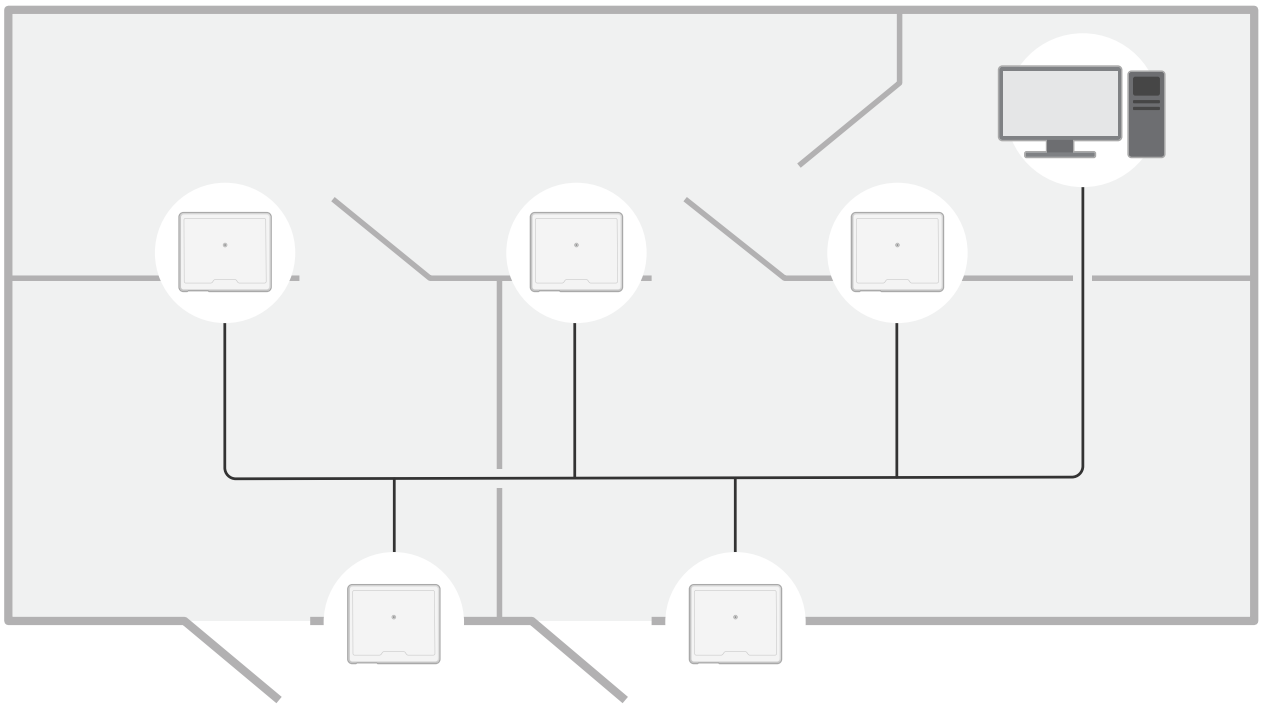
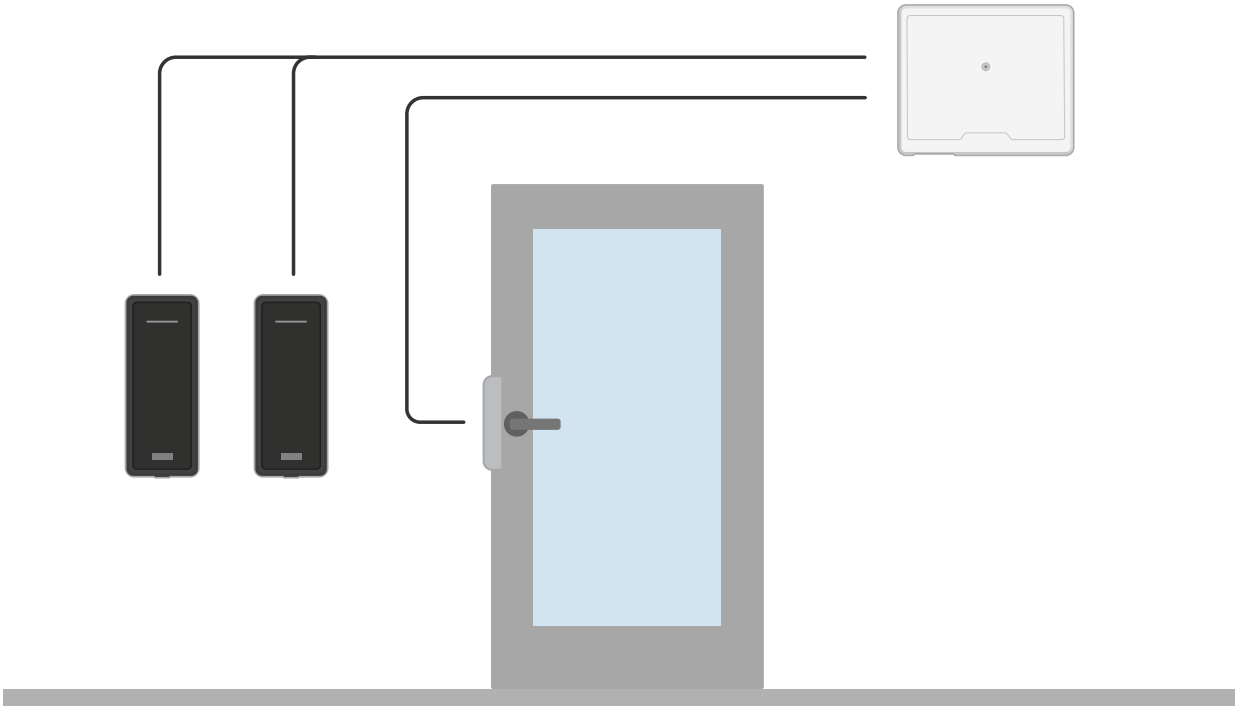
Índice

Visão geral da solução 2
Instalação 3
..... 3
Introdução 4
Encontre o dispositivo na rede 4
Suporte a navegadores 4
Abra a interface web do dispositivo 4
Crie uma conta de administrador 4
Senhas seguras 5
Certifique-se de que o software do dispositivo não foi manipulado 5
Visão geral da interface Web 5
Configure seu dispositivo 6
Door override (Anulação de porta) 6
Perfil de LED OSDP 6
Formato do cartão 7
A interface Web 9
Saiba mais 10
Cibersegurança 10
SO assinado 10
Inicialização segura 10
Axis Edge Vault 10
ID de dispositivo Axis 10
Especificações 11
Visão geral do produto 11
..... 11
Indicadores de LED 11
Botões 12
Botão de controle 12
Conectores 12
Conector de rede 12
Prioridade da alimentação 12
Conector do leitor 12
Conector de porta 14
Conector do relé 14
Conector auxiliar 15
Conector externo 16
Conector de energia 17
Entradas supervisionadas 17
Solução de problemas 18
Restauração das 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
Entre em contato com o suporte 21
Cibersegurança 22
Gerenciamento de vulnerabilidades 22
Notificações de segurança 22
Ciclo de vida seguro do produto 22

Visão geral da solução



O controlador de porta em rede pode ser facilmente conectado à e alimentado pela sua rede IP existente sem a necessidade de cabeamento especial.



Cada controlador de porta em rede é um dispositivo inteligente que pode ser montado facilmente próximo a uma porta. Ela pode alimentar e controlar até dois leitores.

Instalação


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

Introdução

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	*	*	*	*

✓: Recomendada

*: 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 *Crie uma conta de administrador, on page 4*.

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)**.

Importante

O dispositivo não possui conta padrão. Se você perder a senha da sua conta de administrador, deverá redefinir o dispositivo. Consulte *Restauração das configurações padrão de fábrica, on page 18*.

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.

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

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 *Restauração das configurações padrão de fábrica, on page 18*.
   Após a redefinição, uma inicialização segura garantirá o estado do dispositivo.
2. Configure e instale o dispositivo.

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

Para obter instruções de configuração do dispositivo, consulte o *Manual do Usuário do AXIS Camera Station* ou soluções de terceiros.

Door override (Anulação de porta)

Importante

Este recurso assume o controle direto dos relés das portas e substitui a configuração dos relés no AXIS Camera Station. Utilize-o apenas se o suporte da Axis tiver orientado a fazê-lo.

1. Desative o serviço Secure Entry no AXIS Camera Station.
2. Na interface web da controladora de acesso, vá para **Advanced (Avançado) > Door override (Anulação de porta)**.
3. Leia atentamente as informações contidas nessa página e, em seguida, clique em **I understand (Compreendo)**.
4. Ative a opção **Door override (Anulação de porta)** e clique em **Enable (Ativar)**.
5. Vá para o relé da porta e clique em **Lock (Bloquear)**, **Unlock (Desbloquear)**, ou **Acess (Acessar)** para bloquear a porta, desbloquear a porta ou conceder acesso.
6. Vá para o relé que deseja realizar a configuração e clique em **Activate (Ativar)** ou **Deactivate (Desativar)** para ativar ou desativar o relé.

Perfil de LED OSDP

Você pode personalizar os perfis de LED do seu leitor OSDP para definir as luzes e os sons usados em diferentes eventos. Para obter uma lista completa de perfis, consulte *LED profiles (Perfis de LED)*.

Defina os níveis de luz e áudio

1. Acesse **Peripherals (Periféricos)** > **Readers (Leitores)** > **OSDP LED profile (Perfil de LED OSDP)**.
2. Expanda o menu suspenso **Light and audio levels (Níveis de luz e nível de áudio)**.
3. Use o controle deslizante para ajustar a intensidade da faixa de LED, da luz de fundo de LED e do som.
4. Clique em **Save (Salvar)**.

Observação

Quando você altera os níveis de luz e de áudio, as configurações são realizadas para todos os leitores conectados ao controlador.

Teste as configurações do LED OSDP:

Você pode usar o menu **OSDP LED test (Teste de LED OSDP)** para verificar as configurações de áudio e luz de qualquer um dos seus perfis de leitor.

Para testar as configurações dos seus perfis de LED OSDP:

1. Acesse **Peripherals (Periféricos)** > **Readers (Leitores)** > **OSDP LED profile (Perfil de LED OSDP)**.
2. Expanda o menu suspenso **OSDP LED test (Teste de LED OSDP)**.
3. Escolha um indicador de retorno de LED.
4. Escolha o leitor que você gostaria de testar.
5. Clique em **Start (Iniciar)**.
6. Clique em **Edit feedback (Editar feedback)** para alterar as configurações de luz e áudio do seu perfil.
   - Escolha uma nova cor no menu suspenso **Color (Cor)**.
   - Escolha uma frequência de áudio no menu suspenso **Audio (Áudio)**, se aplicável.

- Você também pode redefinir as configurações do perfil clicando em **Reset to default values (Redefinir para os valores padrão)**.
- Clique em **Save (Salvar)**.

Altere as configurações do perfil de LED OSDP:

1. Acesse **Peripherals (Periféricos)** > **Readers (Leitores)** > **OSDP LED profile (Perfil de LED OSDP)**.
2. Acesse **OSDP LED profile (Perfil de LED OSDP)**.
3. Clique em ao lado do perfil que deseja editar.
4. Edite as configurações aplicáveis:
   - Escolha o comportamento que seus LEDs seguirão no menu suspenso **Behavior (Comportamento)**.
   - Escolha a cor dos seus LEDs no menu suspenso **Color (Cor)**.
   - Defina a configuração de **Duration on (Duração ligado)** e **Duration off (Duração desligado)** para os LEDs.
   - Defina a **Recurrence (Periodicidade)** da resposta do LED.
   - A partir do menu suspenso **Audio (Áudio)**, escolha a **Beep duration, on (Duração do bipe, ligado)** e a **Beep duration, off (Duração do bipe, desligado)**, e configure a **Recurrence (Recorrência)** da resposta da campainha. Certifique-se de que a **Beep duration, on (Duração do bipe, ligado)** e a **Beep duration, off (Duração do bipe, desligado)** sejam iguais.
5. Clique em **Save (Salvar)**.

Importar configurações existentes de outro controlador

1. Acesse **Peripherals (Periféricos)** > **Readers (Leitores)** > **OSDP LED profile (Perfil de LED OSDP)**.
2. Clique em **Import (Importar)**.
3. Escolha o arquivo que deseja enviar.
4. Clique em **Import (Importar)**.

Exportar as configurações atuais

1. Acesse **Peripherals (Periféricos)** > **Readers (Leitores)** > **OSDP LED profile (Perfil de LED OSDP)**.
2. Clique em **Export (Exportar)**.
3. Escolha onde deseja salvar o arquivo JSON e clique em **Save (Salvar)**.

Formato do cartão

Esse recurso destina-se exclusivamente ao uso por especialistas. Assim que **Card format (Formatar cartão)** for ativado:

- Se você estiver usando uma credencial de 37 bits, os últimos 5 bits serão removidos.
- Se você estiver usando uma credencial de 64 bits (código QR), a primeira sequência de 24 bits será removida.

Você pode usar os dados de exemplo ou o leitor de cartões para realizar a exibição das credenciais.

1. Acesse **Advanced (Avançado)** > **Card format (Formatar cartão)**.
2. Leia o aviso e clique em **I understand (Entendi)** para ativar a opção de **Card format (Formatar cartão)**.
3. No menu suspenso **Reader data visualization (Visualização de dados do leitor)**, escolha o seu leitor.

4. Clique em **Get reader data (Obter dados do leitor)** ou **Use sample data (Usar dados de amostra)** para gerar uma saída de cartão. Essa medida será aplicada a todos os titulares de cartões registrados no dispositivo.
5. Ative a opção **Trim reader data (Cortar dados do leitor)** para remover os bits finais das credenciais do cartão.
6. Clique em **Enable (Ativar)**.

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

Cibersegurança

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

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

SO assinado

O SO assinado é implementado pelo fornecedor de software que assina a imagem do AXIS OS com uma chave privada. Quando a assinatura é conectada ao sistema operacional, o dispositivo valida o software antes de instalá-lo. Se o dispositivo detectar que a integridade do software está comprometida, a atualização do AXIS OS será rejeitada.

Inicialização segura

A inicialização segura é um processo de inicialização que consiste em uma cadeia inquebrável de software validada criptograficamente e que começa em uma memória imutável (ROM de inicialização). Baseada no uso de SO assinado, a inicialização segura garante que um dispositivo possa ser inicializado somente com software autorizado.

Axis Edge Vault

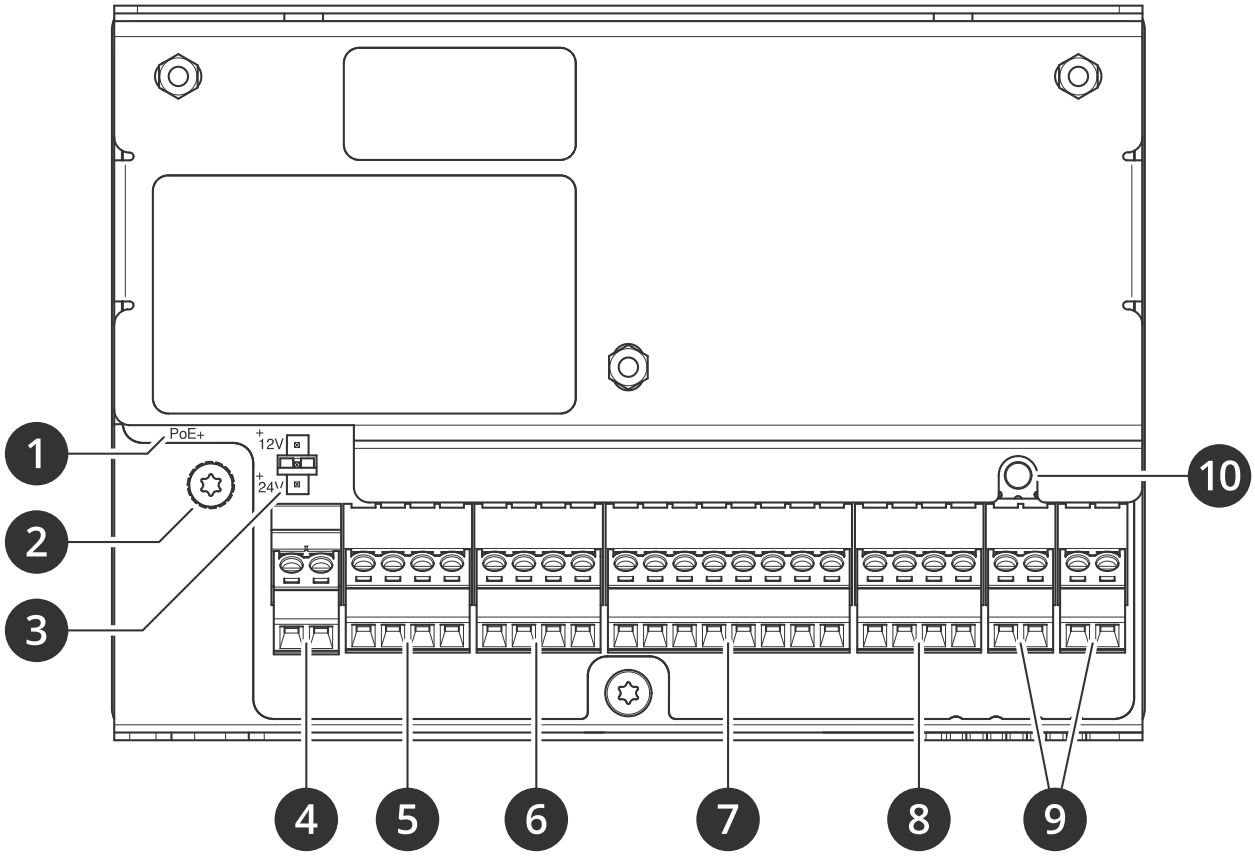
O Axis Edge Vault fornece uma plataforma de segurança cibernética baseada em hardware que protege o dispositivo Axis. Ele oferece recursos para garantir a identidade e a integridade do dispositivo e para proteger suas informações confidenciais contra acessos não autorizados. Ele se baseia em uma base sólida de módulos de computação criptográfica (elemento seguro e TPM) e segurança SoC (TEE e inicialização segura), combinada com a experiência em segurança de dispositivos de borda.

ID de dispositivo Axis

É crucial conseguir verificar a origem do dispositivo para estabelecer confiança na identidade do dispositivo. Durante a produção, os dispositivos com o Axis Edge Vault recebem um certificado de ID de dispositivo Axis exclusivo, fornecido de fábrica e compatível com IEEE 802.1AR. Isso funciona como um passaporte para comprovar a origem do dispositivo. A ID do dispositivo é armazenada de forma segura e permanente no armazenamento seguro de chaves como um certificado assinado pelo certificado raiz do Axis. O ID de dispositivo pode ser utilizado pela infraestrutura de TI do cliente para integração automatizada de dispositivos seguros e identificação de dispositivos seguros

Especificações

Visão geral do produto



1 *Conector de rede*
2 *Posição de aterramento*
3 *Jumper do relé*
4 *Conector de energia*
5 *Conector do relé*
6 *Conector de porta*
7 *Conector do leitor*
8 *Conector auxiliar*
9 *Conectores externos*
10 *Botão de controle*

Indicadores de LED

LED	Cor	Indicação
Status	Verde	Aceso em verde para operação normal.
	Âmbar	Aceso durante a inicialização e na restauração de configurações.
	Vermelho	Pisca lentamente para falha na atualização.
Rede	Verde	Aceso para conexão a uma rede de 100 Mbps. Pisca para atividade de rede.
	Âmbar	Aceso continuamente para uma conexão a uma rede de 10 Mbps. Pisca para atividade de rede.
	Apagado	Sem conexão de rede.

Alimentação	Verde	Funcionamento normal.
	Âmbar	Pisca em verde/âmbar durante a atualização do firmware.
Relé	Verde	Relé ativo.[1]
	Apagado	Relé inativo.

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 18*.

Conectores

Conector de rede

Conector Ethernet RJ45 com Power over Ethernet Plus (PoE+).

UL: O Power over Ethernet (PoE) deve ser implementado com um injetor Ethernet IEEE 802.3af/802.3at Tipo 1 Classe 3 ou Power over Ethernet Plus (PoE+) IEEE 802.3at Tipo 2 Classe 4 com limitação de potência capaz de fornecer 44 – 57 VCC e 15,4 W/30 W. O Power over Ethernet (PoE) foi avaliado pela UL com o uso de um AXIS T8133 Midspan 30 W 1-port.

Prioridade da alimentação

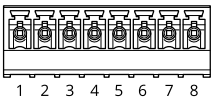
Este dispositivo pode ser alimentado via PoE ou entrada CC. Consulte *Conector de rede, on page 12* e *Conector de energia, on page 17*.

- Quando PoE e CC são ambos conectados antes do dispositivo ser alimentado, o PoE é usado como fonte de alimentação.
- PoE e CC estão conectados e PoE está alimentando. Quando o PoE é perdido, o dispositivo usa CC como fonte de alimentação sem precisar reiniciar.
- PoE e CC estão conectados e CC está alimentando. Quando CC é perdido, o dispositivo reinicia e usa PoE como fonte de alimentação.
- Quando o CC é usado durante a inicialização e o PoE é conectado após o dispositivo ser iniciado, CC é usado como fonte de alimentação.
- Quando o PoE é usado durante a inicialização e CC é conectado após o dispositivo ser iniciado, PoE é usado como fonte de alimentação.

Conector do leitor

Um bloco de terminais com 8 pinos com suporte aos protocolos OSDP e Wiegand para comunicação com o leitor.

Ele pode conectar até dois leitores OSDP (multi-drop) ou um leitor Wiegand. 500 mA a 12 VCC são reservados para todos os leitores conectados ao controlador de porta.



Configurado para um leitor OSDP

1. *Relé está ativo quando COM está conectado a NO.*

Função	Pin	Observação	Especificações
Terra CC (GND)	1		0 VCC
Saída CC (+12 V)	2	Fornece energia para o leitor.	12 VCC, máx. 500 mA
A	3	Half duplex	
B	4	Half duplex	

Configurado para dois leitores OSDP (multidrop)

Função	Pin	Observação	Especificações
Terra CC (GND)	1		0 VCC
Saída CC (+12 V)	2	Fornece energia para ambos os leitores.	12 VCC, máx. 500 mA combinados para ambos os leitores
A	3	Half duplex	
B	4	Half duplex	

Importante

- Quando o leitor é alimentado pelo controlador, o comprimento de cabo qualificado é de até 200 m (656 ft). Verificado somente para leitores Axis.
- Quando o leitor não é alimentado pelo controlador, o comprimento de cabo qualificado para dados do leitor é de até 1000 m (3280,8 ft) quando os seguintes requisitos de cabo são atendidos: 1 par trançado blindado, AWG 24, impedância de 120 ohm. Verificado somente para leitores Axis.

Configurado para um leitor Wiegand

Função	Pin	Observação	Especificações
Terra CC (GND)	1		0 VCC
Saída CC (+12 V)	2	Fornece energia para o leitor.	12 VCC, máx. 500 mA
D0	3		
D1	4		
LED 1	5	LED vermelho	
LED 2	6	LED verde	
VIOLAÇÃO	7	Entrada digital – Conecte ao pino 1 para ativar ou deixe aberta (desconectada) para desativar.	0 a 30 VCC máx.
SINAL SONORO	8	Saída digital — 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 VCC máx., dreno aberto, 100 mA

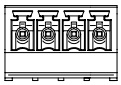
Importante

- Quando o leitor é alimentado pelo controlador, o comprimento de cabo qualificado é de até 150 m (500 ft).
- Quando o leitor não é alimentado pelo controlador, o comprimento de cabo qualificado para dados do leitor é de até 150 m (500 ft) quando o seguinte requisito de cabo é atendido: AWG 22.

Conector de porta

Um bloco de terminais com 4 pinos para monitoramento de dispositivos de portas (entrada digital).

O monitor de porta oferece suporte à supervisão com resistores terminadores. Se a conexão for interrompida, um alarme será acionado. Para usar entradas supervisionadas, instale resistores de terminação. Use o diagrama de conexão para entradas supervisionadas. Consulte *page 17*.



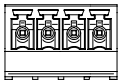
Função	Pin	Observações	Especificações
Terra CC	1, 3		0 VCC
Entrada	2, 4	Para comunicação com o monitor da porta. Entrada digital ou Entrada supervisionada – Conecte ao pino 1 ou 3 respectivamente para ativar ou deixe flutuante (desconectada) para desativar.	0 a 30 VCC máx.

Importante

O comprimento de cabo qualificado é de até 200 m (656 pés) quando o seguinte requisito de cabo é atendido: AWG 24.

Conector do relé

Um bloco de terminais com 4 pinos para relés C que podem ser usados, por exemplo, para controlar uma trava ou uma interface para um portão.



Função	Pin	Observações	Especificações
Terra CC (GND)	1		0 VCC
NÃO	2	normalmente aberto. Para conectar dispositivos de relé. Conecte uma trava de segurança contra falhas entre o terra NO e o terra CC. Os dois pinos de relé são galvanicamente separados do resto do circuito se os jumpers não forem usados.	Corrente máxima = 2 A Tensão máxima = 30 V CC
COM	3	Comum	

NC	4	normalmente fechado. Para conectar dispositivos de relé. Conecte uma trava fail--safe entre o terra NC e o terra CC. Os dois pinos de relé são galvanicamente separados do resto do circuito se os jumpers não forem usados.	

Jumper de alimentação do relé

Quando o jumper de alimentação está instalado, ele conecta a alimentação 12 VCC ou 24 VCC ao pino COM do relé.

Ele pode ser usado para conectar uma trava entre os pinos GND e NO ou GND e NC.

Fonte de alimentação	Potência máxima em 12 VCC	Potência máxima em 24 VCC
ENTRADA CC	1600 mA	800 mA
PoE	900 mA	450 mA

OBSERVAÇÃO

Se a trava for não polarizada, recomendamos adicionar um diodo flyback externo.

Conector auxiliar

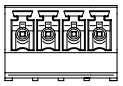
Use o conector auxiliar com dispositivos externos em combinação com, por exemplo, detecção de movimento, acionamento de eventos e notificações de alarmes. Além do ponto de referência de 0 VCC e alimentação (saída CC), o conector auxiliar fornece a interface para:

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.

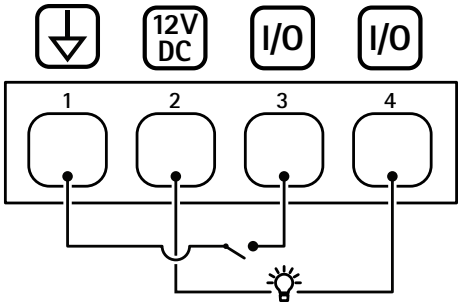
Saída digital – Para conectar dispositivos externos, como relés e LEDs. Os dispositivos conectados podem ser ativados pela interface de programação de aplicativos VAPIX® ou via página da Web do produto.

Bloco de terminais com 4 pinos



Função	Pin	Observações	Especificações
Terra CC	1		0 VCC
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 no total
Configurável (entrada ou saída)	3-4	Entrada digital ou entrada supervisionada – Conecte ao pino 1 para ativar ou deixe aberta (desconectada) para desativar. Para usar a entrada supervisionada, instale resistores de terminação. Veja o diagrama de conexão para obter informações de como conectar os resistores.	0 a 30 VCC 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. As E/ /Ss serão capazes de alimentar uma carga externa de 12 VCC, 50 mA (máx. combinadas), se uma saída interna de 12 VCC (pino 2) for usada. No caso do uso de conexões de dreno abertas em conjunto com uma fonte de alimentação externa, as E/S podem gerenciar uma alimentação CC de 0 a 30 VCC, 100 mA cada.	0 a 30 VCC máx., dreno aberto, 100 mA



1 *Terra CC*
2 *Saída CC 12 V*
3 *E/S configurada como entrada*
4 *E/S configurada como saída*

Conector externo

Blocos de terminais com 2 pinos para dispositivos externos, por exemplo, detectores de quebra de vidros ou incêndio.

UL: O conector não foi avaliado pelo UL para uso em alarme antifurto ou de incêndio.



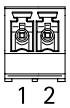
Função	Pin	Observações	Especificações
Terra CC	1		0 VCC
VIOLAÇÃO	2	Entrada digital – Conecte ao pino 1 para ativar ou deixe aberta (desconectada) para desativar.	0 a 30 VCC máx.



Função	Pin	Observações	Especificações
Terra CC	1		0 VCC
ALARME	2	Entrada digital – Conecte ao pino 1 para ativar ou deixe aberta (desconectada) para desativar.	0 a 30 VCC máx.

Conector de energia

Bloco de terminais com 2 pinos para entrada de energia CC Use uma fonte de energia com limitação (LPS) 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.



Função	Pin	Observações	Especificações
Terra CC (GND)	1		0 VCC
Entrada CC	2	Para alimentar o dispositivo sem usar Power over Ethernet. Observação: esse pino pode ser usado somente como entrada de energia.	12 VCC, máx., 36 W

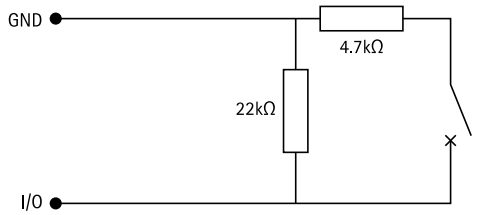
UL: Alimentação CC a ser fornecida por uma fonte de alimentação UL 603 relacionada, dependendo do aplicativo, com as classificações apropriadas.

Entradas supervisionadas

Para usar entradas supervisionadas, instale resistores terminadores de acordo com o diagrama abaixo.

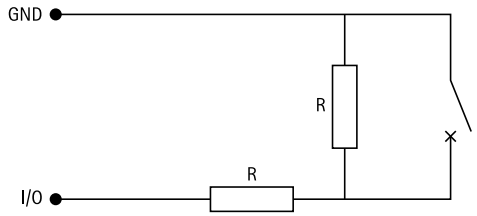
Conexão paralela primeiro

Os valores dos resistores devem ser 4,7 kΩ e 22 kΩ.



Conexão serial primeiro

Os valores dos resistores devem ser iguais, e possíveis valores são 1 kΩ, 2,2 kΩ, 4,7 kΩ e 10 kΩ.



Observação

Recomenda-se usar cabos blindados e trançados. Conecte a blindagem a 0 VCC.

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 11*.
3. Mantenha o botão de controle pressionado por 25 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 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, 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 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*.
- Como o banco de dados de usuários, grupos, credenciais e outros dados são atualizados depois de uma atualização do AXIS OS, a primeira inicialização pode levar alguns minutos para ser concluída. O tempo necessário depende da quantidade de dados.

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.

4. Quando o produto tiver sido reiniciado, limpe o cache do navegador.

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 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*.

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.

T10181041_pt

2026-10 (M11.6)

© 2022 – 2026 Axis Communications AB