

# AXIS D3110 Mk II Connectivity Hub

## Visão geral da solução

Este dispositivo torna possível a integração de sensores e áudio em sistemas de vídeo em rede que não têm esses recursos ou precisam de recursos adicionais. Ideal em uma solução ponta a ponta da Axis, ele ajuda a aumentar o reconhecimento da cena sem comprometer a segurança da rede.

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 Audio Manager Center** – Serviço em nuvem para acesso remoto e gerenciamento de sistemas multissite.
  - *Manual do usuário do AXIS Audio Manager Center*

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

## Instalação



Para assistir a este vídeo, vá para a versão Web deste documento.

## Início

### 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](http://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™	Firefox®	Edge™	Safari®
Windows®	recomendada	✓	recomendada	
macOS®	recomendada	✓	recomendada	✓*
Linux®	recomendada	✓	recomendada	
Outros sistemas operacionais	✓	✓	✓	✓

\*Não é totalmente compatível. Se tiver problemas de streaming de vídeo, use um navegador diferente.

### 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

Esta seção aborda todas as configurações importantes que um instalador precisa fazer para colocar o produto em funcionamento após a conclusão da instalação do hardware.

### Configuração de regras de eventos

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.

#### Detecção de manipulação com sinal de entrada

Este exemplo explica como enviar um email quando o sinal de entrada é cortado ou colocado em curto-circuito. Para mais informações sobre o conector E/S, veja .

1. Vá para **System > Accessories (Sistema > Acessórios) > I/O ports (Portas E/S)** e ative **Supervised (Supervisionada)** para a porta relevante.

Adicionar um destinatário de email:

1. Vá para **System > Events > Recipients (Sistema > Eventos > Destinatários)** e adicione um destinatário.
2. Digite um nome para o destinatário.
3. Selecione **Email**.
4. Digite um endereço de email para o qual a mensagem será enviada.
5. O dispositivo não tem seu próprio servidor de e-mail, portanto, será necessário fazer login em outro servidor de e-mail para enviar e-mails. Preencha as demais informações de acordo com seu provedor de email.
6. Para enviar um email de teste, clique em **Test (Testar)**.
7. Clique em **Salvar**.

Crie uma regra:

1. Acesse **System > Events > Rules (Sistema > Eventos > Regras)** e adicione uma regra:
2. Digite um nome para a regra.
3. Na lista de condições, em **I/O (E/S)**, selecione **Supervised input tampering is active (A detecção de manipulação da entrada supervisionada está ativa)**.
4. Selecione a porta relevante.
5. Na lista de ações, em **Notifications (Notificações)**, selecione **Send notification to email (Enviar notificação para email)** e, em seguida, selecione o destinatário na lista.
6. Digite um assunto e uma mensagem para o email.
7. Clique em **Salvar**.

## Ativar uma lâmpada quando a janela for aberta

Este exemplo explica como conectar um contato de janela a um hub de conectividade e como configurar um evento para ativar uma lâmpada quando uma janela com um contato instalado for aberta.

### Pré-requisitos

- Conecte um cabo de 2 fios (terra, E/S) ao contato da janela e ao conector de E/S no hub de conectividade.
- Conecte a lâmpada à alimentação e ao conector do relé no hub de conectividade.

### Configure as portas de E/S no hub de conectividade

1. Vá para **System > Accessories (Sistema > Acessórios)**.
2. Insira as seguintes informações em **Port 1 (Porta 1)**:
  - **Nome:** Sensor da janela
  - **Direction (Direção):** Entrada
  - **Normal state (Estado normal):** Circuito fechado
3. Insira as seguintes informações em **Port 2 (Porta 2)**:
  - **Nome:** Lâmpada
  - **Direction (Direção):** Saída
  - **Normal state (Estado normal):** Circuito aberto

### Crie duas regras no hub de conectividade

1. vá para **System > Events (Sistema > Eventos)** e adicione uma regra.
2. Insira as seguintes informações:
  - **Nome:** Sensor da janela
  - **Condition (Condição):** Entrada digital  
Selecione **Use this condition as a trigger (Usar esta condição como acionador)**.
  - **Porta:** Sensor da janela
  - **Action (Ação):** Toggle I/O while the rule is active (Alternar E/S enquanto a regra está ativa)
  - **Porta:** Lâmpada
  - **Estado:** Ativo
3. Clique em **Salvar**.

## Ativar o hub de conectividade via MQTT quando a câmera detectar movimento

### Pré-requisitos

- Configure um dispositivo para a porta de E/S 1 no hub de conectividade.
- Configure um broker de MQTT e obtenha endereço IP, nome de usuário e senha do agente.
- Configure o AXIS Motion Guard na câmera.

### Configure o cliente MQTT na câmera

1. Na interface de dispositivo 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 hub de conectividade

1. Na interface de dispositivo do hub de conectividade, 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):** Porta 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 hub de conectividade 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):** E/S > Toggle I/O while the rule is active (Alternar E/S enquanto a regra está ativa):

- Port (Porta): E/S 1.
3. Clique em Salvar.

### Abrir uma fechadura quando um botão é pressionado

Este exemplo explica como conectar um relé ao hub de conectividade e como configurar um evento para abrir uma fechadura quando alguém pressiona um botão conectado ao hub de conectividade.

#### Pré-requisitos

- Conecte um cabo de 2 fios (COM, NO) à fechadura e ao conector de relé no hub de conectividade.
- Conecte um cabo de 2 fios (terra, E/S) ao botão e ao conector de E/S no hub de conectividade.

#### Configure as portas de E/S no hub de conectividade

1. Vá para **System > Accessories (Sistema > Acessórios)**.
2. Insira as seguintes informações em **Port 1 (Porta 1)**:
  - **Nome:** Botão
  - **Direction (Direção):** Entrada
  - **Normal state (Estado normal):** Circuito aberto
3. Insira as seguintes informações em **Port 9 (Porta 9)**:
  - **Nome:** Travamento
  - **Normal state (Estado normal):** Circuito aberto

#### Crie uma regra no hub de conectividade

1. vá para **System > Events (Sistema > Eventos)** e adicione uma regra.
2. Insira as seguintes informações:
  - **Nome:** Abrir fechadura
  - **Condition (Condição):** I/O > Digital input is active (E/S > A entrada digital está ativa)  
Selecione **Use this condition as a trigger (Usar esta condição como acionador)**.
  - **Porta:** Botão
  - **Action (Ação):** I/O > Toggle I/O once (E/S > Alternar E/S uma vez):
  - **Porta:** Travamento
  - **Estado:** Ativo
  - **Duração:** 10 s
3. Clique em Salvar.

## Áudio

### Gravar áudio em cartão SD

Este exemplo explica como configurar a gravação de dois microfones em um cartão SD.

#### Antes de começar

- Conecte dois microfones e insira um cartão microSD no hub de conectividade.
1. Acesse **Áudio > Device settings (Configurações do dispositivo)** e ative **Input 0: IN 1 (Entrada 0: IN 1)** e **Input 1: IN 2 (Entrada 1: IN 2)**.
  2. Selecione **Input type (Tipo de entrada)** e **Power type (Tipo de alimentação)**.
  3. Se você espera que os níveis de som variem em toda a sala, ative o **Automatic gain control (Controle automático de ganho)**.
  4. Vá para **System > Storage > Onboard storage (Sistema > Armazenamento > Armazenamento interno)** e defina o **Retention time (Tempo de retenção)**.

5. Vá para **Audio > Stream (Áudio > Stream)** e selecione **Encoding (Codificação)**.

**Observação**

Para manter a carga da CPU baixa ao executar vários streams (por exemplo, gravação e transmissão ao vivo da mesma fonte), use a mesma codificação para ambos os streams.

6. Acesse **Audio > Listen and record (Áudio > Escutar e gravar)** e clique em .
7. Clique em .

## 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

### 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.

### 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.

### Cientes 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.

### 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.

## Analíticos

### AXIS Audio Analytics

**Deteção de áudio adaptativa:** ative para monitorar picos súbitos no volume sonoro detectado nas proximidades do dispositivo.

#### Configurações avançadas

- **Threshold (Limite):** mova o controle deslizante para ajustar o limiar de deteção. O limiar mínimo registrará até mesmo pequenos picos no som como deteção, enquanto o limiar máximo registrará apenas picos significativos.
- **Testar alarmes:** clique em **Testar** para acionar um evento de deteção para fins de teste.

**Classificação de áudio:** ative para monitorar tipos de sons específicos detectados nas proximidades do dispositivo.

#### Configurações avançadas

- **Grito:** ligue para ativar a deteção de gritos.
- **Berro:** ligue para ativar a deteção de berros.
- **Glass break (Quebra de vidro):** ligue para ativar a deteção de quebra de vidro.
- **Testar alarmes:** clique em **Testar** para acionar a deteção de um tipo de som 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.

**Tipo de entrada** ⓘ : selecione o tipo de entrada; por exemplo, microfone interno ou linha.

**Tipo de alimentação** ⓘ : selecione o tipo de alimentação para a entrada.

**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.

**Saída:** mostra o tipo de saída.

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

**Controle automático de volume** ⓘ : Ative para que o dispositivo ajuste o ganho de forma automática e dinâmica, com base no nível de ruído ambiente. O controle automático de volume afeta todas as saídas de áudio, incluindo linha e telebobina.

### 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.

## Melhoria de áudio

### Entrada

**Ten Band Graphic Audio Equalizer (Equalizador de áudio gráfico com dez faixas):** ative para ajustar o nível das diferentes faixas de frequência dentro de um sinal de áudio. Este recurso destina-se a usuários avançados com experiência em configuração de áudio.

**Faixa de talkback**  : Escolha o intervalo operacional para coletar conteúdo de áudio. Um aumento na faixa operacional causa uma redução dos recursos de comunicação bidirecional simultâneos.

**Melhoria de voz**  : Ative para aprimorar o conteúdo de voz em relação a outros sons.

## 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.

## 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](http://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.
  - **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.

- **Format (Formatar):** Selecione o formato a ser usado ao inserir a latitude e a longitude de seu dispositivo.
- **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](http://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 intercepções):** Ative para ativar o relatório de intercepções. O dispositivo usa intercepções para enviar mensagens sobre eventos importantes ou alterações de status para um sistema de gerenciamento. Na interface Web, você pode configurar intercepções para SNMP v1 e v2c. As intercepções serão desativadas automaticamente se você mudar para SNMP v3 ou desativar o SNMP. Se você usa SNMP v3, é possível configurar intercepções via aplicativo de gerenciamento do SNMP v3.
  - **Trap address (Endereço da intercepção):** Insira o endereço IP ou nome de host do servidor de gerenciamento.
  - **Trap community (Comunidade de intercepção):** Insira a comunidade que é usada quando o dispositivo envia uma mensagem de intercepção para o sistema de gerenciamento.
  - **Traps (Intercepções):**
    - **Cold start (Partida a frio):** Envia uma mensagem de intercepção quando o dispositivo é iniciado.
    - **Link up (Link ativo):** Envia uma mensagem de intercepção quando um link muda de inativo para ativo.
    - **Link down (Link inativo):** Envia uma mensagem de intercepção quando um link muda de ativo para inativo.
    - **Falha de autenticação:** Envia uma mensagem de intercepção quando uma tentativa de autenticação falha.

#### Observação

Todas as intercepções MIB de vídeo Axis são habilitados quando você ativa as intercepções 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 intercepções SNMP v1 e v2c não criptografadas. Se você usa SNMP v3, é possível configurar intercepções 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 tecla segura será selecionada, vá para [help.axis.com/en-us/axis-os#cryptographic-support](http://help.axis.com/en-us/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

**Activate (Ativar):** Ative o firewall.

**Default Policy (Política padrão):** Selecione o estado padrão do firewall.

- **Permitir:** Permite todas as conexões ao dispositivo. Essa opção é definida por padrão.
- **Deny (Negar):** Nega todas as conexões ao dispositivo.

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

- **Endereço:** Insira um endereço no formato IPv4/IPv6 ou CIDR ao qual deseja permitir ou negar o acesso.
- **Protocol (Protocolo):** Selecione um protocolo ao qual deseja permitir ou negar acesso.
- **Porta:** Insira um número de porta ao qual deseja permitir ou negar o acesso. Você pode adicionar um número de porta entre 1 e 65535.
- **Policy (Política):** Selecione a política da regra.



: Clique para criar outra regra.

**Adicionar regras:** Clique para adicionar as regras que você definiu.

- **Time in seconds (Tempo em segundos):** Defina um limite de tempo para testar as regras. O limite de tempo padrão está definido como 300 segundos. Para ativar as regras imediatamente, defina o tempo como 0 segundo.
- **Confirm rules (Confirmar regras):** Confirme as regras e o limite de tempo. Se você definiu um limite de tempo superior a 1 segundo, as regras permanecerão ativas nesse período. Se tiver definido o tempo para 0, as regras estarão ativas imediatamente.

**Pending rules (Regras pendentes):** Uma visão geral das regras testadas mais recentes que você ainda não confirmou.

### Observação

As regras com limite de tempo são exibidas em **Active rules (Regras ativas)** até que o temporizador exibido acabe ou até serem confirmados. Se elas não forem confirmadas, elas serão exibidas em **Pending rules (Regras pendentes)** assim que o temporizador chegar em zero e o firewall será revertido às configurações definidas anteriormente. Se você as confirmar, elas substituirão as regras ativas atuais.

**Confirm rules (Confirmar regras):** Clique para ativar as regras pendentes.

**Active rules (Regras ativas):** Uma visão geral das regras que você está executando no dispositivo.



: Clique para excluir uma regra ativa.



: Clique para excluir todas as regras, pendentes e ativas.

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 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*.

## 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.
- **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

Este dispositivo não é compatível com perfis ONVIF.

## 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.

## 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.

### Configuração de USB

**Enable on reboot (Ativar na reinicialização):** Ligue para ativar a funcionalidade USB. É necessário reiniciar o dispositivo para as alterações entrarem em vigor.

## 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.

### 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.

**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

### 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](http://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](http://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.
- **Autorollback (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)**  : redefine 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

#### 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](http://help.axis.com).

#### AXIS Audio Analytics

O AXIS Audio Analytics detecta aumentos súbitos no volume sonoro e tipos de sons específicos, como gritos dentro do alcance do dispositivo no qual ele 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*.

#### Cibersegurança

Para obter informações específicas do produto sobre segurança cibernética, consulte a folha de dados do produto em [axis.com](http://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](http://axis.com/security-notification-service).

#### Gerenciamento de vulnerabilidades

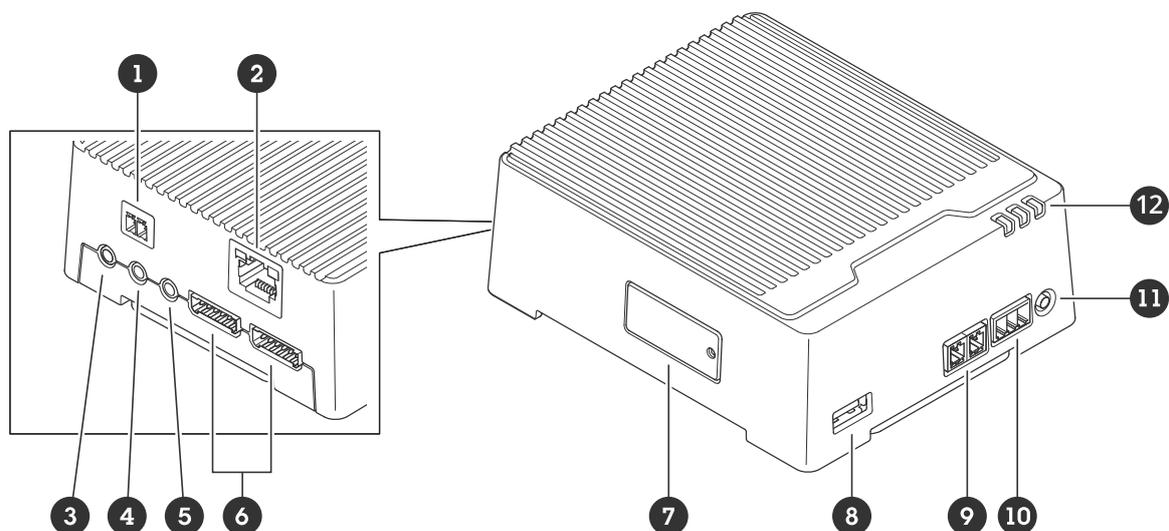
Para minimizar o risco de exposição dos clientes, a Axis, na condição de **Autoridade de Numeração (CNA) de Vulnerabilidades e Exposições Comuns (CVE)**, segue os padrões do setor para gerenciar e responder a vulnerabilidades descobertas em nossos dispositivos, software e serviços. Para obter mais informações 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](http://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 Conector de energia
- 2 Conector Ethernet RJ45
- 3 Porta do microfone 2 (analógica)
- 4 Porta 1 para microfone (digital e analógica)
- 5 Saída de áudio
- 6 2 x Conectores de E/S (6 pinos)
- 7 Entrada para cartão MicroSD
- 8 Porta USB
- 9 Conector RS485/RS422
- 10 Conector do relé
- 11 Botão de controle
- 12 LED de estado

### Slot de cartão SD

Para obter recomendações sobre cartões SD, consulte [axis.com](http://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:

- 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.

## Conectores

### Conector de rede

Conector Ethernet RJ45.

Entrada: Conector Ethernet RJ45 com Power over Ethernet (PoE).

Saída: Conector Ethernet RJ45 com Power over Ethernet (PoE).

### Conector de áudio

- **Entrada de áudio** (porta do microfone 1) – 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** (porta do microfone 2) – Entrada de 3,5 mm para um microfone mono analógico ou um sinal mono de entrada de áudio (o canal esquerdo é usado de um sinal estéreo).
- **Saída de áudio** – Saída de áudio (nível de linha) de 3,5 mm que pode ser conectada a um sistema de anúncio ao público (PA) ou um alto-falante ativo com amplificador integrado. Um par de fones de ouvido também pode ser conectado. É necessário um conector estéreo para a saída de áudio.



#### 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
Microfone equalizado (com ou sem alimentação phantom) ou entrada de áudio, sinal "quente"	Microfone equalizado (com ou sem alimentação phantom) ou entrada de áudio, sinal "frio"	Terra
Sinal digital	Ring power, se selecionado	Terra

#### Saída de áudio

1 Ponta	2 Anel	3 Luva
Canal 1, linha não equalizada, mono	Canal 1, linha não equalizada, mono	Terra

### Conector de E/S

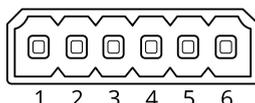
Use o conector de E/S com dispositivos externos em combinação com, por exemplo, detectores de movimento, acionadores de eventos e notificações de alarmes. Além do ponto de referência de 0 V CC e da alimentação (saída CC de 12 V), o conector do terminal de E/S fornece a interface para:

**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.

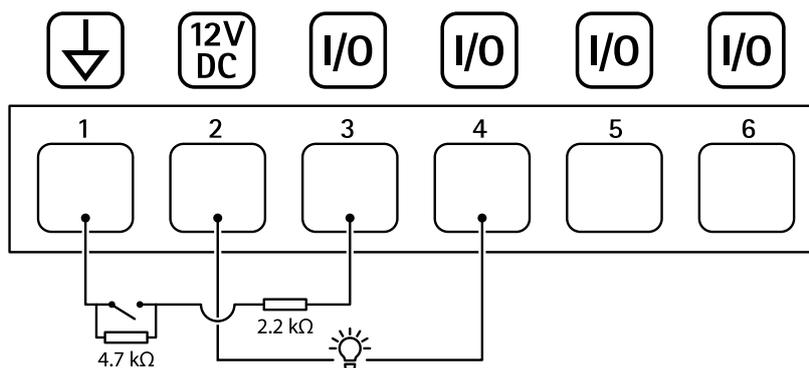
**Saída digital** – Para conectar dispositivos externos, como relés e LEDs. Os dispositivos conectados podem ser ativados pela interface de programação de aplicativos VAPIX®, por meio de um evento ou via interface web do dispositivo.

Bloco de terminais com 6 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)	3-6	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
- 5 E/S configurável
- 6 E/S configurável

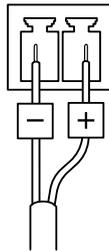
Especificação do desenho elétrico para E/S digital

Parâmetro	Valor
Durabilidade mínima da tensão de entrada	-30 V CC
Durabilidade máxima da tensão de entrada	+30 V CC
Tensão baixa máxima de entrada digital	+0,50 V a 25 °C +0,40 V a 85 °C
Tensão baixa mínima de entrada digital	+1,5 V
Tensão baixa máxima de saída a 100 mA	+0,6 V
Tensão baixa máxima de saída a 10 mA	+0,06 V

Tempo máximo de subida (incluindo atraso do GPIO) a 10 kHz	5 $\mu$ s
Tempo máximo de queda (incluindo atraso do GPIO) a 10 kHz	5 $\mu$ s
Corrente máxima de afundamento de saída	100 mA
Corrente máxima de fuga de E/S	100 $\mu$ A a 12 V CC

### Conector de energia

Bloco de terminais com 2 pinos para entrada de energia CC Use uma fonte de energia com limitação compatível com os requisitos de voltagem de segurança extra baixa (SELV) e com potência de saída nominal restrita a  $\leq 100$  W ou corrente de saída nominal limitada a  $\leq 5$  A.

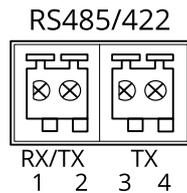


### Conector RS485/RS422

Blocos terminais com 2 pinos para interface serial RS485/RS422.

A porta serial pode ser configurada para suportar:

- RS485 com 2 fios half duplex
- RS485 com 4 fios full duplex
- RS422 com 2 fios simplex
- RS422 com 4 fios full duplex com comunicação ponto a ponto



Função	Pino	Observações
RS485/RS422 RX/TX A	1	(RX) Para RS485/RS422 full duplex (RX/TX) Para RS485 half duplex
RS485/RS422 RX/TX B	2	
RS485/RS422 TX A	3	(TX) Para RS485/RS422 full duplex
RS485/RS422 TX B	4	

## Limpeza do dispositivo

Você pode limpar o dispositivo com água morna.

### **OBSERVAÇÃO**

- Produtos químicos abrasivos podem danificar o dispositivo. Não use produtos químicos como limpavidros ou acetona 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 umedecido com água morna.
  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 cerca de 15 a 30 segundos até que o indicador do LED de estado pisque com a cor âmbar.
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 para atribuir um endereço IP, definir a senha e acessar o dispositivo.  
As ferramentas de software de instalação e gerenciamento estão disponíveis nas páginas de suporte em [axis.com/support](http://axis.com/support).

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](http://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](http://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](http://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](http://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 <b>Maintenance (Manutenção)</b> .

### 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 <code>ping</code> e o endereço IP do dispositivo): <ul style="list-style-type: none"><li>Se você receber: <code>Reply from &lt;IP address&gt;: bytes=32; time=10...</code>, 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.</li><li>Se você receber: <code>Request timed out</code>, significa que o endereço IP está disponível para uso com o dispositivo Axis. Verifique todo o cabeamento e reinstale o dispositivo.</li></ul>
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 <code>http</code> ou <code>https</code> 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 <a href="http://axis.com/support">axis.com/support</a> .
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 <b>System &gt; Date and time (Sistema &gt; Data e hora)</b> .

### 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](http://axis.com/vms).

### 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.

### Considerações sobre desempenho

Os seguintes fatores importantes devem ser considerados:

- A utilização pesada da rede devido à infraestrutura ruim afeta a largura de banda.
- Executar várias atividades ao mesmo tempo pode afetar o desempenho de áudio.

### Entre em contato com o suporte

Se precisar de ajuda adicional, acesse [axis.com/support](https://axis.com/support).



T10208737\_pt

2025-05 (M4.10)

© 2025 Axis Communications AB