

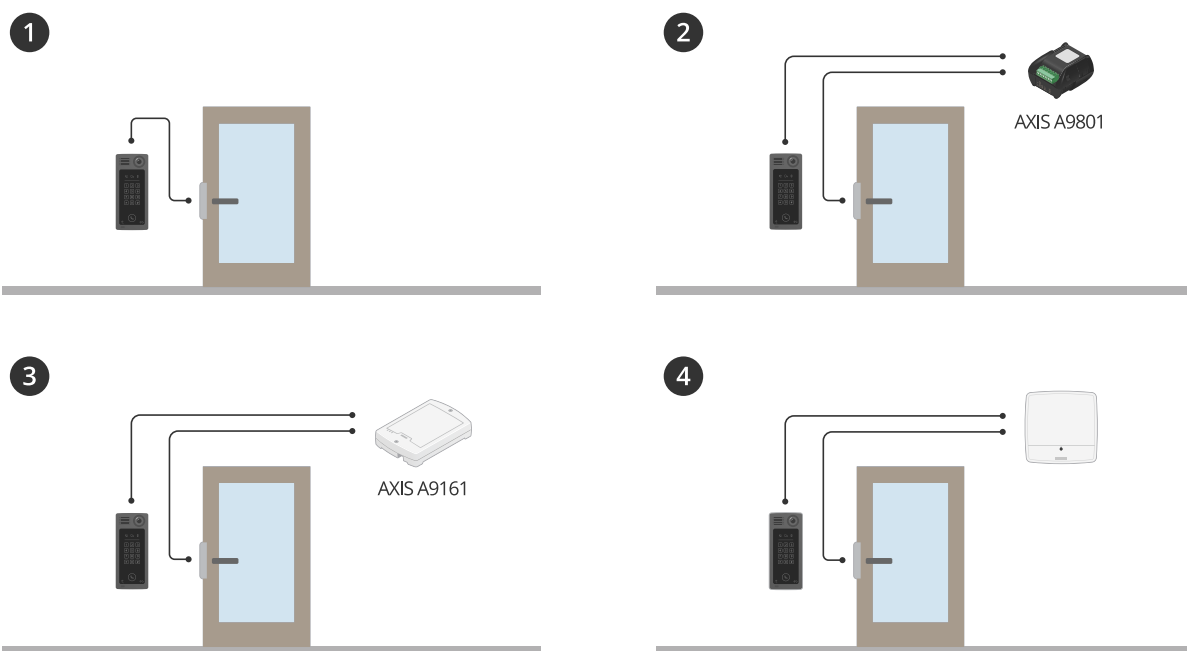
AXIS A8207-VE Mk II Network Video Door Station

Índice

Visão geral da solução.....	4
Visão geral do produto	5
Instalação	7
Início.....	8
Encontre o dispositivo na rede	8
Suporte a navegadores.....	8
Abra a interface web do dispositivo.....	8
Criar uma conta de administrador.....	8
Senhas seguras	9
Certifique-se de que o software do dispositivo não foi violado	9
Visão geral da interface Web.....	9
Configurações adicionais.....	10
Alteração da senha de root.....	10
Calibrar e executar um teste de alto-falante remoto	10
Configuração de SIP direto (P2P).....	10
Configuração de SIP por meio de um servidor (PBX)	11
Criar um contato.....	12
Configurar o botão de chamada.....	12
Configurar como leitor.....	12
Use a lista de entradas para permitir que os detentores de credencial abram a porta	13
Configure como leitor de cartão usando um controlador de porta	13
Use dados protegidos em cartões para aumentar a segurança	14
Use DTMF para destravar a porta para um visitante.....	15
Transmitir vídeo ao vivo para um monitor	15
A interface Web.....	17
Saiba mais	18
Voice over IP (VoIP)	18
Session Initiation Protocol (SIP).....	18
SIP ponto a ponto (P2PSIP).....	18
Private Branch Exchange (PBX)	19
Configuração de regras de eventos.....	20
Analíticos e aplicativos	20
AXIS Client for Unified Communication Systems	20
Uso diário	21
Use o teclado.....	21
Solução de problemas.....	22
Redefinição para as configurações padrão de fábrica	22
Verificar a versão atual do AXIS OS	22
Atualizar o AXIS OS	22
Problemas técnicos, dicas e soluções	23
Considerações sobre desempenho	24
Especificações	25
Indicadores e controles do painel frontal	25
Ícones indicadores	25
Faixa de indicadores do leitor de cartões	25
Botão de chamada.....	25
Indicadores de LED	25
Slot de cartão SD	25
Botões	25
Botão de controle	25
Conectores	26
Conector HDMI	26
Conector de rede	26

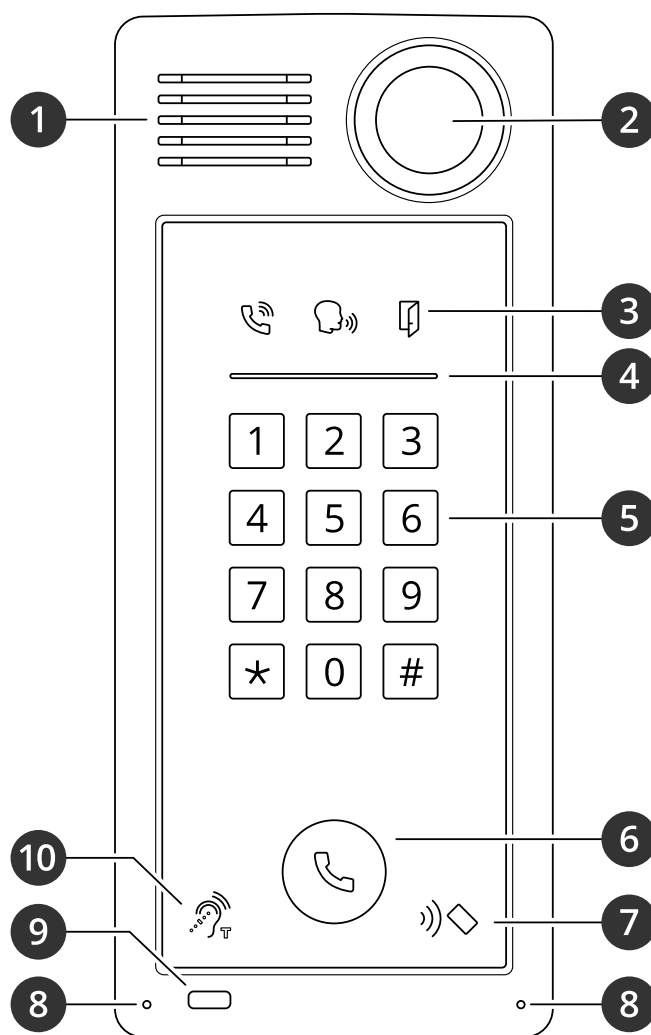
Conector de áudio	26
Conector do relé.....	26
Conector do leitor.....	27
Conector de E/S.....	27
Conector de energia.....	28
Informações sobre segurança	29
Níveis de perigo	29
Outros níveis de mensagens	29
Cibersegurança.....	30
Gerenciamento de vulnerabilidades.....	30
Notificações de segurança.....	30
Ciclo de vida seguro do produto.....	30

Visão geral da solução

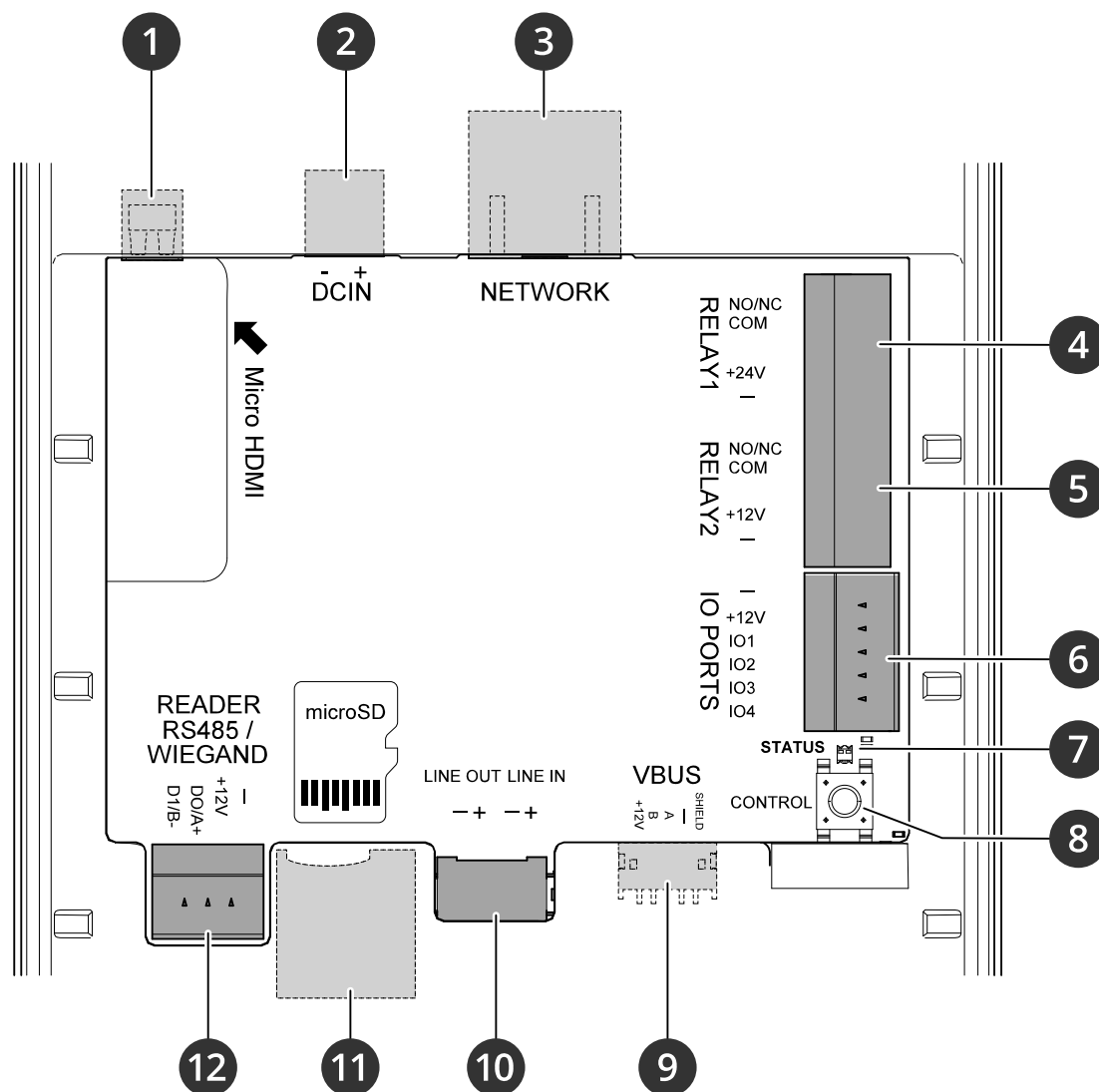


- 1 Videoporteiro
- 2 Porteiro eletrônico combinado com AXIS A9801
- 3 Porteiro eletrônico combinado com AXIS A9161
- 4 Porteiro eletrônico combinado com um sistema de controle de acesso, por exemplo, AXIS A1001 ou AXIS A1601

Visão geral do produto



- 1 Alto-falante
- 2 Câmera
- 3 Ícones indicadores, on page 25
- 4 Faixa de indicadores do leitor de cartões, on page 25
- 5 Teclado
- 6 Botão de chamada, on page 25
- 7 Ícone do leitor de cartões
- 8 Microfone
- 9 Sensor de PIR
- 10 Ícone de bobina em T



- 1 Conector HDMI, on page 26 (microHDMI)
- 2 Conector de energia, on page 28
- 3 Conector de rede, on page 26 (PoE+)
- 4 Conector do relé, on page 26
- 5 Conector do relé, on page 26
- 6 Conector de E/S, on page 27
- 7 LED de estado
- 8 Botão de controle, on page 25
- 9 2N VBUS (não usado)
- 10 Conector de áudio, on page 26
- 11 Slot de cartão SD, on page 25 (microSD/microSDHC/microSDXC)
- 12 Conector do leitor, on page 27

Instalação



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

Vídeo de instalação para o leitor A8207-VE.



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

Vídeo de instalação do relé A8207-VE.

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 8*.

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 9*.
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 22*.

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 22*.
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

Configurações adicionais

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.

Alteração da senha de root

1. Faça login na interface do dispositivo e vá para **System > Users (Sistema > Usuários)**.
2. Para o usuário root, clique em  > **Update user (Atualizar usuário)**.
3. Insira uma nova senha e salve.

Calibrar e executar um teste de alto-falante remoto

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

Observação

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

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

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

Observação

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

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

Observação

Também é possível executar a calibração pressionando o botão de controle no dispositivo físico. Consulte *Visão geral do produto*, on page 5 para identificar o botão de controle.

Configuração de SIP direto (P2P)

VoIP (Voice over IP) é um grupo de tecnologias que permite a comunicação por voz e multimídia via redes IP. Para obter mais informações, consulte *Voice over IP (VoIP)*, on page 18.

Neste dispositivo, o VoIP é habilitado pelo protocolo SIP. Para obter mais informações sobre SIP, consulte *Session Initiation Protocol (SIP)*, on page 18

Há dois tipos de configurações para SIP: direta ou ponto a ponto (P2P) é uma delas. 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 informações sobre como configurar esse tipo de comunicação, consulte *SIP ponto a ponto (P2PSIP)*, on page 18.

1. Vá para **Communication > SIP > Settings (Comunicação > SIP > Configurações de SIP)** e selecione **Enable SIP (Habilitar SIP)**.
2. Para permitir que o dispositivo receba chamadas, selecione **Allow incoming SIP calls (Permitir recebimento de chamadas SIP)**.

OBSERVAÇÃO

Quando você permite o recebimento de chamadas, o dispositivo aceita chamadas de qualquer dispositivo conectado à rede. Se o dispositivo puder ser acessado de uma rede pública ou pela Internet, recomendamos não permitir o recebimento de chamadas.

3. Clique em **Call handling (Tratamento de chamadas)**.
4. Em **Calling timeout (Tempo limite de chamada)**, defina por quantos segundos a chamada irá durar se não houver resposta.
5. Se você tiver permitido o recebimento de chamadas defina o número de segundos antes da espera de chamadas de entrada no **Incoming call timeout (Tempo limite de recebimento de chamadas)**.
6. Clique em **Ports (Portas)**.
7. Insira o número da **SIP port (Porta SIP)** e o número da **TLS port (Porta TLS)**.

Observação

- **SIP port (Porta SIP)** – Para sessões de SIP. O tráfego de sinalização por essa porta não é criptografado. O número da porta padrão é 5060.
 - **TLS port (Porta TLS)** – Para sessões de SIP protegidas por SIPS e TLS. O tráfego de sinalização por meio dessa porta é criptografado com o Transport Layer Security (TLS). O número da porta padrão é 5061.
 - **RTP start port (Porta de início de RTP)** – a porta usada para o primeiro stream de mídia RTP em uma chamada SIP. A porta de início padrão é 4000. Alguns firewalls podem bloquear o tráfego de RTP em determinados números de portas. O número da porta deve ser entre 1024 e 65535.
8. Clique em **NAT traversal**.
 9. 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 .

10. Clique em **Salvar**.

Configuração de SIP por meio de um servidor (PBX)

VoIP (Voice over IP) é um grupo de tecnologias que permite a comunicação por voz e multimídia via redes IP. Para obter mais informações, consulte *Voice over IP (VoIP)*, on page 18.

Neste dispositivo, o VoIP é habilitado pelo protocolo SIP. Para obter mais informações sobre SIP, consulte *Session Initiation Protocol (SIP)*, on page 18

Há dois tipos de configurações para SIP: um servidor PBX é uma delas. Use um servidor PBX quando a comunicação precisar ser feita entre um número infinito de agentes de usuário dentro e fora da rede IP. Recursos adicionais podem ser adicionados à configuração dependendo do provedor de PBX. Para obter mais informações, consulte *Private Branch Exchange (PBX)*, on page 19.

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. Acesse **Communication > SIP > Accounts (Comunicação > SIP > Contas)** e clique em **+ Add account (+ Adicionar conta)**.
3. Insira um **Name (Nome)** para a conta.

4. Selecione **Registered (Registrado)**.
5. Selecione um modo de transporte.
6. Adicione as informações da conta a partir do provedor de PBX.
7. Clique em **Salvar**.
8. Defina as configurações de SIP da mesma forma que para ponto a ponto, consulte *Configuração de SIP direto (P2P)*, on page 10. Use a porta de início de RTP do provedor de PBX.

Criar um contato

Este exemplo explica como criar um novo contato na lista de contatos. Antes de iniciar, ative o SIP em **Communication > SIP (Comunicação > SIP)**.

Para criar um novo contato:

1. Vá para **Communication > Contact list (Comunicação > Lista de contatos)**.
2. Clique em **+ Add contact (+ Adicionar contato)**.
3. Insira o nome e o sobrenome do contato.
4. Insira o endereço SIP do contato.

Observação

Para obter informações sobre os endereços SIP, consulte *Session Initiation Protocol (SIP)*, on page 18.

5. Selecione a conta SIP da qual a chamada será efetuada.

Observação

As opções de disponibilidade são definidas em **System (Sistema) > Events (Eventos) > Schedules (Agendamentos)**.

6. Escolha a **Availability (Disponibilidade)** do contato. Se houver uma chamada quando o contato não estiver disponível, a chamada é cancelada, a menos que haja um contato de fallback.

Observação

Um fallback é um contato para quem a chamada é encaminhada se o contato original não responde ou fica indisponível.

7. Em **Fallback**, selecione **Nenhum**.
8. Clique em **Salvar**.

Configurar o botão de chamada

Por padrão, o botão de chamada é configurado para fazer chamadas de VMS (sistema de gerenciamento de vídeo). Se você deseja manter essa configuração, basta adicionar o intercomunicador Axis ao VMS.

Este exemplo explica como configurar o sistema para ligar para um contato da lista de contatos quando um visitante pressionar o botão de chamada.

1. Acesse **Communication > Calls > Call button (Comunicação > Chamadas > Botão de chamadas)**.
2. Em **Recipients (Destinatários)**, remova **VMS**.
3. Em **Recipients (Destinatários)**, selecione um existente ou crie um contato.

Para desativar o botão de chamada, desative **Enable call button (Ativar botão de chamada)**.

Configurar como leitor

É possível configurar sua estação de porta como um leitor para permitir que os detentores de credencial abram a porta.

Ao usar a lista de entradas, a estação da porta armazena as credenciais localmente e pode funcionar como um leitor independente para até cinquenta detentores de credencial.

Ao conectar a estação de porta a um controlador de porta, a estação de porta ainda pode armazenar até cinquenta credenciais e, se a credencial solicitada for encontrada na lista de entradas, a estação de porta gerencia as permissões de acesso. Se uma credencial solicitada não for encontrada na lista de entradas e a opção **Usar controlador de porta conectado** estiver ativada, a solicitação será encaminhada para o controlador de porta, que então gerenciará as permissões de acesso.

Use a lista de entradas para permitir que os detentores de credencial abram a porta

Com a lista de entradas, você pode possibilitar que os detentores de credenciais usem sua credencial para acionar ações, como abrir uma porta. Este exemplo explica como adicionar um detentor de credencial que pode usar o cartão para abrir a porta dez vezes.

Pré-requisitos

- O tipo de chip correto deve estar ativo em **Reader > Chip types (Leitor > Tipos de chip)**.

Ative a lista de entradas e adicione um detentor de credencial:

1. Acesse **Reader > Entry list (Leitor > Lista de entrada)**.
2. Ative a opção **Use Entry list (Usar lista de entrada)**.
3. Clique em **+ Add credential holder (+ Adicionar detentor de credencial)**.
4. Digite o nome e o sobrenome do detentor da credencial. O nome deve ser único.
5. Selecione **Card (Cartão)**.
6. Passe o cartão do detentor de credencial no dispositivo e clique em **Get latest (Obter mais recente)**.
7. Mantenha a condição do evento como **Access granted (Acesso concedido)**.
8. Em **Valid to (Válido até)**, selecione **Number of times (Número de vezes)**.
9. Em **Number of times (Número de vezes)**, insira **10**.
10. Clique em **Salvar**.

Crie uma regra:

1. Acesse **System > Events (Sistema > Eventos)**.
2. Em **Rules (Regras)**, clique em **+Add a rule (+ Adicionar regra)**.
3. Em **Nome**, digite **Abrir porta**.
4. Na lista de condições, selecione **Entry list > Access granted (Lista de entrada > Acesso concedido)**.
5. Na lista de ações, selecione **I/O > Toggle I/O once (E/S > Alternar E/S uma vez)**.
6. Na lista de portas, selecione **Door (Porta)**.
7. Em **State (Estado)**, selecione **Active (Ativo)**.
8. Defina a duração para **00:00:07**.
9. Clique em **Salvar**.

Configure como leitor de cartão usando um controlador de porta

Conexão de rede

Para usar o porteiro eletrônico como um leitor de cartões, você deve conectá-lo a um controlador de porta. O controlador de porta armazena todas as credenciais e controla quem pode passar pela porta. Neste exemplo, conectamos os dispositivos pela rede. Também modificamos os tipos de cartões permitidos.

Importante

A conexão de rede funciona somente com controladores de porta Axis. Para conectar a um controlador de porta não Axis, você precisa conectar fisicamente os dispositivos com fios. Consulte *Conexão com fio, on page 14*.

Configurar o porteiro eletrônico como um leitor de cartões

1. Vá para **Reader (Leitor) > Connection (Conexão)**.

2. Selecione o tipo de protocolo do VAPIX reader (Leitor de VAPIX).
3. Selecione o protocolo para comunicação com o controlador de porta.

Observação

Recomendamos ativar a opção **Verify certificate (Verificar certificado)** se estiver usando HTTPS.

4. Insira o endereço IP do controlador de porta.
5. Insira as credenciais do controlador de porta.
6. Clique em **Conectar**.
7. Selecione o leitor de entrada para a porta apropriada.
8. Clique em **Salvar**.

Conexão com fio

Para usar o porteiro eletrônico como um leitor de cartões, você deve conectá-lo a um controlador de porta. O controlador de porta armazena todas as credenciais e controla quem pode passar pela porta. Neste exemplo, conectamos os dispositivos com fios, usamos o protocolo Wiegand, ativamos o beeper e usamos uma porta de E/S para o LED. Também modificamos os tipos de cartão permitidos.

Importante

Use as portas de E/S que ainda não estão em uso. Se você usar portas de E/S já em uso, todos os eventos criados para essas portas deixarão de funcionar.

Antes de começar

- Conecte o porteiro eletrônico a um controlador de porta. Consulte os desenhos da fiação elétrica, que podem ser baixados em axis.com/products/axis-a8207-ve-mk-ii/support.
- Configure o hardware do controlador de porta usando o protocolo Wiegand para o leitor. Consulte o manual do usuário do controlador de porta para obter instruções.

Configurar o porteiro eletrônico como um leitor de cartões

1. Vá para **Reader (Leitor) > Connection (Conexão)**.
2. Selecione **Wiegand** como tipo de protocolo.
3. Ative o **Beeper (Bipe)**.
4. Em **Input for beeper (Entrada para bipe)**, selecione I3.
5. Em **Input used for LED control (Entrada usada para controle de LED)**, selecione 1.
6. Em **Entrada para LED1**, selecione I1.
7. Selecione as cores a serem usadas para cada estado.
8. Em **Keypress format (Formato do pressionamento de tecla)**, selecione **FourBit**.
9. Clique em **Salvar**.
10. Vá para **Reader > Chip types (Leitor > Tipos de chip)** e ative os tipos de chip que deseja usar.

Observação

Você pode manter o conjunto padrão de tipos de chip, mas recomenda-se modificar a lista de acordo com suas necessidades específicas.

11. Clique em **Add data set (Adicionar conjunto de dados)** para especificar os conjuntos de dados para os diferentes tipos de chips.
12. Clique em **Save (Salvar)**.

Use dados protegidos em cartões para aumentar a segurança

Para aumentar a segurança em seu sistema de controle de acesso, você pode optar por usar dados de cartões seguros armazenados em alguns tipos de cartões. Os dados são protegidos por uma chave secreta. Para ler os dados do cartão, você precisa armazenar a chave secreta e outras informações sobre o cartão no dispositivo.

1. Vá para **Reader > Chip types (Leitor > Tipos de chip)**.
2. Em **Data sets (Conjuntos de dados)**, selecione o tipo de chip que deseja editar e clique em **Add data set (Adicionar conjunto de dados)**.
3. Insira informações sobre os dados do cartão. As informações a serem inseridas dependerão do tipo de cartão e do modo como os cartões estão inscritos.
4. Se você usa os protocolos OSDP ou Wiegand, selecione **Use as UID (Usar como UID)** para enviar os dados seguros como UID/CSN em vez do UID/CSN normal.
5. Para permitir que somente cartões em conformidade com os dados do cartão especificado sejam enviados para o controlador de acesso, selecione **Required data (Dados necessários)**. Os cartões que não são compatíveis são ignorados silenciosamente pelo leitor.
6. Clique em **Salvar**.

Use DTMF para destravar a porta para um visitante

Quando um visitante faz uma chamada no porteiro eletrônico, a pessoa que responde pode usar sinalização Dual-Tone Multi-Frequency (DTMF) do seu dispositivo SIP para destravar a porta. O controlador de porta destrava e trava a porta.

Este exemplo explica como:

- definir o sinal DTMF no porteiro eletrônico
- configurar o porteiro eletrônico para:
 - solicitar ao controlador de porta o destravamento da porta ou
 - destravar a porta usando o relé interno.

Todas as configurações são ajustadas na página da Web do porteiro eletrônico.

Antes de começar

- Permita chamadas SIP do dispositivo e crie uma conta SIP. Consulte *Configuração de SIP direto (P2P)*, on page 10 e *Configuração de SIP por meio de um servidor (PBX)*, on page 11.

Defina o sinal DTMF no porteiro eletrônico

1. Acesse **Communication > SIP > DTMF (Comunicação > SIP > DTMF)**.
2. Clique em **+ Add sequence (+ Adicionar sequência)**.
3. Em **Sequence (Sequência)**, insira **1**.
4. Em **Descrição**, insira **Destravar porta**.
5. Em **Accounts (Contas)**, selecione a conta SIP.
6. Clique em **Salvar**.

Configure o porteiro eletrônico para destravar a porta usando o relé interno

7. Acesse **System > Events > Rules (Sistema > Eventos > Regras)** e adicione uma regra:
8. No campo **Nome**, insira **DTMF Destravar porta**.
9. Na lista de condições, em **Call (Chamada)**, selecione **DTMF** e **Unlock door (Destravar porta)**.
10. Na lista de ações, em **I/O (E/S)**, selecione **Toggle I/O once (Alternar E/S uma vez)**.
11. Na lista de portas, selecione **Relay 1 (Port 4) (Relé 1 (Porta 4))**.
12. Altere **Duration (Duração)** para **00:00:07**, o que significa que a porta está aberta por 7 segundos.
13. Clique em **Salvar**.

Transmitir vídeo ao vivo para um monitor

Seu dispositivo pode transmitir um fluxo de vídeo ao vivo para um monitor HDMI sem conexão de rede. Use o monitor para ver quem está na porta.

1. Conecte um monitor externo para o conector HDMI.

2. Ajuste as configurações de HDMI em System > Video out (Sistema > Saída de vídeo).

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*.

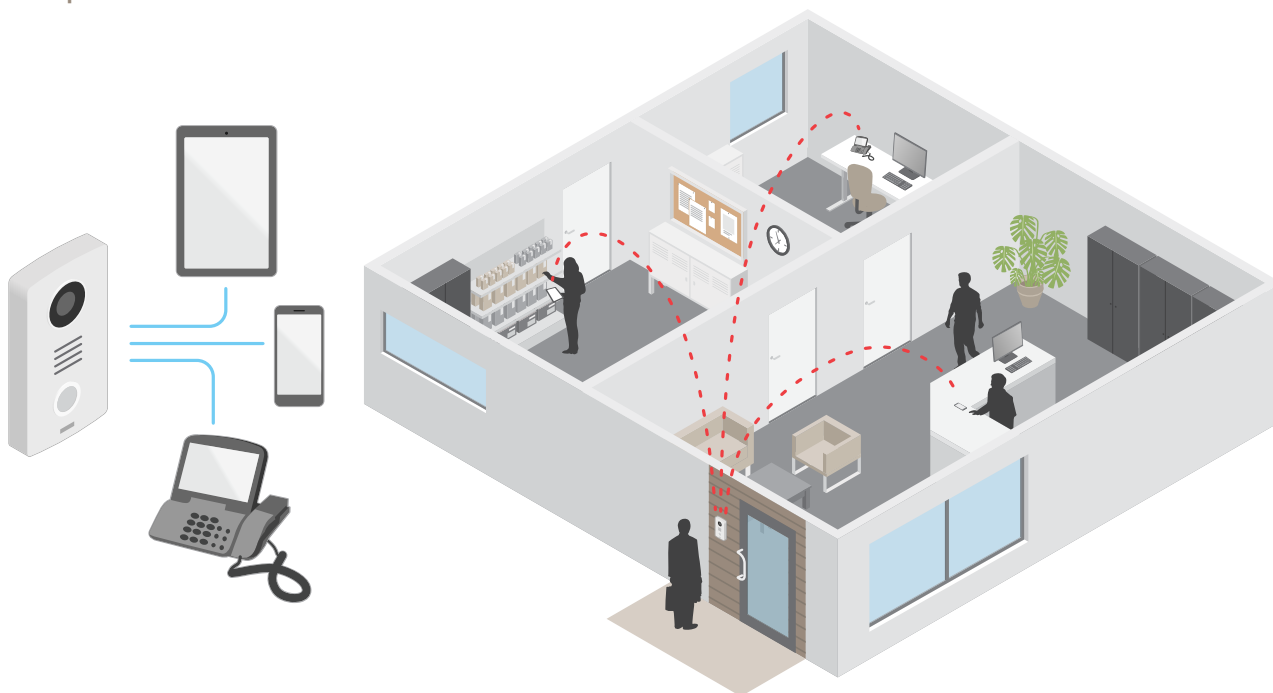
Saiba mais

Voice over IP (VoIP)

Voice over IP (VoIP) é um grupo de tecnologias que permite a comunicação por voz e sessões multimídia via redes IP, como a Internet. Em chamadas telefônicas tradicionais, os sinais analógicos são enviados através de transmissões de circuito através da rede de telefonia comutada pública (PSTN). Em uma chamada VoIP, os sinais analógicos são convertidos em sinais digitais para possibilitar o envio de pacotes de dados via redes IP locais ou pela Internet.

No produto Axis, o VoIP é possibilitado pelo Session Initiation Protocol (SIP) e a sinalização Dual-Tone multi-Frequency (DTMF).

Exemplo:



Quando você pressiona o botão de chamada em um porteiro eletrônico Axis, uma chamada é iniciada para um ou mais destinatários predefinidos. Quando um destinatário responde, uma chamada é estabelecida. A voz e o vídeo são transmitidos por meio de tecnologias VoIP.

Session Initiation Protocol (SIP)

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

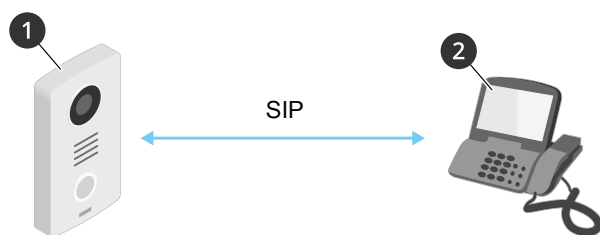
O áudio ou vídeo efetivos são trocados entre os agentes de usuário SIP com um protocolo de transporte, por exemplo, RTP (Real-Time Transport Protocol).

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

SIP ponto a ponto (P2PSIP)

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

Exemplo:



1 Agente de usuário A – porteiro eletrônico. Endereço SIP: sip:192.168.1.101

2 Agente de usuário B – telefone compatível com SIP. Endereço SIP: sip:192.168.1.100

Você pode configurar a estação de porta Axis para chamar, por exemplo, um telefone compatível com SIP na mesma rede usando uma configuração de SIP ponto a ponto.

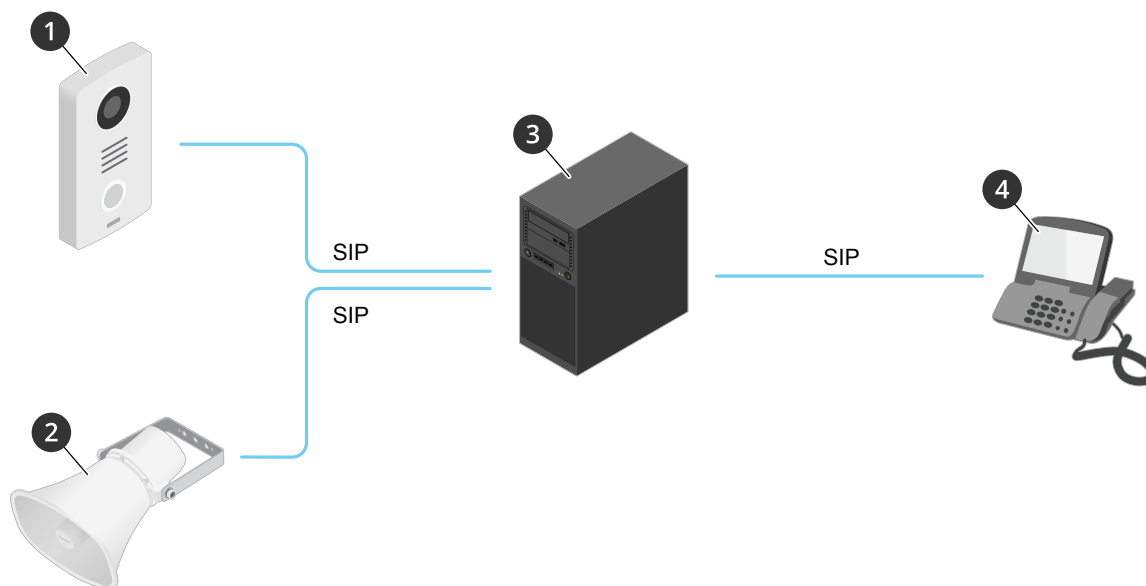
Private Branch Exchange (PBX)

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

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

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

Exemplo:



1 sip:minhaporta@empresa.com

2 sip:meualtofalante@empresa.com

3 PBX sip.empresa.com

4 sip:escritório@empresa.com

Quando você pressiona o botão de chamada em um porteiro eletrônico Axis, a chamada é encaminhada através de um ou mais PBXs para um endereço SIP na rede IP local ou via Internet.

Configuração de regras de eventos

Você pode criar regras para fazer com que o dispositivo realize ações quando certos eventos ocorrem. Uma regra consiste em condições e ações. As condições podem ser usadas para acionar as ações. Por exemplo, o dispositivo pode iniciar uma gravação ou enviar um email quando detecta movimento ou mostrar um texto de sobreposição enquanto o dispositivo está gravando.

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

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 Client for Unified Communication Systems

Com este aplicativo, você pode fazer chamadas entre dispositivos Axis habilitados para SIP e contas vinculadas do Microsoft® Teams. Para obter mais informações, consulte o *manual do usuário do AXIS Client for Unified Communication Systems*.

Uso diário

Use o teclado

Eu quero...	Ação
Ligar para alguém que possa me deixar entrar no edifício.	Pressione  .
Ligar para uma pessoa no edifício.	Insira o número de discagem rápida da pessoa e pressione  .
Abrir a porta com meu cartão e PIN.	Toque o cartão e insira o PIN.
Abrir a porta com meu PIN.	Insira o PIN e pressione #.
Abrir a porta com meu cartão.	Toque o cartão.

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 5.
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)**.

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, dicas e soluções

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

Problemas ao atualizar o firmware	
Falha na atualização do firmware	Se a atualização do firmware falhar, o dispositivo recarregará o firmware anterior. O motivo mais comum é que o arquivo de firmware incorreto foi carregado. Verifique se o nome do arquivo de firmware corresponde ao seu dispositivo e tente novamente.

Problemas na configuração do endereço IP

O dispositivo está localizado em uma sub-rede diferente	Se o endereço IP destinado ao dispositivo e o endereço IP do computador usado para acessar o dispositivo estiverem localizados em sub-redes diferentes, você não poderá definir o endereço IP. Entre em contato com o administrador da rede para obter um endereço IP.
O endereço IP está sendo usado por outro dispositivo	Desconecte o dispositivo Axis da rede. Execute o comando ping (em uma janela de comando/DOS, digite <code>ping</code> e o endereço IP do dispositivo): • Se você receber: <code>Reply from <IP address>: bytes=32; time=10...</code>, significa que o endereço IP já pode estar sendo usado por outro dispositivo na rede. Obtenha um novo endereço IP junto ao administrador da rede e reinstale o dispositivo. • Se você receber: <code>Request timed out</code>, significa que o endereço IP está disponível para uso com o dispositivo Axis. Verifique todo o cabeamento e reinstale o dispositivo.
Possível conflito de endereço IP com outro dispositivo na mesma sub-rede	O endereço IP estático no dispositivo Axis é usado antes que o DHCP defina um endereço dinâmico. Isso significa que, se o mesmo endereço IP estático padrão também for usado por outro dispositivo, poderá haver problemas para acessar o dispositivo.

O dispositivo não pode ser acessado por um navegador

Não é possível fazer login	Quando o HTTPS estiver ativado, certifique-se de que o protocolo correto (HTTP ou HTTPS) seja usado ao tentar fazer login. Talvez seja necessário digitar manualmente <code>http</code> ou <code>https</code> no campo de endereço do navegador. Se a senha do usuário root for perdida, o dispositivo deverá ser restaurado para as configurações padrão de fábrica. Consulte <i>Redefinição para as configurações padrão de fábrica</i> , on page 22.
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).

O dispositivo está acessível local, mas não externamente

Para acessar o dispositivo externamente, recomenda-se usar um dos seguintes aplicativos para Windows®:

- AXIS Companion: grátis, ideal para sistemas pequenos com necessidades básicas de monitoramento.
- AXIS Camera Station: versão de avaliação grátis por 30 dias, ideal para sistemas de pequeno a médio porte.

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

Considerações sobre desempenho

Ao configurar seu sistema, é importante considerar como diferentes configurações e situações afetam o desempenho. Alguns fatores afetam a largura de banda (taxa de bits), outros afetam a taxa de quadros e alguns afetam ambos.

Os fatores mais importantes a serem considerados são:

- Alta resolução de imagem ou níveis de compactação menores geram imagens com mais dados que, por sua vez, afetarão a largura de banda.
- O acesso por um grande número de clientes H.264/H.265/AV1 unicast ou Motion JPEG pode afetar a largura de banda.
- A exibição simultânea de diferentes streams (resolução, compactação) por diferentes clientes afeta a taxa de quadros e a largura de banda.
Use streams idênticos sempre que possível para manter uma alta taxa de quadros. Perfis de stream podem ser usados para garantir que streams sejam idênticos.
- O acesso a streams de vídeo com diferentes codecs afeta simultaneamente a taxa de quadros e a largura de banda. Para obter o desempenho ideal, use streams com o mesmo codec.
- O uso pesado de configurações de eventos afeta a carga da CPU do produto que, por sua vez, impacta a taxa de quadros.
- Usar HTTPS pode reduzir a taxa de quadros, especialmente se houver transmissão de Motion JPEG.
- A utilização pesada da rede devido à infraestrutura ruim afeta a largura de banda.
- A exibição em computadores clientes com desempenho ruim reduz o desempenho percebido e afeta a taxa de quadros.
- Executar vários aplicativos AXIS Camera Application Platform (ACAP) simultaneamente pode afetar a taxa de quadros e o desempenho geral.

Especificações

Indicadores e controles do painel frontal

Quando você conecta o produto à energia, os indicadores do painel frontal acendem por alguns segundos.

Ícones indicadores

Ícone	Indicação
	Azul estável quando a chamada enviada é iniciada. Pisca em azul quando a chamada recebida é iniciada.
	Âmbar estável para chamada em andamento.
	Aceso em verde quando a porta está aberta.

Faixa de indicadores do leitor de cartões

A faixa indica feedback do leitor.

Botão de chamada

Você pode usar a luz integrada ao redor do botão de chamada para iluminar os rostos dos visitantes.

Indicadores de LED

LED de estado	Indicação
Verde	Aceso em verde para operação normal.

Slot de cartão SD

OBSERVAÇÃO

- Risco de danos ao cartão SD. Não use ferramentas afiadas, objetos de metal ou força excessiva para inserir ou remover o cartão SD. Use os dedos para inserir e remover o cartão.
- Risco de perda de dados ou gravações corrompidas. Desmonte o cartão SD pela interface web do dispositivo antes de removê-lo. Não remova o cartão SD com o produto em funcionamento.

Esse dispositivo é compatível com cartões microSD/microSDHC/microSDXC.

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 22*.

Conectores

Conector HDMI

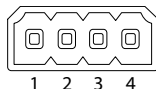
Use o conector microHDMI™ para conectar uma tela ou um monitor de exibição pública.

Conector de rede

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

Conector de áudio

Bloco de terminais com 4 pinos para entrada e saída de áudio.

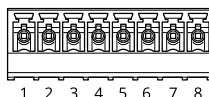


Função	Pino	Observações
Entrada de linha	1	Entrada de áudio (mono)
GND	2	Aterramento de áudio
Saída de linha	3	Saída de linha
GND	4	Aterramento de áudio

Conector do relé

Bloco de terminais com 8 pinos para relés de estado sólido que podem ser usados das seguintes formas:

- Como um relé padrão que abre e fecha circuitos auxiliares.
- Para controlar diretamente uma trava.
- Para controlar uma trava através de um relé de segurança. Usar um relé de segurança no lado seguro da porta evita hotwiring.



Função	Pino	Observações	Especificações
NO/NC	1	Normalmente aberto/Normalmente fechado Para conectar dispositivos de relé. Os dois pinos de relé estão galvanicamente separados do resto do circuito.	Corrente máxima 1 A Tensão máxima 30 V CC
COM	2	Comum	
24 VCC	3	Para equipamento auxiliar de alimentação. Observação: esse pino pode ser usado somente como saída de energia.	Tensão de saída 24 VCC Corrente máxima 50 mA ¹ Corrente máxima 350 mA ²
Terra CC	4		0 VCC
NO/NC	5	Normalmente aberto/Normalmente fechado Para conectar dispositivos de relé.	Corrente máxima 1 A Tensão máxima 30 V CC

1. Quando alimentado por Power over Ethernet IEEE 802.3af/802.3at Tipo 1 Classe 3.

2. Quando alimentado por Power over Ethernet Plus (PoE+) IEEE 802.3at Tipo 2 Classe 4 ou entrada de alimentação CC.

		Os dois pinos de relé estão galvanicamente separados do resto do circuito.	
COM	6	Comum	
12 V CC	7	Para equipamento auxiliar de alimentação. Observação: esse pino pode ser usado somente como saída de energia.	Tensão de saída 12 VCC Corrente máxima 100 mA ³ Corrente máxima 700 mA ⁴
Terra CC	8		0 VCC

Conector do leitor

Bloco de terminais com 4 pinos para conectar leitor externo.

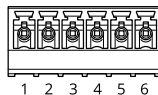
Função	Pino	Observações	Especificações
Terra CC	1		0 VCC
12 V CC	2	Para equipamento auxiliar de alimentação. Observação: esse pino pode ser usado somente como saída de energia.	Tensão de saída 12 VCC
D0/A+	3	Wiegand: saída DATA0 RS485: A+	
D1/B-	4	Wiegand: saída DATA1 RS485: B-	

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.

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.

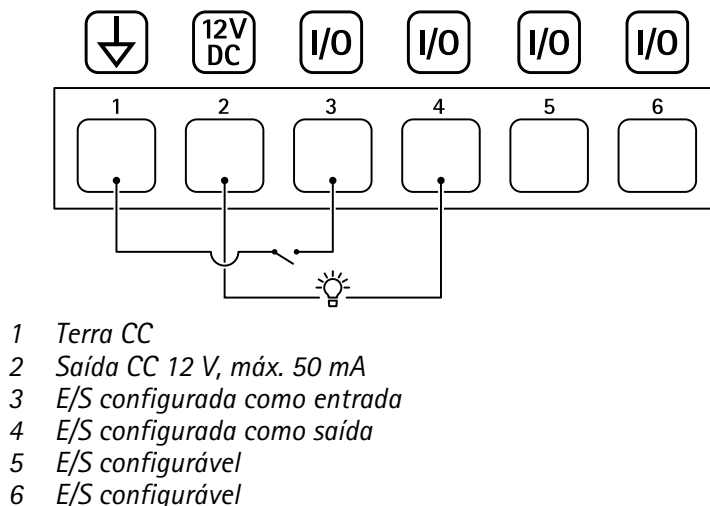


Função	Pino	Observações	Especificações
Terra CC	1		0 V CC
Saída CC	2	 Pode ser usada para alimentar equipamentos auxiliares.	12 V CC Carga máxima = 50 mA

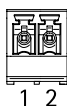
3. Quando alimentado por Power over Ethernet IEEE 802.3af/802.3at Tipo 1 Classe 3.

4. Quando alimentado por Power over Ethernet Plus (PoE+) IEEE 802.3at Tipo 2 Classe 4 ou entrada de alimentação CC.

		Observação: esse pino pode ser usado somente como saída de energia.	
Configurável (entrada ou saída)	3–6	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:

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	Pino	Observações	Especificações
Terra CC	1		0 VCC
Entrada CC	2	Para controlador de alimentação sem usar Power over Ethernet. Observação: esse pino pode ser usado somente como entrada de energia.	8 – 28 VCC, máx. 22 W Carga máx. em saídas 9 W

Informações sobre segurança

Níveis de perigo

▲ PERIGO

Indica uma situação perigosa que, se não evitada, irá resultar em morte ou lesões graves.

▲ AVISO

Indica uma situação perigosa que, se não evitada, poderá resultar em morte ou lesões graves.

▲ CUIDADO

Indica uma situação perigosa que, se não evitada, poderá resultar em lesões leves ou moderadas.

OBSERVAÇÃO

Indica uma situação perigosa que, se não evitada, poderá resultar em danos à propriedade.

Outros níveis de mensagens

Importante

Indica informações significativas que são essenciais para o produto funcionar corretamente.

Observação

Indica informações úteis que ajudam a obter o máximo do produto.

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.

T10176599_pt

2026-07 (M25.2)

© 2021 – 2026 Axis Communications AB