AXIS D8204-E PoE++ Switch

Manual do Usuário

Índice

Sobre este manual 3
Abreviações 3
Visão geral da solução 4
Introdução 5
Acesse o produto a partir de um navegador 5
Conheça o site do seu produto 5
Conheça a ajuda embutida do seu produto 6
Exemplos de configuração 7
Configurar VLANs de acesso 7
Reserve um endereço de IP baseado no endereço MAC 8
Crie links redundantes entre interruptores para redundância de rede 8
Use o VAPIX para ativar ou desativar o PoE em uma porta 9
Configurar o MACsec 9
CAK estático 9
CAK dinâmico 10
Conexão de um módulo SFP de 1 Gbps 12
Mantenha seu sistema 13
Reinicie o produto 13
Restauração das configurações padrão de fábrica 13
Atualizar o software do dispositivo 14
Inverter para imagem de software alternativa 14
Especificações 15
Visão geral do produto 15
Solução de problemas 16
Cibersegurança 17
Gerenciamento de vulnerabilidades 17
Notificações de segurança 17
Ciclo de vida seguro do produto 17

Sobre este manual

Observação

A intenção é que o produto seja usado pelos administradores de rede que são responsáveis por operar e dar manutenção nos equipamentos de rede. Conhecimento básico de trabalho de funções gerais do interruptor, segurança, o Protocolo de Internet (IP) e o Protocolo Simples de Gerenciamento de Rede (SNMP) é esperado.

Este manual do usuário fornece informações sobre como:

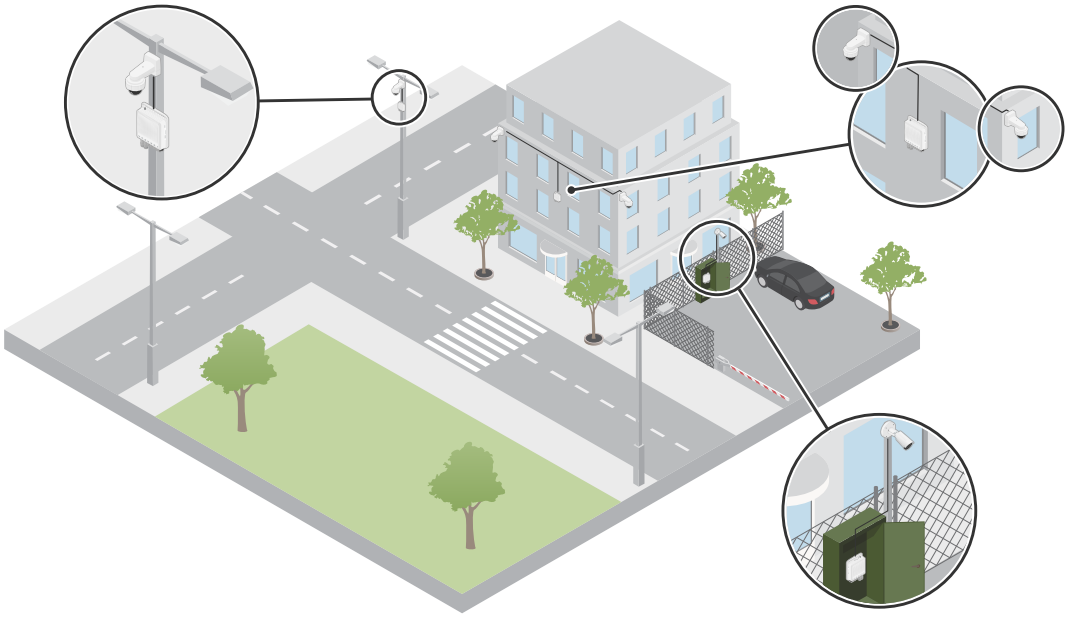
- acessar o produto
- configurar exemplos de definição selecionados
- executar manutenção no produto

Características do produto e suas configurações são cobertos em mais detalhe na ajuda embutida sensível a contexto do produto.

Abreviações

Abreviação	Descrição
MACsec	Segurança do Controle de Acesso de Mídia
802.1X	Controle de acesso à rede
802.1AE	Igual ao MACsec
CAK	Chave da Associação de Conectividade
CKN	Nome da chave de conectividade
DHCP	Dynamic Host Configuration Protocol (Protocolo de configuração de hosts dinâmicos)
OpenSSL	Biblioteca de Software de Código Aberto
PoE	Power over Ethernet
RAIO	Remote Authentication Dial-in User Service
SFP	Interface de fibra, plugue com fator de forma pequeno
SFP+	Plugue aprimorado de formato compacto
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VLAN	Rede local virtual

Visão geral da solução



Os dispositivos de borda Axis são instalados nas instalações e conectados aos switches Axis por meio de Ethernet. Os switches são conectados por meio de fibra.

Introdução

Acesse o produto a partir de um navegador

Observação

- Instale, conecte e ligue o dispositivo como especificado no guia de instalação.
- Depois de seguir as etapas descritas nesta seção, você acessará a página da Web do produto e poderá configurar e gerenciar o produto.

1. Use o Utilitário AXIS IP ou Gerente de Dispositivo AXIS para encontrar o dispositivo na rede. Para obter mais informações sobre como descobrir dispositivos, vá para *axis.com/support*.
2. Insira o nome de usuário e senha fornecidos na etiqueta do produto.
   O nome de usuário padrão é root.
3. Siga os passos no assistente de configuração para:

– Mudar a senha (recomendado por motivos de segurança)

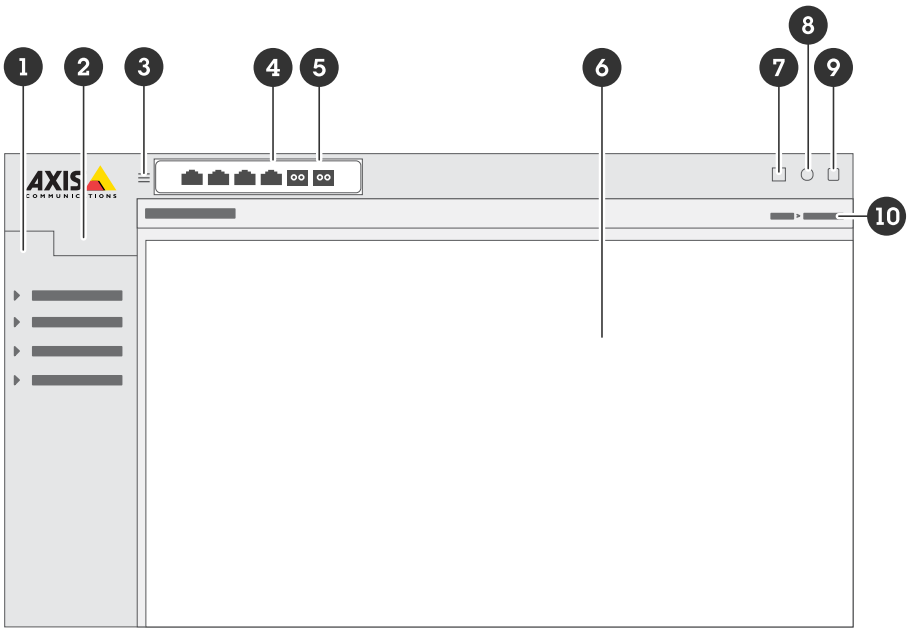
– Definir o endereço de IP via DHCP ou manualmente

– Definir as informações de data e hora

– Definir as informações de sistema

4. Clique em **Save (Salvar)**.
5. Faça login novamente usando a nova senha.

Conheça o site do seu produto



1 Recursos básicos
2 Recursos avançados
3 Botão de alternância - oculta ou exibe o menu
4 Indicadores de status da porta RJ45
5 Indicadores de status da porta SFP
6 Área de conteúdo para recursos básicos/avançados
7 Botão Salvar - salva suas configurações no arquivo de configuração de inicialização
8 Botão Ajuda - acesse a ajuda embutida sensível ao contexto
9 Botão Sair
10 Caminho do menu

Conheça a ajuda embutida do seu produto

O seu produto tem uma ajuda embutida sensível ao contexto. A ajuda oferece informações mais detalhadas sobre os recursos básicos e avançados do produto e suas configurações. Para acessar o conteúdo de ajuda para qualquer exibição específica, clique em

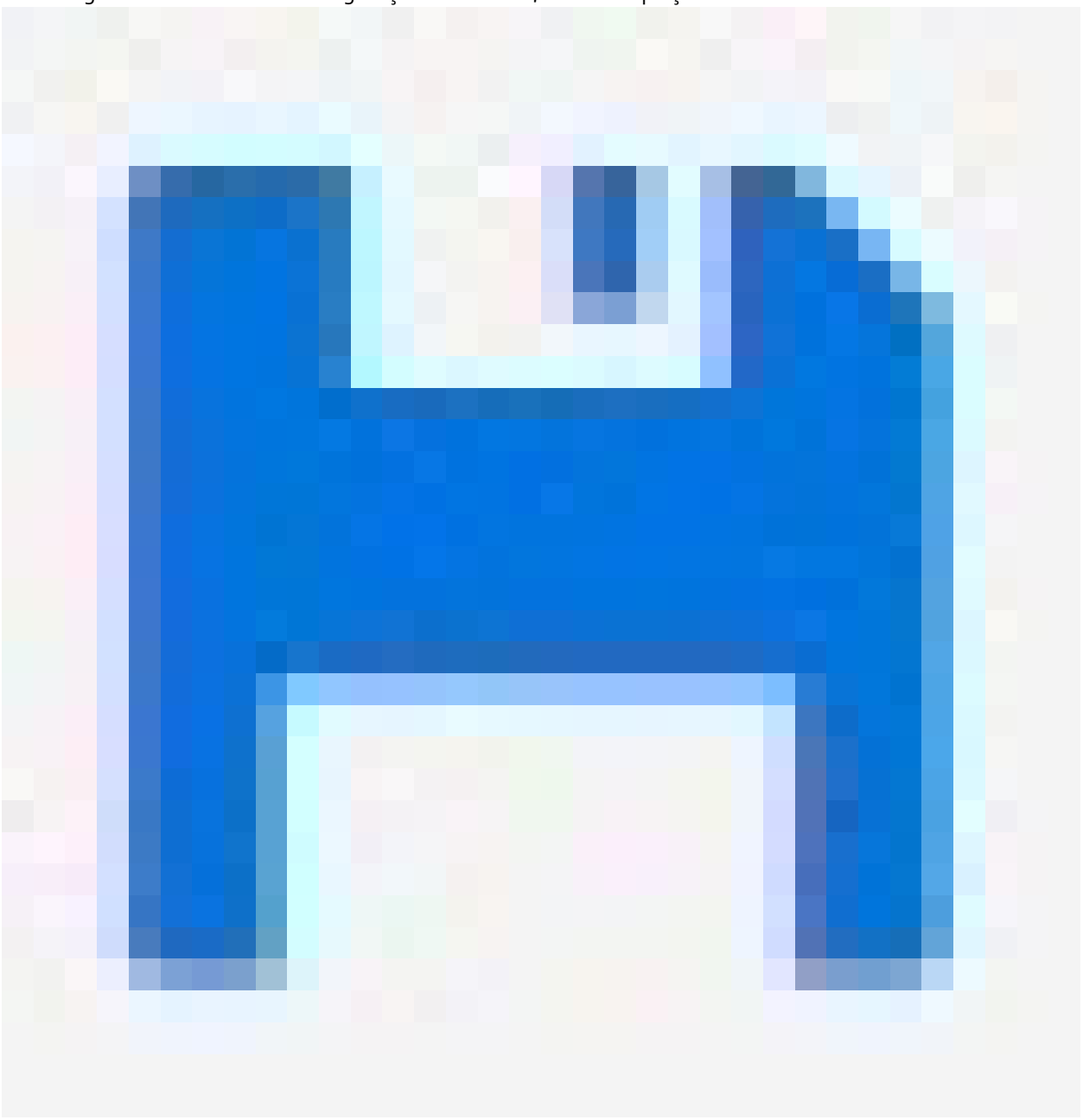


. Algum conteúdo de ajuda também inclui termos e acrônimos clicáveis que são explicados em mais detalhes no glossário embutido.

Exemplos de configuração

Observação

Ao configurar ou atualizar as configurações do switch, não se esqueça de clicar em



para salvar as atualizações no arquivo de configuração inicial.

O arquivo de configuração inicial permanece quando você reinicia ou reinicializa o switch, mas não depois de redefinir o switch para as configurações padrão de fábrica.

Configurar VLANs de acesso

VLANS normalmente são usadas em grandes redes para criar vários domínios de transmissão, mas também podem ser usadas para segregar tráfego de rede. Por exemplo, tráfego de vídeo pode fazer parte de uma VLAN, e outros tráfego de rede pode fazer parte de outra.

1. Vá para **Advanced (avançado)** > **VLANs** > **Configuration (configuração)**.
2. Em **Global VLAN Configuration (configuração VLAN global)**, no campo **Allowed Access VLANs (VLANs de acesso permitido)**, insira os IDs das VLANs a serem criadas. Por exemplo, se você inserir: 1, 10-13, 200, 300; serão criados os seguintes IDs de VLAN: 1, 10, 11, 12, 13, 200 e 300.

3. Para atribuir uma determinada porta a um ID de VLAN criado, em **Port VLAN Configuration (configuração de porta VLAN)**, insira o ID no campo **Porta VLAN**.
4. Clique em **Save (Salvar)**.

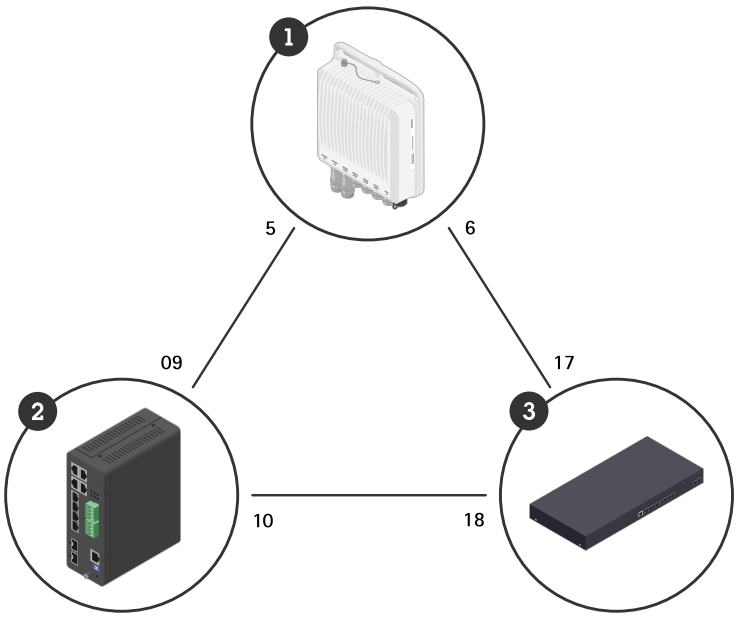
Reserve um endereço de IP baseado no endereço MAC

1. Vá para **Advanced (avançado)** > **DHCP** > **Server (servidor)** > **Configuration (configuração)** > **Pool**.
2. Clique em **Adicionar novo repositório**.
3. Insira um nome para o pool e clique em **Save (salvar)**. Não são permitidos espaços no nome.
4. Para acessar as configurações do repositório, clique no nome adicionado.
5. No menu suspenso **Tipo**, selecione **Host**.
6. Insira outras configurações exigidas, como endereço de **IP**, **Máscara da subrede** e **Roteador padrão**.
7. No menu suspenso **Identificador do cliente**, selecione **MAC**.
8. No campo **Endereço do Hardware** , digite o endereço MAC do dispositivo.
9. Clique em **Save (Salvar)**.

Crie links redundantes entre interruptores para redundância de rede

Se for necessária redundância de rede, você pode criar links redundantes entre interruptores usando configuração de árvore abrangente.

Exemplo:
Neste exemplo, as chaves AXIS D8204-E (1), AXIS D8208-R (2) e AXIS T8516 (3) estão conectadas por um link redundante, sem VLANs adicionais. Se qualquer dos links entre os interruptores falhar, o link redundante é ativado e fornece conectividade de rede:



Device name (Nome do dispositivo):	Nome do modelo	Portas CIST
Interruptor - 01	AXIS D8204-E	5, 6
Interruptor - 02	AXIS D8208-R	9, 10
Interruptor - 03	AXIS T8516	17, 18

Para criar um link redundante em cada site do interruptor:

1. Vá para **Advanced (avançado)** > **Spanning Tree (árvore abrangente)** > **Configuration (configuração)** > **Bridge Settings (configurações da ponte)**.
2. Em **Basic settings (configurações básicas)** no menu suspenso **Protocol Version (versão do protocolo)**, selecione **RSTP**, e clique em **Save (salvar)**.
3. Vá para **Advanced (avançado)** > **Spanning Tree (árvore abrangente)** > **Configuration (configuração)** > **CIST Port (porta CIST)**.
4. Em **Configuração da Porta Normal CIST**, certifique-se de que **STP habilitado** esteja selecionado para as portas do interruptor, como segue:

- Interruptor – 01: portas 5 e 6
- Interruptor – 02: portas 9 e 10
- Interruptor – 03: portas 17 e 18

5. Clique em **Save (Salvar)**.

Observação

Se você quiser garantir que uma certa porta é usada como um link de comunicação principal, insira **Custo do caminho** para essa porta em **Configuração da Porta Normal CIST**. Se não for especificado, o interruptor seleciona a porta automaticamente. Por exemplo, se você deseja usar a porta 17 como o link de comunicação primário, insira o valor de **Path Cost (Custo do Caminho)**10 para a porta 6 e o valor de**Path Cost (Custo do Caminho)**50 para a porta 18.

Use o VAPIX para ativar ou desativar o PoE em uma porta

Você pode usar os seguintes comandos no VAPIX para ativar ou desativar o PoE em uma porta específica:

- Ativar PoE:
  `http://[IP address of the switch]/axis-cgi/nvr/poe/setportmode.cgi?port=[number of the port on the switch]&enabled=yes&schemaversion=1`
- Desativar PoE:
  `http://[IP address of the switch]/axis-cgi/nvr/poe/setportmode.cgi?port=[number of the port on the switch]&enabled=no&schemaversion=1`

Configurar o MACsec

A configuração do MACsec estabelece uma conexão segura entre dois dispositivos compatíveis com MACsec, a fim de garantir que a comunicação entre seus dispositivos seja confidencial, submetida a autenticação e protegida contra ataques de repetição.

CAK estático

Uma Chave de Associação de Conectividade (CAK) é uma chave criptográfica que garante a comunicação segura entre dispositivos. Deve ter 32 caracteres hexadecimais para uma chave de 128 bits ou 64 caracteres hexadecimais para uma chave de 256 bits.

Um Nome de Chave de Conectividade (CKN) identifica a chave necessária para estabelecer uma conexão MACsec segura entre dispositivos e permite que apenas dispositivos autorizados participem da comunicação segura. O CKN deve ter entre 2 e 64 caracteres hexadecimais, e o número de caracteres deve ser um número par. O CKN identifica qual CAK deve ser usado, e tanto a CAK quanto o CKN devem coincidir em ambas as extremidades do link para estabelecer a comunicação MACsec.

Você pode criar os arquivos CAK e CKN manualmente ou gerá-los com o OpenSSL.

Gerar CAK e CKN com o OpenSSL

1. Abra um prompt de comando em um computador que tenha o OpenSSL instalado.
2. Para gerar uma CAK:

- Tipo openssl rand -hex 16.
- Pressione Enter.

3. Para gerar um CKN:
   - Tipo openssl rand -hex 8.
   - Pressione Enter.
4. Salve a CAK e o CKN. Você vai precisar deles mais tarde.

Configurar dispositivo AXIS OS

1. Na interface web do dispositivo,vá para **System (Sistema)** > **Security (Segurança)** > **Network access control and encryption (Controle de acesso à rede e criptografia)**.
2. Em **Authentication method (Método de autenticação)**, selecione **IEEE 802.1AE MACsec (Static CAK/ /Pre-Shared Key)**.
3. Em **Key agreement connectivity association key name (nome da chave de associação de conectividade do acordo**, digite o CKN.
4. Para **a chave de associação de conectividade do acordo de chaves**, digite a CAK.
5. Clique em **Save (Salvar)**.

Configure a chave

1. Na interface web do switch, vá para **Advanced (avançado)** > **Security (segurança)** > **MACsec** > **Configuration (configuração)** > **Policies (políticas)**.
2. Clique em **Add Policy (adicionar política)**.
3. Insira um nome para a política.
4. Selecione **Enable (ativar)** e digite a CAK e o CKN que você gerou.
5. Clique em **Save (Salvar)**.
6. Vá para **Advanced (avançado)** > **Security (segurança)** > **MACsec** > **Configuration (configuração)** > **Interfaces**.
   - Para a **interface** conectada ao dispositivo, selecione a nova política na lista suspensa.
   - Clique em **Save (Salvar)**.

Verifique a conexão

1. Na interface web do switch, vá para **System (sistema)** > **Security (segurança)** > **MACsec** > **Status** > **Status**.
2. Verifique se**State (estado)** apresenta um indicador verde.

CAK dinâmico

O CAK é gerado por meio de um processo de autenticação e gerenciamento de chaves que utiliza o padrão IEEE 802.1X e um servidor de autenticação. Com isso, você pode gerar e realizar o gerenciamento de chaves dinamicamente, de modo que não seja necessário realizar a configuração manual das chaves de longo prazo.

Observação

- Certifique-se de que um servidor RADIUS esteja configurado e tenha acesso na rede.
- Instale o *certificado CA de identificação do dispositivo Axis* no servidor RADIUS.

Configure o dispositivo conectado

1. Na interface web do dispositivo,vá para **System (Sistema)** > **Security (Segurança)** > **Network access control and encryption (Controle de acesso à rede e criptografia)**.
2. Em **Authentication method (método de autenticação)**, selecione **IEEE 802.1X EAP-TLS / IEEE 802.1AE MACsec (CAK dinâmico)**.

3. Em **Client certificate (certificado do cliente)**, selecione o certificado de ID do dispositivo Axis no qual o servidor RADIUS confia<. O servidor de autenticação usa o certificado para validar a identidade do cliente.
4. Para **certificados CA**, quando nenhum certificado é selecionado, o dispositivo realiza a autenticação independentemente da rede à qual esteja conectado.
5. No campo **EAP Identity (Identidade EAP)**, digite a identidade do usuário associada ao certificado do cliente. A identidade EAP deve corresponder ao campo Common Name (Nome Comum (CN)) no certificado de cliente selecionado.
6. Na lista **EAPOL Version (versão EAPOL)**, selecione a versão utilizada pelo switch de rede.
7. Ative **Use IEEE 802.1X** para usar o protocolo IEEE 802.1X.
8. Clique em **Save (Salvar)**.

Configure 802.1X no switch

1. Na interface web do switch, vá para **Advanced (avançado)** > **Security (segurança)** > **Radius** > **Configuration (configuração)**.
2. Clique em **Add new server (Adicionar novo servidor)** e digite o nome de host e a senha.
3. Clique em **Save (Salvar)**.
4. Vá para **Advanced (avançado)** > **Spanning Tree (árvore abrangente)** > **Configuration (configuração)** > **CIST Ports (portas CIST)**.
5. Limpe a caixa de seleção **STP Enabled (STP ativado)** da porta conectada ao seu dispositivo.
6. Clique em **Save (Salvar)**.
7. Vá para **Advanced (avançado)** > **Security (segurança)** > **802.1X** > **Configuration (configuração)**.
8. Na lista **Mode (Modo)**, selecione **Enabled (Ativado)**.
9. Para a porta relevante, defina **Admin state (estado admin)** para **Port-based 802.1X (baseado em porta)**.
10. Clique em **Save (Salvar)**.

Verifique a conexão 802.1x

1. Na interface web do dispositivo, vá para **System (sistema)** > **Security (segurança)**.
2. Verifique se **802.1X Authorized (Autorizado)** apresenta um indicador de estado verde.

Configure o MACsec na chave

1. Na interface web do switch, vá para **Advanced (avançado)** > **Security (segurança)** > **MACsec** > **Configuration (configuração)** > **Policies (políticas)**.
2. Clique em **Add policy (Adicionar política)** e digite um nome para a política.
3. Clique em **Save (Salvar)**.
4. Vá para **Advanced (avançado)** > **Security (segurança)** > **MACsec** > **Configuration (configuração)** > **Interfaces**.
5. Para a interface conectada ao dispositivo, selecione a política recém-criada na lista.
6. Clique em **Save (Salvar)**.

Verifique a conexão MACsec

1. Vá para **System (sistema)** > **Security (segurança)** > **MACsec** > **Status** > **Status**.
2. Verifique se**State (estado)** apresenta um indicador verde.

Observação

Se o estado da conexão permanecer como pending (pendente), reinicie o dispositivo.

Conexão de um módulo SFP de 1 Gbps

1. Vá para **Advanced (Avançado)** > **Ports (Portas)** > **Configuration (Configuração)**.
2. Para a porta à qual você conectou o módulo (5 ou 6), defina **Configured (Configurado)** como **1 Gbps FDX (FDX de 1 Gbps)**.

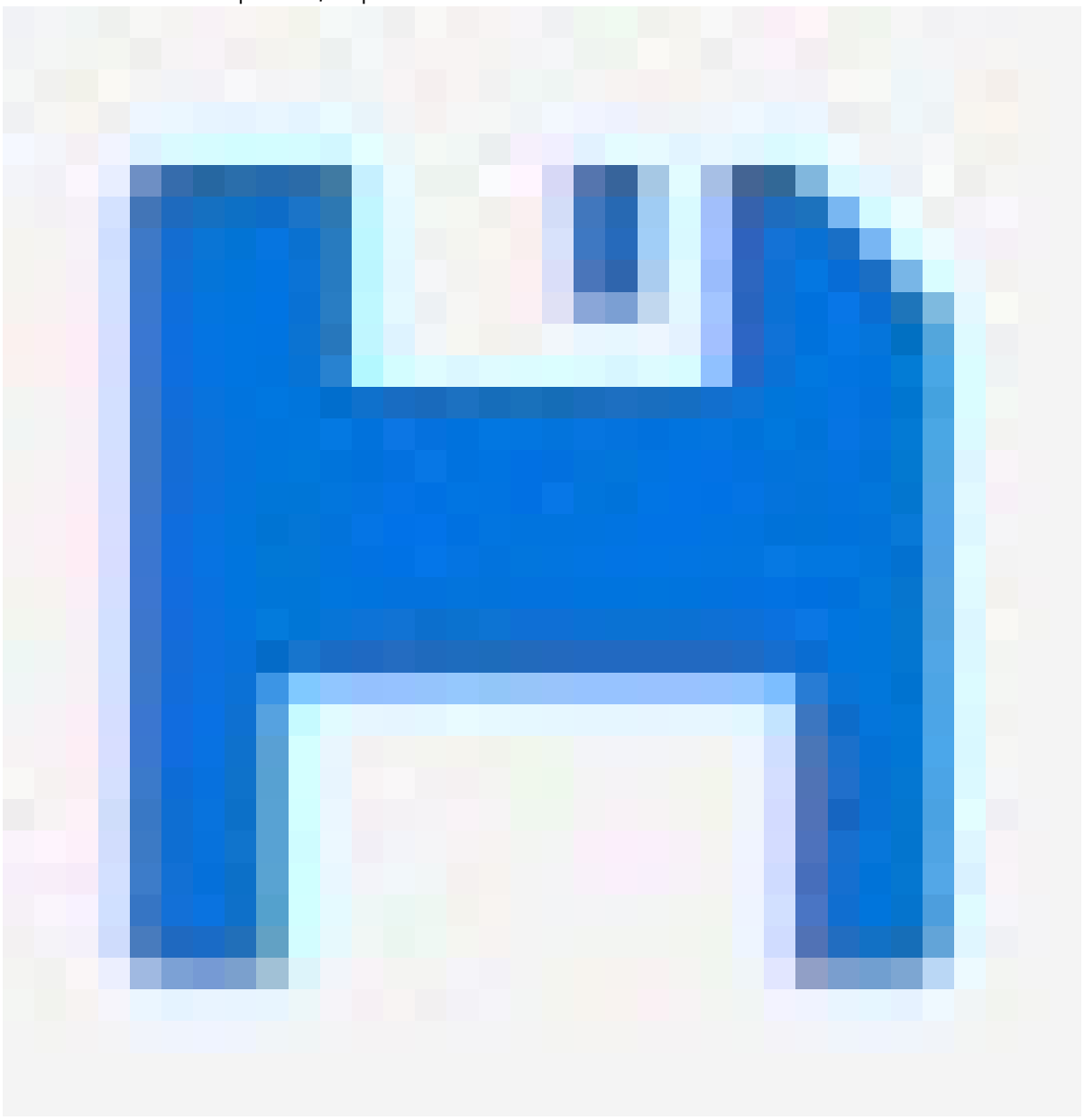
Observação

Se você definir a porta como **Auto**, tanto SFP quando SFP+ funcionarão.

Mantenha seu sistema

Reinicie o produto

Observação

- O tráfego através do produto é afetado durante a reinicialização.
- Antes de reiniciar o dispositivo, clique em  para salvar suas configurações no arquivo de configuração de inicialização.

1. Vá para **Advanced (avançado)** > **Maintenance (manutenção)** > **Restart Device (reiniciar dispositivo)**.
2. Clique em **Sim**. Depois da reinicialização, o produto será iniciado normalmente.

Restauração das configurações padrão de fábrica

Importante

Qualquer configuração salva será restaurada para os valores padrões de fábrica.

1. Vá para **Advanced (avançado)** > **Maintenance (manutenção)** > **Factory Defaults (padrões de fábrica)**.
2. Clique em **Sim**.

Siga estas etapas para restaurar o padrão de fábrica caso tenha esquecido a senha:

1. Desconecte tudo da chave, inclusive a alimentação elétrica.
2. Conecte um cabo RJ45 entre as portas 1 e 2.
3. Conecte o cabo de alimentação e ligue a chave.
4. Após 5 minutos, desconecte o cabo RJ45. O cabo de alimentação deve permanecer conectado.
5. Conecte a unidade ao computador e o endereço IP deverá voltar a ser o endereço IP padrão, 192.168.0.254.
6. Vá para **Advanced (avançado)** > **Maintenance (manutenção)** > **Factory Defaults (padrões de fábrica)**.
7. Clique em **Sim**.

Atualizar o software do dispositivo

Importante

A atualização do software leva até 10 minutos. Não reinicie nem desligue o dispositivo durante este tempo.

Observação

O tráfego através do produto é afetado durante a atualização.

1. Vá para **Advanced (avançado)** > **Maintenance (manutenção)**> **Device Software (software do dispositivo)** > **Software Upgrade (upgrade de software)**.
2. Para selecionar o arquivo de software a partir de um local específico, clique em **Select file... (selecionar arquivo)**.
3. Clique em **Atualizar**.

Depois da atualização do software, o produto será reiniciado normalmente.

Inverter para imagem de software alternativa

É possível escolher usar a imagem de software alternativa (backup) em vez da imagem de software ativa (principal) no produto. As tabelas de informações em ambas as imagens são mostradas em **Avançado > Manutenção > Software do Dispositivo > Seleção de Software**.

Observação

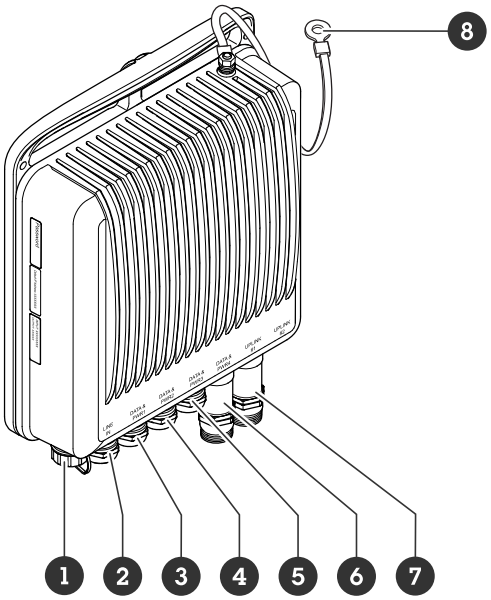
- Se a imagem ativa já estiver definida como a imagem alternativa, apenas a tabela de **Imagem Ativa** é mostrada e o botão **Ativar imagem alternartiva** é desabilitado.
- Se a imagem alternativa já estiver definida como a imagem ativa (seja manualmente ou devido a uma imagem principal corrompida), e uma nova imagem de software for carregada no produto, a nova imagem será automaticamente definida como imagem ativa.
- A versão do software e as informações de data serão vazias para versões de software mais antigas. Isso é normal.

Para definir a imagem alternativa como a imagem ativa:

1. Vá para **Avançado > Manutenção > Software do Dispositivo > Seleção de Software**.
2. Clique em **Ativar imagem alternativa**.

Especificações

Visão geral do produto



1 Porta do conector de alimentação
2 – 5. Porta PoE RJ45
6 – 7. Slot SFP
8 Cabo de aterramento

Solução de problemas

Problemas com o acesso ao dispositivo

Não é possível fazer login ao acessar o dispositivo em um navegador

Quando o HTTPS estiver ativado, certifique-se de utilizar o protocolo correto (HTTP ou HTTPS) ao tentar fazer login. Talvez seja necessário digitar manualmente `http` ou `https` no campo de endereço do navegador.

Caso tenha perdido a senha da conta root, será necessário redefinir o dispositivo para as configurações padrão de fábrica. Para obter instruções, consulte *Restauração das configurações padrão de fábrica, on page 13*.

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 precisar de mais ajuda, vá para *axis.com/support* ou consulte *o Guia de Configuração dos Switches de Rede Axis*.

Cibersegurança

A segurança cibernética oferece suporte a um ciclo de vida de produto bem-sucedido com riscos minimizados. Você pode encontrar informações detalhadas e documentação sobre nossa abordagem à segurança cibernética em *axis.com/about-axis/cybersecurity*. Siga as diretrizes de segurança cibernética abaixo para receber notificações de segurança da Axis sobre o produto e para realizar a configuração do produto, de modo a garantir um ciclo de vida e um descomissionamento seguros.

No *Axis Trust Center*, você pode encontrar informações sobre como a Axis implementa a conformidade de segurança, a transparência, a proteção de dados e a privacidade.

Gerenciamento de vulnerabilidades

A Axis é uma *Autoridade de numeração de vulnerabilidades e exposições comuns (CVE) (CNA)*. Para minimizar seu risco de exposição, seguimos os padrões do setor ao identificar e resolver vulnerabilidades em nossos dispositivos, software e serviços. Consulte *axis.com/vulnerability-management* para obter informações sobre nossa política de gerenciamento de vulnerabilidades ou para relatar uma vulnerabilidade.

Notificações de segurança

Inscreva-se para receber emails de notificação de segurança da Axis em *axis.com/security-notification-service*. Enviaremos a você informações sobre vulnerabilidades, alertas de segurança correspondentes e outros assuntos relacionados à segurança do seu produto Axis.

Ciclo de vida seguro do produto

A Axis minimiza os riscos durante toda a vida útil de nossos produtos por meio do gerenciamento seguro do ciclo de vida. Use nossos guias para aumento do nível de proteção em *help.axis.com* para configurar e operar com mais segurança seus produtos Axis e para encontrar informações sobre:

Uso seguro desde o primeiro uso – Os produtos Axis são pré-configurados com alta proteção padrão para permitir a inicialização segura e a comunicação criptografada desde o início.

Uso pretendido e erros comuns de configuração – Nossos guias fornecem informações sobre o uso pretendido dos produtos Axis, incluindo erros comuns de configuração e usos indevidos relevantes para a segurança que devem ser evitados.

Gerenciamento de vulnerabilidades e transparência da cadeia de suprimentos – Uma lista de materiais de software (SBOM) é publicada com cada versão de software em *axis.com* para divulgar vulnerabilidades e aumentar a transparência da cadeia de suprimentos.

Descomissionamento e exclusão segura de dados – Para desativar um produto com segurança quando ele chegar ao fim de seu ciclo de vida, redefina-o para as configurações padrão de fábrica. Isso apaga suas configurações, dados armazenados e informações confidenciais.

T10231182_pt

2026-11 (M1.17)

© 2025 – 2026 Axis Communications AB