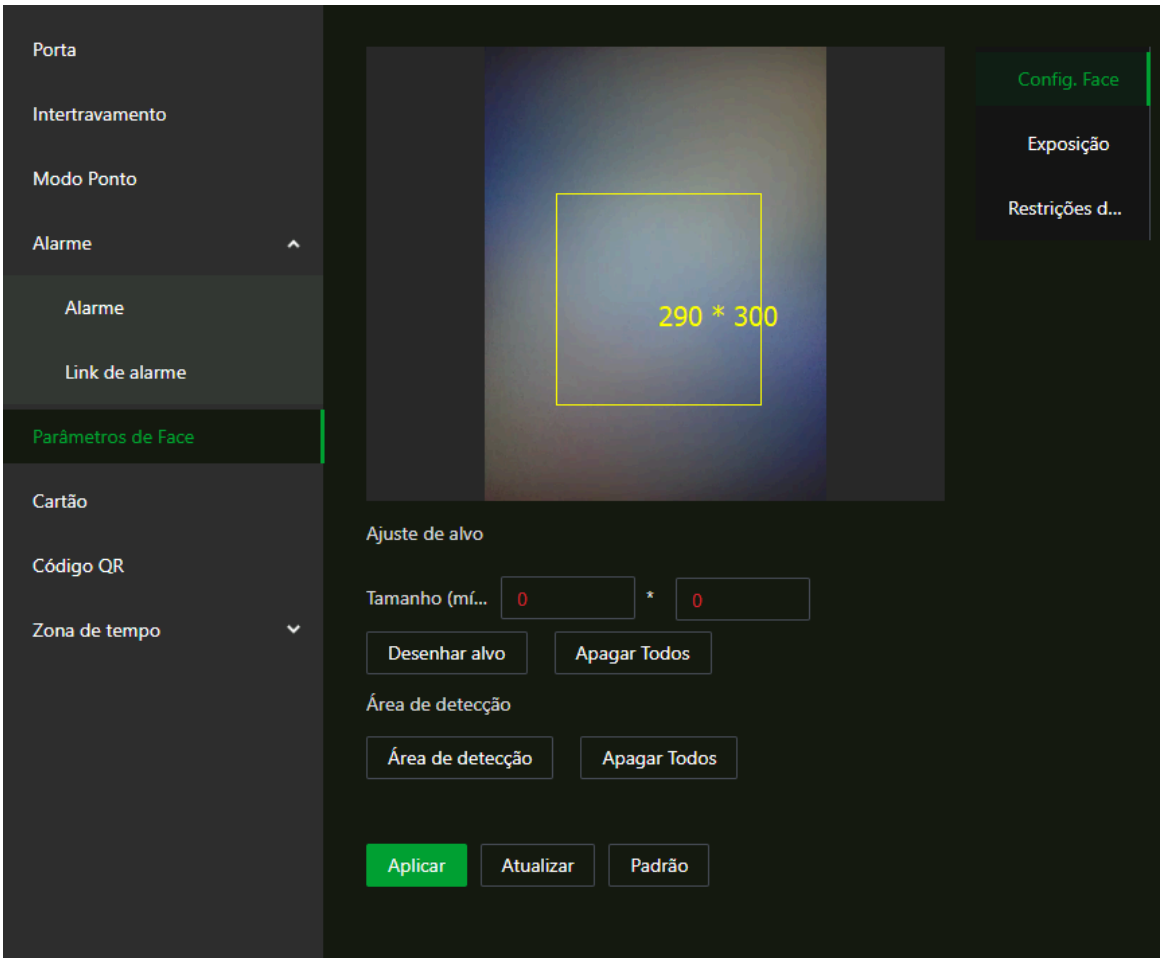
# Parâmetros de Face

Esse menu permite configurar os parâmetros de detecção facial.

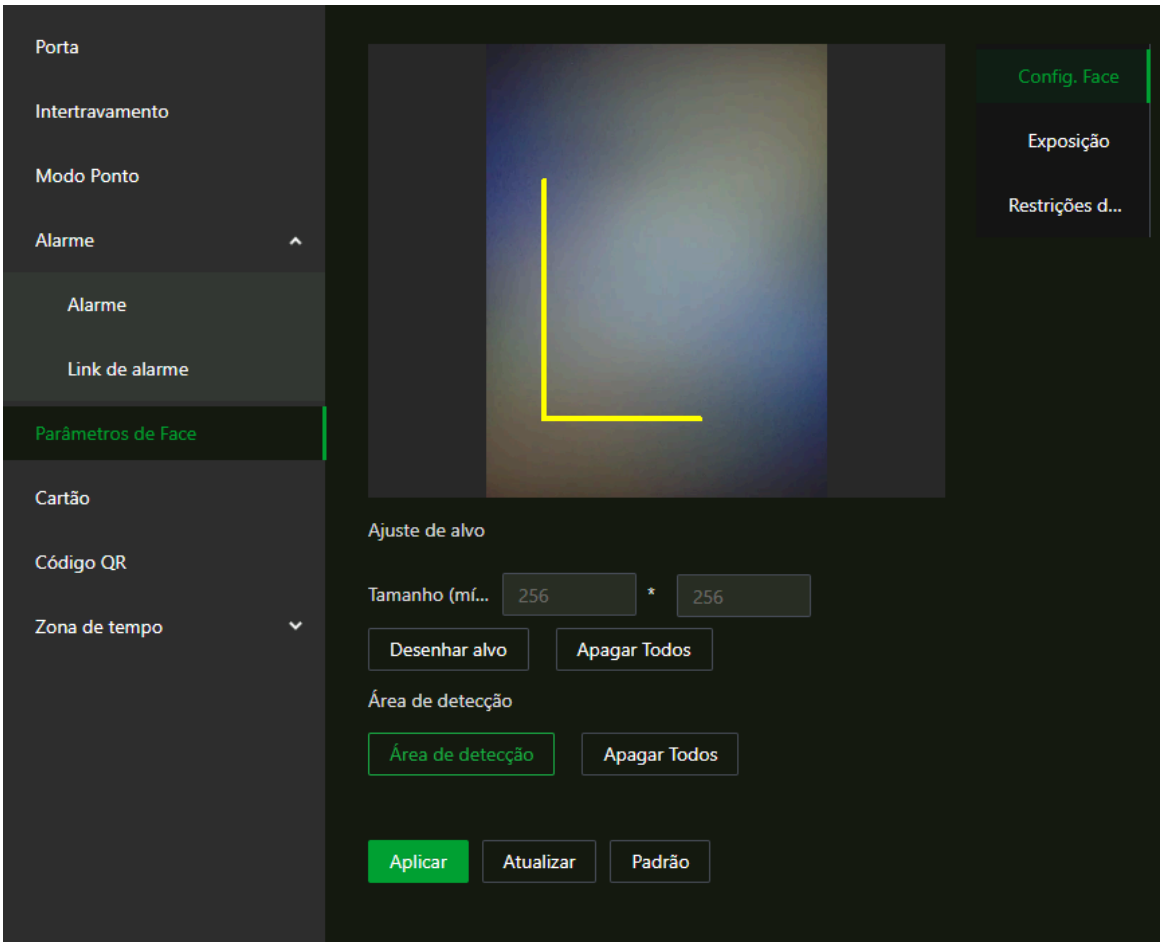


- **Ajuste de alvo:**
- **Desenhar alvo:** Clique em "Desenhar alvo" e, em seguida, você pode desenhar uma área mínima que o rosto precisa ocupar. Enquanto a edição está ativa, também é possível definir os valores digitando.
- **Apagar todos:** Clicando em "Apagar todos", ao lado direito de "Desenhar alvo", remove-se o quadro já desenhado.

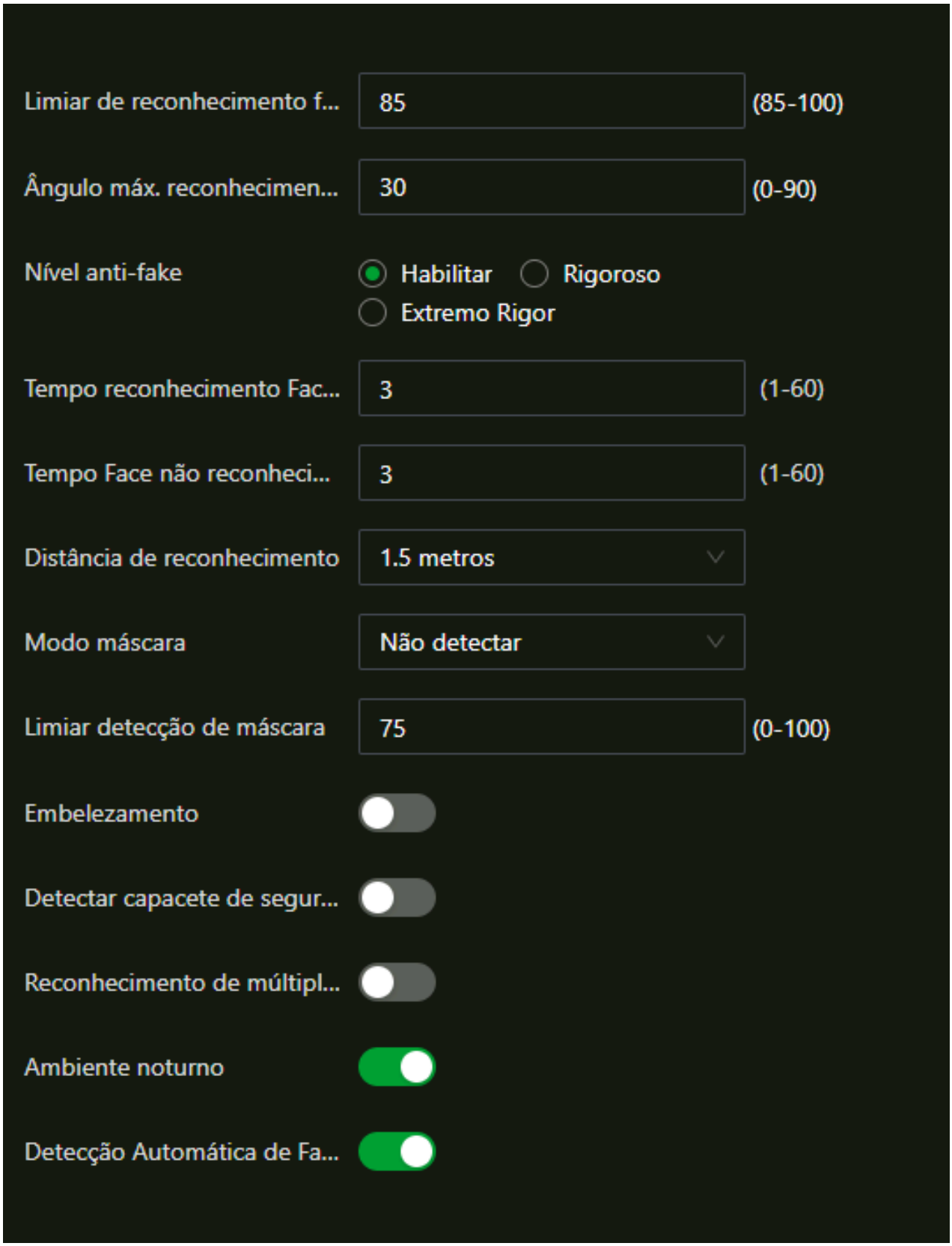
  OBS.: Quanto maior o quadrado mais próximo do dispositivo o usuário terá de estar.




- **Área de detecção:**
- **Área de detecção:** Clique em "Detectar região" e, com o botão esquerdo do mouse, clique nos pontos da imagem de vídeo que serão os vértices de uma forma geométrica de até 20 vértices. Para finalizar a definição da região, clique com o botão direito do mouse.
- **Apagar todos:** Clicando em "Apagar todos", ao lado direito de "Área de detecção", remove-se a região já desenhada.


Porta
Intertravamento
Modo Ponto
Alarme
Alarme
Link de alarme
Parâmetros de Face
Cartão
Código QR
Zona de tempo
Config. Face
Exposição
Restrições d...
Ajuste de alvo
Tamanho (mí...
256
*
256
Desenhar alvo
Apagar Todos
Área de detecção
Área de detecção
Apagar Todos
Aplicar
Atualizar
Padrão

# Configuração de parâmetros




- **Limiar de reconhecimento facial:** Ajuste a precisão do reconhecimento facial. Quanto maior o valor, maior será a semelhança necessária entre a captura feita pelo dispositivo e a foto cadastrada. Isso significa que a tolerância a variações de aparência, como expressões faciais, barba, acessórios e envelhecimento, será menor. O valor padrão é 85.

- **Ângulo máximo reconhecimento facial:** Ajusta o ângulo do perfil aceito pelo dispositivo para iniciar o reconhecimento facial.

Valor padrão é 30°.

- **Nível anti-fake:** Previne o uso de fotos, imagens ou vídeos em meio impresso ou digital de ter acesso ao dispositivo.
  - **Habilitar**: Habilita a função antifalsificação em nível moderado, ou seja, para inibir **parcialmente** o uso de imagem ou fotografia em frente ao dispositivo que tente reproduzir uma face humana.
  - **Rigoroso**: Habilita a função antifalsificação em nível elevado, ou seja, inibi totalmente o uso de imagem, fotografia ou outra forma que tente reproduzir uma face humana cadastrada no dispositivo. Além disso, aumenta o nível de rigor na comparação entre a foto cadastrada e a face detecta (similaridade acima de 90%).
  - **Extremo Rigor**: Habilita a função antifalsificação em nível extremo de verificação, ou seja, além de inibir totalmente o uso de imagem, fotografia ou outra forma que tente reproduzir uma face humana cadastrada no dispositivo, irá considerar conceder acesso para faces cadastradas no dispositivo, com similaridade acima de 96%.

    ***Obs.:*** *O valor de similaridade verificada pela algoritmo de reconhecimento facial ao comparar a face cadastrada com a face reconhecida, não é o mesmo configurado no campo "Limiar de reconhecimento facial".*

- **Tempo reconhecimento facial(s):** Tempo limite entre a apresentação para o reconhecimento facial e a mensagem de acesso liberado.
- **Tempo face não reconhecida:** Tempo limite entre o momento que se apresenta a face que não tem acesso no dispositivo e a mensagem de acesso negado.
- **Distância de reconhecimento:** Representa a distância entre a face e a lente.
- **Modo máscara:**
  - **Não Detectar:** A máscara não é detectada durante o reconhecimento facial.
  - **Alertar:** A máscara é detectada durante o reconhecimento facial. Se a pessoa não estiver usando uma máscara, o sistema irá lembrá-la de usar, mas o acesso será permitido.
  - **Sem Autorização sem Máscara:** A máscara é detectada durante o reconhecimento facial. Se a pessoa não estiver usando uma máscara, o sistema irá lembrá-la de usá-la e o acesso será negado.
- **Limiar detecção de máscara.** Quanto maior o limite, mais preciso será o reconhecimento facial quando a pessoa estiver usando uma máscara, e a taxa de reconhecimento falso será menor.
- **Embelezamento:** Permite habilitar ou desabilitar filtros para melhora de imagem.
- **Detectar Capacete de segurança:** Detecta capacetes de segurança. A porta não será destrancada se a pessoa não estiver usando o capacete.
- **Reconhecimento de múltiplas faces:** Detecta de 4 a 6 imagens faciais ao mesmo tempo. O acesso por multi-usuários não pode ser utilizada com essa função, e a porta será destrancada assim que uma das pessoas for verificada com sucesso.
- **Ambiente noturno:** Em ambientes escuros, a tela de espera exibe uma imagem de fundo branca para melhorar o brilho durante a verificação facial.
- **Detecção Automática de Face:** Quando habilitado, permite que a tela seja ligada quando houver detecção de um rosto. Padrão de fábrica vem habilitado.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.

- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

## Exposição

- **Nr. Canal:** São duas opções: a primeira para a câmera de luz visível e a segunda para a câmera de luz infravermelha.
- **Ativar Exposição Facial:** Ao ativar essa opção, prepara o dispositivo para funcionar melhor em ambientes mais iluminados para que a face seja detectada de forma clara.
- **Brilho Alvo Face:** Define o brilho conforme o necessário
- **IIntervalo de exposição facial:** A face será exposta apenas uma vez dentro de um intervalo definido.

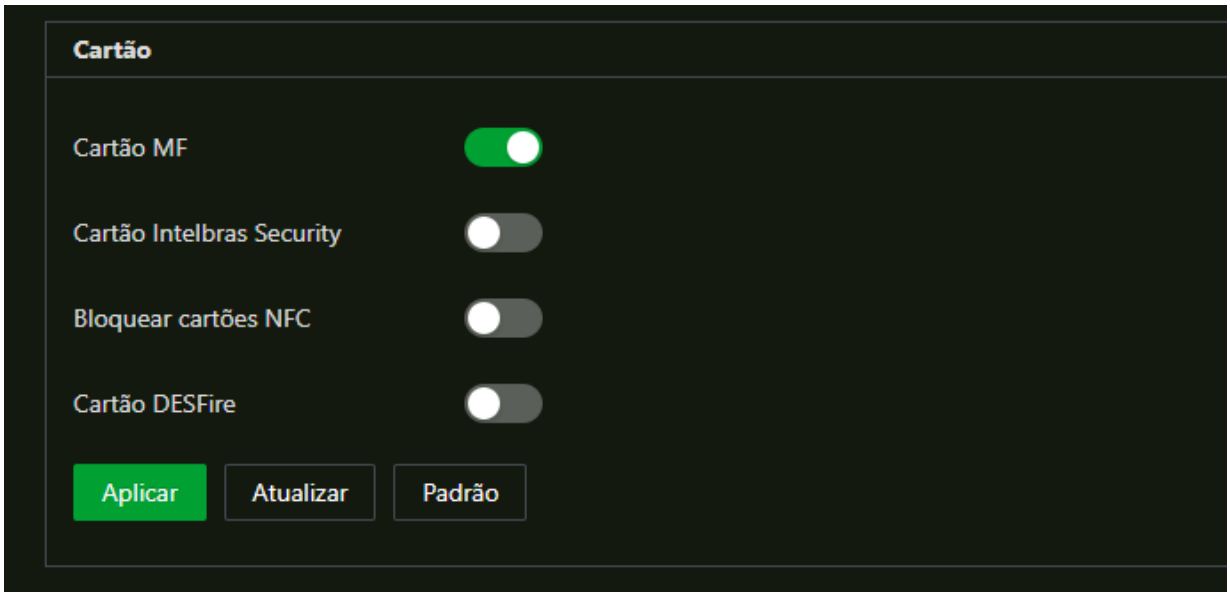
## Restrições da fotografia

- **Restrições da fotografia:** Executa um filtro para garantir a qualidade mínima da foto a ser cadastrada no sistema. Possui dois modos: Simples e Rigoroso.

- **Simples:**: Verifica os pontos principais para detecção e reconhecimento da face humana para cadastramento no sistema.
- **Rigoroso**: Verifica todos os pontos e qualidade da imagem para detecção e reconhecimento da face humana para cadastramento no sistema. Caso não esteja adequada, o sistema não aceitará a fotografia.

# Cartão

Esse menu permite realizar configurações dos parâmetros para leitor de cartão RFID.




- **Cartão MF:** Essa função pode habilitar ou desabilitar a leitura do RFID direto no dispositivo

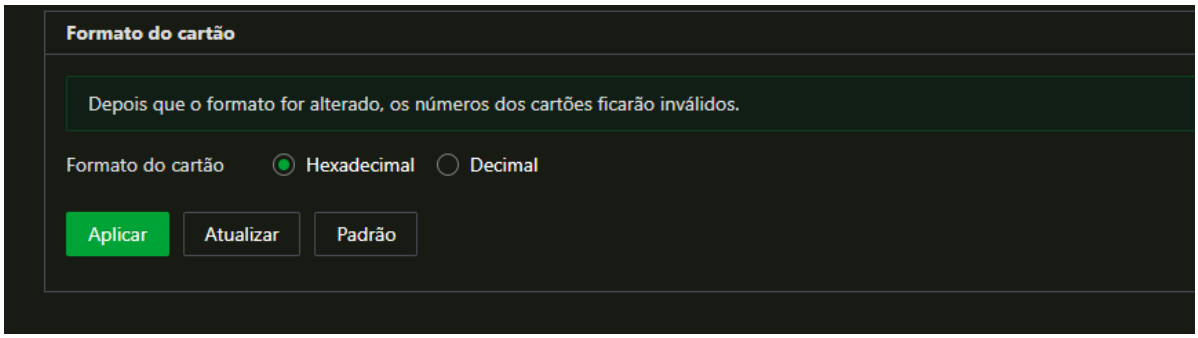
- **Cartão Intelbras Security:** Habilita ou desabilita o dispositivo a realizar apenas leitura com cartões criptografados com tecnologia Intelbras Security

**Obs.:** Para utilizar essa função é obrigatório o uso dos cartões e leitores com a tecnologia Intelbras Security

- **Bloquear cartões NFC:** Quando habilitada, evita o desbloqueio de portas com cartões NFC duplicados.
- **Cartão DESFire:**Quando habilitada, o dispositivo poderá ler o numero hexadecimal do cartão Desfire.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

## Formato do cartão

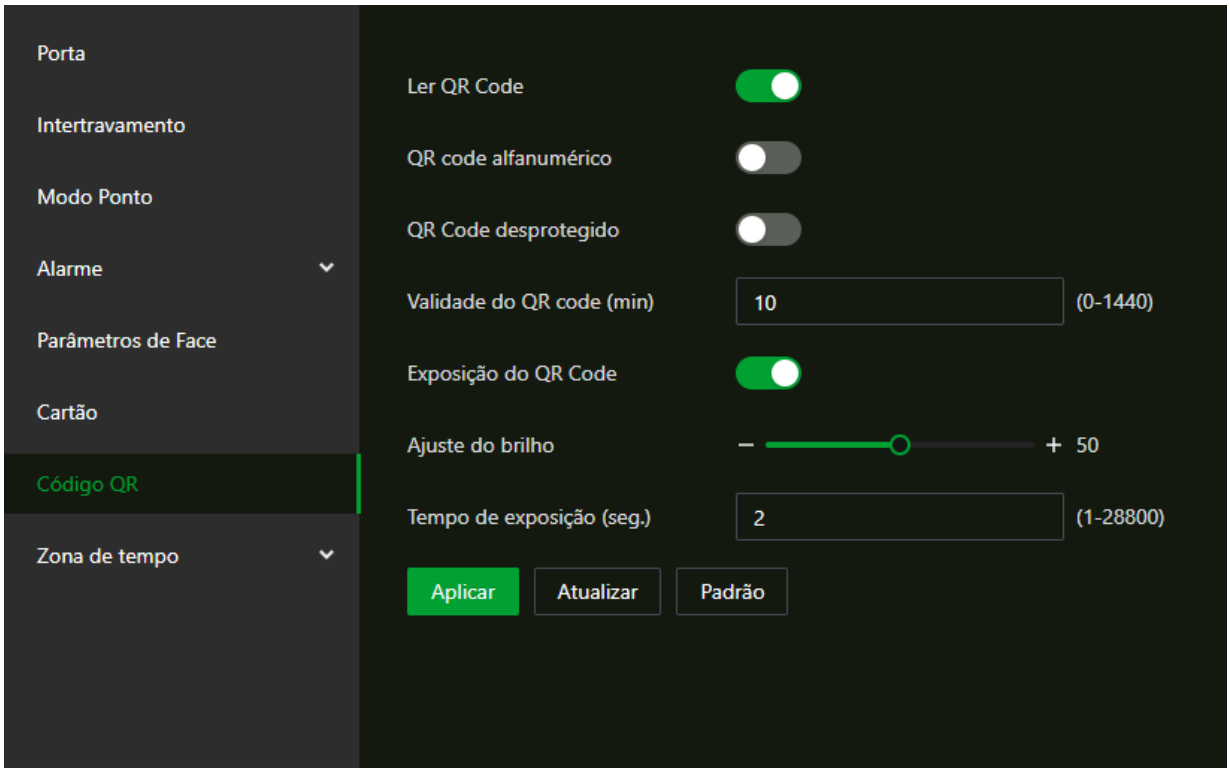
- **Formato do cartão:** Permite que o dispositivo realize a leitura do RFID no formato decimal ou hexadecimal para o número do cartão ao conectar um leitor de cartão Wiegand. O formato selecionado será aplicado tanto para entrada quanto para saída.




**Obs.:** Após selecionar uma das opções, o controlador de acesso realizará a leitura do cartão ou tag apenas no formato escolhido. Caso o formato seja alterado, o número será considerado inválido, resultando em acesso negado. Será necessário realizar um novo cadastro no formato selecionado.

## Código QR

Esse campo é relacionado as configurações para leitura do QR Code no através do controlador de acesso.




- **Ler QR Code:** Habilita ou desabilita o controlador de acesso realizar leituras de QR code.
- **QR code alfanumérico:** Quando habilitado, permite enviar strings alfanumérico no QR code.
- **QR Code desprotegido:** Quando habilitado, permite remover a criptografia do QR code, **por padrão essa função vem desabilitada.**

Para mais detalhes, consulte a documentação API, clicando aqui. (https://intelbras-caco-api.intelbras.com.br/configuracoes_de_credenciais_qrcode)

- **Validade do QR code (min):** Após o código QR ser gerado, sua validade durará por um período definido antes de expirar.
- **Exposição do QR Code:** Quando habilitado, o QR code será exibido com o brilho definido, permitindo sua detecção e leitura clara.
- **Ajuste do brilho:** Ajusta o brilho referente a leitura do QR code.
- **Tempo de exposição (s):** Define o tempo em código QR será exibido apenas uma vez dentro do intervalo definido.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

# Zona de Tempo

Nesse submenu, são configuradas as seções de horário e os planos de feriados para definir quando um usuário terá permissão para destrancar portas.

# Zona de tempo

É possível configurar até 128 períodos de tempo (de nº 0 a nº 127). Para cada período, é necessário definir os horários de acesso às portas para os dias da semana. Os usuários poderão destrancar a porta apenas durante os horários programados.

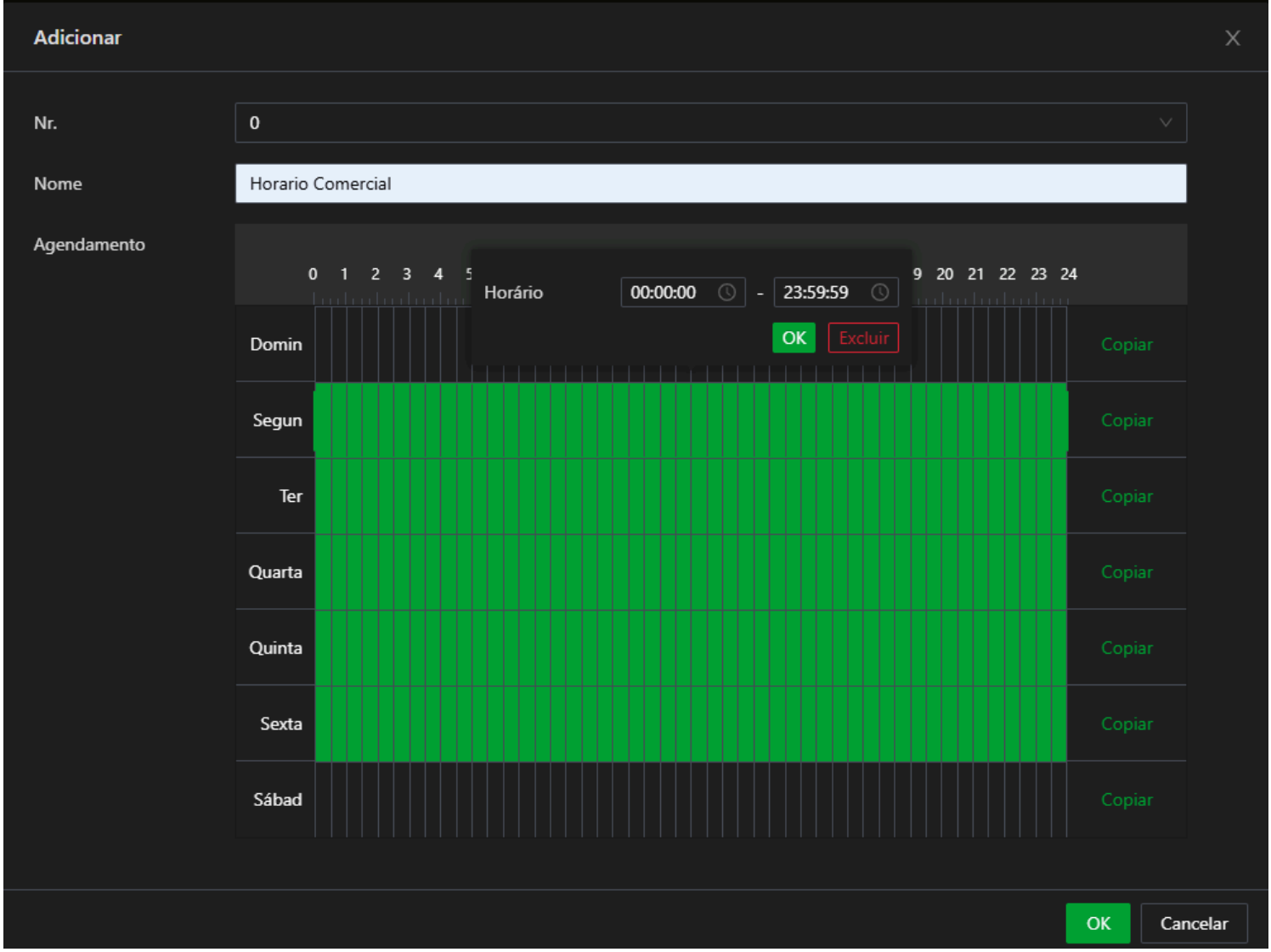
## Como Adicionar uma Nova Zona de Tempo

Clique no botão Adicionar ( 

), escolha um número para atribuir à nova zona de tempo criada e insira um nome de sua preferência.

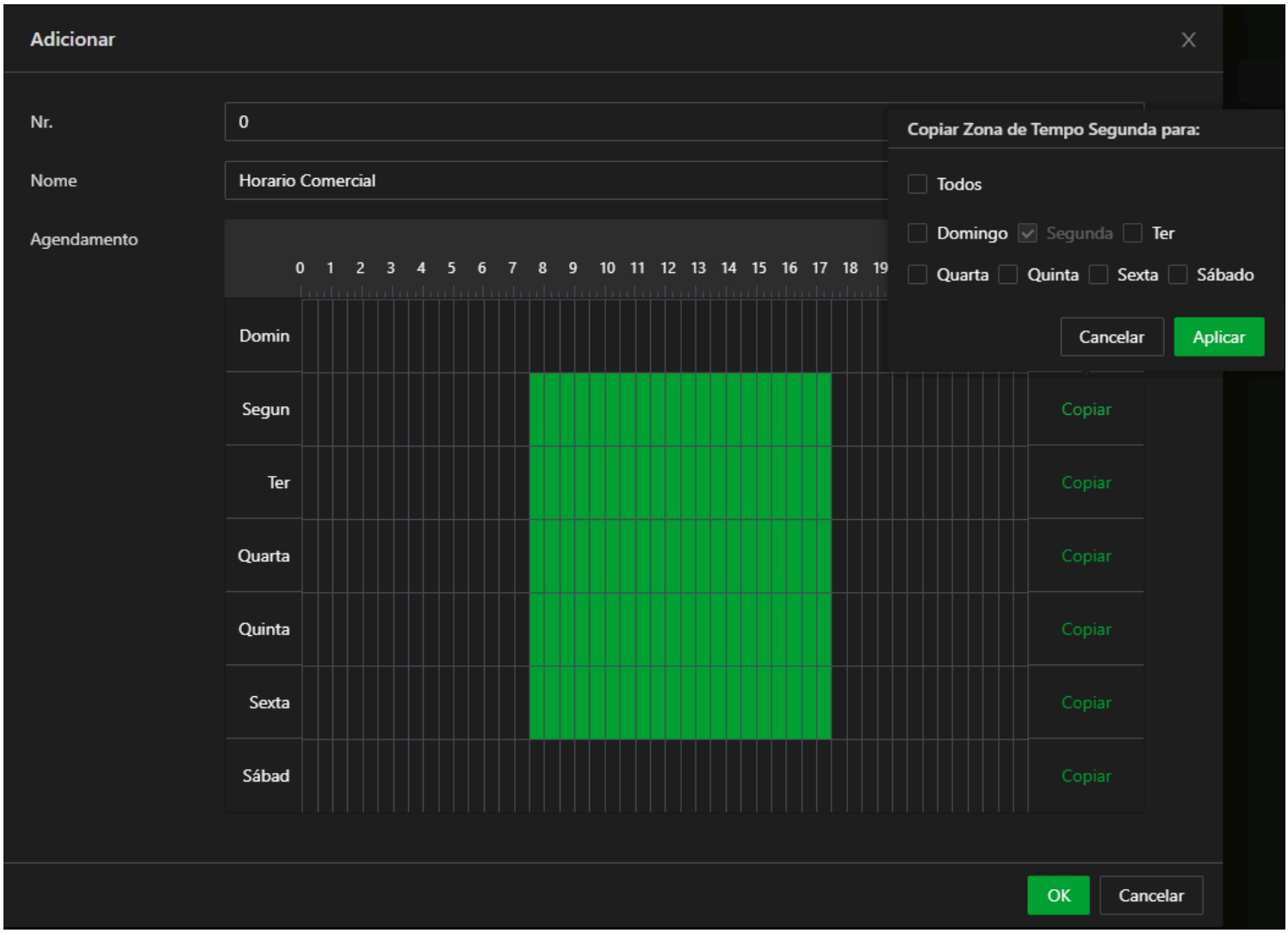
## Como Configurar Horários

Selecione o dia da semana desejado e insira os horários manualmente. Opcionalmente, arraste o controle deslizante com o mouse sobre a barra de tempo para definir o período de acesso.



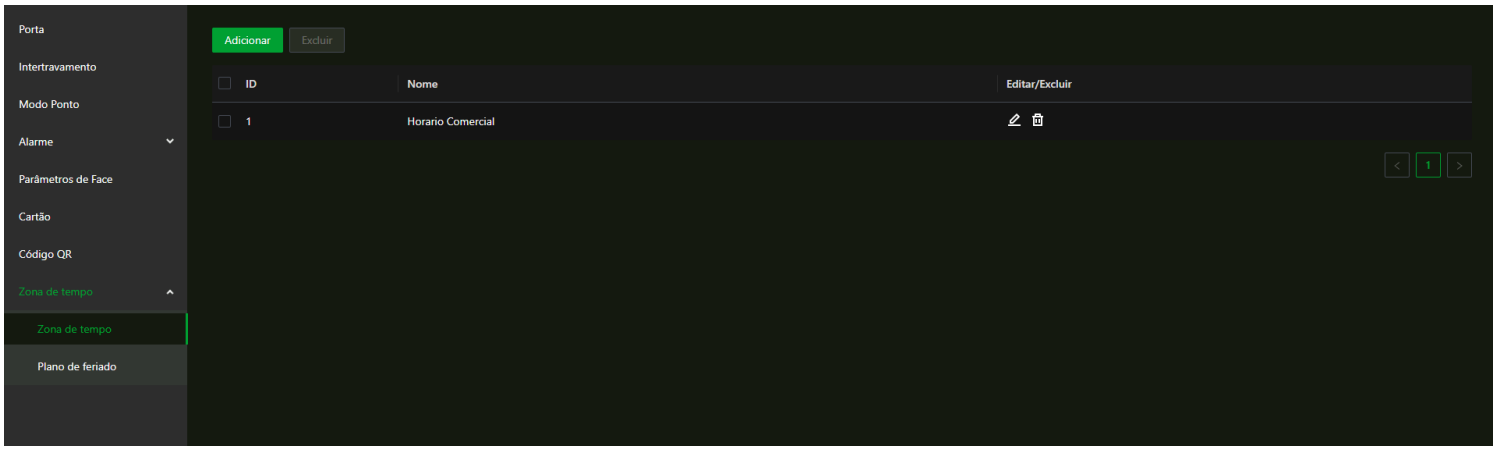

Além de definir os horários manualmente ou arrastando o controle deslizante, é possível, de forma opcional, copiar a configuração de um dia para os demais dias da semana. Clique no botão Copiar referente ao dia configurado e selecione os dias nos quais deseja replicar a configuração. Ao finalizar as operações de dia da semana e horário, clique no botão Aplicar para salvar as configurações realizadas.

- **Ok:** Salva as alterações feitas.
- **Cancelar:** Cancela as configurações realizadas.



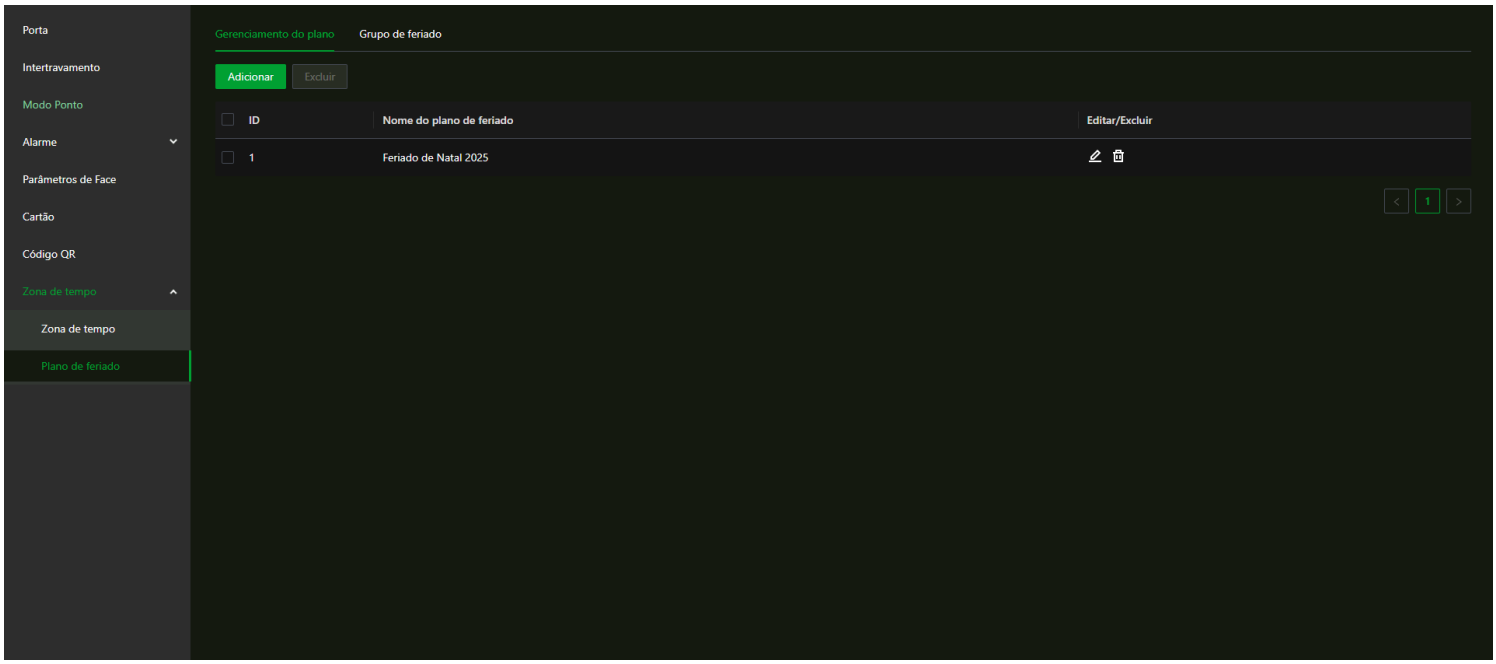

## Editando zona de tempo

Para editar as zonas de tempo ja criadas, clique no ícone ( ), para excluir a zona de tempo criada clique no ícone ( ).




# Plano de feriado

O plano de feriados permite configurar até 128 grupos de feriados (de nº 0 a nº 127). Para cada grupo, é possível adicionar até 16 feriados, garantindo uma gestão eficiente de acessos em datas específicas.



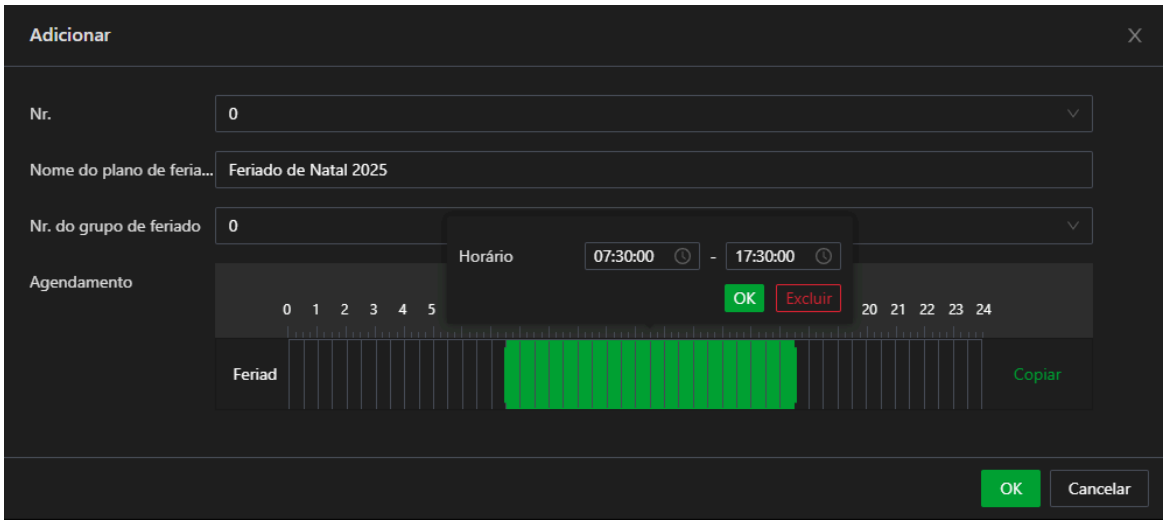

# Gerenciamento do plano

Nesse submenu é criado o plano de feriado definindo o nome, qual grupo será vinculado e o horario de operação para esse plano.

## Como Adicionar um plano de feriado

Clique no botão Adicionar ( 

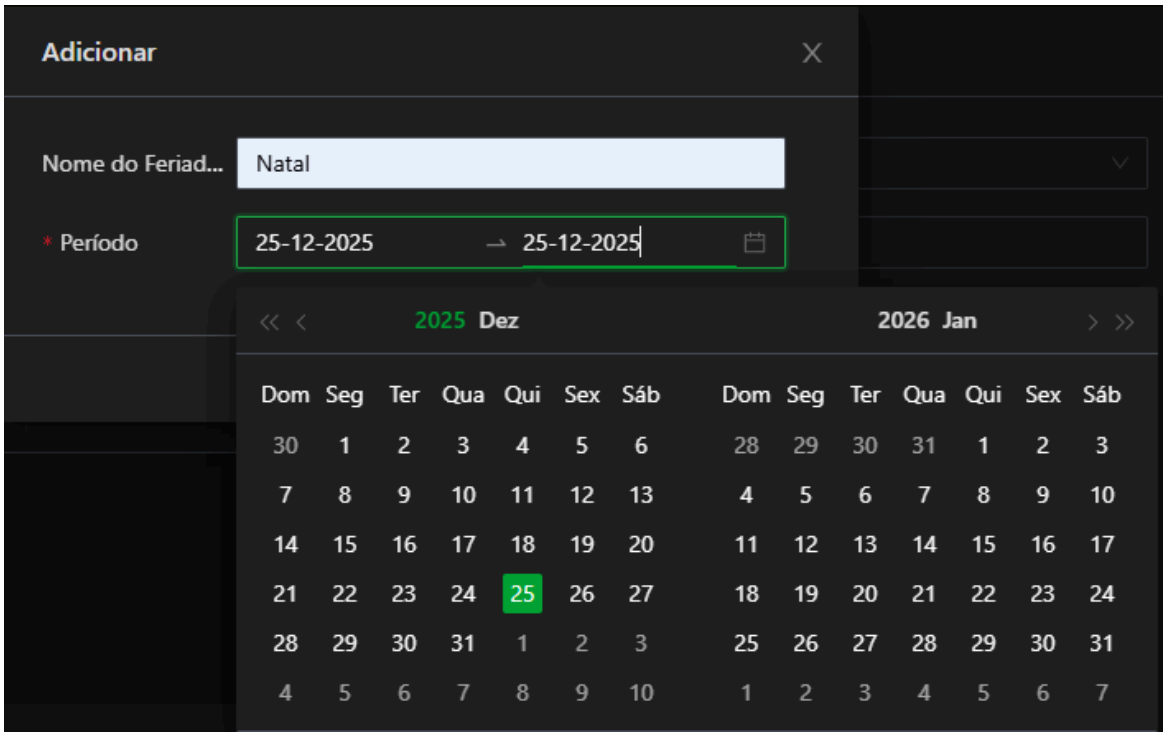
), escolha um número para atribuir o feriado criado e insira um nome de sua preferência. Selecione o número do grupo de feriado criado e configure o horário a ser definido, podendo ser manualmente ou arrastando o controle deslizante com mouse. Ao finalizar as operações de dia da semana e horário, clique no botão Aplicar para salvar as configurações realizadas.

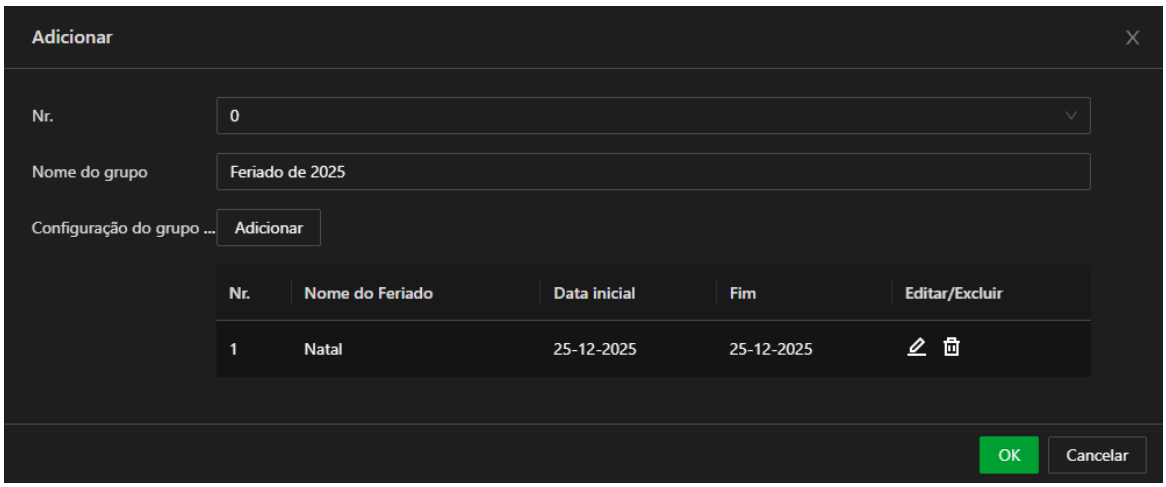



**Obs.:** Para realizar a configuração do gerenciamento de feriado, primeiramente deve ser criado o grupo de feriado.

# Grupo de feriado

Nesse submenu é criado o grupo de feriado definindo o nome e o período em que ele será utilizado.



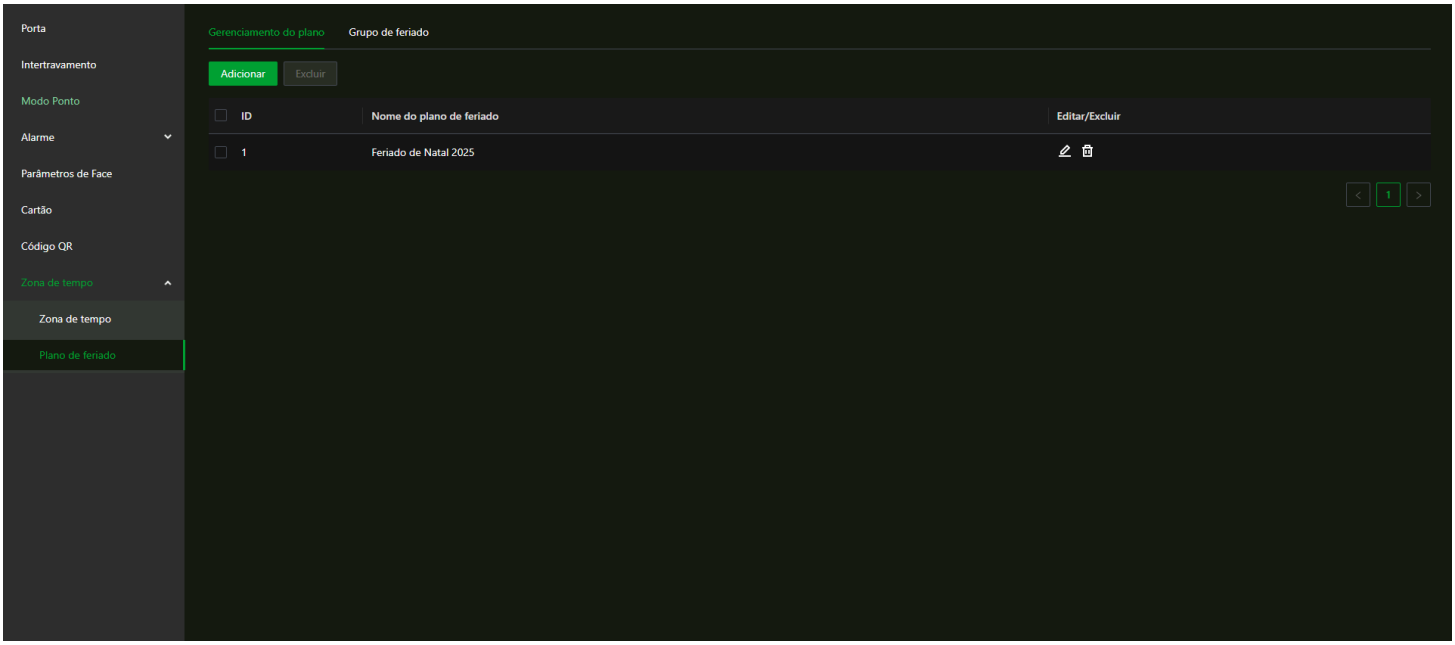




Ao finalizar as operações de dia da semana e horário, clique no botão Aplicar para salvar as configurações realizadas.

- **Ok:** Salva as alterações feitas.
- **Cancelar:** Cancela as configurações realizadas.

## Editando plano de feriado

Para editar os planos de feriado e os grupos de feriados ja criados, clique no ícone ( ), para excluir os grupos e plano de feriado clique no ícone ( ).




# INTERCOMUNICAÇÃO

Este menu permite que o usuário administrador configure uma conta SIP no controlador de acesso, seja com servidores SIP externos ou utilizando o próprio controlador de acesso como servidor. As principais funções incluem a gestão de ramais para criação e gerenciamento de listas, envio de mensagens e comunicação eficiente com terminais de vídeo.

## Observações

- A função SIP do dispositivo se destina a sistemas de portaria remota e relacionados.
- Suporta uma conta SIP com os codecs G.711a, G.711u e H.264.
- Suporta acionamento de porta via DTMF.
- Protocolo SIP-INFO. O tempo de atraso entre o envio do comando e a execução pode variar de 2 a 5 segundos.
- Protocolo RFC 2833. Para acionamento da fechadura nesse protocolo é necessário discar # antes e depois do comando DTMF.
  Ex: Senha DTMF 123, para realizar abertura digitar #123#
- Suporta chamada por botão físico via ALM-IN. Nesse caso a função inicial de entrada de alarme é perdida.
- Verifique se a função Reinvite e ALG está desabilitada na central para cada ramal.
- O horário do controlador de acesso facial será automaticamente sincronizado com o horário do servidor SIP após o registro. No entanto, se o horário do servidor SIP estiver incorreto, essa imprecisão será refletida no horário do controlador. Para evitar essa situação e manter o horário do controlador de acesso facial sempre correto, recomendamos a ativação do serviço NTP (Network Time Protocol), que sincroniza o horário com servidores de tempo precisos na internet.

## Servidores SIP compatíveis

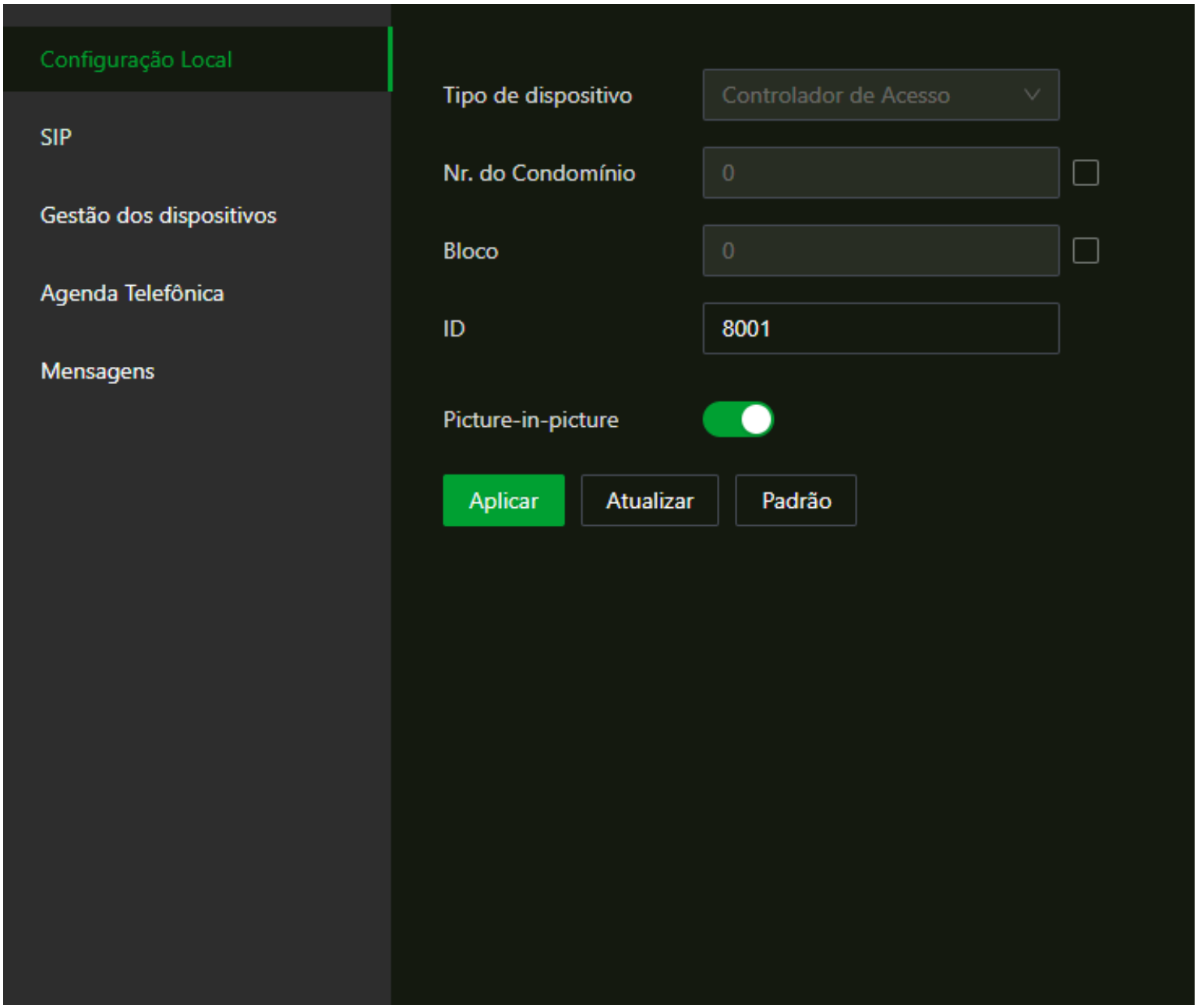
- WideVoice Intelbras
- CIP 92200
- CIP 850
- Unniti
- Asterisk
- IAD 100

### Terminais compatíveis

- TVIP 3000 WIFI (Somente para uso com a função SIP servidor de terceiros)
- TVIP 2210, TVIP 2220 e TVIP 2221 (Uso exclusivo na função SIP com o tipo de servidor dispositivo)
- Intelbras MobiliTI PRO (Softphone)*

*Consultar Servidores compatíveis

# Configuração local




- **Tipo de dispositivo:** Por padrão já vem o dispositivo como controlador de acesso.

- **Nr. do Condomínio:** Implementação futura
- **Bloco:** Implementação futura
- **ID:** Número de ramal definido para a conta SIP do facial.

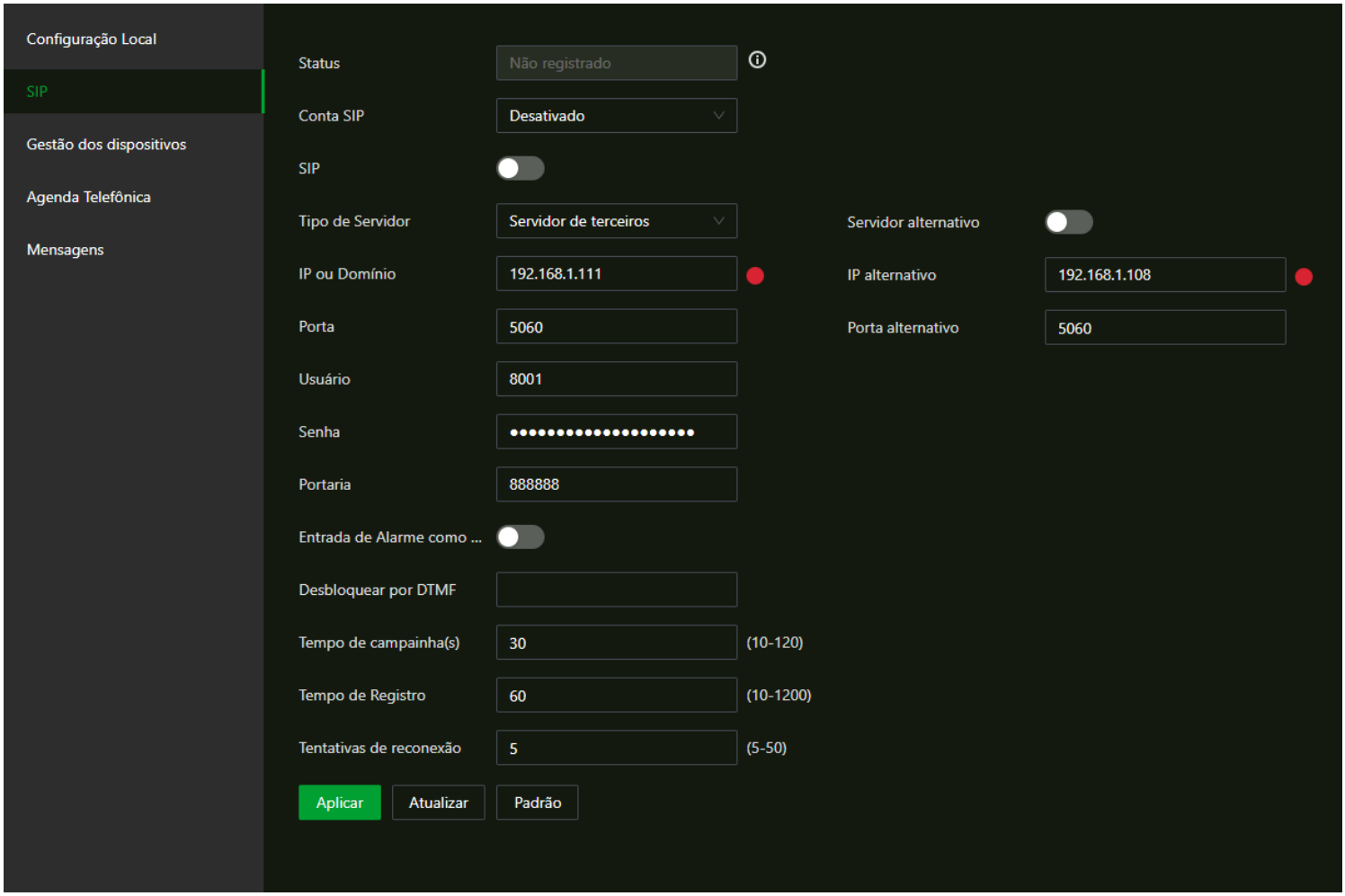
**Obs.:** O número deve ter 4 dígitos, os dois primeiros dígitos devem ser 80, e os dois últimos devem começar a partir de 01 (por exemplo, 8001). Os número não podem se repetir se usado mais de um facial no mesmo ambiente.

- **Picture-in-picture:** Quando habilitado, permite exibir na tela do facial o vídeo do número discado, como a visualização do agente de portaria remota que atendeu a ligação. Para o funcionamento correto, é necessário que o ramal atendedor possua uma câmera para transmitir a imagem.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:**Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

# Configurações SIP Servidor de terceiros

Para mais informações sobre os servidores SIP homologados, consulte o item INTERCOMUNICAÇÃO.

## Facial conectado ao servidor SIP



- **Status:** Este campo exibe o status da conexão com o servidor, indicando se o registro foi efetuado com sucesso. O ícone  oferece informações adicionais, como mensagens de erro. Por exemplo: "Acesso Negado" ou "Erro 403: Servidor SIP negou a conexão," que pode indicar um ramal já em uso ou a senha SIP digitada incorretamente.
- **Conta SIP:** Esta opção permite ativar ou desativar a função SIP do dispositivo, fazendo com que ele opere de acordo com os parâmetros definidos nos campos "SIP" ou "Tipo de Servidor".

  Quando habilitado será possível escolher até três formas para discagem na tela do controlador de acesso;

- **Multi-teclas:** Essa opção permite, ao utilizar a tela de discagem, abrir um teclado numérico para que seja possível realizar a discagem do número desejado.
- **Portaria:** Essa opção permite, ao utilizar a tela de discagem, realizar uma discagem direta para o ramal de portaria configurado no campo "Portaria".
- **Personalizado:** Essa opção permite, ao utilizar a tela de discagem, realizar uma discagem direta para um ramal específico configurado no campo "Ramal".

- **Servidor de terceiros:** Quando habilitada, a conexão é estabelecida como um ramal de um servidor SIP de terceiros.
- **IP ou Domínio:** Endereço IP do servidor SIP. Ao lado o indicador ficará vermelho quando não houver conexão com servidor e verde quando a conexão for estabelecida.
- **Porta:** Porta do servidor SIP.
- **Servidor alternativo:** Quando habilitada, essa opção permite que o dispositivo facial em modo SIP reconecte-se automaticamente a um servidor secundário caso o servidor principal perca a conexão.
- **IP alternativo:** Endereço IP do servidor SIP secundário. Ao lado o indicador ficará vermelho quando não houver conexão com servidor e verde quando a conexão for estabelecida.
- **Porta alternativa:** Porta do servidor SIP secundário.

**Obs.: Para o funcionamento correto da função de servidor alternativo, é indispensável que o plano de numeração e a senha SIP sejam idênticos aos do servidor principal.**

- **Usuário:** Usuário SIP do dispositivo ou numero de registro.

**Obs.: No campo usuário utilizar apenas caracteres alfanuméricos.**

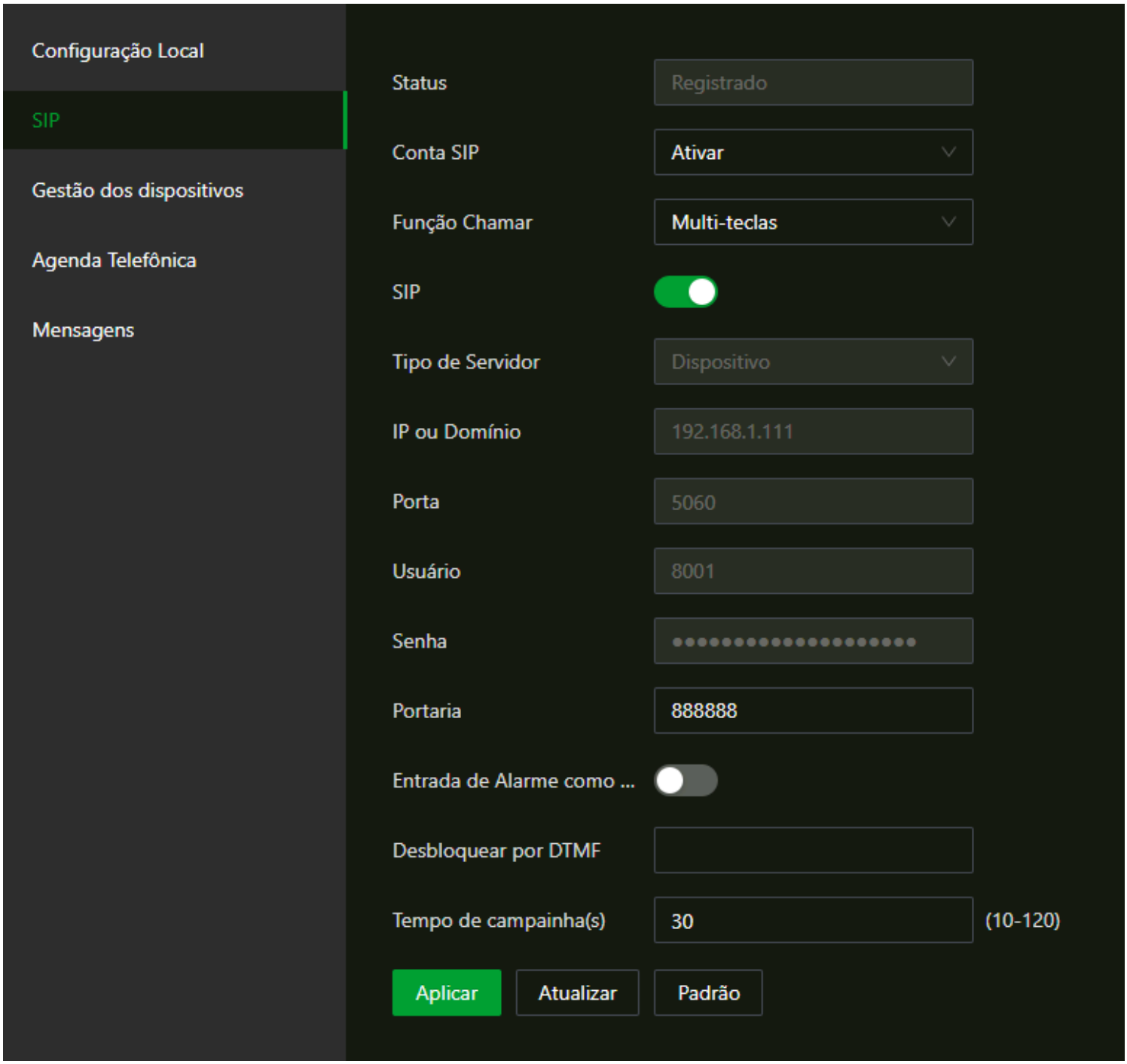
- **Senha:** Senha do usuário do servidor SIP.
- **Portaria:** Número cadastrado para chamada via tecla “Portaria”, via chamada direta ou via função Entrada de Alarme como botão;
- **Entrada de alarme como botão:** Essa função possibilita o uso da entrada de alarme (ALM1_IN) e (GND) para iniciar uma chamada direta para o “Número de Portaria”, previamente cadastrado.
- **Desbloquear por DTMF:** Essa função permite cadastrar uma sequência de até nove dígitos para desbloquear via **DTMF**
- **Tempo de campainha(s):** Essa função permite o ajuste (10 - 120) do tempo o qual o dispositivo aguardará em chamada. Caso o tempo configurado expire e o dispositivo não seja atendido, a chamada será encerrada automaticamente.
- **Tempo de registro:** Este é o intervalo de tempo em que o dispositivo facial envia uma mensagem ao servidor SIP para confirmar sua disponibilidade e conexão.

- **Tentativas de reconexão:** É a tentativa de restabelecer a conexão entre os dispositivos e o servidores, garantindo que a comunicação seja retomada quando houver falhas na conexão.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:**Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

# Configurações SIP Dispositivo

Para mais informações sobre os servidores SIP homologados, consulte o item INTERCOMUNICAÇÃO.

## Facial como servidor SIP



- **Status:** Este campo exibe o status da conexão com o servidor, indicando se o registro foi efetuado com sucesso. O ícone oferece informações adicionais, como mensagens de erro. Por exemplo: "Acesso Negado" ou "Erro 403: Servidor SIP negou a conexão," que pode indicar um ramal já em uso ou a senha SIP digitada incorretamente.
- **Conta SIP:** Esta opção permite ativar ou desativar a função SIP do dispositivo, fazendo com que ele opere de acordo com os parâmetros definidos nos campos "Configuração" ou "Tipo de Servidor".

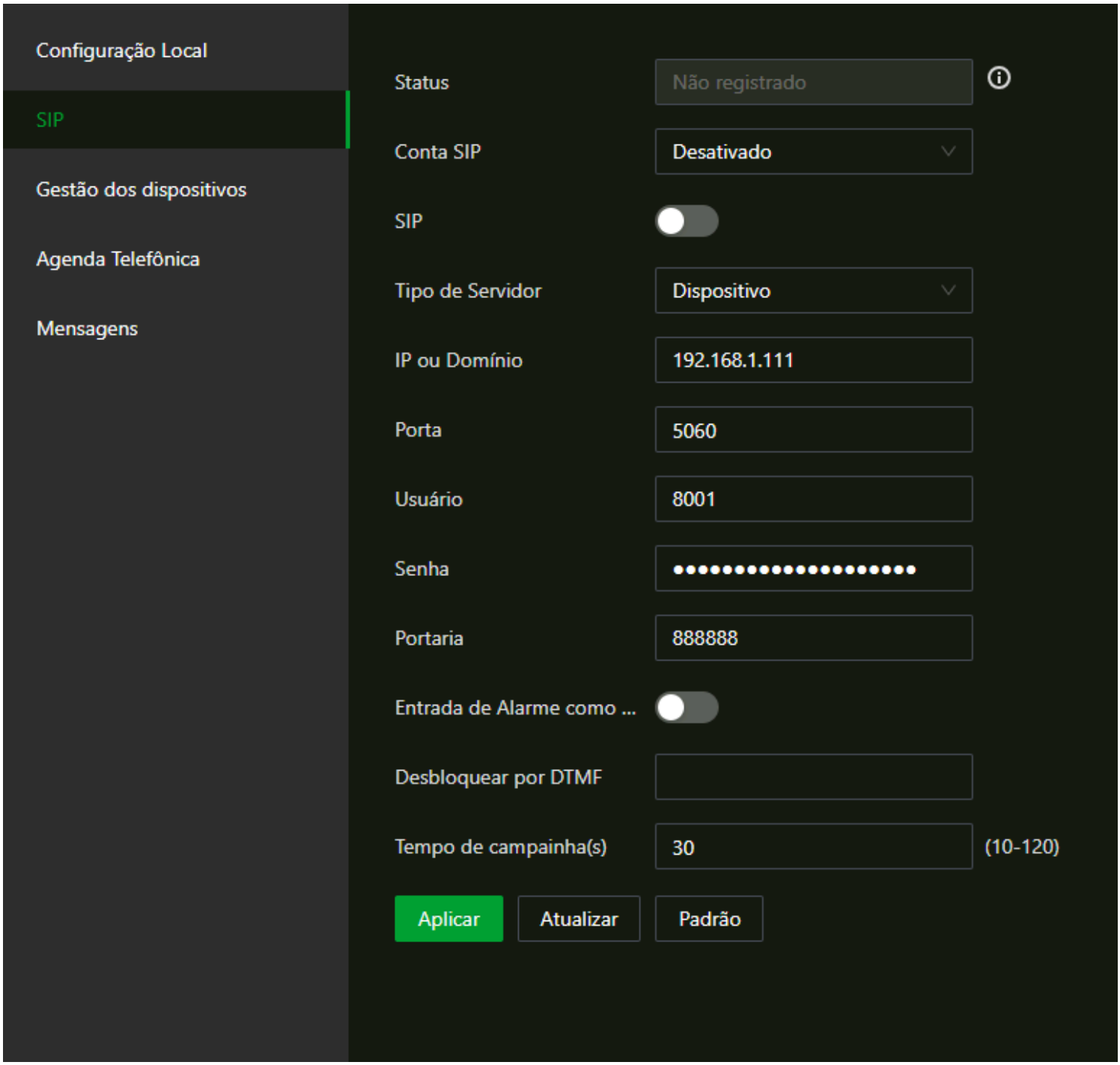
Quando habilitado será possível escolher até três formas para discagem na tela do controlador de acesso;

- **Multi-teclas:** Essa opção permite, ao utilizar a tela de discagem, abrir um teclado numérico para que seja possível realizar a discagem do número desejado.
- **Portaria:** Essa opção permite, ao utilizar a tela de discagem, realizar uma discagem direta para o ramal de portaria configurado no campo "Portaria".
- **Personalizado:** Essa opção permite, ao utilizar a tela de discagem, realizar uma discagem direta para um ramal específico configurado no campo "Ramal".

**Importante: a conta de ramal do facial servidor habilitada receberá por padrão o número 8001, que não pode ser alterado. O mesmo acontece com a porta SIP, que independente da configuração a porta passa a ser 5060.**

- **SIP:** Quando a opção de configuração for habilitada, o controlador de acesso facial atuará como um servidor SIP (dispositivo principal), gerenciando todas as comunicações entre o dispositivo facial e as telas dos modelos TVIP 2210, TVIP 2220 e TVIP 2221.
- **Portaria:** Número cadastrado para chamada via tecla “Portaria”, via chamada direta ou via função Entrada de Alarme como botão;
- **Entrada de alarme como botão:** Essa função possibilita o uso da entrada de alarme (ALM1_IN) e (GND) para iniciar uma chamada direta para o “Número de Portaria”, previamente cadastrado.
- **Desbloquear por DTMF:** Essa função permite cadastrar uma sequência de até nove dígitos para desbloquear via **DTMF**
- **Tempo de campainha(s):** Essa função permite o ajuste (10 - 120) do tempo o qual o dispositivo aguardará em chamada. Caso o tempo configurado expire e o dispositivo não seja atendido, a chamada será encerrada automaticamente.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:**Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

# Facial como cliente ao servidor SIP




- **Status:** Este campo exibe o status da conexão com o servidor, indicando se o registro foi efetuado com sucesso. O ícone oferece informações adicionais, como mensagens de erro. Por exemplo: "Acesso Negado" ou "Erro 403: Servidor SIP negou a conexão," que pode indicar um ramal já em uso ou a senha SIP digitada incorretamente.
- **Conta SIP:** Esta opção permite ativar ou desativar a função SIP do dispositivo, fazendo com que ele opere de acordo com os parâmetros definidos nos campos "Configuração" ou "Tipo de Servidor".

  Quando habilitado será possível escolher até três formas para discagem na tela do controlador de acesso;

- **Multi-teclas:** Essa opção permite, ao utilizar a tela de discagem, abrir um teclado numérico para que seja possível realizar a discagem do número desejado.
- **Portaria:** Essa opção permite, ao utilizar a tela de discagem, realizar uma discagem direta para o ramal de portaria configurado no campo "Portaria".

- **Personalizado:** Essa opção permite, ao utilizar a tela de discagem, realizar uma discagem direta para um ramal específico configurado no campo "Ramal".
- **Endereço IP:** Endereço IP do servidor SIP ou facial em modo servidor SIP principal.
- **Portas:** Porta do servidor SIP (Quando utilizado como função servidor SIP principal, utilizar porta 5060).
- **Usuário:** Usuário SIP do dispositivo ou numero de registro do facial.

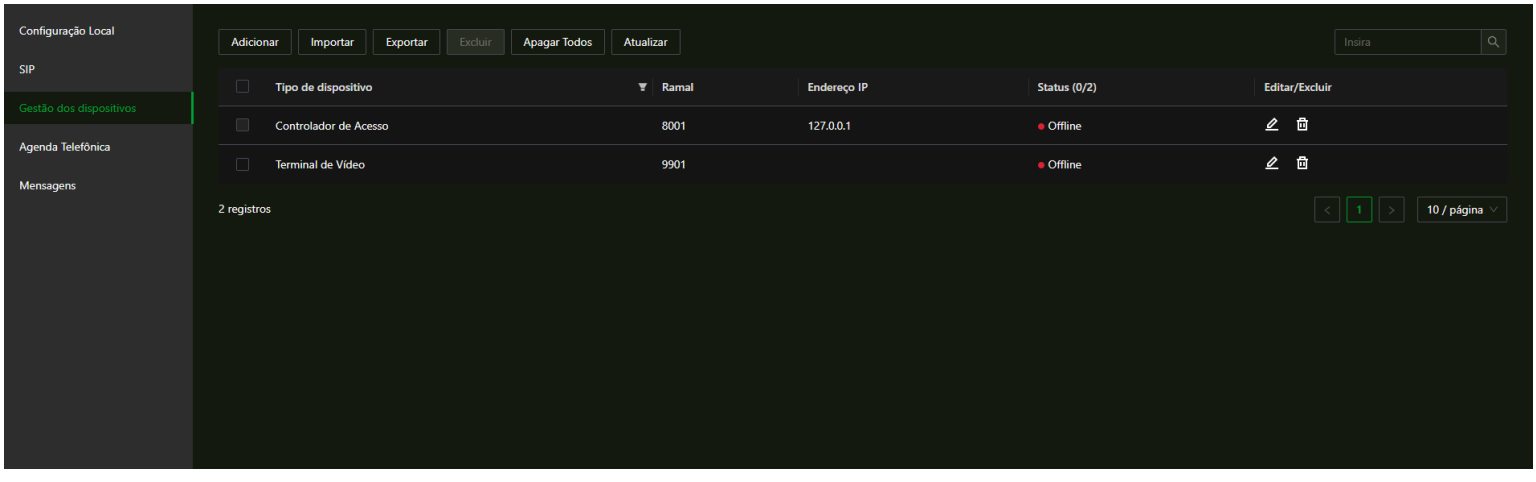
**Obs.: No campo usuário utilizar apenas caracteres alfanuméricos.**

- **Senha:** Senha do usuário do servidor SIP ou do facial modo servidor SIP principal. (padrão de fabrica: 123456).
- **Portaria:** Número cadastrado para chamada via tecla “Portaria”, via chamada direta ou via função Entrada de Alarme como botão;
- **Entrada de alarme como botão:** Essa função possibilita o uso da entrada de alarme (ALM1_IN) e (GND) para iniciar uma chamada direta para o “Número de Portaria”, previamente cadastrado.
- **Desbloquear por DTMF:** Essa função permite cadastrar uma sequência de até nove dígitos para desbloquear via **DTMF**
- **Tempo de campainha(s):** Essa função permite o ajuste (10 - 120) do tempo o qual o dispositivo aguardará em chamada. Caso o tempo configurado expire e o dispositivo não seja atendido, a chamada será encerrada automaticamente.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:**Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

# Gestão dos dispositivos

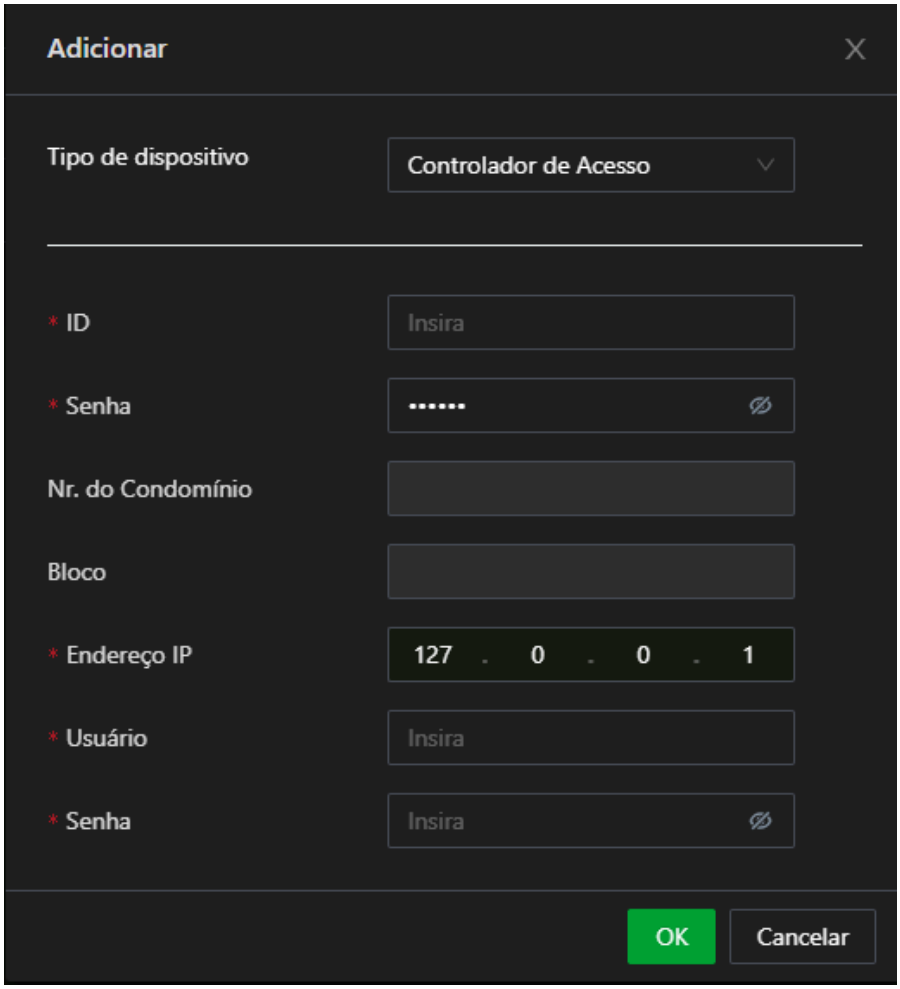
Essa função permite cadastrar os controladores de acesso facial como clientes de um dispositivo facial que atuará como servidor SIP principal. Também é possível cadastrar as telas dos modelos TVIP 2210, TVIP 2220 e TVIP 2221 para receber chamadas. Recomenda-se configurar até 8 dispositivos faciais, podendo combinar livremente os modelos SS 35x1, SS 35x2, SS 55x1, SS 55x2 e PVIP 2216 em um mesmo cenário. Para o correto funcionamento, é necessário configurar os demais dispositivos no modo de operação facial como clientes do servidor SIP.

Para editar as configurações dos controladores de acesso e as telas utilize o ícone  . Para excluir um controlador de acesso ou telas utilize o ícone 



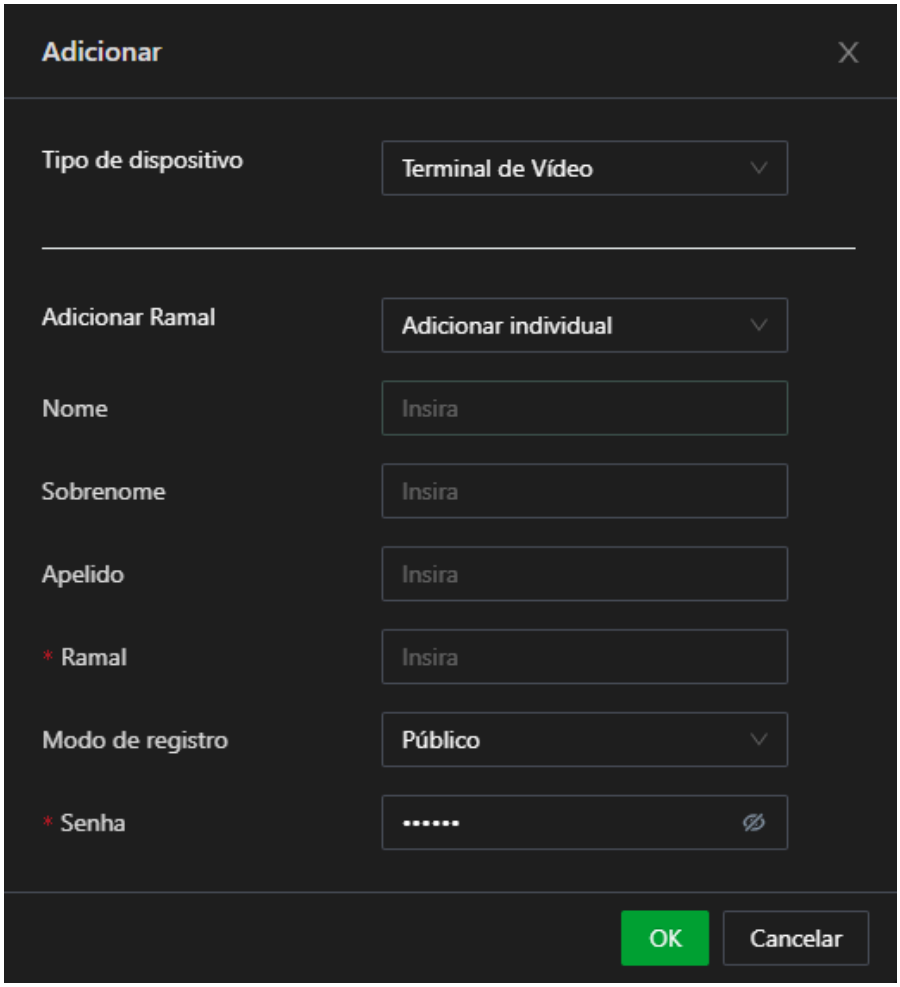
**Obs.: A função facial como servidor SIP não contempla o uso do aplicativo SVIP Intelbras e SVIP Admin, esses aplicativos é de uso exclusivo do sistema SVIP 2000.**

# Adicionando controlador facial como cliente SIP




- **Tipo de dispositivo:** Para usar o controlador de acesso facial como cliente, mantenha a opção marcada **controlador de acesso.**
- **ID:** Número do ramal configurado para o controlador de acesso. Para mais detalhe clique para ver as configurações do dispositivo
- **Senha:** Senha SIP do facial como servidor SIP principal. (padrão de fabrica: 123456).
- **Nr. do Condomínio:** Implementação futura.
- **Bloco:** Implementação futura.
- **Endereço IP:** Endereço IP do controlador facial configurado como servidor SIP
- **Senha:** Senha admin de acesso do controlador facial configurado como servidor SIP. Mesma senha criada na inicialização do produto.
- **Ok:** Salva as alterações feitas.
- **Cancelar:** Cancela as configurações realizadas.

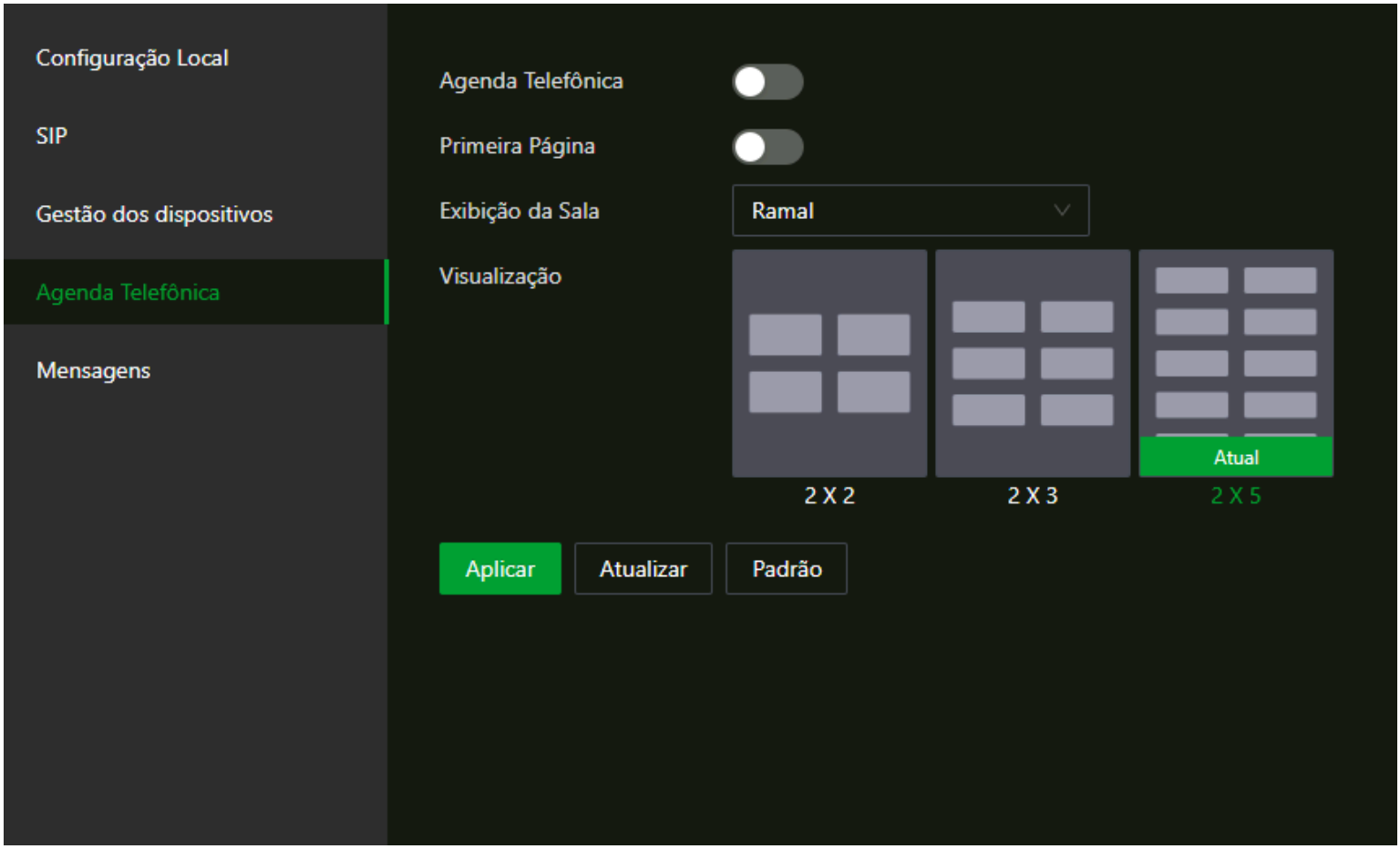
# Adicionando Telas de vídeo




- **Tipo de dispositivo:** Para usar o tela de vídeo escolha opção **terminal de video.**
- **Adicionar Ramal:** Permite adicionar terminais de vídeo individualmente ou por lote.
- **Nome:** Nome do morador do apartamento.
- **Sobrenome:** Sobrenome do morador do apartamento.
- **Apelido:** Apelido do morador do apartamento.
- **Ramal:** Ramal a ser configurado no terminal de vídeo.
- **Modo de registro:** Manter como padrão opção Público.
- **Senha:** Senha SIP do facial como servidor SIP principal. (padrão de fabrica: 123456).
- **Ok:** Salva as alterações feitas.
- **Cancelar:** Cancela as configurações realizadas.

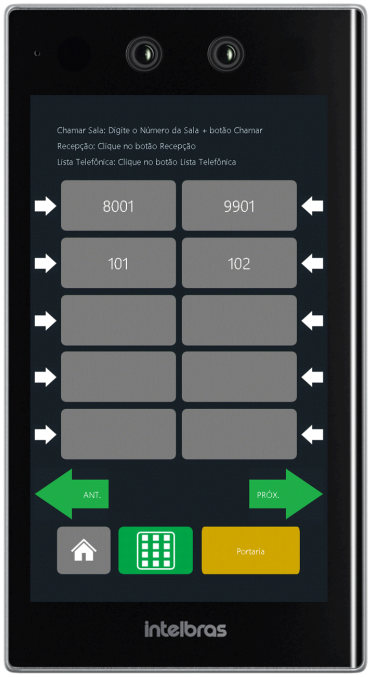
# Agenda Telefônica

Quando habilitada, essa função permite exibir os apartamentos na tela de discagem, mostrando o número, nome ou apelido configurado ao adicionar telas de video.




- **Primeira Página:** Quando habilitada, adiciona uma opção na tela de discagem para abrir a lista telefônica.

- **Primeira página:** Quando habilitada, ao pressionar o botão de discagem, os ramais configurados serão exibidos na primeira tela.

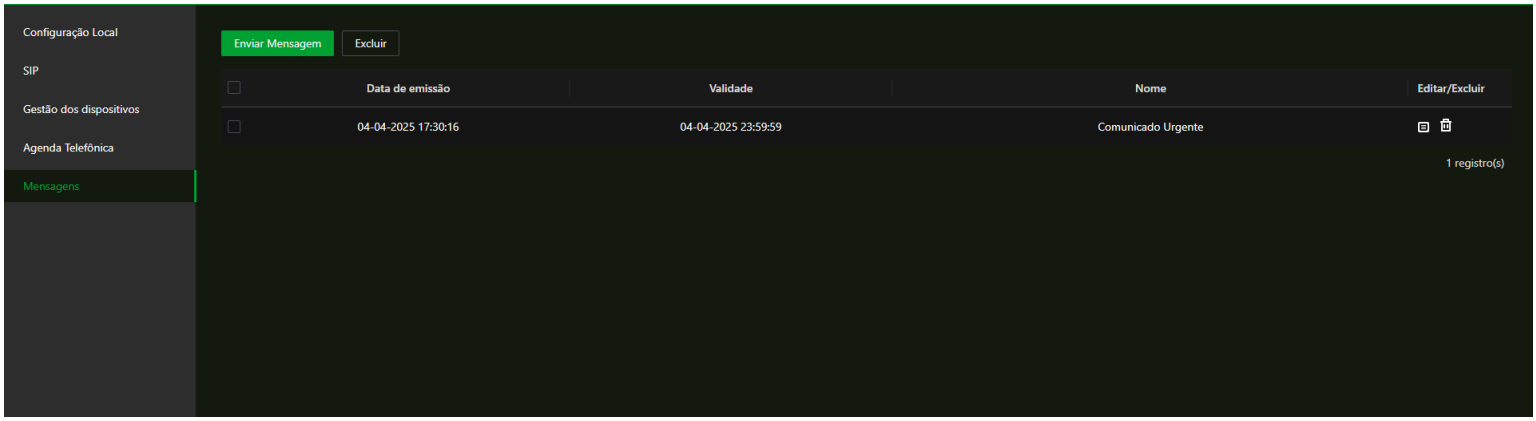



- **Exibição da Sala:** Permite selecionar quantos apartamentos serão exibidos por página.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:**Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

# Mensagens

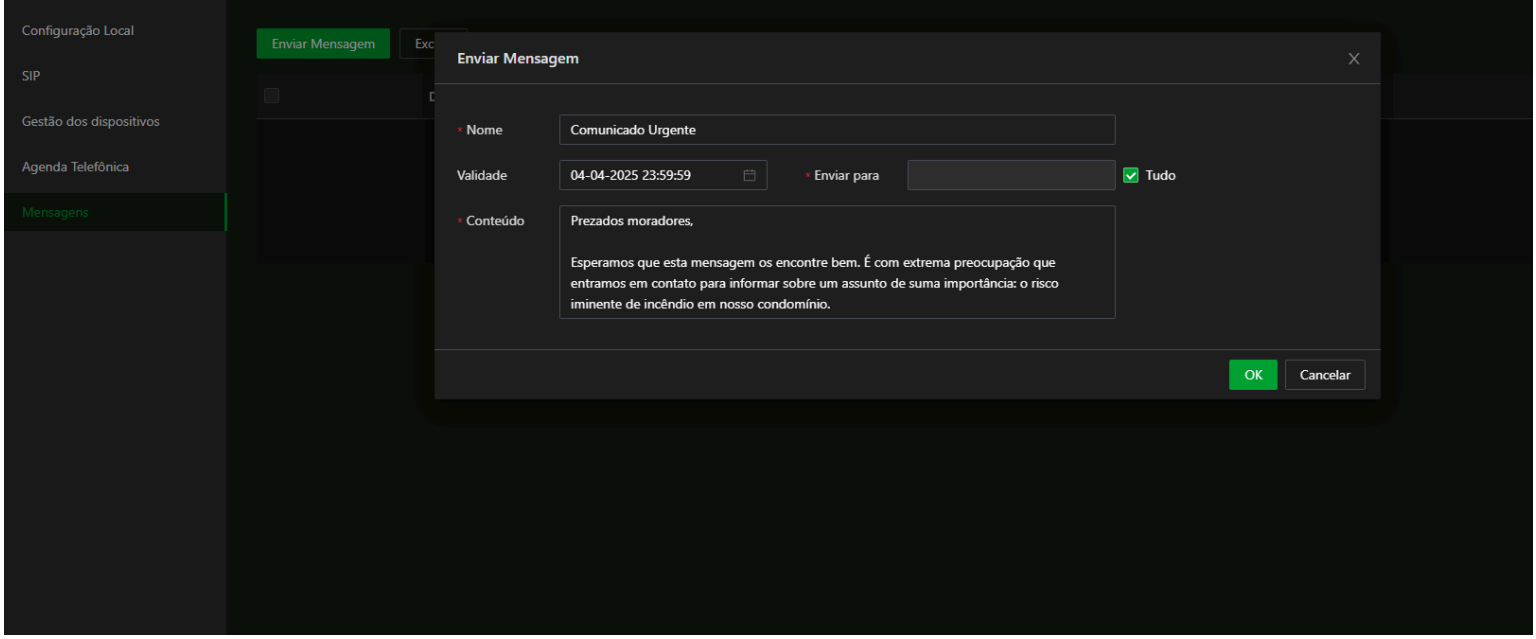
Esse menu permite enviar mensagens para facilitar a comunicação com os moradores do empreendimento. Também é possível consultar o histórico de mensagens clicando no ícone ou excluir clicando no ícone

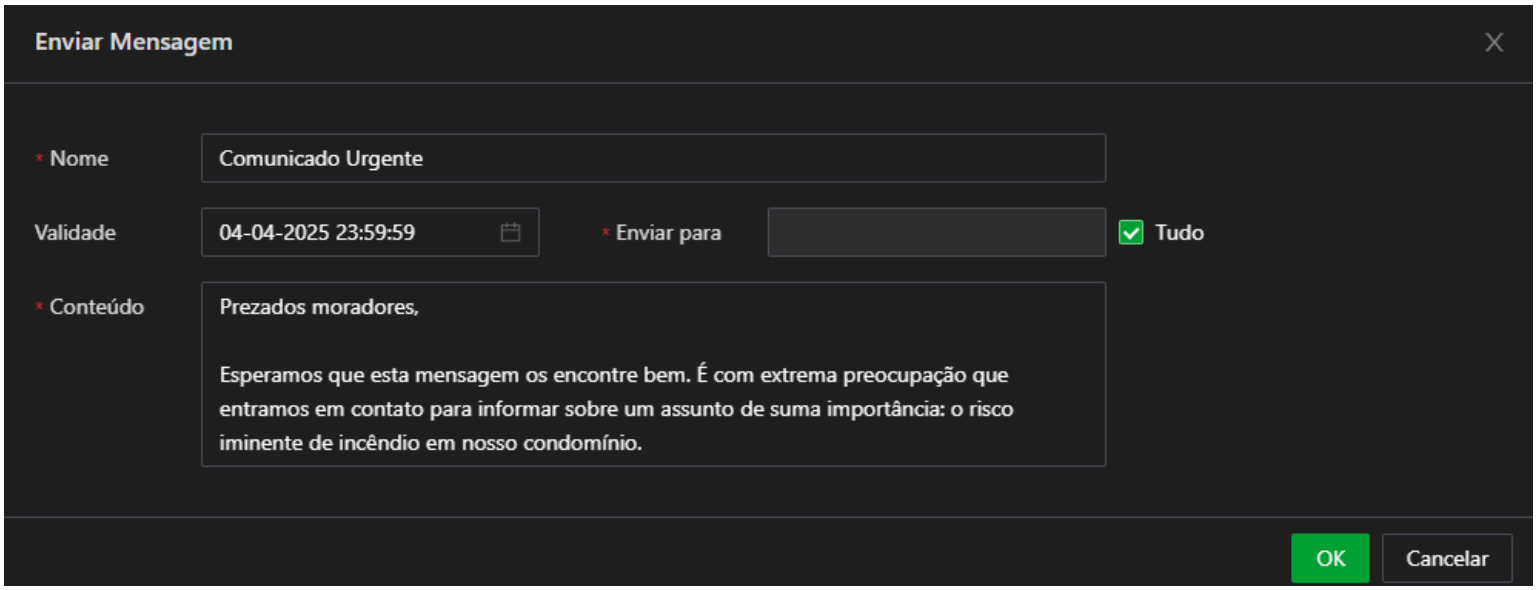
Essa função está disponível apenas para os modelos de tela TVIP 2210, TVIP 2220 e TVIP 2221.




# Enviar Mensagem

Para enviar mensagens, clique na opção enviar mensagens para abrir a janela onde você poderá preencher os parâmetros de envio e selecionar os destinatários.




- **Nome:** Insira um título para a mensagem, com um máximo de 28 caracteres.
- **Validade:** Define até quando o sistema tentará enviar a mensagem para o apartamento. Se o usuário do apartamento 101 estiver de férias e desligar seu TVIP, a mensagem será entregue quando ele ligar, desde que esteja dentro do período de validade.
- **Enviar para:** É possível enviar a mensagem para todos os TVIP 2210, TVIP 2220 e TVIP 2221 do condomínio selecionando a opção "Tudo". Para enviar a mensagem a um apartamento específico, desmarque a opção "Tudo" e preencha o número do apartamento desejado.
- **Conteúdo:** Insira a mensagem que deseja enviar, com um máximo de 256 caracteres.
- **Ok:** Salva as alterações feitas.
- **Cancelar:** Cancela as configurações realizadas.

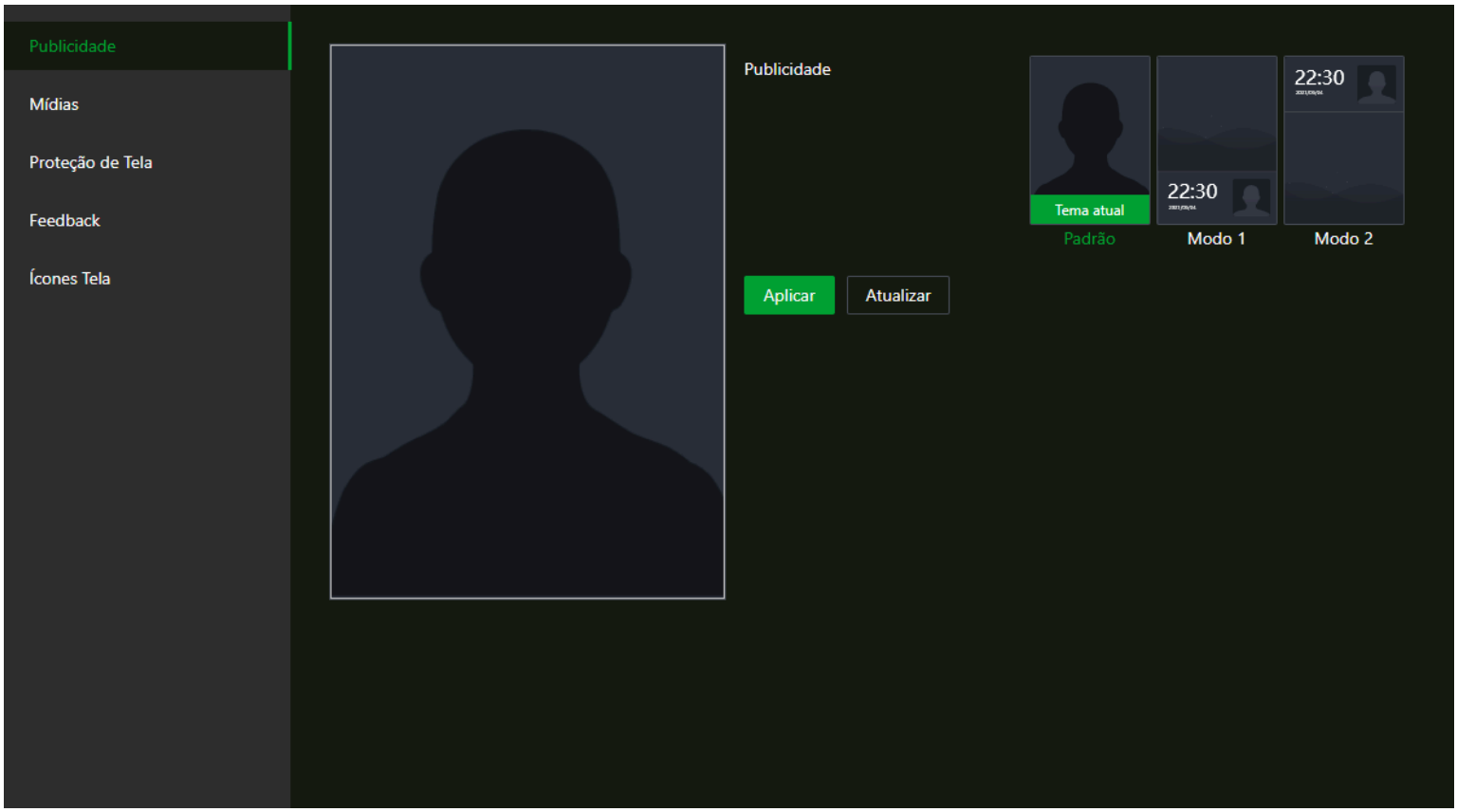
---

# TELA

Nesse menu é possível configurar modo publicidade, proteção de tela, feedback e mídias e icones de tela.

# Publicidade

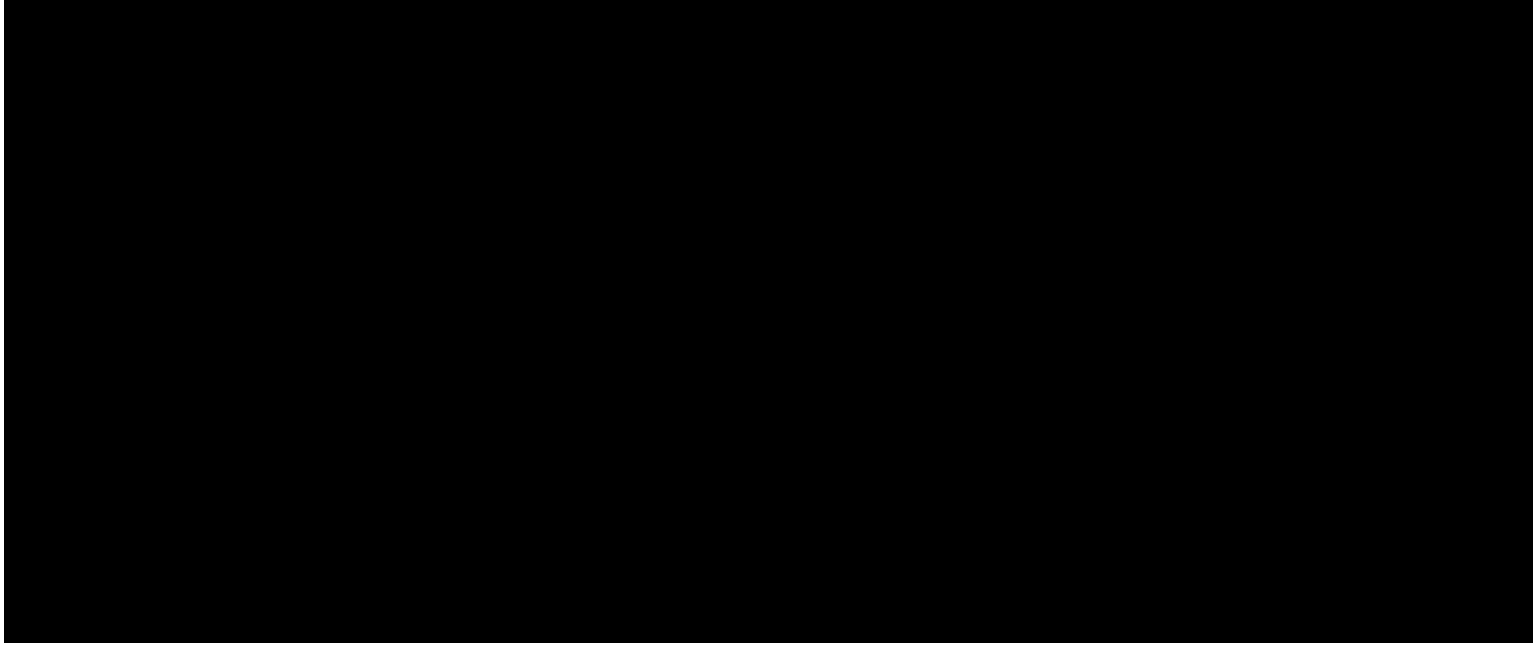
Esse menu permite configurar a forma como o controlador de acesso exibirá as informações na tela. Há três opções de exibição: Modo Padrão, Modo 1 e Modo 2. Nos Modos 1 e 2, é possível adicionar fotos, vídeos e textos personalizados.




- **Padrão:** Exibe a imagem do rosto em tela cheia.
- **Modo 1:** A parte superior exibe anúncios, enquanto a parte inferior exibe o horário e a detecção facial.
- **Modo 2:** A parte superior exibe o horário e a detecção facial, enquanto a parte inferior exibe anúncios.

# Configurações modo publicidade

O Vídeo abaixo mostra adição de dois arquivos, uma foto e um vídeo.



Para vídeos e fotos, é possível configurar a exibição em tela cheia ou na escala original. Além disso, é possível definir até 10 períodos de exibição e ajustar o intervalo entre as mídias, com duração de 1 a 20 segundos.

O Vídeo abaixo mostra adição de texto na tela do dispositivo

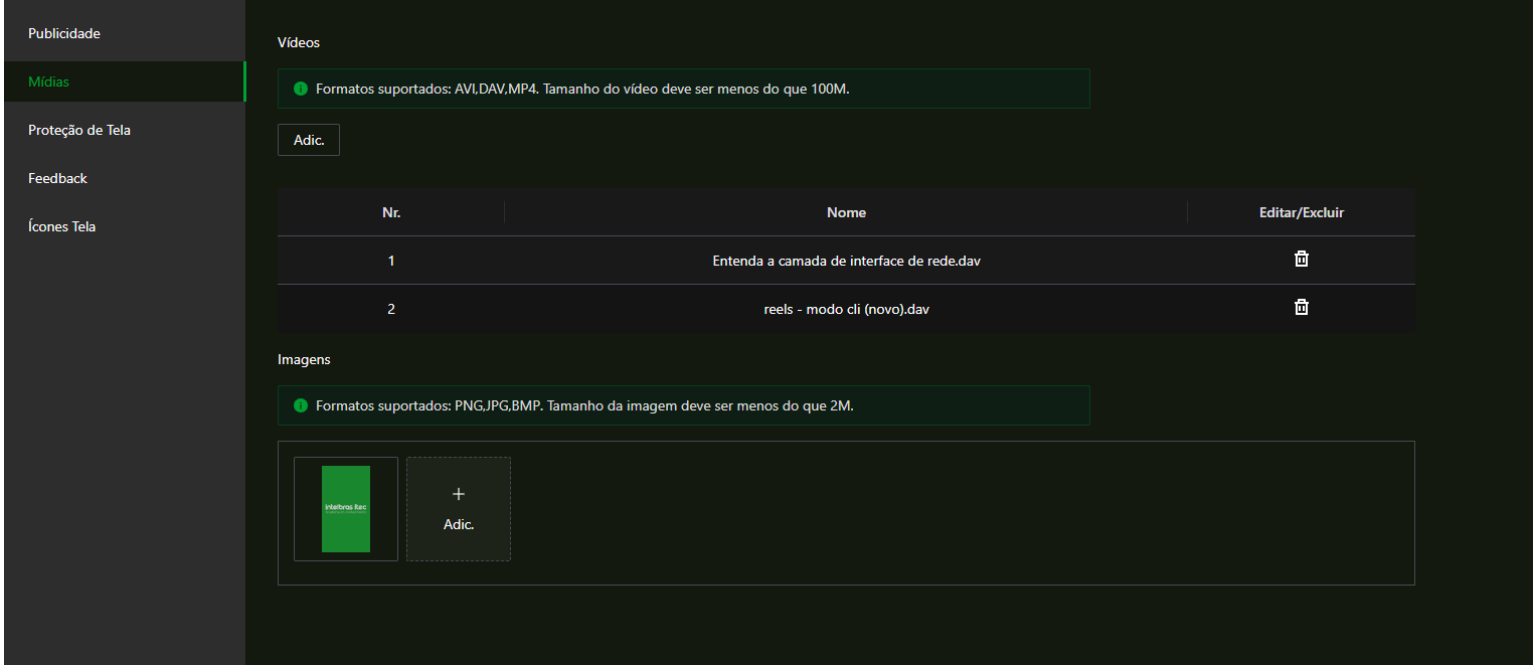
Para configurações de texto, é possível escolher até três modelos de plano de fundo, adicionar um título de até 30 caracteres e um subtítulo de até 60 caracteres.

**Observação:** Ao ativar o modo publicidade (Modo 1 e 2) com vídeo sendo reproduzido, não será vocalizado a mensagem de áudio para os feedbacks de acesso.

Apenas um modo de exibição pode ser selecionado por vez, ou seja, não é possível mesclar a exibição de mídias e texto simultaneamente.

# Mídias

É possível fazer o upload de vídeos e imagens para o dispositivo, que podem ser usados nas abas "Publicidade" e "Proteção de Tela". O dispositivo suporta até 10 imagens nos formatos PNG, JPG e BMP, com tamanho máximo de 2 MB. Além disso, suporta até 5 vídeos nos formatos AVI, DAV e MP4, com tamanho inferior a 100 MB.




O Vídeo abaixo mostra com fazer o upload de mídias para o dispositivo

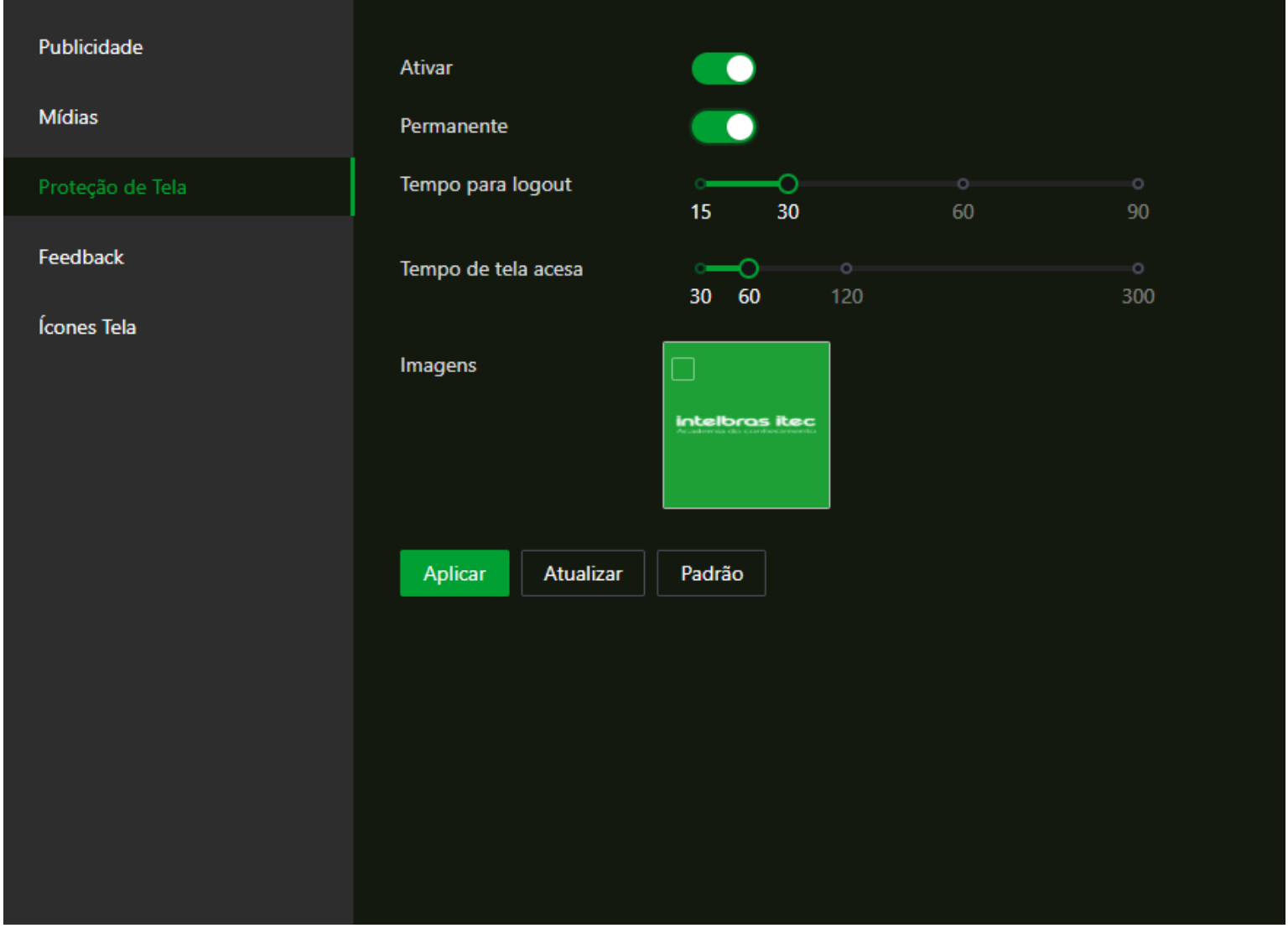
**Observação:** Para fazer o upload do vídeo ao dispositivo (carregar o vídeo), é necessário baixar o plug-in que será disponibilizado pela interface web do equipamento. Esse plug-in é um conversor de mídia e é necessário para o correto funcionamento do vídeo junto ao produto.

Uma vez instalado, não será mais necessário sua reinstalação para os próximos vídeos enviados ao dispositivo.

*Esse plug-in não será disponibilizado fora da interface web do dispositivo.*

# Proteção de tela

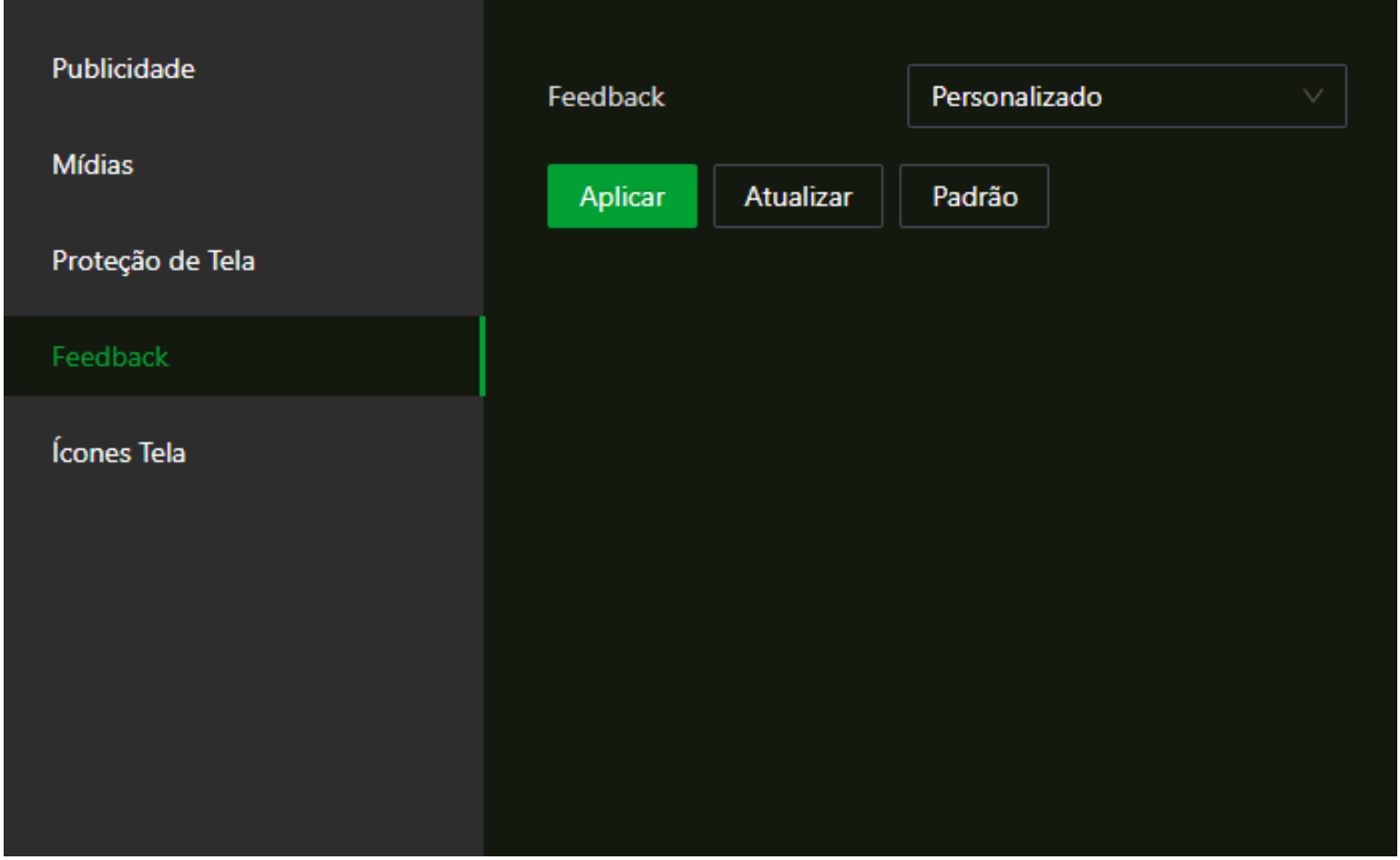
Quando o dispositivo estiver em repouso e a proteção de tela estiver ativa, a imagem selecionada será exibida. É possível escolher apenas uma imagem. Se a opção "Permanente" for ativada, a imagem ficará na tela continuamente enquanto o dispositivo estiver em repouso. Caso contrário, a imagem será exibida pelo tempo configurado em segundos e, em seguida, a tela será desligada.




- **Ativar:** Habilita ou desabilita o modo de proteção de tela.
- **Permanente:** Se a opção for ativada, a imagem ficará na tela continuamente enquanto o dispositivo estiver em repouso.
- **Tempo para logout:** Tempo, em segundos, para o dispositivo sair do modo de configuração devido à inatividade.
- **Tempo de tela acessa:** Tempo, onde sistema retorna para a tela de espera e, após um tempo definido de inatividade, a tela é desligada ou uma imagem será exibida quando habilitado o modo "Permanente".

# Feedback

O dispositivo oferece cinco opções de feedback. Para ativá-las, é necessário que o dispositivo esteja configurado em "modo padrão" na aba "Publicidade".

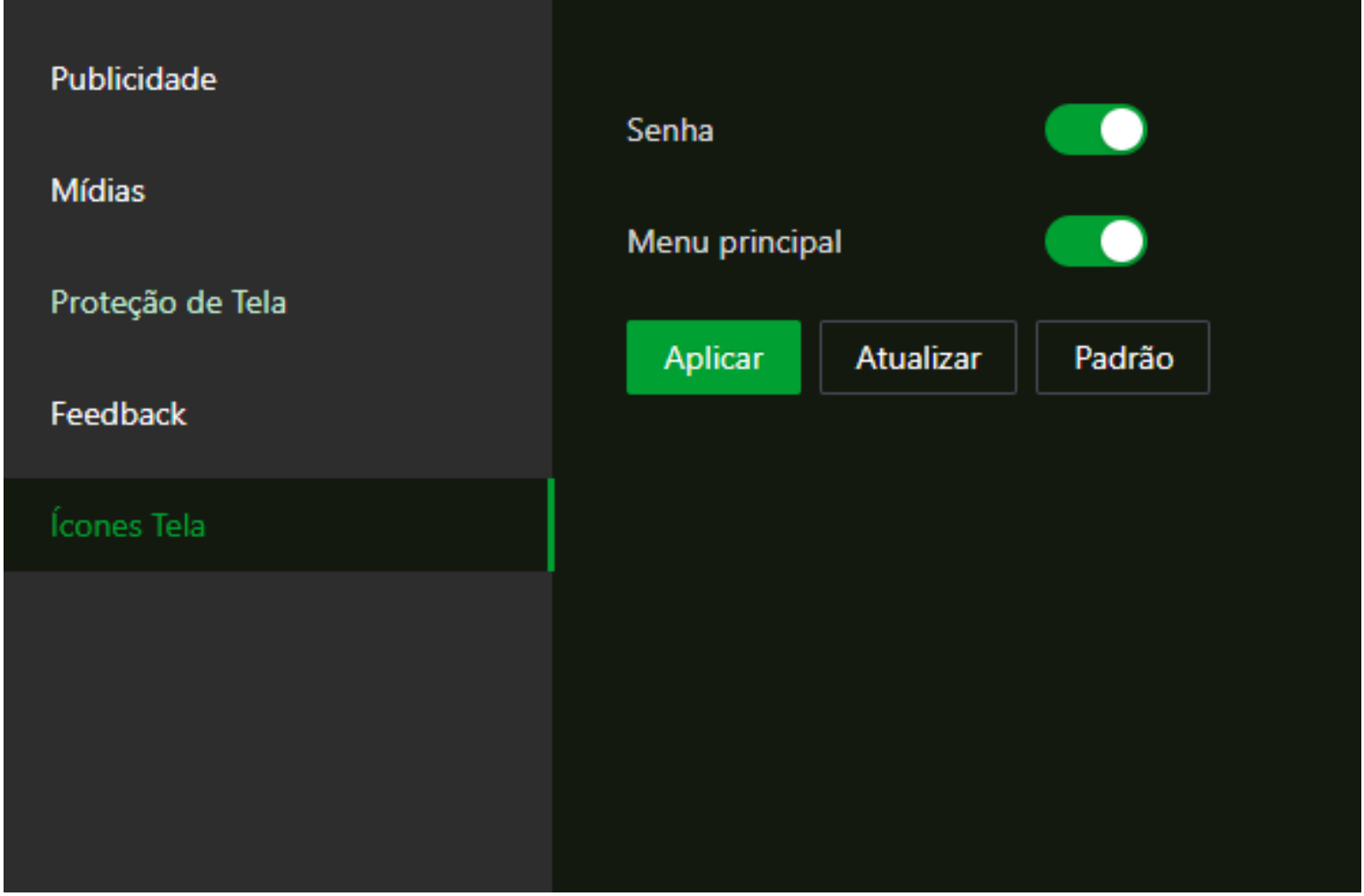



## As cinco opções de feedback são:

- **Sucesso ou falha.**
- **Somente nome.**
- **Padrão.**
- **Foto, imagem e nome.**
- **Personalizado.**
- **Nenhum.**

## Ícones Tela

Permite ao usuário habilitar ou desabilitar o ícone senha ( ) e o ícone menu ( ) da tela do dispositivo .



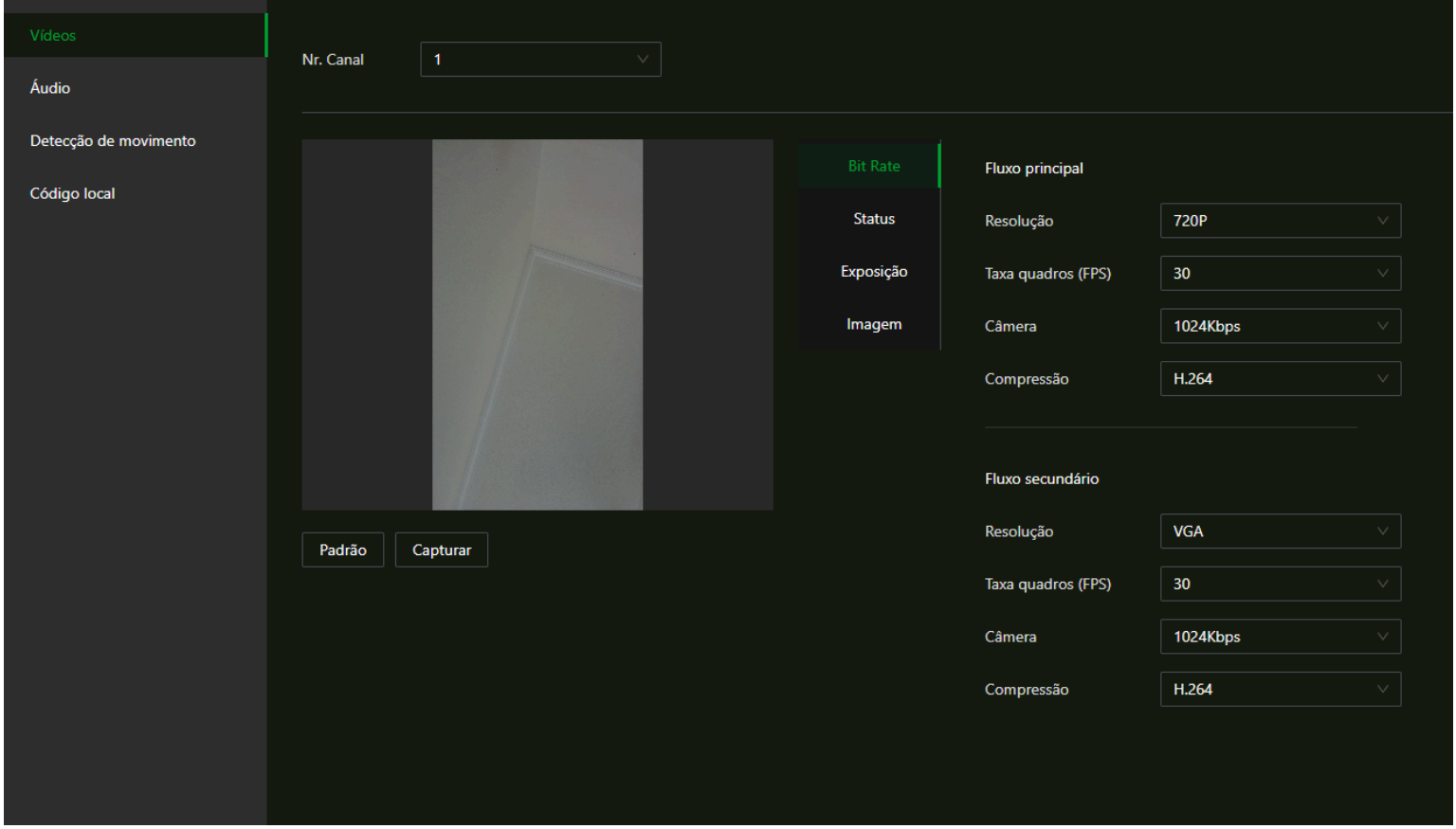

---

# ÁUDIO E VÍDEO

Menu para configurações dos parâmetros de áudio e vídeo do controlador de acesso.

## Config. de vídeo câmera 1 (RGB)

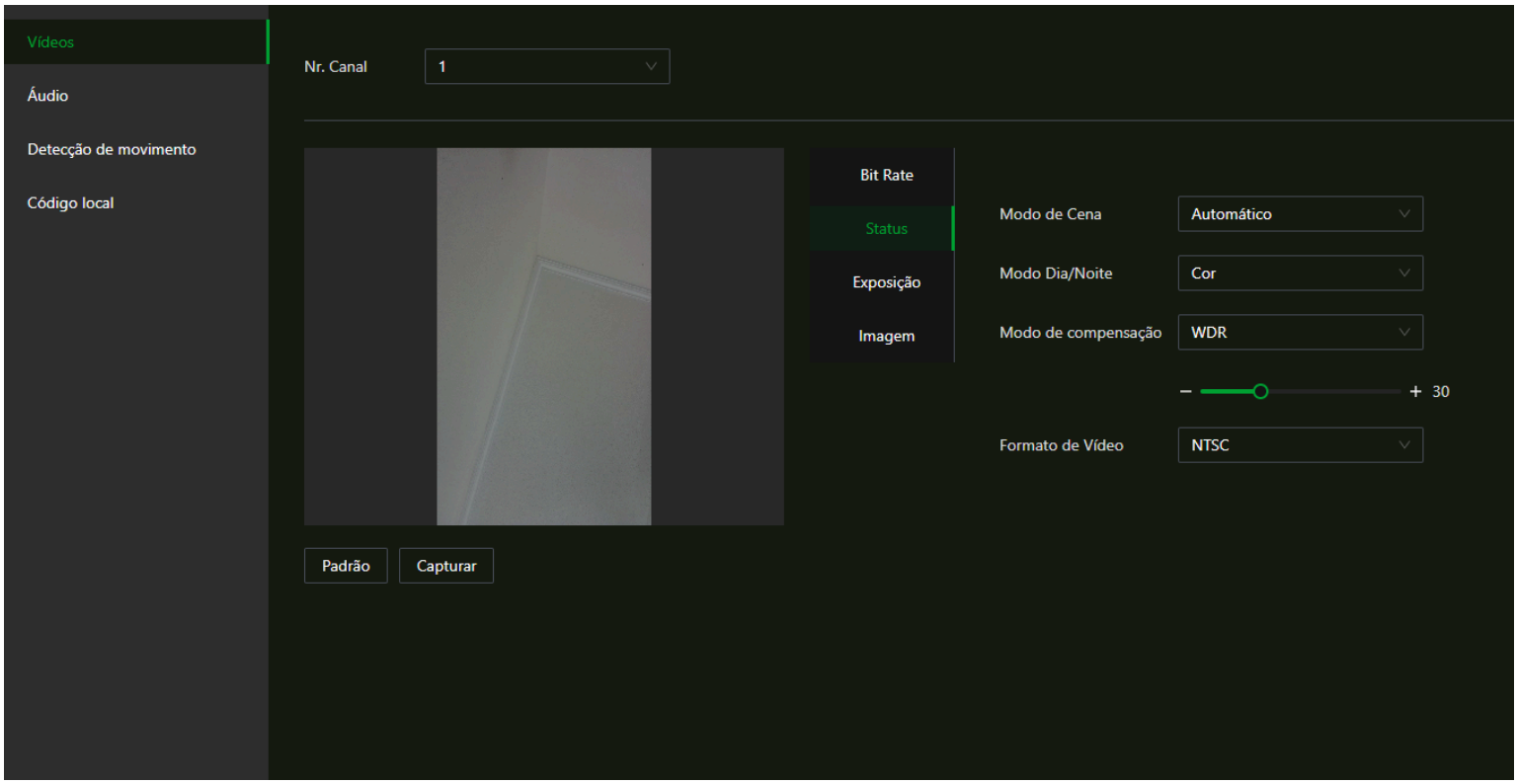
Você pode definir parâmetros, incluindo taxa de dados, parâmetros de imagem (brilho, contraste, matiz, saturação, e mais) e exposição na página de configuração de vídeo.




- **ID canal:** Alterna entre as configurações para a câmera RGB (1) e câmera infravermelho (2).
- **Padrão:** Restaura as configurações para os valores padrão.
- **Captura:** Captura uma imagem instantânea da visualização atual.
- **Bit Rate:**

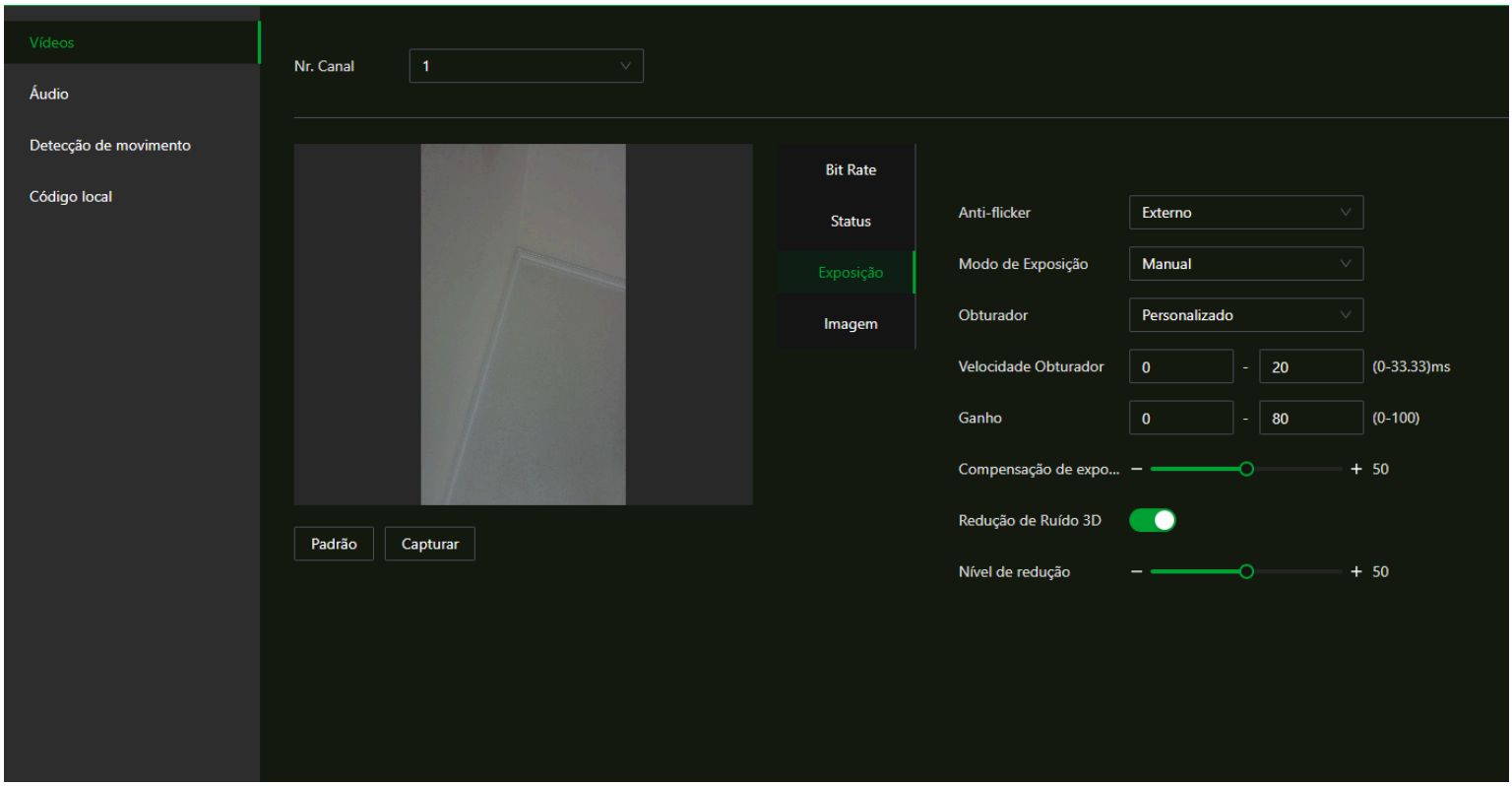
  Configuração disponível apenas para a câmera principal.

  - **Fluxo principal:** Transmissão de vídeo do canal RGB via RTSP.
    - **Resolução:**
      - **D1:** Define a resolução do vídeo em NTSC para 704x480px e em PAL para 704x576px.
      - **VGA:** Define a resolução do vídeo para 640x480px.
      - **720P:** Define a resolução do vídeo para 1280x720px.
      - **1080P:** Define a resolução do vídeo para 1920x1080px.
    - **Taxa de quadros (FPS):** Define a taxa de quadros por segundo do vídeo.
    - **Câmera:** Define o número de bits que são transmitidos ou processados por unidade de tempo.
    - **Compressão:** Exibe a compressão de vídeo da imagem.
  - **Fluxo secundário:** Transmissão de vídeo do canal IR via RTSP.
    - **Resolução:**
      - **D1:** Define a resolução do vídeo em NTSC para 704x480px e em PAL para 704x576px.
      - **VGA:** Define a resolução do vídeo para 640x480px.
    - **Taxa de quadros:** Define a taxa de quadros por segundo do vídeo.
    - **Câmera:** Define o número de bits que são transmitidos ou processados por unidade de tempo.
    - **Compressão:** Exibe a compressão de vídeo da imagem.



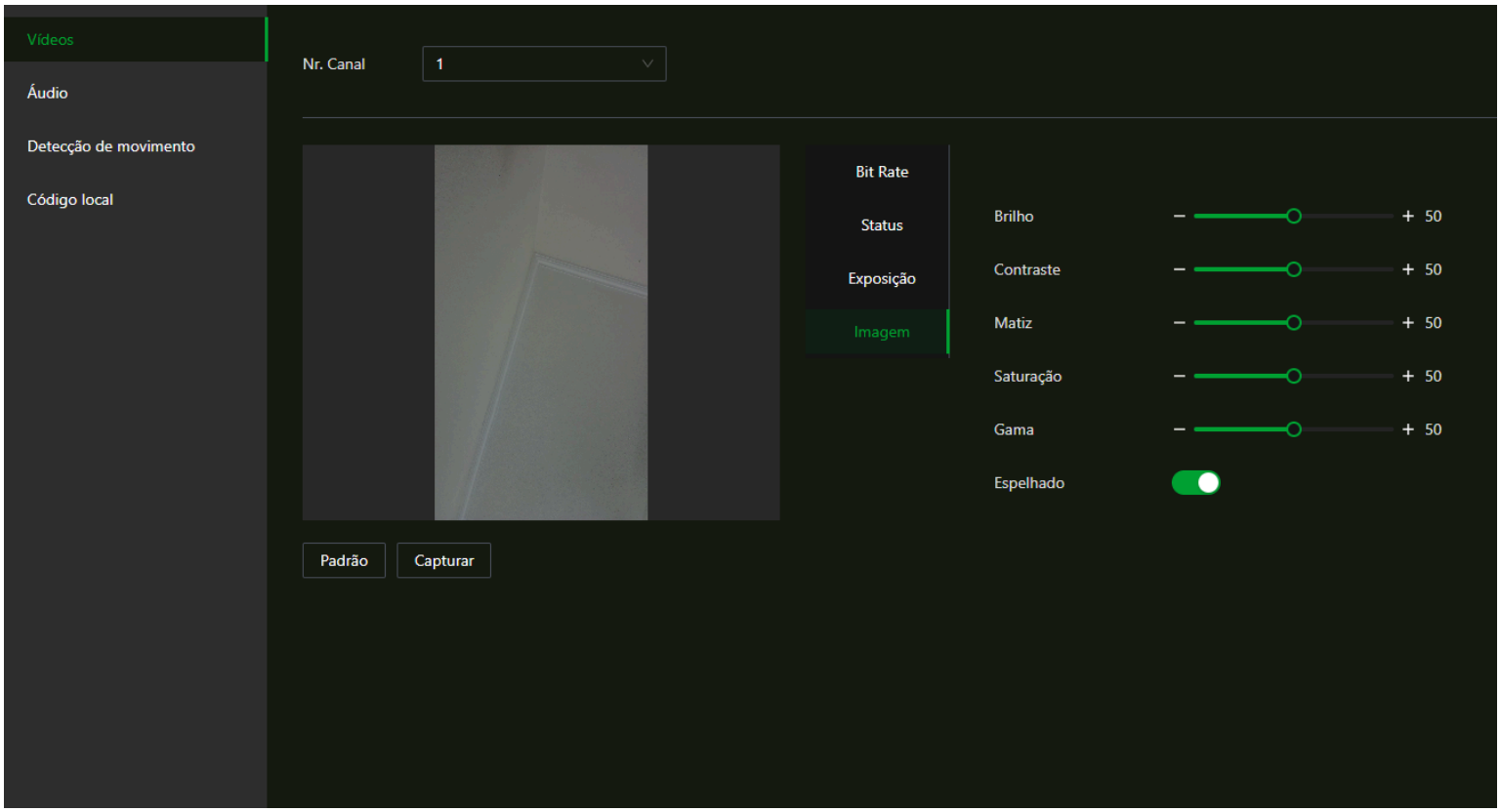

- **Status:**
  - **Modo de cena:** Altera parâmetros de imagem para adaptá-la melhor ao ambiente capturado pela câmera.
    - **Desativar:** Sem qualquer adaptação na imagem capturada pela câmera.
    - **Automático:** O sistema ajusta automaticamente o modo de cena para adaptar-se ao ambiente capturado pela câmera.
    - **Ensolarado:** Neste modo, a tonalidade da imagem será reduzida.
    - **Noite:** Neste modo, a tonalidade da imagem será aumentada.

      Obs.: Automático é valor padrão.
  - **Modo Dia/Noite:** O Modo Dia/Noite decide o status de trabalho da luz de preenchimento.
    - **Automático:** O sistema ajusta automaticamente entre os Modo Dia/Noite.
    - **Cor:** Neste modo, as imagens ficam com cores.
    - **Preto e branco:** Neste modo, as imagens são em preto e branco.
  - **Modo de compensação:**
    - **Desativar:** Sem compensação de luz de fundo.
    - **BLC:** A compensação de luz de fundo corrige regiões com níveis extremamente altos ou baixos níveis de luz para manter um nível de luz normal e utilizável para o objeto em foco.
    - **WDR:** No modo de ampla faixa dinâmica, o sistema escurece as áreas claras e compensa as áreas escuras para garantir a definição dos objetos no áreas claras e áreas escuras. Quando rostos humanos estão na luz de fundo, você precisa habilitar o WDR.
    - **Inibição:** A compensação de destaque é necessária para compensar superexposição de destaques ou fontes de luz fortes como holofotes, faróis, luzes da varanda, etc. para criar uma imagem que seja utilizável e não ultrapassado por uma luz brilhante.
    - **Formato de vídeo:** Permite alternar o formato de vídeo entre NTSC e PAL.



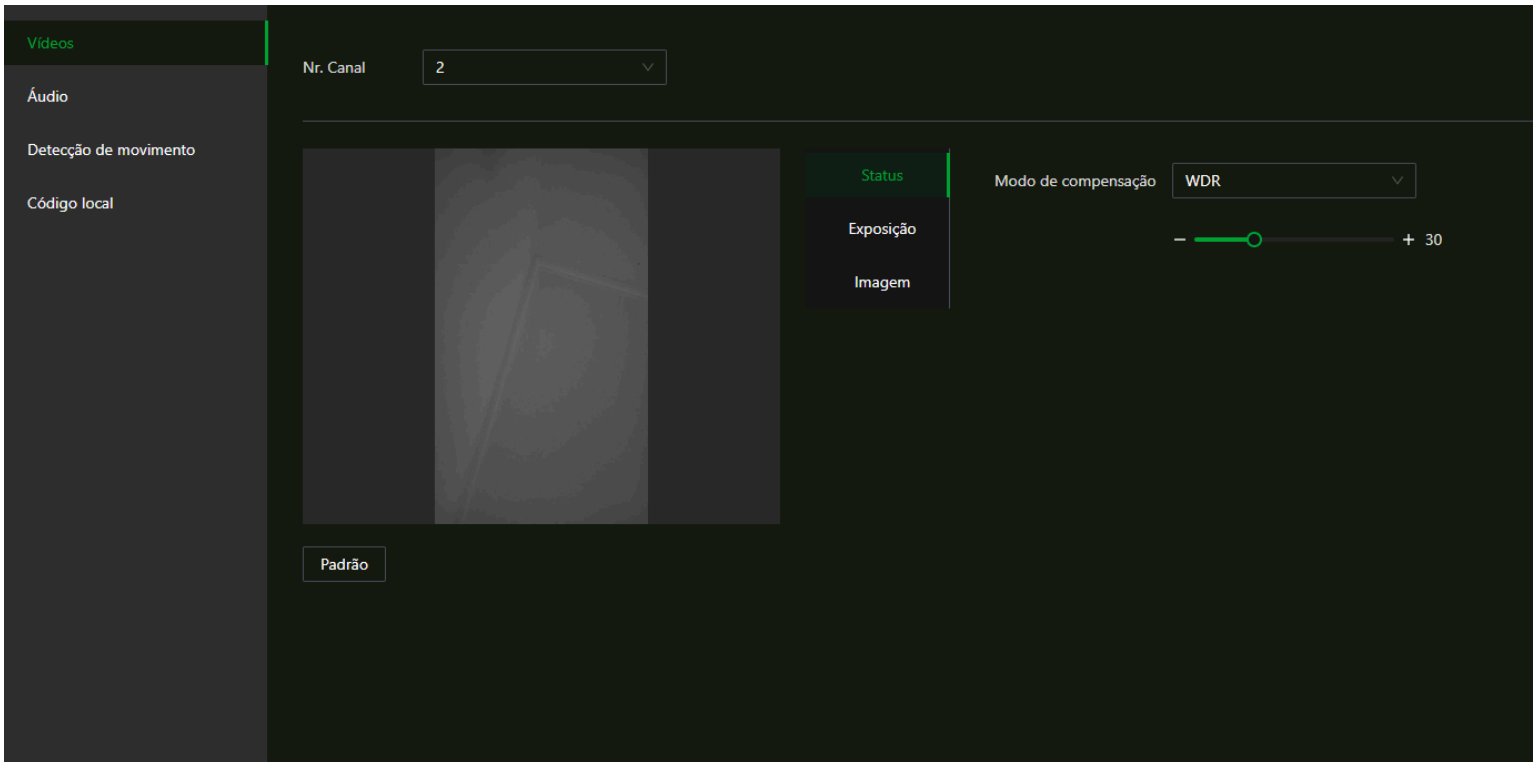

- **Exposição**
  - **Anti-flicker:** Se a frequência das lâmpadas que iluminam o ambiente estiverem na mesma frequência de captura da câmera, a imagem do vídeo pode apresentar cintilação (efeito flicker), em que listras ou faixas aparecem na imagem. Para contornar isso, altere a frequência de captura de imagem.
    - **Externo:** Quando selecionado, o habilita a opção "Prioridade Obturador" dentro do menu "Modo de exposição", que se selecionada, permite a seleção do valor do obturador da câmera.
    - **50Hz:** Quando a frequência da iluminação do ambiente é 50Hz, a exposição é automaticamente ajustada para garantir que não haja listras na imagem.
    - **60Hz:** Quando a frequência da iluminação do ambiente é 60Hz, a exposição é automaticamente ajustada para garantir que não haja listras na imagem.
  - **Modo de exposição:** Controla a quantidade de brilho capturado pela câmera
    - **Automático:** O controlador de acesso ajustará automaticamente o brilho das imagens capturadas.
    - **Prioridade Obturador:** O controlador de acesso ajustará o brilho das imagens capturadas de acordo com a faixa de exposição configurada para o obturador. No entanto, se o brilho da imagem capturada não for o suficiente e o valor do obturador estiver no limite superior ou inferior, o controlador de acesso ajustará automaticamente o ganho para obter o brilho ideal para a imagem.
    - **Manual:** Você pode configurar os valores de ganho e do obturador manualmente para ajustar o brilho da imagem.
      - **Obturador:** Define a abertura da câmera para permitir a passagem de luz. É definido em ms.
        - 1/100000
        - 1/300000
        - 1/10000
        - 1/4000
        - 1/2000
        - 1/500

        - 1/250
        - 1/120
        - 1/60
        - 1/30
        - **Personalizado:** Permite definir manualmente o valor do obturador em milissegundos com range de 0~33.33ms.
    - **Ganho:** Define um range do ganho de brilho aplicado à imagem na captura. Pode variar de 0 a 100
- **Compensação de exposição:** Você pode aumentar o brilho do vídeo ajustando o valor de compensação de exposição.
- **Redução de ruído 3D:** Quando a Redução de Ruído 3D (RD) está habilitada, o ruído de vídeo pode ser reduzido e vídeos de alta definição serão produzidos.
    - **Nível de redução:** Quando redução de ruído 3D estiver habilitado, é possível ajustar seu valor. Quanto maior o valor, menor será o ruído.

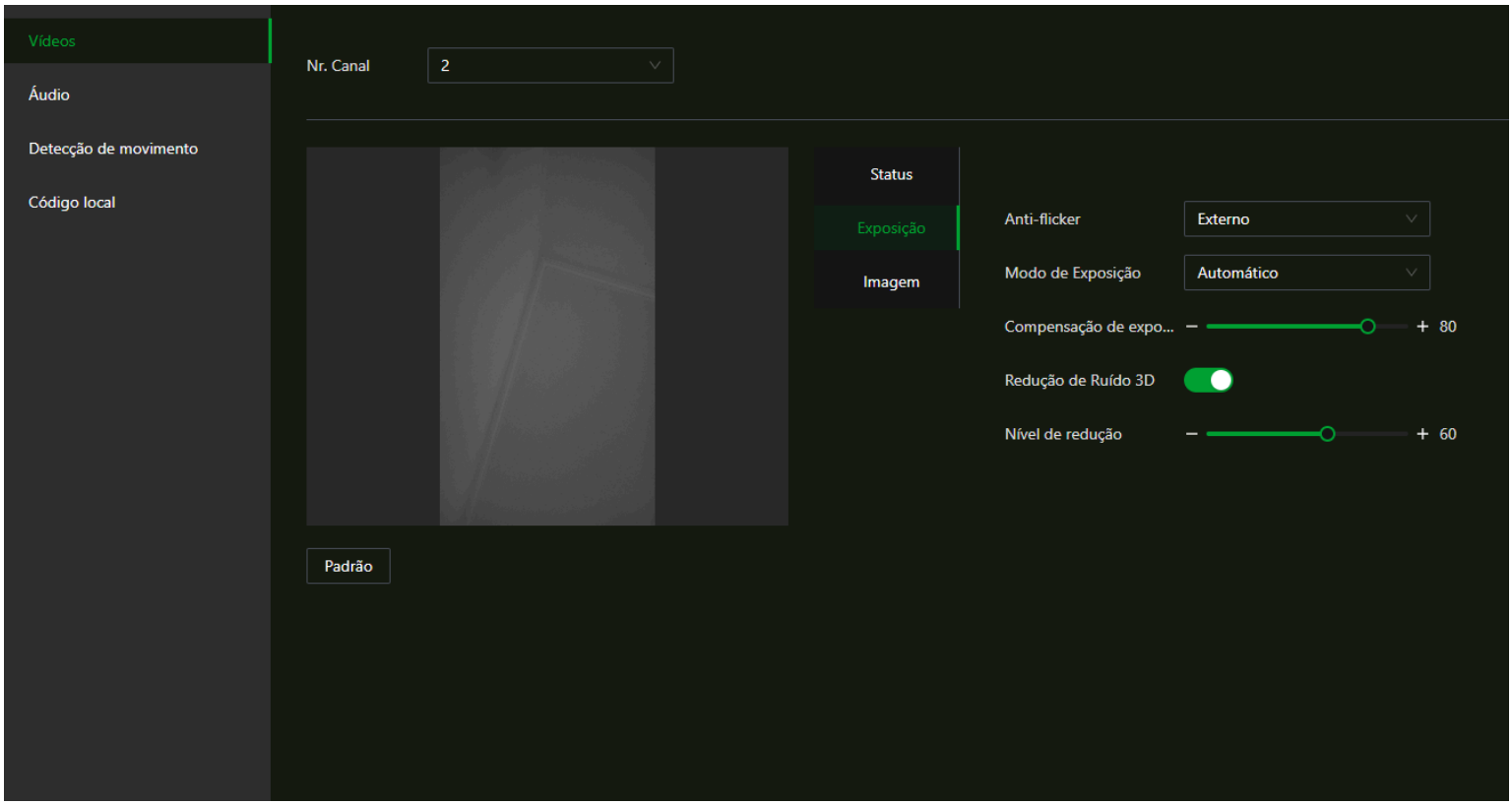



- **Imagem**
    - **Brilho:** Define o brilho da imagem. Quanto maior o valor, maior o brilho da imagem será. Varia de 0 a 100.
    - **Contraste:** Contraste é a diferença de luminância ou cor que torna um objeto distinguível. Quanto maior for o valor de contraste, maior será o brilho e o contraste da cor.
    - **Matiz:** Quanto maior o valor, mais acentuada será a cor.
    - **Saturação:** Quanto maior o valor, mais vibrantes serão as cores.
    - **Espelhado:** Se habilitado, espelha a imagem.

# Config. de vídeo câmera 2 (IR)

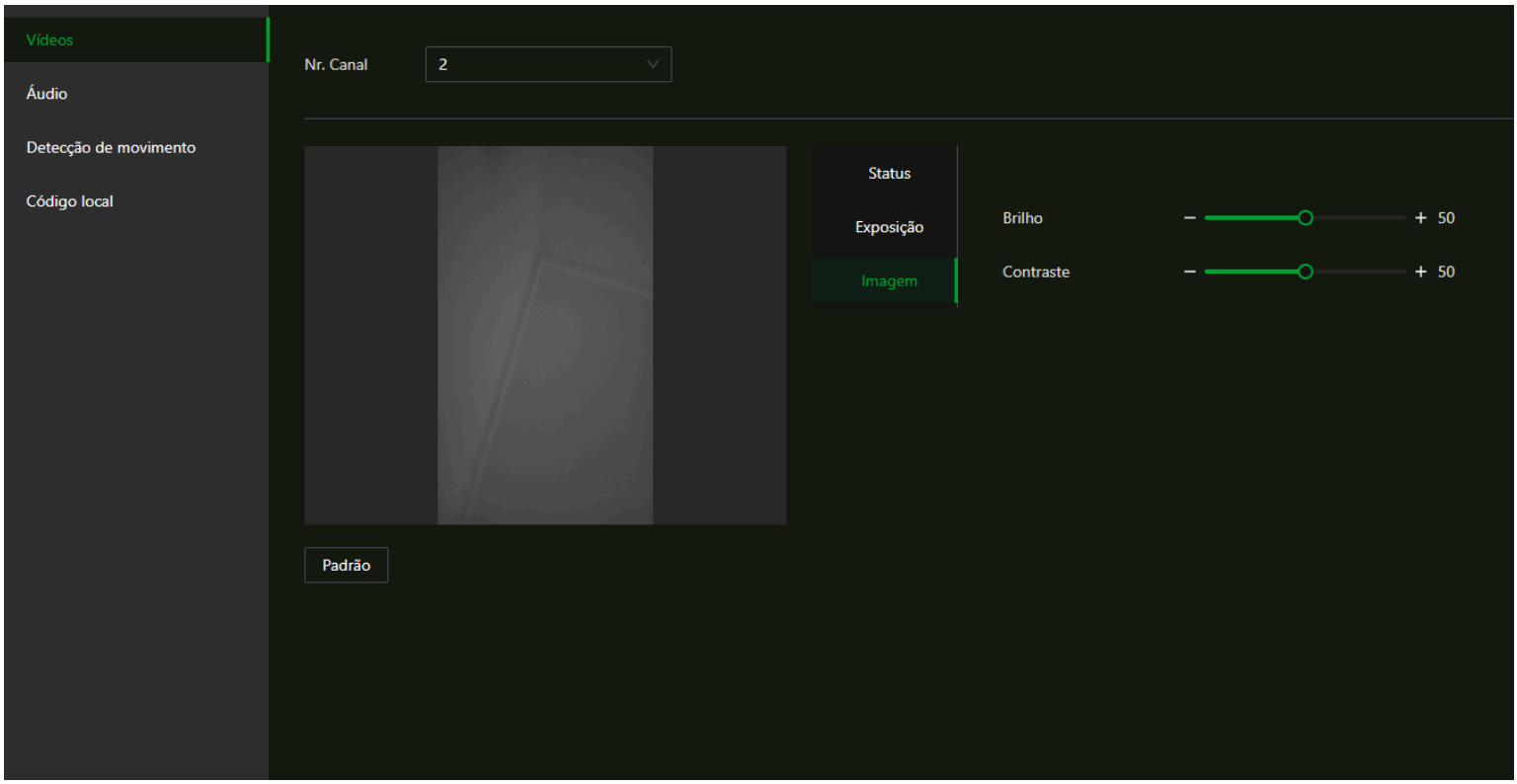



- **Status:**
  - **Modo de compensação:**
    - **Desativar:** Sem compensação de luz de fundo.
    - **BLC:** A compensação de luz de fundo corrige regiões com níveis extremamente altos ou baixos níveis de luz para manter um nível de luz normal e utilizável para o objeto em foco.
    - **WDR:** No modo de ampla faixa dinâmica, o sistema escurece as áreas claras e compensa as áreas escuras para garantir a definição dos objetos no áreas claras e áreas escuras. Quando rostos humanos estão na luz de fundo, você precisa habilitar o WDR.
    - **Inibição:** A compensação de destaque é necessária para compensar superexposição de destaques ou fontes de luz fortes como holofotes, faróis, luzes da varanda, etc. para criar uma imagem que seja utilizável e não ultrapassado por uma luz brilhante.
    - **Formato de vídeo:** Permite alternar o formato de vídeo entre NTSC e PAL.




- **Exposição**
  - **Anti-flicker:** Se a frequência das lâmpadas que iluminam o ambiente estiverem na mesma frequência de captura da câmera, a imagem do vídeo pode apresentar cintilação (efeito flicker), em que listras ou faixas aparecem na imagem. Para contornar isso, altere a frequência de captura de imagem.
    - **Externo:** Quando selecionado, o habilita a opção "Prioridade Obturador" dentro do menu "Modo de exposição", que se selecionada, permite a seleção do valor do obturador da câmera.
    - **50Hz:** Quando a frequência da iluminação do ambiente é 50Hz, a exposição é automaticamente ajustada para garantir que não haja listras na imagem.
    - **60Hz:** Quando a frequência da iluminação do ambiente é 60Hz, a exposição é automaticamente ajustada para garantir que não haja listras na imagem.
  - **Modo de exposição:** Controla a quantidade de brilho capturado pela câmera
    - **Automático:** O controlador de acesso ajustará automaticamente o brilho das imagens capturadas.
    - **Prioridade Obturador:** O controlador de acesso ajustará o brilho das imagens capturadas de acordo com a faixa de exposição configurada para o obturador. No entanto, se o brilho da imagem capturada não for o suficiente e o valor do obturador estiver no limite superior ou inferior, o controlador de acesso ajustará automaticamente o ganho para obter o brilho ideal para a imagem.
    - **Manual:** Você pode configurar os valores de ganho e do obturador manualmente para ajustar o brilho da imagem.
      - **Obturador:** Define a abertura da câmera para permitir a passagem de luz. É definido em ms.
        - 1/100000
        - 1/300000
        - 1/10000
        - 1/4000
        - 1/2000

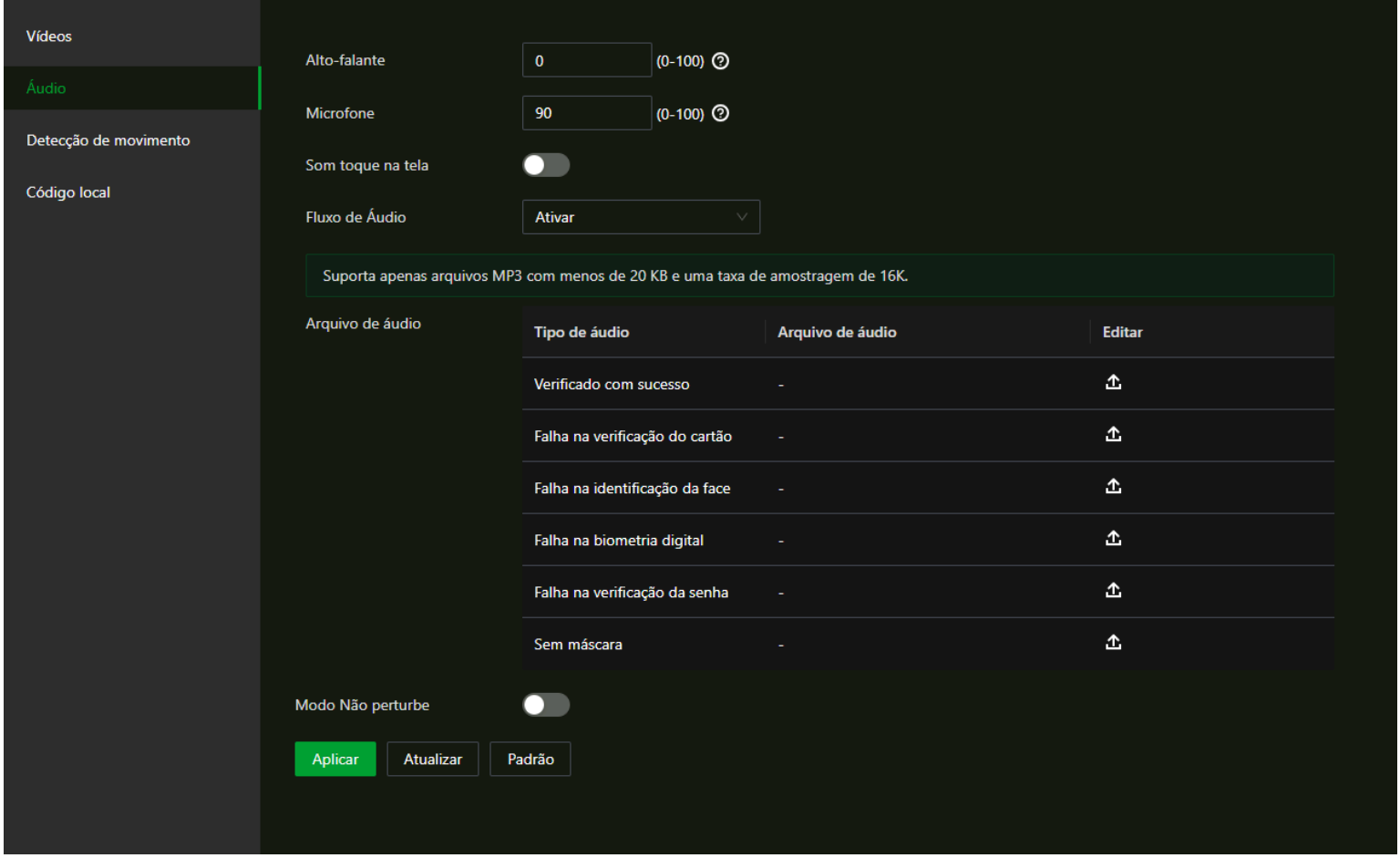
        - 1/500
        - 1/250
        - 1/120
        - 1/60
        - 1/30
        - **Personalizado:** Permite definir manualmente o valor do obturador em milissegundos com range de 0~33.33ms.
    - **Ganho:** Define um range do ganho de brilho aplicado à imagem na captura. Pode variar de 0 a 100
- **Compensação de exposição:** Você pode aumentar o brilho do vídeo ajustando o valor de compensação de exposição.
- **Redução de ruído 3D:** Quando a Redução de Ruído 3D (RD) está habilitada, o ruído de vídeo pode ser reduzido e vídeos de alta definição serão produzidos.
    - **Nível de redução:** Quando redução de ruído 3D estiver habilitado, é possível ajustar seu valor. Quanto maior o valor, menor será o ruído.




- **Imagem**
    - **Brilho:** Define o brilho da imagem. Quanto maior o valor, maior o brilho da imagem será. Varia de 0 a 100.
    - **Contraste:** Contraste é a diferença de luminância ou cor que torna um objeto distinguível. Quanto maior for o valor de contraste, maior será o brilho e o contraste da cor.

# Áudio

Nessa seção é possível ajustar o volume do alto-falante do dispositivo, sensibilidade do microfone e personalização de feedbacks de acesso.

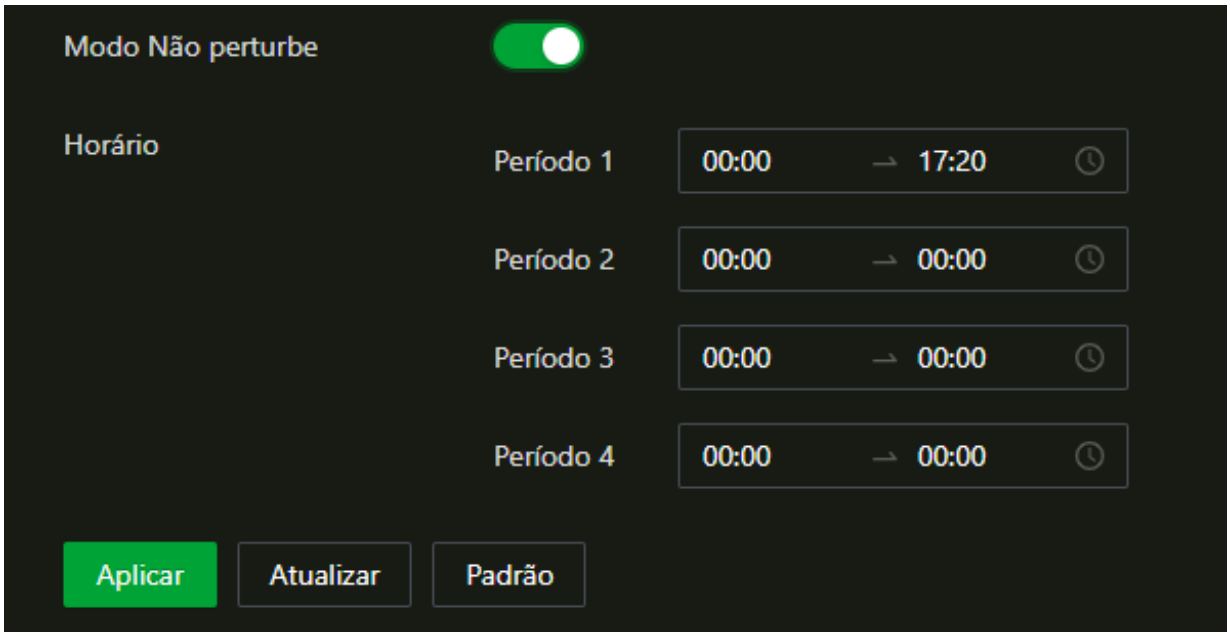



- **Alto-falante:** Ajuste o volume do alto-falante.
- **Microfone:** Ajusta a sensibilidade do microfone.
- **Som toque na tela:** Quando ativado, o dispositivo emitirá um som ao tocar na tela. Se o volume do alto-falante estiver configurado como "0", nenhum som será reproduzido.
- **Fluxo de Áudio:** Quando ativado, o som do microfone do dispositivo será capturado durante a visualização ao vivo e a gravação em uma chamada SIP.

  **Arquivo de áudio:** É possível adicionar um áudio para cada uma das seis notificações do controlador.

  **Obs.: Esta funcionalidade está disponível apenas para os acessos liberado e negado no modo stand-alone, e a personalização de áudio não é permitida para acessos via botoeira e liberações de acesso remoto.**

- **Modo Não perturbe:** Quando habilitado, o dispositivo não emitirá som de feedback ao identificar ou negar um usuário durante o período configurado, mesmo que um valor de volume tenha sido definido. É possível configurar até 4 períodos de tempo.

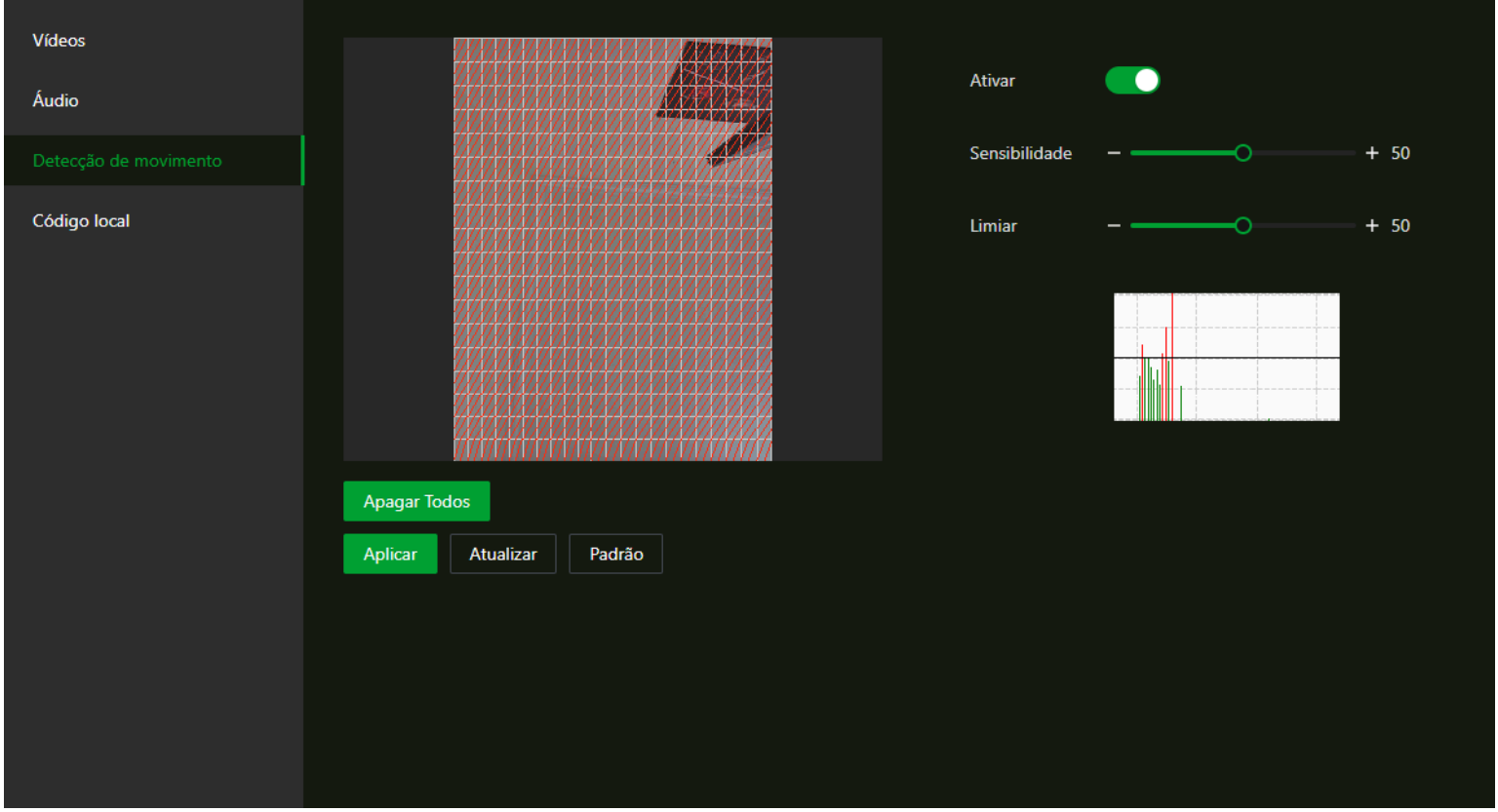



- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

## Detecção de movimento

Quando habilitado, ao detectar objetos em movimento, o LED infravermelho (IR) será acionado. Para garantir o reconhecimento facial em ambientes com baixa luminosidade, a tela será ativada assim que um rosto for identificado dentro do limite configurado.

A área de detecção de movimento é exibida em vermelho.



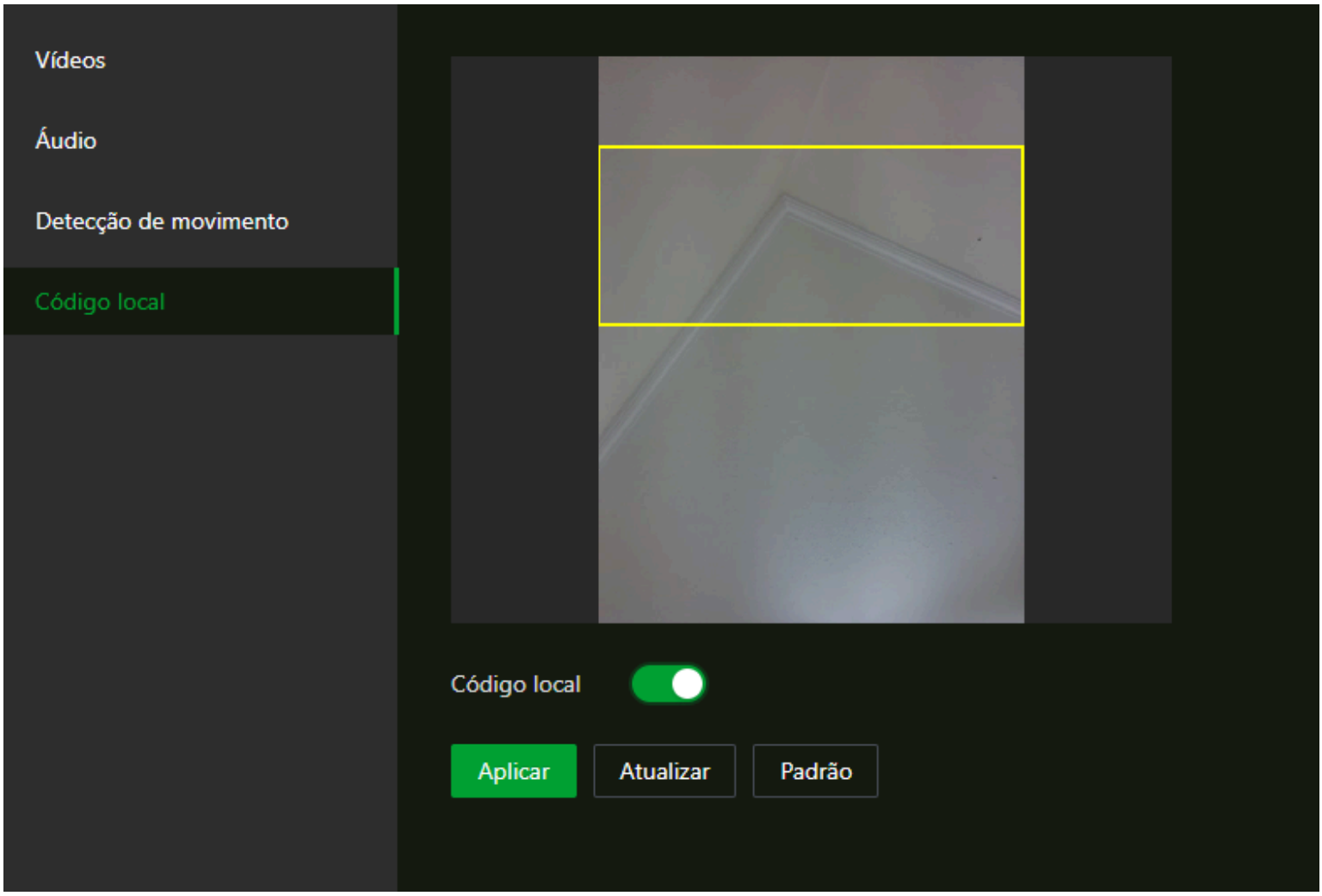

- **Ativar:** Habilita ou desabilita a detecção de movimento.
- **Sensibilidade:** Define o quão sensível o sistema é ao ambiente. Quanto maior a sensibilidade, mais facilmente será a detecção.
- **Limiar:** Representa a porcentagem da área do objeto em movimento dentro da área de detecção. Um limite maior facilita o acionamento.
- **Apagar todos:** Clique em apagar todos para remover a área de detecção de movimento existente.
  A área que você desenhar será considerada uma área sem detecção de movimento, caso seja desenhada sobre a área padrão de detecção.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

# Código local

Determina o recorte do vídeo que será enviado por streaming (RTSP e Onvif).

# Configuração de área de captura

Se "Código local" estiver habilitado, com o botão esquerdo do mouse, clique, segure e então araste o retângulo verde para cima ou para baixo.




- **Código Local:** Habilita ou desabilita o recorte para widescreen da imagem capturada.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

---

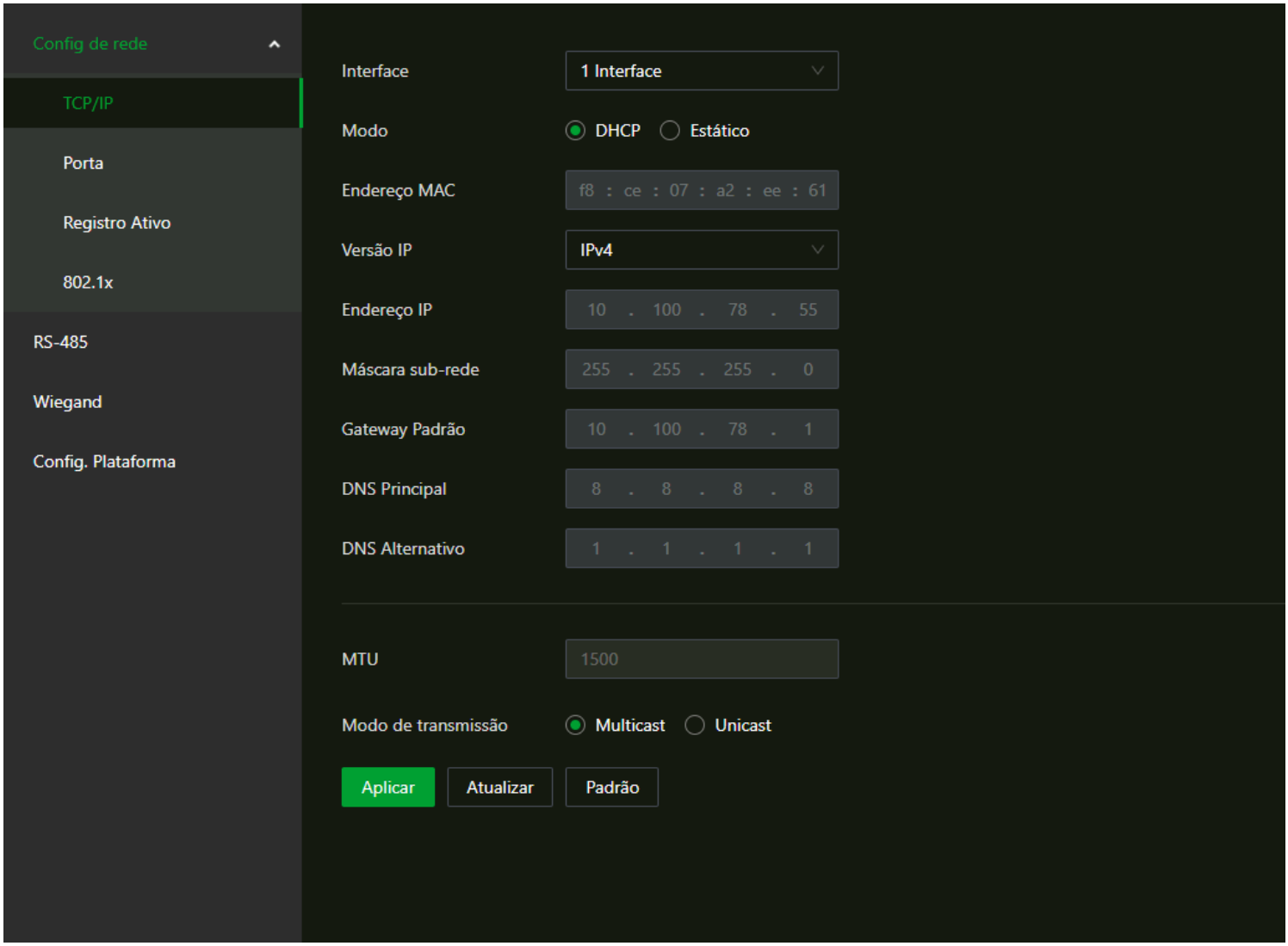
# REDE

Nesse menu é realizado as configurações de rede TCP/IP, plataforma de eventos, RS-485 e Wiegand.

## Config de rede

Essa opção permite configurar a interface de rede do dispositivo, garantindo a comunicação com outros dispositivos.

# TCP/IP




- **Modo:**
  - **Estático: Permite definir manualmente os parâmetros de rede.**
    - **Endereço de IP:** Define o endereço de IP do dispositivo. É definido por 4 números, de 0 a 255, separados por pontos.
    - **Máscara de sub-rede:** Define a máscara de sub-rede do dispositivo. É definido por 4 números, de 0 a 255, separados por pontos.
    - **Gateway padrão:** Define o gateway padrão do dispositivo. É definido por 4 números, de 0 a 255, separados por pontos.

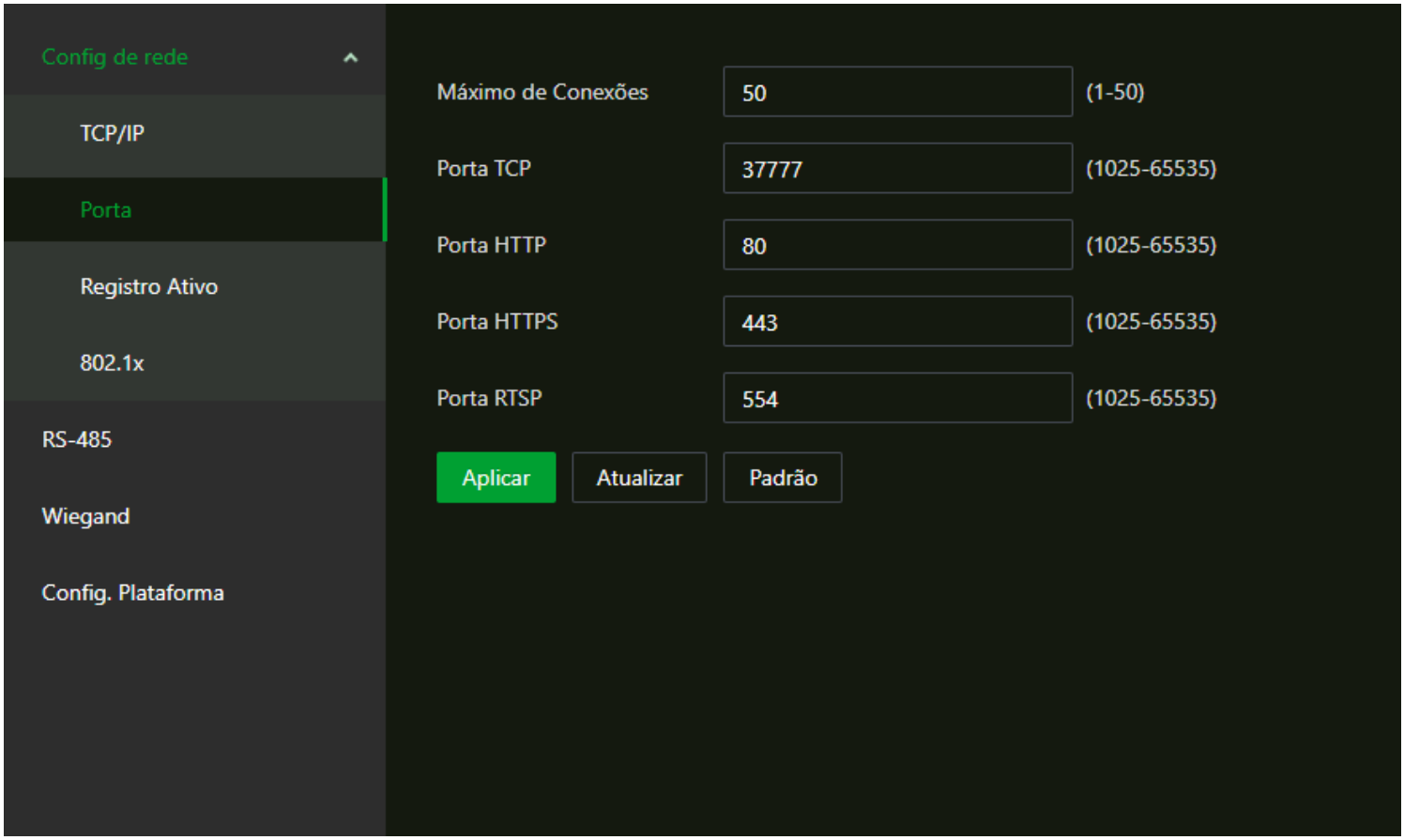
      Obs.: Endereço de IP e gateway padrão precisam estar na mesma faixa de valores.
  - **DHCP:** Define automaticamente os parâmetros de rede conforme disponível.
    - Depois que o DHCP está ativo, endereço de IP, máscara de sub-rede e gateway padrão não podem ser configurados manualmente

- Se o DHCP foi efetivo, endereço de IP, máscara de sub-rede e gateway padrão serão mostrados automaticamente; se não foi efetivo, endereço de IP, máscara de sub-rede e gateway padrão serão "0.0.0.0".
- Se quiser visualizar o endereço de IP padrão quando o DHCP foi efetivamente ativado, é necessário desabilitar o DHCP.

- **Endereço MAC:** O endereço MAC do dispositivo é mostrado.
- **Versão IP:** Define a versão do protocolo a ser usada.
- **Servidor DNS principal:** Define o endereço do DNS preferencial.
- **Servidor DNS alternativo:** Define o endereço do DNS alternativo.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

## Portas

Define o número máximo de conexões com clientes aos quais o controlador de acesso pode ser conectado e os números de porta.

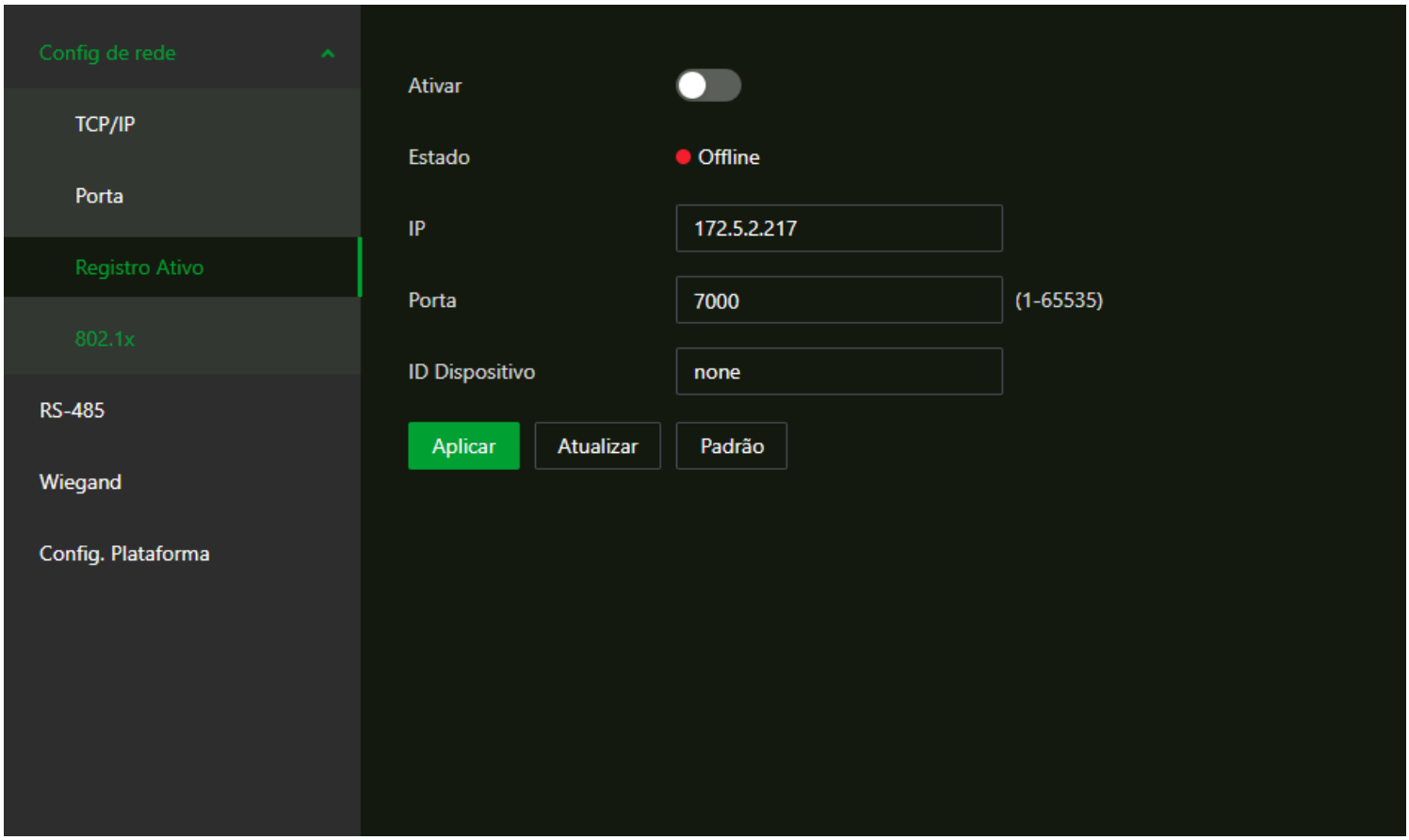



- **Máx de número de conexões:** Você pode definir o número máximo de conexões com clientes aos quais o controlador de acesso pode ser conectado.
- **Porta TCP:** Define a porta TCP. O valor padrão é 37777.
- **Porta HTTP:** Define a porta HTTP. O valor padrão é 80. Se outro valor for usado como número de porta, será necessário adicionar esse valor após o endereço de IP ao fazer o login por meio de navegadores.
- **Porta HTTPS:** Define a porta HTTPS. O valor padrão é 443.

- **Porta RTSP:** Define a porta RTSP. O valor padrão é 554.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

## Registro Ativo

Quando conectado à uma rede externa, o controlador de acesso informar seu endereço de IP ao servidor que foi designado pelo usuário para que os clientes possam ter acesso ao controlador de acesso.

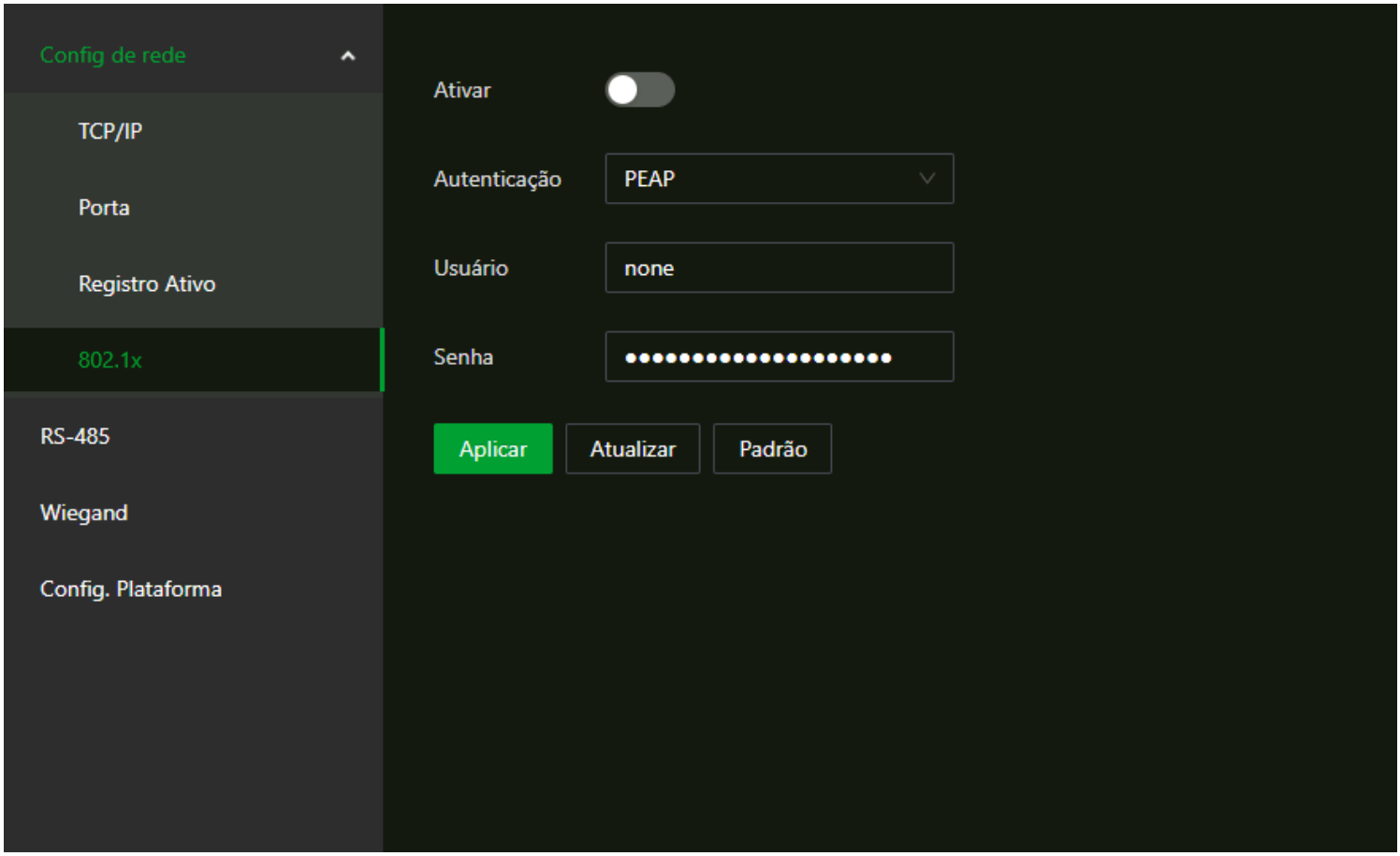



- **Ativar:** Habilita conexões com rede externa.
- **Estado:** Exibe informação do status de conexão.
- **IP:** Endereço de IP do servidor ou nome de domínio do servidor.
- **Porta:** Porta do servidor usada para registro automático.
- **ID do dispositivo:** Identificador do controlador de acesso atribuído pelo servidor
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

## 802.1x

Ativa ou desativa o padrão de segurança de rede 802.1x.

O 802.1X oferece autenticação baseada em portas, o que significa que antes de um dispositivo ser autorizado a se conectar à rede, ele deve passar por um processo de autenticação. Isso é especialmente útil em ambientes onde a segurança da rede é crítica, como empresas, universidades e organizações governamentais..




Em Autenticação há duas opções de protocolo, PEAP e TSL.

**PEAP**, sigla para "Protected Extensible Authentication Protocol", é um protocolo de autenticação de rede que proporciona um método seguro para autenticar dispositivos e usuários em redes sem fio (Wi-Fi). Ele é projetado para proteger a troca de credenciais durante o processo de autenticação.

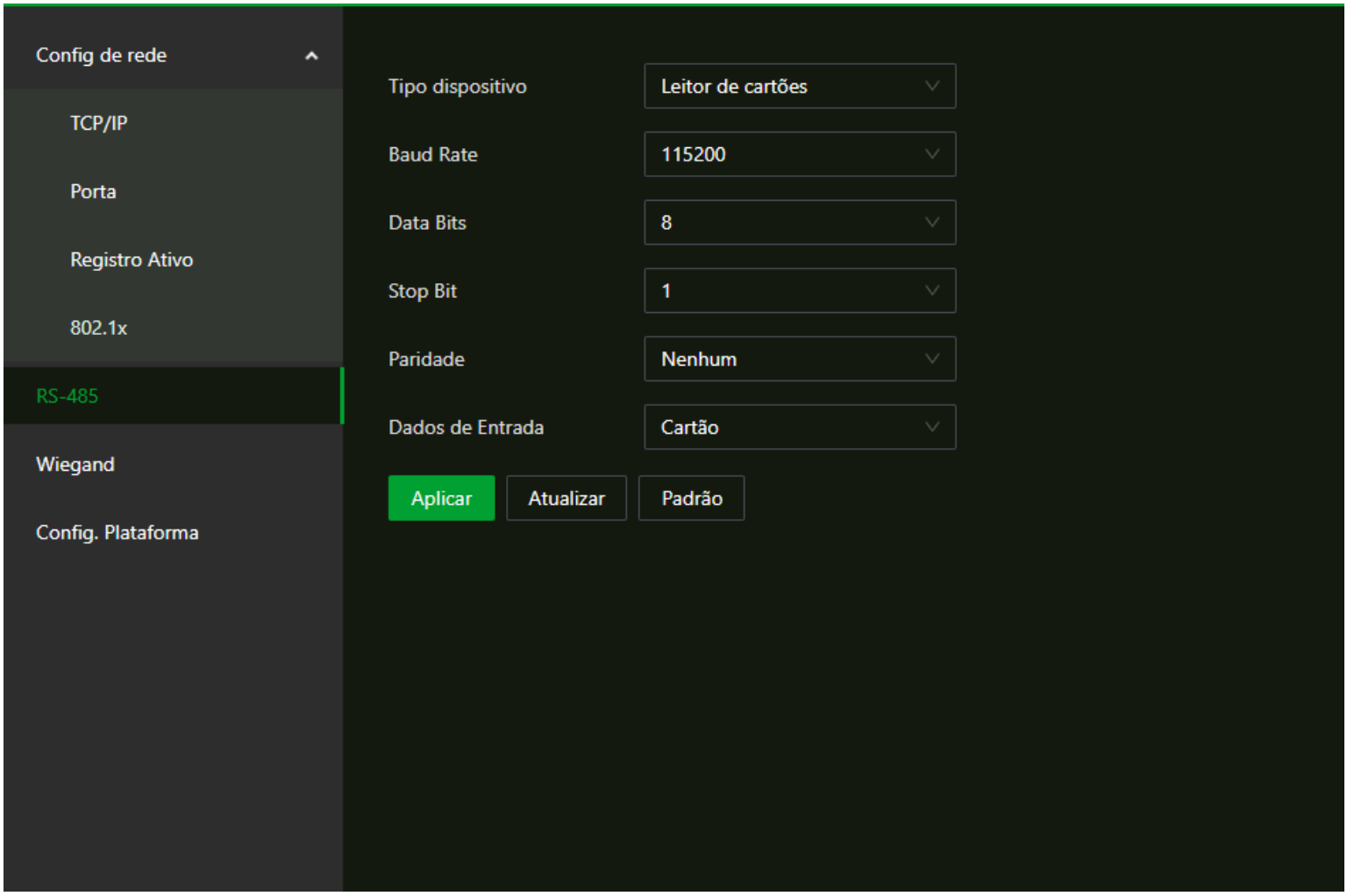
**TLS**, sigla para "Transport Layer Security", é um protocolo de segurança que oferece comunicações seguras através da internet. Ele é uma evolução do protocolo SSL (Secure Sockets Layer) e é projetado para garantir a privacidade e integridade dos dados transmitidos entre um cliente (como um navegador web) e um servidor.

- **Usuário:** Usuário definido no servidor Radius.
- **Senha:** Senha definido no servidor Radius.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

# RS-485

Esse menu permite que seja configurado os parâmetros RS-485 caso esteja conectando um dispositivo externo à porta RS-485.

**Obs.:** O dispositivo possui uma única porta para comunicação RS-485 e Wiegand, sendo possível definir o barramento de comunicação por meio de uma chave seletora.



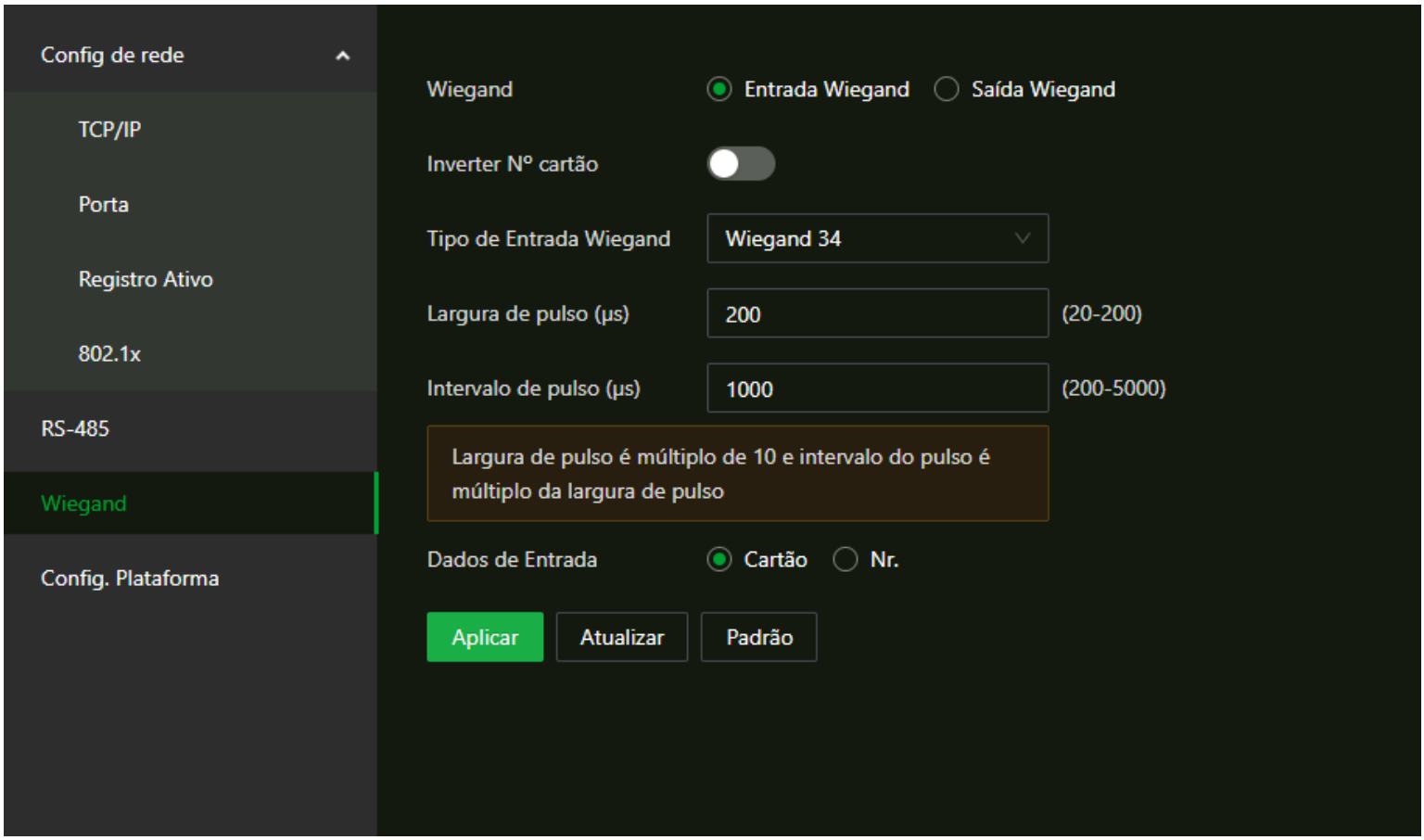

- **Tipo dispositivo:**
  - **Controladora:** O dispositivo funciona como um leitor de cartão e envia os dados para um controlador de acesso externo para gerenciamento de entrada.
  - Leitor de cartão: O dispositivo atua como um controlador de acesso e se conecta a um leitor de cartão externo.
  - **Leitor (OSDP):** O dispositivo se conecta a um leitor de cartão utilizando o protocolo OSDP.
  - **Módulo de Segurança:** Ao ativar o módulo de segurança, o botão de saída da porta, a fechadura, o sensor de porta e o acionamento por alarme de incêndio ficarão inoperantes.
  - **Catraca:** Implementação futura.
- **Baud Rate:** Ajuste da taxa de transmissão entre 9600 e 115200.
- **Data Bits:** Define a quantidade de bits usados para transmitir a informação real na comunicação serial.
- **Stop Bit:** É um bit enviado após os dados e os bits de paridade (se houver) para indicar o fim de uma transmissão de dados.
- **Dados de Entrada/Tipo da saída:** O dispositivo passa a transmitir o ID do usuário ou o número do cartão por meio do leitor auxiliar ou de outro controlador.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.

- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

# Wiegand

Esse menu permite configurar e ajustar os parâmetros dos dispositivos conectados via protocolo Wiegand.

**Obs.:** O dispositivo possui uma única porta para comunicação RS-485 e Wiegand, sendo possível definir o barramento de comunicação por meio de uma chave seletora.




- **Wiegand:**
  - **Entrada Wiegand:** Selecione essa opção quando conectar um leitor auxiliar no dispositivo.
  - **Saída Wiegand:** Selecione essa opção quando o controlador de acesso atuar como leitor de cartão e precisar ser conectado a outro controlador de acesso.
- **Inverter Nº cartão:** Ative a inversão do número do cartão ao conectar o dispositivo via Wiegand, se o número lido estiver invertido.
- **Tipo de Entrada Wiegand:** Selecione um formato Wiegand para leitura dos números do cartão ou ID entre 26 a 66 bits.
- **Largura de pulso:** Usado para definir a largura de pulso do protocolo Wiegand.
- **Intervalo de pulso:** Usado para definir o intervalo de pulso do protocolo Wiegand
- **Dados de Entrada:** O dispositivo passa a transmitir o ID do usuário ou o número do cartão.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.

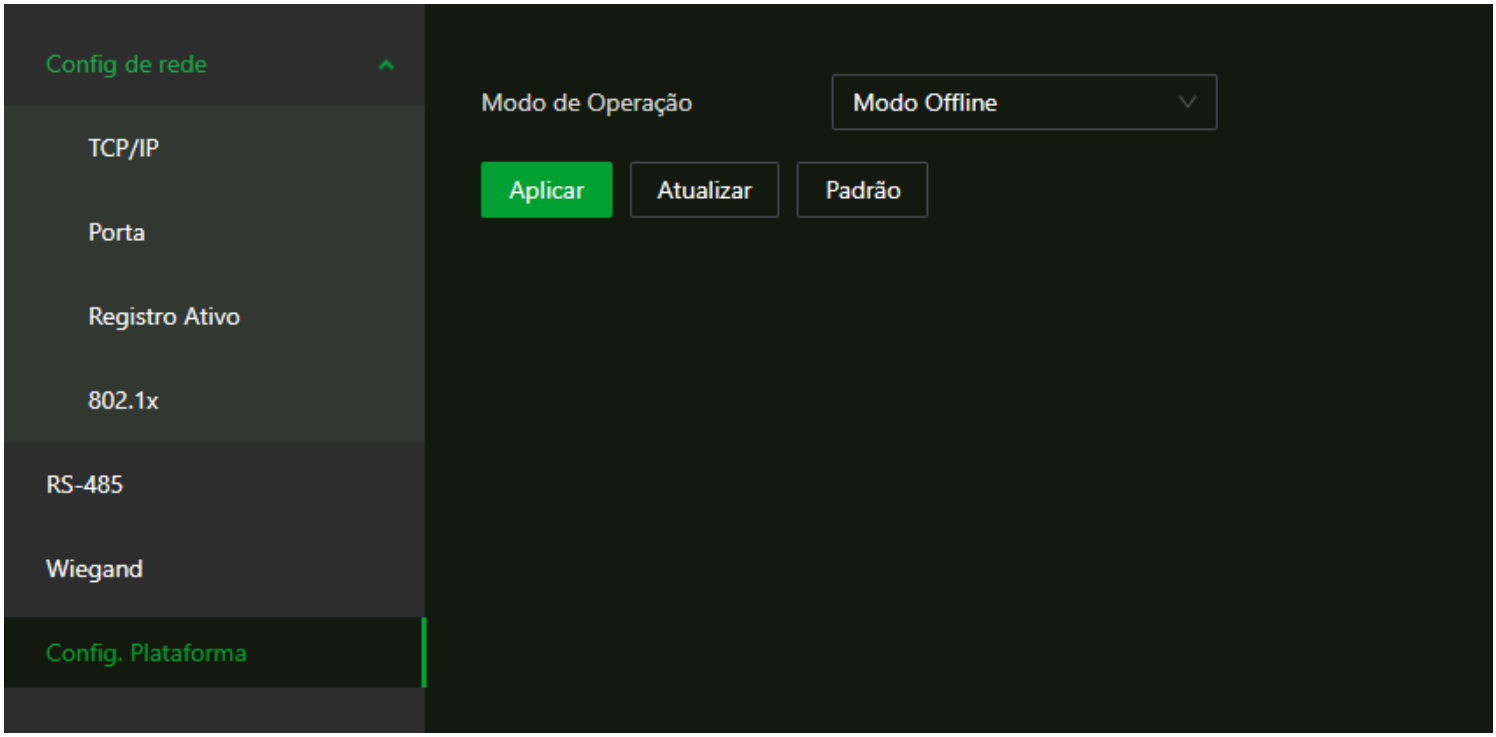
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

# Config. Plataforma

O controlador de acesso permite configurar 3 modos de operação do dispositivo, modo Standalone, modo post eventos e modo online.

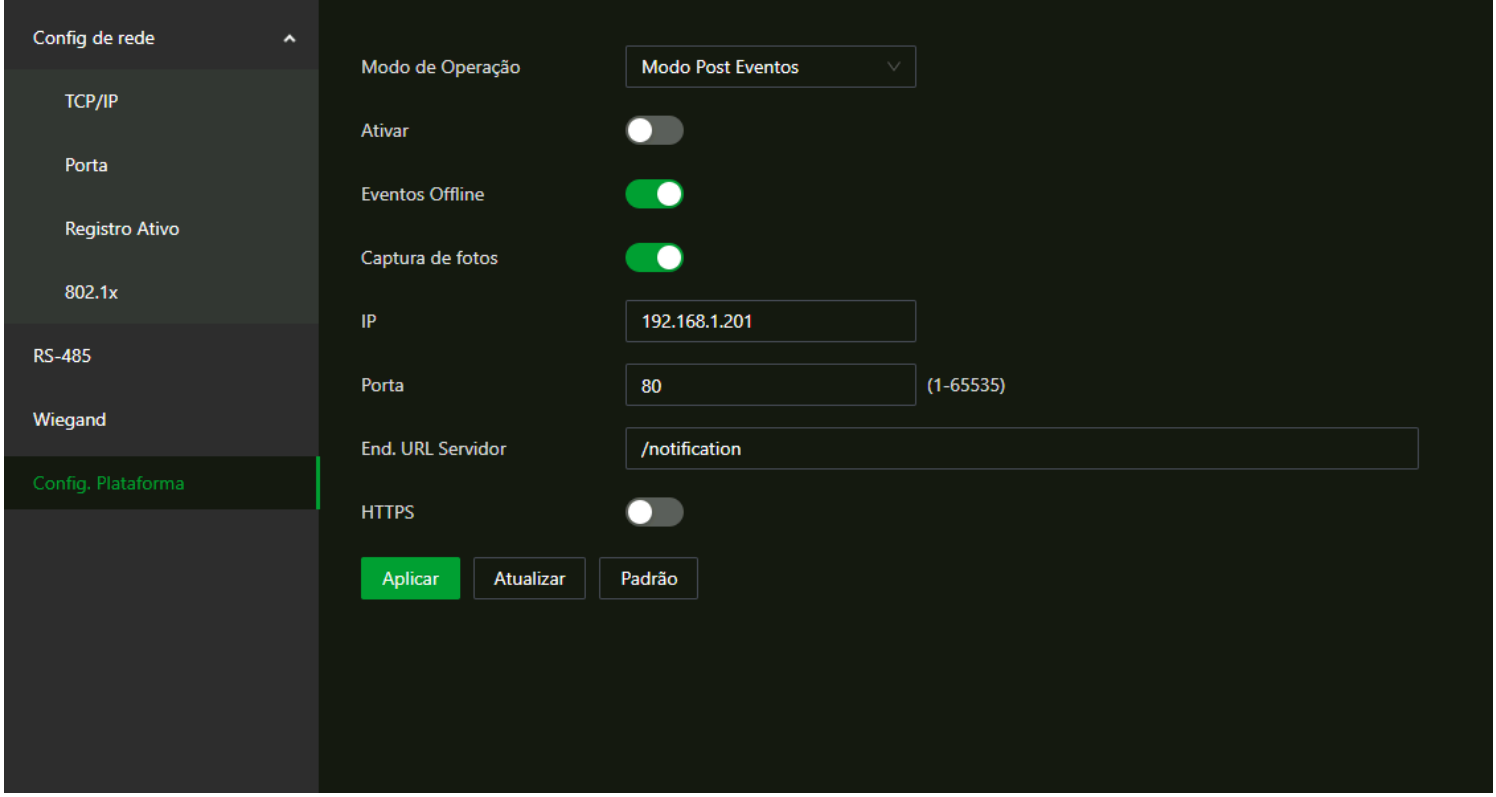
## Modo Offline

Quando o dispositivo estiver offline, todas as tentativas de acesso serão analisadas com base nos usuários cadastrados. Os eventos gerados serão armazenados na memória do dispositivo. Esse modo vem ativado por padrão.




## Modo POST Eventos

Por meio do servidor de envio de eventos, no modo POST eventos, é possível realizar a configuração de um endereço de IP ou host. Desta forma, os eventos são reportados do dispositivo ao servidor definido.



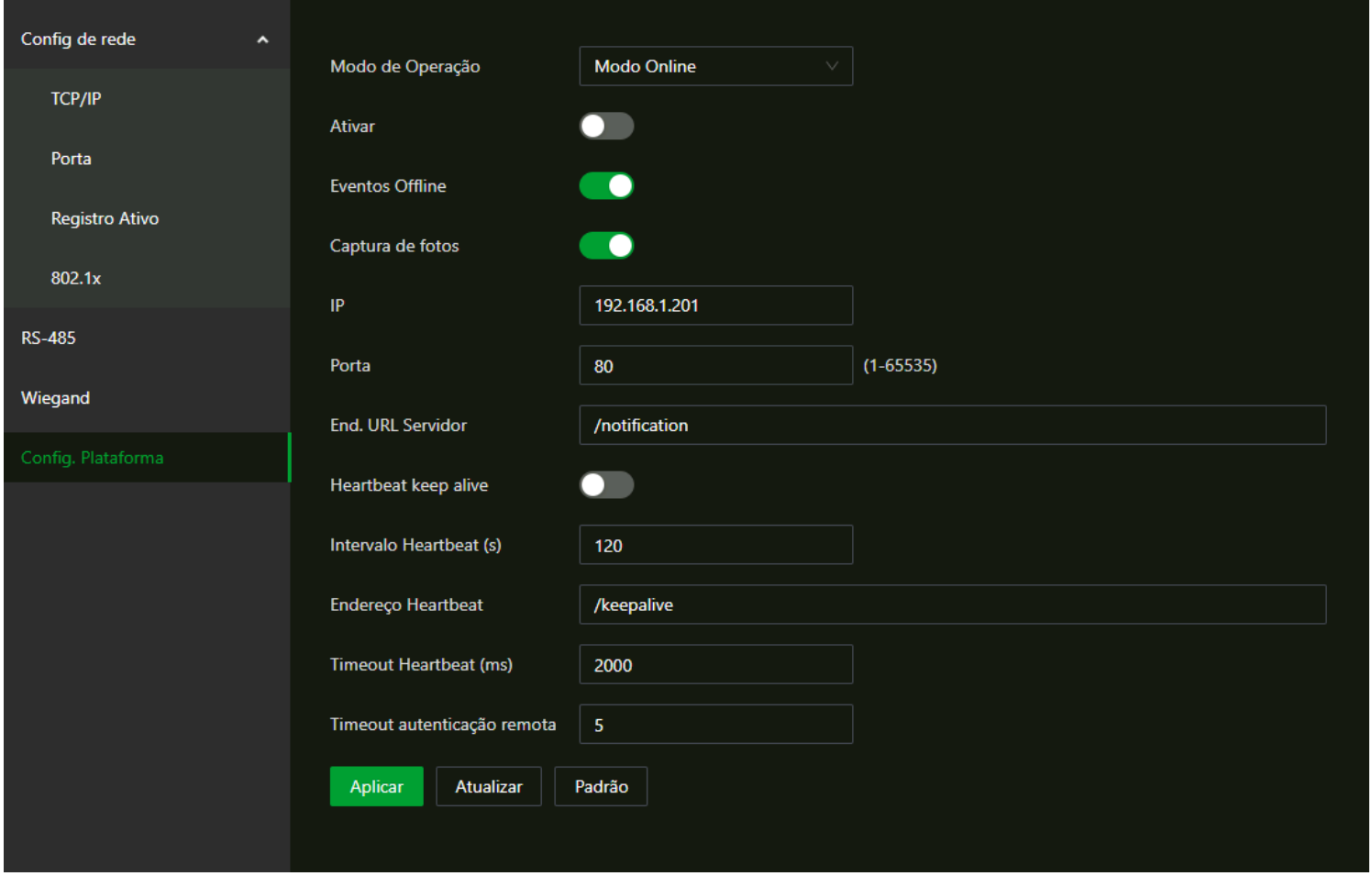

- **Ativar:** Ativa o modo de operação definido. Necessário ser selecionado na opção "Modo de operação".
- **Eventos Offline:** Habilita ou desabilita o envio de eventos ocorridos de forma offline para o servidor após a perda de conexão. Por padrão, essa função é ativada.
- **Captura de fotos:** Marque para que o evento de acesso seja acompanhado da foto do acesso.
- **IP:** Endereço IP do servidor.
- **Porta:** Porta do servidor que será utilizada.
- **End. URL Servidor:** Caminho dentro do servidor para onde serão enviados os eventos.
- **HTTPS:** Habilita o envio dos eventos em HTTPS quando selecionado.

  Para mais informações e exemplos, verifique a **documentação da API (https://intelbras-caco-api.intelbras.com.br/obtendo_eventos/servidor_de_envio_de_eventos)**

- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

## Modo Online

Quando o dispositivo estiver no estado online, todos que tentarem acessá-lo terão o evento postado, e o dispositivo aguardará uma resposta de autorização do servidor contendo três campos: id, auth e message.




- **Ativar:** Ativa o modo de operação definido. Necessário ser selecionado na opção "Modo de operação".
- **Transmissão continuada:** Habilita ou desabilita o envio de eventos ocorridos de forma offline para o servidor após a perda de conexão. Por padrão, essa função é ativada.
- **Captura de fotos:** Marque para que o evento de acesso seja acompanhado da foto do acesso.
- **IP:** Endereço IP do servidor.
- **Porta:** Porta do servidor que será utilizada.
- **End. URL Servidor:** Caminho dentro do servidor para onde serão enviados os eventos.
- **Heartbeat keep alive:** Quando habilitado, o dispositivo realizará tentativas de requisição GET no endereço especificado em “End. URL Servidor”.
- **Intervalo Heartbeat (s):** TTempo, em segundos, para a repetição do processo "Heartbeat Keep Alive" pelo dispositivo.
- **Endereço Heartbeat:** Local onde o dispositivo fará a requisição GET.
- **Timeout Heartbeat (ms):** Tempo limite para receber uma resposta do servidor para as requisições GET.
- **Timeout autenticação remota:** Tempo máximo que o servidor tem para responder a uma verificação de credencial. Caso ultrapasse esse tempo, o dispositivo tomará uma decisão offline de acesso, baseado nos usuários cadastrados em seu banco de dados.

  Para mais informações e exemplos, verifique a **documentação da API: (https://intelbras-caco-api.intelbras.com.br/modo_online)**

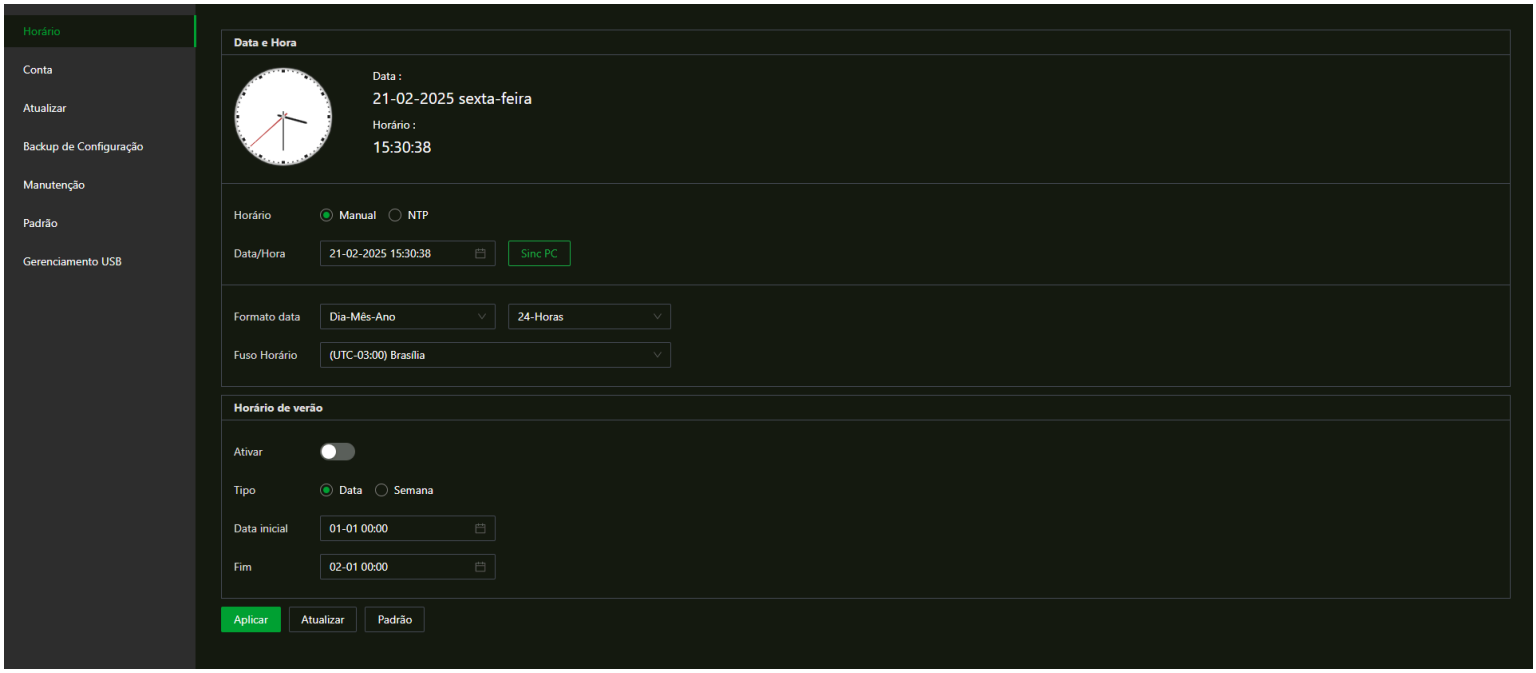
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

# SISTEMA

Nesse menu, é possível configurar a hora do sistema, alterar a senha do administrador, redefinir a senha, realizar backup do dispositivo, restaurar as configurações de fábrica, entre outras opções.

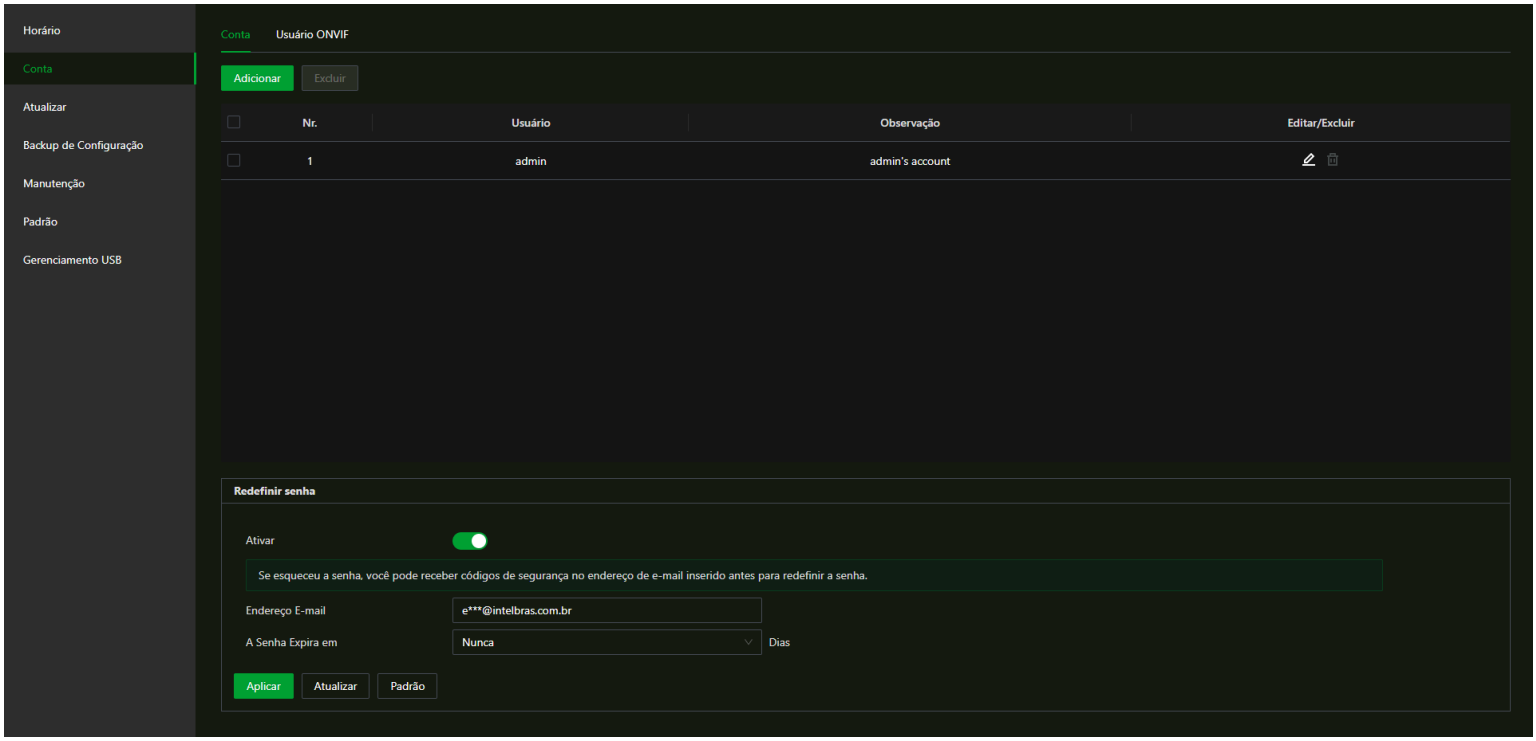
## Horário

Nessa seção é possível confira a data, hora, fuso horário, NTP e sincronização como PC.




## Conta

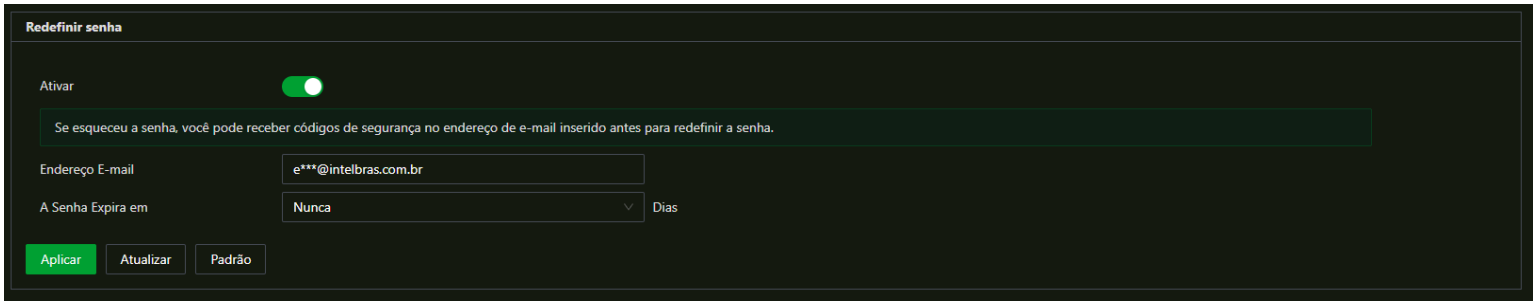
Permite cadastrar novos usuários administradores, editar o usuário admin e conceder acesso à interface web e local do dispositivo.



- **Adicionar:** Adiciona um novo usuário.
- **Editar:** Selecionando o ícone é possível editar os dados do usuário.
- **Excluir:** Selecionando o ícone é possível excluir o usuário.

# Reset de senha

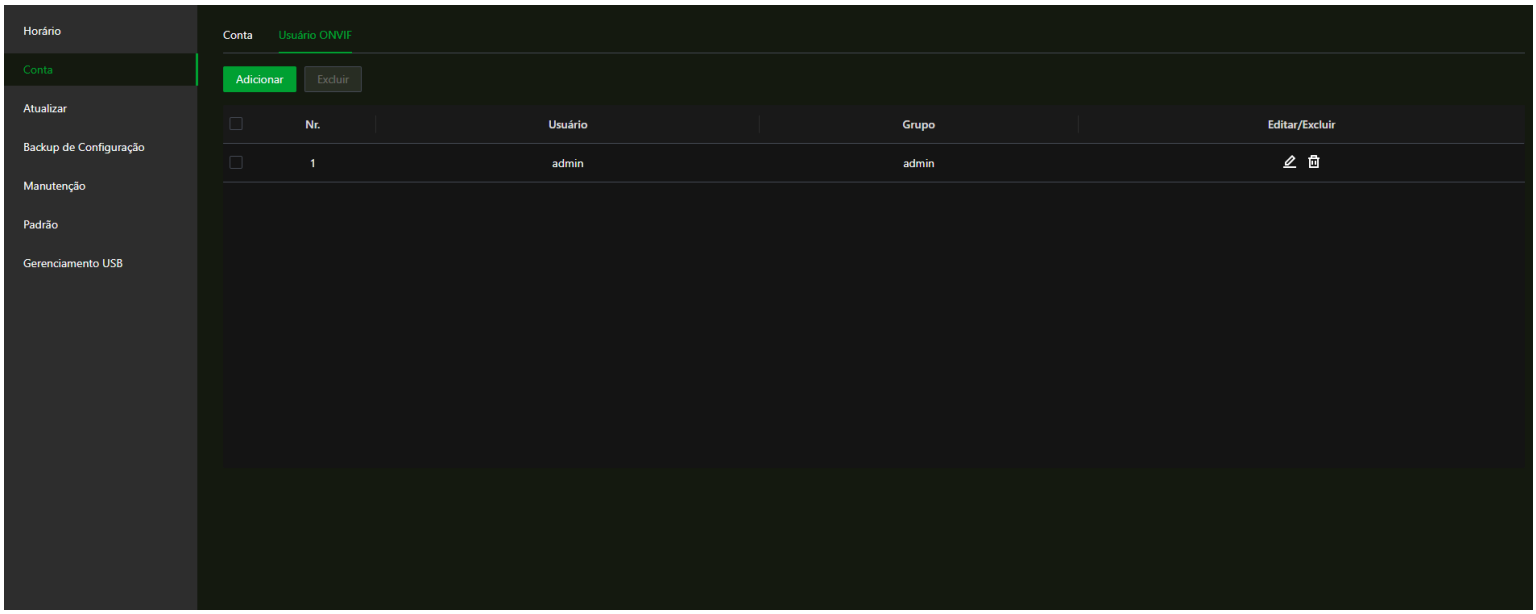
Também é possível habilitar ou desabilitar a redefinição de senha, alterar o e-mail cadastrado e definir o tempo de validade da senha do administrador.




- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

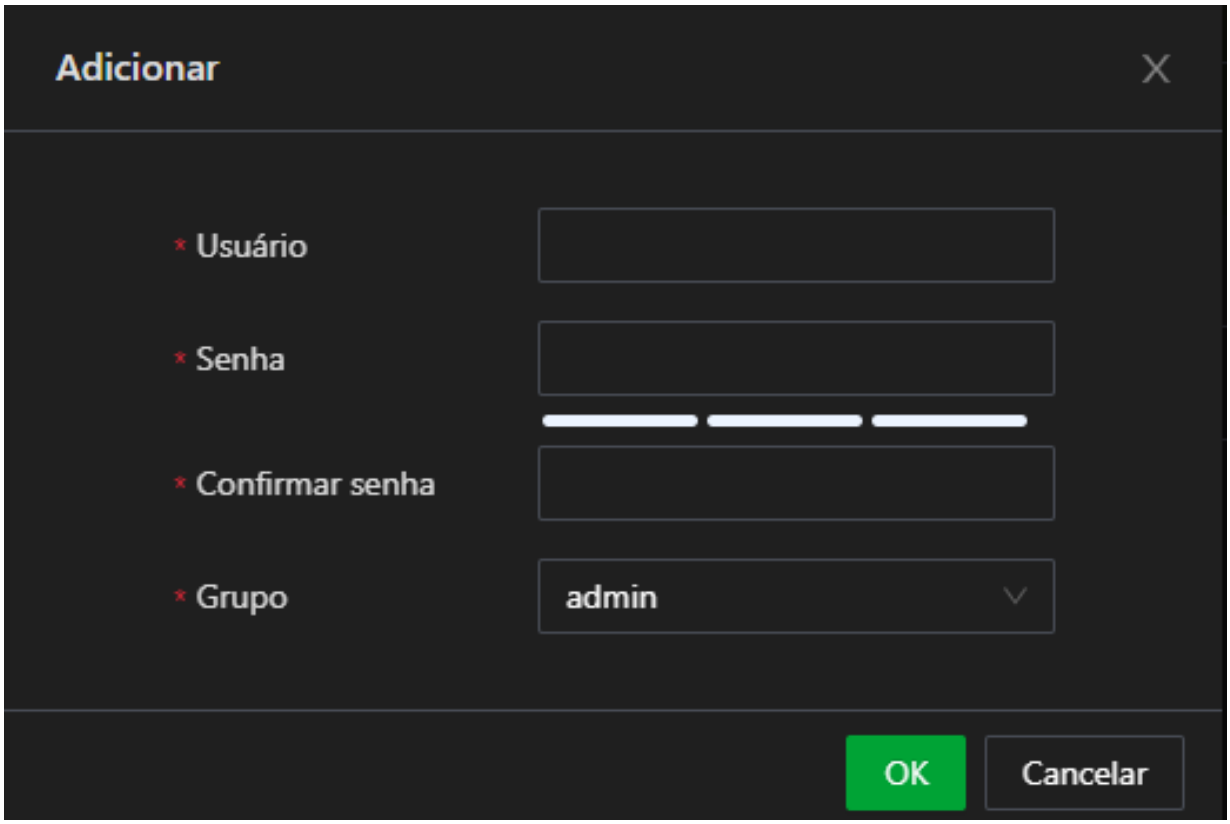
# Usuário Onvif

Open Network Video Interface Forum (ONVIF), ou Forum de Interface de Vídeo de Rede Aberta, é um fórum global e aberto da industria com o objetivo de facilitar o desenvolvimento e uso de um padrão aberto global para a interface de produtos físicos de segurança baseados em IP. Quando o ONVIF é usado, administrador, operador e usuário tem permissões diferentes do servidor ONVIF. Crie Usuários ONVIF conforme necessário.




- **Editar:** Selecionando o ícone é possível editar os dados do usuário.
- **Excluir:** Selecionando o ícone é possível excluir o usuário.

- **Adicionar:** Adiciona um novo usuário.

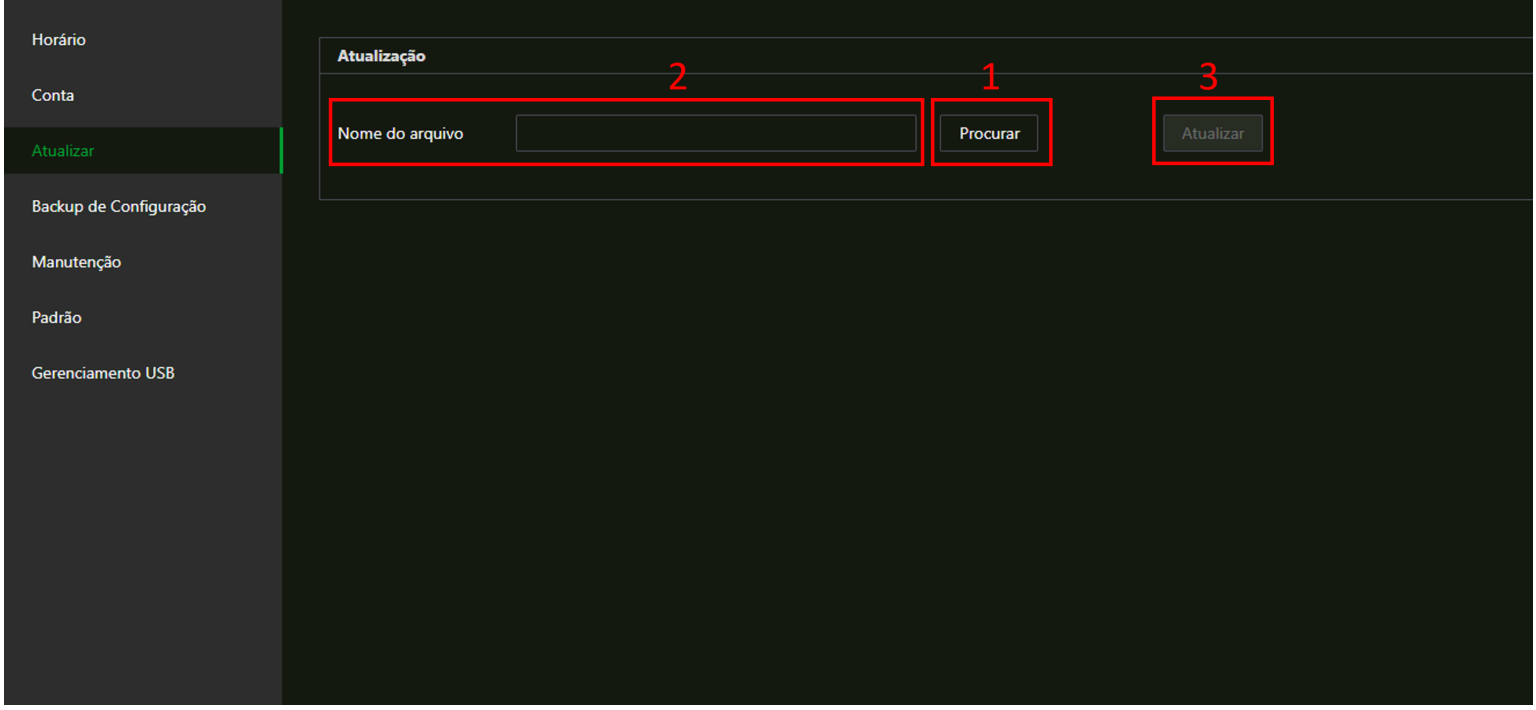



  - **Usuário:** Nome do usuário.
  - **Senha:** Senha definida para o usuário.
  - **Confirmar senha:** Senha digitada anteriormente.
  - **Grupo:** Existem três grupos de permissão, cada um representando um nível diferente de acesso.
    - **admin:** Pode visualizar e gerenciar outras contas de usuários no ONVIF.
    - **operador:** Não pode visualizar ou gerenciar outras contas de usuários no ONVIF.
    - **usuario:** Não pode visualizar ou gerenciar outras contas de usuários nem acessar os logs do sistema no ONVIF.
    - **Ok:** Salva as alterações feitas.
    - **Cancelar:** Cancela as configurações realizadas.

# ATUALIZAR

**Importante:** Utilize apenas arquivos fornecidos pela Intelbras. Mantenha o dispositivo energizado durante todo o processo de atualização.

A atualização inicia pelo botão Procurar para indicar a localização do arquivo. Utilize arquivos locais, arquivos em rede podem causar falha no processo de atualização.

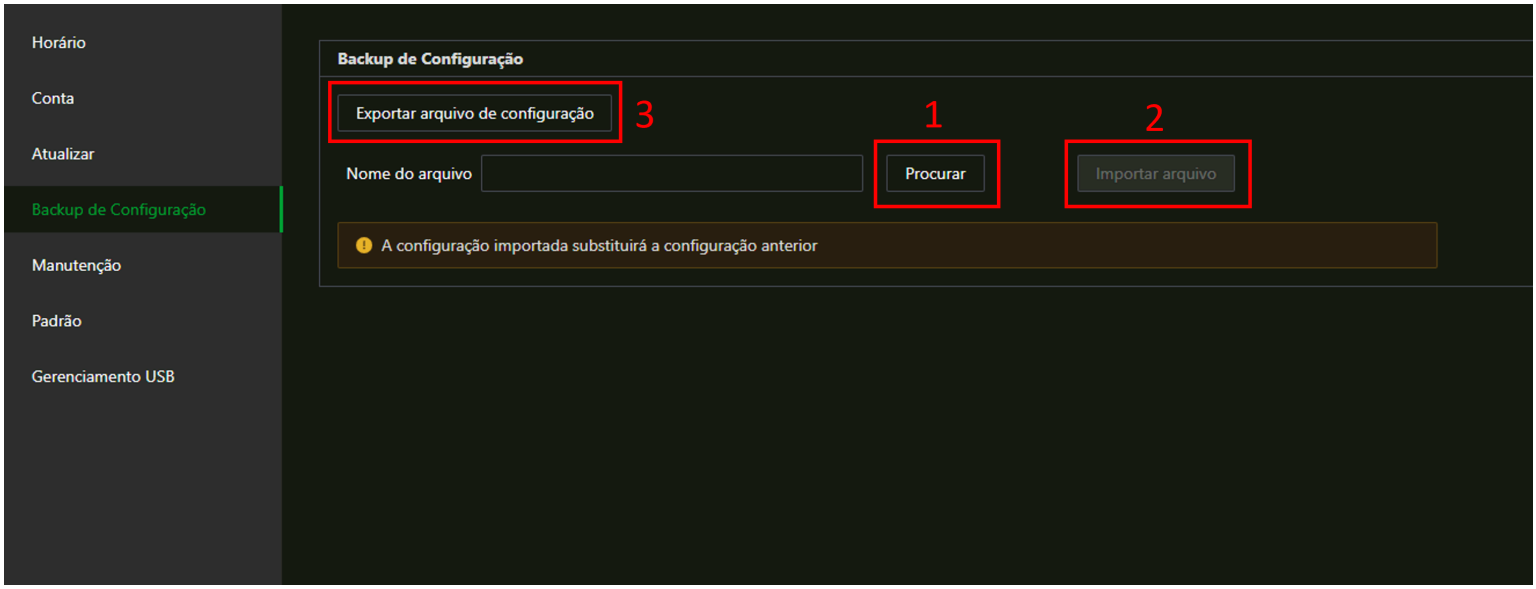



- **Procurar 1:** Busca no computador o arquivo de firmware para a atualização.
- **Nome do arquivo 2:** Mostra o firmware que será usado para atualizar o dispositivo.
- **Atualizar 3:** Executa a atualização usando o firmware selecionado.

# Backup de Configuração

Permite ao usuário administrador salvar uma cópia das configurações do dispositivo ou restaurar uma configuração previamente criada. Pode ser utilizado quando vários dispositivos necessitam utilizar a mesma configuração.

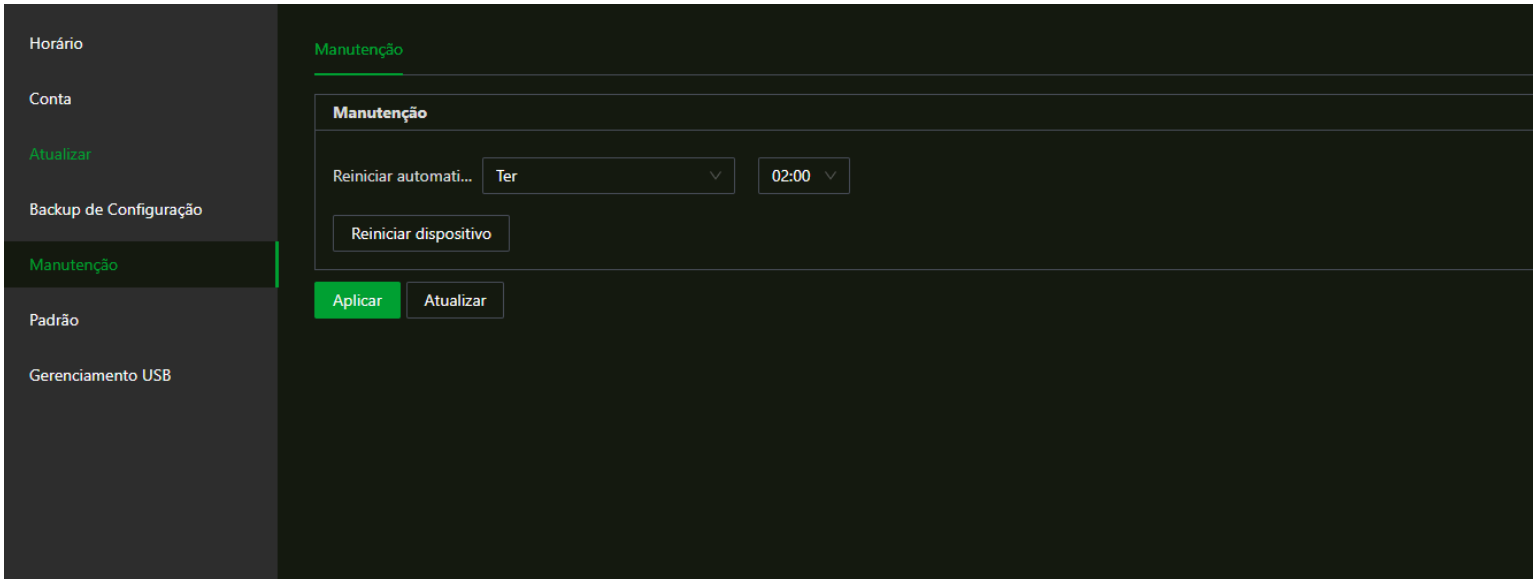
Para salvar as configurações do seu dispositivo pressione Exportar configurações e um arquivo será salvo no seu dispositivo. A importação pode ser realizada iniciando por Procurar o arquivo desejado e então Importar configurações.




- **Procurar 1:** Acessa as pastas local para carregar o arquivo **.backup** do computador.
- **Importar configurações 2:** Importa para o dispositivo o arquivo **.backup** do computador selecionado.
- **Exportar configurações 3:** Exporta do dispositivo um arquivo **.backup** para o computador.

# Manutenção

Configurações para manutenção do dispositivo.



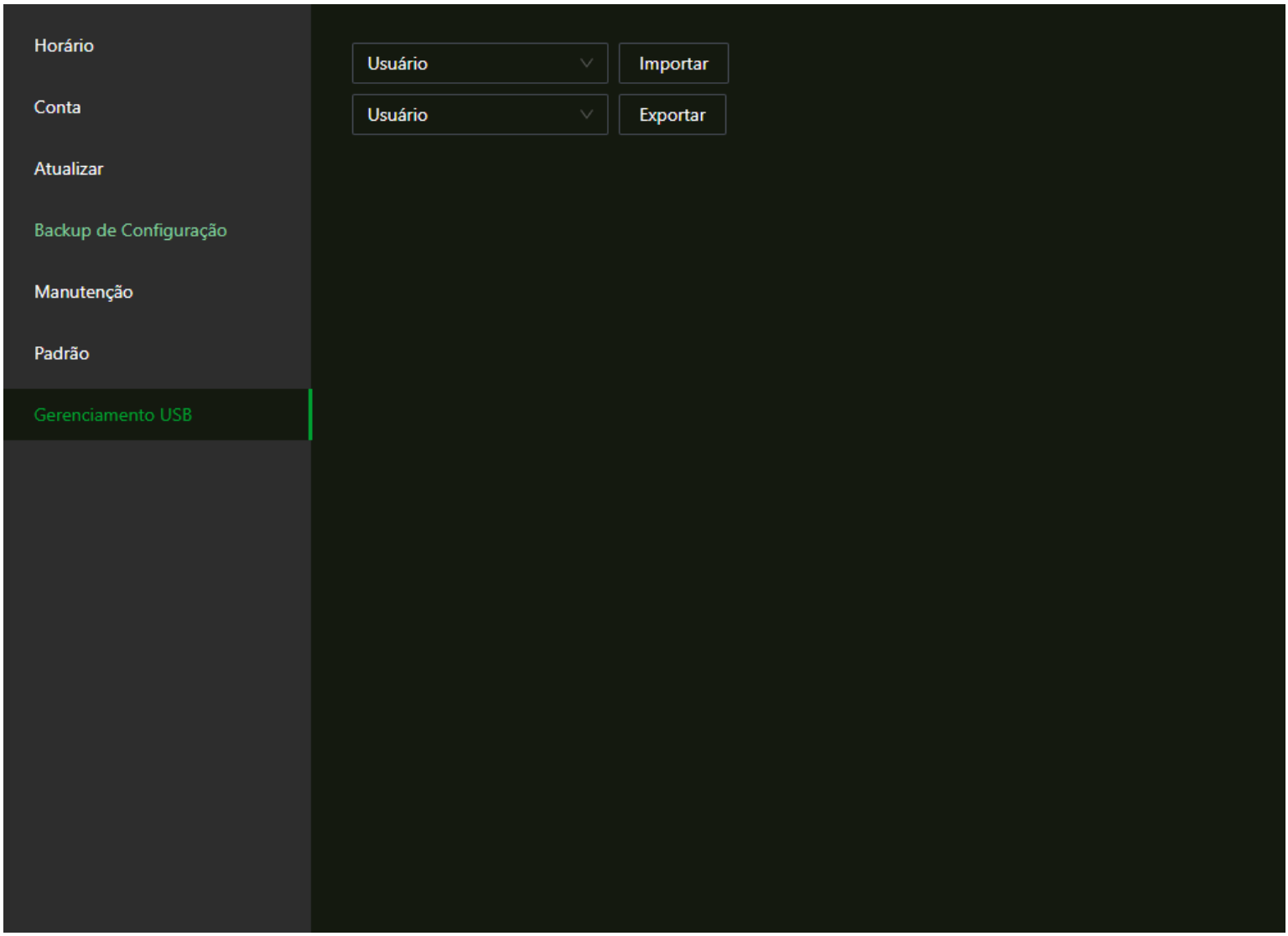

- **Reiniciar automaticamente:** Opção para agendar a data e hora que o dispositivo será reiniciado.
- **Reiniciar dispositivo:** O dispositivo é reiniciado imediatamente.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.

# Padrão

O padrão oferece a opção de dois modos distintos de restauração de fábrica: um que exclui os usuários e eventos, e outro que preserva todos os usuários e eventos..


# Gerenciamento USB

Esse menu permite ao administrador conectar um pendrive ao dispositivo e efetuar importação e exportação de dados diretamente pela pagina web.



Certifique-se de que um dispositivo USB esteja inserido no controlador de acesso antes de exportar dados ou atualizar o sistema.

Não remova o USB ou interrompa operações durante o processo para evitar falhas.

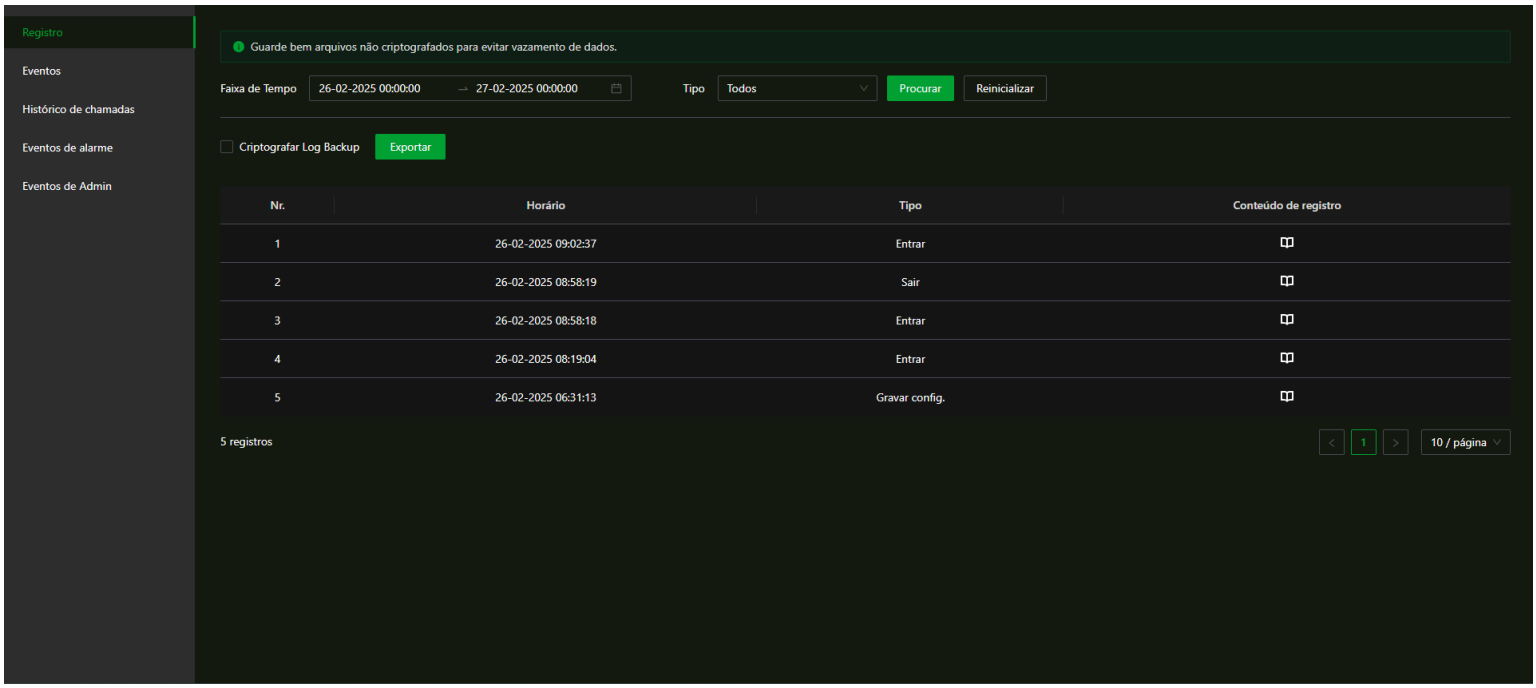
---

# LOGS

Nesse menu, é possível visualizar registros como logs do sistema, logs de administradores, históricos de chamadas SIP, eventos de acesso e eventos de alarmes.

## Registro

Nesse submenu, é possível visualizar os logs do sistema.



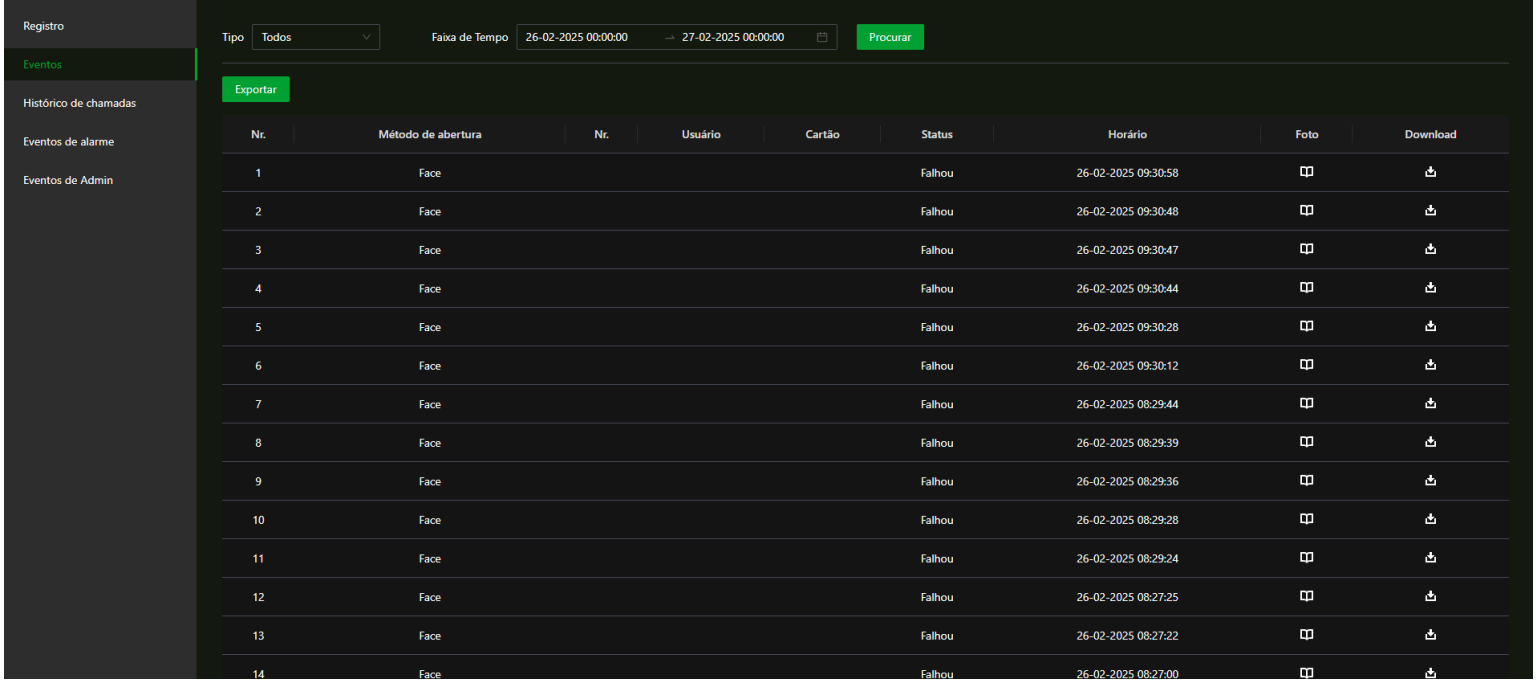

Selecione uma faixa de tempo inicial e final para buscar o evento desejado.

Para visualizar os detalhes de um evento clique no ícone 🕮

Clique em "Criptografar Backup de Log" e insira uma senha. O arquivo exportado só poderá ser aberto após a digitação da senha.

## Eventos

Nesse submenu, é possível visualizar os eventos de acesso realizados.




Selecione uma faixa de tempo inicial e final para buscar o evento desejado.

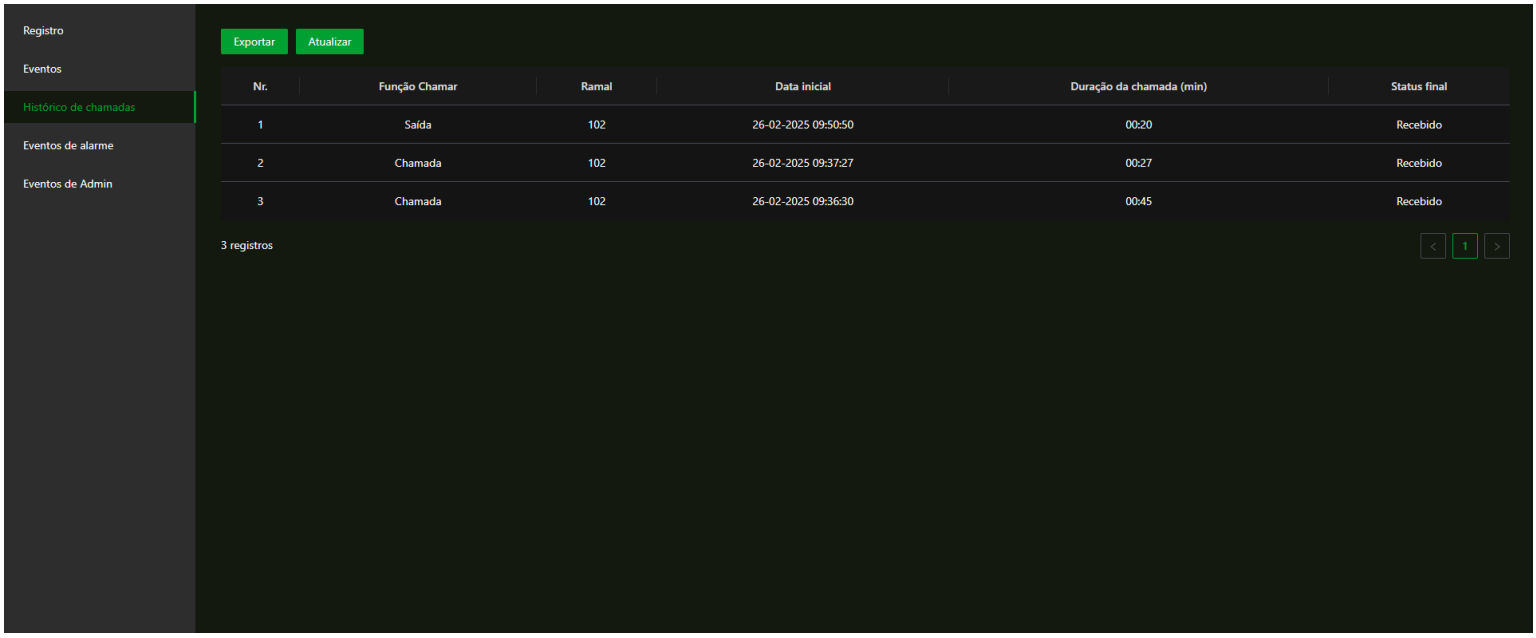
Para visualizar a foto de um evento clique no ícone 

Para realizar o download da foo gerada no evento clique no ícone 

É possível exportar os eventos no formato .xlsx.

# Histórico de chamadas

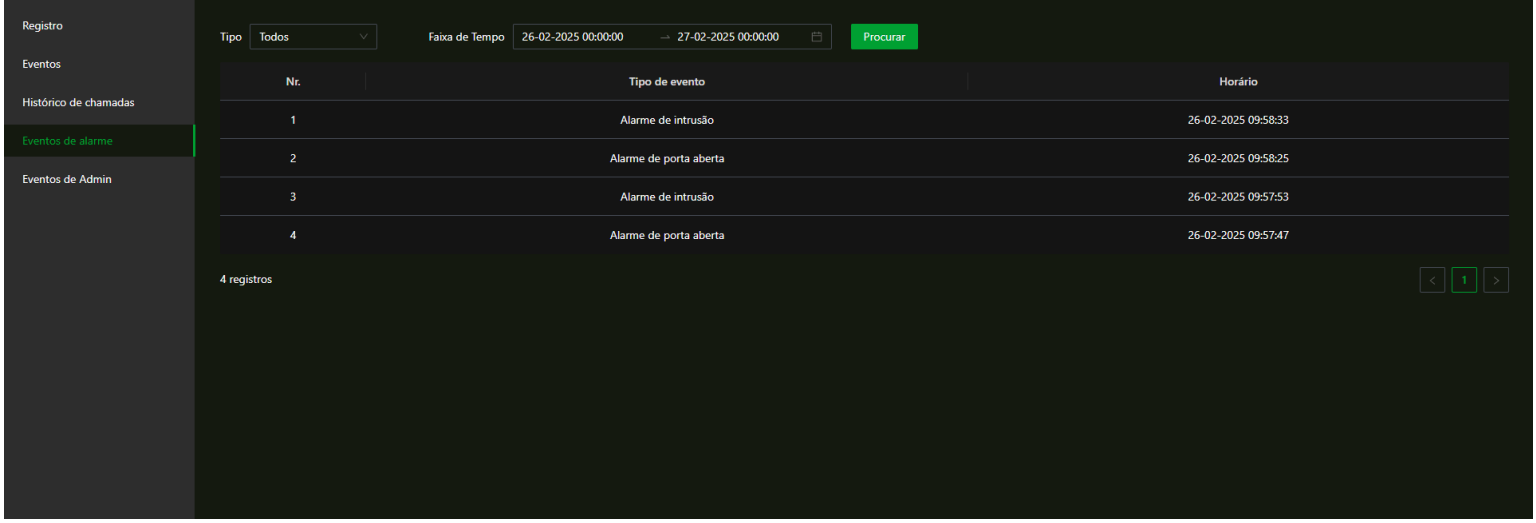
Nesse submenu, é possível visualizar as chamadas SIP e o tempo de duração.




É possível exportar os eventos no formato .xlsx.

# Eventos de Alarme

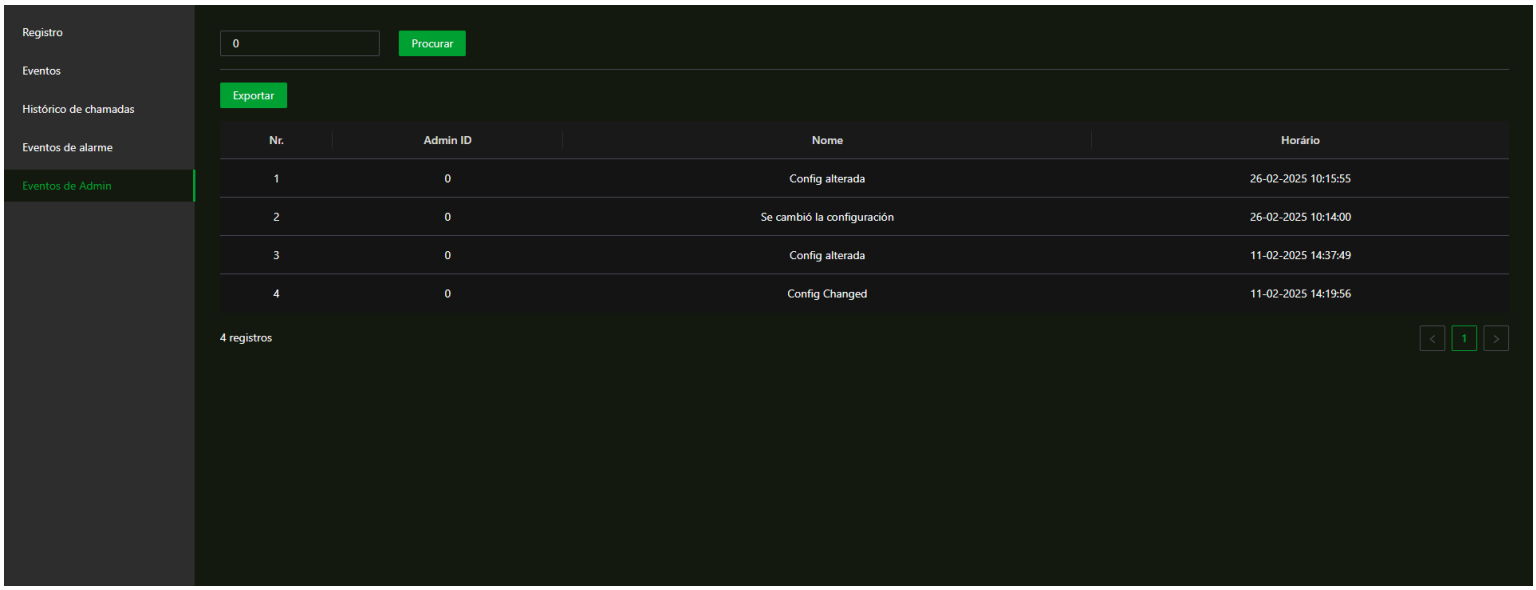
Nesse submenu, é possível visualizar os eventos de alarmes gerados.




Selecione uma faixa de tempo inicial e final para buscar o evento desejado.

## Eventos de Admin

Nesse submenu, é possível visualizar os logs de administrador usando o ID do administrador, ID do administrador é **0**.




É possível exportar os eventos no formato .xlsx.

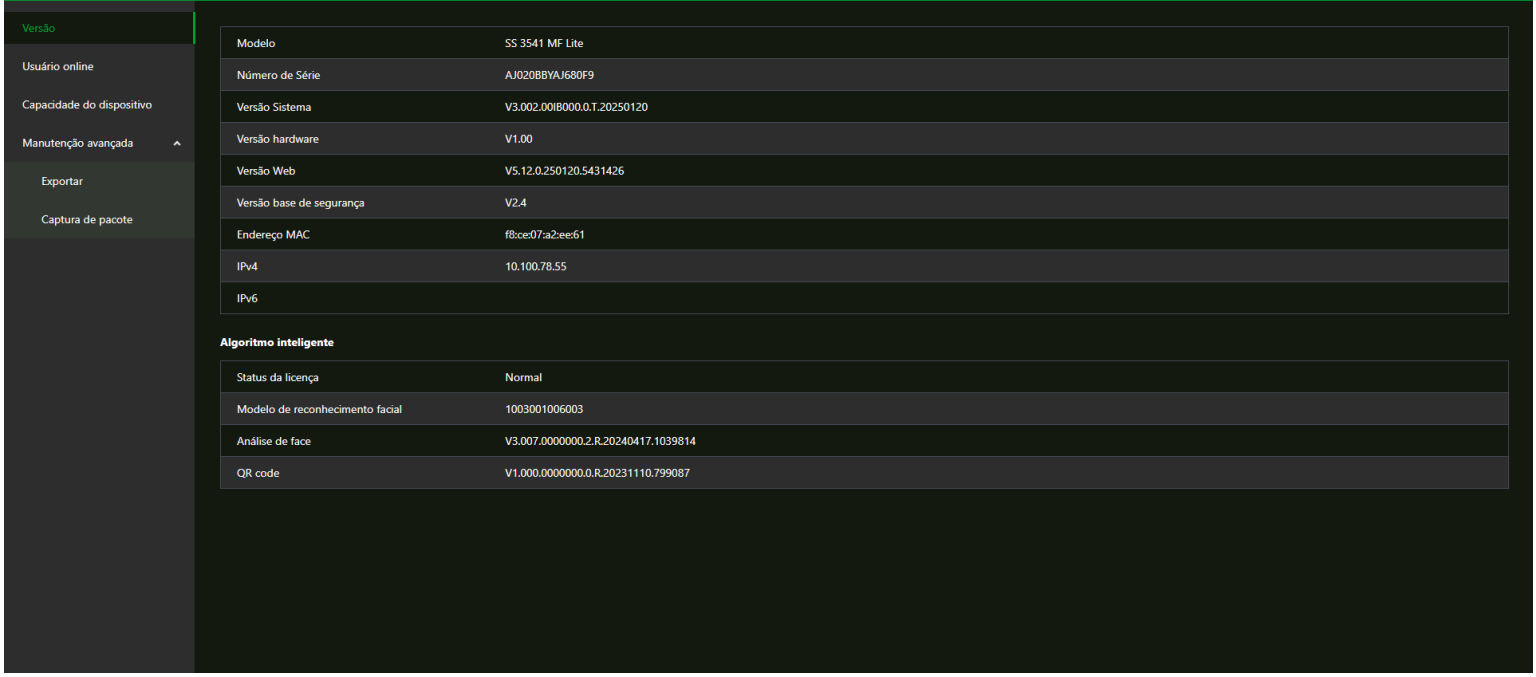
---

# INFO

Esse menu permite visualizar informações do dispositivo, quantidade de usuarios administradores conectados ao dispositivo, capacidade do dispositivo e manutenção avançada.

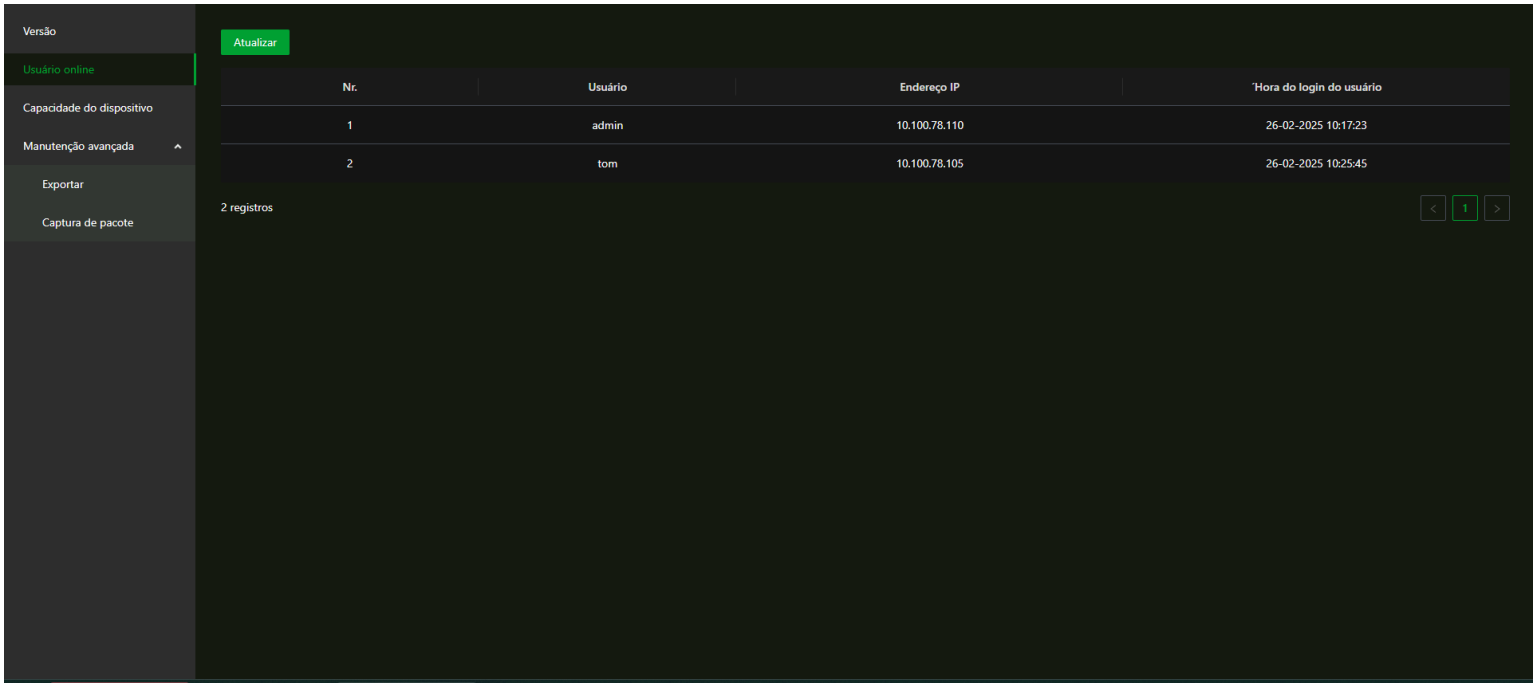
## Versão

Nesse submenu, é possível visualizar informações do sistema, como versão do firmware, versão da interface web, número de série, endereço MAC, entre outros.




# Usuários Online

Nesse submenu, é possível visualizar uma lista com a quantidade de usuários conectados, incluindo o nome do usuário, endereço IP e horário do login.




# Capacidade do Dispositivo

Nesse submenu, é possível visualizar a capacidade de armazenamento de cada tipo de dado, como usuários, credenciais, entre outros.


## Manutenção Avançada

Nesse submenu, é possível obter informações do dispositivo e capturar pacotes de dados, facilitando a análise e solução de problemas pela equipe de suporte Intelbras.

### Exportar

Essa função é dedicada ao time de suporte Intelbras.

### Captura de Pacote

Essa função é dedicada ao time de suporte Intelbras.

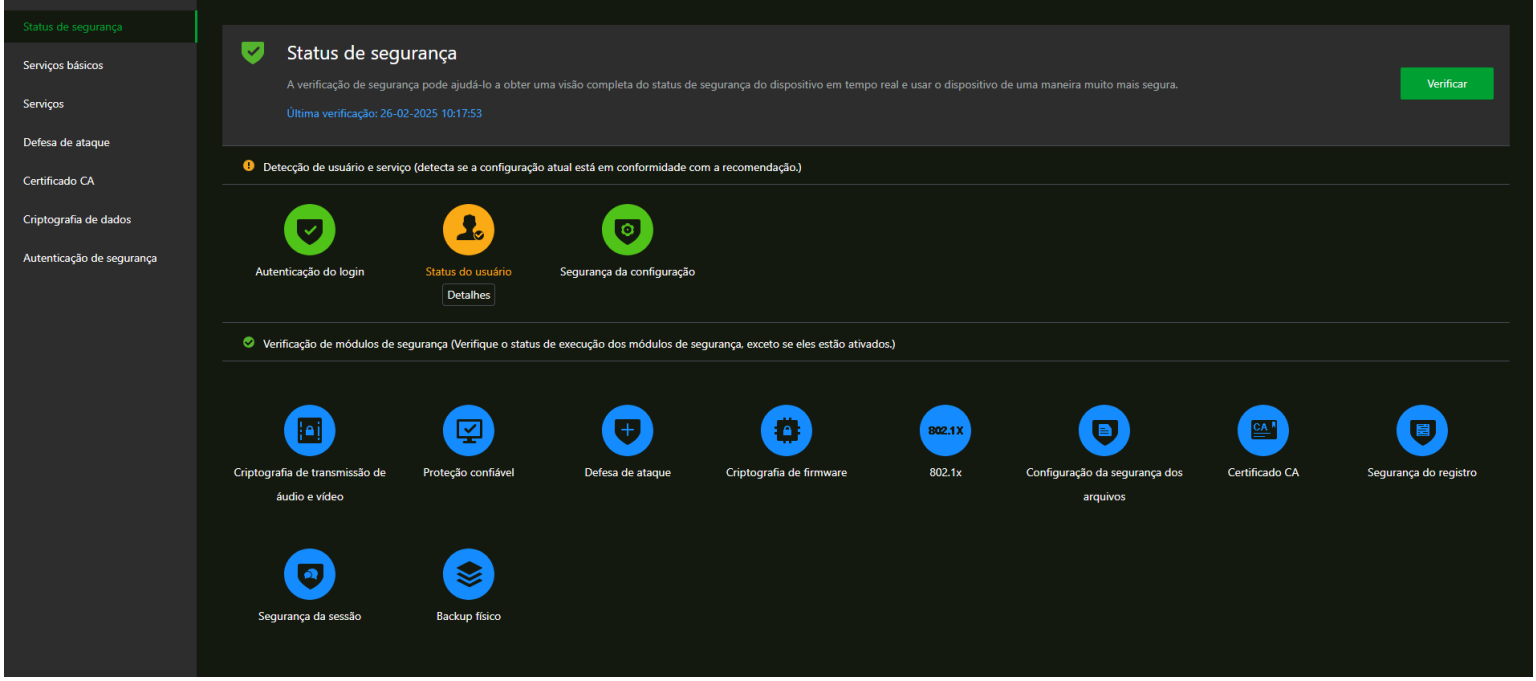
---

# SEGURANÇA

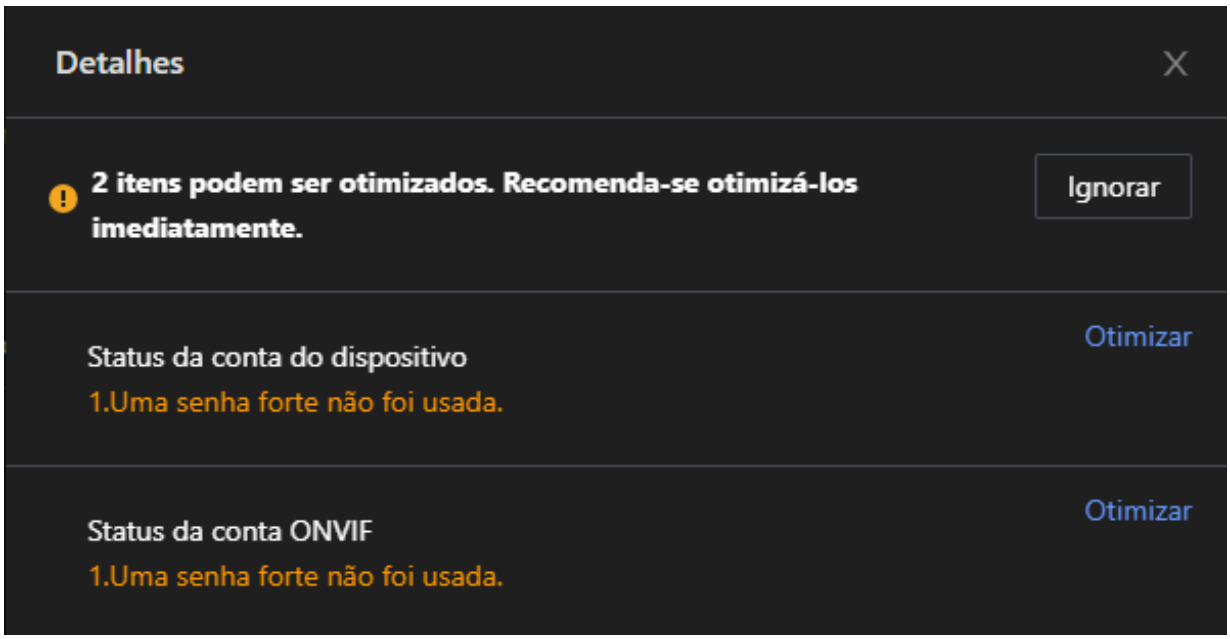
Esse menu permite realizar configurações de segurança, certificados entre outros.

## Status de segurança

Esse submenu, permite configurar as funções Detecção de usuário e serviço e Módulos de segurança.



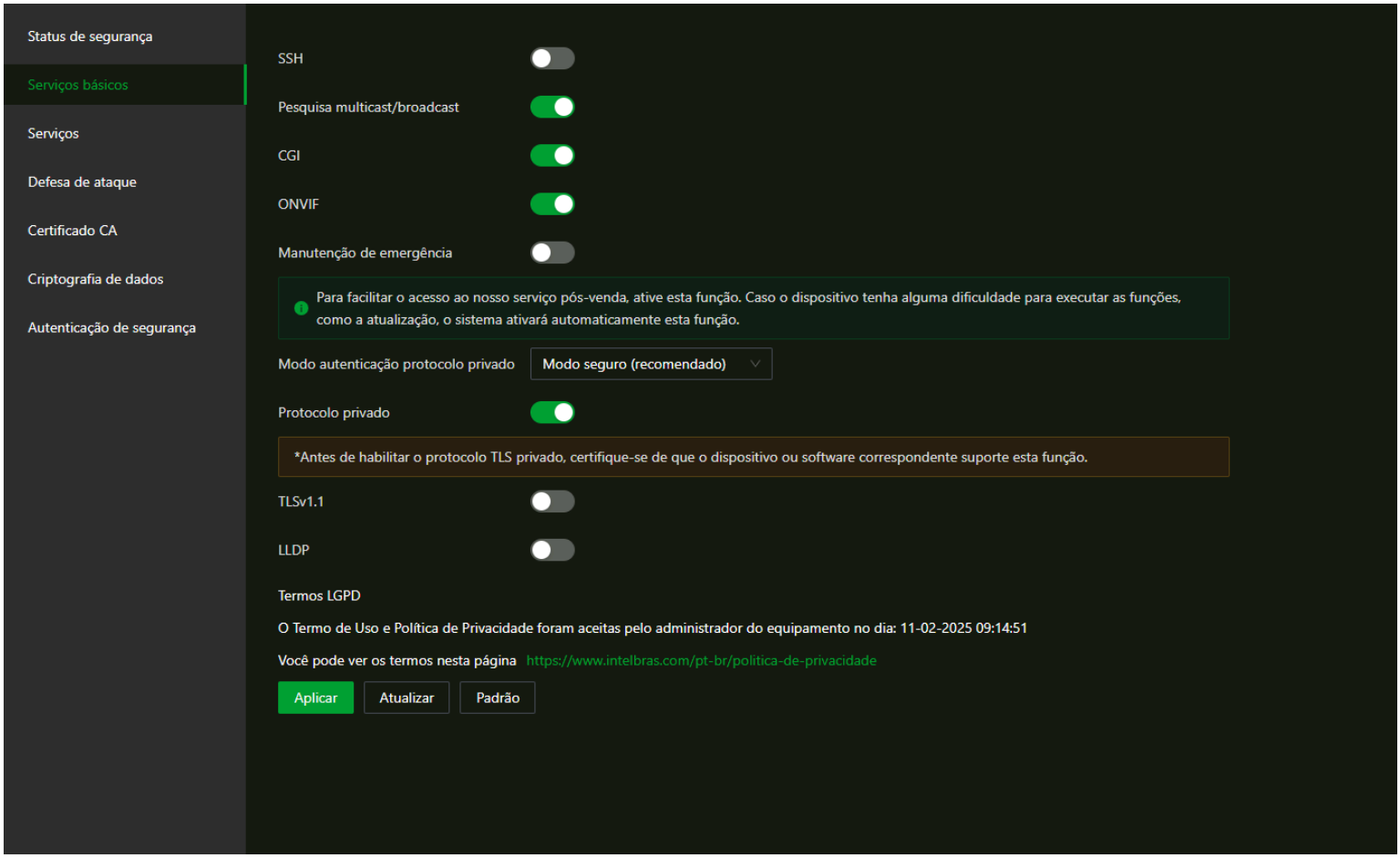

- **Detecção de Usuário e serviço:** Corresponde aos ícones de Conta, Configurações e Login. Os ícones podem ficar verde ou amarelo. Quando um ícone está verde indica que o sistema está seguro. Quando um ícone está amarelo indica que há alguma configuração que pode ser melhorada para tornar o sistema mais seguro
- **Módulos de segurança:** Mostra funcionalidades e protocolos que o equipamento possui para torna-lo seguro. Os ícones não são responsivos.
- **Examinar** Ao clicar sobre o botão para atualizar, o status da detecção de usuário e serviço será verificado e atualizado conforme a configuração atual do dispositivo. Após realizar a varredura, os resultados serão exibidos em diferentes cores:
  - **Amarelo:** Indica que os módulos de segurança estão anormais.
  - **Verde:** Indica que os módulos de segurança estão normais.




- **Ações disponíveis:**
  - **Detalhes:** Exibe informações detalhadas sobre o resultado da varredura.
  - **Ignorar:** Permite ignorar a anomalia, que não será mais escaneada e ficará destacada em cinza.
  - **Otimizar:** Inicia a correção automática da anomalia identificada.

# Serviços básicos

Mostra as opções que podem ser selecionadas em relação aos serviços de segurança.

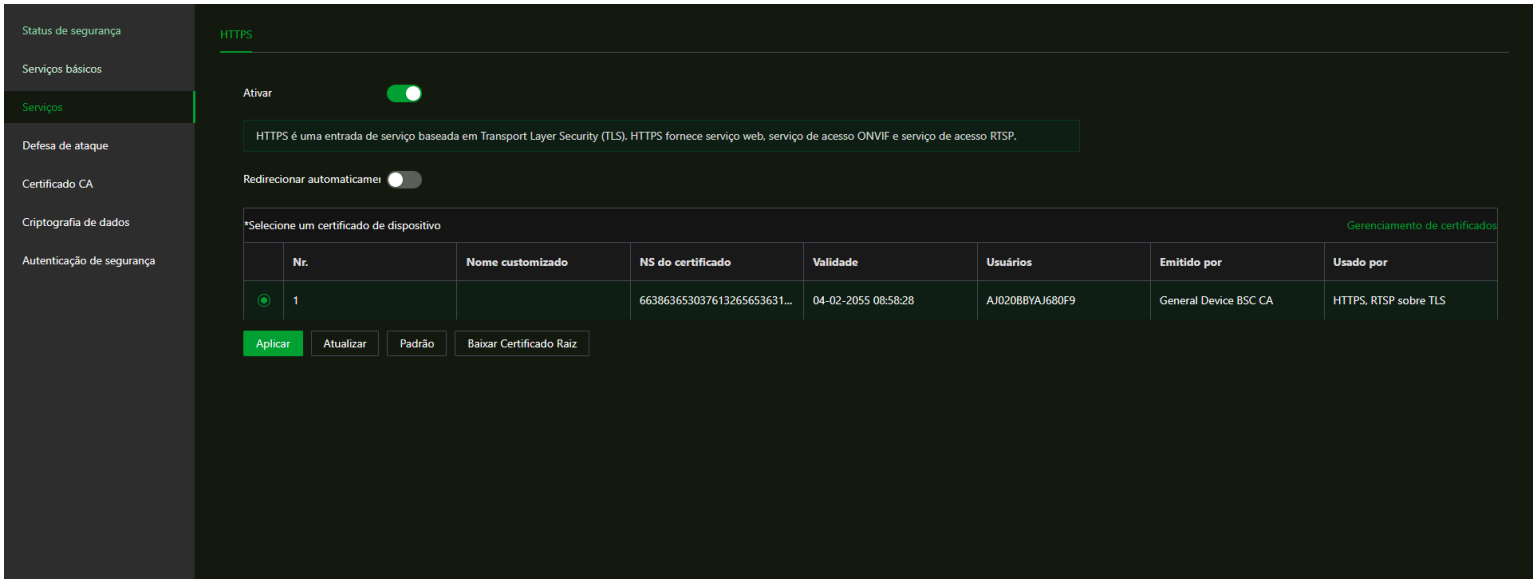



- **SSH:** Habilita o protocolo de segurança SSH.
- **Pesquisa multicast/broadcast:** Habilita a pesquisa de dispositivos utilizando os protocolos multicast ou broadcast.
- **CGI:** Oferece um protocolo para servidores web executarem aplicações. Habilita o uso do protocolo CGI.
- **ONVIF:** Habilita o protocolo ONVIF.
- **Manutenção de emergência:** Habilitado por padrão. Uso dedicado ao suporte Intelbras.
- **Modo autenticação protocolo privado:** Alterar entre o modo seguro (recomendado) e modo de compatibilidade.
- **Protocolo privado:** Manter essa opção habilitado por padrão.
- **Compatível com TLSv1.1:** Habilita a compatibilidade com TLSv1.1.
- **LLDP:** Quando habilitado, permite que dispositivos de rede, como switches, roteadores ou servidores, troquem informações sobre suas identidades e capacidades entre si.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.

- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

# Serviços

Esse menu permite habilitar o uso de um certificado autenticado para acessar a interface web do dispositivo via HTTPS, garantindo uma comunicação segura.




- **Redirecionar automaticamente para HTTPS:** Quando habilitado, o controlador redireciona automaticamente para o protocolo HTTPS ao acessar o IP do dispositivo.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.
- **Baixar certificado:** Permite realizar o download do certificado.
- **Gerenciamento de certificados:** Ao clicar, será redirecionado para página Certificado CA

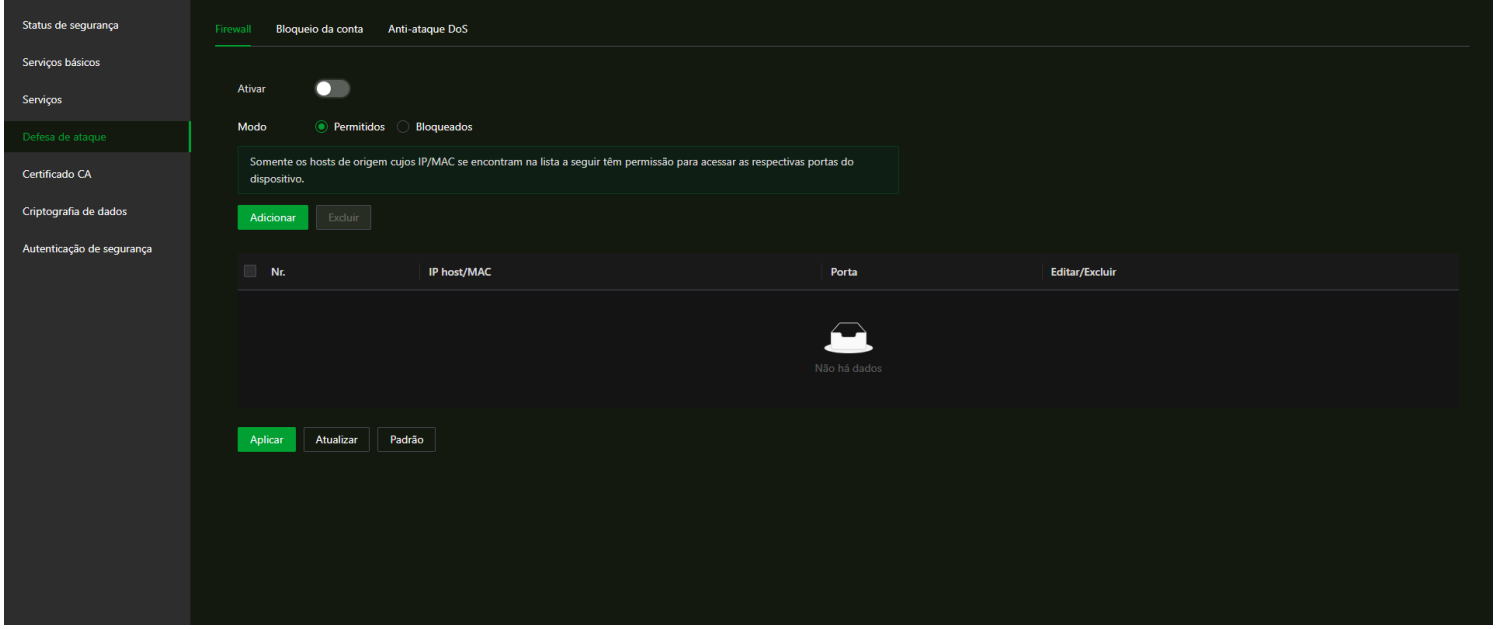
# Defesa de Ataque

Esse menu permite configurar o firewall para restringir o acesso ao dispositivo.

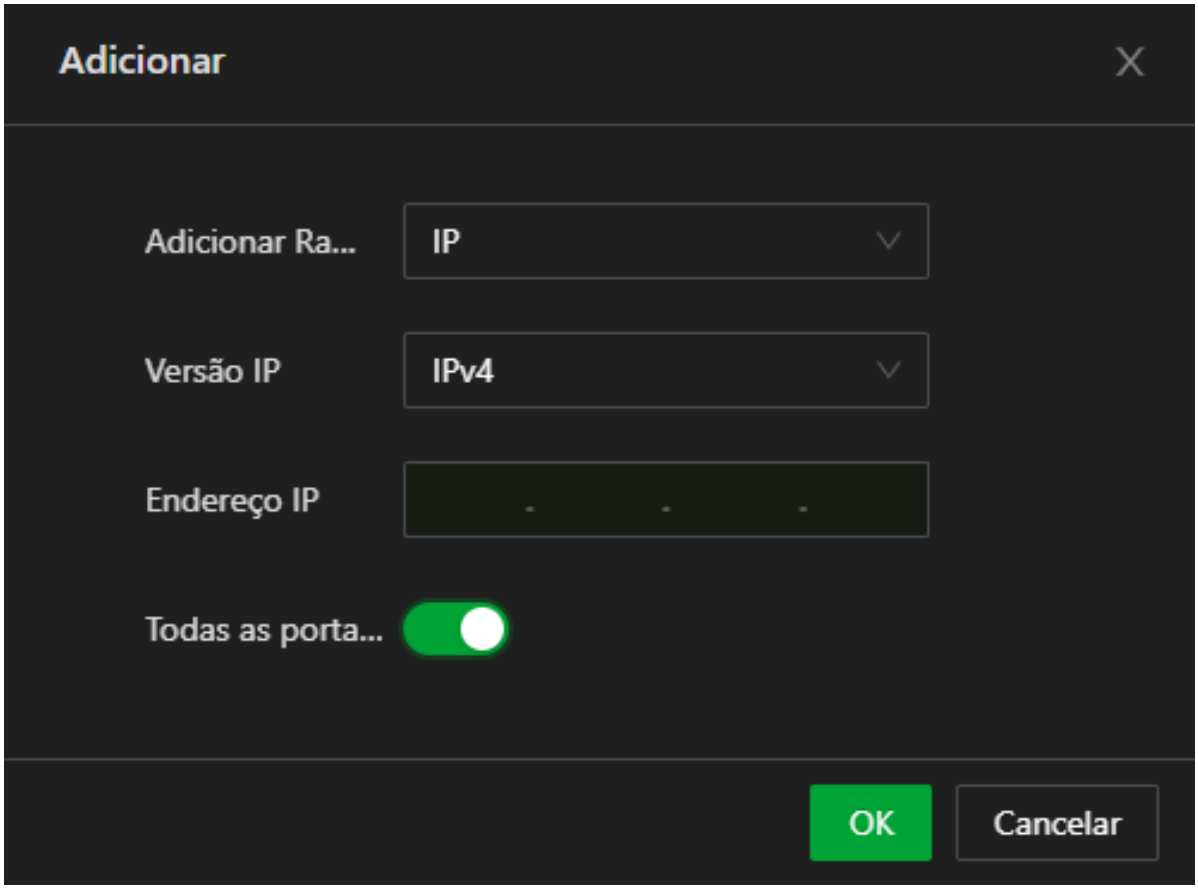
## Firewall

Quando habilitado, permite criar uma lista de IPs autorizados a acessar o dispositivo ou uma lista de IPs bloqueados, impedindo seu acesso.

- **Permitidos:** Quando habilitado, somente os endereços IP/MAC que estiverem na lista de permissões poderão acessar o dispositivo.
- **Bloqueados:** Quando habilitado, somente os endereços IP/MAC que estiverem na lista de bloqueio não poderão acessar o dispositivo.



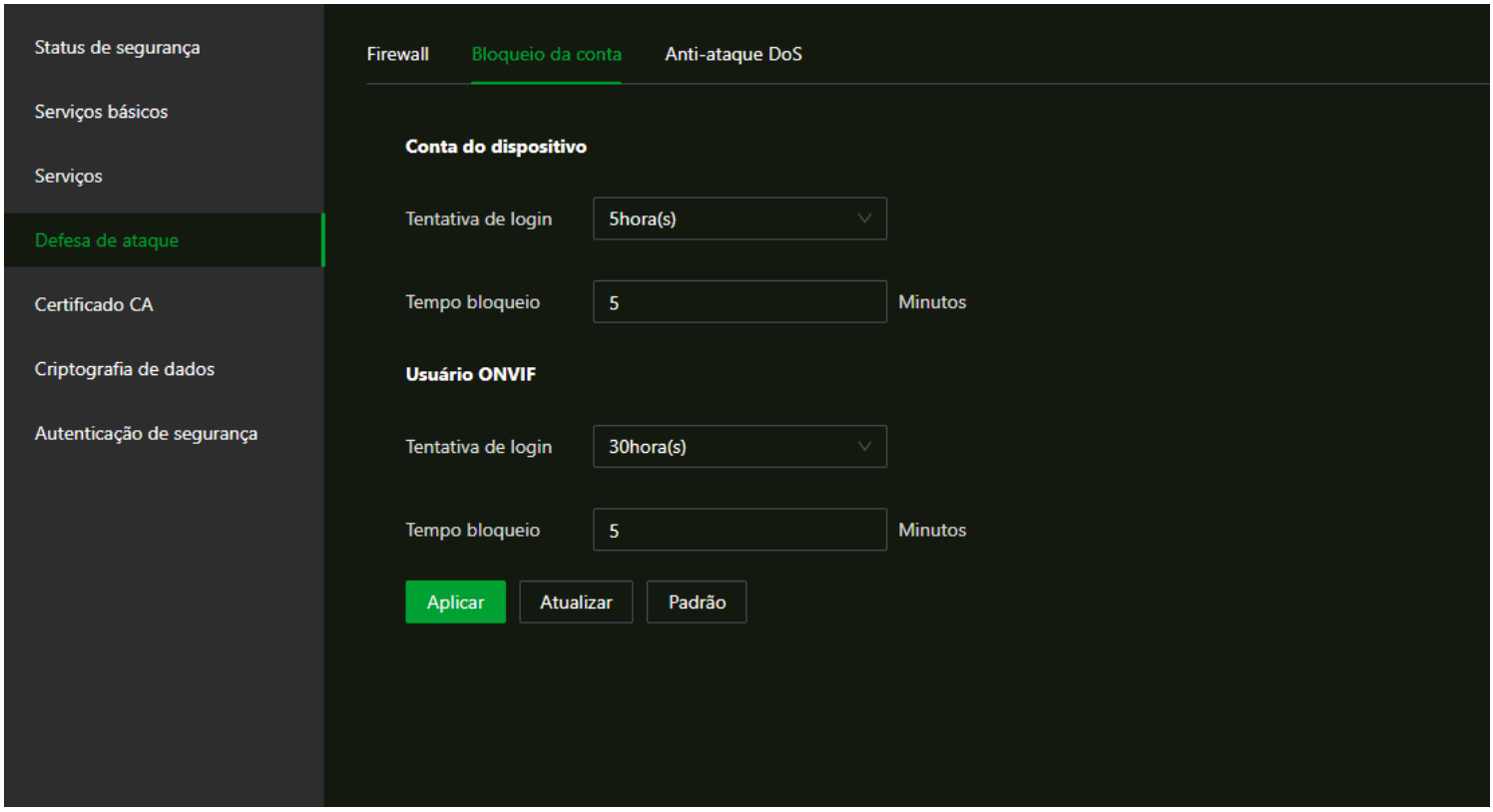

Ao clicar em "Adicionar", uma tela será exibida para inserir os parâmetros referentes ao IP, permitindo configurar a lista de permissões ou bloqueios conforme necessário.




- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

# Bloqueio da Conta

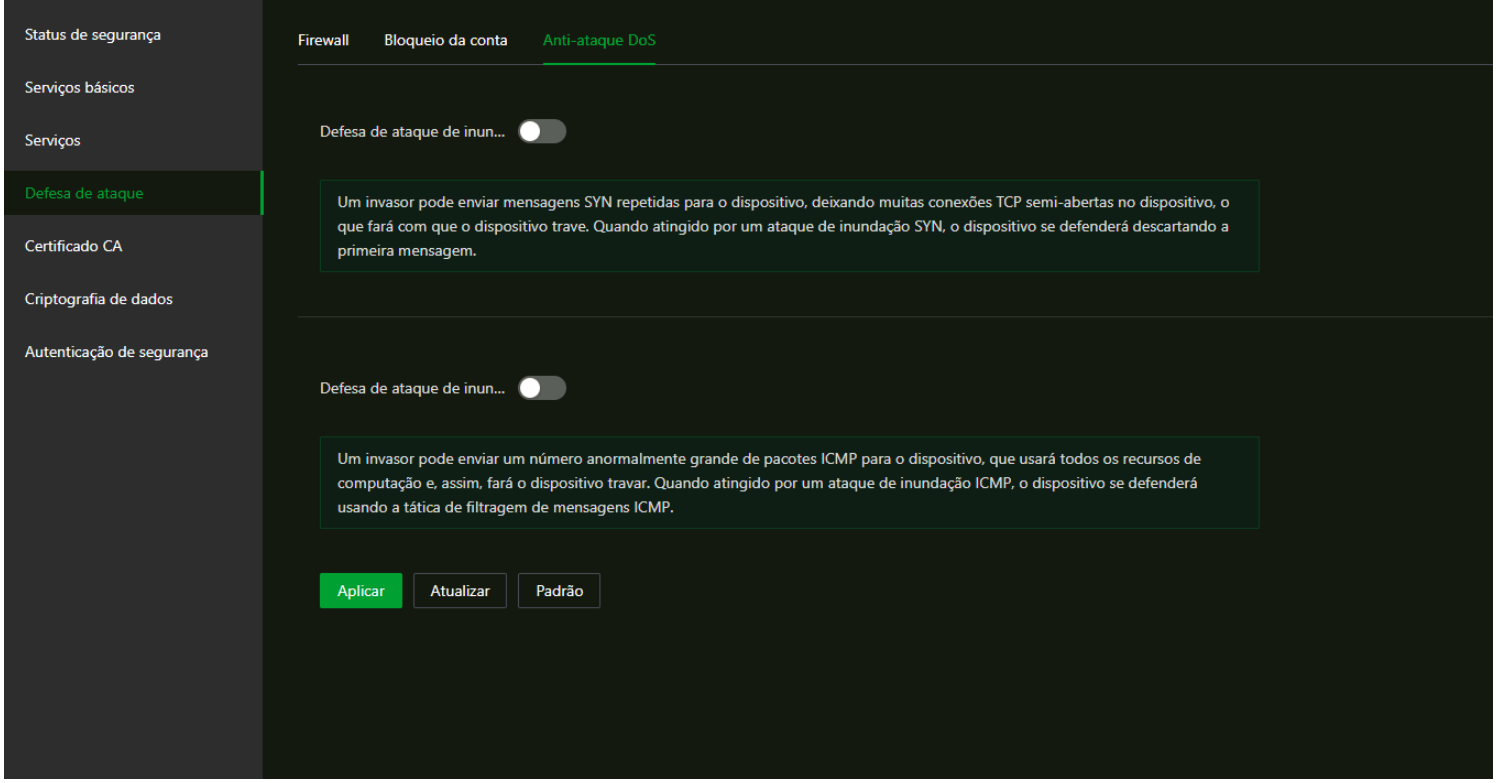
Esse menu permite configurar o bloqueio da conta de acesso ao dispositivo e da conta de acesso ao login ONVIF, caso uma senha incorreta seja inserida um número definido de vezes.




- **Tentativa de login:** Pode ser configurado entre 1 e 30 tentativas. O padrão de fábrica é 5 tentativas.
- **Tempo de bloqueio:** Define por quanto tempo a conta permanecerá bloqueada antes que seja possível tentar um novo login.
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

# Anti-ataque DoS

Esse menu permite habilitar a Defesa contra Ataques SYN Flood e a Defesa contra Ataques ICMP Flood para proteger o dispositivo contra ataques DoS (Denial of Service). Essas defesas ajudam a bloquear tráfego malicioso que tenta sobrecarregar o dispositivo, tornando-o inacessível para usuários legítimos.



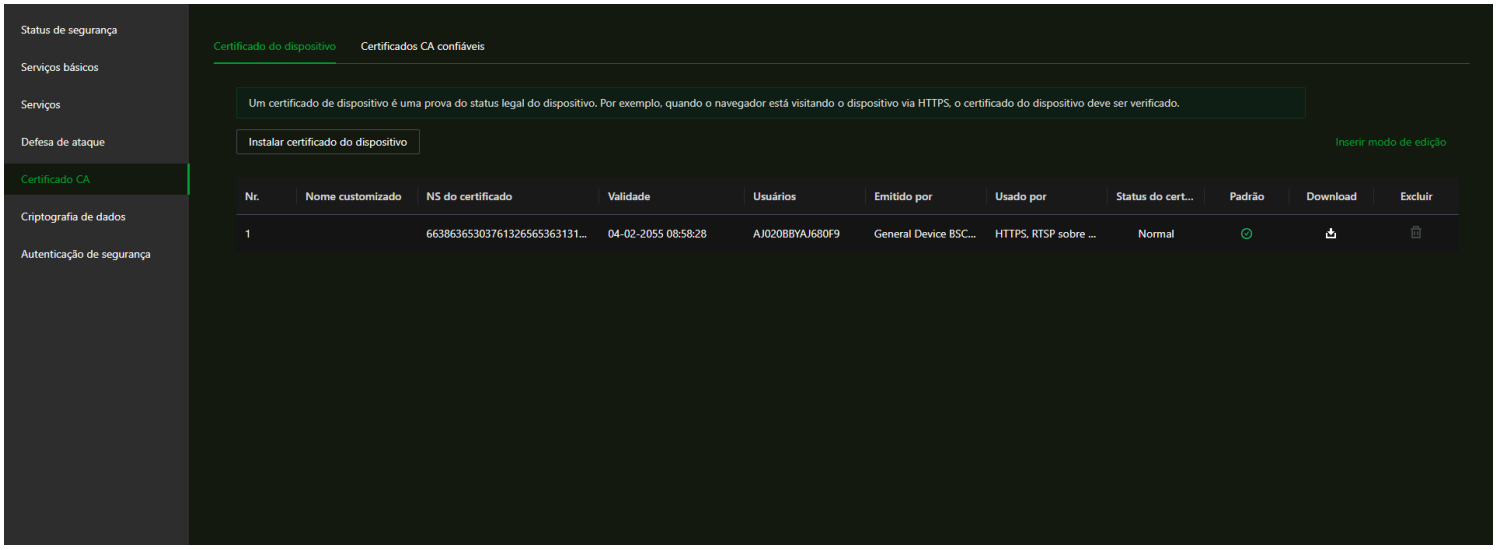

- **Defesa de ataque de inundação SYN:** Marque esta opção para habilitar a defesa contra Flood Attack.
- **Defesa de ataque de inundação ICMP:**: Marque esta opção para habilitar a defesa contra ataques ICMP
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

# Certificado CA

Esse menu permite visualizar um certificado já instalado e criar um certificado ou fazer o upload de um certificado autenticado para permitir o acesso à interface web do dispositivo via HTTPS e 802.1X.

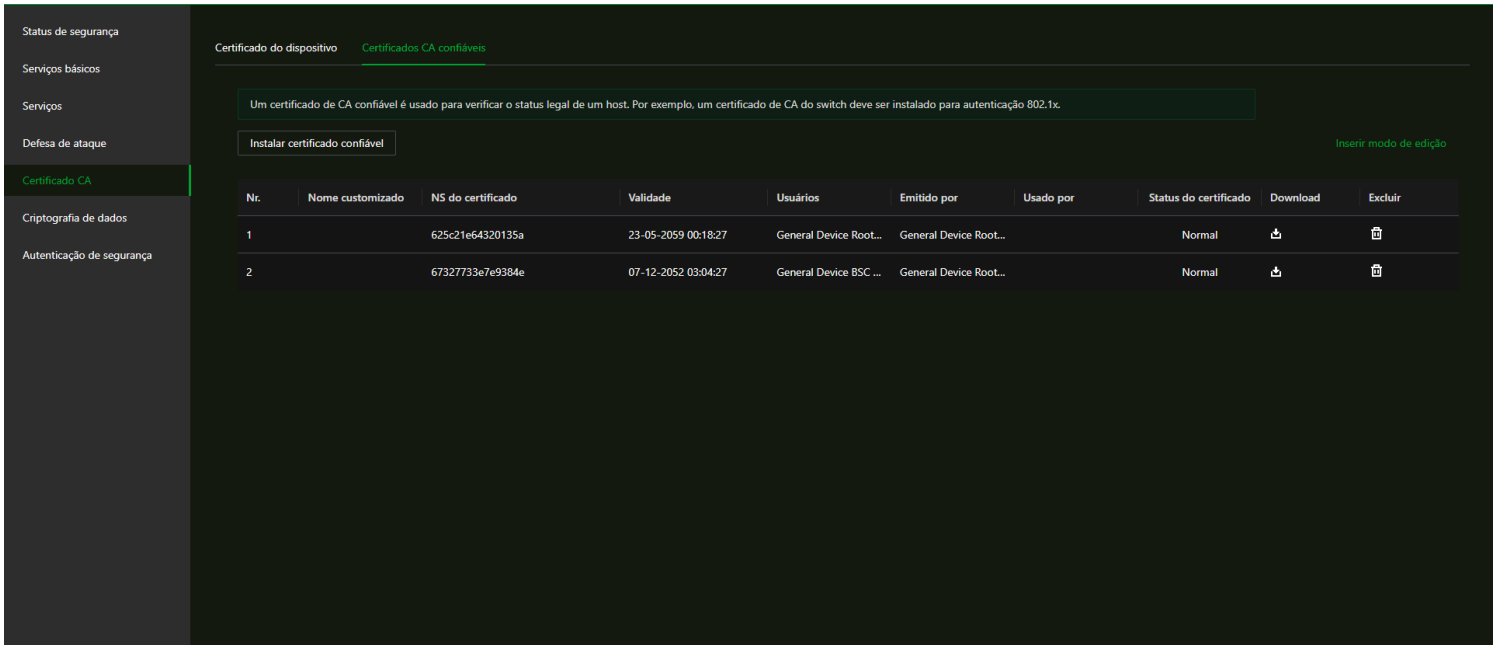
## Certificado do dispositivo

Esse menu permite instalar ou criar um certificado HTTPS para o dispositivo.



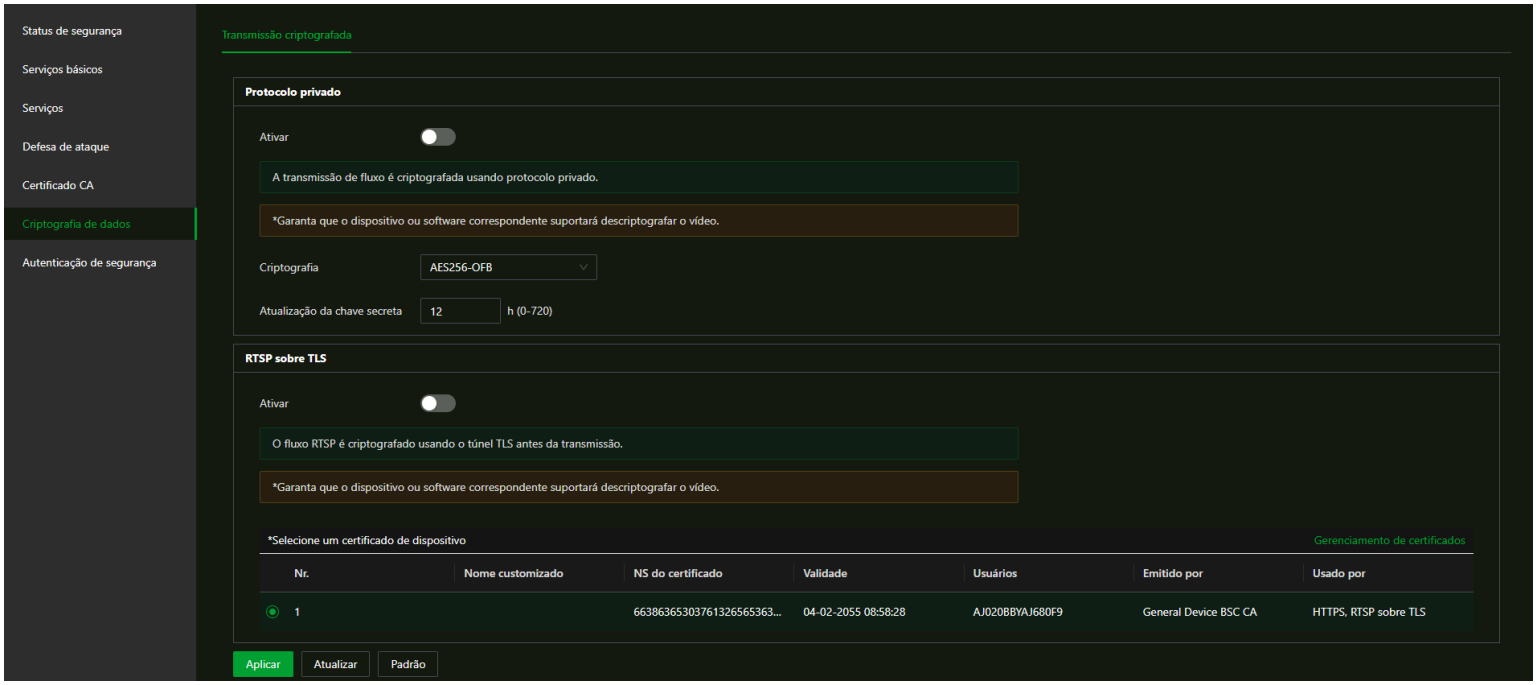
# Certificados CA confiáveis

Esse menu permite instalar um certificado para verificar o status legal de um host.




# Criptografia de dados

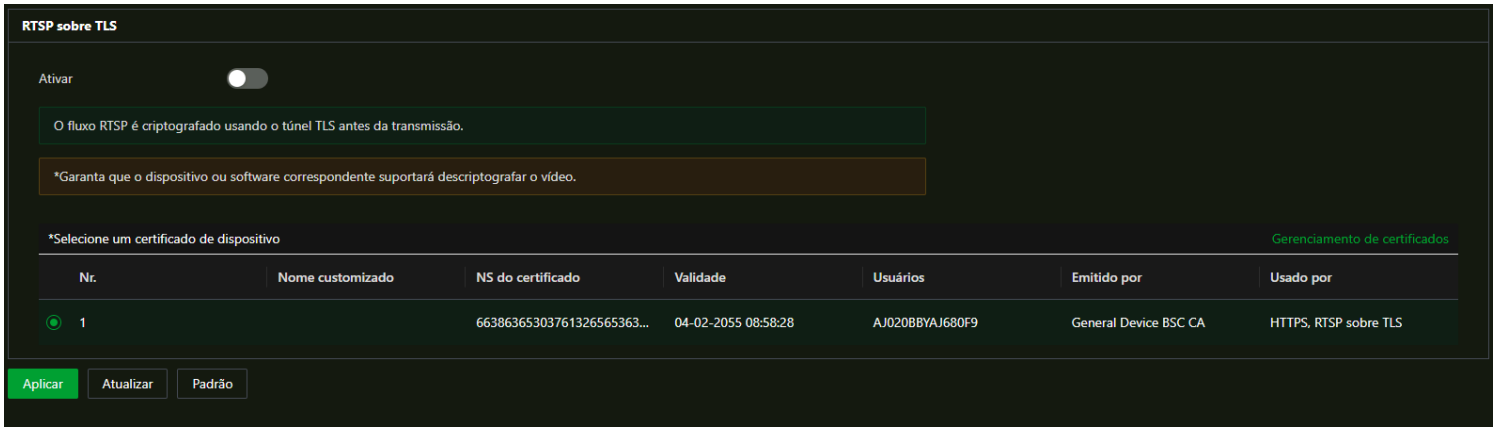
Esse menu permite configurar criptografia de áudio e vídeo do dispositivo par ao fluxo privado.



# Protocolo privado


- **Ativar:** Quando habilitado, os fluxos de dados são criptografados durante a transmissão por meio de um protocolo privado, garantindo maior segurança na comunicação entre os dispositivos.
- **Criptografia:** Padrão AES256-OFB
- **Atualização da chave secreta:** Selecione a cada quantas horas a chave de criptografia será atualizada.

# RTSP sobre TLS

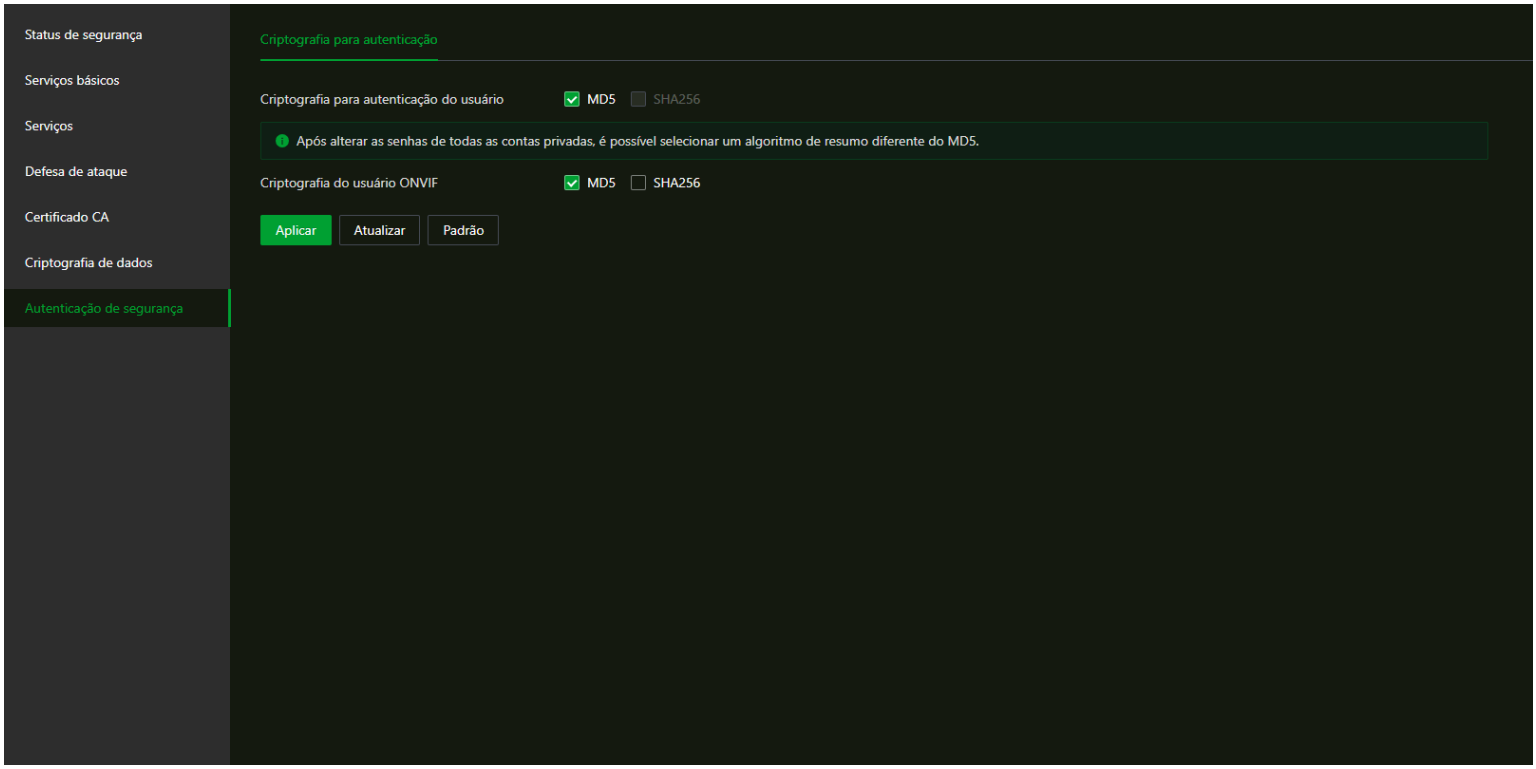



- **Ativar:** Quando habilitado, o fluxo RTSP é criptografado durante a transmissão por meio de um túnel TLS.
- **Gerenciamento de certificados:** Permite criar ou importar um certificado. Ao clicar, será redirecionado para página Certificado CA
- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.

- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

## Autenticação de segurança

Esse menu permite gerenciar a criptografia do login de usuário no dispositivo.




- **Aplicar:** Salva as alterações feitas.
- **Atualizar:** Atualiza a página do dispositivo exibindo as configurações atuais.
- **Padrão:** Define todos os parâmetros da página para o padrão de fábrica. É necessário clicar em "Aplicar" para salvar os parâmetros alterados.

---

# POLITICA DE PRIVACIDADE

Esta é a Política de privacidade (“Política”) que é firmada entre você, de agora em diante denominado Usuário, e a Intelbras S/A - INDÚSTRIA de Telecomunicação Eletrônica Brasileira, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o n° 82.901.000/0001-27, estabelecida na rodovia BR 101, km 210, Área Industrial, São José/SC, representando, neste ato, todas as suas filiais, de agora em diante denominada INTELBRAS. Esta Política foi projetada para regular a coleta, o armazenamento, o uso e o compartilhamento de informações compartilhadas com a INTELBRAS. Ao aceitar esta Política, o Usuário reconhece que analisou e concordou com as condições descritas, a Intelbras não acessa, transfere, capta, nem realiza qualquer outro tipo tratamento de dados pessoais a partir deste produto. de acordo com os termos desta Política, bem como manifesta ciência de que a Política pode ser modificada, a qualquer tempo, com todas as atualizações publicadas nesta página. Sendo usuário menor de idade ou incapaz em quaisquer aspectos, precisará da permissão de seus pais ou responsáveis, que também deverão concordar com a Política e suas condições.

Qualquer dúvida em relação à Política de Privacidade pode ser esclarecida nos contatos:

E-mail: *privacidade@intelbras.com.br*

## 1. Coleta de Informações

Ao utilizar a aplicação disponibilizada pela INTELBRAS, fica o Usuário ciente de que a INTELBRAS não acessa, transfere, capta, nem realiza qualquer outro tipo tratamento de dados pessoais a partir deste produto, tais como nome, telefone, e-mail, endereço, conforme descrito nesta Política. As informações podem ser classificadas em dois tipos: pessoais e não pessoais.

Informações pessoais são dados que estão relacionados ao Usuário, e que permitem a sua identificação, incluindo, mas não se limitando ao nome, data de nascimento, endereço de contato, número de contato, endereço de e-mail e arquivos de conteúdo em vídeo que podem conter informações de identidade visual pessoal.

Informações não pessoais são dados que não estabelecem qualquer relação com um indivíduo específico, como ocupação, idioma, código de área, números de série do produto, URLs, comportamento do usuário, arquivos de conteúdo em vídeo que não contenham informações de identidade visual pessoais, etc.

## 2. Armazenamento de informações pessoais

Conforme estipulado na Política, a INTELBRAS Intelbras não acessa, transfere, capta, nem realiza qualquer outro tipo tratamento de dados pessoais a partir deste produto, e também realizará uma revisão periódica da eficácia dos atuais métodos de armazenamento e tratamento, incluindo precauções de segurança física, para evitar o acesso não autorizado

A INTELBRAS possui as melhores práticas, incluindo tecnologias e estratégias razoáveis para a proteção dos dados, mas a INTELBRAS não pode garantir que suas informações pessoais estejam sob segurança absoluta, tendo em vista a tecnologia de segurança da informação existente. O Usuário reconhece que a INTELBRAS não se responsabiliza por quaisquer perdas no caso de suas informações pessoais serem reveladas, furtadas ou roubadas por motivo de força maior ou problemas de segurança que não tenham sido causados pela INTELBRAS.

## 3. Uso de informações pessoais

A fim de proporcionar uma melhor experiência ao usuário, a INTELBRAS poderá usar suas informações pessoais para os seguintes propósitos:

» Viabilizar o uso da aplicação com todas as suas soluções e funcionalidades, armazenando o histórico necessário para o seu funcionamento e melhor experiência do Usuário.

» Aumentar a segurança do aplicativo e de outros serviços prestados pela INTELBRAS, tais como autenticação de usuários, proteção de segurança, detecção de fraudes, arquivamento e backups.

» A menos que o Usuário opte por cancelar a inscrição, a INTELBRAS poderá contatá-lo enviando comunicações eletrônicas para informar sobre novos produtos e serviços. A INTELBRAS também poderá utilizar informações pessoais para fins internos, tais como auditorias, análise de dados e pesquisas.

## 4. Compartilhamento de informações pessoais

A INTELBRAS não divulgará suas informações pessoais, a menos que (i) tenha seu consentimento prévio por escrito; (ii) esteja de acordo com as leis e regulamentos aplicáveis ou exigidos pelas autoridades; (iii) seja obrigada por decisão judicial; (iv) esteja de acordo com os termos da Política; (v) seja essencial para a proteção dos interesses legítimos da INTELBRAS

A INTELBRAS poderá permitir que seus funcionários acessem os dados em ocasiões específicas com base na necessidade de conhecimento, e assegurará que cumpram com as obrigações no mesmo nível estabelecido pela Política.

Além disso, a INTELBRAS pode disponibilizar certas informações não pessoais a parceiros estratégicos confiáveis que ocasionalmente trabalham com a INTELBRAS para proporcionar uma melhor experiência ao Usuário e aumentar a qualidade dos serviços da aplicação. Sob essas circunstâncias, a aceitação da Política significa que o Usuário concorda e autoriza a INTELBRAS a fornecer suas informações a tais terceiros.

## 5. Âmbito de aplicação

Esta Política diz respeito a todos os aplicativos, sites e outros serviços prestados pela INTELBRAS, exceto quando indicado de outra forma.

Os sites da INTELBRAS podem conter links para serviços fornecidos por terceiros. As informações dos usuários podem ser coletadas por terceiros quando do uso destes links,portanto, a INTELBRAS recomenda que o Usuário conheça suas práticas de privacidade

As informações não pessoais não são regidas pela Política, além disso, você concorda que a INTELBRAS tem o direito de coletar, armazenar, usar e compartilhar suas informações não pessoais para quaisquer e todos os fins, incluindo, sem limitação:

» Entender o comportamento do usuário, a fim de otimizar sua experiência, aperfeiçoar o design funcional, e fornecer melhores serviços;

Analisar o banco de dados, em parte ou no todo, para fins comerciais, incluindo, mas não se limitando a: análise de dados e uso dos dados obtidos a partir do número de visitas do usuário, período das visitas, preferências do usuário e outros dados.

## 6. Cookies e tecnologias semelhantes

A INTELBRAS usa cookies (pequenos arquivos de texto inseridos no dispositivo do usuário) e tecnologias semelhantes para fornecer serviços online e sites e ajudar a coletar dados.Os cookies armazenam as preferências e configurações do usuário, permitindo, entre outras ações: iniciar a sessão rapidamente, identificar os interesses dos usuários e promover anúncios com base nesses interesses, combater fraudes e analisar o desempenho de sites e serviços online.

A INTELBRAS usa web beacons para ajudar a enviar cookies e a reunir dados de desempenho. Os sites podem incluir web beacons e cookies de fornecedores de serviços de terceiros.

O usuário tem à sua disposição uma variedade de ferramentas para controlar os cookies, web beacons e tecnologias semelhantes, incluindo controles de navegador para bloquear e eliminar cookies e controles de provedores de serviços de análise de terceiros para recusar a coleta de dados através de web beacons e tecnologias semelhantes. O navegador e outras escolhas do usuário podem ter impacto em suas experiências com o uso deste aplicativo, software ou serviço.

## 7. Atualizações na Política de Privacidade

Esta Política passa por constante atualizações, assim, a INTELBRAS recomenda rever periodicamente esta página para acompanhar e estar ciente das modificações. Caso sejam feitas alterações relevantes nos termos desta Política, a INTELBRAS publicará a nova Política, notificando o Usuário.

Se você suspeitar de que suas informações pessoais estejam sendo coletadas ou utilizadas de maneira ilegal, ou que qualquer regra desta Política esteja sendo infringida de qualquer maneira, entre em contato com a INTELBRAS, imediatamente, através do site www.intelbras.com.br ou e-mail *privacidade@intelbras.com.br*.

---

# TERMOS DE USO DA INTERFACE

## 1. Aceitação do contrato

Este é um contrato firmado entre você, de agora em diante denominado de USUÁRIO, e a Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o n° 82.901.000/0001-27, estabelecida na rodovia BR 101, km 210, Área Industrial, São José/SC, e de agora em diante denominada simplesmente de Intelbras. Estes Termos de uso de serviço regem o uso da serviço disponibilizado gratuitamente pela Intelbras e/ou seus parceiros, denominado INTERFACE WEB - Bio-T, desenvolvido para computadores em LAN. Se você não concordar com estes termos não use esse serviço. Leia-as atentamente, pois, se você começou a usar esse serviço, ficará configurado que aceitou todos os termos e concorda em cumpri-los. Se você, usuário, for menor de idade ou declarado incapaz em quaisquer aspectos, precisará da permissão de seus pais ou responsáveis, que também deverão concordar com estes mesmos termos e condições.

## 2. Licença limitada

Você recebeu uma licença limitada, não transferível, não exclusiva, livre de royalties e revogável, para baixar, instalar, executar e utilizar esse serviço em seu dispositivo. Você reconhece e concorda que a Intelbras concede ao usuário uma licença exclusiva para uso e, dessa forma, não lhe transfere os direitos sobre o produto. O serviço deverá ser utilizado por você, usuário. A venda, transferência, modificação, engenharia reversa ou distribuição, bem como a cópia de textos, imagens ou quaisquer itens contidos no software são expressamente proibidas. Você reconhece que a Intelbras é proprietária de todos os direitos, títulos e interesses referentes a INTERFACE WEB - Bio-T e ao software relacionado. INTERFACE WEB - Bio-T é a marca comercial ou registrada da Intelbras. Você não pode alterar, destruir, ocultar ou remover de outra forma qualquer as informações sobre direito autoral, os rótulos ou avisos de propriedade dos softwares da Intelbras.

## 3. Do Cadastro

Para a acesso ao software é necessário que o USUÁRIO realize um cadastro prévio onde forneça voluntariamente informações sobre si, tais como: USUÁRIO, senha, endereço de e-mail (Dados). O USUÁRIO declara que os Dados fornecidos são fiéis e verdadeiros e compromete-se a manter seus dados sempre atualizados

INTELBRAS não é responsável pelas informações prestadas, , a Intelbras não acessa, transfere, capta, nem realiza qualquer outro tipo tratamento de dados pessoais a partir deste produto.

O titular e administrador da conta será aquele definido no momento do cadastro, a partir dos Dados oferecidos pelo USUÁRIO. A conta é pessoal e poderá ser acessada unicamente mediante a utilização do USUÁRIO e senha criados pelo próprio USUÁRIO no momento do cadastro, sendo este o único e exclusivo responsável por manter o sigilo de seu USUÁRIO e senha, a fim de garantir a segurança de sua conta e impedir o acesso não autorizado por terceiros. O USUÁRIO é o único responsável por todas as atividades associadas a sua conta.

O USUÁRIO deverá seguir os padrões de segurança de registro de senha e realizar a troca imediata da senha padrão.

## 4. Direitos autorais

O USUÁRIO não adquire, pelo presente instrumento ou pela utilização da aplicação, nenhum direito de propriedade intelectual ou outros direitos exclusivos, incluindo patentes, desenhos, marcas, direitos autorais ou quaisquer direitos sobre informações confidenciais ou segredos de negócio, bem como sobre o conteúdo disponibilizado no software, incluindo, mas não se limitando a textos, gráficos, imagens, logotipos, ícones, fotografias, conteúdo editorial, notificações, softwares e qualquer outro material, sobre a INTELBRAS ou relacionados a ele ou a qualquer parte dele. O USUÁRIO também não adquire nenhum direito sobre o SOFTWARE ou relacionado a ele ou a qualquer componente dele, além dos direitos expressamente licenciados ao USUÁRIO neste Termo ou em qualquer outro contrato mutuamente acordado por escrito entre as partes.

Ao utilizar o SOFTWARE, o USUÁRIO concorda em cumprir com as seguintes diretrizes:

I. Não é permitido postar ou transmitir informação, dado, texto, software, gráficos, sons, fotografias, vídeos, mensagens ou outro conteúdo que seja ilegal, ofensivo, impreciso, difamatório, obsceno, fraudulento, prejudicial, ameaçador ou abusivo.

II. Não interferir no uso de outros usuários da aplicação.

III. Não postar ou fazer upload de qualquer vírus, worms, arquivo corrompido ou outro software capaz de perturbar, incapacitar ou prejudicar o funcionamento da aplicação.

IV. Cumprir com este Termo e quaisquer leis ou regulamentos aplicáveis;

V. Não se passar por qualquer pessoa ou entidade, declarar falsamente ou deturpar sua afiliação com uma pessoa ou entidade.

VI. Não enviar ou transmitir conteúdo que o USUÁRIO não tem o direito de publicar ou transmitir sob qualquer lei ou sob relações contratuais ou fiduciárias (tais como informação privilegiada, informações confidenciais, etc).

VII. Não usar o SOFTWARE para solicitar, obter ou armazenar dados pessoais ou senhas de outros usuários.

## 5. Alterações, modificações e rescisão

A Intelbras reserva-se o direito de, a qualquer tempo, modificar estes termos, seja incluindo, removendo ou alterando quaisquer de suas cláusulas. Tais modificações terão efeito imediato após a publicação. Ao continuar com o uso do serviço você terá aceitado e concordado em cumprir os termos modificados. Assim como, a Intelbras pode, de tempos em tempos, modificar ou descontinuar (temporária ou permanentemente) a distribuição ou a atualização desse serviço. O USUÁRIO não poderá responsabilizar a Intelbras nem seus diretores, executivos, funcionários, afiliados, agentes, contratados ou licenciadores por quaisquer modificações, suspensões ou descontinuidade do serviço.

Para fins contratuais, o USUÁRIO concorda em receber comunicações da INTELBRAS de forma eletrônica (termos e condições, acordos, notificações, divulgações e outras comunicações da INTELBRAS), seja por e-mail ou comunicação interna no próprio SOFTWARE e que, desta forma estabelecida, as comunicações da INTELBRAS satisfazem e cumprem com os requisitos legais, como se fosse em via impressa.

## 6. Indenização

Em nenhum caso a INTELBRAS será responsável por danos pessoais ou qualquer prejuízo incidental, especial, indireto ou consequente, incluindo, sem limitação, prejuízos por perda de lucro, corrupção ou perda de dados, falha de transmissão ou recepção de dados, não continuidade do negócio ou qualquer outro prejuízo ou perda comercial, decorrentes ou relacionados ao uso da aplicação ou a sua inabilidade em usar o SOFTWARE, por qualquer motivo.

## 7. Consentimento para coleta e proteção do uso de dados

O USUÁRIO concorda que a INTELBRASpode coletar os dados pessoais de cadastro e perfil, e usar dados técnicos de seu dispositivo, tais como especificações, configurações, versões de sistema operacional, tipo de conexão à internet e afins.

Os dados pessoais coletados do USUÁRIO serão exclusivamente utilizados para fins de execução do presente contrato, com o objetivo principal de ativação das funcionalidades da aplicação, sendo que o uso destes dados é intrínseco ao próprio funcionamento da aplicação, e para uso e benefícios do titular. Ainda, alguns recursos do 115 SOFTWARE poderão solicitar dados adicionais do USUÁRIO, tais como, nome, telefone, endereço, funcionários, instaladores, serviços prestados, região de atendimento, treinamentos realizados, clientes atendidos, e todos outros dados vinculados à sua atividade comercial. O aceite do USUÁRIO ao presente Contrato desde já autoriza a INTELBRAS a indicar o USUÁRIO como parceiro da INTELBRAS e publicar os dados públicos de contato nos sites, softwares e demais mídias sociais da INTELBRAS, de acordo com a previsão do Manual do Programa de Canais e demais políticas definidas pela INTELBRAS e compartilhadas previamente com o USUÁRIO.

No desenvolvimento de quaisquer atividades relacionadas com a execução do presente Contrato, as Partes observam o regime legal de proteção de dados pessoais, empenhando-se em proceder a todo o tratamento de dados pessoais que venha a mostrar-se necessário ao desenvolvimento do Contrato no estrito e rigoroso cumprimento da Lei.

Os dados pessoais aqui elencados consideram-se os dados das próprias Partes ou mesmo os dados pessoais de seus colaboradores, contratados ou subcontratados.

A fim de garantir a proteção dos dados, o USUÁRIO obriga-se a:

a. Tratar e usar os dados pessoais da INTELBRAS ou de seus PARCEIROS nos termos legalmente permitidos, em especial recolhendo, registrando, organizando, conservando, consultando ou transmitindo os mesmos, apenas e somente nos casos em que seu titular tenha dado o consentimento expresso e inequívoco, ou nos casos legalmente previstos;

b. Tratar os dados de modo compatível com as finalidades para os quais tenha sido recolhidos;

c. Conservar os dados apenas durante o período necessário à prossecução das finalidades da recolha ou do tratamento posterior, garantindo a sua confidencialidade;

d. Implementar as medidas técnicas e organizativas necessárias para proteger os dados contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizada, bem como contra qualquer outra forma de tratamento ilícito dos mesmos;

e. Informar imediatamente a INTELBRAS, devendo prestar toda a colaboração necessária a qualquer investigação que venha a ser realizada, caso exista alguma quebra de segurança, ou suspeita da mesma, independentemente de 116 colocar ou não em causa a segurança e integridade dos dados pessoais;

f. Garantir o exercício, pelos titulares, dos respectivos direitos de informação, acesso e oposição;

O USUÁRIO será responsabilizado perante a INTELBRAS ou terceiros em caso de qualquer violação, compartilhamento, exclusão, cessão, venda, alteração automática dos dados sem prévio e expresso consentimento do seu titular.

## 8. Marcas Registradas e Direitos de Propriedade Intelectual da Intelbras

O USUÁRIO reconhece que as Marcas Registradas e os Direitos de Propriedade Intelectual da INTELBRAS representam um dos ativos estratégicos da INTELBRAS sendo de exclusiva propriedade da mesma.

Durante a vigência deste Termo, será concedido ao USUÁRIO o direito de uso não exclusivo das Marcas Registradas e outros Direitos de Propriedade Intelectual da INTELBRAS, sendo que o USUÁRIO deverá utilizá-los estritamente de acordo com o (i) “Manual da Marca Intelbras”; e (ii) quaisquer outras instruções recebidas da INTELBRAS. O LICENCIADO também garante que suas atividades de propaganda e promocionais cumpram com o (i) Manual da Marca Intelbras; (ii) Programa de Canais Intelbras; e (iii) e a legislação aplicável.

O USUÁRIO não poderá registrar quaisquer Direitos de Propriedade Intelectual da INTELBRAS, tais como qualquer palavra, símbolo, marca identificativa ou nome semelhante às Marcas Registradas da INTELBRAS ou nome de domínio durante a vigência deste contrato ou mesmo após o seu encerramento.

Todo e qualquer direito do USUÁRIO de utilizar as Marcas Registradas e outros Direitos de Propriedade Intelectual da INTELBRAS cessará automaticamente quando do encerramento do presente termo.

O USUÁRIO deverá prontamente notificar a INTELBRAS, por escrito, de qualquer suspeita de uso não autorizado ou infração aos Direitos de Propriedade Intelectual da INTELBRAS e que venha a ter conhecimento. Se solicitado pela INTELBRAS, o USUÁRIO deverá auxiliar a INTELBRAS em quaisquer investigações, negociações 117 ou procedimentos judiciais em virtude de qualquer alegação de uso indevido ou de violação aos Direitos de Propriedade Intelectual da INTELBRAS.

O USUÁRIO compromete-se a não fazer qualquer tipo de anúncio, propaganda, material publicitário dos Produtos Intelbras, contemplando preços e condições de pagamento vinculando produtos INTELBRAS com produtos de concorrentes, devendo tais propagandas serem feitas de forma separada, sem vinculação de qualquer produto concorrente. A INTELBRAS recomenda que o USUÁRIO não faça mala direta constando preços dos produtos.

É vedada a cópia ou qualquer outra forma de reprodução das informações, manuais, literatura técnica e outros documentos fornecidos pela INTELBRAS, exceto para o cumprimento de obrigações estabelecidas nos termos deste instrumento, e de acordo com a legislação aplicável relativamente a direitos autorais e propriedade intelectual.

As obrigações estabelecidas na presente cláusula obrigam o USUÁRIO durante a vigência do presente instrumento, bem como após seu encerramento ou rescisão manutenção da confidencialidade.

## 9. Isenção de garantias e limitações de responsabilidade

Esse serviço estará em contínuo desenvolvimento e pode conter erros, por isso, o uso é fornecido no estado em que se encontra e sob risco do usuário final. Na extensão máxima permitida pela legislação aplicável, a INTELBRAS e seus fornecedores isentam-se de quaisquer garantias e condições expressas ou implícitas incluindo, sem limitação, garantias de comercialização, adequação a um propósito específico, titularidade e não violação no que diz respeito ao serviço e a qualquer um de seus componentes ou ainda à prestação ou não de serviços de suporte. A INTELBRAS não garante que a

operação desse serviço seja contínua e sem defeitos. Com exceção do estabelecido neste documento, não há outras garantias, condições ou promessas vinculadas ao serviço, expressas ou implícitas, e todas essas garantias, condições e promessas podem ser excluídas de acordo com o que é permitido por lei sem prejuízo à Intelbras e a seus colaboradores

I. A INTELBRAS não garante, declara ou assegura que o uso desse serviço será ininterrupto ou livre de erros e você concorda que a Intelbras poderá remover por períodos indefinidos ou cancelar esse serviço a qualquer momento sem que você seja avisado.

II. A INTELBRAS não garante, declara nem assegura que esse serviço esteja livre de perda, interrupção, ataque, vírus, interferência, pirataria ou outra ameaça à segurança e isenta-se de qualquer responsabilidade em relação a essas 118 questões. Você é responsável pelo backup dos arquivos armazenados em seu dispositivo.

III. Em hipótese alguma a INTELBRAS, bem como seus diretores, executivos, funcionários, afiliadas, agentes, contratados ou licenciadores responsabilizar- -se-ão por perdas ou danos causados pelo uso do serviço.

## 10. Validade técnica

Fica estipulado que a INTELBRAS, seus fornecedores ou distribuidores não oferecem um período de validade técnica da INTERFACE WEB - Bio-T. Não se pode considerar que a aplicação esteja isenta de erros, que seu funcionamento seja ininterrupto ou que suas funções satisfaçam os requisitos dos usuários, razão pela qual fica expressamente estipulado que o licenciado o utiliza por sua conta e risco. Devido à complexidade da relação entre software e hardware, a INTELBRAS não garante que a aplicação INTERFACE WEB - Bio-T será compatível com todos os sistemas de software e hardware, que irá operar corretamente ou atender às suas expectativas.

## 11. Foro para dirimir controvérsias

Estes Termos de uso serão regidos e interpretados de acordo com as leis do Brasil. As partes se submetem à jurisdição exclusiva dos tribunais do Brasil. Para dirimir eventuais dúvidas acerca do presente instrumento, bem como de qualquer evento relacionado à utilização de nossos serviços, fica desde logo eleito o foro da comarca de São José, estado de Santa Catarina, por mais privilegiado que outro foro seja. Se você ainda possui alguma dúvida sobre a forma de utilização de nosso produto, sobre nossos Termos de uso ou sobre nossa Política de privacidade, entre em contato com a Intelbras. Ficaremos felizes com o seu contato.

## 12. LGPD - Lei Geral de Proteção de Dados Pessoais

Este produto faz tratamento de dados pessoais, porém a Intelbras não possui acesso aos dados a partir deste produto.

intelbras


**Suporte a clientes:** (48) 2106 0006

**Fórum:** forum.intelbras.com.br (http://forum.intelbras.com.br)

**Suporte via chat:** chat.apps.intelbras.com.br (https://chat.apps.intelbras.com.br/)

**Suporte via e-mail**: suporte@intelbras.com.br

**Treinamentos - iTEC:** cursos.intelbras.com.br (https://cursos.intelbras.com.br)

**SAC:** 0800 7042767

**Onde comprar? Quem instala?:** 0800 7245115

Importado por: Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira

Rodovia SC 281, km 4,5 – Sertão do Maruim – São José/SC - 88122-001

www.intelbras.com.br (http://www.intelbras.com.br)