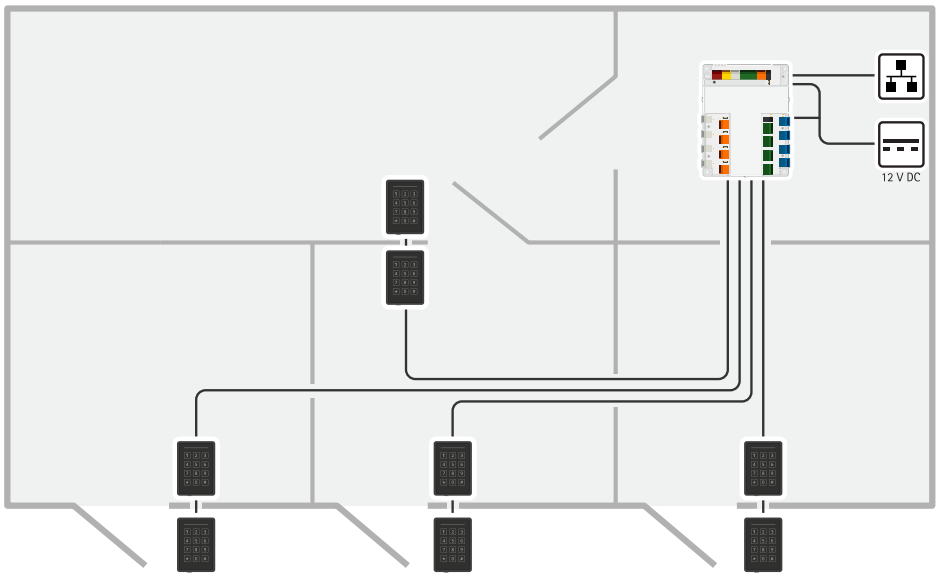
AXIS A1710-B Network Door Controller

Manual do Usuário

Índice

Visão geral da solução

Visão geral da solução



O controlador de porta de rede pode ser facilmente conectado à sua rede IP existente. Cada controlador de portas em rede pode alimentar e controlar até 8 leitores.

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

Para usar a interface Web do AXIS OS com o iOS 15 ou iPadOS 15, acesse* ***Configurações > 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 4*.

Para obter descrições de todos os controles e opções presentes na interface Web do dispositivo, consulte *A interface Web na página 7*.

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 4*.
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 32*.

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 software do dispositivo não foi manipulado

Para certificar-se de que o dispositivo tenha o AXIS OS original ou para assumir o controle total do dispositivo após um ataque de segurança:

1. Restauração das configurações padrão de fábrica. Consulte *Redefinição para as configurações padrão de fábrica na página 32*.

   Após a redefinição, uma inicialização segura garantirá o estado do dispositivo.

2. Configure e instale o dispositivo.

Visão geral da interface Web

Este vídeo oferece uma visão geral sobre a interface Web do dispositivo.

Interface Web de um dispositivo Axis

Configure seu dispositivo

Configure seu dispositivo

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

Observação

O AXIS Door Controller Extension ACAP vem pré-instalado no sistema. É necessária uma licença para usá-lo.

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.
- **Alterar conta**: Saia da conta atual e faça login em uma nova conta.
- **Desconectar**: Faça logout da conta atual.

O menu de contexto contém:

- **Analytics data (Dados de analíticos)**: 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)**: veja informações do dispositivo, incluindo versão e número de série do AXIS OS.

Status

Conexão da porta

Porta: Mostra o status das portas conectadas.

Informações do dispositivo

Mostra as informações do dispositivo, incluindo versão e o número de série do AXIS OS.

Upgrade AXIS OS (Atualizar o AXIS OS): atualize o software em seu dispositivo. Abre a página Maintenance (Manutenção), na qual é possível atualizar.

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 **Time and location (Hora e local)** na qual é possível alterar as configurações de NTP.

Segurança

Mostra os tipos de acesso ao dispositivo que estão ativos, quais protocolos de criptografia estão em uso e se aplicativos não assinados são permitidos. 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.

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 o endereço IP, o protocolo, a porta e o PID/Processo de cada conexão.

Dispositivo

Alarmes

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

- **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)**.

Periféricos

Leitores

Adicionar leitor: Clique para adicionar um novo leitor.**Nome**: Insira um nome para o leitor.**Leitor**: Selecione um leitor na lista suspensa.**Endereço IP**: Insira o endereço IP do leitor manualmente.**Username (Nome de usuário)**: Insira o nome de usuário do leitor.**Senha**: Insira a senha do leitor.**Ignore server certificate verification (Ignorar verificação do certificado do servidor)**: Ative para ignorar a verificação.

Fechaduras sem fio

É necessário ter uma licença para usar esse recurso.

Conectar o hub de comunicação: Clique para conectar as fechaduras sem fio.

Atualizar leitores

Upgrade readers (Atualizar leitores): clique para atualizar os leitores para uma nova versão do AXIS OS. O recurso só pode atualizar leitores compatíveis quando eles estão online.

Apps

Adicionar app: 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.**Permitir apps não assinados** : Ative para permitir a instalação de aplicativos não assinados.**Permitir apps com privilégios 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. 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.
- **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.
  - **Max NTP poll time (Tempo máximo da pesquisa NTP)**: selecione o tempo máximo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
  - **Min NTP poll time (Tempo mínimo da pesquisa NTP)**: selecione o tempo mínimo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
- **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.
  - **Max NTP poll time (Tempo máximo da pesquisa NTP)**: selecione o tempo máximo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
  - **Min NTP poll time (Tempo mínimo da pesquisa NTP)**: selecione o tempo mínimo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
- **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.
  - **Max NTP poll time (Tempo máximo da pesquisa NTP)**: selecione o tempo máximo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
  - **Min NTP poll time (Tempo mínimo da pesquisa NTP)**: selecione o tempo mínimo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
- **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.

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

- **DHCP**: Adota o fuso horário do servidor DHCP. O dispositivo deve estar conectado a um servidor DHCP para que você possa selecionar esta opção.
- **Manual**: Selecione um fuso horário na lista suspensa.

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.

- **Latitude**: Valores positivos estão ao norte do equador.
- **Longitude**: Valores positivos estão a leste do meridiano de Greenwich.
- **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.**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.**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.

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.**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 -.**Ative as atualizações de DNS dinâmicas**: Permita que o dispositivo faça a atualização automática dos registros do servidor de nomes de domínio sempre que o endereço IP for alterado.**Registrar o nome do DNS**: Digite um nome de domínio exclusivo que aponte para o endereço IP de seu dispositivo. Os caracteres permitidos são A – Z, a – z, 0 – 9 e -.**TTL**: O tempo de vida (TTL) define por quanto tempo um registro DNS permanecerá válido até que precise ser atualizado.

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 e HTTPS

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 de criptografia 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.**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.**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.**LLDP e CDP**: Ative para permitir a descoberta automática na rede. Desligar as configurações LLDP e o CDP pode afetar a negociação de energia PoE. Para resolver quaisquer problemas com a negociação de energia PoE, configure a chave PoE somente para negociação de energia PoE de hardware.

Proxies globais

Http proxy (Proxy Http): Especifique um host proxy global ou um endereço IP de acordo com o formato permitido.**Https proxy (Proxy Https)**: Especifique um host proxy global ou um endereço IP de acordo com o formato permitido.
Formatos permitidos para proxies http e https:

- **http(s)://host:port**
- **http(s)://user@host:port**
- **http(s)://user:pass@host:port**

Observação

Reinicie o dispositivo para aplicar as configurações de proxy global.

No proxy (Nenhum proxy): use **No proxy (Nenhum proxy)** para ignorar os proxies globais. Digite uma das opções da lista ou várias opções separadas por vírgula:

- Deixar vazio
- Especificar um endereço IP
- Especificar um endereço IP no formato CIDR
- Especifique um nome de domínio, por exemplo: **www.<nome de domínio>.com**
- Especifique todos os subdomínios em um domínio específico, por exemplo, **.<nome de domínio>.com**

Conexão com a nuvem com apenas 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):

- **Um clique**: Esta 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.
- **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.**Porta**: Insira o número da porta usada para acesso.**Login** e **Senha**: Se necessário, insira um nome de usuário e uma senha para o servidor proxy.**Authentication method (Método de autenticação)**:

- **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 **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**.
  - **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 **gravação**.
  - **Activate traps (Ativar interceptações)**: Ative para ativar o relatório de interceptações. O dispositivo usa interceptações para enviar mensagens sobre eventos importantes ou alterações de status para um sistema de gerenciamento. Na interface Web, você pode configurar interceptações para SNMP v1 e v2c. As interceptações serão desativadas automaticamente se você mudar para SNMP v3 ou desativar o SNMP. Se você usa SNMP v3, é possível configurar interceptações via aplicativo de gerenciamento do SNMP v3.
  - **Trap address (Endereço da interceptação)**: Insira o endereço IP ou nome de host do servidor de gerenciamento.
  - **Trap community (Comunidade de interceptação)**: Insira a comunidade que é usada quando o dispositivo envia uma mensagem de interceptação para o sistema de gerenciamento.
  - **Traps (Interceptações)**:
  - **Cold start (Partida a frio)**: Envia uma mensagem de interceptação quando o dispositivo é iniciado.
  - **Partida a quente**: Envia uma mensagem de interceptação quando uma configuração de SNMP é alterada.
  - **Link up (Link ativo)**: Envia uma mensagem de interceptação quando um link muda de inativo para ativo.
  - **Falha de autenticação**: Envia uma mensagem de interceptação quando uma tentativa de autenticação falha.

Observação

Todas as interceptações MIB de vídeo Axis são habilitados quando você ativa as interceptações 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 interceptações SNMP v1 e v2c não criptografadas. Se você usa SNMP v3, é possível configurar interceptações 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

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 de CA pré-instalados serão reinstalados.

Adicionar certificado : Clique para adicionar um certificado.

- **Mais** : Mostrar 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.

Controle de acesso à rede e criptografia

IEEE 802.1xO 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).**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.**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.**Authentication method (Método de autenticação)**: Selecione um tipo de EAP usado para autenticação.**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 certificates (Certificados 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.Essas configurações só estarão disponíveis se você usar **IEEE 802.1x PEAP-MSCHAPv2** como método de autenticação:

- **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.

Essas configurações só estarão disponíveis se você usar o **IEEE 802.1ae MACsec (CAK estático/chave pré-compartilhada)** como método de autenticação:

- **Nome da chave de associação de conectividade do acordo de chaves**: Insira o nome da associação de conectividade (CKN). Deve ter de 2 a 64 (divisível por 2) caracteres hexadecimais. O CKN deve ser configurado manualmente na associação de conectividade e deve corresponder em ambas as extremidades do link para ativar inicialmente o MACsec.
- **Chave de associação de conectividade do acordo de chaves**: Insira a chave da associação de conectividade (CAK). Ela deve ter 32 ou 64 caracteres hexadecimais. O CAK deve ser configurado manualmente na associação de conectividade e deve corresponder em ambas as extremidades do link para ativar inicialmente o MACsec.

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.

Firewall

Activate (Ativar): Ative o firewall.
Default Policy (Política padrão): Selecione o estado padrão do firewall.

- **Permitir:** Permite todas as conexões ao dispositivo. Essa opção é definida por padrão.
- **Deny (Negar):** Nega todas as conexões ao dispositivo.

Para fazer exceções à política padrão, você pode criar regras que permitem ou negam conexões ao dispositivo a partir de endereços, protocolos e portas específicos.

- **Endereço**: Insira um endereço no formato IPv4/IPv6 ou CIDR ao qual deseja permitir ou negar o acesso.
- **Protocol (Protocolo)**: Selecione um protocolo ao qual deseja permitir ou negar acesso.
- **Porta**: Insira um número de porta ao qual deseja permitir ou negar o acesso. Você pode adicionar um número de porta entre 1 e 65535.
- **Policy (Política)**: Selecione a política da regra.

 : Clique para criar outra regra.
Adicionar regras: Clique para adicionar as regras que você definiu.

- **Time in seconds (Tempo em segundos):** Defina um limite de tempo para testar as regras. O limite de tempo padrão está definido como **300** segundos. Para ativar as regras imediatamente, defina o tempo como **0** segundo.
- **Confirm rules (Confirmar regras):** Confirme as regras e o limite de tempo. Se você definiu um limite de tempo superior a 1 segundo, as regras permanecerão ativas nesse período. Se tiver definido o tempo para **0**, as regras estarão ativas imediatamente.

Pending rules (Regras pendentes): Uma visão geral das regras testadas mais recentes que você ainda não confirmou.
Observação

As regras com limite de tempo são exibidas em **Active rules (Regras ativas)** até que o temporizador exibido acabe ou até serem confirmados. Se elas não forem confirmadas, elas serão exibidas em **Pending rules (Regras pendentes)** assim que o temporizador chegar em zero e o firewall será revertido às configurações definidas anteriormente. Se você as confirmar, elas substituirão as regras ativas atuais.

Confirm rules (Confirmar regras): Clique para ativar as regras pendentes.**Active rules (Regras ativas)**: Uma visão geral das regras que você está executando no dispositivo.  : Clique para excluir uma regra ativa.  : Clique para excluir todas as regras, pendentes e ativas.

Certificado do AXIS OS com assinatura personalizada

Para instalar o software de teste ou outro software personalizado da Axis no dispositivo, certificado do AXIS OS com assinatura personalizada é necessário. O certificado verifica se o software é aprovado pelo proprietário do dispositivo e pela Axis. O software só pode ser executado em um dispositivo específico identificado por seu número de série e ID de chip exclusivos. Somente a Axis pode criar certificados do AXIS OS 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 software. O menu de contexto contém:

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

Contas

Contas

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)**.
- **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.

Contas SSH

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.**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.

Virtual host (Host virtual)

Add virtual host (Adicionar host virtual): clique para adicionar um novo host virtual.**Enabled (Ativado)**: selecione para usar este host virtual.**Server name (Nome do servidor)**: insira o nome do servidor. Use somente números 0 – 9, letras A – Z e hífen (-).**Porta**: insira a porta à qual o servidor está conectado.**Tipo**: selecione o tipo de autenticação que será usada. Selecione entre **Basic**, **Digest** e **Open ID**. O menu de contexto contém:

- **Update (Atualizar)**: atualizar o host virtual.
- **Excluir**: excluir o host virtual.

Disabled (Desativado): o servidor está desativado.

Configuração de OpenID

Importante

Se você não puder usar OpenID para fazer login, use as credenciais Digest ou Básicas que você usou quando configurou OpenID para fazer login.

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.**Remote user (Usuário remoto)**: insira um valor para identificar usuários remotos. Isso ajudará a exibir o usuário atual na interface Web do dispositivo.**Scopes (Escopos)**: Escopos opcionais que poderiam fazer parte do token.**Segredo do cliente**: Insira a senha OpenID novamente **Save (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.

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 a 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 software 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.

Cliente MQTT

Connect (Conectar): Ative ou desative o cliente MQTT.**Status**: Mostra o status atual do cliente MQTT.**BrokerHost**: Insira o nome de host ou endereço IP do servidor MQTT.**Protocol (Protocolo)**: Selecione o protocolo que será usado.**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.**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)**.**Reconnect automatically (Reconectar automaticamente)**: Especifica se o cliente deve se reconectar automaticamente após uma desconexão.**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 (Reter)**: selecione para manter o estado do cliente neste **Topic (Tópico)QoS**: Altere a camada de QoS para o fluxo do pacote.**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 (Reter)**: selecione para manter o estado do cliente neste **Topic (Tópico)QoS**: Altere a camada de QoS para o fluxo do pacote.

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. **Adicionar condição**: clique para adicionar uma condição.**Retain (Reter)**: 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.

Assinaturas MQTT

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.

Acessórios

Portas de E/S

Use a entrada digital para conectar dispositivos externos que podem alternar entre um circuito aberto ou fechado, por exemplo, sensores PIR, contatos de portas ou janelas e detectores de quebra de vidros.

Use a saída digital para conectar dispositivos externos, como relés e LEDs. Você pode ativar dispositivos conectados via interface de programação de aplicativos VAPIX® ou na interface Web.

Detecção automáticaNome: Edite o texto para renomear a porta.**Direção**: indica que a porta é uma porta de entrada. indica que é uma porta de saída. Se a porta for configurável, você poderá clicar nos ícones para alternar entre entrada e saída.**Normal state (Estado normal)**: Clique em para circuito aberto e para circuito fechado.**Current state (Estado atual)**: Mostra o estado atual da porta. A entrada ou saída é ativada quando o estado atual é diferente do estado normal. Uma entrada no dispositivo tem um circuito aberto quando desconectada ou quando há uma tensão acima de 1 VCC.

Observação

Durante a reinicialização, o circuito de saída é aberto. Quando a reinicialização é concluída, o circuito retorna para a posição normal. Se você alterar qualquer configuração nesta página, os circuitos de saída voltarão para suas posições normais, independentemente de quaisquer acionadores ativos.

Supervisionado : Ative para possibilitar a detecção e o acionamento de ações se alguém manipular 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 manipulou (ou seja, cortada ou em curto). Supervisionar a conexão requer hardware adicional (resistores de fim de linha) no loop de E/S externo.

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.

Rastreamento 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)**.

Acesse o sistema remotamente

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.

Servidor: Clique para adicionar um novo servidor.**Host**: Insira o nome de host ou endereço IP do servidor.**Format (Formatar)**: 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)

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.

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 802.1X
- Configurações de O3C
- Endereço IP do servidor DNS

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 software de dispositivo Axis é digitalmente assinado para garantir que somente software 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 "Axis Edge Vault" em *axis.com*.

Atualização do AXIS OS: atualize para uma nova versão do AXIS OS. As novas versões podem conter funcionalidades aprimoradas, correções de falhas ou ainda recursos inteiramente novos. Recomendamos sempre utilizar a versão mais recente do AXIS OS. 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 AXIS OS.
- **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 AXIS OS 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 anterior do AXIS OS.

AXIS OS rollback (Reversão do AXIS OS): reverta para a versão anteriormente instalada do AXIS OS.

Saiba mais

Cibersegurança

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

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

Serviço de notificação de segurança Axis

A Axis fornece um serviço de notificação com informações sobre vulnerabilidades e outras questões relacionadas à segurança para os dispositivos Axis. Para receber notificações, inscreva-se em *axis.com/security-notification-service*.

Gerenciamento de vulnerabilidades

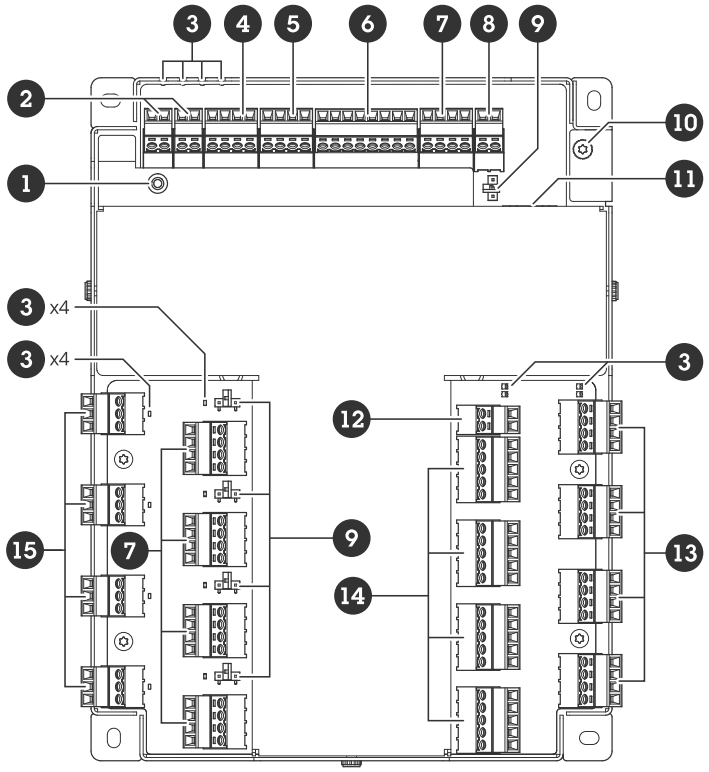
Para minimizar o risco de exposição dos clientes, a Axis, na condição de **Autoridade de Numeração (CNA) de Vulnerabilidades e Exposições Comuns (CVE)**, segue os padrões do setor para gerenciar e responder a vulnerabilidades descobertas em nossos dispositivos, software e serviços. Para obter mais informações sobre a política de gerenciamento de vulnerabilidades da Axis, como relatar vulnerabilidades, vulnerabilidades já conhecidas e as respectivas orientações de segurança, consulte *axis.com/vulnerability-management*.

Operação segura de dispositivos Axis

Os dispositivos Axis com configurações padrão de fábrica são pré-configurados com mecanismos de proteção padrão seguros. Recomendamos usar mais configuração de segurança ao instalar o dispositivo. Para saber mais sobre os guias de fortalecimento da Axis e outras documentações relacionadas a segurança cibernética, acesse *axis.com/support/cybersecurity/resources*.

Especificações

Visão geral do produto



1 *Botão de controle*
2 *Manipulação/alarme*
3 *LEDs*
4 *Conector auxiliar*
5 *Conector de saída*
6 *Conector de entrada*
7 *Conector do relé*
8 *Conector de alimentação (DC IN)*
9 *Jumper do relé*
10 *Posição de aterramento*
11 *Conector de rede*
12 *Conector de alimentação (PORTAS 1-4 DE ENTRADA CC)*
13 *Conector do leitor*
14 *Conector de porta*
15 *Conector do relé AUX*

Indicadores de LED

LED	Cor	Indicação
Status (ESTATÍSTICA)	Verde	Aceso em verde para operação normal.
	Âmbar	Aceso durante a inicialização e na restauração de configurações.
	Vermelho	Pisca lentamente para falha na atualização.
Rede (NET)	Verde	Aceso para conexão a uma rede de 100 Mbps. Pisca para atividade de rede.
	Âmbar	Aceso continuamente para uma conexão a uma rede de 10 Mbps. Pisca para atividade de rede.
	Apagado	Sem conexão de rede.
Alimentação (PWR)	Verde	Funcionamento normal.
	Âmbar	Pisca em verde/âmbar durante a atualização do firmware.
Relé (RELÉ)	Verde	Relé ativo. (*)
	Apagado	Relé inativo.

LEDPORTAS 1–4	Cor	Indicação
Status (ESTATÍSTICA)	Verde	Pisca (aceso por 1 segundo, apagado por 1 segundo) quando offline.
	Verde	Pisca (ligado por 200 milissegundos, desligado por 2 segundos) quando on-line.
	Vermelho	Pisca em verde/vermelho durante a atualização do software do dispositivo.
Alimentação (PWR)	Verde	Funcionamento normal.
Excesso de corrente em RS485 (LEITOR OC)	Vermelho	Falha de excesso de corrente ou subtensão em qualquer porta RS485.
Excesso de corrente no relé (RELÉ OC)	Vermelho	Falha de excesso de corrente ou subtensão em qualquer porta de relé.
Relé (RELÉ)	Verde	Relé ativo. (*)
	Apagado	Relé inativo.
Relé AUX (RELÉ)	Verde	Relé ativo. (*)
	Apagado	Relé inativo.

(*) 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 32*.

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 30 W Midspan.

Opções de alimentação

Para alimentar o dispositivo, você precisa conectar os seguintes conectores:

1. PoE ou ENTRADA CC. Consulte *Prioridade da alimentação na página 24*.
2. PORTAS 1-4 DE ENTRADA CC

Prioridade da alimentação

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

Conector de energia

Dois blocos de terminais com 2 pinos para entrada de energia CC. Consulte *Opções de alimentação na página 24*.

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.

ENTRADA CC

Opcional para alimentar o dispositivo. Em vez disso, você pode usar PoE. Consulte *Prioridade da alimentação na página 24*.

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

PORTAS 1-4 DE ENTRADA CC

Obrigatório para alimentar o dispositivo.

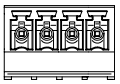
Função	Pino	Observações	Especificações
Terra CC (GND)	1		0 VCC
Entrada CC	2	Obrigatório para alimentar o dispositivo. Observação: esse pino pode ser usado somente como entrada de energia.	12 VCC, máx., 100 W

UL: alimentação CC a ser fornecida por uma fonte de alimentação UL 294, UL 603 ou UL 2610 relacionada, dependendo do aplicativo, com as classificações apropriadas.

Conector do leitor

Quatro blocos de terminais de 4 pinos compatíveis com o protocolo OSDP para comunicação com o leitor.

Ele pode conectar até oito leitores OSDP ou WIegand com acessório (AXIS TA1101-B Wiegand a OSDP Converter em multidrop). 2 A a 12 V CC são reservados para leitores conectados às PORTAS 1-4.



Configurado para um leitor OSDP

Função	Pino	Observação	Especificações
Terra CC (GND)	1		0 VCC
Saída CC (+12 V)	2	Fornece energia para o leitor.	12 V CC, total combinado de 2 A para todos os conectores do leitor.
A	3	Half duplex	
B	4	Half duplex	

Configurado para dois leitores OSDP (multidrop)

Função	Pino	Observação	Especificações
Terra CC (GND)	1		0 VCC
Saída CC (+12 V)	2	Fornece energia para ambos os leitores.	12 V CC, total combinado de 2 A para todos os conectores do leitor.
A	3	Half duplex	
B	4	Half duplex	

Especificações

Importante

- Quando o leitor é alimentado pelo controlador, o comprimento do cabo qualificado é de até 200 m (656 pés) se o seguinte requisito de cabo for atendido: AWG 22-14. Verificado somente para leitores Axis.
- Quando o leitor não é alimentado pelo controlador, o comprimento do cabo qualificado de dados do leitor é de até 1000 m (3.280,8 pés) se os seguintes requisitos de cabo forem atendidos: 1 par trançado, AWG 26-14. Verificado somente para leitores Axis.

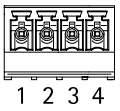
Conector de entrada

Um bloco de terminais com 8 pinos

Função	Pino	Observação	Especificações
Terra CC (GND)	1, 3, 5, 7		0 VCC
Entrada	2, 4, 6	Entrada digital – Conecte ao pino 1 para ativar ou deixe aberta (desconectada) para desativar. Possibilidade de supervisão. Consulte *Entradas supervisionadas na página 31*.	0–30 V CC
+12 VCC	8		Máx. 190 mA

Conector de saída

Um bloco de terminais com 4 pinos

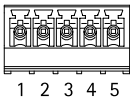


Função	Pino	Especificações
Terra CC (GND)	1	0 VCC
Saída	2,3,4	Dreno aberto, 0 a máx. 0–30 V CC, máx. 100 mA

Conector de porta

Quatro blocos de terminais com 5 pinos para monitoramento de dispositivos de portas (entrada digital).

O monitor de porta oferece suporte à supervisão com resistores terminadores. Se a conexão for interrompida, um alarme será acionado. Para usar entradas supervisionadas, instale resistores terminadores. Use o diagrama de conexão para entradas supervisionadas. Consulte *página 31*.



Especificações

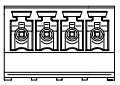
Função	Pino	Observações	Especificações
Terra CC (GND)	1, 3		0 VCC
Entrada	2, 4	Para comunicação com o monitor da porta. Entrada digital ou Entrada supervisionada – Conecte ao pino 1 ou 3 respectivamente para ativar ou deixe flutuante (desconectada) para desativar.	0 a 30 VCC máx.
+12 VCC	5	Fornece energia a dispositivos, tais como sensores de porta.	Total combinado de 400 mA para todos os conectores da porta

Importante

O comprimento de cabo qualificado é de até 200 m (656 pés) quando o seguinte requisito de cabo é atendido: 24–14 AWG.

Conector do relé

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



Função	Pino	Observações	Especificações
Terra CC (GND)	1		0 VCC
NO	2	normalmente aberto. Para conectar dispositivos de relé. Conecte uma trava de segurança contra falhas entre o terra NO e o terra CC. O relé é galvanicamente separado do resto do circuito se os jumpers não forem usados.	Corrente máxima = 2 A Tensão máxima = 30 V CC
COM	3	Comum	
NC	4	normalmente fechado. Para conectar dispositivos de relé. Conecte uma trava fail-safe entre o terra NC e o terra CC. O relé é galvanicamente separado do resto do circuito se os jumpers não forem usados.	

Jumper de alimentação do relé

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

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

Fonte de alimentação	Potência máxima em 12 VCC	Potência máxima em 24 VCC
ENTRADA CC	1 900 mA	1000 mA

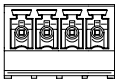
PoE	150 mA	50 mA
PoE+	920 mA	420 mA

OBSERVAÇÃO

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

Conector do relé da porta

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



Função	Pino	Observações	Especificações
Terra CC (GND)	1		0 VCC
NO	2	normalmente aberto. Para conectar dispositivos de relé. Conecte uma trava de segurança contra falhas entre o terra NO e o terra CC. O relé é galvanicamente separado do resto do circuito se os jumpers não forem usados.	Corrente máxima = 4 A Tensão máxima = 30 V CC
COM	3	Comum	
NC	4	normalmente fechado. Para conectar dispositivos de relé. Conecte uma trava fail-safe entre o terra NC e o terra CC. O relé é galvanicamente separado do resto do circuito se os jumpers não forem usados.	

Jumper de alimentação do relé

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

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

Fonte de alimentação	Potência máxima em 12 VCC	Potência máxima em 24 VCC
COM Total combinado de 46 W para todos os conectores do relé da porta	Total combinado de 3,8 W para todos os conectores do relé da porta	Total combinado de 1,5 W para todos os conectores do relé da porta

OBSERVAÇÃO

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

Especificações

Conector do relé AUX

Quatro blocos de terminais com 3 pinos para relés C que podem ser usados, por exemplo, para controlar uma trava ou uma interface para um portão.

Função	Pino	Observações	Especificações
NO	1	normalmente aberto. Para conectar dispositivos de relé. Conecte uma trava de segurança contra falhas entre o terra NO e o terra CC. O relé é galvanicamente separado do resto do circuito se os jumpers não forem usados.	Corrente máxima = 2 A Tensão máxima = 30 V CC
COM	2	Comum	
NC	3	normalmente fechado. Para conectar dispositivos de relé. Conecte uma trava fail-safe entre o terra NC e o terra CC. O relé é galvanicamente separado do resto do circuito se os jumpers não forem usados.	

OBSERVAÇÃO

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

Conector auxiliar

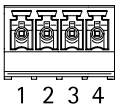
Use o conector auxiliar com dispositivos externos em combinação com, por exemplo, detecção de movimento, acionamento de eventos e notificações de alarmes. Além do ponto de referência de 0 VCC e alimentação (saída CC), o conector auxiliar fornece a interface para:

Entrada digital – Para conectar dispositivos que podem alternar entre um circuito aberto ou fechado, por exemplo, sensores PIR, contatos de portas/janelas e detectores de quebra de vidros.

Entrada supervisionada – Permite detectar manipulações em entradas digitais.

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

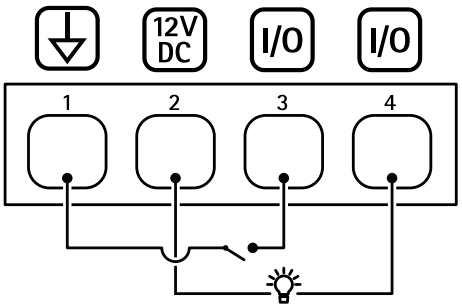
Bloco de terminais com 4 pinos



Função	Pino	Observações	Especificações
Terra CC	1		0 VCC

Especificações

Saída CC	2	Pode ser usada para alimentar equipamentos auxiliares. Observação: esse pino pode ser usado somente como saída de energia.	12 V CC Carga máxima = 250 mA no total
Configurável (entrada ou saída)	3–4	Entrada digital ou entrada supervisionada – Conecte ao pino 1 para ativar ou deixe aberta (desconectada) para desativar. Para usar a entrada supervisionada, instale resistores de terminação. Veja o diagrama de conexão para obter informações de como conectar os resistores.	0 a 30 VCC máx.
		Saída digital – Conectado internamente ao pino 1 (terra CC) quando ativo, flutuante (desconectado) quando inativo. Se for usado com uma carga indutiva, por exemplo, um relé, conecte um diodo em paralelo com a carga para proteger contra transientes de tensão. As E/Ss são capazes de acionar uma carga externa de 12 VCC, 50 mA (máximo combinado), se a saída interna de 12 VCC (pino 2) for usada. No caso do uso de conexões de dreno abertas em conjunto com uma fonte de alimentação externa, as E/S podem gerenciar uma alimentação CC de 0 a 30 VCC, 100 mA cada.	0 a 30 VCC máx., dreno aberto, 100 mA

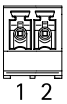


1 *Terra CC*
2 *Saída CC 12 V*
3 *E/S configurada como entrada*
4 *E/S configurada como saída*

Conector de alarme/manipulação

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
VIOLAÇÃO	2	Entrada digital – Conecte ao pino 1 para ativar ou deixe aberta (desconectada) para desativar. Possibilidade de supervisão. Consulte *Entradas supervisionadas na página 31*.	0 a 30 VCC máx.

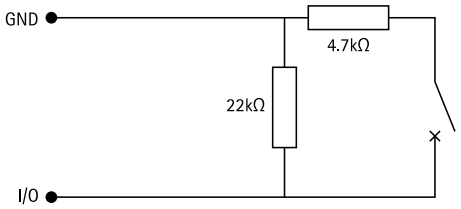
Função	Pino	Observações	Especificações
Terra CC	1		0 VCC
ALARME	2	Entrada digital – Conecte ao pino 1 para ativar ou deixe aberta (desconectada) para desativar. Possibilidade de supervisão. Consulte *Entradas supervisionadas na página 31*.	0 a 30 VCC máx.

Entradas supervisionadas

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

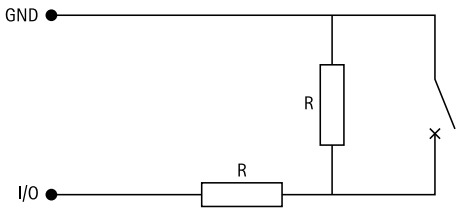
Conexão paralela primeiro

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



Conexão serial primeiro

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



Observação

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

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 está em curto-circuito com o TERRA.
Cortado	O cabo de E/S foi cortado e deixado aberto sem um caminho de corrente para o TERRA.

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 22*.
3. Mantenha o botão de controle pressionado por 25 segundos até que o LED indicador de status se torne âmbar pela segunda vez.
4. Solte o botão de controle. O processo estará concluído quando o indicador do LED de estado ficar verde. Se nenhum servidor DHCP estiver disponível na rede, o endereço IP do dispositivo 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, atribua um endereço IP, defina a senha e acesse o produto.

Você também pode redefinir os parâmetros para as configurações padrão de fábrica na interface Web do dispositivo. Vá para **Maintenance (Manutenção)** > **Factory default (Padrão de fábrica)** e clique em **Default (Padrão)**.

Opções do AXIS OS

A Axis oferece o gerenciamento de software de dispositivo de acordo com a trilha ativa ou com as trilhas de suporte de longo prazo (LTS). Estar na trilha ativa significa que você obtém acesso contínuo a todos os recursos de produtos mais recentes, enquanto as trilhas de LTS fornecem uma plataforma fixa com versões periódicas voltadas principalmente para correções de erros e atualizações de segurança.

Usar os AXIS OS da trilha ativa é recomendado se você deseja acessar os recursos mais recentes ou se você usa as ofertas de sistema ponta a ponta Axis. As trilhas de LTS são recomendados se você usa integrações de outros fabricantes, as quais podem não ser continuamente validadas com a trilha ativa mais recente. Com o LTS, os produtos podem manter a segurança cibernética sem apresentar quaisquer alterações funcionais significativas nem afetar quaisquer integrações existentes. Para obter informações mais detalhadas sobre a estratégia de software de dispositivos Axis, acesse *axis.com/support/device-software*.

Verificar a versão atual do AXIS OS

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

Para verificar a versão atual do AXIS OS:

1. Vá para a interface Web do dispositivo > **Status**.
2. Em **Device info (Informações do dispositivo)**, consulte a versão do AXIS OS.

Solução de problemas

Atualizar o AXIS OS

Importante

- As configurações pré-configuradas e personalizadas são salvas quando você atualiza o software do dispositivo (desde que os recursos estejam disponíveis no novo AXIS OS), 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 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*.

Observação

Como o banco de dados de usuários, grupos, credenciais e outros dados são atualizados depois de uma atualização do AXIS OS, a primeira inicialização pode levar alguns minutos para ser concluída. O tempo necessário depende da quantidade de dados.

1. Baixe o arquivo do AXIS OS para seu computador, o qual está disponível gratuitamente em *axis.com/support/device-software*.
2. Faça login no dispositivo como um administrador.
3. Vá para **Maintenance (Manutenção) > AXIS OS upgrade (Atualização do AXIS OS)** e clique em **Upgrade (Atualizar)**.

Após a conclusão da atualização, o produto será reiniciado automaticamente.

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

Problemas técnicos, 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 AXIS OS	
Falha na atualização do AXIS OS	Se a atualização falhar, o dispositivo recarregará a versão anterior. O motivo mais comum é que o arquivo de incorreto do AXIS OS foi carregado. Verifique se o nome do arquivo do AXIS OS corresponde ao seu dispositivo e tente novamente.
Problemas após a atualização do AXIS OS	Se você tiver problemas após a atualização, reverta para a versão instalada anteriormente na página **Maintenance (Manutenção)**.

Problemas na configuração do endereço IP	
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 `ping` e o endereço IP do dispositivo): • Se você receber: `Responder do <endereço IP> bytes=32; time=10...`, isso significa que o endereço IP já pode estar sendo usado por outro dispositivo na rede. Obtenha um novo endereço IP junto ao administrador da rede e reinstale o dispositivo. • Se você receber: `Request timed out`, isso significa que o endereço IP está disponível para uso com o dispositivo Axis. Verifique todo o cabeamento e reinstale o dispositivo.
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.

Solução de problemas

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 `http` ou `https` 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 *Redefinição para as configurações padrão de fábrica na página 32*.
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 Camera Station Edge: grátis, ideal para sistemas pequenos com necessidades básicas de monitoramento.
- AXIS Camera Station 5: versão de avaliação grátis por 30 dias, ideal para sistemas de pequeno a médio porte.
- AXIS Camera Station Pro: versão de avaliação grátis por 90 dias, ideal para sistemas de pequeno a médio porte.

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

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. • Se o servidor/broker suporta WebSocket/WebSocket Secure (WS/WSS), geralmente na porta 443, use este protocolo em vez do MQTT. Verifique com o provedor do servidor/broker para saber se o WS/WSS é suportado e qual porta e caminho base devem ser usados. • Se o servidor/corretor suportar ALPN, o uso do MQTT poderá ser negociado em uma porta aberta, como a 443. Verifique com seu provedor de servidor/corretor se há suporte para ALPN e qual protocolo e porta ALPN usar.

Entre em contato com o suporte

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

Manual do Usuário
AXIS A1710-B Network Door Controller

Ver. M1.11
Data: Novembro 2024
Nº da peça T10217727