AXIS D4100-VE Mk II Network Strobe Siren

Manual do Usuário

Índice

Instalação 4
..... 4
Introdução 5
..... 5
Encontre o dispositivo na rede 5
Suporte a navegadores 5
Abra a interface web do dispositivo 5
Crie uma conta de administrador 5
Senhas seguras 5
Configure seu dispositivo 7
Desativara o modo de manutenção após a instalação da sirene 7
Ativar modo de manutenção 7
Configurar um perfil 7
Importar ou exportar um perfil 7
Configuração de SIP direto (P2P) 7
Configuração de SIP por meio de um servidor (PBX) 8
Configuração de regras de eventos 9
Acionar uma ação 9
Iniciar um perfil quando um alarme for acionado 9
Iniciar um perfil via SIP 9
Controle mais de um perfil através de extensões SIP 10
Executar dois perfis com prioridades diferentes 11
Ativar uma sirene estroboscópica por meio de uma entrada virtual quando uma câmera detectar movimento 11
Ativar uma sirene estroboscópica via HTTP post quando uma câmera detectar movimento 12
Ativar a sirene estroboscópica via MQTT quando a câmera detectar movimento 14
A interface Web 16
Saiba mais 17
Session Initiation Protocol (SIP) 17
SIP ponto a ponto (P2PSIP) 17
Private Branch Exchange (PBX) 17
NAT traversal 17
Especificações 18
Visão geral do produto 18
..... 18
Indicadores de LED 18
Botões 18
Botão de controle 18
Conectores 19
Conector de rede 19
Conector de E/S 19
Nomes de padrões de luz 20
Nomes de padrões sonoros 20
Limpeza do dispositivo 22
Solução de problemas 23
Restauração das configurações padrão de fábrica 23
Opções do AXIS OS 23
Verificar a versão atual do AXIS OS 23
Atualizar o AXIS OS 24
Problemas técnicos e possíveis soluções 24
..... 26
Considerações sobre desempenho 26
Entre em contato com o suporte 26

Cibersegurança 27
Gerenciamento de vulnerabilidades 27
Notificações de segurança 27
Ciclo de vida seguro do produto 27

Instalação


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

Introdução

⚠ AVISO

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

Encontre o dispositivo na rede

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	*	*	*	*

✓: Recomendada

*: Compatível com limitações

Abra a interface web do dispositivo

1. Digite o nome de usuário e a senha. Se você acessar o dispositivo pela primeira vez, você deverá criar uma conta de administrador. Consulte *Crie uma conta de administrador, on page 5*.

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

Crie uma conta de administrador

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

1. Insira uma conta.
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)**.

Senhas seguras

Importante

Use HTTPS (que vem ativado por padrão) para definir sua senha ou outras configurações confidenciais pela rede. 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.

Configure seu dispositivo

Desativara o modo de manutenção após a instalação da sirene

⚠ CUIDADO

Para proteger o instalador contra danos auditivos e contra ofuscamento por luz muito intensa, se que o modo de manutenção permaneça ativado durante a instalação do dispositivo.

Quando você instala o dispositivo pela primeira vez, o modo de manutenção é ativado por padrão. Quando o dispositivo está no modo de manutenção, a sirene não emite nenhum som e a luz apresenta padrões intermitentes de iluminação branca.

Vá para **Overview (Visão geral)** > **Maintenance (Manutenção)** para desativar o **Maintenance mode (Modo de manutenção)**.

Ativar modo de manutenção

Para realizar a manutenção e serviços no dispositivo, vá para **Overview (Visão geral)** > **Maintenance (Manutenção)** e ative o **Maintenance mode (Modo de manutenção)**. As atividades normais de luz e sirene são pausadas.

Configurar um perfil

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

Para definir um novo perfil:

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

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

Importar ou exportar um perfil

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

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

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

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

Configuração de SIP direto (P2P)

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

Para 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 calls (Permitir recebimento de chamadas)**.
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 **Save (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 **Save (Salvar)**.
7. Defina as configurações de SIP da mesma forma que para ponto a ponto. Consulte *SIP* para obter mais informações.

Configuração de regras de eventos

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

Acionar uma ação

1. Vá para **System (Sistema)** > **Events (Eventos)** e clique em **+ Add a rule (+Adicionar 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 **Ação** executar quando as condições forem atendidas.

Iniciar um perfil quando um alarme for acionado

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

Defina a direção de entrada para a porta:

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

Crie uma regra:

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

Iniciar um perfil via SIP

Este exemplo explica como acionar um alarme via SIP.

Ativar a SIP:

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

3. Clique em **Save (Salvar)**.

Crie uma regra:

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

Controle mais de um perfil através de extensões SIP

Ativar a SIP:

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

Crie uma regra para iniciar um perfil:

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

Crie uma regra para parar um perfil:

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

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

Executar dois perfis com prioridades diferentes

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

Observação

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

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

Criar perfis:

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

Crie uma regra:

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

Ativar uma sirene estroboscópica por meio de uma entrada virtual quando uma câmera detectar movimento

Este exemplo explica como conectar uma câmera a uma sirene estroboscópica e ativar um perfil na sirene estroboscópica sempre que o aplicativo AXIS Motion Guard instalado na câmera detectar movimento.

Antes de começar:

- Crie uma conta com os privilégios de Operador ou Administrador na sirene estroboscópica.
- Crie um perfil na sirene estroboscópica.
- Configure o AXIS Motion Guard na câmera e crie um perfil chamado "Camera profile" (Perfil da câmera).

Crie dois destinatários na câmera:

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

5. Adicione um segundo destinatário com as seguintes informações:
   - **Nome**: Deactivate virtual port (Desativar porta virtual)
   - **Type (Tipo)**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi
     Substitua <IPaddress> pelo endereço da sirene estroboscópica.
   - A conta e a senha da conta recém-criada da sirene estroboscópica.
6. Clique em **Test (Testar)** para garantir que todos os dados sejam válidos.
7. Clique em **Save (Salvar)**.

Crie duas regras na câmera:

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

Crie uma regra na sirene estroboscópica:

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

Ativar uma sirene estroboscópica via HTTP post quando uma câmera detectar movimento

Este exemplo explica como conectar uma câmera a uma sirene estroboscópica e ativar um perfil na sirene estroboscópica sempre que o aplicativo AXIS Motion Guard instalado na câmera detectar movimento.

Antes de começar:

- Crie um novo usuário com a função Operador ou Administrador na sirene estroboscópica.
- Crie um perfil na sirene estroboscópica chamada: "Perfil de Siren estroboscópica".
- Configure o AXIS Motion Guard na câmera e crie um perfil chamado: “Camera profile” (Perfil da câmera).
- Certifique-se de usar o AXIS Device Assistant com versão de firmware 10.8.0 ou posterior.

Crie um destinatário na câmera

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

Crie duas regras na câmera:

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

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

Não deixe de inserir as mesmas informações inseridas em '**"profile" : <>**' (perfil) idênticas àquelas inseridas ao criar o perfil na sirene estroboscópica, neste caso: "Perfil de Siren estroboscópica".

3. Clique em **Save (Salvar)**.
4. Adicione outra regra com as seguintes informações:
   - **Nome**: Desativar sirene estrobosópica com movimento
   - **Condition** (Condição): **Applications > Motion Guard: Camera profile Aplicativos > Motion Guard: Perfil da câmera**
   - Selecione **Invert this condition (Inverter esta condição)**.
   - **Action** (Ação): **Notifications > Send notification through HTTP (Notificações > Enviar notificação via HTTP)**
   - **Recipient** (Destinatário): **Sirene estroboscópica**
     As informações devem ser as mesmas que você digitou anteriormente em **Events > Recipients > Name (Eventos > Destinatários > Nome)**.
   - **Method** (Método): **Post (Publicação)**

- **Body (Corpo)**:

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

Não deixe de inserir as mesmas informações inseridas em '**"profile" : <>**' (perfil) idênticas àquelas inseridas ao criar o perfil na sirene estroboscópica, neste caso: "Perfil de Siren estroboscópica".

5. Clique em **Save (Salvar)**.

Ativar a sirene estroboscópica via MQTT quando a câmera detectar movimento

Este exemplo explica como conectar uma câmera a uma sirene estroboscópica via MQTT e ativar um perfil na sirene estroboscópica sempre que o aplicativo AXIS Motion Guard instalado na câmera detectar movimento.

Antes de começar:

- Crie um perfil na sirene estroboscópica.
- 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 (Aplicações > Alarme de movimento)**
   - **Action (Ação)**: **MQTT > Send MQTT publish message (Enviar mensagem de publicação de MQTT)**
   - **Topic (Tópico)**: Movimento
   - **Payload (Carga)**: Ligado
   - **QoS**: 0, 1 ou 2.
3. Clique em **Save (Salvar)**.
4. Adicione outra regra com as seguintes informações:
   - **Nome**: sem movimento
   - **Condition** (Condição): **Applications > Motion alarm (Aplicações > 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 **Save (Salvar)**.

Configure o cliente MQTT na sirene estroboscópica:

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

Crie uma regra na sirene estroboscópica 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)**: Ligado
   - **Action** (Ação): **Light and siren > Run light and siren profile while the rule is active (Luz e sirene > Executar perfil de luz e sirene quando a regra está ativa)**
   - **Profile (Perfil)**: Selecione o perfil que deseja ativar.
3. Clique em **Save (Salvar)**.

A interface Web

Para saber mais sobre todos os recursos e configurações disponíveis na interface Web dos 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 IP típico nesse caso seria `sip:<local-ip>`.

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 IP típico nesse caso seria `sip:<user>@<domain>` or `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.

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

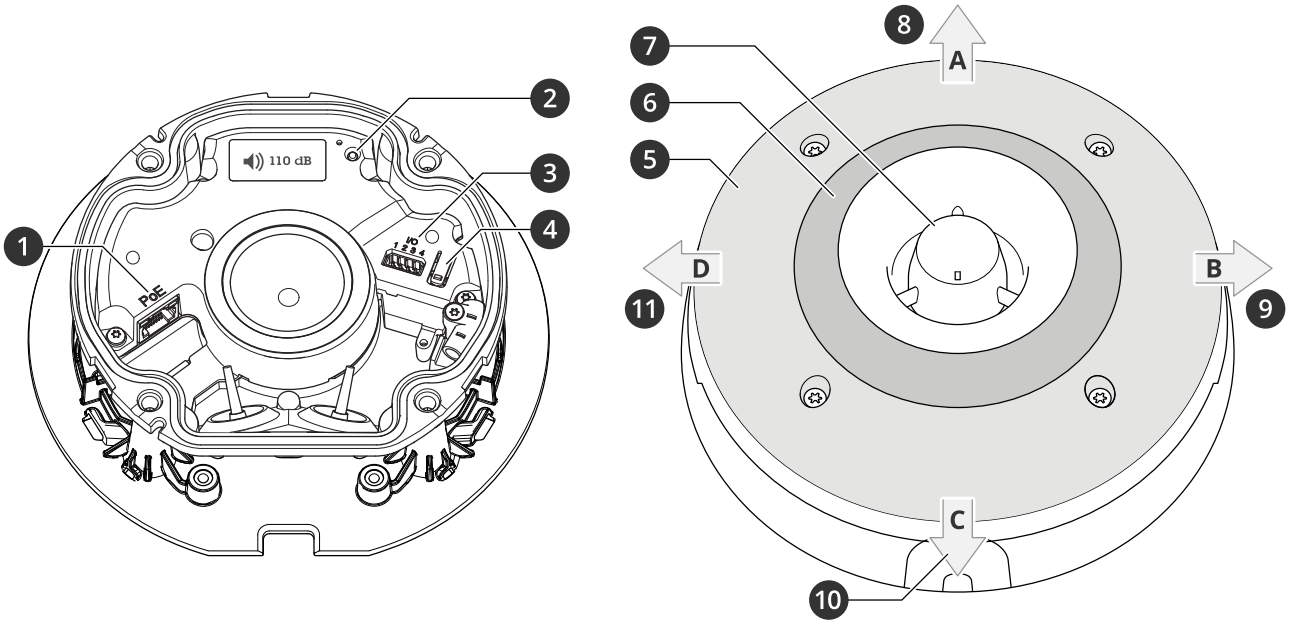
O roteador deve ser compatível com o NAT traversal e UPnP®.

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.

Especificações

Visão geral do produto



1 *Conector de rede PoE*
2 *LED indicador de status*
3 *Conector de E/S*
4 *Botão de controle*
5 *LEDs brancos*
6 *LEDs RGBA (vermelho, azul, verde, âmbar)*
7 *Siren (Sirene):*
8 *Direção da luz A*
9 *Direção da luz B*
10 *Direção da luz C*
11 *Direção da luz D*

Indicadores de LED

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

Botões

Botão de controle

O botão de controle é usado para:

- Restaurar o produto para as configurações padrão de fábrica. Consulte *Restauração das configurações padrão de fábrica, on page 23*.
- 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

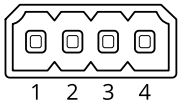
Conector Ethernet RJ45 com Power over Ethernet (PoE).

Conector de E/S

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.

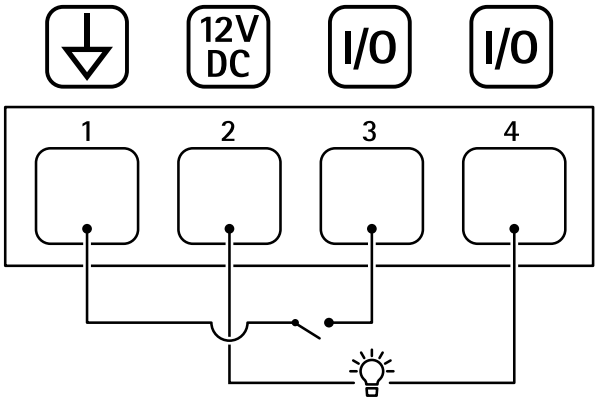
Saída digital – Para conectar dispositivos externos, como relés e LEDs. Os dispositivos conectados podem ser ativados pela interface de programação de aplicativos VAPIX®, por meio de um evento ou via interface web do dispositivo.

Bloco de terminais com 4 pinos



Função	Pin	Observações	Especificações
Terra CC	1		0 V CC
Saída CC	2	⚠ Pode ser usada para alimentar equipamentos auxiliares. Observação: esse pino pode ser usado somente como saída de energia.	12 V CC Carga máxima = 50 mA
Configurável (entrada ou saída)	3-4	Entrada digital – Conecte ao pino 1 para ativar ou deixe aberta (desconectada) para desativar.	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*
4 *E/S configurada como saída*

Nomes de padrões de luz

Desligado
Steady (Aceso)
Branco estável + flash de cor
Alternada
Pulse (Pulso):
Escalonar 3 etapas
Piscar
Piscar 3x
Piscar 4x
Piscar 3x e esmaecer
Piscar 4x e esmaecer
Flash 1x
Flash 3x
Flash 1x branco + cor estável
Flash 3x branco + cor estável
Direção A + cor estável
Direção B + cor estável
Direção C + cor estável
Direção D + cor estável
Girar em branco + cor estável
Girar cauda branca + cor estável
Branco aleatório + cor estável
Giro branco + cor estável
Branco estável + cor estável

Nomes de padrões sonoros

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

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

Limpeza do dispositivo

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

OBSERVAÇÃO

- Produtos químicos abrasivos podem danificar o dispositivo. Não use produtos químicos como limpa-vidros ou acetona para limpar o dispositivo.
- Evite limpar o dispositivo sob luz solar direta ou em temperaturas elevadas, visto que isso pode causar manchas.

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

Para obter mais informações sobre a limpeza de dispositivos Axis, consulte o white paper *Resistência química a agentes de limpeza comuns*.

Solução de problemas

Restauração das configurações padrão de fábrica

Importante

A restauração para as 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 18*.
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 será padrão para um dos seguintes:
   - **Dispositivos com AXIS OS 12.0 e versões posteriores:** Obtidos da sub-rede de endereço local do link (169.254.0.0/16)
   - **Dispositivos com AXIS SO 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*.

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 atualmente instalado do software for AXIS OS 11.2, você terá que instalar a versão LTS AXIS OS 11.11 antes de poder fazer o upgrade do dispositivo para 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 receber: `Request timed out`, isso 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 *Restauração das configurações padrão de fábrica, on page 23*.

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 5*.

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 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*.

Problemas com o som	
O dispositivo não está tão alto quanto esperado	Certifique-se de que o dispositivo esteja fechado corretamente e de que não haja obstruções na corneta ou no elemento do alto-falante.
O dispositivo não emite som	Verifique se o dispositivo está no **Maintenance mode (Modo de manutenção)**. Se estiver no modo de manutenção, desative-o.

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

Considerações sobre desempenho

Os fatores mais importantes a serem considerados são:

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

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 detalhadas e documentação sobre nossa abordagem à segurança cibernética em *axis.com/about-axis/cybersecurity*. Siga as diretrizes de segurança cibernética abaixo para receber notificações de segurança da Axis sobre o produto e para realizar a configuração do produto, de modo a garantir um ciclo de vida e um descomissionamento 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

Inscreva-se para receber emails de notificação de segurança da Axis em *axis.com/security-notification-service*. Enviaremos a você informações sobre vulnerabilidades, alertas de segurança correspondentes e outros assuntos relacionados à segurança do 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.

T10223803_pt

2026-10 (M7.2)

© 2025 – 2026 Axis Communications AB