AXIS D4200-VE Network Strobe Speaker

Manual do Usuário

Índice

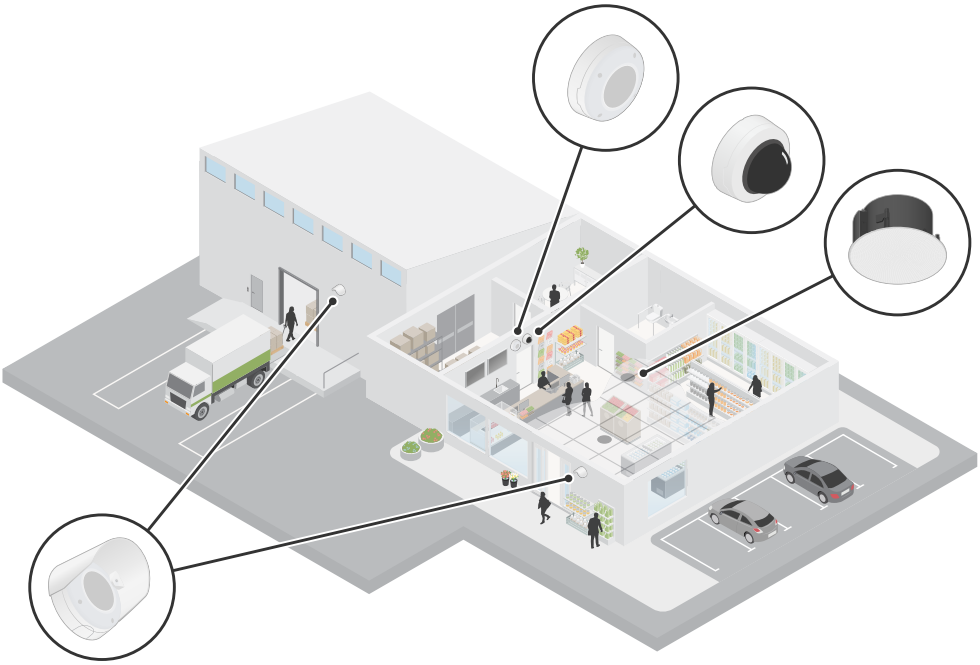
Visão geral da solução

Este manual descreve como tornar o dispositivo acessível em seu sistema de áudio e como configurá-lo diretamente na respectiva interface.

Se estiver usando um software de gerenciamento de áudio ou vídeo, você poderá usar esse software para configurar o dispositivo. O seguinte software de gerenciamento está disponível para controlar seu sistema de áudio:

- **AXIS Audio Manager Edge** — Software de gerenciamento de áudio para sistemas de pequeno porte. Fornecido pré-instalado em todos os dispositivos de áudio com um firmware igual ou superior a 10.0.
  - *Manual do Usuário do AXIS Audio Manager Edge*
- **AXIS Audio Manager Pro** — Software de gerenciamento de áudio avançado para sistemas de grande porte.
  - *Manual do Usuário do AXIS Audio Manager Pro*
- **AXIS Camera Station Pro** — Software de gerenciamento de vídeo avançado para sistemas de grande porte.
  - *Manual do Usuário do AXIS Camera Station Pro*

Para obter mais informações, consulte *Software de gerenciamento de áudio*.



Instalação

Importante

Não instale o alto-falante com estroboscópio e os dispositivos conectados a menos de 3 metros do centro da linha férrea.

Este vídeo é um exemplo de como instalar o AXIS D4200-VE Network Strobe Speaker.

Início

AVISO

Luzes piscando ou cintilando podem causar convulsões em pessoas com epilepsia fotossensível.

Encontre o dispositivo na rede

Para encontrar dispositivos Axis na rede e atribuir endereços IP a eles no Windows®, use o AXIS IP Utility ou o AXIS Device Manager. Ambos os aplicativos são grátis e podem ser baixados de *axis.com/support*.

Para obter mais informações sobre como encontrar e atribuir endereços IP, acesse *Como atribuir um endereço IP e acessar seu dispositivo*.

Suporte a navegadores

O dispositivo pode ser usado com os seguintes navegadores:

	Chrome™	Edge™	Firefox®	Safari®
Windows®	✓	✓	*	*
macOS®	✓	✓	*	*
Linux®	✓	✓	*	*
Outros sistemas operacionais	*	*	*	*

✓: Recomendado

*: Compatível com limitações

Abra a interface web do dispositivo

1. Abra um navegador e digite o endereço IP ou o nome de host do dispositivo Axis.
   Se você não souber o endereço IP, use o AXIS IP Utility ou o AXIS Device Manager para localizar o dispositivo na rede.
2. Digite o nome de usuário e a senha. Se você acessar o dispositivo pela primeira vez, você deverá criar uma conta de administrador. Consulte .

Para obter descrições de todos os controles e opções presentes na interface Web do dispositivo, consulte .

Criar uma conta de administrador

Na primeira vez que fizer login no dispositivo, você deverá criar uma conta de administrador.

1. Insira um nome de usuário.
2. Insira uma senha. Consulte .
3. Insira a senha novamente.
4. Aceite o contrato de licença.
5. Clique em **Add account (Adicionar conta)**.

Importante

O dispositivo não possui conta padrão. Se você perder a senha da sua conta de administrador, deverá redefinir o dispositivo. Consulte .

Senhas seguras

Importante

Use HTTPS (que é ativado por padrão) para definir sua senha ou outras configurações confidenciais pela rede. O HTTPS permite conexões de rede seguras e criptografadas, protegendo assim dados confidenciais, como senhas.

A senha do dispositivo é a proteção primária para seus dados e serviços. Os dispositivos Axis não impõem uma política de senhas, pois os produtos podem ser usados em vários tipos de instalações.

Para proteger seus dados, recomendamos enfaticamente que você:

- Use uma senha com pelo menos 8 caracteres, preferencialmente criada por um gerador de senhas.
- Não exponha a senha.
- Altere a senha em um intervalo recorrente pelo menos uma vez por ano.

Certifique-se de que o software do dispositivo não foi violado

Para certificar-se de que o dispositivo tenha o AXIS OS original ou para assumir o controle total do dispositivo após um ataque de segurança:

1. Restauração das configurações padrão de fábrica. Consulte .
   Após a redefinição, uma inicialização segura garantirá o estado do dispositivo.
2. Configure e instale o dispositivo.

Configure seu dispositivo

Configurar um perfil

Um perfil é um conjunto de configurações definidas. Você pode ter até 30 perfis com diferentes prioridades e padrões.

Para definir um novo perfil:

1. Acesse **Profiles (Perfis)** e clique em + **Create (Criar)**.
2. Insira um **Name (Nome)** e uma **Description (Descrição)**.
3. Selecione as configurações de **Light (Luz)** e **Siren (Sirene)** desejadas para seu perfil.
4. Defina a **Priority (Prioridade)** da luz e da sirene e clique em **Save (Salvar)**.

Para editar um perfil, clique em ⋮ e selecione **Edit (Editar)**.

Configurar um perfil com um arquivo de áudio de sirene personalizado

É possível configurar um perfil com um arquivo de áudio personalizado. Você pode salvar arquivos de áudio de até 100 Mb no dispositivo. Para arquivos de áudio maiores, use um cartão SD.

Carregue um arquivo de áudio:

1. Vá para **Media (Mídia)** e clique em + **Add (Adicionar)**.
2. Procure e selecione o arquivo em seu computador.
3. Selecione **Storage location (Local de armazenamento)**.
4. Clique em **Salvar**.

Para usar o arquivo de áudio em um perfil:

1. Acesse **Profiles (Perfis)** e crie um perfil. Para obter mais informações, consulte .
2. Ao configurar **Siren (Sirene)**, selecione o arquivo de áudio carregado como **Pattern (Padrão)**.

Importar ou exportar um perfil

Se desejar usar um perfil com configurações predefinidas, você poderá importá-lo:

1. Acesse **Profiles (Perfis)** e clique em + **Import (Importar)**.
2. Procure para localizar o arquivo ou arraste e solte o arquivo que deseja importar.
3. Clique em **Salvar**.

Para copiar um ou mais perfis e salvar em outros dispositivos, você poderá exportá-los:

1. Selecione os perfis.
2. Clique em **Export (Exportar)**.
3. Procure os arquivos .json.

Configuração de SIP direto (P2P)

Use ponto a ponto quando a comunicação for feita entre alguns agentes de usuário na mesma rede IP e não houver necessidade de recursos adicionais que poderiam ser fornecidos por um servidor PBX. Para entender melhor como o P2P funciona, consulte .

Para obter mais informações sobre as opções de configuração, consulte .

1. Vá para **System (Sistema)** > **SIP** > **SIP settings (Configurações de SIP)** e selecione **Enable SIP (Ativar SIP)**.
2. Para permitir que o dispositivo receba chamadas, selecione **Allow incoming SIP calls (Permitir recebimento de chamadas SIP)**.
3. Em **Call handling (Tratamento da chamada)**, defina o tempo limite e a duração da chamada.
4. Em **Ports (Portas)**, insira os números de porta.
   - **SIP port (Porta SIP)**– A porta de rede usada para comunicação via SIP. O tráfego de sinalização por essa porta não é criptografado. O número da porta padrão é 5060. Insira um número de porta diferente, se necessário.
   - **TLS port (Porta TLS)** – A porta de rede usada para comunicação criptografada via SIP. O tráfego de sinalização por meio dessa porta é criptografado com o Transport Layer Security (TLS). O número da porta padrão é 5061. Insira um número de porta diferente, se necessário.
   - **RTP start port (Porta de início de RTP)** – Insira a porta usada para o primeiro stream de mídia RTP em uma chamada SIP. A porta de início padrão para transporte de mídia é 4000. Alguns firewalls podem bloquear o tráfego RTP em determinados números de porta. O número da porta deverá ser entre 1024 e 65535.
5. Em **NAT traversal**, selecione os protocolos que deseja ativar para o NAT traversal.

Observação

Use o NAT traversal quando o dispositivo estiver conectado à rede por trás de um roteador NAT ou um firewall. Para obter mais informações consulte .

6. Em **Audio (Áudio)**, selecione pelo menos um codec de áudio com a qualidade de áudio desejada para as chamadas SIP. Arraste e solte para alterar a prioridade.
7. Em **Additional (Adicional)**, selecione opções adicionais.
   - **UDP-to-TCP switching (Alternância de UDP para TCP)** – Selecione para permitir que as chamadas alternem temporariamente os protocolos de transporte de UDP (User Datagram Protocol) para TCP (Transmission Control Protocol). O motivo da comutação é evitar fragmentação, e a mudança poderá ocorrer se uma solicitação estiver dentro de 200 bytes da unidade máxima de transmissão (MTU) ou for superior a 1.300 bytes.
   - **Allow via rewrite (Permitir via regravação)** – Selecione para enviar o endereço IP local em vez de endereço IP público do roteador.
   - **Allow contact rewrite (Permitir regravação de contato)** – Selecione para enviar o endereço IP local em vez de endereço IP público do roteador.
   - **Register with server every (Registrar com o servidor a cada)** – Defina a frequência na qual você deseja que o dispositivo se registre com o servidor SIP para contas SIP existentes.
   - **DTMF payload type (Tipo de carga DTMF)** – Altera o tipo de carga padrão para DTMF.
8. Clique em **Salvar**.

Configuração de SIP por meio de um servidor (PBX)

Use um servidor PBX quando os agentes de usuário se comunicarem dentro e fora da rede IP. Recursos adicionais podem ser adicionados à configuração dependendo do provedor de PBX. Para entender melhor como o P2P funciona, consulte .

Para obter mais informações sobre as opções de configuração, consulte .

1. Solicite as seguintes informações do seu provedor de PBX:

- ID de usuário
- Domínio
- Senha

- ID de autenticação
- ID do chamador
- Registrador
- Porta de início de RTP

2. Para adicionar uma nova conta, vá para **System (Sistema)** > **SIP** > **SIP accounts (Contas SIP)** e clique em **+ Account (+ Conta)**.
3. Insira os detalhes que você recebeu de seu provedor de PBX.
4. Selecione **Registered (Registrado)**.
5. Selecione um modo de transporte.
6. Clique em **Salvar**.
7. Defina as configurações de SIP da mesma forma que para ponto a ponto. Consulte para obter mais informações.

Calibrar e executar um teste de alto-falante remoto

É possível executar um teste de alto-falante para verificar remotamente se um alto-falante funciona conforme o planejado. O alto-falante executa o teste reproduzindo uma série de tons de teste registrados pelo microfone integrado. Toda vez que você executa o teste, os valores registrados são comparados aos valores que foram registrados durante a calibração.

Observação

O teste deve ser calibrado a partir de sua posição montada no local de instalação. Se o alto-falante for movido ou se o ambiente local mudar, por exemplo, se uma parede for construída ou removida, o alto-falante deverá ser calibrado novamente.

Durante a calibração, recomenda-se que alguém permaneça fisicamente presente no local da instalação para ouvir os tons de teste e garantir que eles não estejam sendo abafados ou bloqueados por quaisquer obstruções não intencionais no caminho acústico do alto-falante.

1. Vá para a interface do dispositivo > **Audio > Speaker test (Áudio > Teste de alto-falante)**.
2. Para calibrar o dispositivo de áudio, clique em **Calibrate (Calibrar)**.

Observação

Após o produto Axis ser calibrado, o teste de alto-falante poderá ser executado a qualquer momento.

3. Para executar o teste de alto-falante, clique em **Run the test (Executar o teste)**.

Observação

Também é possível executar a calibração pressionando o botão de controle no dispositivo físico. Consulte para identificar o botão de controle.

Configuração de regras de eventos

Você pode criar regras para fazer com que o dispositivo realize ações quando certos eventos ocorrem. Uma regra consiste em condições e ações. As condições podem ser usadas para acionar as ações. Por exemplo, o dispositivo pode reproduzir um clipe de áudio de acordo com um agendamento ou ao receber uma chamada ou enviar um email se o endereço IP do dispositivo mudar.

Para saber mais, consulte nosso guia *Introdução a regras de eventos*.

Acionar uma ação

1. vá para **System > Events (Sistema > Eventos)** e adicione uma regra. A regra define quando o dispositivo executará determinadas ações. Você pode configurar regras como agendadas, recorrentes ou acionadas manualmente.
2. Insira um **Name (Nome)**.

3. Selecione a **Condition (Condição)** que deve ser atendida para acionar a ação. Se você especificar mais de uma condição para a regra, todas as condições deverão ser atendidas para acionar a ação.
4. Selecione qual **Action (Ação)** o dispositivo deverá executar quando as condições forem atendidas.

Observação

Se você fizer alterações em uma regra ativa, a regra deverá ser ativada novamente para que as alterações entrem em vigor.

Iniciar um perfil quando um alarme for acionado

Este exemplo explica como acionar um alarme quando o sinal de entrada digital mudar.

Defina a direção de entrada para a porta:

1. Vá para **System (Sistema)** > **Accessories (Acessórios)** > **I/O ports (Portas de E/S)**.
2. Vá para **Port 1 (Porta 1)** > **Normal state (Estado normal)** e clique em **Circuit closed (Circuito fechado)**.

Crie uma regra:

1. Vá para **System (Sistema)** > **Events (Eventos)** e adicione uma regra:
2. Digite um nome para a regra.
3. Na lista de condições, selecione **I/O (E/S)** > **Digital input is active (A entrada digital está ativa)**.
4. Selecione **Port 1 (Porta 1)**:
5. Na lista de ações, selecione **Run light and siren profile while the rule is active (Executar perfil de luz e sirene quando a regra está ativa)**.
6. Selecione o perfil de stream que deseja iniciar.
7. Clique em **Salvar**.

Iniciar um perfil via SIP

Este exemplo explica como acionar um alarme via SIP.

Ativar a SIP:

1. Vá para **System (Sistema)** > **SIP** > **SIP settings (Configurações do SIP)**.
2. Selecione **Enable SIP (Ativar SIP)** e **Allow incoming calls (Permitir chamadas recebidas)**.
3. Clique em **Salvar**.

Crie uma regra:

1. Vá para **System (Sistema)** > **Events (Eventos)** e adicione uma regra:
2. Digite um nome para a regra.
3. Na lista de condições, selecione **Call (Chamar)** > **State (Estado)**.
4. Na lista de estados, selecione **Active (Ativo)**.
5. Na lista de ações, selecione **Run light and siren profile while the rule is active (Executar perfil de luz e sirene quando a regra está ativa)**.
6. Selecione o perfil de stream que deseja iniciar.
7. Clique em **Salvar**.

Controle mais de um perfil através de extensões SIP

Ativar a SIP:

1. Vá para **System (Sistema)** > **SIP** > **SIP settings (Configurações do SIP)**.
2. Selecione **Enable SIP (Ativar SIP)** e **Allow incoming calls (Permitir chamadas recebidas)**.

3. Clique em **Salvar**.

Crie uma regra para iniciar um perfil:

1. Vá para **System (Sistema)** > **Events (Eventos)** e adicione uma regra:
2. Digite um nome para a regra.
3. Na lista de condições, selecione **Call (Chamar)** > **State change (Alteração de estado)**.
4. Na lista de motivos, selecione **Accepted by device (Aceito pelo dispositivo)**.
5. Em **Call direction (Direção da chamada)**, selecione **Incoming (Entrada)**.
6. Em **Local SIP URI (URI SIP local)**, digite **sip:[Ext]@[Endereço IP]**, onde [Ext] é a extensão usada para o perfil e [Endereço IP] é o endereço do dispositivo. Por exemplo, **sip:1001@192.168.0.90**.
7. Na lista de ações, selecione **Light and Siren (Luz e sirene)** > **Run light and siren profile (Executar perfil de luz e sirene)**.
8. Selecione o perfil de stream que deseja iniciar.
9. Selecione a ação **Start (Iniciar)**.
10. Clique em **Salvar**.

Crie uma regra para parar um perfil:

1. Vá para **System (Sistema)** > **Events (Eventos)** e adicione uma regra:
2. Digite um nome para a regra.
3. Na lista de condições, selecione **Call (Chamar)** > **State change (Alteração de estado)**.
4. Na lista de motivos, selecione **Terminated (Demitido)**.
5. Em **Call direction (Direção da chamada)**, selecione **Incoming (Entrada)**.
6. Em **Local SIP URI (URI SIP local)**, digite **sip:[Ext]@[Endereço IP]**, onde [Ext] é a extensão usada para o perfil e [Endereço IP] é o endereço do dispositivo. Por exemplo, **sip:1001@192.168.0.90**.
7. Na lista de ações, selecione **Light and Siren (Luz e sirene)** > **Run light and siren profile (Executar perfil de luz e sirene)**.
8. Selecione o perfil de stream que deseja parar.
9. Selecione a ação **Stop (Parar)**.
10. Clique em **Salvar**.

Repita as etapas para criar regras de início e parada para cada perfil que deseja controlar via SIP.

Executar dois perfis com prioridades diferentes

Se você executar dois perfis com prioridades diferentes, o perfil com um número de prioridade mais alto interromperá o perfil com um número de prioridade menor.

Observação

Se você executar dois perfis com a mesma prioridade, o perfil mais recente cancelará o anterior.

Este exemplo explica como configurar o dispositivo para mostrar um perfil com prioridade 4 sobre outro perfil com prioridade 3 quando acionado pela porta de E/S digital.

Criar perfis:

1. Crie um perfil com prioridade 3.
2. Crie outro perfil com prioridade 4.

Crie uma regra:

1. Vá para **System (Sistema)** > **Events (Eventos)** e adicione uma regra:
2. Digite um nome para a regra.

3. Na lista de condições, selecione **I/O (E/S)** > **Digital input is active (A entrada digital está ativa)**.
4. Selecione uma porta.
5. Na lista de ações, selecione **Run light and siren profile while the rule is active (Executar perfil de luz e sirene quando a regra está ativa)**.
6. Selecione o perfil com o número de prioridade mais alto.
7. Clique em **Salvar**.
8. Vá para **Profiles (Perfis)** e inicie o perfil com o número de prioridade mais baixo.

Ativar um alto-falante com estroboscópio via HTTP post quando uma câmera detectar movimento

Este exemplo explica como conectar uma câmera a um alto-falante com estroboscópio e ativar um perfil no alto-falante com estroboscópio sempre que o aplicativo AXIS Motion Guard instalado na câmera detectar movimento.

Antes de começar:

- Crie um novo usuário com a função Operator (Operador) ou Administrator (Administrador) no alto-falante com estroboscópio.
- Crie um perfil no alto-falante com estroboscópio chamado: "Strobe siren profile" (Perfil do alto-falante com estroboscópio).
- Configure o AXIS Motion Guard na câmera e crie um perfil chamado: "Camera profile" (Perfil da câmera).
- Certifique-se de usar o AXIS Device Assistant com versão de firmware 10.8.0 ou posterior.

Crie um destinatário na câmera

1. Na interface de dispositivos da câmera, vá para **System > Events > Recipients (Sistema > Eventos > Destinatários)** e adicione um destinatário.
2. Insira as seguintes informações:
   - **Nome**: Strobe speaker (Alto-falante com estroboscópio)
   - **Type (Tipo)**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/siren_and_light.cgi
     Substitua <IPaddress> pelo endereço do alto-falante com estroboscópio.
   - O nome de usuário e a senha do usuário recém-criado do alto-falante com estroboscópio.
3. Clique em **Test (Testar)** para garantir que todos os dados sejam válidos.
4. Clique em **Salvar**.

Crie duas regras na câmera:

1. Vá para **Rules (Regras)** e adicione uma regra.
2. Insira as seguintes informações:
   - **Nome**: Ativar o alto-falante com estroboscópio com movimento
   - **Condition (Condição)**: **Aplicativos > Motion Guard: Perfil da câmera**
   - **Action (Ação)**: **Notifications > Send notification through HTTP (Notificações > Enviar notificação via HTTP)**
   - **Recipient (Destinatário)**: **Strobe speaker (Alto-falante com estroboscópio)**.
     As informações devem ser as mesmas que você digitou anteriormente em **Events > Recipients > Name (Eventos > Destinatários > Nome)**.
   - **Method (Método)**: **Post**
   - **Body (Corpo)**:

```
{  "apiVersion": "1.0",  "method": "start",  "params": {
"profile" : "Strobe speaker profile"  } }
```

Certifique-se de inserir as mesmas informações em '**"profile" : <>**' que você inseriu ao criar o perfil no alto-falante com estroboscópio, neste caso: "Strobe speaker profile" (Perfil do alto-falante com estroboscópio).

3. Clique em **Salvar**.
4. Adicione outra regra com as seguintes informações:
   - **Nome**: Desativar o alto-falante com estroboscópio com movimento
   - **Condition (Condição)**: **Aplicativos > Motion Guard: Perfil da câmera**
   - Selecione **Invert this condition (Inverter esta condição)**.
   - **Action (Ação)**: **Notifications > Send notification through HTTP (Notificações > Enviar notificação via HTTP)**
   - **Recipient (Destinatário)**: **Strobe speaker (Alto-falante com estroboscópio)**
     As informações devem ser as mesmas que você digitou anteriormente em **Events > Recipients > Name (Eventos > Destinatários > Nome)**.
   - **Method (Método)**: **Post**
   - **Body (Corpo)**:

```
{  "apiVersion": "1.0",  "method": "stop",  "params": {    "profile" : "Strobe speaker profile"  } }
```

Certifique-se de inserir as mesmas informações em '**"profile" : <>**' que você inseriu ao criar o perfil no alto-falante com estroboscópio, neste caso: "Strobe speaker profile" (Perfil do alto-falante com estroboscópio).

5. Clique em **Salvar**.

Ativar um alto-falante com estroboscópio via entrada virtual quando uma câmera detectar movimento

Este exemplo explica como conectar uma câmera a um alto-falante com estroboscópio e ativar um perfil no alto-falante com estroboscópio sempre que o aplicativo AXIS Motion Guard instalado na câmera detectar movimento.

Antes de começar:

- Crie uma conta com os privilégios de Operador ou Administrador no alto-falante com estroboscópio.
- Crie um perfil no alto-falante com estroboscópio.
- Configure o AXIS Motion Guard na câmera e crie um perfil chamado "Camera profile" (Perfil da câmera).

Crie dois destinatários na câmera:

1. Na interface de dispositivos da câmera, vá para **System > Events > Recipients (Sistema > Eventos > Destinatários)** e adicione um destinatário.
2. Insira as seguintes informações:
   - **Nome**: Activate virtual port (Ativar porta virtual)
   - **Type (Tipo)**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/virtualinput/activate.cgi
     Substitua <IPaddress> pelo endereço do alto-falante com estroboscópio.
   - A conta e a senha da conta recém-criada do alto-falante com estroboscópio.
3. Clique em **Test (Testar)** para garantir que todos os dados sejam válidos.
4. Clique em **Salvar**.
5. Adicione um segundo destinatário com as seguintes informações:
   - **Nome**: Deactivate virtual port (Desativar porta virtual)
   - **Type (Tipo)**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi
     Substitua <IPaddress> pelo endereço do alto-falante com estroboscópio.
   - A conta e a senha da conta recém-criada do alto-falante com estroboscópio.
6. Clique em **Test (Testar)** para garantir que todos os dados sejam válidos.
7. Clique em **Salvar**.

Crie duas regras na câmera:

1. Vá para **Rules (Regras)** e adicione uma regra.
2. Insira as seguintes informações:
   - **Nome**: Activate virtual IO1 (Ativar ES1 virtual)
   - **Condition (Condição)**: **Aplicativos > Motion Guard: Perfil da câmera**
   - **Action (Ação)**: **Notifications > Send notification through HTTP (Notificações > Enviar notificação via HTTP)**
   - **Recipient (Destinatário)**: **Activate virtual port (Ativar porta virtual)**
   - **Query string suffix (Sufixo da string de consulta)**: schemaversion=1&port=1
3. Clique em **Salvar.**
4. Adicione outra regra com as seguintes informações:
   - **Nome**: Deactivate virtual IO1 (Desativar ES1 virtual)
   - **Condition (Condição)**: **Aplicativos > Motion Guard: Perfil da câmera**
   - Selecione **Invert this condition (Inverter esta condição)**.
   - **Action (Ação)**: **Notifications > Send notification through HTTP (Notificações > Enviar notificação via HTTP)**
   - **Recipient (Destinatário)**: **Deactivate virtual port (Desativar porta virtual)**
   - **Query string suffix (Sufixo da string de consulta)**: schemaversion=1&port=1
5. Clique em **Salvar.**

Crie uma regra no alto-falante com estroboscópio:

1. Na interface Web do alto-falante com estroboscópio, vá para **System > Events (Sistema > Eventos)** e adicione uma regra.
2. Insira as seguintes informações:
   - **Nome**: Trigger on virtual input 1 (Acionador na entrada virtual 1)
   - **Condition (Condição)**: **E/S > Entrada virtual**
   - **Porta**: **1**
   - **Action (Ação)**: **Light and siren > Run light and siren profile while the rule is active (Luz e sirene > Executar perfil de luz e sirene quando a regra está ativa)**
   - **Profile (Perfil)**: selecione o perfil recém-criado
3. Clique em **Salvar.**

Ativar o alto-falante com estroboscópio via MQTT quando a câmera detectar movimento

Este exemplo explica como conectar uma câmera ao alto-falante com estroboscópio por MQTT e ativar um perfil no alto-falante com estroboscópio sempre que a câmera detectar movimento.

Antes de começar:

- Crie um perfil no alto-falante com estroboscópio.
- Configure um broker de MQTT e obtenha endereço IP, nome de usuário e senha do agente.
- Certifique-se de que o aplicativo de detecção de movimento esteja configurado e em execução na câmera.

Configure o cliente MQTT na câmera:

1. Na interface Web da câmera, vá para **System > MQTT > MQTT client > Broker (Sistema > MQTT > Cliente MQTT > Broker)** e insira as seguintes informações:
   - **Host**: endereço IP do broker
   - **Client ID (ID do cliente)**: por exemplo, Câmera 1
   - **Protocol (Protocolo)**: o protocolo para o qual o broker está definido

- **Porta**: o número da porta usada pelo broker
- O **Username (Nome de usuário)** e a **Password (Senha)** do broker

2. Clique em **Save (Salvar)** e em **Connect (Conectar)**.

Crie duas regras na câmera para a publicação MQTT:

1. Acesse **System > Events > Rules (Sistema > Eventos > Regras)** e adicione uma regra:
2. Insira as seguintes informações:
   - **Nome**: Movimento detectado
   - **Condition (Condição)**: **Applications > Motion alarm (Aplicativos > Alarme de movimento)**
   - **Action (Ação)**: **MQTT > Send MQTT publish message (Enviar mensagem de publicação de MQTT)**
   - **Topic (Tópico)**: Movimento
   - **Payload (Carga)**: ativada
   - **QoS**: 0, 1 ou 2.
3. Clique em **Salvar**.
4. Adicione outra regra com as seguintes informações:
   - **Nome**: sem movimento
   - **Condition (Condição)**: **Applications > Motion alarm (Aplicativos > Alarme de movimento)**
     - Selecione **Invert this condition (Inverter esta condição)**.
   - **Action (Ação)**: **MQTT > Send MQTT publish message (Enviar mensagem de publicação de MQTT)**
   - **Topic (Tópico)**: Movimento
   - **Payload (Carga)**: Desligado
   - **QoS**: 0, 1 ou 2.
5. Clique em **Salvar**.

Configure o cliente MQTT no alto-falante com estroboscópio:

1. Na interface Web do alto-falante com estroboscópio, vá para **System > MQTT > MQTT client > Broker (Sistema > MQTT > Cliente MQTT > Broker)** e insira as seguintes informações:
   - **Host**: endereço IP do broker
   - **Client ID (ID do cliente)**: Sirene 1
   - **Protocol (Protocolo)**: o protocolo para o qual o broker está definido
   - **Porta**: o número da porta usada pelo broker
   - **Username (Nome de usuário)** e **Password (Senha)**
2. Clique em **Save (Salvar)** e em **Connect (Conectar)**.
3. Vá para **MQTT subscriptions (Assinaturas MQTT)** e adicione uma assinatura.
   Insira as seguintes informações:
   - **Subscription filter (Filtro de assinatura)**: Movimento
   - **Subscription type (Tipo de assinatura)**: Stateful
   - **QoS**: 0, 1 ou 2.
4. Clique em **Salvar**.

Crie uma regra no alto-falante com estroboscópio para assinaturas MQTT:

1. Acesse **System > Events > Rules (Sistema > Eventos > Regras)** e adicione uma regra:
2. Insira as seguintes informações:
   - **Nome**: Movimento detectado
   - **Condition (Condição)**: **MQTT > Stateful**

- **Subscription filter (Filtro de assinatura)**: **Movimento**
- **Payload (Carga)**: ativada
- **Action (Ação)**: **Light and siren > Run light and siren profile while the rule is active (Luz e sirene > Executar perfil de luz e sirene quando a regra está ativa)**
- **Profile (Perfil)**: Selecione o perfil que deseja ativar.

3. Clique em **Salvar**.

Envio de um email em caso de falha no teste de alto-falante

Neste exemplo, o dispositivo de áudio é configurado para enviar um email para um destinatário definido quando um teste de alto-falante falha. O teste de alto-falante é configurado para ser realizado às 18h todos os dias.

1. Configure um agendamento para o teste de alto-falante:
   1.1. Vá para a interface do dispositivo > **System (Sistema)** > **Events (Eventos)** > **Schedules (Agendamentos)**.
   1.2. Crie um agendamento que começa às 18h e termina às 18h01 todos os dias. Nomeie-o como "Daily at 6pm" (Diariamente às 18h).
2. Crie um destinatário de email:
   2.1. Vá para a interface do dispositivo > **System (Sistema)** > **Events (Eventos)** > **Recipients (Destinatários)**.
   2.2. Clique em **Add recipient (Adicionar destinatário)**.
   2.3. Nomeie o destinatário como "Speaker test recipients" (Destinatários do teste de alto-falante)
   2.4. Em **Type (Tipo)**, selecione **Email**.
   2.5. Em **Send email to (Enviar email para)**, insira os endereços de email dos destinatários. Use vírgulas para separar vários endereços.
   2.6. Insira os detalhes da conta de email do remetente.
   2.7. Clique em **Test (Testar)** para enviar um email de teste.

   Observação

   Alguns provedores de email possuem filtros de segurança que impedem os usuários de receber ou exibir grandes quantidades de anexos, emails agendados e itens semelhantes. Verifique a política de segurança do provedor de email para evitar problemas de entrega e contas de email bloqueadas.

   2.8. Clique em **Salvar**.
3. Configure o teste de alto-falante automatizado:
   3.1. Vá para a interface do dispositivo > **System (Sistema)** > **Events (Eventos)** > **Rules (Regras)**.
   3.2. Clique em **Add a rule (Adicionar uma regra)**.
   3.3. Insira um nome para a regra.
   3.4. Em **Condition (Condição)**, selecione **Schedule (Agendamento)** e selecione na lista de acionadores
   3.5. Em **Schedule (Agendamento)**, selecione seu agendamento ("Daily at 6pm" (Diariamente às 18h)).
   3.6. Em **Action (Ação)**, selecione **Run automatic speaker test (Executar teste de alto-falante automático)**.
   3.7. Clique em **Salvar**.
4. Configure a condição para enviar um email quando o teste de alto-falante falhar:
   4.1. Vá para a interface do dispositivo > **System (Sistema)** > **Events (Eventos)** > **Rules (Regras)**.
   4.2. Clique em **Add a rule (Adicionar uma regra)**.
   4.3. Insira um nome para a regra.

4.4. Em **Condition (Condição)**, selecione **Speaker test result (Resultado do teste de alto-falante)**.

4.5. Em **Speaker test status (Status do teste de alto-falante)**, select **Didn't pass the test (Reprovado no teste)**.

4.6. Em **Action (Ação)**, selecione **Send notification to email (Enviar notificação para email)**.

4.7. Em **Recipient (Destinatário)**, selecione seu destinatário ("Speaker test recipients" (Destinatários do teste de alto-falante))

4.8. Insira um assunto e uma mensagem e clique em **Save (Salvar)**.

Reproduzir um clipe personalizado quando um alarme for acionado

Este exemplo explica como acionar um arquivo de áudio personalizado quando o sinal de entrada digital mudar.

Carregue um arquivo de áudio:

1. Vá para **Media (Mídia)** e clique em + **Add (Adicionar)**.
2. Clique para procurar e selecionar o arquivo de áudio em seu computador.
3. Selecione **Storage location (Local de armazenamento)**.
4. Clique em **Salvar**.

Crie um perfil com o arquivo de áudio:

1. Acesse **Profiles (Perfis)** e clique em + **Create (Criar)**.
2. Digite um nome em **Name (Nome)** e selecione o padrão de luz do perfil.
3. Na seção da sirene, selecione o arquivo de áudio carregado.
4. Selecione **Intensity (Intensidade)** e **Duration (Duração)**.
5. Clique em **Salvar**.

Defina a direção de entrada para a porta:

1. Vá para **System (Sistema)** > **Accessories (Acessórios)** > **I/O ports (Portas de E/S)**.
2. Vá para **Port 1 (Porta 1)** > **Normal state (Estado normal)** e clique em **Circuit closed (Circuito fechado)**.

Crie uma regra:

1. Vá para **System (Sistema)** > **Events (Eventos)** e adicione uma regra:
2. Insira um nome para a regra.
3. Na lista de condições, selecione **I/O (E/S)> Digital input is active (A entrada digital está ativa)**.
4. Selecione **Port 1 (Porta 1)**:
5. Na lista de ações, selecione **Run light and siren profile while the rule is active (Executar perfil de luz e sirene quando a regra está ativa)**.
6. Selecione o perfil com o arquivo de áudio carregado.
7. Clique em **Salvar**.

Parar áudio com DTMF

Este exemplo explica como:

- Configure o DTMF em um dispositivo.
- Configure um evento para parar o áudio quando um comando DTMF é enviado para o dispositivo.

1. Vá para **System (Sistema)** > **SIP** > **SIP settings (Configurações do SIP)**.
2. Certifique-se de que **Enable SIP (Ativar SIP)** esteja ativada.
   Se for necessário ativá-la, lembre-se de clicar em **Save (Salvar)** posteriormente.

3. Vá para **SIP accounts (Contas SIP)**.
4. Ao lado da conta SIP, clique em ⋮ > **Edit (Editar)**.
5. Em **DTMF**, clique em **+ DTMF sequence (+ Sequência DTMF)**.
6. Em **Sequence (Sequência)**, insira "1".
7. Em **Description (Descrição)**, insira "stop audio" (parar áudio).
8. Clique em **Salvar**.
9. Vá para **System (Sistema)** > **Events (Eventos)** > **Rules (Regras)** e clique em **+ Add a rule (+ Adicionar uma regra)**.
10. Em **Name (Nome)**, digite "DTMF stop audio" (Parar áudio DTMF).
11. Em **Condition (Condição)**, selecione **DTMF**.
12. Em **DTMF Event ID (ID do evento DTMF)**, selecione **stop audio (parar áudio)**.
13. Em **Action (Ação)**, selecione **Stop playing audio clip (Parar reprodução de clipe de áudio)**.
14. Clique em **Salvar**.

Configurar áudio para chamadas de entrada SIP

Você pode configurar uma regra que reproduza um clipe de áudio ao receber uma chamada SIP.

Você também pode configurar uma regra adicional que atende à chamada SIP automaticamente após o clipe de áudio ser encerrado. Isso pode ser útil em casos em que um operador de alarme deseja chamar a atenção de alguém próximo a um dispositivo de áudio e estabelecer uma linha de comunicação. Isso é feito ao fazer uma chamada SIP para o dispositivo de áudio, o qual reproduzirá um clipe de áudio para alertar as pessoas próximas ao dispositivo de áudio. Quando o clipe de áudio para de ser reproduzido, a chamada SIP é atendida automaticamente pelo dispositivo de áudio e a comunicação entre o operador de alarme e as pessoas próximas ao dispositivo de áudio pode ser realizada.

Ativar configurações de SIP:

1. Vá para a interface de dispositivo do alto-falante inserindo seu endereço IP em um navegador da Web.
2. Vá para **System (Sistema)** > **SIP** > **SIP settings (Configurações de SIP)** e selecione **Enable SIP (Ativar SIP)**.
3. Para permitir que o dispositivo receba chamadas, selecione **Allow incoming SIP calls (Permitir recebimento de chamadas SIP)**.
4. Clique em **Save (Salvar)**.
5. Vá para **SIP accounts (Contas SIP)**.
6. Ao lado da conta SIP, clique em ⋮ > **Edit (Editar)**.
7. Desmarque **Answer automatically (Atender automaticamente)**.

Reproduzir áudio quando uma chamada SIP for recebida:

1. Vá para **Settings > System > Events > Rules (Configurações > Sistema > Eventos)** e adicione uma regra.
2. Digite um nome para a regra.
3. Na lista de condições, selecione **State (Estado)**.
4. Na lista de estados, selecione **Ringing (Tocando)**.
5. Na lista de ações, selecione **Play audio clip (Reproduzir clipe de áudio)**.
6. Na lista de clipes, selecione o clipe de áudio que deseja reproduzir.
7. Selecione quantas vezes deseja repetir o clipe de áudio. 0 significa "reproduzir uma vez".
8. Clique em **Save (Salvar)**.

Atender a chamada SIP automaticamente após o clipe de áudio ser encerrado:

1. Vá para **Settings > System > Events > Rules (Configurações > Sistema > Eventos)** e adicione uma regra.
2. Digite um nome para a regra.
3. Na lista de condições, selecione **Audio clip playing (Reprodução de clipe de áudio)**.
4. Marque a opção **Use this condition as a trigger (Usar esta condição como acionador).**
5. Marque **Invert this condition (Inverter esta condição)**.
6. Clique em **+ Add a condition (+ Adicionar uma condição)** para adicionar uma segunda condição ao evento.
7. Na lista de condições, selecione **State (Estado)**.
8. Na lista de estados, selecione **Ringing (Tocando)**.
9. Na lista de ações, selecione **Answer call (Atender chamada)**.
10. Clique em **Save (Salvar)**.

A interface Web

Para alcançar a interface Web do dispositivo, digite o endereço IP do dispositivo em um navegador da Web.

Observação

O suporte aos recursos e às configurações descritas nesta seção variam para cada dispositivo. Este ícone  indica que o recurso ou configuração está disponível somente em alguns dispositivos.

 Mostre ou oculte o menu principal.

 Acesse as notas de versão.

 Acesse a ajuda do produto.

 Altere o idioma.

 Defina o tema claro ou escuro.

 O menu de usuário contém:

- Informações sobre o usuário que está conectado.
-  **Alterar conta**: Saia da conta atual e faça login em uma nova conta.
-  **Desconectar**: Faça logout da conta atual.

 O menu de contexto contém:

- **Analytics data (Dados de analíticos)**: Aceite para compartilhar dados de navegador não pessoais.
- **Feedback (Comentários)**: Compartilhe qualquer feedback para nos ajudar a melhorar sua experiência de usuário.
- **Legal**: veja informações sobre cookies e licenças.
- **About (Sobre)**: veja informações do dispositivo, incluindo versão e número de série do AXIS OS.

Status

Informações do dispositivo

Mostra as informações do dispositivo, incluindo versão e o número de série do AXIS OS.

Upgrade AXIS OS (Atualizar o AXIS OS): atualize o software em seu dispositivo. Abre a página Maintenance (Manutenção), na qual é possível atualizar.

Status de sincronização de horário

Mostra as informações de sincronização de NTP, incluindo se o dispositivo está em sincronia com um servidor NTP e o tempo restante até a próxima sincronização.

NTP settings (Configurações de NTP): Exiba e atualize as configurações de NTP. Leva você para a página **Time and location (Hora e local)** na qual é possível alterar as configurações de NTP.

Segurança

Mostra os tipos de acesso ao dispositivo que estão ativos, quais protocolos de criptografia estão em uso e se aplicativos não assinados são permitidos. Recomendações para as configurações são baseadas no Guia de Fortalecimento do AXIS OS.

Hardening guide (Guia de fortalecimento): Clique para ir para o *Guia de Fortalecimento do AXIS OS*, onde você poderá aprender mais sobre segurança cibernética em dispositivos Axis e práticas recomendadas.

Localizar dispositivo

Mostra as informações de local do dispositivo, incluindo número de série e endereço IP.

Locate device (Localizar dispositivo): Reproduz um som que ajudará você a identificar o alto-falante. Para alguns produtos, o dispositivo piscará um LED.

Teste de alto-falante

Mostra se o alto-falante foi calibrado ou não.

Speaker test (Teste de alto-falante):  : Calibrar o alto-falante. Leva você à página **Speaker test (Teste de alto-falante)**, onde você pode fazer a calibração e executar o teste de alto-falante.

Status de potência

Mostra as informações de status de potência, incluindo a potência atual, potência média e potência máxima.

Power settings (Configurações de energia): Exiba e atualize as configurações de alimentação elétrica do dispositivo. Encaminha você para a página de configurações de energia, onde é possível alterar essas configurações.

Gravação em andamento

Mostra as gravações em andamento e seu espaço de armazenamento designado.

Gravações: Exibir gravações em andamento e filtradas e suas fontes. Para obter mais informações, consulte

 Mostra o espaço de armazenamento no qual a gravação é salva.

Clientes conectados

Mostra o número de conexões e os clientes conectados.

View details (Exibir detalhes): Exiba e atualize a lista dos clientes conectados. A lista mostra o endereço IP, o protocolo, a porta e o PID/Processo de cada conexão.

Analíticos

AXIS Audio Analytics

Nível de pressão sonora

Show threshold and events in graph (Mostrar limites e eventos no gráfico): Ative para mostrar no gráfico quando um pico de som foi detectado.

Threshold (Limite): Ajuste os valores de limite para detecção. O aplicativo registrará um evento de áudio para todos os sons que estiverem fora dos valores limite.

Detecção de áudio adaptativa

Show events in graph (Mostrar eventos no gráfico): Ative para mostrar no gráfico quando um pico de som foi detectado.

Threshold (Limite): mova o controle deslizante para ajustar o limiar de detecção. O limar mínimo registrará até mesmo pequenos picos no som como detecção, enquanto o limiar máximo registrará apenas picos significativos.

Testar alarmes: clique em **Testar** para acionar um evento de detecção para fins de teste.

Classificação de áudio

Show events in graph (Mostrar eventos no gráfico) : Ative para mostrar no gráfico quando um tipo específico de som foi detectado.

Classifications (Classificações) : Selecione os tipos de sons que deseja que o aplicativo detecte.

Test alarms (Testar alarmes) : Clique em **Test (Testar)** para acionar um evento de detecção de um som específico para fins de teste.

Áudio

AXIS Audio Manager Edge

AXIS Audio Manager Edge: Inicie o aplicativo.

Segurança do site de áudio

CA certificate (Certificado de CA): Selecione o certificado a ser usado quando você adicionar dispositivos ao site de áudio. É necessário ativar a autenticação TLS no AXIS Audio Manager Edge.

Save (Salvar): Ative e salve sua seleção.

Configurações do dispositivo

Entrada: ative ou desative a entrada de áudio. Mostra o tipo de entrada.

Input type (Tipo de entrada): Selecione o tipo de entrada. Por exemplo, microfone ou linha.

Power type (Tipo de alimentação): selecione o tipo de alimentação para a entrada.

Apply changes (Aplicar alterações): Aplique sua seleção.

Echo cancellation (Cancelamento de eco) : Ative para remover ecos durante uma comunicação bidirecional.

Controles de ganho separados : ative para ajustar o ganho separadamente para cada tipo de entrada.

Controle de ganho automático : ative para adaptar dinamicamente o ganho às alterações no som.

Gain (Ganho): use o controle deslizante para mudar o ganho. Clique no ícone de microfone para silenciar ou remover o silenciamento.

Stream

Codificação: selecione a codificação que será usada para o streaming da fonte de entrada. Você só poderá escolher a codificação se a entrada de áudio estiver ativada. Se a entrada de áudio estiver desativada, clique em **Enable audio input (Ativar entrada de áudio)** para ativá-la.

Clipes de áudio

Adicionar clipe: Adicione um novo clipe de áudio. É possível usar arquivos .au, .mp3, .opus, .vorbis, .wav.

Executar o clipe de áudio.

Parar de executar o clipe de áudio.

O menu de contexto contém:

- **Rename (Renomear)**: Altere o nome do clipe de áudio.
- **Create link (Criar link)**: crie um URL que reproduz o clipe de áudio no dispositivo. Especifique o volume e o número de vezes para reproduzir o clipe.
- **Download (Baixar)**: baixe o clipe de áudio em seu computador.
- **Excluir**: exclua o clipe de áudio do dispositivo.

Escutar e gravar

Clique para escutar.

Inicie uma gravação contínua do stream de áudio ao vivo. Clique novamente para parar a gravação. Se uma gravação estiver em andamento, ela será retomada automaticamente depois de uma reinicialização.

Observação

Você só poderá escutar e gravar se a entrada estiver ativada para o dispositivo. Vá para **Audio > Device settings (Áudio > Configurações do dispositivo)** para garantir que a entrada seja ativada.

Mostra o armazenamento configurado para o dispositivo. Para configurar o armazenamento, você deve estar conectado como administrador.

Teste de alto-falante

É possível usar o teste de alto-falante para verificar remotamente se o alto-falante funciona conforme o planejado.

Calibrate (Calibrar): É necessário calibrar o alto-falante antes do primeiro teste. Durante a calibração, o alto--falante reproduz uma série de tons de teste que são registrados pelo microfone integrado. Para calibrar um alto-falante, ele deve estar instalado em sua posição final. Se você movimentar o alto-falante depois, ou se os arredores mudarem, por exemplo, se uma parede for construída ou removida, será necessário calibrar novamente.

Run the test (Executar o teste): Reproduz a mesma série de tons de teste que foram reproduzidos durante a calibração e compara-os com os valores registrados durante a calibração.

Visão geral

Status do LED de sinalização

Mostra as diferentes atividades do LED de sinalização em execução no dispositivo. É possível ter até 10 atividades na lista de status do LED de sinalização ao mesmo tempo. Quando duas ou mais atividades são executadas ao mesmo tempo, aquela com a prioridade mais alta mostra o status do LED de sinalização. Essa linha será destacada na lista de status.

Status do LED de áudio

Mostra as diferentes atividades do LED de áudio em execução no dispositivo. É possível ter até 10 atividades na lista de status do LED de áudio ao mesmo tempo. Quando duas ou mais atividades são executadas ao mesmo tempo, aquela com a prioridade mais alta é executada. Essa linha será destacada em verde na lista de status.

Status do alto-falante

Mostra as diferentes atividades de alto-falante em execução no dispositivo. É possível ter até 10 atividades na lista de status do alto-falante ao mesmo tempo. Quando duas ou mais atividades são executadas ao mesmo tempo, aquela com a prioridade mais alta é executada. Essa linha será destacada em verde na lista de status.

Verificação de integridade

Check (Verificar): Faça uma verificação de integridade do dispositivo para garantir que a luz e a sirene estejam funcionando corretamente. Essa opção ativa cada seção de luz uma após a outra e reproduz um tom de teste para verificar o funcionamento do dispositivo. Se a verificação de integridade não for aprovada, vá para os logs do sistema para obter mais informações.

Perfis

Perfis

Um perfil é um conjunto de configurações definidas. Você pode ter até 30 perfis com diferentes prioridades e padrões. Os perfis são listados para fornecer uma visão geral das configurações de nome, prioridade e luz e sirene.

Crie: Clique para criar um novo perfil.

- **Preview/Stop preview (Visualizar/Parar visualização)**: Inicie ou interrompa uma visualização do perfil antes de salvá-lo.

Observação

Não é possível ter dois perfis com o mesmo nome.

- **Nome**: Insira um nome para o perfil.
- **Description (Descrição)**: Insira uma descrição para o perfil.
- **Light (Luz)**: Selecione no menu suspenso o tipo de **Pattern (Padrão)**, **Speed (Velocidade)**, **Intensity (Intensidade)** e **Color (Cor)** da luz desejados.
- **Siren (Sirene)**: Selecione no menu suspenso o tipo de **Pattern (Padrão)** e **Intensity (Intensidade)** desejados para a sirene.
- Inicie ou interrompa uma visualização apenas da luz ou sirene.
- **Duration (Duração)**: Defina a duração das atividades.
  - **Continuous (Continua)**: após ser iniciada, é executada até ser interrompida.
  - **Time (Hora)**: Defina quanto tempo a atividade deverá durar.
  - **Repetitions (Repetições)**: Defina quantas vezes a atividade deve se repetir.
- **Priority (Prioridade)**: Defina a prioridade de uma atividade como um número entre 1 e 10. As atividades com números de prioridade superiores a 10 não podem ser removidas da lista de status. Há três atividades com prioridade superiores a 10, **Manutenção** (11), **Identificação** (12) e **Verificação de integridade** (13).

Importar: Adicione um ou mais perfis com configurações predefinidas.

- **Add (Adicionar)** : Adicione perfis novos.
- **Delete and add (Excluir e adicionar)** : Os perfis antigos são excluídos e você pode carregar novos perfis.
- **Overwrite (Sobrescrever)**: Os perfis atualizados sobrescrevem os perfis existentes.

Para copiar um perfil e salvá-lo em outros dispositivos, selecione um ou mais perfis e clique em **Export (Exportar)**. Um arquivo .json é exportado.

Iniciar um perfil. O perfil e suas atividades aparecem na lista de status.

Escolha entre **Edit (Editar)**, **Copy (Copiar)**, **Export (Exportar)** ou **Delete (Excluir)** o perfil.

Gravações

Ongoing recordings (Gravações em andamento): Mostre todas as gravações em andamento no dispositivo.

Inicie uma gravação no dispositivo.

Escolha o dispositivo de armazenamento que será usado para salvar.

Pare uma gravação no dispositivo.

Gravações acionadas serão paradas manualmente ou quando o dispositivo for desligado.

As **gravações contínuas** continuarão até ser interrompidas manualmente. Mesmo se o dispositivo for desligado, a gravação continuará quando o dispositivo iniciar novamente.

Reproduza a gravação.

Pare a execução da gravação.

Mostre ou oculte informações sobre a gravação.

Set export range (Definir faixa de exportação): se você só quiser exportar uma parte da gravação, informe um intervalo de tempo. Observe que, se você trabalha em um fuso horário diferente do local do dispositivo, o intervalo de tempo será baseado no fuso horário do dispositivo.

Encrypt (Criptografar): Selecione para definir uma senha para as gravações exportadas. Não será possível abrir o arquivo exportado sem a senha.

Clique para excluir uma gravação.

Export (Exportar): Exporte a gravação inteira ou uma parte da gravação.

Clique para filtrar as gravações.

From (De): mostra as gravações realizadas depois de determinado ponto no tempo.

To (Até): mostra as gravações até determinado ponto no tempo.

Source (Fonte): mostra gravações com base na fonte. A fonte refere-se ao sensor.

Event (Evento): mostra gravações com base em eventos.

Armazenamento: mostra gravações com base no tipo de armazenamento.

Mídia

+ Add (Adicionar): Clique para adicionar um novo arquivo.

Storage location (Local de armazenamento): Escolha armazenar o arquivo na memória interna ou no armazenamento interno (cartão SD, se disponível).

O menu de contexto contém:

- **Information (Informações)**: Exiba informações sobre o arquivo.
- **Copy link (Copiar link)**: Copie o link do local do arquivo no dispositivo.
- **Excluir**: Exclua o arquivo do local de armazenamento.

Apps

Adicionar app: Instale um novo aplicativo.

Find more apps (Encontrar mais aplicativos): Encontre mais aplicativos para instalar. Você será levado para uma página de visão geral dos aplicativos Axis.

Permitir apps não assinados : Ative para permitir a instalação de aplicativos não assinados.

Veja as atualizações de segurança nos aplicativos AXIS OS e ACAP.

Observação

O desempenho do dispositivo poderá ser afetado se você executar vários aplicativos ao mesmo tempo.

Use a chave ao lado do nome do aplicativo para iniciar ou parar o aplicativo.

Open (Abrir): Acesse às configurações do aplicativo. As configurações disponíveis dependem do aplicativo. Alguns aplicativos não têm configurações.

O menu de contexto pode conter uma ou mais das seguintes opções:

- **Open-source license (Licença de código aberto)**: Exiba informações sobre as licenças de código aberto usadas no aplicativo.
- **App log (Log do aplicativo)**: Exiba um log dos eventos de aplicativos. Este log é útil quando é necessário entrar em contato com o suporte.
- **Activate license with a key (Ativar licença com uma chave)**: Se o aplicativo exigir uma licença, você deverá ativá-la. Use essa opção se o dispositivo não tiver acesso à Internet.
  Se você não tiver uma chave de licença, acesse *axis.com/products/analytics*. Você precisa de um código de licença e do número de série do produto Axis para gerar uma chave de licença.
- **Activate license automatically (Ativar licença automaticamente)**: Se o aplicativo exigir uma licença, você deverá ativá-la. Use essa opção se o dispositivo tiver acesso à Internet. Um código de licença é necessário para ativar a licença.
- **Deactivate the license (Desativar a licença)**: Desative a licença para substituí-la por outra licença, por exemplo, ao migrar de uma licença de avaliação para uma licença completa. Se você desativar a licença, ela será removida do dispositivo.
- **Settings (Configurações)**: configure os parâmetros.
- **Excluir**: Exclua o aplicativo permanentemente do dispositivo. Se você não desativar a licença primeiro, ela permanecerá ativa.

Sistema

Hora e local

Data e hora

O formato de hora depende das configurações de idioma do navegador da Web.

Observação

Recomendamos sincronizar a data e a hora do dispositivo com um servidor NTP.

Synchronization (Sincronização): Selecione uma opção para sincronização da data e da hora do dispositivo.

- **Automatic date and time (manual NTS KE servers) (Data e hora automáticas (servidores NTS KE manuais))**: Sincronizar com os servidores estabelecimentos de chave NTP seguros conectados ao servidor DHCP.
  - **Manual NTS KE servers (Servidores NTS KE manuais)**: Insira o endereço IP de um ou dois servidores NTP. Quando você usa dois servidores NTP, o dispositivo sincroniza e adapta sua hora com base na entrada de ambos.
  - **Trusted NTS KE CA certificates (Certificados CA NTS KE confiáveis)**: Selecione os certificados CA confiáveis a serem usados para a sincronização segura de horário do NTS KE ou selecione None (Nenhum).
  - **Max NTP poll time (Tempo máximo da pesquisa NTP)**: selecione o tempo máximo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
  - **Min NTP poll time (Tempo mínimo da pesquisa NTP)**: selecione o tempo mínimo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
- **Automatic date and time (NTP servers using DHCP) (Data e hora automáticas (servidores NTP usando DHCP))**: sincronize com os servidores NTP conectados ao servidor DHCP.
  - **Fallback NTP servers (Servidores NTP de fallback)**: insira o endereço IP de um ou dois servidores de fallback.
  - **Max NTP poll time (Tempo máximo da pesquisa NTP)**: selecione o tempo máximo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
  - **Min NTP poll time (Tempo mínimo da pesquisa NTP)**: selecione o tempo mínimo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
- **Automatic date and time (manual NTP servers) (Data e hora automáticas (servidores NTP manuais))**: sincronize com os servidores NTP de sua escolha.
  - **Manual NTP servers (Servidores NTP manuais)**: Insira o endereço IP de um ou dois servidores NTP. Quando você usa dois servidores NTP, o dispositivo sincroniza e adapta sua hora com base na entrada de ambos.
  - **Max NTP poll time (Tempo máximo da pesquisa NTP)**: selecione o tempo máximo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
  - **Min NTP poll time (Tempo mínimo da pesquisa NTP)**: selecione o tempo mínimo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
- **Custom date and time (Data e hora personalizadas)**: defina manualmente a data e a hora. Clique em **Get from system (Obter do sistema)** para obter as configurações de data e hora uma vez em seu computador ou dispositivo móvel.

Fuso horário: Selecione qual fuso horário será usado. A hora será ajustada automaticamente para o horário de verão e o horário padrão.

- **DHCP**: Adota o fuso horário do servidor DHCP. O dispositivo deve estar conectado a um servidor DHCP para que você possa selecionar esta opção.
- **Manual**: Selecione um fuso horário na lista suspensa.

Observação

O sistema usa as configurações de data e hora em todas as gravações, logs e configurações do sistema.

Local do dispositivo

Insira o local do dispositivo. Seu sistema de gerenciamento de vídeo pode usar essa informação para posicionar o dispositivo em um mapa.

- **Latitude**: Valores positivos estão ao norte do equador.
- **Longitude**: Valores positivos estão a leste do meridiano de Greenwich.
- **Cabeçalho**: Insira a direção da bússola para a qual o dispositivo está voltado. 0 representa o norte.
- **Label (Rótulo)**: Insira um nome descritivo para seu dispositivo.
- **Save (Salvar)**: Clique em para salvar a localização do dispositivo.

Rede

IPv4

Assign IPv4 automatically (Atribuir IPv4 automaticamente): Selecione para permitir que o roteador de rede atribua um endereço IP ao dispositivo automaticamente. Recomendamos utilizar IP (DHCP) automático para a maioria das redes.

Endereço IP: Insira um endereço IP exclusivo para o dispositivo. Endereços IP estáticos podem ser atribuídos aleatoriamente em redes isoladas, desde que cada endereço seja único. Para evitar conflitos, é altamente recomendável entrar em contato o administrador da rede antes de atribuir um endereço IP estático.

Máscara de sub-rede: Insira a máscara de sub-rede para definir quais endereços estão dentro da rede local. Qualquer endereço fora da rede local passa pelo roteador.

Router (Roteador): Insira o endereço IP do roteador padrão (gateway) usado para conectar dispositivos conectados a diferentes redes e segmentos de rede.

Fallback to static IP address if DHCP isn't available (Retornar como contingência para o endereço IP estático se o DHCP não estiver disponível): Selecione se você deseja adicionar um endereço IP estático para usar como contingência se o DHCP não estiver disponível e não puder atribuir um endereço IP automaticamente.

Observação

Se o DHCP não estiver disponível e o dispositivo usar um fallback de endereço estático, o endereço estático será configurado com um escopo limitado.

IPv6

Assign IPv6 automatically (Atribuir IPv6 automaticamente): Selecione para ativar o IPv6 e permitir que o roteador de rede atribua um endereço IP ao dispositivo automaticamente.

Nome de host

Assign hostname automatically (Atribuir nome de host automaticamente): Selecione para permitir que o roteador de rede atribua um nome de host ao dispositivo automaticamente.

Nome de host: Insira o nome de host manualmente para usar como uma maneira alternativa de acessar o dispositivo. O relatório do servidor e o log do sistema usam o nome de host. Os caracteres permitidos são A – Z, a – z, 0 – 9 e -.

Ative as atualizações de DNS dinâmicas: Permita que o dispositivo faça a atualização automática dos registros do servidor de nomes de domínio sempre que o endereço IP for alterado.

Registrar o nome do DNS: Digite um nome de domínio exclusivo que aponte para o endereço IP de seu dispositivo. Os caracteres permitidos são A – Z, a – z, 0 – 9 e -.

TTL: O tempo de vida (TTL) define por quanto tempo um registro DNS permanecerá válido até que precise ser atualizado.

Servidores DNS

Assign DNS automatically (Atribuir o DNS automaticamente): Selecione para permitir que o servidor DHCP atribua domínios de pesquisa e endereços de servidor DNS ao dispositivo automaticamente. Recomendamos utilizar DNS (DHCP) automático para a maioria das redes.

Search domains (Domínios de pesquisa): Ao usar um nome de host que não está totalmente qualificado, clique em **Add search domain (Adicionar domínio de pesquisa)** e insira um domínio para pesquisar o nome de domínio usado pelo dispositivo.

DNS servers (Servidores DNS): Clique em **Add DNS server (Adicionar servidor DNS)** e insira o endereço IP do servidor DNS. Esse servidor fornece a tradução dos nomes de host em endereços IP na sua rede.

HTTP e HTTPS

O HTTPS é um protocolo que fornece criptografia para solicitações de páginas de usuários e para as páginas retornadas pelo servidor Web. A troca de informações de criptografia é regida pelo uso de um certificado HTTPS que garante a autenticidade do servidor.

Para usar HTTPS no dispositivo, é necessário instalar certificado HTTPS. Vá para **System > Security (Sistema > Segurança)** para criar e instalar certificados.

Allow access through (Permitir acesso via): Selecione se um usuário tem permissão para se conectar ao dispositivo via protocolos **HTTP**, **HTTPS** ou **HTTP and HTTPS (HTTP e HTTPS)**.

Observação

Se você exibir páginas da Web criptografadas via HTTPS, talvez haja uma queda no desempenho, especialmente quando uma página é solicitada pela primeira vez.

HTTP port (Porta HTTP): Insira a porta HTTP que será usada. O dispositivo permite a porta 80 ou qualquer porta no intervalo 1024 – 65535. Se você estiver conectado como um administrador, também poderá inserir qualquer porta no intervalo 1 – 1023. Se você usar uma porta nesse intervalo, receberá um aviso.

HTTPS port (Porta HTTPS): Insira a porta HTTPS que será usada. O dispositivo permite a porta 443 ou qualquer porta no intervalo 1024 – 65535. Se você estiver conectado como um administrador, também poderá inserir qualquer porta no intervalo 1 – 1023. Se você usar uma porta nesse intervalo, receberá um aviso.

Certificate (Certificado): Selecione um certificado para ativar o HTTPS para o dispositivo.

Protocolos de descoberta de rede

Bonjour®: Ative para permitir a descoberta automática na rede.

Nome Bonjour: Insira um nome amigável para ser visível na rede. O nome padrão é o nome do dispositivo e seu endereço MAC.

UPnP®: Ative para permitir a descoberta automática na rede.

Nome UPnP: Insira um nome amigável para ser visível na rede. O nome padrão é o nome do dispositivo e seu endereço MAC.

WS-Discovery: Ative para permitir a descoberta automática na rede.

LLDP e CDP: Ative para permitir a descoberta automática na rede. Desligar as configurações LLDP e o CDP pode afetar a negociação de energia PoE. Para resolver quaisquer problemas com a negociação de energia PoE, configure a chave PoE somente para negociação de energia PoE de hardware.

Proxies globais

Http proxy (Proxy Http): Especifique um host proxy global ou um endereço IP de acordo com o formato permitido.

Https proxy (Proxy Https): Especifique um host proxy global ou um endereço IP de acordo com o formato permitido.

Formatos permitidos para proxies http e https:

- http(s)://host:port
- http(s)://user@host:port
- http(s)://user:pass@host:port

Observação

Reinicie o dispositivo para aplicar as configurações de proxy global.

No proxy (Nenhum proxy): use **No proxy (Nenhum proxy)** para ignorar os proxies globais. Digite uma das opções da lista ou várias opções separadas por vírgula:

- Deixar vazio
- Especificar um endereço IP
- Especificar um endereço IP no formato CIDR
- Especifique um nome de domínio, por exemplo: www.<nome de domínio>.com
- Especifique todos os subdomínios em um domínio específico, por exemplo, .<nome de domínio>.com

Conexão com a nuvem com apenas um clique

O One-Click Cloud Connect (O3C), em conjunto com um serviço O3C, fornece acesso via Internet fácil e seguro a vídeo ao vivo e gravado a partir de qualquer local. Para obter mais informações, consulte *axis.com/end-to-end--solutions/hosted-services*.

Allow O3C (Permitir O3):

- **Um clique**: Esta é a opção padrão. Para se conectar ao O3C, pressione o botão de controle no dispositivo. Dependendo do modelo do dispositivo, pressione e solte ou pressione e segure, até que o LED status pisque. Registre o dispositivo no serviço O3C dentro de 24 horas para ativar **Always (Sempre)** e permanecer conectado. Se não se registrar, o dispositivo será desconectado do O3C.
- **Sempre**: O dispositivo tenta continuamente conectar a um serviço O3C pela Internet. Depois de registrar o dispositivo, ele permanece conectado. Use essa opção se o botão de controle estiver fora de alcance.
- **Não**: Desconecta o serviço O3C.

Proxy settings (Configurações de proxy): Se necessário, insira as configurações de proxy para conectar ao servidor proxy.

Host: Insira o endereço do servidor proxy.

Porta: Insira o número da porta usada para acesso.

Login e **Senha**: Se necessário, insira um nome de usuário e uma senha para o servidor proxy.

Authentication method (Método de autenticação):

- **Básico**: Este método é o esquema de autenticação mais compatível para HTTP. Ele é menos seguro do que o método de **Digest**, pois ele envia o nome de usuário e a senha não criptografados para o servidor.
- **Digest**: Esse método é mais seguro porque sempre transfere a senha criptografada pela rede.
- **Auto**: Essa opção permite que o dispositivo selecione o método de autenticação automaticamente dependendo dos métodos suportados. Ela prioriza o método **Digest** sobre o método **Básico**.

Owner authentication key (OAK) (Chave de autenticação do proprietário (OAK): Clique em **Get key (Obter chave)** para buscar a chave de autenticação do proprietário. Isso só será possível se o dispositivo estiver conectado à Internet sem um firewall ou proxy.

SNMP

O Simple Network Management Protocol (SNMP) possibilita o acesso e o gerenciamento remotos de dispositivos de rede.

SNMP: Selecione a versão de SNMP que deve ser utilizada.

- **v1 and v2c (v1 e v2c)**:
  - **Read community (Comunidade de leitura)**: Insira o nome da comunidade que tem acesso somente de leitura a todos os objetos SNMP suportados. O valor padrão é **public**.
  - **Write community (Comunidade de gravação)**: Insira o nome da comunidade que tem acesso de leitura ou gravação em todos os objetos SNMP suportados (exceto objetos somente leitura). O valor padrão é **gravação**.
  - **Activate traps (Ativar interceptações)**: Ative para ativar o relatório de interceptações. O dispositivo usa interceptações para enviar mensagens sobre eventos importantes ou alterações de status para um sistema de gerenciamento. Na interface Web, você pode configurar interceptações para SNMP v1 e v2c. As interceptações serão desativadas automaticamente se você mudar para SNMP v3 ou desativar o SNMP. Se você usa SNMP v3, é possível configurar interceptações via aplicativo de gerenciamento do SNMP v3.
  - **Trap address (Endereço da interceptação)**: Insira o endereço IP ou nome de host do servidor de gerenciamento.
  - **Trap community (Comunidade de interceptação)**: Insira a comunidade que é usada quando o dispositivo envia uma mensagem de interceptação para o sistema de gerenciamento.
  - **Traps (Interceptações)**:
    - **Cold start (Partida a frio)**: Envia uma mensagem de interceptação quando o dispositivo é iniciado.
    - **Link up (Link ativo)**: Envia uma mensagem de interceptação quando um link muda de inativo para ativo.
    - **Link down (Link inativo)**: Envia uma mensagem de interceptação quando um link muda de ativo para inativo.
    - **Falha de autenticação**: Envia uma mensagem de interceptação quando uma tentativa de autenticação falha.

Observação

Todas as interceptações MIB de vídeo Axis são habilitados quando você ativa as interceptações SNMP v1 e v2c. Para obter mais informações, consulte *AXIS OS portal > SNMP*.

- **v3**: O SNMP v3 é uma versão mais segura que fornece criptografia e senhas seguras. Para usar o SNMP v3, recomendamos ativar o HTTPS, pois as senhas serão enviadas via HTTPS. Isso também impede que partes não autorizadas acessem interceptações SNMP v1 e v2c não criptografadas. Se você usa SNMP v3, é possível configurar interceptações via aplicativo de gerenciamento do SNMP v3.
  - **Password for the account "initial" (Senha para a conta "initial")**: Insira a senha do SNMP para a conta chamada "initial". Embora a senha possa ser enviada sem ativar o HTTPS, isso não é recomendável. A senha do SNMP v3 só pode ser definida uma vez e, preferivelmente, quando o HTTPS está ativado. Após a senha ser definida, o campo de senha não será mais exibido. Para definir a senha novamente, o dispositivo deverá ser redefinido para as configurações padrões de fábrica.

Segurança

Certificados

Certificados são usados para autenticar dispositivos em uma rede. O dispositivo oferece suporte a dois tipos de certificados:

- **Certificados cliente/servidor**
  Um certificado cliente/servidor valida a identidade do produto e pode ser autoassinado ou emitido por uma autoridade de certificação (CA). Um certificado autoassinado oferece proteção limitada e pode ser usado antes que um certificado emitido por uma CA tenha sido obtido.
- **Certificados CA**
  Você pode usar um certificado de CA para autenticar um certificado de par, por exemplo, para validar a identidade de um servidor de autenticação quando o dispositivo se conecta a uma rede protegida por IEEE 802.1X. O dispositivo possui vários certificados de CA pré-instalados.

Os seguintes formatos são aceitos:

- Formatos de certificado: .PEM, .CER e .PFX
- Formatos de chave privada: PKCS#1 e PKCS#12

Importante

Se você redefinir o dispositivo para o padrão de fábrica, todos os certificados serão excluídos. Quaisquer certificados de CA pré-instalados serão reinstalados.

Adicionar certificado : Clique para adicionar um certificado. Um guia passo a passo é aberto.

- **Mais** : Mostrar mais campos para preencher ou selecionar.
- **Secure keystore (Armazenamento de chaves seguro)**: Selecione para usar **Trusted Execution Environment (SoC TEE)**, **Secure element** (Elemento seguro) ou **Trusted Platform Module 2.0** para armazenar de forma segura a chave privada. Para obter mais informações sobre qual armazenamento de chaves seguro selecionar, acesse *help.axis.com/axis-os#cryptographic-support*.
- **Tipo da chave**: Selecione o algoritmo de criptografia padrão ou diferente na lista suspensa para proteger o certificado.

O menu de contexto contém:

- **Certificate information (Informações do certificado)**: Exiba as propriedades de um certificado instalado.
- **Delete certificate (Excluir certificado)**: Exclua o certificado.
- **Create certificate signing request (Criar solicitação de assinatura de certificado)**: Crie uma solicitação de assinatura de certificado para enviar a uma autoridade de registro para se aplicar para um certificado de identidade digital.

Secure keystore (Armazenamento de chaves seguro) :

- **Trusted Execution Environment (SoC TEE)**: Selecione para usar o SoC TEE para armazenamento de chaves seguro.
- **Secure element (CC EAL6+) (Elemento seguro (CC EAL6+))**: Selecione para usar o elemento seguro no armazenamento de chaves seguro.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Nível 2)**: Selecione para usar TPM 2.0 para armazenamento de chaves seguro.

Política criptográfica

A política criptográfica define como a criptografia é usada para proteger os dados.

Active (Ativa): Selecione a política criptográfica a ser aplicada ao dispositivo:

- **Default — OpenSSL (Padrão - OpenSSL)**: segurança e desempenho equilibrados para uso geral.
- **FIPS — Policy to comply with FIPS 140–2 (FIPS - Política de conformidade com FIPS 140-2)**: Criptografia em conformidade com o FIPS 140-2 para indústrias regulamentadas.

Controle de acesso à rede e criptografia

IEEE 802.1x

O IEEE 802.1x é um padrão do IEEE para controle de admissão em redes baseado em portas que fornece autenticação segura de dispositivos em rede com e sem fio. O IEEE 802.1x é baseado no EAP (Extensible Authentication Protocol).

Para acessar uma rede protegida pelo IEEE 802.1x, os dispositivos de rede devem se autenticar. A autenticação é executada por um servidor de autenticação, geralmente, um servidor RADIUS (por exemplo, FreeRADIUS e Microsoft Internet Authentication Server).

IEEE 802.1AE MACsec

O IEEE 802.1AE MACsec é um padrão IEEE para segurança de controle de acesso à mídia (MAC) que define a confidencialidade e integridade de dados sem conexão para protocolos independentes de acesso à mídia.

Certificados

Quando configurado sem um certificado de CA, a validação do certificado do servidor é desativada e o dispositivo tenta se autenticar independentemente da rede à qual está conectado.

Ao usar um certificado, na implementação da Axis, o dispositivo e o servidor de autenticação se autenticam com certificados digitais usando EAP-TLS (Extensible Authentication Protocol – Transport Layer Security).

Para permitir que o dispositivo acesse uma rede protegida por certificados, é necessário instalar um certificado de cliente assinado no dispositivo.

Authentication method (Método de autenticação): Selecione um tipo de EAP usado para autenticação.

Client certificate (Certificado de cliente): Selecione um certificado de cliente para usar o IEEE 802.1x. O servidor de autenticação usa o certificado para validar a identidade do cliente.

CA certificates (Certificados CA): Selecione certificados CA para validar identidade do servidor de autenticação. Quando nenhum certificado é selecionado, o dispositivo tenta se autenticar independentemente da rede à qual está conectado.

EAP identity (Identidade EAP): Insira a identidade do usuário associada ao seu certificado de cliente.

EAPOL version (Versão EAPOL): Selecione a versão EAPOL que é usada no switch de rede.

Use IEEE 802.1x (Usar IEEE 802.1x): Selecione para usar o protocolo IEEE 802.1 x.

Essas configurações só estarão disponíveis se você usar **IEEE 802.1x PEAP-MSCHAPv2** como método de autenticação:

- **Senha**: Insira a senha para sua identidade de usuário.
- **Peap version (Versão do Peap)**: Selecione a versão do Peap que é usada no switch de rede.
- **Label (Rótulo)**: Selecione 1 para usar a criptografia EAP do cliente; selecione 2 para usar a criptografia PEAP do cliente. Selecione o rótulo que o switch de rede usa ao utilizar a versão 1 do Peap.

Essas configurações só estarão disponíveis se você usar o **IEEE 802.1ae MACsec (CAK estático/chave pré-compartilhada)** como método de autenticação:

- **Nome da chave de associação de conectividade do acordo de chaves**: Insira o nome da associação de conectividade (CKN). Deve ter de 2 a 64 (divisível por 2) caracteres hexadecimais. O CKN deve ser configurado manualmente na associação de conectividade e deve corresponder em ambas as extremidades do link para ativar inicialmente o MACsec.
- **Chave de associação de conectividade do acordo de chaves**: Insira a chave da associação de conectividade (CAK). Ela deve ter 32 ou 64 caracteres hexadecimais. O CAK deve ser configurado manualmente na associação de conectividade e deve corresponder em ambas as extremidades do link para ativar inicialmente o MACsec.

Impedir ataques de força bruta

Blocking (Bloqueio): Ative para bloquear ataques de força bruta. Um ataque de força bruta usa tentativa e erro para adivinhar informações de login ou chaves de criptografia.

Blocking period (Período de bloqueio): Insira o número de segundos para bloquear um ataque de força bruta.

Blocking conditions (Condições de bloqueio): Insira o número de falhas de autenticação permitidas por segundo antes do início do bloco. Você pode definir o número de falhas permitidas em nível de página ou em nível de dispositivo.

Firewall

Firewall: Ative para ativar o firewall.

Default Policy (Política padrão): Selecione como deseja que o firewall trate as solicitações de conexão não cobertas por regras.

- **ACCEPT (ACEITAR):** Permite todas as conexões com o dispositivo. Essa opção é definida por padrão.
- **DROP (DESCARTAR):** Bloqueia todas as conexões com o dispositivo.

Para criar exceções à política padrão, você pode criar regras que permitem ou bloqueiam conexões com o dispositivo a partir de endereços, protocolos e portas específicos.

+ New rule (+ Nova regra): clique para criar uma regra.

Rule type (Tipo de regra):

- **FILTER (FILTRAR)**: Selecione para permitir ou bloquear conexões de dispositivos que correspondam aos critérios definidos na regra.
  - **Policy (Política)**: Selecione **Accept (Aceitar)** ou **Drop (Descartar)** a regra de firewall.
  - **IP range (Faixa IP)**: Selecione para especificar uma faixa de endereços a serem permitidos ou bloqueados. Use IPv4/IPv6 em **Start (Início)** e **End (Fim)**.
  - **Endereço IP**: Digite um endereço que você deseja permitir ou bloquear. Use o formato IPv4/ /IPv6 ou CIDR.
  - **Protocol (Protocolo)**: Selecione um protocolo de rede (TCP, UDP ou ambos) para permitir ou bloquear. Se você selecionar um protocolo, também deverá especificar uma porta.
  - **MAC**: Digite o endereço MAC de um dispositivo que você deseja permitir ou bloquear.
  - **Port range (Faixa de portas)**: Selecione para especificar a faixa de portas a serem permitidas ou bloqueadas. Adicione-as a **Start (Início)** e **End (Fim)**.
  - **Porta**: Insira um número de porta que você deseje permitir ou bloquear. Os números de portas devem estar entre 1 e 65535.
  - **Traffic type (Tipo de tráfego)**: Selecione o tipo de tráfego que você deseja permitir ou bloquear.
    - **UNICAST**: Tráfego de um único remetente para um único destinatário.
    - **BROADCAST**: Tráfego de um único remetente para todos os dispositivos na rede.
    - **MULTICAST**: Tráfego de um ou mais remetentes para um ou mais destinatários.
- **LIMIT (LIMITAR)**: Selecione para aceitar conexões de dispositivos que correspondam aos critérios definidos na regra, mas aplique limites para reduzir o tráfego excessivo.
  - **IP range (Faixa IP)**: Selecione para especificar uma faixa de endereços a serem permitidos ou bloqueados. Use IPv4/IPv6 em **Start (Início)** e **End (Fim)**.
  - **Endereço IP**: Digite um endereço que você deseja permitir ou bloquear. Use o formato IPv4/ /IPv6 ou CIDR.
  - **Protocol (Protocolo)**: Selecione um protocolo de rede (TCP, UDP ou ambos) para permitir ou bloquear. Se você selecionar um protocolo, também deverá especificar uma porta.
  - **MAC**: Digite o endereço MAC de um dispositivo que você deseja permitir ou bloquear.
  - **Port range (Faixa de portas)**: Selecione para especificar a faixa de portas a serem permitidas ou bloqueadas. Adicione-as a **Start (Início)** e **End (Fim)**.
  - **Porta**: Insira um número de porta que você deseje permitir ou bloquear. Os números de portas devem estar entre 1 e 65535.
  - **Unit (Unidade)**: Selecione o tipo de conexão a ser permitida ou bloqueada.
  - **Period (Período)**: Selecione o período de tempo relacionado a **Amount (Quantidade)**.
  - **Amount (Quantidade)**: Defina o número máximo de vezes que um dispositivo tem permissão para se conectar dentro do período definido em **Period (Período)**. O valor máximo é 65535.

- **Burst (Surto)**: Insira o número de conexões que podem exceder o valor definido em **Amount (Quantidade)** uma vez durante o período definido em **Period (Período)**. Quando o número for atingido, somente a quantidade definida durante o período definido será permitida.
- **Traffic type (Tipo de tráfego)**: Selecione o tipo de tráfego que você deseja permitir ou bloquear.
  - **UNICAST**: Tráfego de um único remetente para um único destinatário.
  - **BROADCAST**: Tráfego de um único remetente para todos os dispositivos na rede.
  - **MULTICAST**: Tráfego de um ou mais remetentes para um ou mais destinatários.

Test rules (Testar regras): Clique para testar as regras que você definiu.

- **Test time in seconds (Tempo de teste em segundos)**: Defina um limite de tempo para testar as regras.
- **Roll back (Reverter)**: Clique para reverter o firewall ao seu estado anterior, antes de testar as regras.
- **Apply rules (Aplicar regras)**: Clique para ativar as regras sem testar. Não recomendamos fazer isso.

Certificado do AXIS OS com assinatura personalizada

Para instalar o software de teste ou outro software personalizado da Axis no dispositivo, certificado do AXIS OS com assinatura personalizada é necessário. O certificado verifica se o software é aprovado pelo proprietário do dispositivo e pela Axis. O software só pode ser executado em um dispositivo específico identificado por seu número de série e ID de chip exclusivos. Somente a Axis pode criar certificados do AXIS OS com assinatura personalizada, pois é a Axis que possui a chave para assiná-los.

Install (Instalar): Clique para instalar o certificado. É necessário instalar o certificado antes de instalar o software.

⋮ O menu de contexto contém:

- **Delete certificate (Excluir certificado)**: Exclua o certificado.

Contas

Contas

Adicionar conta: Clique para adicionar uma nova conta. É possível adicionar até 100 contas.

Account (Conta): Insira um nome de conta exclusivo.

New password (Nova senha): Insira uma senha para o nome da conta. As senhas devem conter 1 a 64 caracteres de comprimento. Somente caracteres ASCII imprimíveis (código 32 a 126) são permitidos na senha, por exemplo, letras, números, pontuação e alguns símbolos.

Repeat password (Repetir senha): Insira a mesma senha novamente.

Privileges (Privilégios):

- **Administrator (Administrador)**: Tem acesso irrestrito a todas as configurações. Os administradores também podem adicionar, atualizar e remover outras contas.
- **Operator (Operador)**: Tem acesso a todas as configurações, exceto:
  - Todas as configurações do **System (Sistema)**.
- **Viewer (Visualizador)**: Não tem acesso para alterar as configurações.

O menu de contexto contém:

Update account (Atualizar conta): Edite as propriedades da conta.

Delete account (Excluir conta): Exclua a conta. Não é possível excluir a conta root.

Acesso anônimo

Allow anonymous viewing (Permitir visualização anônima): Ative para permitir que qualquer pessoa acesse o dispositivo como um visualizador sem precisar fazer login com uma conta.

Permitir operação de PTZ anônima : Ative para permitir que usuários anônimos façam pan, tilt e zoom da imagem.

Contas SSH

Adicionar conta SSH: Clique para adicionar uma nova conta SSH.

- **Enable SSH (Ativar SSH)**: Ative para usar o serviço SSH.

Account (Conta): Insira um nome de conta exclusivo.

New password (Nova senha): Insira uma senha para o nome da conta. As senhas devem conter 1 a 64 caracteres de comprimento. Somente caracteres ASCII imprimíveis (código 32 a 126) são permitidos na senha, por exemplo, letras, números, pontuação e alguns símbolos.

Repeat password (Repetir senha): Insira a mesma senha novamente.

Comentário: Insira um comentário (opcional).

O menu de contexto contém:

Update SSH account (Atualizar conta SSH): Edite as propriedades da conta.

Delete SSH account (Excluir conta SSH): Exclua a conta. Não é possível excluir a conta root.

Virtual host (Host virtual)

Add virtual host (Adicionar host virtual): clique para adicionar um novo host virtual.

Enabled (Ativado): selecione para usar este host virtual.

Server name (Nome do servidor): insira o nome do servidor. Use somente números 0 – 9, letras A – Z e hífen (-).

Porta: insira a porta à qual o servidor está conectado.

Tipo: selecione o tipo de autenticação que será usada. Selecione entre **Basic**, **Digest** e **Open ID**.

O menu de contexto contém:

- **Update (Atualizar)**: atualizar o host virtual.
- **Excluir**: excluir o host virtual.

Disabled (Desativado): o servidor está desativado.

Configuração de concessão de credenciais de cliente

Reivindicação de administrador: Insira um valor para a função de administrador.

Verification URI (URI de verificação): Insira o link Web para a autenticação do ponto de extremidade de API.

Reivindicação de operador: Insira um valor para a função do operador.

Exigir reivindicação: Insira os dados que deveriam estar no token.

Reivindicação de visualizador: insira o valor da função de visualizador.

Save (Salvar): Clique para salvar os valores.

Configuração de OpenID

Importante

Se você não puder usar OpenID para fazer login, use as credenciais Digest ou Básicas que você usou quando configurou OpenID para fazer login.

Client ID (ID do cliente): Insira o nome de usuário de OpenID.

Proxy de saída: insira o endereço proxy da conexão OpenID para usar um servidor proxy.

Reivindicação de administrador: Insira um valor para a função de administrador.

URL do provedor: Insira o link Web para a autenticação do ponto de extremidade de API. O formato deve ser https://[inserir URL]/.bem conhecido/openid-configuration

Reivindicação de operador: Insira um valor para a função do operador.

Exigir reivindicação: Insira os dados que deveriam estar no token.

Reivindicação de visualizador: insira o valor da função de visualizador.

Remote user (Usuário remoto): insira um valor para identificar usuários remotos. Isso ajudará a exibir o usuário atual na interface Web do dispositivo.

Scopes (Escopos): Escopos opcionais que poderiam fazer parte do token.

Segredo do cliente: Insira a senha OpenID novamente

Save (Salvar): Clique em para salvar os valores de OpenID.

Ativar OpenID: Ative para fechar a conexão atual e permita a autenticação do dispositivo via URL do provedor.

Eventos

Regras

Uma regra define as condições que fazem com que o produto execute uma ação. A lista mostra todas as regras configuradas no produto no momento.

Observação

Você pode criar até 256 regras de ação.

Adicionar uma regra: Crie uma regra.

Nome: Insira um nome para a regra.

Wait between actions (Aguardar entre ações): insira o tempo mínimo (hh:mm:ss) que deve passar entre ativações de regras. Ela será útil se a regra for ativada, por exemplo, em condições de modo diurno/noturno, para evitar que pequenas mudanças de iluminação durante o nascer e o pôr do sol ativem a regra várias vezes.

Condition (Condição): selecione uma condição na lista. Uma condição deve ser atendida para que o dispositivo execute uma ação. Se várias condições forem definidas, todas elas deverão ser atendidas para acionar a ação. Para obter informações sobre condições específicas, consulte *Introdução às regras de eventos*.

Use this condition as a trigger (Usar esta condição como acionador): selecione para que essa primeira função opere apenas como acionador inicial. Isso significa que, uma vez que a regra for ativada, ela permanecerá ativa enquanto todas as outras condições forem atendidas, independentemente do estado da primeira condição. Se você não marcar essa opção, a regra simplesmente será ativada quando todas as condições forem atendidas.

Invert this condition (Inverter esta condição): marque se você quiser que a condição seja o contrário de sua seleção.

Adicionar uma condição: clique para adicionar uma condição.

Action (Ação): selecione uma ação na lista e insira as informações necessárias. Para obter informações sobre ações específicas, consulte *Introdução às regras de eventos*.

Seu produto pode ter algumas das seguintes regras pré-configuradas:

Front-facing LED Activation (Ativação do LED frontal): Stream ao vivo: quando o microfone está ligado e um stream ao vivo é recebido, o LED frontal no dispositivo de áudio torna-se verde.

Front-facing LED Activation (Ativação do LED frontal): Gravação : quando o microfone está ligado e uma gravação está em andamento, o LED frontal no dispositivo de áudio torna-se verde.

Front-facing LED Activation (Ativação do LED frontal): SIP : Quando o microfone está ligado e uma chamada SIP está ativa, o LED frontal no dispositivo de áudio torna-se verde. O SIP deve ser ativado no dispositivo de áudio para acionar este evento.

Pre-announcement tone (Tom de pré-comunicado): reproduz o tom ao receber uma chamada: Quando uma chamada SIP é feita para o dispositivo de áudio, o dispositivo toca um clipe de áudio pré-definido. É necessário ativar o SIP para o dispositivo de áudio. Para que o chamador SIP ouça um tom de toque enquanto o dispositivo toca o clipe de áudio, é necessário configurar a conta SIP para o dispositivo de áudio para não atender à chamada automaticamente.

Pre-announcement tone (Tom de pré-comunicado): atenda a chamada após o tom de chamada recebida: Quando o clipe de áudio termina, a chamada SIP recebida é respondida. É necessário ativar o SIP para o dispositivo de áudio.

Loud ringer (Campainha alta): Quando uma chamada SIP é feita para o dispositivo de áudio, um clipe de áudio pré-definido é tocado enquanto a regra está ativa. É necessário ativar o SIP para o dispositivo de áudio.

Destinatários

Você pode configurar seu dispositivo para notificar os destinatários sobre eventos ou enviar arquivos.

Observação

Se você configurar seu dispositivo para usar FTP ou SFTP, não altere nem remova o número de sequência exclusivo que é adicionado aos nomes dos arquivos. Se fizer isso, apenas uma imagem por evento poderá ser enviada.

A lista mostra todos os destinatários atualmente configurados no produto, juntamente com informações sobre suas configurações.

Observação

É possível criar até 20 destinatários.

Add a recipient (Adicionar um destinatário): clique para adicionar um destinatário.

Nome: insira um nome para o destinatário.

Tipo: selecione na lista:

- FTP
  - **Host**: insira o endereço IP ou o nome de host do servidor. Se você inserir um nome de host, verifique se um servidor DNS está especificado em **System > Network > IPv4 and IPv6 (Sistema > Rede > IPv4 e IPv6)**.
  - **Porta**: Insira o número da porta usada pelo servidor FTP. O padrão é 21.
  - **Folder (Pasta)**: insira o caminho para o diretório em que deseja armazenar arquivos. Se esse diretório ainda não existir no servidor FTP, você receberá uma mensagem de erro ao fazer upload de arquivos.
  - **Username (Nome de usuário)**: insira o nome de usuário para o login.
  - **Senha**: insira a senha para o login.
  - **Use temporary file name (Usar nome de arquivo temporário)**: marque para carregar arquivos com nomes temporários e gerados automaticamente. Os arquivos serão renomeados para os nomes desejados quando o upload for concluído. Se o upload for cancelado/interrompido, nenhum arquivo será corrompido. No entanto, provavelmente você ainda obterá os arquivos temporários. Dessa forma, você saberá que todos os arquivos com o nome desejado estão corretos.
  - **Use passive FTP (Usar FTP passivo)**: Em circunstâncias normais, o produto simplesmente solicita que o servidor FTP de destino abra a conexão de dados. O dispositivo inicia ativamente as conexões de controle de FTP e dados para o servidor de destino. Isso é normalmente necessário quando há um firewall entre o dispositivo e o servidor FTP de destino.
- HTTP
  - **URL**: Insira o endereço de rede do servidor HTTP e o script que cuidará da solicitação. Por exemplo, http://192.168.254.10/cgi-bin/notify.cgi.
  - **Username (Nome de usuário)**: insira o nome de usuário para o login.
  - **Senha**: insira a senha para o login.
  - **Proxy**: ative e insira as informações necessárias se houver a necessidade de passar por um servidor proxy para se conectar ao servidor HTTP.
- HTTPS
  - **URL**: Insira o endereço de rede do servidor HTTPS e o script que cuidará da solicitação. Por exemplo, https://192.168.254.10/cgi-bin/notify.cgi.
  - **Validate server certificate (Validar certificado do servidor)**: marque para validar o certificado que foi criado pelo servidor HTTPS.
  - **Username (Nome de usuário)**: insira o nome de usuário para o login.
  - **Senha**: insira a senha para o login.
  - **Proxy**: ative e insira as informações necessárias se houver a necessidade de passar por um servidor proxy para se conectar ao servidor HTTPS.
- Armazenamento de rede
  Você pode adicionar armazenamento de rede, como um NAS (Network Attached Storage), e utilizá-lo como destinatário para armazenar arquivos. Os arquivos são armazenados no formato Matroska (MKV).
  - **Host**: Insira o endereço IP ou o nome de host do armazenamento de rede.
  - **Compartilhamento**: Insira o nome do compartilhamento no host.

- **Folder (Pasta)**: insira o caminho para o diretório em que deseja armazenar arquivos.
- **Username (Nome de usuário)**: insira o nome de usuário para o login.
- **Senha**: insira a senha para o login.

- SFTP
  - **Host**: insira o endereço IP ou o nome de host do servidor. Se você inserir um nome de host, verifique se um servidor DNS está especificado em **System > Network > IPv4 and IPv6 (Sistema > Rede > IPv4 e IPv6)**.
  - **Porta**: Insira o número da porta usada pelo servidor SFTP. O padrão é 22.
  - **Folder (Pasta)**: insira o caminho para o diretório em que deseja armazenar arquivos. Se esse diretório ainda não existir no servidor SFTP, você receberá uma mensagem de erro ao fazer upload de arquivos.
  - **Username (Nome de usuário)**: insira o nome de usuário para o login.
  - **Senha**: insira a senha para o login.
  - **SSH host public key type (MD5) (Tipo de chave pública do host SSH [MD5])**: insira a impressão digital da chave pública do host remoto (sequência de 32 dígitos hexadecimais). O cliente SFTP oferece suporte a servidores SFTP que utilizam SSH-2 com os tipos de chave de host RSA, DSA, ECDSA e ED25519. RSA é o método preferido durante a negociação, seguido por ECDSA, ED25519 e DSA. Certifique-se de inserir a chave de host MD5 certa que é usada pelo seu servidor SFTP. Embora o dispositivo Axis ofereça suporte a chaves de hash MD5 e SHA-256, recomenda-se usar a SHA-256 devido à segurança mais forte do que o MD5. Para obter mais informações sobre como configurar um servidor SFTP com um dispositivo Axis, acesse o *Portal do AXIS OS*.
  - **SSH host public key type (SHA256) (Tipo de chave pública do host SSH [SHA256])**: insira a impressão digital da chave pública do host remoto (string codificada em Base64 com 43 dígitos). O cliente SFTP oferece suporte a servidores SFTP que utilizam SSH-2 com os tipos de chave de host RSA, DSA, ECDSA e ED25519. RSA é o método preferido durante a negociação, seguido por ECDSA, ED25519 e DSA. Certifique-se de inserir a chave de host MD5 certa que é usada pelo seu servidor SFTP. Embora o dispositivo Axis ofereça suporte a chaves de hash MD5 e SHA-256, recomenda-se usar a SHA-256 devido à segurança mais forte do que o MD5. Para obter mais informações sobre como configurar um servidor SFTP com um dispositivo Axis, acesse o *Portal do AXIS OS*.
  - **Use temporary file name (Usar nome de arquivo temporário)**: marque para carregar arquivos com nomes temporários e gerados automaticamente. Os arquivos serão renomeados para os nomes desejados quando o upload for concluído. Se o upload for cancelado ou interrompido, nenhum arquivo será corrompido. No entanto, provavelmente você ainda obterá os arquivos temporários. Dessa forma, você saberá que todos os arquivos com o nome desejado estão corretos.

- SIP ou VMS :
  SIP: Selecione para fazer uma chamada SIP.
  VMS: Selecione para fazer uma chamada VMS.
  - **From SIP account (Da conta SIP)**: selecione na lista.
  - **To SIP address (Para endereço SIP)**: Insira o endereço SIP.
  - **Teste**: Clique para testar se suas configurações de chamada funcionam.
- **E-mail**
  - **Enviar email para**: insira o endereço para enviar os emails. Para inserir vários emails, use vírgulas para separá-los.
  - **Enviar email de**: insira o endereço de email do servidor de envio.
  - **Username (Nome de usuário)**: insira o nome de usuário para o servidor de email. Deixe esse campo em branco se o servidor de email não precisar de autenticação.

- **Senha**: insira a senha para o servidor de email. Deixe esse campo em branco se o servidor de email não precisar de autenticação.
- **Email server (SMTP) (Servidor de email (SMTP))**: Insira o nome do servidor SMTP. Por exemplo, smtp.gmail.com, smtp.mail.yahoo.com.
- **Porta**: Insira o número da porta do servidor SMTP usando valores na faixa 0 – 65535. O valor padrão é 587.
- **Criptografia**: para usar criptografia, selecione SSL ou TLS.
- **Validate server certificate (Validar certificado do servidor)**: se você usar criptografia, marque para validar a identidade do dispositivo. O certificado pode ser autoassinado ou emitido por uma Autoridade de Certificação (CA).
- **POP authentication (Autenticação POP)**: Ative para inserir o nome do servidor POP. Por exemplo, pop.gmail.com.

Observação

Alguns provedores de email possuem filtros que impedem que os usuários recebam ou exibam anexos grandes, emails recorrentes e outros semelhantes. Verifique a política de segurança do provedor de email para evitar que sua conta de email seja bloqueada ou que as mensagens que você está esperando não sejam recebidas.

- **TCP**
  - **Host**: insira o endereço IP ou o nome de host do servidor. Se você inserir um nome de host, verifique se um servidor DNS está especificado em **System > Network > IPv4 and IPv6 (Sistema > Rede > IPv4 e IPv6)**.
  - **Porta**: Insira o número da porta usada para acessar o servidor.

Testar: clique para testar a configuração.

⋮ O menu de contexto contém:

View recipient (Exibir destinatário): clique para exibir todos os detalhes do destinatário.

Copy recipient (Copiar destinatário): clique para copiar um destinatário. Ao copiar, você pode fazer alterações no novo destinatário.

Delete recipient (Excluir destinatário): clique para excluir o destinatário permanentemente.

Programações

Agendamentos e pulsos podem ser usados como condições em regras. A lista mostra todas os agendamentos e pulsos configurados no momento no produto, juntamente com várias informações sobre suas configurações.

+ **Adicionar agendamento**: clique para criar um cronograma ou pulso.

Acionadores manuais

É possível usar o acionador manual para acionar manualmente uma regra. O acionador manual pode ser usado, por exemplo, para validar ações durante a instalação e a configuração do produto.

MQTT

O MQTT (Message Queuing Telemetry Transport) é um protocolo de troca de mensagens padrão para a Internet das Coisas (IoT). Ele foi desenvolvido para integração simplificada com a IoT e é usado em uma ampla variedade de setores para conectar dispositivos remotos com o mínimo de código e largura de banda de rede. O cliente MQTT no software do dispositivo Axis pode simplificar a integração de dados e eventos produzidos no dispositivo a sistemas que não são software de gerenciamento de vídeo (VMS).

Configure o dispositivo como um cliente MQTT. A comunicação MQTT baseia-se em duas entidades, os clientes e o broker. Os clientes podem enviar e receber mensagens. O broker é responsável por rotear mensagens entre os clientes.

Saiba mais sobre MQTT na *Base de conhecimento do AXIS OS*.

ALPN

O ALPN é uma extensão do TLS/SSL que permite a seleção de um protocolo de aplicação durante a fase de handshake da conexão entre o cliente e o servidor. Isso é usado para permitir o tráfego MQTT na mesma porta que é utilizada para outros protocolos, como o HTTP. Em alguns casos, pode não haver uma porta dedicada aberta para a comunicação MQTT. Uma solução nesses casos é usar o ALPN para negociar o uso do MQTT como protocolo de aplicação em uma porta padrão permitida pelos firewalls.

Cliente MQTT

Connect (Conectar): Ative ou desative o cliente MQTT.

Status: Mostra o status atual do cliente MQTT.

Broker

Host: Insira o nome de host ou endereço IP do servidor MQTT.

Protocol (Protocolo): Selecione o protocolo que será usado.

Porta: Insira o número da porta.

- 1883 é o valor padrão para **MQTT sobre TCP**
- 8883 é o valor padrão para **MQTT sobre SSL**
- 80 é o valor padrão para **MQTT sobre WebSocket**
- 443 é o valor padrão para **MQTT sobre WebSocket Secure**

Protocol ALPN: Insira o nome do protocolo ALPN fornecido pelo seu provedor de broker de MQTT. Isso se aplica apenas com MQTT sobre SSL e MQTT sobre o WebSocket Secure.

Username (Nome de usuário): Insira o nome de usuário que será usado pelo cliente para acessar o servidor.

Senha: Insira uma senha para o nome de usuário.

Client ID (ID do cliente): Insira um ID de cliente. O identificador do cliente é enviado para o servidor quando o cliente se conecta a ele.

Clean session (Limpar sessão): Controla o comportamento na conexão e na desconexão. Quando selecionada, as informações de estado são descartadas na conexão e desconexão.

HTTP proxy (Proxy HTTP): Um URL com comprimento máximo de 255 bytes. Deixe o campo vazio se não quiser usar um proxy HTTP.

HTTPS proxy (Proxy HTTPS): Um URL com comprimento máximo de 255 bytes. Deixe o campo vazio se não quiser usar um proxy HTTPS.

Keep alive interval (Intervalo de Keep Alive): Permite que o cliente detecte quando o servidor não está mais disponível sem que seja necessário aguardar o longo tempo limite de TCP/IP.

Timeout (Tempo limite): O intervalo de tempo em segundos para permitir que uma conexão seja concluída. Valor padrão: 60

Device topic prefix (Prefixo do tópico do dispositivo): Usado nos valores padrão para o tópico na mensagem de conexão e na mensagem de LWT na guia **MQTT client (Cliente MQTT)** e nas condições de publicação na guia **MQTT publication (Publicação MQTT)**.

Reconnect automatically (Reconectar automaticamente): Especifica se o cliente deve se reconectar automaticamente após uma desconexão.

Mensagem de conexão

Especifica se uma mensagem deve ser enviada quando uma conexão é estabelecida.

Send message (Enviar mensagem): ative para enviar mensagens.

Use default (Usar padrão): Desative para inserir sua própria mensagem padrão.

Topic (Tópico): insira o tópico para a mensagem padrão.

Payload (Carga): insira o conteúdo para a mensagem padrão.

Retain (Reter): selecione para manter o estado do cliente neste **Topic (Tópico)**

QoS: Altere a camada de QoS para o fluxo do pacote.

Mensagem de Último desejo e testamento

A opção Last Will Testament (LWT) permite que um cliente forneça uma prova juntamente com suas credenciais ao conectar ao broker. Se o cliente se desconectar abruptamente em algum momento mais tarde (talvez porque sua fonte de energia seja interrompida), ele pode permitir que o broker envie uma mensagem para outros clientes. Essa mensagem de LWT tem o mesmo formato que uma mensagem comum e é roteada através da mesma mecânica.

Send message (Enviar mensagem): ative para enviar mensagens.

Use default (Usar padrão): Desative para inserir sua própria mensagem padrão.

Topic (Tópico): insira o tópico para a mensagem padrão.

Payload (Carga): insira o conteúdo para a mensagem padrão.

Retain (Reter): selecione para manter o estado do cliente neste **Topic (Tópico)**

QoS: Altere a camada de QoS para o fluxo do pacote.

Publicação MQTT

Use default topic prefix (Usar prefixo de tópico padrão): selecione para usar o prefixo de tópico padrão, o qual é definido com o uso do prefixo de tópico de dispositivo na guia **MQTT client (Cliente MQTT)**.

Include topic name (Incluir nome do tópico): selecione para incluir o tópico que descreve a condição no tópico MQTT.

Include topic namespaces (Incluir namespaces de tópico): selecione para incluir espaços para nome de tópico ONVIF no tópico MQTT.

Include serial number (Incluir número de série): selecione para incluir o número de série do dispositivo na carga MQTT.

Adicionar condição: clique para adicionar uma condição.

Retain (Reter): define quais mensagens MQTT são enviadas como retidas.

- **None (Nenhuma)**: envia todas as mensagens como não retidas.
- **Property (Propriedade)**: envia somente mensagens stateful como retidas.
- **All (Todas)**: envie mensagens stateful e stateless como retidas.

QoS: selecione o nível desejado para a publicação MQTT.

Assinaturas MQTT

Adicionar assinatura: clique para adicionar uma nova assinatura MQTT.

Subscription filter (Filtro de assinatura): insira o tópico MQTT no qual deseja se inscrever.

Use device topic prefix (Usar prefixo de tópico do dispositivo): adicione o filtro de assinatura como prefixo ao tópico MQTT.

Subscription type (Tipo de assinatura):

- **Stateless**: selecione para converter mensagens MQTT em mensagens stateless.
- **Stateful**: selecione para converter mensagens MQTT em condições. A carga é usada como estado.

QoS: selecione o nível desejado para a assinatura MQTT.

SIP

Definições

O Session Initiation Protocol (SIP) é usado para as sessões de comunicação interativa entre os usuários. As sessões podem incluir elementos de áudio e vídeo.

SIP setup assistant (Assistente de configuração de SIP): Clique para definir e configurar o SIP passo a passo.

Enable SIP (Ativar SIP): marque esta opção para possibilitar o início e o recebimento de chamadas SIP.

Permitir chamadas recebidas: Marque esta opção para permitir o recebimento de chamadas de outros dispositivos SIP.

Tratamento da chamada

- **Tempo limite da chamada**: Defina a duração máxima de uma tentativa de chamada se ninguém atender.
- **Incoming call duration (Duração da chamada recebida)**: defina a duração máxima de uma chamada recebida (máx. 10 minutos).
- **End calls after (Encerrar chamadas após)**: defina a duração máxima de uma chamada (máx. 60 minutos). Selecione **Infinite call duration (Duração de chamada infinita)** se não quiser limitar a duração de uma chamada.

Portas

O número da porta deverá ser entre 1024 e 65535.

- **Porta SIP**: a porta de rede usada para comunicação SIP. O tráfego de sinalização por essa porta não é criptografado. O número da porta padrão é 5060. Insira um número de porta diferente, se necessário.
- **Porta TLS**: a porta de rede usada para comunicação SIP criptografada. O tráfego de sinalização por meio dessa porta é criptografado com o Transport Layer Security (TLS). O número da porta padrão é 5061. Insira um número de porta diferente, se necessário.
- **Porta de início de RTP**: a porta de rede usada para o primeiro stream de mídia RTP em uma chamada SIP. O número da porta de início padrão é 4000. Alguns firewalls bloqueiam o tráfego RTP em determinados números de porta.

NAT traversal

Use o NAT (Network Address Translation) traversal quando o dispositivo estiver localizado em uma rede privada (LAN) e você quiser torná-lo disponível na parte externa de rede.

Observação

Para o NAT traversal funcionar, o roteador deve oferecer suporte a ele. O roteador também deverá oferecer suporte a UPnP®.

Cada protocolo de NAT traversal pode ser usado separadamente ou em diferentes combinações, dependendo do ambiente de rede.

- **ICE**: O protocolo ICE (Interactive Connectivity Establishment) aumenta as chances de encontrar o caminho mais eficiente para uma comunicação bem-sucedida entre dispositivos. Se você também ativar o STUN e o TURN, poderá melhorar as chances do protocolo ICE.
- **STUN**: O STUN (Session Traversal Utilities for NAT) é um protocolo de rede cliente-servidor que permite que o dispositivo determine se ele está localizado atrás de um NAT ou firewall e, em caso afirmativo, obtenha o endereço IP público mapeado e o número da porta alocada para conexões a hosts remotos. Insira o endereço do servidor STUN, por exemplo, um endereço IP.
- **TURN**: O TURN (Traversal Using Relays around NAT) é um protocolo que permite que um dispositivo atrás de um roteador NAT ou firewall receba dados de outros hosts via TCP ou UDP. Insira o endereço e as informações de login do servidor TURN.

Áudio

- **Audio codec priority (Prioridade do codec de áudio)**: Selecione pelo menos um codec de áudio com a qualidade de áudio desejada para as chamadas SIP. Arraste e solte para alterar a prioridade.

Observação

Os codecs selecionados deve corresponder ao codec do destinatário da chamada, pois o codec do destinatário é decisivo quando uma chamada é feita.

- **Audio direction (Direção do áudio)**: selecione as direções de áudio permitidas.

Adicionais

- **UDP-to-TCP switching (Alternância de UDP para TCP)**: selecione para permitir que as chamadas alternem temporariamente os protocolos de transporte de UDP (User Datagram Protocol) para TCP

(Transmission Control Protocol). O motivo da comutação é evitar fragmentação, e a mudança poderá ocorrer se uma solicitação estiver dentro de 200 bytes da unidade máxima de transmissão (MTU) ou for superior a 1.300 bytes.

- **Allow via rewrite (Permitir via regravação)**: selecione para enviar o endereço IP local em vez de endereço IP público do roteador.
- **Allow contact rewrite (Permitir regravação de contato)**: selecione para enviar o endereço IP local em vez de endereço IP público do roteador.
- **Register with server every (Registrar com o servidor a cada)**: defina a frequência na qual você deseja que o dispositivo se registre com o servidor SIP para contas SIP existentes.
- **DTMF payload type (Tipo de carga DTMF)**: altera o tipo de carga padrão para DTMF.
- **Max retransmissions (Máximo de retransmissões)**: defina o número máximo de vezes que o dispositivo tenta se conectar ao servidor SIP antes de parar de tentar.
- **Seconds until failback (Segundos até a contingência)**: defina o número de segundos até que o dispositivo tente se reconectar ao servidor SIP primário após ter feito a contingência para um servidor SIP secundário.

Contas

Todas as contas SIP atuais estão listadas em **SIP accounts (Contas SIP)**. Para contas registradas, o círculo colorido permite saber o status.

A conta foi registrada com êxito no servidor SIP.

Há um problema com a conta. Possíveis motivos podem ser falha de autorização, credenciais de conta incorretas ou o servidor SIP não consegue encontrar a conta.

A conta **peer to peer (default) (ponto a ponto (padrão))** é uma conta criada automaticamente. Você poderá excluí-la se criar pelo menos mais uma conta e configurá-la como padrão. A conta padrão é sempre usada quando uma chamada à VAPIX® Application Programming Interface (API) é feita sem que a conta SIP de origem seja especificada.

Adicionar conta: clique para criar uma conta SIP.

- **Active (Ativa)**: Selecione para poder usar a conta.
- **Tornar padrão**: Selecione para tornar esta a conta padrão. Deve haver uma conta padrão, e somente uma conta padrão pode existir.
- **Answer automatically (Atender automaticamente)**: Selecione para atender automaticamente a uma chamada recebida.
- **Priorizar IPv6 sobre IPv4** : Selecione para priorizar endereços IPv6 em vez de endereços IPv4. Isso é útil quando você conecta a contas ponto a ponto ou nomes de domínio que resolvem tanto em endereços IPv4 quanto IPv6. Só é possível priorizar IPv6 para nomes de domínio mapeados em endereços IPv6.
- **Nome**: Insira um nome descritivo. Isso pode ser, por exemplo, um nome e sobrenome, uma função ou um local. O nome não é exclusivo.
- **ID de usuário**: insira o número exclusivo do ramal ou telefone atribuído ao dispositivo.
- **Ponto a ponto**: use para direcionar chamadas para outro dispositivo SIP na rede local.
- **Registrada**: Use para fazer chamadas para dispositivos SIP fora da rede local através de um servidor SIP.
- **Domain (Domínio)**: Se disponível, insira o nome do domínio público. Ele será mostrado como parte do endereço SIP nas chamadas feitas para outras contas.
- **Senha**: insira a senha associada à conta SIP para autenticação no servidor SIP.
- **ID de autenticação**: Insira o ID de autenticação usado para autenticar no servidor SIP. Se ele for o mesmo que o ID de usuário, não será necessário inserir o ID de autenticação.
- **ID do chamador**: o nome apresentado para o destinatário das chamadas do dispositivo.
- **Registrador**: insira o endereço IP do registrador.
- **Modo de transporte**: selecione o modo de transporte de SIP para a conta: UPD, TCP ou TLS.
- **TLS version (Versão do TLS)** (somente com o modo de transporte TLS): Selecione a versão de TLS que deve ser utilizada. As versões **v1.2** e **v1.3** são as mais seguras. **Automatic (Automático)** seleciona a versão mais segura com a qual o sistema pode lidar.
- **Media encryption (Criptografia de mídia)** (somente com o modo de transporte TLS): Selecione o tipo de criptografia de mídia (áudio e vídeo) em chamadas SIP.
- **Certificate (Certificado)** (somente com o modo de transporte TLS): Selecione um certificado.
- **Verify server certificate (Verifique o certificado do servidor)** (somente com o modo de transporte TLS): Marque para verificar o certificado do servidor.
- **Secondary SIP server (Servidor SIP secundário)**: ative se quiser que o dispositivo tente se registrar em um servidor SIP secundário se o registro no servidor SIP primário falhar.
- **SIP secure (SIP seguro)**: Selecione para usar o Secure Session Initiation Protocol (SIPS). O SIPS usa o modo de transporte TLS para criptografar o tráfego.

- **Proxies**
  - **Proxy**: clique para adicionar um proxy.
  - **Prioritize (Priorizar)**: Se você adicionou dois ou mais proxies, clique para priorizá-los.
  - **Server address (Endereço do servidor)**: insira o endereço IP do servidor proxy SIP.
  - **Username (Nome de usuário)**: Se necessário, insira o nome de usuário do servidor proxy SIP.
  - **Senha**: Se necessário, insira a senha para o servidor proxy de SIP.
- **Vídeo**
  - **View area (Área de exibição)**: Selecione a área de exibição que será usada nas chamadas com vídeo. Se você selecionar nenhum, o modo de exibição nativo será usado.
  - **Resolução**: selecione a resolução que será usada nas chamadas com vídeo. A resolução afeta a largura de banda necessária.
  - **Taxa de quadros**: selecione o número de quadros por segundo para as chamadas com vídeo. A taxa de quadros afeta a largura de banda necessária.
  - **Perfil H.264**: selecione o perfil que será usado nas chamadas com vídeo.

DTMF

Adicionar sequência: Clique para criar uma nova sequência de multifrequência de duplo tom (DTMF). Para criar uma regra ativada pelo tom de toque, vá para **Events > Rules (Eventos > Regras)**.

Sequência: Insira os caracteres para ativar a regra. Caracteres permitidos: 0–9, A-D, # e *.

Description (Descrição): insira uma descrição da ação a ser acionada por sequência.

Contas: Selecione as contas que usarão a sequência DTMF. Se você escolher **ponto a ponto**, todas as contas ponto a ponto compartilharão a mesma sequência DTMF.

Protocolos

Selecione os protocolos a serem usados para cada conta. Todas as contas ponto a ponto compartilham as mesmas configurações de protocolo.

Use RTP (RFC2833) (Usar RTP (RFC2833)): Ative para permitir a sinalização DTMF (Dual-Tone Multifrequency), outros sinais de tom e eventos de telefonia em pacotes RTP.

Usar SIP INFO (RFC2976): Ative para incluir o método INFO no protocolo SIP. O método INFO adiciona informações opcionais da camada de aplicação, em geral relacionadas à sessão.

Testar chamada

Conta SIP: selecione a conta que realizará a chamada.

Endereço SIP: Insira um endereço SIP e clique em para realizar uma chamada de teste e verificar se a conta está funcionando.

Lista de acesso

Usar lista de acesso: Ative-se para restringir quem pode fazer chamadas para o dispositivo.

Policy (Política):

- **Permitir**: Selecione para permitir chamadas recebidas somente das fontes na lista de acesso.
- **Bloquear**: Selecione para bloquear chamadas recebidas somente das fontes na lista de acesso.

Adicionar origem: Clique em para criar uma nova entrada na lista de acessos.

SIP source (Origem SIP): Digite a ID do chamador ou o endereço do servidor SIP da fonte.

Controlador multicast

User multicast controller (Usar controlador multicast): Ative para ativar o controlador multicast.

Audio codec (Codec de áudio): Selecione um codec de áudio.

Source (Fonte): Adicione uma nova fonte de controlador multicast.

- **Label (Rótulo)**: Insira o nome de um rótulo que ainda não seja usado por uma fonte.
- **Source (Fonte)**: Insira uma fonte.
- **Porta**: Insira uma porta.
- **Priority (Prioridade)**: Selecione uma prioridade.
- **Profile (Perfil)**: Selecione um perfil.
- **SRTP key (Chave SRTP)**: Insira uma chave SRTP.

O menu de contexto contém:

Edit (Editar): Edite a fonte do controlador multicast.

Excluir: Exclua a fonte do controlador multicast.

Armazenamento

Armazenamento de rede

Ignore (Ignorar): Ative para ignorar o armazenamento de rede.

Add network storage (Adicionar armazenamento de rede): clique para adicionar um compartilhamento de rede no qual você pode salvar as gravações.

- **Endereço**: insira o endereço IP ou nome de host do servidor host, em geral, um NAS (armazenamento de rede). Recomendamos configurar o host para usar um endereço IP fixo (e não DHCP, pois os endereços IP dinâmicos podem mudar) ou então usar DNS. Não há suporte a nomes SMB/CIFS Windows.
- **Network share (Compartilhamento de rede)**: Insira o nome do local compartilhado no servidor host. Vários dispositivos Axis podem usar o mesmo compartilhamento de rede, já que cada dispositivo tem sua própria pasta.
- **User (Usuário)**: se o servidor exigir um login, insira o nome de usuário. Para fazer login em um servidor de domínio específico, digite `DOMAIN\username`.
- **Senha**: Se o servidor exigir um login, digite a senha.
- **SMB version (Versão SMB)**: selecione a versão do protocolo de armazenamento SMB para se conectar ao NAS. Se você selecionar **Auto**, o dispositivo tentará negociar uma das versões seguras de SMB: 3.02, 3.0 ou 2.1. Selecione 1.0 ou 2.0 para se conectar ao NAS antigo que não oferece suporte a versões posteriores. Leia mais sobre o suporte a SMB em dispositivos Axis *aqui*.
- **Add share without testing (Adicionar compartilhamento sem testar)**: selecione para adicionar o compartilhamento de rede mesmo se um erro for descoberto durante o teste de conexão. O erro pode ser, por exemplo, que você não digitou uma senha, embora o servidor precise de uma.

Remove network storage (Remover armazenamento em rede): Clique para desmontar, desvincular e remover a conexão com o compartilhamento de rede. Isso remove todas as configurações do compartilhamento de rede.

Unbind (Desvincular): Clique para desvincular e desconectar o compartilhamento de rede.
Bind (Vincular): Clique para vincular e conectar o compartilhamento de rede.

Unmount (Desmontar): Clique para desmontar o compartilhamento de rede.
Mount (Montar): Clique para montar o compartilhamento de rede.

Write protect (Proteção contra gravação): Ative para parar de gravar no compartilhamento de rede e proteger as gravações contra remoção. Não é possível formatar um compartilhamento de rede protegido contra gravação.

Retention time (Tempo de retenção): Selecione por quanto tempo as gravações serão mantidas para limitar a quantidade de gravações antigas ou atender a regulamentações relativas ao armazenamento de dados. Se o armazenamento de rede ficar cheio, as gravações antigas serão removidas antes do período de tempo selecionado se esgotar.

Ferramentas

- **Test connection (Testar conexão)**: Teste a conexão com o compartilhamento de rede.
- **Format (Formatar)**: formate o compartilhamento de rede, por exemplo, quando for necessário apagar rapidamente todos os dados. CIFS é a opção de sistema de arquivos disponível.

Use tool (Usar ferramenta): Clique para ativar a ferramenta selecionada.

Armazenamento interno

Importante

Risco de perda de dados ou gravações corrompidas. Não remova o cartão SD com o dispositivo em funcionamento. Desmonte o cartão SD antes de removê-lo.

Unmount (Desmontar): Clique para remover com segurança o cartão SD.

Write protect (Proteção contra gravação): Ative essa opção para parar de escrever no cartão SD e proteger as gravações contra remoção. Não é possível formatar um cartão SD protegido contra gravação.

Autoformat (Formatação automática): ative para formatar automaticamente um cartão SD recém-inserido. Ele formata o sistema de arquivos em ext4.

Ignore (Ignorar): ative para parar de armazenar gravações no cartão SD. Quando você ignora o cartão SD, o dispositivo passa a não reconhecer que o cartão existe. A configuração está disponível somente para administradores.

Retention time (Tempo de retenção): selecione por quanto tempo as gravações serão mantidas para limitar a quantidade de gravações antigas ou atender a regulamentações de armazenamento de dados. Quando o cartão SD está cheio, ele exclui gravações antigas antes que o tempo de retenção tenha passado.

Ferramentas

- **Check (Verificar)**: Verifica se há erros no cartão SD.
- **Repair (Reparar)**: Repare erros no sistema de arquivos.
- **Format (Formatar)**: Formate o cartão SD para alterar o sistema de arquivos e apagar todos os dados. Só é possível formatar o cartão SD para o sistema de arquivos ext4. Um driver ou aplicativo de terceiros compatível com ext4 será necessário para acessar o sistema de arquivos no Windows®.
- **Encrypt (Criptografar)**: Use essa ferramenta para formatar o cartão SD e ativar a criptografia. Isso exclui todos os dados armazenados no cartão SD. Todos os novos dados armazenados no cartão SD serão criptografados.
- **Decrypt (Descriptografar)**: Use essa ferramenta para formatar o cartão SD sem criptografia. Isso exclui todos os dados armazenados no cartão SD. Nenhum novo dado armazenado no cartão SD será criptografado.
- **Change password (Alterar senha)**: Altere a senha necessária para criptografar o cartão SD.

Use tool (Usar ferramenta): Clique para ativar a ferramenta selecionada.

Wear trigger (Acionador de uso): Defina um valor para o nível de uso do cartão SD no qual você deseja acionar uma ação. O nível de desgaste varia de 0 a 200%. Um novo cartão SD que nunca foi usado tem um nível de desgaste de 0%. Um nível de desgaste de 100% indica que o cartão SD está próximo de seu tempo de vida esperado. Quando o nível de desgaste atinge 200%, há um alto risco de falha do cartão SD. Recomendamos configurar o acionador de desgaste entre 80 – 90%. Isso permite baixar qualquer gravação, bem como substituir o cartão SD a tempo antes que ele possa se deteriorar. O acionador de desgaste permite a você configurar um evento e obter uma notificação quando o nível de desgaste atingir o valor definido.

ONVIF

Contas ONVIF

O ONVIF (Open Network Video Interface Forum) é um padrão de interface global que facilita aos usuários finais, integradores, consultores e fabricantes aproveitarem as possibilidades oferecidas pela tecnologia de vídeo em rede. O ONVIF permite interoperabilidade entre produtos de diferentes fornecedores, maior flexibilidade, custo reduzido e sistemas sempre atuais.

Ao criar uma conta ONVIF, você ativa a comunicação ONVIF automaticamente. Use o nome da conta e a senha em toda a comunicação ONVIF com o dispositivo. Para obter mais informações, consulte a Comunidade de desenvolvedores Axis em *axis.com*.

Add accounts (Adicionar contas): Clique para adicionar um nova conta ONVIF.

Account (Conta): Insira um nome de conta exclusivo.

New password (Nova senha): Insira uma senha para o nome da conta. As senhas devem conter 1 a 64 caracteres de comprimento. Somente caracteres ASCII imprimíveis (código 32 a 126) são permitidos na senha, por exemplo, letras, números, pontuação e alguns símbolos.

Repeat password (Repetir senha): Insira a mesma senha novamente.

Role (Função):

- **Administrator (Administrador)**: Tem acesso irrestrito a todas as configurações. Os administradores também podem adicionar, atualizar e remover outras contas.
- **Operator (Operador)**: Tem acesso a todas as configurações, exceto:
  - Todas as configurações do **System (Sistema)**.
  - Adicionando aplicativos.
- **Media account (Conta de mídia)**: Permite acesso apenas ao stream de vídeo.

O menu de contexto contém:

Update account (Atualizar conta): Edite as propriedades da conta.

Delete account (Excluir conta): Exclua a conta. Não é possível excluir a conta root.

Perfis de mídia ONVIF

Um perfil de mídia ONVIF consiste em um conjunto de configurações que podem ser usadas para alterar opções de stream de mídia. Você pode criar novos perfis com seu próprio conjunto de configurações ou usar perfis pré-configurados para uma configuração rápida.

Adicionar perfil de mídia: clique para adicionar um novo perfil de mídia ONVIF.

Nome do perfil: Adicione um nome para o perfil de mídia.

Video source (Origem do vídeo): Selecione a fonte de vídeo para sua configuração.

- **Selecione a configuração**: Selecione uma configuração definida pelo usuário da lista. As configurações na lista suspensa correspondem aos canais de vídeo do dispositivo, incluindo multivisualizações, áreas de visualização e canais virtuais.

Video encoder (Codificador de vídeo): Selecione o formato de codificação de vídeo para sua configuração.

- **Selecione a configuração**: Selecione uma configuração definida pelo usuário na lista e ajuste as configurações de codificação. As configurações na lista suspensa atuam como identificadores/nomes da configuração do codificador de vídeo. Selecione o usuário de 0 a 15 para aplicar suas próprias configurações ou selecione um dos usuários padrão se desejar usar configurações predefinidas para um formato de codificação específico.

Observação

Ative o áudio no dispositivo para obter a opção de selecionar uma fonte de áudio e uma configuração do codificador de áudio.

Fonte de áudio : Selecione a fonte de entrada de áudio para a sua configuração.

- **Selecione a configuração**: Selecione uma configuração definida pelo usuário da lista e ajuste as configurações de áudio. As configuraçãos na lista suspensa correspondem às entradas de áudio do dispositivo. Se o dispositivo tiver uma entrada de áudio, é user0. Se o dispositivo tiver várias entradas de áudio, haverá usuários adicionais na lista.

Codificador de áudio : Selecione o formato de codificação de áudio para a sua configuração.

- **Selecione a configuração**: Seleciione uma configuração definida pelo usuário da lista e ajuste as configurações de codificação de áudio. As configurações na lista suspensa agem como identificadores/ /nomes da configuração do codificador de áudio.

Audio decoder (Decodificador de áudio) : Selecione o formato de decodificação de áudio para a sua configuração.

- **Selecione a configuração**: Selecione uma configuração definida pelo usuário da lista e ajuste as configurações. As configurações na lista suspensa agem como identificadores/nomes da configuração.

Saída de áudio : Selecione o formato da saída de áudio para a sua configuração.

- **Selecione a configuração**: Selecione uma configuração definida pelo usuário da lista e ajuste as configurações. As configurações na lista suspensa agem como identificadores/nomes da configuração.

Metadados: Selecione os metadados para incluir na sua configuração.

- **Selecione a configuração**: Selecione uma configuração definida pelo usuário da lista e ajuste as configurações de metadados. As configuraçãos na lista suspensa agem como identificadores/nomes da configuração de metadados.

PTZ : Selecione as configurações PTZ para a sua configuração.

- **Selecione a configuração**: Selecione uma configuração definida pelo usuário da lista e ajuste as configurações PTZ. As configurações na lista suspensa correspondem aos canais de vídeo do dispositivo com suporte PTZ.

Create (Criar): Clique para salvar suas configurações e criar o perfil.

Cancelar: Clique para cancelar a configuração e limpar todas as configurações.

profile_x: Clique no nome do perfil para abrir e editar o perfil pré-configurado.

Detectores

Detecção de áudio

Essas configurações estão disponíveis para cada entrada de áudio.

Sound level (Nível sonoro): ajuste o nível sonoro para um valor entre 0 e 100, em que 0 é o mais sensível e 100 é o menos sensível. Use o indicador de atividade como guia ao definir o nível sonoro. Ao criar eventos, você pode usar o nível sonoro como uma condição. Você pode optar por acionar uma ação se o nível sonoro ultrapassar, ficar abaixo ou passar pelo valor definido.

Medidor de potência

Uso de energia

Mostra o uso de energia atual, o uso médio de energia, o uso máximo de energia e o consumo de energia ao longo do tempo.

O menu de contexto contém:

- **Export (Exportar)**: Clique em para exportar os dados do gráfico.

Acessórios

Portas de E/S

Use a entrada digital para conectar dispositivos externos que podem alternar entre um circuito aberto ou fechado, por exemplo, sensores PIR, contatos de portas ou janelas e detectores de quebra de vidros.

Use a saída digital para conectar dispositivos externos, como relés e LEDs. Você pode ativar dispositivos conectados via interface de programação de aplicativos VAPIX® ou na interface Web.

Detecção automática

Nome: Edite o texto para renomear a porta.

Direção:  indica que a porta é uma porta de entrada.  indica que é uma porta de saída. Se a porta for configurável, você poderá clicar nos ícones para alternar entre entrada e saída.

Normal state (Estado normal): Clique em  para circuito aberto e  para circuito fechado.

Current state (Estado atual): Mostra o estado atual da porta. A entrada ou saída é ativada quando o estado atual é diferente do estado normal. Uma entrada no dispositivo tem um circuito aberto quando desconectada ou quando há uma tensão acima de 1 VCC.

Observação

Durante a reinicialização, o circuito de saída é aberto. Quando a reinicialização é concluída, o circuito retorna para a posição normal. Se você alterar qualquer configuração nesta página, os circuitos de saída voltarão para suas posições normais, independentemente de quaisquer acionadores ativos.

Supervisionado  : Ative para possibilitar a detecção e o acionamento de ações se alguém manipular a conexão com dispositivos de E/S digitais. Além de detectar se uma entrada está aberta ou fechada, você também pode detectar se alguém a manipulou (ou seja, cortada ou em curto). Supervisionar a conexão requer hardware adicional (resistores de fim de linha) no loop de E/S externo.

Logs

Relatórios e logs

Relatórios

- **View the device server report (Exibir o relatório do servidor de dispositivos)**: Exiba informações sobre o status do produto em uma janela pop-up. O Log de acesso é incluído automaticamente no Relatório do servidor.
- **Download the device server report (Baixar o relatório do servidor de dispositivos)**: Ele cria um arquivo .zip que contém um arquivo de texto do relatório completo do servidor no formato UTF-8, bem como um instantâneo da imagem da visualização ao vivo atual. Inclua sempre o arquivo. zip do relatório do servidor ao entrar em contato com o suporte.
- **Download the crash report (Baixar o relatório de falhas inesperadas)**: Baixe um arquivo com informações detalhadas sobre o status do servidor. O relatório de panes contém informações que fazem parte do relatório do servidor, além de informações de depuração detalhadas. Esse relatório pode conter informações sensíveis, como rastreamentos de rede. A geração do relatório poderá demorar vários minutos.

Logs

- **View the system log (Exibir o log do sistema)**: Clique para mostrar informações sobre eventos do sistema, como inicialização de dispositivos, avisos e mensagens críticas.
- **View the access log (Exibir o log de acesso)**: clique para mostrar todas as tentativas de acessar o dispositivo que falharam, por exemplo, quando uma senha de login incorreta é usada.
- **View the audit log (Exibir o log de auditoria)**: Clique para mostrar informações sobre as atividades do usuário e do sistema, por exemplo, autenticações e configurações bem-sucedidas ou com falha.

Rastreamento de rede

Importante

Um arquivo de rastreamento de rede pode conter informações confidenciais, por exemplo, certificados ou senhas.

Um arquivo de trace de rede pode ajudar a solucionar problemas gravando as atividades na rede.

Trace time (Tempo de trace): Selecione a duração do trace em segundos ou minutos e clique em **Download (Baixar)**.

Acesse o sistema remotamente

O syslog é um padrão para o registro de mensagens. Ele permite a separação do software que gera mensagens, o sistema que as armazena e o software que as relata e analisa. Cada mensagem é rotulada com um código da instalação que indica o tipo de software que gerou a mensagem e recebe um nível de gravidade.

Servidor: Clique para adicionar um novo servidor.

Host: Insira o nome de host ou endereço IP do servidor.

Format (Formatar): Selecione o formato de mensagem do syslog que será usado.

- Axis
- RFC 3164
- RFC 5424

Protocol (Protocolo): Selecione o protocolo que a ser usado:

- UDP (a porta padrão é 514)
- TCP (a porta padrão é 601)
- TLS (a porta padrão é 6514)

Porta: Edite o número da porta para usar uma porta diferente.

Severity (Severidade): Selecione quais mensagens serão enviadas após o acionamento.

Tipo: Selecione os tipos de registros que deseja enviar.

Test server setup (Testar configuração do servidor): Envie uma mensagem de teste para todos os servidores antes de salvar as configurações.

CA certificate set (Certificado CA definido): Consulte as configurações atuais ou adicione um certificado.

Configuração simples

A configuração simples destina-se a usuários avançados com experiência em configuração de dispositivos Axis. A maioria dos parâmetros podem ser definidos e editados nesta página.

Manutenção

Restart (Reiniciar): Reinicie o dispositivo. Isso não afeta nenhuma das configurações atuais. Os aplicativos em execução reiniciam automaticamente.

Restore (Restaurar): Devolve a maioria das configurações para os valores padrão de fábrica. Posteriormente, você deverá reconfigurar o dispositivo e os aplicativos, reinstalar quaisquer apps que não vieram pré-instalados e recriar quaisquer eventos e predefinições.

Importante

As únicas configurações que permanecem salvas após a restauração são:

- Protocolo de inicialização (DHCP ou estático)
- Endereço IP estático
- Roteador padrão
- Máscara de sub-rede
- Configurações 802.1X
- Configurações de O3C
- Endereço IP do servidor DNS

Factory default (Padrão de fábrica): Retorna todas as configurações para os valores padrão de fábrica. Em seguida, você deverá redefinir o endereço IP para tornar o dispositivo acessível.

Observação

Todo software de dispositivo Axis é digitalmente assinado para garantir que somente software verificado seja instalado em seu dispositivo. Esse procedimento aprimora ainda mais o nível de segurança cibernética mínimo dos dispositivos Axis. Para obter mais informações, consulte o white paper "Axis Edge Vault" em *axis.com*.

Atualização do AXIS OS: atualize para uma nova versão do AXIS OS. As novas versões podem conter funcionalidades aprimoradas, correções de falhas ou ainda recursos inteiramente novos. Recomendamos sempre utilizar a versão mais recente do AXIS OS. Para baixar a versão mais recente, vá para *axis.com/support*.

Ao atualizar, é possível escolher entre três opções:

- **Standard upgrade (Atualização padrão)**: atualize para a nova versão do AXIS OS.
- **Factory default (Padrão de fábrica)**: Atualize e retorne todas as configurações para os valores padrão de fábrica. Ao escolher essa opção, você não poderá reverter para a versão anterior do AXIS OS após a atualização.
- **Automatic rollback (Reversão automática)**: Atualize e confirme a atualização dentro do período definido. Se você não confirmar, o dispositivo reverterá para a versão anterior do AXIS OS.

AXIS OS rollback (Reversão do AXIS OS): reverta para a versão anteriormente instalada do AXIS OS.

solução de problemas

Reset PTR (Redefinir PTR) : redefina o PTR se, por algum motivo, as configurações de **Pan (Panorama)**, **Tilt (Inclinação)** ou **Roll (Rolagem)** não funcionarem como esperado. Os motores de PTR são sempre calibrados em uma nova câmera. No entanto, a calibração poderá ser perdida, por exemplo, se a câmera perder energia ou se os motores forem movidos à mão. Quando você redefine o PTR, a câmera é recalibrada e retorna à sua posição padrão de fábrica.

Calibração : clique em **Calibrate (Calibrar)** para recalibrar os motores pan, tilt e roll às suas posições padrão.

Ping: Para verificar se o dispositivo pode acessar um endereço específico, digite o nome de host ou o endereço IP do host no qual deseja executar o ping e clique em **Iniciar**.

Verificação de porta: Para verificar a conectividade do dispositivo com um endereço IP e uma porta TCP/UDP específicos, digite o nome do host ou o endereço IP e o número da porta que deseja verificar e clique em **Iniciar**.

Rastreamento de rede

Importante

Um arquivo de rastreamento de rede pode conter informações confidenciais, como certificados ou senhas.

Um arquivo de trace de rede pode ajudar a solucionar problemas gravando as atividades na rede.

Trace time (Tempo de trace): Selecione a duração do trace em segundos ou minutos e clique em **Download (Baixar)**.

Saiba mais

Session Initiation Protocol (SIP)

O Session Initiation Protocol (SIP) é usado para configurar, manter e encerrar chamadas de VoIP. Você pode fazer chamadas entre duas ou mais partes, chamadas de agentes de usuário SIP. Para fazer uma chamada SIP, você pode usar, por exemplo, telefones SIP, softphones ou dispositivos Axis compatíveis com SIP.

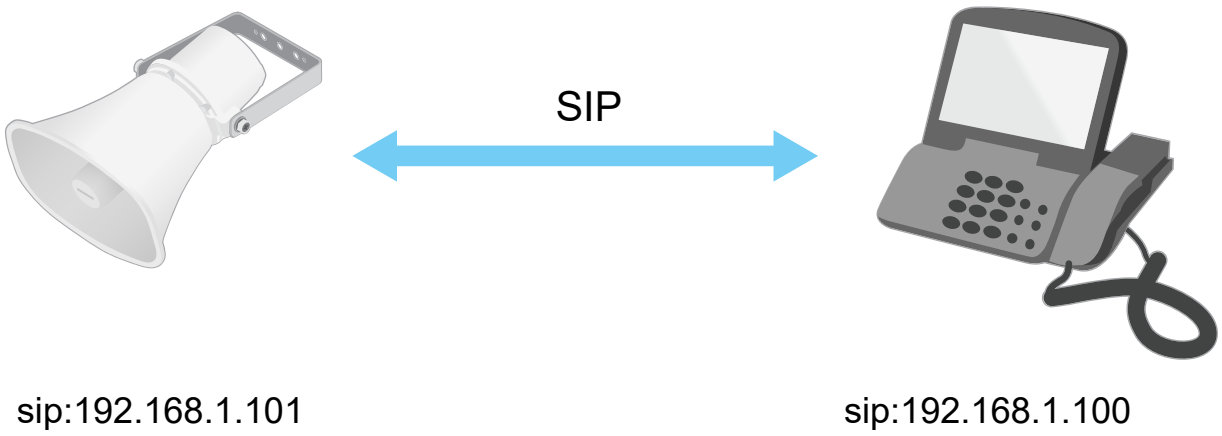
O áudio ou vídeo efetivos são trocados entre os agentes de usuário SIP com um protocolo de transporte, por exemplo, RTP (Real-Time Transport Protocol).

Você pode fazer chamadas em redes locais usando uma configuração ponto a ponto ou através de redes que usam um PBX.

SIP ponto a ponto (P2PSIP)

O tipo mais básico de comunicação SIP ocorre diretamente entre dois ou mais agentes de usuário SIP. Isso é chamado de SIP ponto a ponto (P2PSIP). Se ele ocorre em uma rede local, tudo o que é necessário são os endereços SIP dos agentes de usuário. Um endereço SIP típico, nesse caso, seria `sip:<local-ip>`.

Exemplo:



Também é possível configurar um telefone compatível com SIP para chamar um dispositivo de áudio na mesma rede usando uma configuração de SIP ponto a ponto.

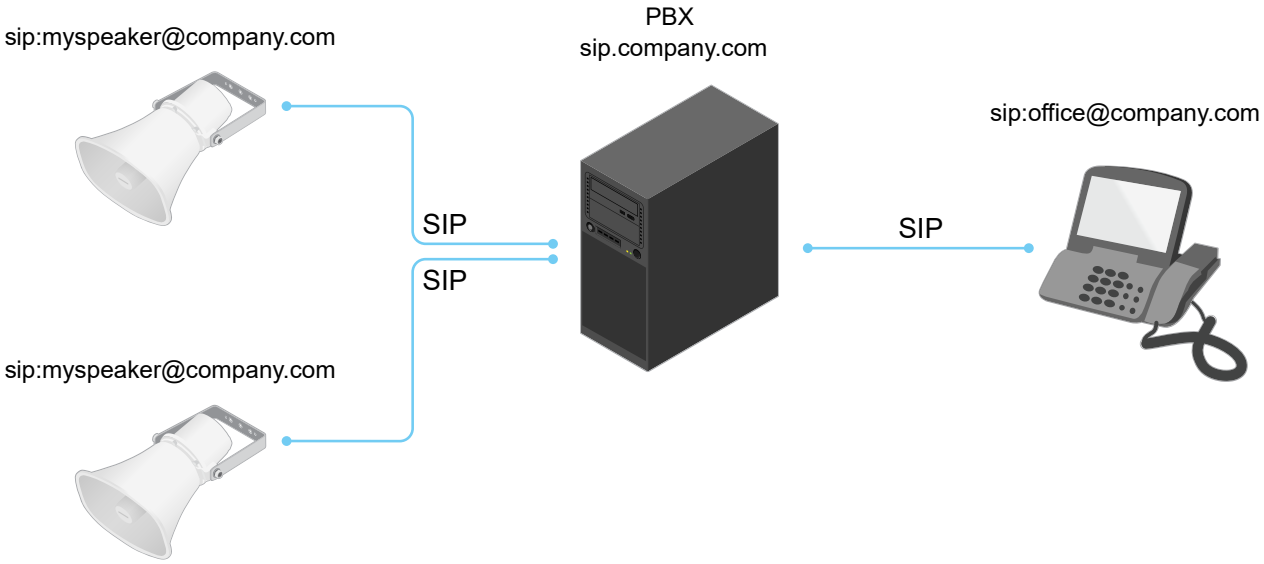
Private Branch Exchange (PBX)

Quando você faz chamadas SIP fora da sua rede IP local, um PBX (Private Branch Exchange) pode atuar como hub central. O componente principal de um PBX é um servidor SIP, o qual também é conhecido como proxy SIP ou registrador. Um PBX funciona como uma mesa telefônica tradicional, mostrando o status atual do cliente e permitindo transferências de chamadas, correio de voz e redirecionamentos.

O servidor SIP de PBX pode ser configurado como uma entidade local ou externa. Ele pode ser hospedado em uma intranet ou por um provedor terceirizado. Quando você faz chamadas SIP entre redes, as chamadas são roteadas através de um conjunto de PBXs, que consultam o local do endereço SIP a ser acessado.

Cada agente de usuário SIP registra-se no PBX e pode, em seguida, alcançar os outros discando o ramal correto. Um endereço SIP típico, nesse caso, seria `sip:<user>@<domain>` ou `sip:<user>@<registrar-ip>`. O endereço SIP é independente de seu endereço IP e o PBX torna o dispositivo acessível, desde que esteja registrado no PBX.

Exemplo:



NAT traversal

Use o NAT (Network Address Translation) traversal quando o dispositivo Axis estiver localizado em uma rede privada (LAN) e você deseja acessá-lo de fora dessa rede.

Observação

O roteador deve ser compatível com o NAT traversal e UPnP®.

Cada protocolo de NAT traversal pode ser usado separadamente ou em diferentes combinações, dependendo do ambiente de rede.

- **ICE** – O protocolo ICE (Interactive Connectivity Establishment) aumenta as chances de encontrar o caminho mais eficiente para uma comunicação bem-sucedida entre dispositivos. Se você também ativar o STUN e o TURN, poderá melhorar as chances do protocolo ICE.
- **STUN** – O STUN (Session Traversal Utilities for NAT) é um protocolo de rede cliente-servidor que permite que o dispositivo Axis determine se ele está localizado atrás de um NAT ou firewall e, em caso afirmativo, obtenha o endereço IP público mapeado e o número da porta alocada para conexões a hosts remotos. Insira o endereço do servidor STUN, por exemplo, um endereço IP.
- **TURN** – O TURN (Traversal Using Relays around NAT) é um protocolo que permite que um dispositivo atrás de um roteador NAT ou firewall receba dados de outros hosts via TCP ou UDP. Insira o endereço do servidor TURN e as informações de login.

Aplicativos

Usando aplicativos, você pode obter mais do seu dispositivo Axis. A AXIS Camera Application Platform (ACAP) é uma plataforma aberta que permite que qualquer pessoa desenvolva aplicativos de análise e outros aplicativos para dispositivos Axis. Os aplicativos podem ser pré-instalados no dispositivo, disponibilizados para download gratuitamente ou mediante uma tarifa de licença.

Para encontrar manuais de usuário para aplicativos da Axis, vá para *help.axis.com*.

AXIS Audio Analytics

O AXIS Audio Analytics detecta aumentos súbitos no volume do som e tipos de sons específicos, como gritos, dentro do alcance do dispositivo no qual está instalado. Essas detecções podem ser configuradas para acionar uma resposta, como gravar vídeo, reproduzir uma mensagem de áudio ou alertar a equipe de segurança. Para saber mais sobre como o aplicativo funciona, consulte o *manual do usuário do AXIS Audio Analytics*.

InformaCast®

O InformaCast é uma plataforma que permite o envio de mensagens de emergência e a comunicação por meio dos canais de comunicação que a sua organização já possui, incluindo os alto-falantes em rede Axis. O sistema de notificação em massa InformaCast fornece alertas de áudio incisivos por toda a instalação. Para saber mais sobre o aplicativo, consulte *Funcionalidade do AXIS Speaker para o Singlewire InformaCast*.

Cibersegurança

Para obter informações específicas do produto sobre segurança cibernética, consulte a folha de dados do produto em axis.com.

Para obter informações detalhadas sobre segurança cibernética no AXIS OS, leia o *guia para aumento do nível de proteção do AXIS OS*.

Serviço de notificação de segurança Axis

A Axis fornece um serviço de notificação com informações sobre vulnerabilidades e outras questões relacionadas à segurança para os dispositivos Axis. Para receber notificações, inscreva-se em *axis.com/security-notification--service*.

Gerenciamento de vulnerabilidades

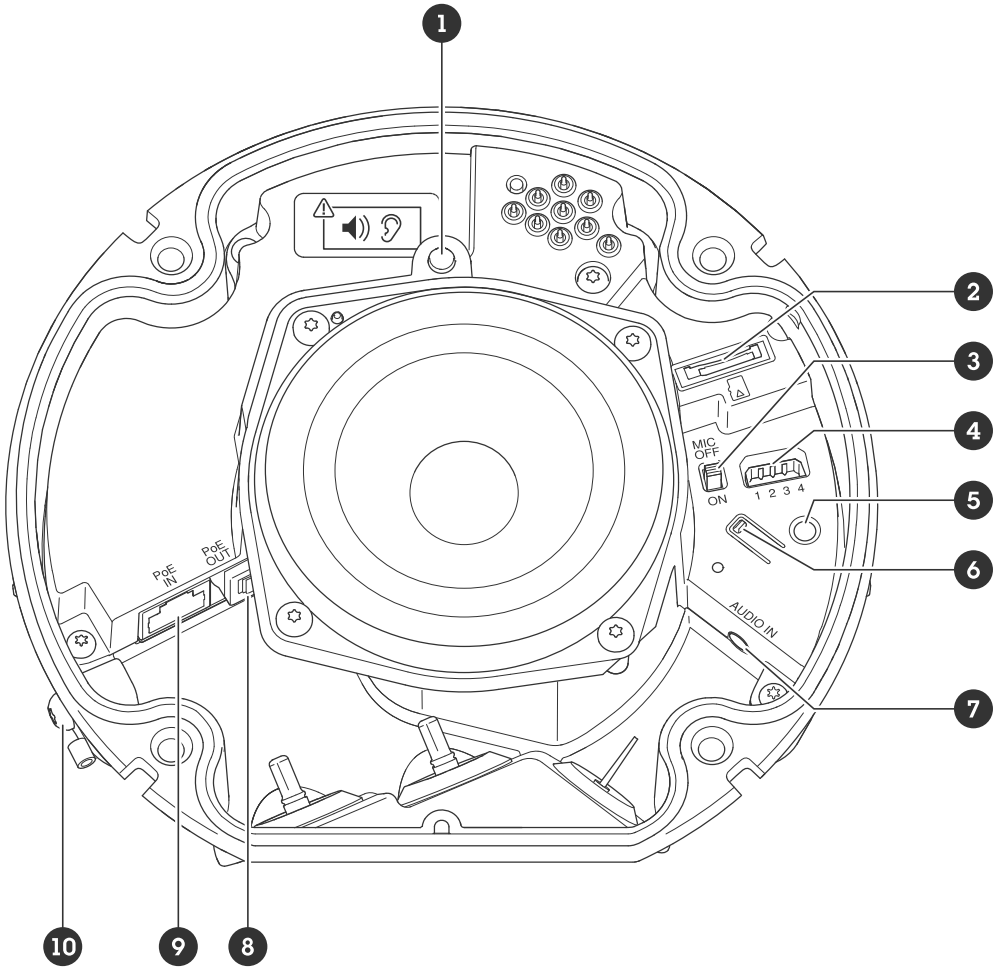
Para minimizar o risco de exposição dos clientes, a Axis, na condição de **Autoridade de Numeração (CNA) de Vulnerabilidades e Exposições Comuns (CVE)**, segue os padrões do setor para gerenciar e responder a vulnerabilidades descobertas em nossos dispositivos, software e serviços. Para obter mais informações sobre a política de gerenciamento de vulnerabilidades da Axis, como relatar vulnerabilidades, vulnerabilidades já conhecidas e as respectivas orientações de segurança, consulte *axis.com/vulnerability-management*.

Operação segura de dispositivos Axis

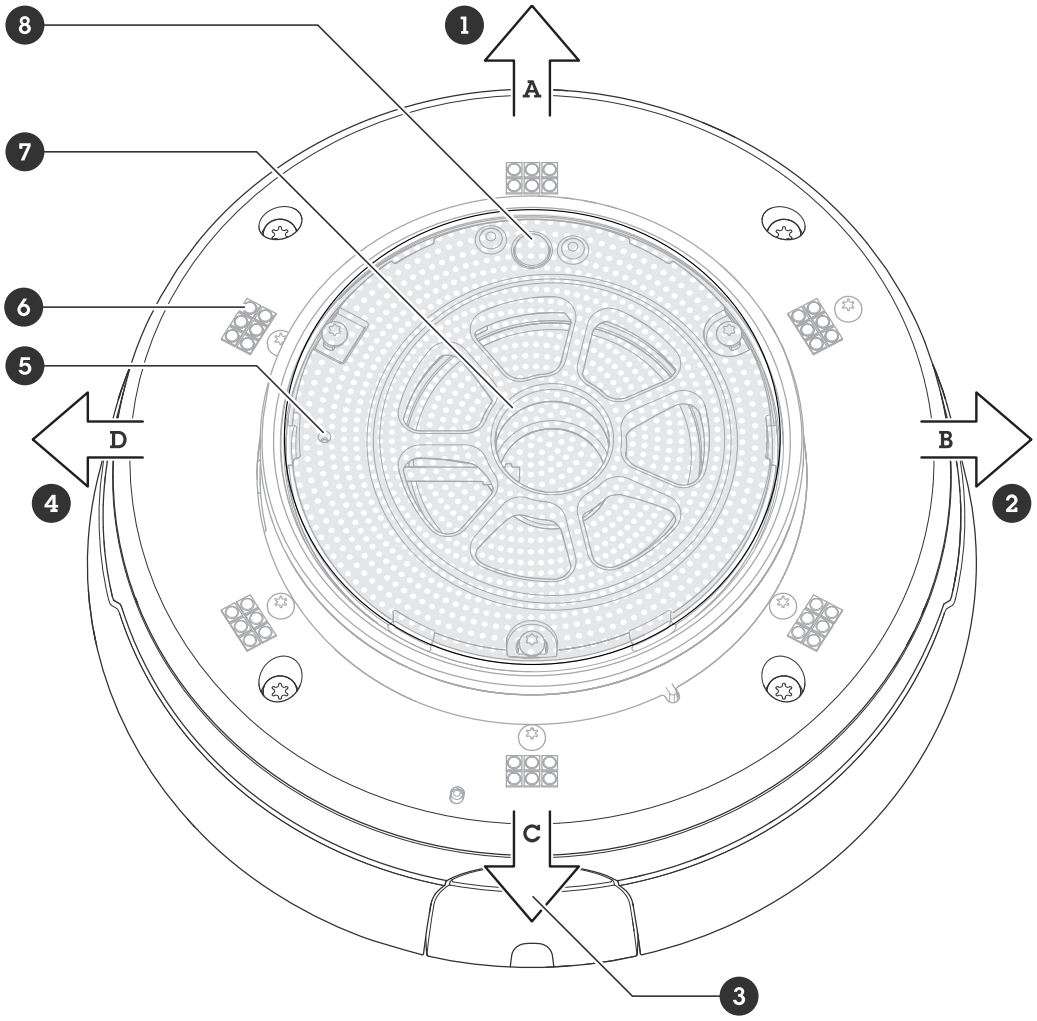
Os dispositivos Axis com configurações padrão de fábrica são pré-configurados com mecanismos de proteção padrão seguros. Recomendamos usar mais configuração de segurança ao instalar o dispositivo. Para saber mais sobre a abordagem da Axis em relação à segurança cibernética, incluindo práticas recomendadas, recursos e diretrizes para proteger seus dispositivos, acesse *https://www.axis.com/about-axis/cybersecurity*.

Especificações

Visão geral do produto



1 *Audio LED*
2 *Entrada para cartão microSD*
3 *Chave de microfone*
4 *Conector de E/S*
5 *LED indicador de status*
6 *Botão de controle*
7 *Conector de áudio*
8 *Conector de rede (PoE OUT)*
9 *Conector de rede (PoE IN)*
10 *Parafuso de aterramento*



1 *Direção da luz A*
2 *Direção da luz B*
3 *Direção da luz C*
4 *Direção da luz D*
5 *Microfone interno*
6 *LEDs de sinalização*
7 *Alto-falante*
8 *Audio LED*

Indicadores de LED

LED de estado	Indicação
Apagado	Conexão e operação normais.
Verde	Permanece aceso em verde por 10 segundos para operação normal após a conclusão da inicialização.
Âmbar	Aceso durante a inicialização, na restauração para os padrões de fábrica ou na restauração de configurações.

Slot de cartão SD

OBSERVAÇÃO

- Risco de danos ao cartão SD. Não use ferramentas afiadas, objetos de metal ou força excessiva para inserir ou remover o cartão SD. Use os dedos para inserir e remover o cartão.
- Risco de perda de dados ou gravações corrompidas. Desmonte o cartão SD pela interface web do dispositivo antes de removê-lo. Não remova o cartão SD com o produto em funcionamento.

Para obter recomendações sobre cartões SD, consulte *axis.com*.

Os logotipos microSD, microSDHC e microSDXC são marcas comerciais da SD-3C LLC. microSD, microSDHC e microSDXC são marcas comerciais ou registradas da SD-3C, LLC nos Estados Unidos e/ou em outros países.

Botões

Botão de controle

O botão de controle é usado para:

- Calibrar o teste de alto-falante. Pressione e solte rapidamente o botão de controle. Um tom de teste é reproduzido.
- Restaurar o produto para as configurações padrão de fábrica. Consulte .
- Conexão a um serviço de conexão em nuvem com um clique (O3C) via Internet. Para conectar, pressione e solte o botão e aguarde até que o LED de status pisque em verde três vezes.

Chave de microfone

Para obter informações sobre a localização da chave do microfone, consulte .

A chave do microfone é usada para **LIGAR** ou **DESLIGAR** mecanicamente o microfone. A configuração padrão de fábrica para essa chave é **LIGADO**.

Conectores

Conector de rede

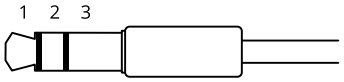
Conector Ethernet RJ45 com Power over Ethernet (PoE).

OBSERVAÇÃO

O dispositivo deve ser conectado a um cabo de rede blindado (STP). Todos os cabos que conectam o dispositivo à rede devem ser blindados e usados somente da forma para a qual foram projetados. Certifique-se de que os dispositivos de rede sejam instalados de acordo com as instruções do fabricante. Para obter informações sobre os requisitos regulatórios, consulte o Guia de Instalação em *www.axis.com*.

Conector de áudio

- **Entrada de áudio** – Entrada de 3,5 mm para um microfone digital, um microfone mono analógico ou um sinal mono de entrada de áudio (o canal esquerdo é usado de um sinal estéreo).



Entrada de áudio

1 Ponta	2 Anel	3 Luva
Microfone não equalizado (com ou sem alimentação de eletreto) ou entrada de áudio	Alimentação de eletreto, se selecionada	Terra
Sinal digital	Ring power, se selecionado	Terra

Observação

O comprimento máximo do cabo conectado é de 30 m (98,4 ft).

Conector de E/S

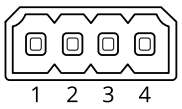
Use o conector de E/S com dispositivos externos em combinação com, por exemplo, detectores de movimento, acionadores de eventos e notificações de alarmes. Além do ponto de referência de 0 V CC e da alimentação (saída CC de 12 V), o conector do terminal de E/S fornece a interface para:

Entrada digital – Para conectar dispositivos que podem alternar entre um circuito aberto ou fechado, por exemplo, sensores PIR, contatos de portas/janelas e detectores de quebra de vidros.

Entrada supervisionada – Permite detectar manipulações em entradas digitais.

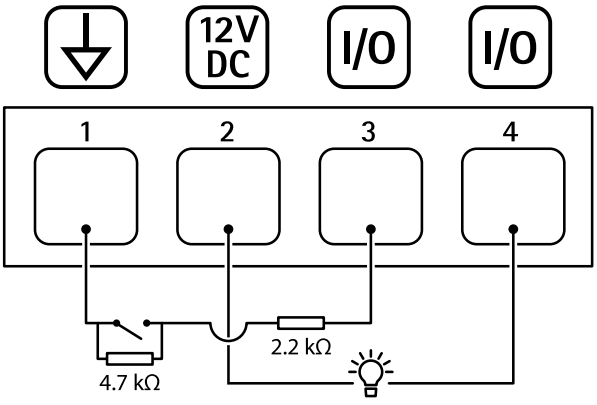
Saída digital – Para conectar dispositivos externos, como relés e LEDs. Os dispositivos conectados podem ser ativados pela interface de programação de aplicativos VAPIX®, por meio de um evento ou via interface web do dispositivo.

Bloco de terminais com 4 pinos



Função	Pino	Observações	Especificações
Terra CC	1		0 V CC
Saída CC	2	⚠ Pode ser usada para alimentar equipamentos auxiliares. Observação: esse pino pode ser usado somente como saída de energia.	12 V CC Carga máxima = 50 mA
Configurável (entrada ou saída)	3–4	Entrada digital ou entrada supervisionada – Conecte ao pino 1 para ativar ou deixe aberta (desconectada) para desativar. Para usar a entrada supervisionada, instale resistores de terminação. Veja o diagrama de conexão para obter informações de como conectar os resistores.	0 a 30 V CC máx.
		Saída digital – Conectado internamente ao pino 1 (terra CC) quando ativo, flutuante (desconectado) quando inativo. Se usada com uma carga indutiva (por exemplo, um relé), conecte um diodo em paralelo à carga para proporcionar proteção contra transientes de tensão.	0 a 30 V CC máx., dreno aberto, 100 mA

Exemplo:



1 Terra CC

2 Saída CC 12 V, máx. 50 mA
3 E/S configurada como entrada supervisionada
4 E/S configurada como saída

Observação

O comprimento máximo do cabo conectado é de 30 m (98,4 ft).

Nomes de padrões de luz

Desligado
Steady (Aceso)
Alternada
Pulso
Escalonar 3 etapas
Piscar
Piscar 3x
Piscar 4x
Piscar 3x e esmaecer
Piscar 4x e esmaecer
Flash 1x
Flash 3x
Direção A
Direção B
Direção C
Direção D
Rotação
Aleatório
Girar

Nomes de padrões sonoros

Alarme: Alarme com som agudo
Alarme: Alarme com som grave
Alarme: Pássaros
Alarme: Buzina de barco
Alarme: Alarme de carro
Alarme: Alarme de carro rápido
Alarme: Relógio clássico
Alarme: Primeiro respondedor
Alarme: Horror

Alarme: Industrial
Alarme: Bipe único
Alarme: Bipe quádruplo suave
Alarme: Bipe triplo suave
Alarme: Agudo triplo
Notificação: Aceito
Notificação: Chamada
Notificação: Negada
Notificação: Pronto
Notificação: Entrada
Notificação: Falhou
Notificação: Pressa
Notificação: Mensagem
Notificação: Avançar
Notificação: Aberta
Siren (Sirene): Alternada
Siren (Sirene): Saltada
Siren (Sirene): Evacuação
Siren (Sirene): Decaimento do tom
Siren (Sirene): Residencial suave

Limpeza do dispositivo

Você pode limpar o dispositivo com água morna e sabão neutro e não abrasivo.

OBSERVAÇÃO

- Produtos químicos abrasivos podem danificar o dispositivo. Não use produtos químicos como limpa-vidros ou acetona para limpar o dispositivo.
- Não borrife detergente diretamente no dispositivo. Borrife o detergente em um pano macio e use-o para limpar o dispositivo.
- Evite limpar o dispositivo sob luz solar direta ou em temperaturas elevadas, visto que isso pode causar manchas.

1. Use ar comprimido para remover qualquer poeira e sujeira solta do dispositivo.
2. Se necessário, limpe o dispositivo com um pano de microfibra macio umedecido com água morna e sabão neutro não abrasivo.
3. Para evitar manchas, seque o dispositivo com um pano limpo e macio.

Solução de problemas

Redefinição para as configurações padrão de fábrica

Importante

A restauração das configurações padrão de fábrica. deve ser feita com muito cuidado. Uma redefinição para os padrões de fábrica restaura todas as configurações, inclusive o endereço IP, para os valores padrão de fábrica.

Para redefinir o produto para as configurações padrão de fábrica:

1. Desconecte a alimentação do produto.
2. Mantenha o botão de controle pressionado enquanto reconecta a alimentação. Consulte .
3. Mantenha o botão de controle pressionado por 10 segundos até que o LED indicador de status se torne âmbar pela segunda vez.
4. Solte o botão de controle. O processo estará concluído quando o indicador do LED de estado ficar verde. Se nenhum servidor DHCP estiver disponível na rede, o endereço IP do dispositivo terá como padrão um dos seguintes:
   - **Dispositivos com AXIS OS 12.0 e posterior:** Obtido da sub-rede de endereços locais de link (169.254.0.0/16)
   - **Dispositivos com AXIS OS 11.11 e anterior:** 192.168.0.90/24
5. Use as ferramentas de software de instalação e gerenciamento, atribua um endereço IP, defina a senha e acesse o produto.

Você também pode redefinir os parâmetros para as configurações padrão de fábrica na interface Web do dispositivo. Vá para **Maintenance (Manutenção)** > **Factory default (Padrão de fábrica)** e clique em **Default (Padrão)**.

Opções do AXIS OS

A Axis oferece o gerenciamento de software de dispositivo de acordo com a trilha ativa ou com as trilhas de suporte de longo prazo (LTS). Estar na trilha ativa significa que você obtém acesso contínuo a todos os recursos de produtos mais recentes, enquanto as trilhas de LTS fornecem uma plataforma fixa com versões periódicas voltadas principalmente para correções de erros e atualizações de segurança.

Usar os AXIS OS da trilha ativa é recomendado se você deseja acessar os recursos mais recentes ou se você usa as ofertas de sistema ponta a ponta Axis. As trilhas de LTS são recomendados se você usa integrações de outros fabricantes, as quais podem não ser continuamente validadas com a trilha ativa mais recente. Com o LTS, os produtos podem manter a segurança cibernética sem apresentar quaisquer alterações funcionais significativas nem afetar quaisquer integrações existentes. Para obter informações mais detalhadas sobre a estratégia de software de dispositivos Axis, acesse *axis.com/support/device-software*.

Verificar a versão atual do AXIS OS

O AXIS OS determina a funcionalidade de nossos dispositivos. Durante o processo de solução de um problema, recomendamos que você comece conferindo a versão atual do AXIS OS. A versão mais recente pode conter uma correção que soluciona seu problema específico.

Para verificar a versão atual do AXIS OS:

1. Vá para a interface Web do dispositivo > **Status**.
2. Em **Device info (Informações do dispositivo)**, consulte a versão do AXIS OS.

Atualizar o AXIS OS

Importante

- As configurações pré-configuradas e personalizadas são salvas quando você atualiza o software do dispositivo (desde que os recursos estejam disponíveis no novo AXIS OS), embora isso não seja garantido pela Axis Communications AB.
- Certifique-se de que o dispositivo permaneça conectado à fonte de alimentação ao longo de todo o processo de atualização.

Observação

Quando você atualiza o dispositivo com a versão mais recente do AXIS OS na trilha ativa, o produto recebe a última funcionalidade disponível. Sempre leia as instruções de atualização e notas de versão disponíveis com cada nova versão antes de atualizar. Para encontrar a versão do AXIS OS e as notas de versão mais recentes, vá para *axis.com/support/device-software*.

1. Baixe o arquivo do AXIS OS para seu computador, o qual está disponível gratuitamente em *axis.com/ /support/device-software*.
2. Faça login no dispositivo como um administrador.
3. Vá para **Maintenance (Manutenção) > AXIS OS upgrade (Atualização do AXIS OS)** e clique em **Upgrade (Atualizar)**.

Após a conclusão da atualização, o produto será reiniciado automaticamente.

Problemas técnicos, dicas e soluções

Se você não conseguir encontrar aqui o que está procurando, experimente a seção de solução de problemas em *axis.com/support*.

Problemas ao atualizar o AXIS OS

Falha na atualização do AXIS OS	Se a atualização falhar, o dispositivo recarregará a versão anterior. O motivo mais comum é que o arquivo de incorreto do AXIS OS foi carregado. Verifique se o nome do arquivo do AXIS OS corresponde ao seu dispositivo e tente novamente.
Problemas após a atualização do AXIS OS	Se você tiver problemas após a atualização, reverta para a versão instalada anteriormente na página **Maintenance (Manutenção)**.

Problemas na configuração do endereço IP

O dispositivo está localizado em uma sub--rede diferente	Se o endereço IP destinado ao dispositivo e o endereço IP do computador usado para acessar o dispositivo estiverem localizados em sub-redes diferentes, você não poderá definir o endereço IP. Entre em contato com o administrador da rede para obter um endereço IP.

O endereço IP está sendo usado por outro dispositivo	Desconecte o dispositivo Axis da rede. Execute o comando ping (em uma janela de comando/DOS, digite `ping` e o endereço IP do dispositivo): • Se você receber: `Reply from <IP address>: bytes=32; time=10...`, significa que o endereço IP já pode estar sendo usado por outro dispositivo na rede. Obtenha um novo endereço IP junto ao administrador da rede e reinstale o dispositivo. • Se você receber: `Request timed out`, significa que o endereço IP está disponível para uso com o dispositivo Axis. Verifique todo o cabeamento e reinstale o dispositivo.
Possível conflito de endereço IP com outro dispositivo na mesma sub-rede	O endereço IP estático no dispositivo Axis é usado antes que o DHCP defina um endereço dinâmico. Isso significa que, se o mesmo endereço IP estático padrão também for usado por outro dispositivo, poderá haver problemas para acessar o dispositivo.

O dispositivo não pode ser acessado por um navegador

Não é possível fazer login	Quando o HTTPS estiver ativado, certifique-se de que o protocolo correto (HTTP ou HTTPS) seja usado ao tentar fazer login. Talvez seja necessário digitar manualmente `http` ou `https` no campo de endereço do navegador. Se a senha da conta root for perdida, o dispositivo deverá ser restaurado para as configurações padrão de fábrica. Consulte .
O endereço IP foi alterado pelo DHCP	Os endereços IP obtidos de um servidor DHCP são dinâmicos e podem mudar. Se o endereço IP tiver sido alterado use o AXIS IP Utility ou o AXIS Device Manager para localizar o dispositivo na rede. Identifique o dispositivo usando seu modelo ou número de série ou nome de DNS (se um nome tiver sido configurado). Se necessário, um endereço IP estático poderá ser atribuído manualmente. Para obter instruções, vá para *axis.com/support*.
Erro de certificado ao usar IEEE 802.1X	Para que a autenticação funcione corretamente, as configurações de data e hora no dispositivo Axis deverão ser sincronizadas com um servidor NTP. Vá para **System > Date and time (Sistema > Data e hora)**.

O dispositivo está acessível local, mas não externamente

Para acessar o dispositivo externamente, recomendamos que você use um dos seguintes aplicativos para Windows®:

- AXIS Camera Station Edge: grátis, ideal para sistemas pequenos com necessidades básicas de monitoramento.
- AXIS Camera Station 5: versão de avaliação grátis por 30 dias, ideal para sistemas de pequeno a médio porte.
- AXIS Camera Station Pro: versão de avaliação grátis por 90 dias, ideal para sistemas de pequeno a médio porte.

Para obter instruções e baixar o aplicativo, acesse *axis.com/vms*.

Problemas com arquivos de som	
Não é possível carregar clipe de mídia	Os seguintes formatos de clipes áudio são suportados: • formato de arquivo AU, codificado em µ-Law e amostragem de 8 ou 16 kHz. • formato de arquivo WAV codificado em áudio PCM. Ele oferece suporte a codificação de 8 ou 16 bits mono ou estéreo e amostragem de 8 a 48 kHz. • formato de arquivo MP3 mono ou estéreo com taxa de bits de 64 kbps a 320 kbps e taxa de amostragem de 8 a 48 kHz.
Um arquivo de som é gravado com um determinado ganho. Se seus clipes de áudio foram criados com ganhos diferentes, eles serão reproduzidos com uma intensidade diferente. Certifique-se de usar clipes com o mesmo ganho.	Os clipes de mídia são reproduzidos com diferentes volumes

Não é possível conectar através da porta 8883 com MQTT sobre SSL.	
O firewall bloqueia o tráfego usando a porta 8883, pois é considerada insegura.	Em alguns casos, o servidor/broker pode não fornecer uma porta específica para a comunicação MQTT. Ainda é possível usar MQTT em uma porta normalmente usada para tráfego HTTP/HTTPS. • Se o servidor/broker suporta WebSocket/WebSocket Secure (WS/WSS), geralmente na porta 443, use este protocolo em vez do MQTT. Verifique com o provedor do servidor/broker para saber se o WS/WSS é suportado e qual porta e caminho base devem ser usados. • Se o servidor/corretor suportar ALPN, o uso do MQTT poderá ser negociado em uma porta aberta, como a 443. Verifique com seu provedor de servidor/ /corretor se há suporte para ALPN e qual protocolo e porta ALPN usar.

Problemas com o som	
O dispositivo não está tão alto quanto esperado	Certifique-se de que o dispositivo esteja fechado corretamente e de que não haja obstruções na corneta ou no elemento do alto-falante.

Problemas com a luz	
O dispositivo não está tão forte quanto esperado	Verifique se uma fonte de alimentação PoE classe 4 está sendo usada. Verifique a temperatura ambiente do dispositivo. Se o dispositivo estiver instalado em um ambiente de alta temperatura, as luzes se esmaecerão automaticamente.

Considerações sobre desempenho

Ao configurar seu sistema, é importante considerar como várias configurações e situações afetam a quantidade de largura de banda (taxa de bits) necessária.

Os seguintes fatores importantes devem ser considerados:

- A utilização pesada da rede devido à infraestrutura ruim afeta a largura de banda.
- Executar vários aplicativos AXIS Camera Application Platform (ACAP) simultaneamente pode afetar o desempenho geral.

Entre em contato com o suporte

Se precisar de ajuda adicional, acesse *axis.com/support*.

T10217687_pt

2025-09 (M4.2)