

AXIS A9210 Network I/O Relay Module

Manual do usuário

AXIS A9210 Network I/O Relay Module

Introdução

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

*Para usar a interface Web do AXIS OS com o iOS 15 ou iPadOS 15, acesse **Ajustes > Safari > Avançado > Recursos** e desative *NSURLSession Websocket*.

Se você precisar de mais informações sobre navegadores recomendados, acesse o *Portal do AXIS OS*.

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 na página 2*.

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 na página 2*.
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 na página 33*.

AXIS A9210 Network I/O Relay Module

Introdução

Senhas seguras

Importante

Os dispositivos Axis enviam a senha definida inicialmente na forma de texto plano via rede. Para proteger seu dispositivo após o primeiro login, configure uma conexão HTTPS segura e criptografada e altere a senha.

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.

Verifique se o firmware não foi violado

Para certificar-se de que o dispositivo tenha o firmware original da Axis, 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 na página 33*.
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.



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

help.axis.com/?&pid=92430§ion=web-interface-overview

Interface Web de um dispositivo Axis

AXIS A9210 Network I/O Relay Module

Configure seu dispositivo

Configure seu dispositivo

Configuração de uma porta de E/S

1. Vá para *I/O ports and relays > Settings > I/O* (Portas de E/S e relés > Configurações > E/S).
 2. Clique em  para expandir as configurações da porta de E/S.
 3. Renomeie a porta.
 4. Configure o estado normal. Clique em  para circuito aberto ou em  para circuito fechado.
 5. Para configurar a porta de E/S como entrada:
 - 5.1 Em *Direction* (Direção), clique em .
 - 5.2 Para monitorar o estado de entrada, ative *Supervised* (Supervisionada). Consulte *Entradas supervisionadas na página 32*.
- Observação**
- Em APIs, as portas de E/S supervisionada funcionam de forma diferente das portas de entrada supervisionada. Para obter mais informações, acesse a *Biblioteca VAPIX®*.
6. Para configurar a porta de E/S como saída:
 - 6.1 Em *Direction* (Direção), clique em .
 - 6.2 Para exibir os URLs para ativar e desativar os dispositivos conectados, vá para *Toggle port URL* (Alternar URL da porta).

Configurar um relé

1. Vá para *I/O ports and relays > Settings > Relays* (Portas de E/S e relés > Configurações > Relés).
2. Clique em  para expandir as configurações do relé.
3. Ative o relé.
4. Renomeie o relé.
5. Para exibir os URLs para ativar e desativar o relé, vá para *Toggle port URL* (Alternar URL da porta).

Configuração de regras de eventos

Para saber mais, consulte nosso guia *Introdução a regras de 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).

AXIS A9210 Network I/O Relay Module

Configure seu dispositivo

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)** o dispositivo deverá executar quando as condições forem atendidas.

Observação

Se você fizer alterações em uma regra ativa, a regra deverá ser ativada novamente para que as alterações entrem em vigor.

AXIS A9210 Network I/O Relay Module

A interface Web

Para alcançar a interface Web do dispositivo, digite o endereço IP do dispositivo em um navegador da Web.

Observação

O suporte aos recursos e às configurações descritas nesta seção variam para cada dispositivo. Este ícone  indica que o recurso ou configuração está disponível somente em alguns dispositivos.

-  Mostre ou oculte o menu principal.
-  Acesse as notas de versão.
-  Acesse a ajuda do produto.
-  Altere o idioma.
-  Defina o tema claro ou escuro.
-    O menu de usuário contém:
 - Informações sobre o usuário que está conectado.
 -  **Change account (Alterar conta)**: Saia da conta atual e faça login em uma nova conta.
 -  **Log out (Fazer logout)** : Faça logout da conta atual.
-  O menu de contexto contém:
 - **Analytics data (Dados de análise)**: Aceite para compartilhar dados de navegador não pessoais.
 - **Feedback (Comentários)**: Compartilhe qualquer feedback para nos ajudar a melhorar sua experiência de usuário.
 - **Legal**: Veja informações sobre cookies e licenças.
 - **About (Sobre)**: Exiba informações do dispositivo, incluindo versão do firmware e número de série.

Status

Device info (Informações do dispositivo)

Mostra as informações do dispositivo, incluindo versão do firmware e número de série.

Upgrade firmware (Atualizar firmware): Atualize o firmware em seu dispositivo. Abre a página Maintenance (Manutenção), na qual é possível atualizar o firmware.

Status de sincronização de horário

Mostra as informações de sincronização de NTP, incluindo se o dispositivo está em sincronia com um servidor NTP e o tempo restante até a próxima sincronização.

NTP settings (Configurações de NTP): Exiba e atualize as configurações de NTP. Leva você para a página Date and time (Data e hora) na qual é possível alterar as configurações de NTP.

Security (Segurança)

AXIS A9210 Network I/O Relay Module

A interface Web

Mostra os tipos de acesso ao dispositivo que estão ativos e quais protocolos de criptografia estão em uso. Recomendações para as configurações são baseadas no Guia de Fortalecimento do AXIS OS.

Hardening guide (Guia de fortalecimento): Clique para ir para o *Guia de Fortalecimento do AXIS OS*, onde você poderá aprender mais sobre segurança cibernética em dispositivos Axis e práticas recomendadas.

Connected clients (Clientes conectados)

Mostra o número de conexões e os clientes conectados.

View details (Exibir detalhes): Exiba e atualize a lista dos clientes conectados. A lista mostra endereço IP, protocolo, porta e PID/Processo de cada cliente.

Portas de E/S e relés

Settings (Configurações)

Input (Entrada)

- **Name (Nome):** Edite o texto para renomear a porta.
- **Direction (Direção):** Indica que é uma porta de entrada.
- **Normal state (Estado normal):** Clique em  para circuito aberto e  para circuito fechado.
- **Supervisionada:** Ative para possibilitar a detecção e o acionamento de ações se alguém violar a conexão com dispositivos de E/S digitais. Além de detectar se uma entrada está aberta ou fechada, você também pode detectar se alguém a adulterou (ou seja, cortada ou em curto). Supervisionar a conexão requer hardware adicional (resistores de fim de linha) no loop de E/S externo.
 - Para usar a primeira conexão paralela, selecione **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Conexão paralela primeiro com um resistor de 22 kΩ em paralelo e um resistor de 4,7 kΩ em série)**.
 - Para usar a primeira conexão serial, selecione **Serial first connection (Primeira conexão serial)** e selecione um valor de resistor na lista suspensa **Resistor values (Valores de resistor)**.

Output (Saída): Ative para habilitar os dispositivos conectados.

- **Name (Nome):** Edite o texto para renomear a porta.
- **Direction (Direção):** Indica que é uma porta de saída.
- **Normal state (Estado normal):** Clique em  para circuito aberto e  para circuito fechado.
- **Alternar URL da porta:** Mostra os URLs para ativar e desativar dispositivos conectados via interface de programação de aplicativos VAPIX®.

I/O (E/S): Ative para habilitar os dispositivos conectados quando a porta estiver configurada como saída.

- **Name (Nome):** Edite o texto para renomear a porta.
- **Direction (Direção):** Clique em  ou em  para configurá-la como entrada ou saída.
- **Normal state (Estado normal):** Clique em  para circuito aberto e  para circuito fechado.
- **Supervisionada:** Ative para possibilitar a detecção e o acionamento de ações se alguém violar a conexão com dispositivos de E/S digitais. Além de detectar se uma entrada está aberta ou fechada, você também pode detectar se alguém a adulterou (ou seja, cortada ou em curto). Supervisionar a conexão requer hardware adicional (resistores de fim de linha) no loop de E/S externo. Ela será exibida somente quando a porta estiver configurada como entrada.
 - Para usar a primeira conexão paralela, selecione **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Conexão paralela primeiro com um resistor de 22 kΩ em paralelo e um resistor de 4,7 kΩ em série)**.
 - Para usar a primeira conexão serial, selecione **Serial first connection (Primeira conexão serial)** e selecione um valor de resistor na lista suspensa **Resistor values (Valores de resistor)**.
- **Alternar URL da porta:** Mostra os URLs para ativar e desativar dispositivos conectados via interface de programação de aplicativos VAPIX®. Ela será exibida somente quando a porta estiver configurada como saída.

AXIS A9210 Network I/O Relay Module

A interface Web

Relés

- **Relé:** Ative ou desative o relé.
- **Name (Nome):** Edite o texto para renomear o relé.
- **Direction (Direção):** Indica que é um relé de saída.
- **Alternar URL da porta:** Mostra os URLs para ativar e desativar o relé via interface de programação de aplicativos VAPIX®.

Alarmes

Device motion (Movimento do dispositivo): Ative para acionar um alarme no sistema quando um movimento do dispositivo for detectado.

Casing open (Abertura da caixa)  : Ative para acionar um alarme no sistema quando a abertura de uma caixa de controlador de porta é detectada. Desative essa configuração para controladores de porta barebone.

External tamper (Violação externa)  : Ative para acionar um alarme no sistema quando uma violação externa é detectada. Por exemplo, quando alguém abre ou fecha o gabinete externo.

- **Supervised input (Entrada supervisionada)**  : Ligue para monitorar o estado de entrada e configure os resistores de fim de linha.
 - Para usar a primeira conexão paralela, selecione **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor** (Conexão paralela primeiro com um resistor de 22 kΩ em paralelo e um resistor de 4,7 kΩ em série).
 - Para usar a primeira conexão serial, selecione **Serial first connection (Primeira conexão serial)** e selecione um valor de resistor na lista suspensa **Resistor values (Valores de resistor)**.

Aplicativos



Add app (Adicionar aplicativo): Instale um novo aplicativo.

Find more apps (Encontrar mais aplicativos): Encontre mais aplicativos para instalar. Você será levado para uma página de visão geral dos aplicativos Axis.

Allow unsigned apps (Permitir aplicativos não assinados)  : Ative para permitir a instalação de aplicativos não assinados.

Allow root-privileged apps (Permitir aplicativos com privilégio de root)  : Ative para permitir que aplicativos com privilégios de root tenham acesso total ao dispositivo.



Veja as atualizações de segurança nos aplicativos AXIS OS e ACAP.

Observação

O desempenho do dispositivo poderá ser afetado se você executar vários aplicativos ao mesmo tempo.

Use a chave ao lado do nome do aplicativo para iniciar ou parar o aplicativo.

Open (Abrir): Acesse às configurações do aplicativo. As configurações disponíveis dependem do aplicativo. Alguns aplicativos não têm configurações.

AXIS A9210 Network I/O Relay Module

A interface Web



O menu de contexto pode conter uma ou mais das seguintes opções:

- **Open-source license (Licença de código aberto):** Exiba informações sobre as licenças de código aberto usadas no aplicativo.
- **App log (Log do aplicativo):** Exiba um log dos eventos de aplicativos. Este log é útil quando é necessário entrar em contato com o suporte.
- **Activate license with a key (Ativar licença com uma chave):** Se o aplicativo exigir uma licença, você deverá ativá-la. Use essa opção se o dispositivo não tiver acesso à Internet. Se você não tiver uma chave de licença, acesse axis.com/products/analytics. Você precisa de um código de licença e do número de série do produto Axis para gerar uma chave de licença.
- **Activate license automatically (Ativar licença automaticamente):** Se o aplicativo exigir uma licença, você deverá ativá-la. Use essa opção se o dispositivo tiver acesso à Internet. Um código de licença é necessário para ativar a licença.
- **Deactivate the license (Desativar a licença):** Desative a licença para substituí-la por outra licença, por exemplo, ao migrar de uma licença de avaliação para uma licença completa. Se você desativar a licença, ela será removida do dispositivo.
- **Settings (Configurações):** configure os parâmetros.
- **Delete (Excluir):** exclua o aplicativo permanentemente do dispositivo. Se você não desativar a licença primeiro, ela permanecerá ativa.

Sistema

Hora e local

Data e hora

O formato de hora depende das configurações de idioma do navegador da Web.

Observação

Recomendamos sincronizar a data e a hora do dispositivo com um servidor NTP.

Synchronization (Sincronização): Selecione uma opção para sincronização da data e da hora do dispositivo.

- **Automatic date and time (manual NTS KE servers) (Data e hora automáticas (servidores NTS KE manuais)):** Sincronizar com os servidores estabelecimentos de chave NTP seguros conectados ao servidor DHCP.
 - **Manual NTS KE servers (Servidores NTS KE manuais):** Insira o endereço IP de um ou dois servidores NTP. Quando você usa dois servidores NTP, o dispositivo sincroniza e adapta sua hora com base na entrada de ambos.
- **Automatic date and time (NTP servers using DHCP) (Data e hora automáticas (servidores NTP usando DHCP)):** Sincronize com os servidores NTP conectados ao servidor DHCP.
 - **Fallback NTP servers (Servidores NTP de fallback):** Insira o endereço IP de um ou dois servidores de fallback.
- **Automatic date and time (manual NTP servers) (Data e hora automáticas (servidores NTP manuais)):** Sincronize com os servidores NTP de sua escolha.
 - **Manual NTP servers (Servidores NTP manuais):** Insira o endereço IP de um ou dois servidores NTP. Quando você usa dois servidores NTP, o dispositivo sincroniza e adapta sua hora com base na entrada de ambos.
- **Custom date and time (Data e hora personalizadas):** Defina manualmente a data e a hora. Clique em **Get from system (Obter do sistema)** para obter as configurações de data e hora uma vez em seu computador ou dispositivo móvel.

Time zone (Fuso horário): Selecione qual fuso horário será usado. A hora será ajustada automaticamente para o horário de verão e o horário padrão.

Observação

O sistema usa as configurações de data e hora em todas as gravações, logs e configurações do sistema.

Local do dispositivo

Insira o local do dispositivo. Seu sistema de gerenciamento de vídeo pode usar essa informação para posicionar o dispositivo em um mapa.

AXIS A9210 Network I/O Relay Module

A interface Web

- **Latitude:** Valores positivos estão ao norte do equador.
- **Longitude:** Valores positivos estão a leste do meridiano de Greenwich.
- **Heading (Cabeçalho):** Insira a direção da bússola para a qual o dispositivo está voltado. 0 representa o norte.
- **Label (Rótulo):** Insira um nome descritivo para o dispositivo.
- **Save (Salvar):** Clique em para salvar a localização do dispositivo.

Rede

IPv4

Assign IPv4 automatically (Atribuir IPv4 automaticamente): Selecione para permitir que o roteador de rede atribua um endereço IP ao dispositivo automaticamente. Recomendamos utilizar IP (DHCP) automático para a maioria das redes.

IP address (Endereço IP): Insira um endereço IP exclusivo para o dispositivo. Endereços IP estáticos podem ser atribuídos aleatoriamente em redes isoladas, desde que cada endereço seja único. Para evitar conflitos, é altamente recomendável entrar em contato o administrador da rede antes de atribuir um endereço IP estático.

Subnet mask (Máscara de sub-rede): Insira a máscara de sub-rede para definir quais endereços estão dentro da rede local. Qualquer endereço fora da rede local passa pelo roteador.

Router (Roteador): Insira o endereço IP do roteador padrão (gateway) usado para conectar dispositivos conectados a diferentes redes e segmentos de rede.

Fallback to static IP address if DHCP isn't available (Retornar como contingência para o endereço IP estático se o DHCP não estiver disponível): Selecione se você deseja adicionar um endereço IP estático para usar como contingência se o DHCP não estiver disponível e não puder atribuir um endereço IP automaticamente.

Observação

Se o DHCP não estiver disponível e o dispositivo usar um fallback de endereço estático, o endereço estático será configurado com um escopo limitado.

IPv6

Assign IPv6 automatically (Atribuir IPv6 automaticamente): Selecione para ativar o IPv6 e permitir que o roteador de rede atribua um endereço IP ao dispositivo automaticamente.

Hostname (Nome de host)

Assign hostname automatically (Atribuir nome de host automaticamente): Selecione para permitir que o roteador de rede atribua um nome de host ao dispositivo automaticamente.

Hostname (Nome de host): Insira o nome de host manualmente para usar como uma maneira alternativa de acessar o dispositivo. O relatório do servidor e o log do sistema usam o nome de host. Os caracteres permitidos são A – Z, a – z, 0 – 9 e -.

DNS servers (Servidores DNS)

Assign DNS automatically (Atribuir o DNS automaticamente): Selecione para permitir que o servidor DHCP atribua domínios de pesquisa e endereços de servidor DNS ao dispositivo automaticamente. Recomendamos utilizar DNS (DHCP) automático para a maioria das redes.

Search domains (Domínios de pesquisa): Ao usar um nome de host que não está totalmente qualificado, clique em **Add search domain (Adicionar domínio de pesquisa)** e insira um domínio para pesquisar o nome de domínio usado pelo dispositivo.

DNS servers (Servidores DNS): Clique em **Add DNS server (Adicionar servidor DNS)** e insira o endereço IP do servidor DNS. Esse servidor fornece a tradução dos nomes de host em endereços IP na sua rede.

HTTP and HTTPS (HTTP e HTTPS)

AXIS A9210 Network I/O Relay Module

A interface Web

O HTTPS é um protocolo que fornece criptografia para solicitações de páginas de usuários e para as páginas retornadas pelo servidor Web. A troca de informações criptografadas é regida pelo uso de um certificado HTTPS que garante a autenticidade do servidor.

Para usar HTTPS no dispositivo, é necessário instalar certificado HTTPS. Vá para **System > Security (Sistema > Segurança)** para criar e instalar certificados.

Allow access through (Permitir acesso via): Selecione se um usuário tem permissão para se conectar ao dispositivo via protocolos HTTP, HTTPS ou HTTP and HTTPS (HTTP e HTTPS).

Observação

Se você exibir páginas da Web criptografadas via HTTPS, talvez haja uma queda no desempenho, especialmente quando uma página é solicitada pela primeira vez.

HTTP port (Porta HTTP): Insira a porta HTTP que será usada. O dispositivo permite a porta 80 ou qualquer porta no intervalo 1024 – 65535. Se você estiver conectado como um administrador, também poderá inserir qualquer porta no intervalo 1 – 1023. Se você usar uma porta nesse intervalo, receberá um aviso.

HTTPS port (Porta HTTPS): Insira a porta HTTPS que será usada. O dispositivo permite a porta 443 ou qualquer porta no intervalo 1024 – 65535. Se você estiver conectado como um administrador, também poderá inserir qualquer porta no intervalo 1 – 1023. Se você usar uma porta nesse intervalo, receberá um aviso.

Certificate (Certificado): Selecione um certificado para ativar o HTTPS para o dispositivo.

Protocolos de descoberta de rede

Bonjour®: Ative para permitir a descoberta automática na rede.

Bonjour name (Nome Bonjour): Insira um nome amigável para ser visível na rede. O nome padrão é o nome do dispositivo e seu endereço MAC.

UPnP®: Ative para permitir a descoberta automática na rede.

UPnP name (Nome UPnP): Insira um nome amigável para ser visível na rede. O nome padrão é o nome do dispositivo e seu endereço MAC.

WS-Discovery: Ative para permitir a descoberta automática na rede.

One-click cloud connection (Conexão em nuvem com um clique)

O One-Click Cloud Connect (O3C), em conjunto com um serviço O3C, fornece acesso via Internet fácil e seguro a vídeo ao vivo e gravado a partir de qualquer local. Para obter mais informações, consulte axis.com/end-to-end-solutions/hosted-services.

Allow O3C (Permitir O3):

- **One-click (Um clique):** Essa é a configuração padrão. Pressione e mantenha pressionado o botão de controle no dispositivo para conectar a um serviço O3C via Internet. Você precisa registrar o dispositivo com o serviço O3C dentro de 24 horas após pressionar o botão de controle. Caso contrário, o dispositivo se desconectará do serviço O3C. Após o dispositivo ser registrado, a opção **Always (Sempre)** será ativada e seu dispositivo Axis permanecerá conectado ao serviço O3C.
- **Sempre:** O dispositivo tenta constantemente conectar a um serviço O3C pela Internet. Uma vez registrado, o dispositivo permanece conectado ao serviço O3C. Use essa opção se o botão de controle do dispositivo estiver fora de alcance.
- **No (Não):** Desativa o serviço O3C.

Proxy settings (Configurações de proxy): Se necessário, insira as configurações de proxy para conectar ao servidor proxy.

Host: Insira o endereço do servidor proxy.

Port (Porta): Insira o número da porta usada para acesso.

Login e Password (Senha): Se necessário, insira um nome de usuário e uma senha para o servidor proxy.

Authentication method (Método de autenticação):

AXIS A9210 Network I/O Relay Module

A interface Web

- **Basic (Básico):** Este método é o esquema de autenticação mais compatível para HTTP. Ele é menos seguro do que o método de **Digest**, pois ele envia o nome de usuário e a senha não criptografados para o servidor.
- **Digest:** Esse método é mais seguro porque sempre transfere a senha criptografada pela rede.
- **Auto:** Essa opção permite que o dispositivo selecione o método de autenticação automaticamente dependendo dos métodos suportados. Ela prioriza o método **Digest** sobre o método **Basic (Básico)**.

Owner authentication key (OAK) (Chave de autenticação do proprietário (OAK): Clique em **Get key (Obter chave)** para buscar a chave de autenticação do proprietário. Isso só será possível se o dispositivo estiver conectado à Internet sem um firewall ou proxy.

SNMP

O Simple Network Management Protocol (SNMP) possibilita o acesso e o gerenciamento remotos de dispositivos de rede.

SNMP: Selecione a versão de SNMP que deve ser utilizada.

- **v1 and v2c (v1 e v2c):**
 - **Read community (Comunidade de leitura):** Insira o nome da comunidade que tem acesso somente de leitura a todos os objetos SNMP suportados. O valor padrão é **public (público)**.
 - **Write community (Comunidade de gravação):** Insira o nome da comunidade que tem acesso de leitura ou gravação em todos os objetos SNMP suportados (exceto objetos somente leitura). O valor padrão é **write (gravação)**.
 - **Activate traps (Ativar intercepções):** Ative para ativar o relatório de intercepções. O dispositivo usa intercepções para enviar mensagens sobre eventos importantes ou alterações de status para um sistema de gerenciamento. Na interface Web, você pode configurar intercepções para SNMP v1 e v2c. As intercepções serão desativadas automaticamente se você mudar para SNMP v3 ou desativar o SNMP. Se você usa SNMP v3, é possível configurar intercepções via aplicativo de gerenciamento do SNMP v3.
 - **Trap address (Endereço da intercepção):** Insira o endereço IP ou nome de host do servidor de gerenciamento.
 - **Trap community (Comunidade de intercepção):** Insira a comunidade que é usada quando o dispositivo envia uma mensagem de intercepção para o sistema de gerenciamento.
 - **Traps (Intercepções):**
 - **Cold start (Partida a frio):** Envia uma mensagem de intercepção quando o dispositivo é iniciado.
 - **Warm start (Partida a quente):** Envia uma mensagem de intercepção quando uma configuração de SNMP é alterada.
 - **Link up (Link ativo):** Envia uma mensagem de intercepção quando um link muda de inativo para ativo.
 - **Authentication failed (Falha de autenticação):** Envia uma mensagem de intercepção quando uma tentativa de autenticação falha.

Observação

Todas as intercepções MIB de vídeo Axis são habilitados quando você ativa as intercepções SNMP v1 e v2c. Para obter mais informações, consulte *AXIS OS portal > SNMP*.

- **v3:** O SNMP v3 é uma versão mais segura que fornece criptografia e senhas seguras. Para usar o SNMP v3, recomendamos ativar o HTTPS, pois as senhas serão enviadas via HTTPS. Isso também impede que partes não autorizadas acessem intercepções SNMP v1 e v2c não criptografadas. Se você usa SNMP v3, é possível configurar intercepções via aplicativo de gerenciamento do SNMP v3.
 - **Password for the account "initial" (Senha para a conta "initial"):** Insira a senha do SNMP para a conta chamada "initial". Embora a senha possa ser enviada sem ativar o HTTPS, isso não é recomendável. A senha do SNMP v3 só pode ser definida uma vez e, preferivelmente, quando o HTTPS está ativado. Após a senha ser definida, o campo de senha não será mais exibido. Para definir a senha novamente, o dispositivo deverá ser redefinido para as configurações padrões de fábrica.

Segurança

Certificados

AXIS A9210 Network I/O Relay Module

A interface Web

Os certificados são usados para autenticar dispositivos em uma rede. O dispositivo oferece suporte a dois tipos de certificados:

- **Certificados cliente/servidor**
Um certificado cliente/servidor valida a identidade do produto e pode ser autoassinado ou emitido por uma autoridade de certificação (CA). Um certificado autoassinado oferece proteção limitada e pode ser usado antes que um certificado emitido por uma CA tenha sido obtido.
- **Certificados CA**
Você pode usar um certificado de CA para autenticar um certificado de par, por exemplo, para validar a identidade de um servidor de autenticação quando o dispositivo se conecta a uma rede protegida por IEEE 802.1X. O dispositivo possui vários certificados de CA pré-instalados.

Os seguintes formatos são aceitos:

- Formatos de certificado: .PEM, .CER e .PFX
- Formatos de chave privada: PKCS#1 e PKCS#12

Importante

Se você redefinir o dispositivo para o padrão de fábrica, todos os certificados serão excluídos. Quaisquer certificados CA pré-instalados serão reinstalados.



Add certificate (Adicionar certificado): Clique para adicionar um certificado.

- **Mais** : Mostre mais campos para preencher ou selecionar.
- **Secure keystore (Armazenamento de chaves seguro):** Selecione para usar Secure element (Elemento seguro) ou Trusted Platform Module 2.0 para armazenar de forma segura a chave privada. Para obter mais informações sobre qual tecla segura será selecionada, vá para help.axis.com/en-us/axis-os#cryptographic-support.
- **Tipo da chave:** Selecione o algoritmo de criptografia padrão ou diferente na lista suspensa para proteger o certificado.



O menu de contexto contém:

- **Certificate information (Informações do certificado):** Exiba as propriedades de um certificado instalado.
- **Delete certificate (Excluir certificado):** Exclua o certificado.
- **Create certificate signing request (Criar solicitação de assinatura de certificado):** Crie uma solicitação de assinatura de certificado para enviar a uma autoridade de registro para se aplicar para um certificado de identidade digital.

Secure keystore (Armazenamento de chaves seguro)

- **Secure element (CC EAL6+) (Elemento seguro (CC EAL6+)):** Selecione para usar o elemento seguro no armazenamento de chaves seguro.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Nível 2):** Selecione para usar TPM 2.0 para armazenamento de chaves seguro.

IEEE 802.1x and IEEE 802.1AE MACsec (IEEE 802.1x e IEEE 802.1AE MACsec)

O IEEE 802.1x é um padrão do IEEE para controle de admissão em redes baseado em portas que fornece autenticação segura de dispositivos em rede com e sem fio. O IEEE 802.1x é baseado no EAP (Extensible Authentication Protocol).

Para acessar uma rede protegida pelo IEEE 802.1x, os dispositivos de rede devem se autenticar. A autenticação é executada por um servidor de autenticação, geralmente, um servidor RADIUS (por exemplo, FreeRADIUS e Microsoft Internet Authentication Server).

Certificados

Quando configurado sem um certificado de CA, a validação do certificado do servidor é desativada e o dispositivo tenta se autenticar independentemente da rede à qual está conectado.

Ao usar um certificado, na implementação da Axis, o dispositivo e o servidor de autenticação se autenticam com certificados digitais usando EAP-TLS (Extensible Authentication Protocol – Transport Layer Security).

Para permitir que o dispositivo acesse uma rede protegida por certificados, é necessário instalar um certificado de cliente assinado no dispositivo.

AXIS A9210 Network I/O Relay Module

A interface Web

Authentication method (Método de autenticação): Selecione um tipo de EAP usado para autenticação. A opção padrão é EAP-TLS. EAP-PEAP/MSCHAPv2 é uma opção mais segura.

Client certificate (Certificado de cliente): Selecione um certificado de cliente para usar o IEEE 802.1x. O servidor de autenticação usa o certificado para validar a identidade do cliente.

CA certificate (Certificado de CA): Selecione certificados CA para validar identidade do servidor de autenticação. Quando nenhum certificado é selecionado, o dispositivo tenta se autenticar independentemente da rede à qual está conectado.

EAP identity (Identidade EAP): Insira a identidade do usuário associada ao seu certificado de cliente.

EAPOL version (Versão EAPOL): Selecione a versão EAPOL que é usada no switch de rede.

Use IEEE 802.1x (Usar IEEE 802.1x): selecione para usar o protocolo IEEE 802.1 x.

IEEE 802.1AE MACsec

O IEEE 802.1AE MACsec é um padrão IEEE para segurança de controle de acesso à mídia (MAC) que define a confidencialidade e integridade de dados sem conexão para protocolos independentes de acesso à mídia.

As configurações só estarão disponíveis se você usar EAP-TLS como método de autenticação:

Mode (Modo)

- **CAK/EAP-TLS dinâmico:** a opção padrão. Após uma conexão segura, o dispositivo verifica o MACsec na rede.
- **CAK estático/chave pré-compartilhada (PSK):** Selecione para definir o nome e o valor da chave para se conectar à rede.

As configurações só estarão disponíveis se você usar EAP-PEAP/MSCHAPv2 como método de autenticação:

- **Password (Senha):** Insira a senha para sua identidade de usuário.
- **Peap version (Versão do Peap):** Selecione a versão do Peap que é usada no switch de rede.
- **Label (Rótulo):** Selecione 1 para usar a criptografia EAP do cliente; selecione 2 para usar a criptografia PEAP do cliente. Selecione o rótulo que o switch de rede usa ao utilizar a versão 1 do Peap.

Prevent brute-force attacks (Impedir ataques de força bruta)

Blocking (Bloqueio): Ative para bloquear ataques de força bruta. Um ataque de força bruta usa tentativa e erro para adivinhar informações de login ou chaves de criptografia.

Blocking period (Período de bloqueio): Insira o número de segundos para bloquear um ataque de força bruta.

Blocking conditions (Condições de bloqueio): Insira o número de falhas de autenticação permitidas por segundo antes do início do bloco. Você pode definir o número de falhas permitidas em nível de página ou em nível de dispositivo.

IP address filter (Filtro de endereços IP)

Use filter (Usar filtro): Selecione para filtrar quais endereços IP têm permissão para acessar o dispositivo.

Policy (Política): Escolha se deseja Allow (Permitir) ou Deny (Negar) acesso para certos endereços IP.

Addresses (Endereços): Insira os números IP que têm acesso permitido ou negado ao dispositivo. Você também pode usar o formato CIDR.

Certificado de firmware assinado personalizado

AXIS A9210 Network I/O Relay Module

A interface Web

Para instalar firmware de teste ou outro firmware personalizado da Axis no dispositivo, um certificado de firmware com assinatura personalizada é necessário. O certificado verifica se o firmware é aprovado pelo proprietário do dispositivo e pela Axis. O firmware pode ser executado somente em um dispositivo específico identificado por seu número de série e ID de chip exclusivos. Somente a Axis pode criar certificados de firmware com assinatura personalizada, pois é a Axis que possui a chave para assiná-los.

Install (Instalar): Clique para instalar o certificado. É necessário instalar o certificado antes de instalar o firmware.



O menu de contexto contém:

- **Delete certificate (Excluir certificado):** Exclua o certificado.

Contas

Accounts (Contas)



Add account (Adicionar conta): Clique para adicionar uma nova conta. É possível adicionar até 100 contas.

Account (Conta): Insira um nome de conta exclusivo.

New password (Nova senha): Insira uma senha para o nome da conta. As senhas devem conter 1 a 64 caracteres de comprimento. Somente caracteres ASCII imprimíveis (código 32 a 126) são permitidos na senha, por exemplo, letras, números, pontuação e alguns símbolos.

Repeat password (Repetir senha): Insira a mesma senha novamente.

Privileges (Privilégios):

- **Administrator (Administrador):** Tem acesso irrestrito a todas as configurações. Os administradores também podem adicionar, atualizar e remover outras contas.
- **Operator (Operador):** Tem acesso a todas as configurações, exceto:
 - Todas as configurações do **System (Sistema)**.
 - Adicionando aplicativos.
- **Viewer (Visualizador):** Não tem acesso para alterar as configurações.



O menu de contexto contém:

Update account (Atualizar conta): Edite as propriedades da conta.

Delete account (Excluir conta): Exclua a conta. Não é possível excluir a conta root.

Anonymous access (Acesso anônimo)

Allow anonymous viewing (Permitir visualização anônima): Ative para permitir que qualquer pessoa acesse o dispositivo como um visualizador sem precisar fazer login com uma conta.

Allow anonymous PTZ operating (Permitir operação de PTZ anônima)  : Ative para permitir que usuários anônimos façam pan, tilt e zoom da imagem.

SSH accounts (Contas SSH)

AXIS A9210 Network I/O Relay Module

A interface Web

+ Add SSH account (Adicionar conta SSH): Clique para adicionar uma nova conta SSH.

- **Restrict root access (Restringir o acesso de root):** Ative essa opção para restringir funcionalidade que requer acesso root.
- **Enable SSH (Ativar SSH):** Ative para usar o serviço SSH.

Account (Conta): Insira um nome de conta exclusivo.

New password (Nova senha): Insira uma senha para o nome da conta. As senhas devem conter 1 a 64 caracteres de comprimento. Somente caracteres ASCII imprimíveis (código 32 a 126) são permitidos na senha, por exemplo, letras, números, pontuação e alguns símbolos.

Repeat password (Repetir senha): Insira a mesma senha novamente.

Comment (Comentário): Insira um comentário (opcional).

⋮ O menu de contexto contém:

Update SSH account (Atualizar conta SSH): Edite as propriedades da conta.

Delete SSH account (Excluir conta SSH): Exclua a conta. Não é possível excluir a conta root.

Configuração de OpenID

Importante

Insira os valores certos para garantir que você possa efetuar login no dispositivo novamente.

Client ID (ID do cliente): Insira o nome de usuário de OpenID.

Proxy de saída: Insira o endereço proxy da conexão OpenID para usar um servidor proxy.

Reivindicação de administrador: Insira um valor para a função de administrador.

URL do provedor: Insira o link Web para a autenticação do ponto de extremidade de API. O formato deve ser `https://[inserir URL]/bem conhecido/openid-configuration`

Reivindicação de operador: Insira um valor para a função do operador.

Exigir reivindicação: Insira os dados que deveriam estar no token.

Reivindicação de visualizador: Insira o valor da função de visualizador.

Usuário remoto: Insira um valor para identificar usuários remotos. Isso ajudará a exibir o usuário atual na interface web do dispositivo.

Escopos: Escopos opcionais que poderiam fazer parte do token.

Segredo do cliente: Insira a senha OpenID novamente

Salvar: Clique em para salvar os valores de OpenID.

Ativar OpenID: Ative para fechar a conexão atual e permita a autenticação do dispositivo via URL do provedor.

Eventos

Regras

Uma regra define as condições que fazem com que o produto execute uma ação. A lista mostra todas as regras configuradas no produto no momento.

AXIS A9210 Network I/O Relay Module

A interface Web

Observação

Você pode criar até 256 regras de ação.



Add a rule (Adicionar uma regra): Crie uma regra.

Name (Nome): insira um nome para a regra.

Wait between actions (Aguardar entre ações): insira o tempo mínimo (hh:mm:ss) que deve passar entre ativações de regras. Ela será útil se a regra for ativada, por exemplo, em condições de modo diurno/noturno, para evitar que pequenas mudanças de iluminação durante o nascer e o pôr do sol ativem a regra várias vezes.

Condition (Condição): selecione uma condição na lista. Uma condição deve ser atendida para que o dispositivo execute uma ação. Se várias condições forem definidas, todas elas deverão ser atendidas para acionar a ação. Para obter informações sobre condições específicas, consulte *Introdução às regras de eventos*.

Use this condition as a trigger (Usar esta condição como acionador): selecione para que essa primeira função opere apenas como acionador inicial. Isso significa que, uma vez que a regra for ativada, ela permanecerá ativa enquanto todas as outras condições forem atendidas, independentemente do estado da primeira condição. Se você não marcar essa opção, a regra simplesmente será ativada quando todas as condições forem atendidas.

Invert this condition (Inverter esta condição): marque se você quiser que a condição seja o contrário de sua seleção.



Add a condition (Adicionar uma condição): clique para adicionar uma condição.

Action (Ação): selecione uma ação na lista e insira as informações necessárias. Para obter informações sobre ações específicas, consulte *Introdução às regras de eventos*.

Destinatários

Você pode configurar seu dispositivo para notificar os destinatários sobre eventos ou enviar arquivos. A lista mostra todos os destinatários atualmente configurados no produto, juntamente com informações sobre suas configurações.

Observação

É possível criar até 20 destinatários.



Add a recipient (Adicionar um destinatário): clique para adicionar um destinatário.

Name (Nome): insira um nome para o destinatário.

Type (Tipo): selecione na lista:

- FTP 
 - **Host:** insira o endereço IP ou o nome de host do servidor. Se você inserir um nome de host, verifique se um servidor DNS está especificado em **System > Network > IPv4 and IPv6 (Sistema > Rede > IPv4 e IPv6)**.
 - **Port (Porta):** insira o número da porta usada pelo servidor FTP. O padrão é 21.
 - **Folder (Pasta):** insira o caminho para o diretório em que deseja armazenar arquivos. Se esse diretório ainda não existir no servidor FTP, você receberá uma mensagem de erro ao fazer upload de arquivos.
 - **Username (Nome de usuário):** insira o nome de usuário para o login.
 - **Password (Senha):** insira a senha para o login.
 - **Use temporary file name (Usar nome de arquivo temporário):** marque para carregar arquivos com nomes temporários e gerados automaticamente. Os arquivos serão renomeados para os nomes desejados quando o upload for concluído. Se o upload for cancelado/interrompido, nenhum arquivo será corrompido. No entanto, provavelmente você ainda obterá os arquivos temporários. Dessa forma, você saberá que todos os arquivos com o nome desejado estão corretos.

AXIS A9210 Network I/O Relay Module

A interface Web

- Use **passive FTP (Usar FTP passivo)**: Em circunstâncias normais, o produto simplesmente solicita que o servidor FTP de destino abra a conexão de dados. O dispositivo inicia ativamente as conexões de controle de FTP e dados para o servidor de destino. Isso é normalmente necessário quando há um firewall entre o dispositivo e o servidor FTP de destino.
- **HTTP**
 - **URL**: insira o endereço de rede do servidor HTTP e o script que cuidará da solicitação. Por exemplo, `http://192.168.254.10/cgi-bin/notify.cgi`.
 - **Username (Nome de usuário)**: insira o nome de usuário para o login.
 - **Password (Senha)**: insira a senha para o login.
 - **Proxy**: ative e insira as informações necessárias se houver a necessidade de passar por um servidor proxy para se conectar ao servidor HTTP.
- **HTTPS**
 - **URL**: Insira o endereço de rede do servidor HTTPS e o script que cuidará da solicitação. Por exemplo, `https://192.168.254.10/cgi-bin/notify.cgi`.
 - **Validate server certificate (Validar certificado do servidor)**: marque para validar o certificado que foi criado pelo servidor HTTPS.
 - **Username (Nome de usuário)**: insira o nome de usuário para o login.
 - **Password (Senha)**: insira a senha para o login.
 - **Proxy**: ative e insira as informações necessárias se houver a necessidade de passar por um servidor proxy para se conectar ao servidor HTTPS.
- **Network storage (Armazenamento de rede)** 

Você pode adicionar armazenamento de rede, como um NAS (Network Attached Storage), e utilizá-lo como destinatário para armazenar arquivos. Os arquivos são armazenados no formato Matroska (MKV).

 - **Host**: Insira o endereço IP ou o nome de host do armazenamento de rede.
 - **Share (Compartilhamento)**: insira o nome do compartilhamento no host.
 - **Folder (Pasta)**: insira o caminho para o diretório em que deseja armazenar arquivos.
 - **Username (Nome de usuário)**: insira o nome de usuário para o login.
 - **Password (Senha)**: insira a senha para o login.
- **SFTP** 
 - **Host**: insira o endereço IP ou o nome de host do servidor. Se você inserir um nome de host, verifique se um servidor DNS está especificado em **System > Network > IPv4 and IPv6 (Sistema > Rede > IPv4 e IPv6)**.
 - **Port (Porta)**: insira o número da porta usada pelo servidor SFTP. O padrão é 22.
 - **Folder (Pasta)**: insira o caminho para o diretório em que deseja armazenar arquivos. Se esse diretório ainda não existir no servidor SFTP, você receberá uma mensagem de erro ao fazer upload de arquivos.
 - **Username (Nome de usuário)**: insira o nome de usuário para o login.
 - **Password (Senha)**: insira a senha para o login.
 - **SSH host public key type (MD5) (Tipo de chave pública do host SSH [MD5])**: insira a impressão digital da chave pública do host remoto (sequência de 32 dígitos hexadecimais). O cliente SFTP oferece suporte a servidores SFTP que utilizam SSH-2 com os tipos de chave de host RSA, DSA, ECDSA e ED25519. RSA é o método preferido durante a negociação, seguido por ECDSA, ED25519 e DSA. Certifique-se de inserir a chave de host MD5 certa que é usada pelo seu servidor SFTP. Embora o dispositivo Axis ofereça suporte a chaves de hash MD5 e SHA-256, recomenda-se usar a SHA-256 devido à segurança mais forte do que o MD5. Para obter mais informações sobre como configurar um servidor SFTP com um dispositivo Axis, acesse o *Portal do AXIS OS*.
 - **SSH host public key type (SHA256) (Tipo de chave pública do host SSH [MD5])**: insira a impressão digital da chave pública do host remoto (string codificada em Base64 com 43 dígitos). O cliente SFTP oferece suporte a servidores SFTP que utilizam SSH-2 com os tipos de chave de host RSA, DSA, ECDSA e ED25519. RSA é o método preferido durante a negociação, seguido por ECDSA, ED25519 e DSA. Certifique-se de inserir a chave de host MD5 certa que é usada pelo seu servidor SFTP. Embora o dispositivo Axis ofereça suporte a chaves de hash MD5 e SHA-256, recomenda-se usar a SHA-256 devido à segurança mais forte do que o MD5. Para obter mais informações sobre como configurar um servidor SFTP com um dispositivo Axis, acesse o *Portal do AXIS OS*.
 - **Use temporary file name (Usar nome de arquivo temporário)**: marque para carregar arquivos com nomes temporários e gerados automaticamente. Os arquivos serão renomeados para os nomes desejados quando o upload for concluído. Se o upload for cancelado ou interrompido, nenhum arquivo será corrompido. No entanto, provavelmente você ainda obterá os arquivos temporários. Dessa forma, você saberá que todos os arquivos com o nome desejado estão corretos.
- **SIP or VMS (SIP ou VMS)**  :
 - SIP: Selecione para fazer uma chamada SIP.
 - VMS: Selecione para fazer uma chamada VMS.

AXIS A9210 Network I/O Relay Module

A interface Web

- **From SIP account (Da conta SIP):** selecione na lista.
- **To SIP address (Para endereço SIP):** Insira o endereço SIP.
- **Test (Testar):** Clique para testar se suas configurações de chamada funcionam.
- **Email**
 - **Send email to (Enviar email para):** insira o endereço para enviar os emails. Para inserir vários emails, use vírgulas para separá-los.
 - **Send email from (Enviar email de):** insira o endereço de email do servidor de envio.
 - **Username (Nome de usuário):** insira o nome de usuário para o servidor de email. Deixe esse campo em branco se o servidor de email não precisar de autenticação.
 - **Password (Senha):** insira a senha para o servidor de email. Deixe esse campo em branco se o servidor de email não precisar de autenticação.
 - **Email server (SMTP) (Servidor de email (SMTP)):** Insira o nome do servidor SMTP. Por exemplo, smtp.gmail.com, smtp.mail.yahoo.com.
 - **Port (Porta):** insira o número da porta do servidor SMTP usando valores na faixa 0–65535. O valor padrão é 587.
 - **Encryption (Criptografia):** para usar criptografia, selecione SSL ou TLS.
 - **Validate server certificate (Validar certificado do servidor):** se você usar criptografia, marque para validar a identidade do dispositivo. O certificado pode ser autoassinado ou emitido por uma Autoridade de Certificação (CA).
 - **POP authentication (Autenticação POP):** Ative para inserir o nome do servidor POP. Por exemplo, pop.gmail.com.

Observação

Alguns provedores de email possuem filtros de segurança que impedem os usuários de receber ou exibir grandes quantidades de anexos, emails agendados e itens semelhantes. Verifique a política de segurança do provedor de email para evitar que sua conta de email seja bloqueada ou que as mensagens que você está esperando não sejam recebidas.

- **TCP**
 - **Host:** insira o endereço IP ou o nome de host do servidor. Se você inserir um nome de host, verifique se um servidor DNS está especificado em **System > Network > IPv4 and IPv6 (Sistema > Rede > IPv4 e IPv6)**.
 - **Port (Porta):** insira o número da porta usada para acessar o servidor.

Test (Testar): clique para testar a configuração.



O menu de contexto contém:

View recipient (Exibir destinatário): clique para exibir todos os detalhes do destinatário.

Copy recipient (Copiar destinatário): clique para copiar um destinatário. Ao copiar, você pode fazer alterações no novo destinatário.

Delete recipient (Excluir destinatário): clique para excluir o destinatário permanentemente.

Agendamentos

Agendamentos e pulsos podem ser usados como condições em regras. A lista mostra todos os agendamentos e pulsos configurados no momento no produto, juntamente com várias informações sobre suas configurações.



Add schedule (Adicionar agendamento): clique para criar um cronograma ou pulso.

Acionadores manuais

É possível usar o acionador manual para acionar manualmente uma regra. O acionador manual pode ser usado, por exemplo, para validar ações durante a instalação e a configuração do produto.

AXIS A9210 Network I/O Relay Module

A interface Web

MQTT

O MQTT (Message Queuing Telemetry Transport) é um protocolo de troca de mensagens padrão para a Internet das Coisas (IoT). Ele foi desenvolvido para integração simplificada com IoT e é usado em uma ampla variedade de setores para conectar dispositivos remotos com o mínimo de código e largura de banda de rede. O cliente MQTT no firmware do dispositivo Axis pode simplificar a integração de dados e eventos produzidos no dispositivo a sistemas que não são software de gerenciamento de vídeo (VMS).

Configure o dispositivo como um cliente MQTT. A comunicação MQTT baseia-se em duas entidades, os clientes e o broker. Os clientes podem enviar e receber mensagens. O broker é responsável por rotear mensagens entre os clientes.

Saiba mais sobre MQTT no *Portal do AXIS OS*.

ALPN

O ALPN é uma extensão do TLS/SSL que permite a seleção de um protocolo de aplicação durante a fase de handshake da conexão entre o cliente e o servidor. Isso é usado para permitir o tráfego MQTT na mesma porta que é utilizada para outros protocolos, como o HTTP. Em alguns casos, pode não haver uma porta dedicada aberta para a comunicação MQTT. Uma solução nesses casos é usar o ALPN para negociar o uso do MQTT como protocolo de aplicação em uma porta padrão permitida pelos firewalls.

MQTT client (Cliente MQTT)

Connect (Conectar): ative ou desative o cliente MQTT.

Status: Mostra o status atual do cliente MQTT.

Broker

Host: Insira o nome de host ou endereço IP do servidor MQTT.

Protocol (Protocolo): Selecione o protocolo que será usado.

Port (Porta): Insira o número da porta.

- 1883 é o valor padrão para MQTT sobre TCP
- 8883 é o valor padrão para MQTT sobre SSL
- 80 é o valor padrão para MQTT sobre WebSocket
- 443 é o valor padrão para MQTT sobre WebSocket Secure

Protocol ALPN: Insira o nome do protocolo ALPN fornecido pelo seu provedor de broker de MQTT. Isso se aplica apenas com MQTT sobre SSL e MQTT sobre o WebSocket Secure.

Username (Nome de usuário): Insira o nome de usuário que será usado pelo cliente para acessar o servidor.

Password (Senha): Insira uma senha para o nome de usuário.

Client ID (ID do cliente): Insira um ID de cliente. O identificador do cliente é enviado para o servidor quando o cliente se conecta a ele.

Clean session (Limpar sessão): Controla o comportamento na conexão e na desconexão. Quando selecionada, as informações de estado são descartadas na conexão e desconexão.

HTTP proxy (Proxy HTTP): Um URL com comprimento máximo de 255 bytes. Deixe o campo vazio se não quiser usar um proxy HTTP.

HTTPS proxy (Proxy HTTPS): Um URL com comprimento máximo de 255 bytes. Deixe o campo vazio se não quiser usar um proxy HTTPS.

Keep alive interval (Intervalo de Keep Alive): Permite que o cliente detecte quando o servidor não está mais disponível sem que seja necessário aguardar o longo tempo limite de TCP/IP.

Timeout (Tempo limite): O intervalo de tempo em segundos para permitir que uma conexão seja concluída. Valor padrão: 60

Device topic prefix (Prefixo do tópico do dispositivo): Usado nos valores padrão para o tópico na mensagem de conexão e na mensagem de LWT na guia MQTT client (Cliente MQTT) e nas condições de publicação na guia MQTT publication (Publicação MQTT).

AXIS A9210 Network I/O Relay Module

A interface Web

Reconnect automatically (Reconectar automaticamente): Especifica se o cliente deve se reconectar automaticamente após uma desconexão.

Connect message (Mensagem de conexão)

Especifica se uma mensagem deve ser enviada quando uma conexão é estabelecida.

Send message (Enviar mensagem): ative para enviar mensagens.

Use default (Usar padrão): desative para inserir sua própria mensagem padrão.

Topic (Tópico): insira o tópico para a mensagem padrão.

Payload (Carga): insira o conteúdo para a mensagem padrão.

Retain (Reeter): selecione para manter o estado do cliente neste **Topic (Tópico)**

QoS: altere a camada de QoS para o fluxo do pacote.

Last Will and Testament message (Mensagem de último desejo e testamento)

A opção Last Will Testament (LWT) permite que um cliente forneça uma prova juntamente com suas credenciais ao conectar ao broker. Se o cliente se desconectar abruptamente em algum momento mais tarde (talvez porque sua fonte de energia seja interrompida), ele pode permitir que o broker envie uma mensagem para outros clientes. Essa mensagem de LWT tem o mesmo formato que uma mensagem comum e é roteada através da mesma mecânica.

Send message (Enviar mensagem): ative para enviar mensagens.

Use default (Usar padrão): desative para inserir sua própria mensagem padrão.

Topic (Tópico): insira o tópico para a mensagem padrão.

Payload (Carga): insira o conteúdo para a mensagem padrão.

Retain (Reeter): selecione para manter o estado do cliente neste **Topic (Tópico)**

QoS: Altere a camada de QoS para o fluxo do pacote.

MQTT publication (Publicação MQTT)

Use default topic prefix (Usar prefixo de tópico padrão): selecione para usar o prefixo de tópico padrão, o qual é definido com o uso do prefixo de tópico de dispositivo na guia **MQTT client (Cliente MQTT)**.

Include topic name (Incluir nome do tópico): selecione para incluir o tópico que descreve a condição no tópico MQTT.

Include topic namespaces (Incluir namespaces de tópico): selecione para incluir espaços para nome de tópico ONVIF no tópico MQTT.

Include serial number (Incluir número de série): selecione para incluir o número de série do dispositivo na carga MQTT.



Add condition (Adicionar condição): clique para adicionar uma condição.

Retain (Reeter): define quais mensagens MQTT são enviadas como retidas.

- **None (Nenhuma):** envia todas as mensagens como não retidas.
- **Property (Propriedade):** envia somente mensagens stateful como retidas.
- **All (Todas):** envie mensagens stateful e stateless como retidas.

QoS: selecione o nível desejado para a publicação MQTT.

MQTT subscriptions (Assinaturas MQTT)

AXIS A9210 Network I/O Relay Module

A interface Web



Add subscription (Adicionar assinatura): clique para adicionar uma nova assinatura MQTT.

Subscription filter (Filtro de assinatura): insira o tópico MQTT no qual deseja se inscrever.

Use device topic prefix (Usar prefixo de tópico do dispositivo): adicione o filtro de assinatura como prefixo ao tópico MQTT.

Subscription type (Tipo de assinatura):

- **Stateless:** selecione para converter mensagens MQTT em mensagens stateless.
- **Stateful:** selecione para converter mensagens MQTT em condições. A carga é usada como estado.

QoS: selecione o nível desejado para a assinatura MQTT.

Logs

Relatórios e logs

Relatórios

- **View the device server report (Exibir o relatório do servidor de dispositivos):** Exiba informações sobre o status do produto em uma janela pop-up. O Log de acesso é incluído automaticamente no Relatório do servidor.
- **Download the device server report (Baixar o relatório do servidor de dispositivos):** Ele cria um arquivo .zip que contém um arquivo de texto do relatório completo do servidor no formato UTF-8, bem como um instantâneo da imagem da visualização ao vivo atual. Inclua sempre o arquivo .zip do relatório do servidor ao entrar em contato com o suporte.
- **Download the crash report (Baixar o relatório de falhas inesperadas):** Baixe um arquivo com informações detalhadas sobre o status do servidor. O relatório de panes contém informações que fazem parte do relatório do servidor, além de informações de depuração detalhadas. Esse relatório pode conter informações sensíveis, como rastreamentos de rede. A geração do relatório poderá demorar vários minutos.

Logs

- **View the system log (Exibir o log do sistema):** Clique para mostrar informações sobre eventos do sistema, como inicialização de dispositivos, avisos e mensagens críticas.
- **View the access log (Exibir o log de acesso):** clique para mostrar todas as tentativas de acessar o dispositivo que falharam, por exemplo, quando uma senha de login incorreta é usada.

Trace de rede

Importante

Um arquivo de rastreamento de rede pode conter informações confidenciais, por exemplo, certificados ou senhas.

Um arquivo de trace de rede pode ajudar a solucionar problemas gravando as atividades na rede.

Trace time (Tempo de trace): Selecione a duração do trace em segundos ou minutos e clique em **Download (Baixar)**.

Log do sistema remoto

O syslog é um padrão para o registro de mensagens. Ele permite a separação do software que gera mensagens, o sistema que as armazena e o software que as relata e analisa. Cada mensagem é rotulada com um código da instalação que indica o tipo de software que gerou a mensagem e recebe um nível de gravidade.

AXIS A9210 Network I/O Relay Module

A interface Web



Server (Servidor): Clique para adicionar um novo servidor.

Host: Insira o nome de host ou endereço IP do servidor.

Format (Formato): Selecione o formato de mensagem do syslog que será usado.

- Axis
- RFC 3164
- RFC 5424

Protocol (Protocolo): Selecione o protocolo que a ser usado:

- UDP (a porta padrão é 514)
- TCP (a porta padrão é 601)
- TLS (a porta padrão é 6514)

Port (Porta): Edite o número da porta para usar uma porta diferente.

Severity (Severidade): Selecione quais mensagens serão enviadas após o acionamento.

CA certificate set (Certificado CA definido): Consulte as configurações atuais ou adicione um certificado.

Configuração simples

A configuração simples destina-se a usuários avançados com experiência em configuração de dispositivos Axis. A maioria dos parâmetros podem ser definidos e editados nesta página.

Manutenção

Restart (Reiniciar): Reinicie o dispositivo. Isso não afeta nenhuma das configurações atuais. Os aplicativos em execução reiniciam automaticamente.

Restore (Restaurar): Devolve a *maioria* das configurações para os valores padrão de fábrica. Posteriormente, você deverá reconfigurar o dispositivo e os aplicativos, reinstalar quaisquer apps que não vieram pré-instalados e recriar quaisquer eventos e predefinições.

Importante

As únicas configurações que permanecem salvas após a restauração são:

- Protocolo de inicialização (DHCP ou estático)
- Endereço IP estático
- Roteador padrão
- Máscara de sub-rede
- Configurações de 802.1X
- Configurações de O3C

Factory default (Padrão de fábrica): Retorna *todas* as configurações para os valores padrão de fábrica. Em seguida, você deverá redefinir o endereço IP para tornar o dispositivo acessível.

Observação

Todo firmware de dispositivo Axis é digitalmente assinado para garantir que somente firmware verificado seja instalado em seu dispositivo. Esse procedimento aprimora ainda mais o nível de segurança cibernética mínimo dos dispositivos Axis. Para obter mais informações, consulte o white paper "Firmware assinado, inicialização segura e segurança de chaves privadas" em axis.com.

AXIS A9210 Network I/O Relay Module

A interface Web

Firmware upgrade (Atualização de firmware): Atualize para uma nova versão de firmware. As versões mais recentes podem conter funcionalidades aprimoradas, correções de falhas ou ainda recursos inteiramente novos. Recomendamos sempre utilizar a versão mais recente. Para baixar a versão mais recente, vá para axis.com/support.

Ao atualizar, é possível escolher entre três opções:

- **Standard upgrade (Atualização padrão):** Atualize para a nova versão do firmware.
- **Factory default (Padrão de fábrica):** Atualize e retorne todas as configurações para os valores padrão de fábrica. Ao escolher essa opção, você não poderá reverter para a versão anterior do firmware após a atualização.
- **Autorollback (Reversão automática):** Atualize e confirme a atualização dentro do período definido. Se você não confirmar, o dispositivo reverterá para a versão de firmware anterior.

Firmware rollback (Reversão de firmware): Reverta para a versão do firmware anteriormente instalada.

AXIS A9210 Network I/O Relay Module

Saiba mais

Saiba mais

Segurança cibernética

Axis Edge Vault

O AXIS Edge Vault oferece uma plataforma 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 foi desenvolvido sobre uma base sólida de módulos de computação criptografados (elemento seguro e TPM) e na segurança de SoC (TEE e inicialização segura), combinada com a experiência em segurança de dispositivos de borda.

Firmware assinado

O firmware assinado é implementado pelo fornecedor de software que assina a imagem de firmware com uma chave privada. Quando um firmware tem essa assinatura conectada a ele, um dispositivo valida o firmware antes de aceitar instalá-lo. Se o dispositivo detectar que a integridade do firmware está comprometida, a atualização do firmware 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 firmware assinado, a inicialização segura garante que um dispositivo possa ser inicializado somente com firmware autorizado.

Armazenamento de chaves seguro

Um ambiente protegido contra violações para proteção de chaves privadas e execução segura de operações de criptografia. Ele também impede o acesso não autorizado e a extração maliciosa em caso de violação de segurança. Dependendo dos requisitos de segurança, um dispositivo Axis pode possuir um ou vários módulos de computação criptográfica baseados em hardware que fornecem um armazenamento de chaves seguro protegido por hardware. Dependendo dos requisitos de segurança, um dispositivo Axis pode possuir um ou vários módulos de computação criptográfica baseados em hardware, como um TPM 2.0 (Trusted Platform Module) ou um elemento seguro e/ou TEE (Trusted Execution Environment), os quais proporcionam um armazenamento de chaves seguro protegido por hardware. Além disso, os produtos Axis selecionados apresentam um recurso de repositório de chaves seguro com certificação FIPS 140-2 Nível 2.

ID de dispositivo Axis

Poder verificar a origem do dispositivo é a chave para estabelecer a confiança na identidade do dispositivo. Durante a produção, os dispositivos com o AXIS Edge Vault são atribuídos a um certificado de ID de dispositivo Axis fornecido de fábrica compatível com IEEE 802.1AR. Ele funciona como um passaporte para provar a origem do dispositivo. O ID do dispositivo é armazenado de forma segura e permanente no armazenamento de chaves seguro como um certificado assinado pelo certificado raiz da 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.

Sistema de arquivos criptografados

Ao aplicar criptografia forte no sistema de arquivos, o armazenamento de chaves seguro impede a extração mal-intencionada de informações e impede a violação da configuração. Isso garante que nenhum dado armazenado no sistema de arquivos seja extraído ou violado quando o dispositivo não estiver sendo usado, acesso não autenticado ao dispositivo for obtido e/ou o dispositivo Axis for roubado. Durante o processo de inicialização segura, o sistema de arquivos de leitura/gravação é descriptografado e pode ser montado e usado pelo dispositivo Axis.

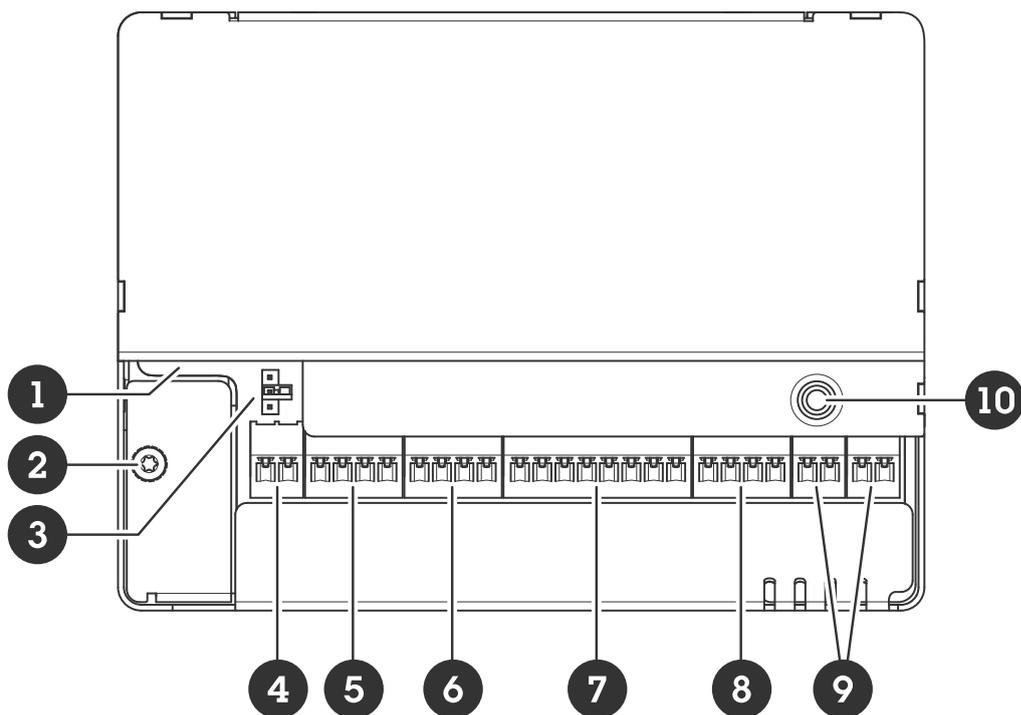
Para saber mais sobre o Axis Edge Vault e os recursos de segurança cibernética em dispositivos Axis, acesse axis.com/learning/white-papers e procure segurança cibernética.

AXIS A9210 Network I/O Relay Module

Especificações

Especificações

Visão geral do produto



- 1 Conector de rede
- 2 Posição de aterramento
- 3 Jumper do relé
- 4 Conector de alimentação
- 5 Conector do relé
- 6 Conector de entrada 1
- 7 RS485 e conector de E/S
- 8 Conector de E/S
- 9 Conector de entrada 2
- 10 Botão de controle

LEDs indicadores

LED	Cor	Indicação
Status	Verde	Aceso em verde para operação normal.
	Âmbar	Aceso durante a inicialização e na restauração de configurações.
	Vermelho	Pisca lentamente em caso de falha na atualização.

AXIS A9210 Network I/O Relay Module

Especificações

Rede	Verde	Aceso para conexão a uma rede de 100 Mbps. Pisca quando há atividade na rede.
	Âmbar	Aceso continuamente para uma conexão a uma rede de 10 Mbps. Pisca quando há atividade na rede.
	Apagado	Sem conexão de rede.
Alimentação elétrica	Verde	Funcionamento normal.
	Âmbar	Pisca em verde/âmbar durante a atualização do firmware.
Relé	Verde	Relé ativo. ¹
	Apagado	Relé inativo.

1. O relé está ativo quando COM está conectado a NO.

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 na página 33*.
- Conexão a um serviço de conexão em nuvem com um clique (O3C) via Internet. Para conectar, mantenha o botão pressionado por aproximadamente 3 segundos até o LED de status piscar em verde.

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 na página 27* e *Conector de alimentação na página 28*.

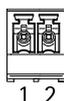
- Quando PoE e CC são ambos conectados antes do dispositivo ser alimentado, o PoE é usado como fonte de alimentação.
- PoE e CC estão conectados e PoE está alimentando. Quando o PoE é perdido, o dispositivo usa CC como fonte de alimentação sem precisar reiniciar.
- PoE e CC estão conectados e CC está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

AXIS A9210 Network I/O Relay Module

Especificações

Conector de alimentação

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.

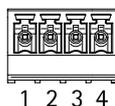


Função	Pino	Observações	Especificações
Terra CC (GND)	1		0 VCC
Entrada CC	2	Para alimentar o dispositivo sem o uso do Power over Ethernet. Observação: esse pino pode ser usado somente como entrada de energia.	12 VCC, máx., 36 W

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

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. Se usado com uma carga indutiva (por exemplo, uma trava), conecte um diodo em paralelo à carga para proporcionar proteção contra transientes de tensão.



Função	Pino	Observações	Especificações
Terra CC (GND)	1		0 VCC
NO	2	Normalmente aberto. Para conectar dispositivos de relé. Conecte uma trava fail-secure entre NO e terra CC. Os pinos do dois relé são separados galvanicamente do resto dos circuitos se os jumpers não são usados.	Corrente máxima = 2 A Tensão máxima = 30 VCC
COM	3	Comum	
NC	4	Normalmente fechado. Para conectar dispositivos de relé. Conecte uma trava fail-safe entre NC e terra CC. Os pinos do dois relé são separados galvanicamente do resto dos circuitos se os jumpers não são usados.	

Jumper de alimentação do relé

AXIS A9210 Network I/O Relay Module

Especificações

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

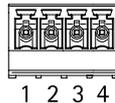
Ele pode ser usado para conectar uma trava entre os pinos GND e NO ou GND e NC.

Fonte de alimentação	Potência máxima em 12 VCC	Potência máxima em 24 VCC
ENTRADA CC	2.000 mA	1.000 mA
PoE	350 mA	150 mA
PoE+	1100 mA	500 mA

Conector de entrada 1

Um bloco de terminais com 4 pinos para entrada.

Ele oferece suporte à supervisão com resistores de fim de linha. Se a conexão for interrompida, um alarme será acionado. Para usar entradas supervisionadas, instale resistores terminadores. Use o diagrama de conexão para entradas supervisionadas. Consulte *Entradas supervisionadas na página 32*.



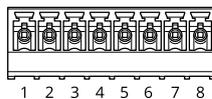
Função	Pino	Observações	Especificações
Terra CC	1, 3		0 VCC
Entrada	2, 4	Entrada digital ou entrada supervisionada – Conecte ao pino 1 ou 3 respectivamente para ativar ou deixe flutuante (desconectada) para desativar.	0 a 30 VCC máx.

Importante

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

RS485 e conector de E/S

Um bloco de terminais com 8 pinos, incluindo RS485 de 4 pinos e E/S de 4 pinos.



RS485

Função	Pino	Observação	Especificações
Terra CC (GND)	1		0 VCC
Saída CC (+12 V)	2	Fornecer energia para dispositivos auxiliares, por exemplo, sensores Modbus.	12 VCC, máx. 200 mA
A	3		
B	4		

E/S

AXIS A9210 Network I/O Relay Module

Especificações

Função	Pino	Observação	Especificações
Saída digital	5	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
Saída digital	6	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
Entrada	7	Entrada digital ou entrada supervisionada – Conecte ao pino 1 para ativar ou deixe flutuante (desconectada) para desativar.	0 a 30 VCC máx.
Saída digital	8	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

- O comprimento de cabo qualificado para RS485 será de até 1000 m (3281 ft) se os seguintes requisitos de cabo forem atendidos: 1 par trançado blindado, AWG 24, impedância de 120 ohm.
- O comprimento do cabo qualificado para E/S é de até 200 m (656 ft).

Conector de E/S

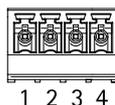
Use o conector auxiliar com dispositivos externos em combinação com, por exemplo, detecção de movimento, acionamento de eventos e notificações de alarmes. Além do ponto de referência de 0 VCC e alimentação (saída CC), o conector auxiliar fornece a interface para:

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 violações 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 Web do produto.

Bloco de terminais com 4 pinos

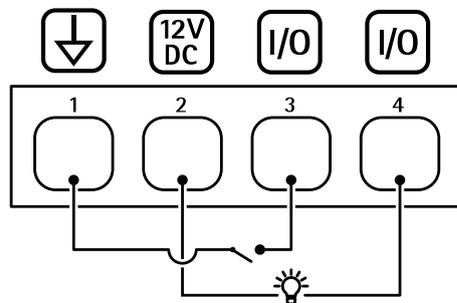


Função	Pino	Observações	Especificações
Terra CC	1		0 VCC
Saída CC	2	Pode ser usado para fornecer energia a equipamentos auxiliares. Observação: Este pino pode ser usado somente como saída de energia.	12 VCC Carga máxima = 50 mA no total

AXIS A9210 Network I/O Relay Module

Especificações

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/Ss 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 de entrada 2

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



AXIS A9210 Network I/O Relay Module

Especificações

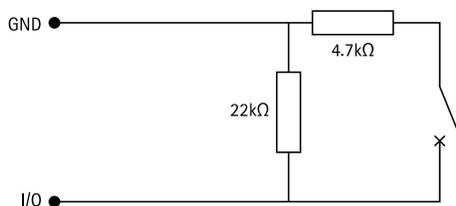
Função	Pino	Observações	Especificações
Terra CC	1		0 VCC
Entrada	2	Entrada digital ou entrada supervisionada – Conecte ao pino 1 para ativar ou deixe aberta (desconectada) para desativar.	0 a 30 VCC máx.

Entradas supervisionadas

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

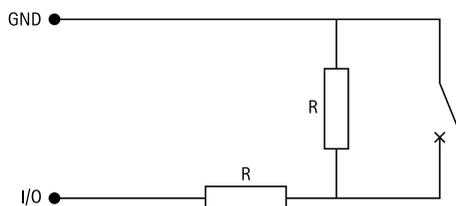
Conexão paralela primeiro

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



Serial first connection (Conexão serial primeiro)

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



Observação

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

Status	Descrição
Aberta	O switch supervisionado está no modo aberto.
Fechada	O switch supervisionado está no modo fechado.
Em curto	O cabo de E/S ou de entrada 1 a 5 está em curto-circuito com o terra.
Cortado	O cabo de E/S ou de entrada 1 a 5 foi cortado e deixado aberto sem um caminho de corrente para o terra.

AXIS A9210 Network I/O Relay Module

Solução de problemas

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 na página 26*.
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 LED indicador de status tornar-se verde. O produto foi então redefinido para as configurações padrão de fábrica. Se não houver um servidor DHCP disponível na rede, o endereço IP padrão será 192.168.0.90.
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 de firmware

A Axis oferece o gerenciamento de firmware dos produtos 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 firmware 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 firmware dos produtos Axis, acesse axis.com/support/device-software.

Verificar a versão atual do firmware

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

Para verificar o firmware atual:

1. Vá para a interface Web do dispositivo > **Status**.
2. Consulte a versão do firmware em **Device info (Informações do dispositivo)**.

AXIS A9210 Network I/O Relay Module

Solução de problemas

Atualização de firmware

Importante

- As configurações pré-configuradas e personalizadas são salvas quando você atualiza o firmware (desde que os recursos estejam disponíveis no novo firmware), embora isso não seja garantido pela Axis Communications AB.
- Certifique-se de que o dispositivo permaneça conectado à fonte de alimentação ao longo de todo o processo de atualização.

Observação

Quando você atualizar o dispositivo com o firmware mais recente no rack ativo, o produto receberá a última funcionalidade disponível. Sempre leia as instruções de atualização e notas de versão disponíveis com cada nova versão antes de atualizar o firmware. Para encontrar o firmware e as notas de versão mais recentes, vá para axis.com/support/device-software.

1. Baixe o arquivo de firmware 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 > Firmware upgrade (Manutenção > Atualização de firmware)** 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 após a atualização do firmware	Se você tiver problemas após uma atualização de firmware, reverta para a versão instalada anteriormente na página Manutenção .

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): <ul style="list-style-type: none">• Se você receber: <code>Reply from <endereço IP>: bytes=32; time=10...</code>, 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.• Se você receber: <code>Request timed out</code>, isso 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.

AXIS A9210 Network I/O Relay Module

Solução de problemas

O dispositivo não pode ser acessado por um navegador

Não é possível fazer login	Quando o HTTPS está 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 da conta root for perdida, o dispositivo deverá ser restaurado para as configurações padrão de fábrica. Consulte <i>Redefinição para as configurações padrão de fábrica na página 33</i> .
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, um endereço IP estático poderá ser atribuído manualmente. 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 dispositivo está acessível local, mas não externamente

Para acessar o dispositivo externamente, recomendamos que você use 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.

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

O firewall bloqueia o tráfego usando a porta 8883, pois é considerada insegura.	Em alguns casos, o servidor/broker pode não fornecer uma porta específica para a comunicação MQTT. Ainda é possível usar MQTT em uma porta normalmente usada para tráfego HTTP/HTTPS. <ul style="list-style-type: none">• 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/broker suportar ALPN, o uso do MQTT pode ser negociado em uma porta aberta, como a 443. Verifique com o seu provedor de servidor/broker se o ALPN é suportado e qual protocolo e porta do ALPN devem ser usados.
---	---

Entre em contato com o suporte

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

