

AXIS XC1311 Explosion-Protected Horn Speaker

Índice

Visão geral da solução.....	3
.....	3
Início.....	4
Encontre o dispositivo na rede.....	4
Suporte a navegadores.....	4
Abra a interface web do dispositivo.....	4
Criar uma conta de administrador.....	4
Senhas seguras.....	5
Visão geral da interface Web.....	5
Configure seu dispositivo.....	6
Calibrar e executar um teste de alto-falante remoto.....	6
Configuração de SIP direto (P2P).....	6
Configuração de SIP por meio de um servidor (PBX).....	7
Configuração de regras de eventos.....	7
Envio de um email em caso de falha no teste de alto-falante.....	8
Reprodução de áudio quando uma câmera detecta movimento.....	9
Parar áudio com DTMF.....	9
Configurar áudio para chamadas de entrada SIP.....	10
A interface Web.....	12
Saiba mais.....	13
Session Initiation Protocol (SIP).....	13
SIP ponto a ponto (P2PSIP).....	13
Private Branch Exchange (PBX).....	13
NAT traversal.....	14
Analíticos e aplicativos.....	14
Especificações.....	15
Visão geral do produto.....	15
Indicadores de LED.....	15
Botões.....	16
Botão de controle.....	16
Conectores.....	16
Terminal de aterramento de proteção.....	16
Conector de rede.....	16
Comandos da API.....	17
Solução de problemas.....	18
Redefinição para as configurações padrão de fábrica.....	18
Opções do AXIS OS.....	18
Verificar a versão atual do AXIS OS.....	18
Atualizar o AXIS OS.....	19
Problemas técnicos e possíveis soluções.....	19
Considerações sobre desempenho.....	21
Entre em contato com o suporte.....	22
Cibersegurança.....	23
Gerenciamento de vulnerabilidades.....	23
Notificações de segurança.....	23
Ciclo de vida seguro do produto.....	23

Visão geral da solução

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

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

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

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



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

Uma visão geral de como o áudio em rede funciona.

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.

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

Suporte a navegadores

O dispositivo pode ser usado com os seguintes navegadores:

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

✓: Recomendado

*: Compatível com limitações

Abra a interface web do dispositivo

1. Abra um navegador e digite o endereço IP ou o nome de host do dispositivo Axis. Se você não souber o endereço IP, use o AXIS IP Utility ou o AXIS Device Manager para localizar o dispositivo na rede.
2. Digite o nome de usuário e a senha. Se você acessar o dispositivo pela primeira vez, você deverá criar uma conta de administrador. Consulte *Criar uma conta de administrador, on page 4*.

Para obter descrições de todos os recursos e configurações na interface Web de dispositivos com AXIS OS, consulte *Ajuda da interface Web do AXIS OS*.

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 *Senhas seguras, on page 5*.
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 *Redefinição para as configurações padrão de fábrica, on page 18*.

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.

Visão geral da interface Web

Este vídeo oferece uma visão geral sobre a interface Web do dispositivo.



Interface Web de um dispositivo Axis

Configure seu dispositivo

Calibrar e executar um teste de alto-falante remoto

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

Observação

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

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

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

Observação

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

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

Observação

Também é possível executar a calibração pressionando o botão de controle no dispositivo físico. Consulte *Visão geral do produto, on page 15* para identificar o botão de controle.

Configuração de SIP direto (P2P)

Use ponto a ponto quando a comunicação for feita entre alguns agentes de usuário na mesma rede IP e não houver necessidade de recursos adicionais que poderiam ser fornecidos por um servidor PBX.

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

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

Observação

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

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

Configuração de SIP por meio de um servidor (PBX)

Use um servidor PBX quando os agentes de usuário se comunicarem dentro e fora da rede IP. Recursos adicionais podem ser adicionados à configuração dependendo do provedor de PBX.

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

1. Solicite as seguintes informações do seu provedor de PBX:
 - ID de usuário
 - Domínio
 - Senha
 - ID de autenticação
 - ID do chamador
 - Registrador
 - Porta de início de RTP
2. Para adicionar uma nova conta, vá para **System (Sistema) > SIP > SIP accounts (Contas SIP)** e clique em **+ Account (+ Conta)**.
3. Insira os detalhes que você recebeu de seu provedor de PBX.
4. Selecione **Registered (Registrado)**.
5. Selecione um modo de transporte.
6. Clique em **Salvar**.
7. Defina as configurações de SIP da mesma forma que para ponto a ponto. Consulte *Configuração de SIP direto (P2P)*, on page 6 para obter mais informações.

Configuração de regras de eventos

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

Para saber mais, consulte *Comece a utilizar regras para eventos*.

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

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

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

Observação

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

- 2.8. Clique em **Salvar**.
3. Configure o teste de alto-falante automatizado:
 - 3.1. Vá para a interface do dispositivo > **System (Sistema)** > **Events (Eventos)** > **Rules (Regras)**.
 - 3.2. Clique em **Add a rule (Adicionar uma regra)**.
 - 3.3. Insira um nome para a regra.
 - 3.4. Em **Condition (Condição)**, selecione **Schedule (Agendamento)** e selecione na lista de acionadores
 - 3.5. Em **Schedule (Agendamento)**, selecione seu agendamento ("Daily at 6pm" (Diariamente às 18h)).
 - 3.6. Em **Action (Ação)**, selecione **Run automatic speaker test (Executar teste de alto-falante automático)**.
 - 3.7. Clique em **Salvar**.
4. Configure a condição para enviar um email quando o teste de alto-falante falhar:
 - 4.1. Vá para a interface do dispositivo > **System (Sistema)** > **Events (Eventos)** > **Rules (Regras)**.
 - 4.2. Clique em **Add a rule (Adicionar uma regra)**.
 - 4.3. Insira um nome para a regra.
 - 4.4. Em **Condition (Condição)**, selecione **Speaker test result (Resultado do teste de alto-falante)**.
 - 4.5. Em **Speaker test status (Status do teste de alto-falante)**, select **Didn't pass the test (Reprovado no teste)**.
 - 4.6. Em **Action (Ação)**, selecione **Send notification to email (Enviar notificação para email)**.
 - 4.7. Em **Recipient (Destinatário)**, selecione seu destinatário ("Speaker test recipients" (Destinatários do teste de alto-falante))
 - 4.8. Insira um assunto e uma mensagem e clique em **Save (Salvar)**.

Reprodução de áudio quando uma câmera detecta movimento

Este exemplo explica como configurar o dispositivo de áudio para reproduzir um clipe de áudio quando uma câmera de rede Axis detecta movimento.

Pré-requisitos

- O dispositivo de áudio Axis e a câmera de rede Axis estão localizados na mesma rede.
 - O aplicativo de detecção de movimento está configurado e em execução na câmera.
1. Preparação de um link para o clipe de áudio
 - 1.1. Vá para **Audio (Áudio) > Audio clips (Clipes de áudio)**.
 - 1.2. Clique em  > **Create link (Criar link)** para obter um clipe de áudio.
 - 1.3. Defina o volume e o número de vezes para repetir o clipe.
 - 1.4. Clique no ícone de cópia para copiar o link.
 2. Crie uma regra de ação:
 - 2.1. Vá para **System (Sistema) > Events (Eventos) > Recipients (Destinatários)**.
 - 2.2. Clique em **+ Add recipient (+ Adicionar destinatário)**.
 - 2.3. Digite um nome para o destinatário, por exemplo, "Alto-falante".
 - 2.4. Selecione **HTTP** na lista suspensa **Type (Tipo)**.
 - 2.5. Cole o link configurado do dispositivo de áudio no campo **URL**.
 - 2.6. Insira o nome de usuário e a senha do dispositivo de áudio.
 - 2.7. Clique em **Salvar**.
 - 2.8. Vá para **Rules (Regras)** e clique em **+ Add a rule (+ Adicionar uma regra)**.
 - 2.9. Digite um nome para a regra de ação. Por exemplo, "Play clip" (Reproduzir clipe).
 - 2.10. Na lista **Condition (Condição)**, selecione uma alternativa de detecção de movimento por vídeo em **Applications (Aplicativos)**.

Observação

Se não houver opções para detecção de movimento por vídeo, vá para **Apps (Aplicativos)**, clique em **AXIS Video Motion Detection** e ative a detecção de movimento por vídeo.

- 2.11. Na lista **Action (Ações)**, selecione **Send notification through HTTP (Enviar notificação via HTTP)**.
- 2.12. Em **Recipient (Destinatário)**, selecione seu destinatário.
- 2.13. Clique em **Save (Salvar)**.

Parar áudio com DTMF

Este exemplo explica como:

- Configure o DTMF em um dispositivo.
 - Configure um evento para parar o áudio quando um comando DTMF é enviado para o dispositivo.
1. Vá para **System (Sistema) > SIP > SIP settings (Configurações do SIP)**.
 2. Certifique-se de que **Enable SIP (Ativar SIP)** esteja ativada.
Se for necessário ativá-la, lembre-se de clicar em **Save (Salvar)** posteriormente.
 3. Vá para **SIP accounts (Contas SIP)**.
 4. Ao lado da conta SIP, clique em  > **Edit (Editar)**.
 5. Em **DTMF**, clique em **+ DTMF sequence (+ Sequência DTMF)**.
 6. Em **Sequence (Sequência)**, insira "1".

7. Em **Description (Descrição)**, insira "stop audio" (parar áudio).
8. Clique em **Salvar**.
9. Vá para **System (Sistema) > Events (Eventos) > Rules (Regras)** e clique em **+ Add a rule (+ Adicionar uma regra)**.
10. Em **Name (Nome)**, digite "DTMF stop audio" (Parar áudio DTMF).
11. Em **Condition (Condição)**, selecione **DTMF**.
12. Em **DTMF Event ID (ID do evento DTMF)**, selecione **stop audio (parar áudio)**.
13. Em **Action (Ação)**, selecione **Stop playing audio clip (Parar reprodução de clipe de áudio)**.
14. Clique em **Salvar**.

Configurar áudio para chamadas de entrada SIP

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

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

Ativar configurações de SIP:

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

Reproduzir áudio quando uma chamada SIP for recebida:

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

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

1. Vá para **Settings > System > Events > Rules (Configurações > Sistema > Eventos)** e adicione uma regra.
2. Digite um nome para a regra.
3. Na lista de condições, selecione **Audio clip playing (Reprodução de clipe de áudio)**.

4. Marque a opção **Use this condition as a trigger** (Usar esta condição como acionador).
5. Marque **Invert this condition** (Inverter esta condição).
6. Clique em **+ Add a condition** (+ Adicionar uma condição) para adicionar uma segunda condição ao evento.
7. Na lista de condições, selecione **State** (Estado).
8. Na lista de estados, selecione **Ringin** (Tocando).
9. Na lista de ações, selecione **Answer call** (Atender chamada).
10. Clique em **Save** (Salvar).

A interface Web

Para ler sobre todos os recursos e configurações disponíveis na interface Web de dispositivos com AXIS OS, vá para *Ajuda da interface Web do AXIS OS*.

Saiba mais

Session Initiation Protocol (SIP)

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

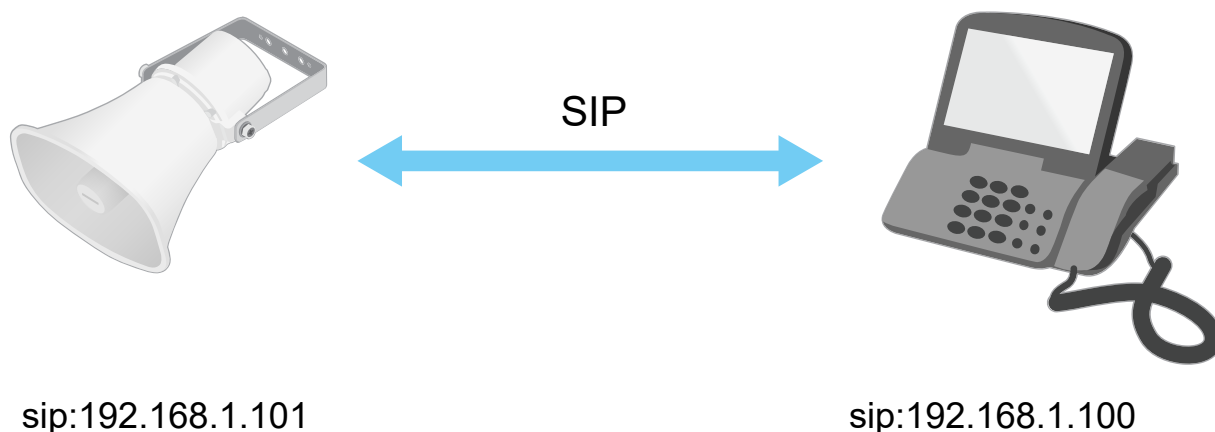
O áudio ou vídeo efetivos são trocados entre os agentes de usuário SIP com um protocolo de transporte, por exemplo, RTP (Real-Time Transport Protocol).

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

SIP ponto a ponto (P2PSIP)

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

Exemplo:



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

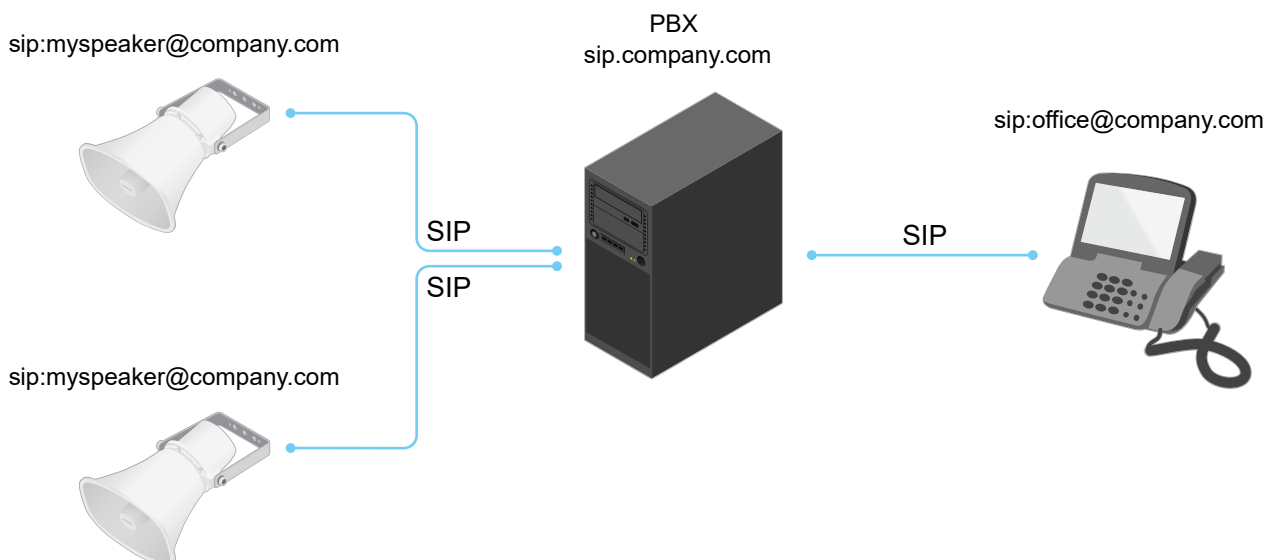
Private Branch Exchange (PBX)

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

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

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

Exemplo:



NAT traversal

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

Observação

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

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

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

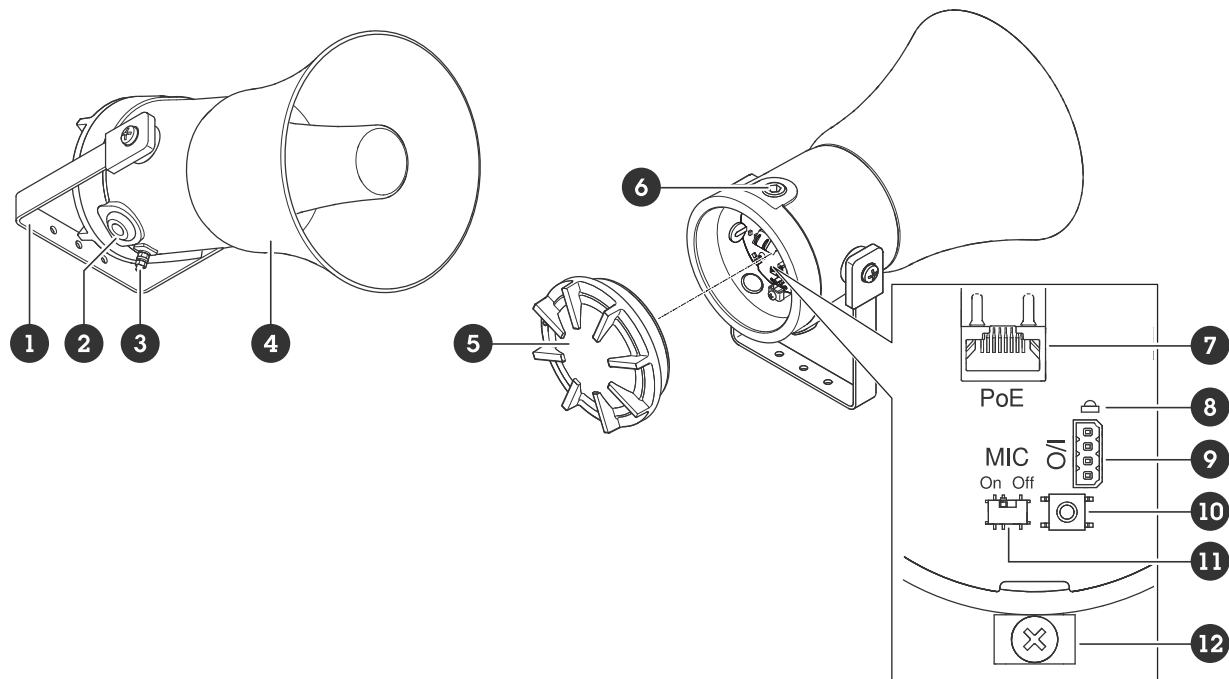
Analíticos e aplicativos

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

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

Especificações

Visão geral do produto



- 1 Suporte
- 2 Gaxeta
- 3 Terminal de aterramento externo
- 4 Corneta
- 5 Tampa
- 6 Gaxeta
- 7 Conector de rede
- 8 LED indicador de status
- 9 Porta de E/S
- 10 Botão de controle
- 11 Chave de desativação do microfone
- 12 Terminal de aterramento interno

Indicadores de LED

LED de estado	Indicação
Apagado	Apagado para funcionamento normal.
Verde	Aceso por 10 segundos para operação normal após a conclusão da inicialização.
Âmbar	Aceso durante a inicialização. Pisca durante uma atualização do software do dispositivo ou redefinição para o padrão de fábrica.
Âmbar/Vermelho	Pisca quando a conexão de rede não está disponível ou foi perdida.
Vermelho	Pisca lentamente se houver falha na atualização.
Vermelho/Verde	Pisca rapidamente quando Locate device (Localizar dispositivo) é selecionado.

Botões

Botão de controle

O botão de controle é usado para:

- Calibrar o teste de alto-falante. Pressione e solte rapidamente o botão de controle. Um tom de teste é reproduzido.
- Restaurar o produto para as configurações padrão de fábrica. Consulte *Redefinição para as configurações padrão de fábrica, on page 18*.

Conectores

Terminal de aterramento de proteção

▲ PERIGO

Risco de choque elétrico. O produto deve ser aterrado por um fio terra. Certifique-se de que ambas as extremidades do fio terra estejam em contato com suas respectivas superfícies de aterramento.

Certifique-se de que o fio de aterramento seja o mais curto possível para minimizar o caminho da corrente.

Conector de rede

Conector Ethernet RJ45 com Power over Ethernet (PoE).

OBSERVAÇÃO

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

Comandos da API

VAPIX® é a API (interface de programação de aplicativos) aberta pertencente à Axis. Você pode controlar quase todas as funcionalidades disponíveis nos dispositivos Axis via VAPIX®. Para obter acesso à documentação completa da VAPIX®, ingresse na comunidade de desenvolvedores Axis em axis.com/developer-community

Insira os comandos em um navegador Web e substitua <deviceIP> pelo endereço IP ou o nome de host do seu dispositivo.

Importante

Os comandos da API são executados imediatamente. Se você restaurar ou redefinir seu dispositivo, todas as configurações serão perdidas. Por exemplo, regras de ação.

Exemplo: Request

Reiniciar o dispositivo

Request

`http://<deviceIP>/axis-cgi/restart.cgi`

Exemplo: Request

Restaure o dispositivo. A solicitação retorna a maioria das configurações para os valores padrão, mas mantém o número IP.

Request

`http://<deviceIP>/axis-cgi/factorydefault.cgi`

Exemplo: Request

Redefina o dispositivo. A solicitação retorna todas as configurações, incluindo o endereço IP, para os valores padrão.

Request

`http://<deviceIP>/axis-cgi/hardfactorydefault.cgi`

Exemplo: Request

Veja uma lista de todos os parâmetros do dispositivo.

Request

`http://<deviceIP>/axis-cgi/param.cgi?action=list`

Exemplo: Request

Obtenha um arquivo de depuração

Request

`http://<deviceIP>/axis-cgi/debug/debug.tgz`

Exemplo: Request

Obtenha um relatório do servidor

Request

`http://<deviceIP>/axis-cgi/serverreport.cgi`

Exemplo: Request

Capture um traço de rede de 300 segundos

Request

`http://<deviceIP>/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=300`

Exemplo: Request

Ative FTP

Request

`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=yes`

Exemplo: Request

Desative FTP

Request

`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no`

Exemplo: Request

Ative SSH

Request

`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=yes`

Exemplo: Request

Desative SSH

Request

`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no`

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 *Visão geral do produto*, on page 15.
3. Mantenha o botão de controle pressionado por 10 segundos até que o LED indicador de status se torne âmbar pela segunda vez.
4. Solte o botão de controle. O processo estará concluído quando o indicador do LED de estado ficar verde. Se nenhum servidor DHCP estiver disponível na rede, o endereço IP do dispositivo terá como padrão um dos seguintes:
 - Dispositivos com AXIS OS 12.0 e posterior: Obtido da sub-rede de endereços locais de link (169.254.0.0/16)
 - Dispositivos com AXIS OS 11.11 e anterior: 192.168.0.90/24
5. Use as ferramentas de software de instalação e gerenciamento, atribua um endereço IP, defina a senha e acesse o produto.

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

Opções do AXIS OS

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

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

Verificar a versão atual do AXIS OS

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

Para verificar a versão atual do AXIS OS:

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

Atualizar o AXIS OS

Importante

- Ao atualizar o software do dispositivo, suas configurações pré-definidas e personalizadas serão salvas. A Axis Communications AB não pode garantir que as configurações sejam salvas, mesmo que os recursos estejam disponíveis na nova versão do AXIS OS.
- A partir do AXIS OS 12.6, é necessário instalar todas as versões LTS entre a versão atual do seu dispositivo e a versão de destino. Por exemplo, se a versão atual do software do dispositivo instalada for AXIS OS 11.2, é necessário instalar a versão LTS AXIS OS 11.11 antes de poder atualizar o dispositivo para o AXIS OS 12.6. Para obter mais informações, consulte *Guia do ciclo de vida do AXIS OS: Caminho de atualização*.
- Certifique-se de que o dispositivo permaneça conectado à fonte de alimentação ao longo de todo o processo de atualização.

Observação

- Quando você atualiza o dispositivo com a versão mais recente do AXIS OS na trilha ativa, o produto recebe a última funcionalidade disponível. Sempre leia as instruções de atualização e notas de versão disponíveis com cada nova versão antes de atualizar. Para encontrar a versão do AXIS OS e as notas de versão mais recentes, vá para axis.com/support/device-software.
1. Baixe o arquivo do AXIS OS para seu computador, o qual está disponível gratuitamente em axis.com/support/device-software.
 2. Faça login no dispositivo como um administrador.
 3. Vá para **Maintenance (Manutenção) > AXIS OS upgrade (Atualização do AXIS OS)** e clique em **Upgrade (Atualizar)**.

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

Problemas técnicos e possíveis soluções

Problemas ao atualizar o AXIS OS

A atualização do AXIS OS falhou

Se a atualização falhar, o dispositivo recarregará a versão anterior. O motivo mais comum é que o arquivo de incorreto do AXIS OS foi carregado. Verifique se o nome do arquivo do AXIS OS corresponde ao seu dispositivo e tente novamente.

Problemas após a atualização do AXIS OS

Se você tiver problemas após a atualização, reverta para a versão instalada anteriormente na página **Maintenance (Manutenção)**.

Problemas na configuração do endereço IP

Não é possível definir o endereço IP

- 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 pode estar sendo utilizado por outro dispositivo. Para verificar:
 1. Desconecte o dispositivo Axis da rede.
 2. Em uma janela de comando/DOS, digite `ping` e o endereço IP do dispositivo.
 3. Se receber: `Reply from <IP address>: bytes=32; time=10...`, isso 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.
 4. Se você receber: `Request timed out`, significa que o endereço IP está disponível para uso com o dispositivo Axis. Verifique todo o cabeamento e reinstale o dispositivo.
- Pode haver um 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.

Problemas com o acesso ao dispositivo

Não é possível fazer login ao acessar o dispositivo em um navegador

Quando o HTTPS estiver ativado, certifique-se de utilizar o protocolo correto (HTTP ou HTTPS) ao tentar fazer login. Talvez seja necessário digitar manualmente `http` ou `https` no campo de endereço do navegador.

Caso tenha perdido a senha da conta root, será necessário redefinir o dispositivo para as configurações padrão de fábrica. Para obter instruções, consulte *Redefinição para as configurações padrão de fábrica, on page 18*.

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, é possível atribuir um endereço IP estático de forma manual. Para obter instruções, vá para axis.com/support.

Erro de certificado ao usar IEEE 802.1X

Para que a autenticação funcione corretamente, as configurações de data e hora no dispositivo Axis deverão ser sincronizadas com um servidor NTP. Vá para **System > Date and time (Sistema > Data e hora)**.

O navegador não é compatível

Para obter uma lista dos navegadores recomendados, consulte *Suporte a navegadores, on page 4*.

Não é possível acessar o dispositivo 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 Pro: versão de avaliação grátis por 90 dias, ideal para sistemas de pequeno a médio porte.

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

Problemas com arquivos de áudio

Não é possível carregar clipe de mídia

Os seguintes formatos de clipes áudio são suportados:

- formato de arquivo AU, codificado em μ -Law e amostragem de 8 ou 16 kHz.
- formato de arquivo WAV codificado em áudio PCM. Ele oferece suporte a codificação de 8 ou 16 bits mono ou estéreo e amostragem de 8 a 48 kHz.
- formato de arquivo MP3 mono ou estéreo com taxa de bits de 64 kbps a 320 kbps e taxa de amostragem de 8 a 48 kHz.

Os clipes de mídia são reproduzidos com diferentes volumes

Um arquivo de som é gravado com um determinado ganho. Se seus clipes de áudio foram criados com ganhos diferentes, eles serão reproduzidos com uma intensidade diferente. Certifique-se de usar clipes com o mesmo ganho.

Problemas com MQTT

Não é possível conectar através da porta 8883 com MQTT sobre SSL.

O firewall bloqueia o tráfego que utiliza a porta 8883, uma vez que é considerado inseguro.

Em alguns casos, o servidor/broker pode não fornecer uma porta específica para a comunicação MQTT. Ainda será 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.

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

Considerações sobre desempenho

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

Os fatores mais importantes a serem considerados são:

- A utilização pesada da rede devido à infraestrutura ruim afeta a largura de banda.

- Executar vários aplicativos AXIS Camera Application Platform (ACAP) simultaneamente pode afetar o desempenho geral.

Entre em contato com o suporte

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

Cibersegurança

A segurança cibernética oferece suporte a um ciclo de vida de produto bem-sucedido com riscos minimizados. Você pode encontrar informações e documentação detalhadas sobre nossa abordagem de segurança cibernética em axis.com/about-axis/cybersecurity. Siga as diretrizes de segurança cibernética abaixo para receber notificações de segurança de produtos da Axis e para configurar seu produto para um ciclo de vida e desativação seguros.

No *Axis Trust Center*, você pode encontrar informações sobre como a Axis implementa a conformidade de segurança, a transparência, a proteção de dados e a privacidade.

Gerenciamento de vulnerabilidades

A Axis é uma *Autoridade de numeração de vulnerabilidades e exposições comuns (CVE) (CNA)*. Para minimizar seu risco de exposição, seguimos os padrões do setor ao identificar e resolver vulnerabilidades em nossos dispositivos, software e serviços. Consulte axis.com/vulnerability-management para obter informações sobre nossa política de gerenciamento de vulnerabilidades ou para relatar uma vulnerabilidade.

Notificações de segurança

Assine os e-mails de notificação de segurança da Axis em axis.com/security-notification-service. Enviaremos a você informações sobre vulnerabilidades, avisos de segurança correspondentes e outros assuntos relacionados à segurança de seu produto Axis.

Ciclo de vida seguro do produto

A Axis minimiza os riscos durante toda a vida útil de nossos produtos por meio do gerenciamento seguro do ciclo de vida. Use nossos guias para aumento do nível de proteção em help.axis.com para configurar e operar com mais segurança seus produtos Axis e para encontrar informações sobre:

Uso seguro desde o primeiro uso – Os produtos Axis são pré-configurados com alta proteção padrão para permitir a inicialização segura e a comunicação criptografada desde o início.

Uso pretendido e erros comuns de configuração – Nossos guias fornecem informações sobre o uso pretendido dos produtos Axis, incluindo erros comuns de configuração e usos indevidos relevantes para a segurança que devem ser evitados.

Gerenciamento de vulnerabilidades e transparência da cadeia de suprimentos – Uma lista de materiais de software (SBOM) é publicada com cada versão de software em axis.com para divulgar vulnerabilidades e aumentar a transparência da cadeia de suprimentos.

Descomissionamento e exclusão segura de dados – Para desativar um produto com segurança quando ele chegar ao fim de seu ciclo de vida, redefina-o para as configurações padrão de fábrica. Isso apaga suas configurações, dados armazenados e informações confidenciais.

T10204691_pt

2026-07 (M11.2)

© 2024 – 2026 Axis Communications AB