

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.

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.

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 *Redefinição para as configurações padrão de fábrica, on page 18*.
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 *Comece a utilizar regras para 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)** deverá ser executada quando as condições forem atendidas.

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 *page 14*.

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** como o tipo de notificação.
4. Digite o endereço de email do destinatário.
5. Digite o endereço de email do qual a câmera enviará as notificações.
6. Forneça os detalhes de login da conta de email remetente, juntamente com o nome do host SMTP e o número da porta.
7. Para testar a configuração de seu email, clique em **Test (Testar)**.
8. 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 uma linha de assunto e a mensagem do 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:** Lock (Trancar)
 - **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:** Lock (Trancar)
 - **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 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

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.

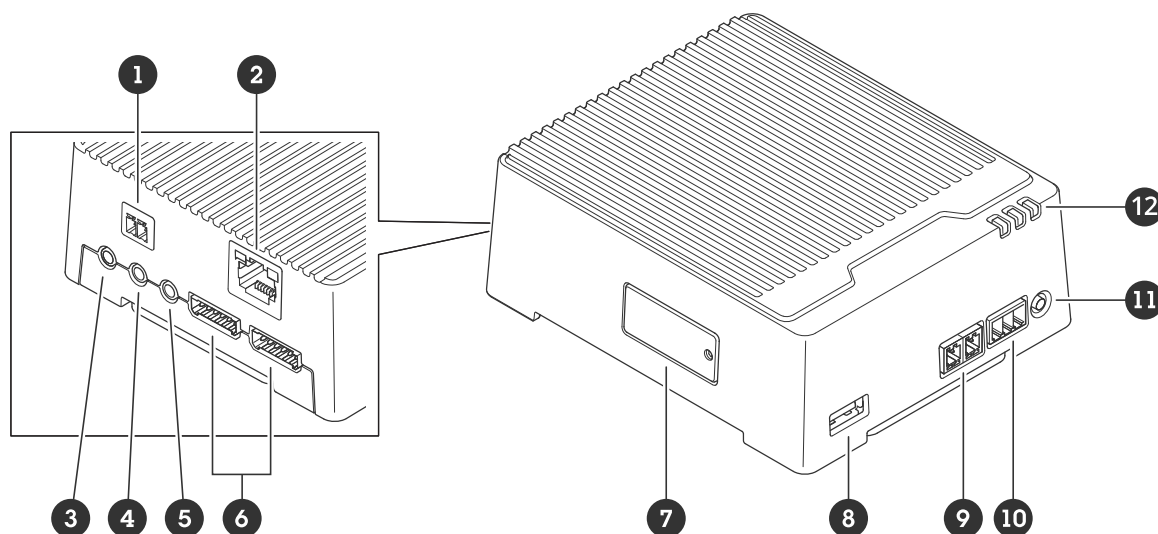
Para encontrar manuais de usuário de analíticos e aplicativos da Axis, vá para *help.axis.com*.

AXIS Audio Analytics

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

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.



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 *Redefinição para as configurações padrão de fábrica*, on page 18.
- 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

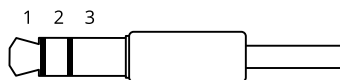
Conector Ethernet RJ45.

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

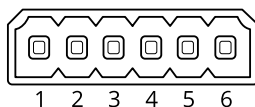
Use o conector de E/S com dispositivos externos em combinação com, por exemplo, detectores de movimento, acionadores de eventos e notificações de alarmes. Além do ponto de referência de 0 V CC e da alimentação (saída CC de 12 V), o conector do terminal de E/S fornece a interface para:

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.

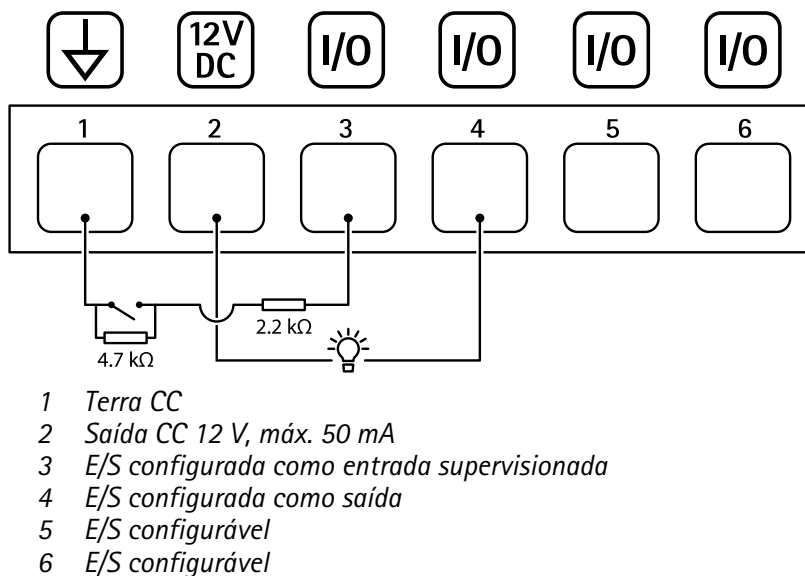
Saída digital – Para conectar dispositivos externos, como relés e LEDs. Os dispositivos conectados podem ser ativados pela interface de programação de aplicativos VAPIX®, por meio de um evento ou via interface web do dispositivo.

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:



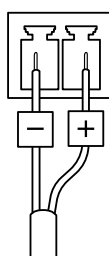
Especificação do desenho elétrico para E/S digital

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 μ s
Tempo máximo de queda (incluindo atraso do GPIO) a 10 kHz	5 μ s
Corrente máxima de afundamento de saída	100 mA
Corrente máxima de fuga de E/S	100 μ 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 ≤ 100 W ou corrente de saída nominal limitada a ≤ 5 A.

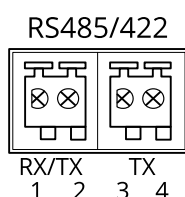


Conector RS485/RS422

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.

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

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 13.
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.

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 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

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.

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.

T10208737_pt

2026-07 (M7.2)

© 2025 – 2026 Axis Communications AB