AXIS D8204-E PoE++ Switch

User manual

Table of Contents

About this manual 3
Abbreviations....3
Solution overview 4
Get started....5
Access the product from a browser 5
Get to know your product's web page....5
Get to know your product's built-in help....6
Setup examples 7
Set up access VLANs....7
Reserve an IP address based on MAC address 8
Create redundant links between switches for network redundancy 8
Use VAPIX to turn PoE on or off for a port....9
Configure MACsec....9
Static CAK 9
Dynamic CAK 10
Connect a 1Gbps SFP module 11
Maintain your system....12
Restart the product 12
Reset to factory default settings 12
Upgrade the device software 13
Revert to alternate software image 13
Specifications....14
Product overview 14
Troubleshooting....15
Cybersecurity 16
Vulnerability management 16
Security notifications....16
Secure product lifecycle....16

About this manual

Note

The product is intended for use by network administrators who are responsible for operating and maintaining network equipment. Basic working knowledge of general switch functions, security, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP) is assumed.

This user manual will give you information on how you:

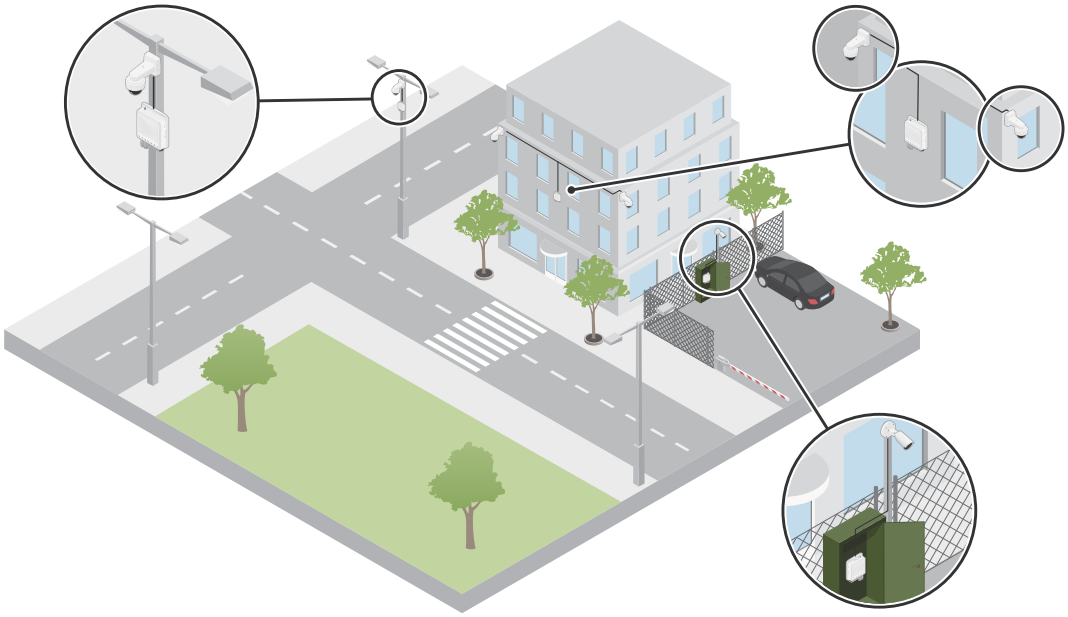
- access the product
- configure selected setup examples
- perform maintenance on the product

Product features and their settings are covered in more detail in the product's context-sensitive built-in help.

Abbreviations

Abbreviation	Description
MACsec	Media Access Control Security
802.1X	Network access control
802.1AE	Same as MACsec
CAK	Connectivity Association Key
CKN	Connectivity Key Name
DHCP	Dynamic Host Configuration Protocol
OpenSSL	Open-Source Software Library
PoE	Power over Ethernet
RADIUS	Remote Authentication Dial-in User Service
SFP	Fiber interface, small form-factor plug
SFP+	Enhanced small form-factor plug
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VLAN	Virtual Local Area Network

Solution overview



Axis edge devices are installed on the premises and are connected to Axis switches through Ethernet. The switches are connected through fiber .

Get started

Access the product from a browser

Note

- Install, connect, and power up the device as specified in the installation guide.
- After following the steps in this section, you will enter the product's web page, and will be able to configure and manage the product.

1. Use AXIS IP Utility or AXIS Device Manager to find the device on the network. For more information about how to discover devices, go to *axis.com/support*.
2. Enter the username and password provided on the product label.
   The default username is root.
3. Follow the steps in the setup wizard to:

– Change the password (recommended for security reasons)

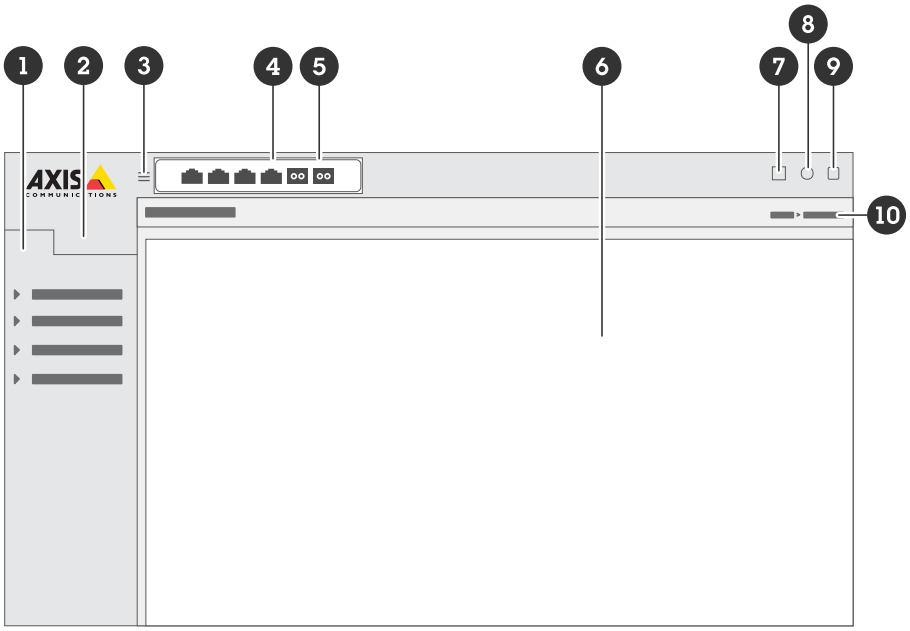
– Set the IP address via DHCP or manually

– Set the date & time information

– Set the system information

4. Click **Save**.
5. Relogin using the new password.

Get to know your product's web page



1 Basic features
2 Advanced features
3 Toggle button - hide or unhide the menu
4 RJ45 port status indicators
5 SFP port status indicators
6 Content area for basic/advanced features
7 Save button - save your settings to the start-up configuration file
8 Help button - access the context-sensitive built-in help
9 Log out button
10 Menu path

Get to know your product's built-in help

Your product has a context-sensitive built-in help. The help provides more detailed information on the product's basic and advanced features and their settings. To access the help content for any given view, click

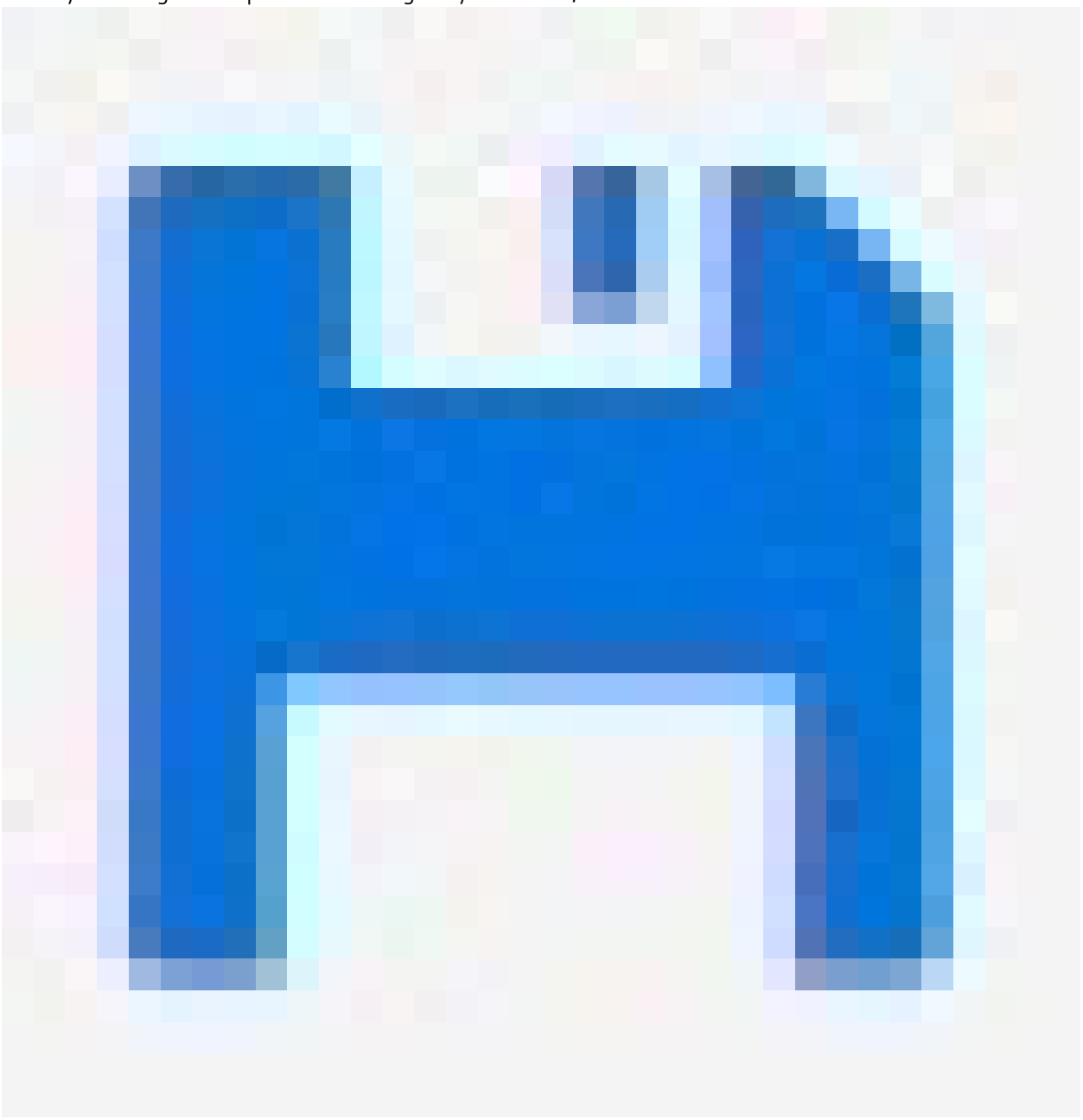


. Some help content also includes clickable terms and acronyms that are explained in more detail in the built-in glossary.

Setup examples

Note

When you configure or update the settings of your switch, make sure to click



to save the updates to the start-up configuration file.

The start-up configuration file remains when you restart or reboot the switch, but not after you reset the switch to its factory default settings.

Set up access VLANs

VLANs are typically used on large networks to create multiple broadcast domains, but they can also be used to segregate network traffic. For example, video traffic can be part of one VLAN, and other network traffic can be part of another.

1. Go to **Advanced** > **VLANs** > **Configuration**.
2. Under **Global VLAN Configuration**, in the **Allowed Access VLANs** field, enter the VLAN IDs to create. For example, if you enter: 1, 10-13, 200, 300, the following VLAN IDs will be created: 1, 10, 11, 12, 13, 200 and 300.

3. To assign a given port to a created VLAN ID under **Port VLAN Configuration**, enter the ID to the **Port VLAN** field.
4. Click **Save**.

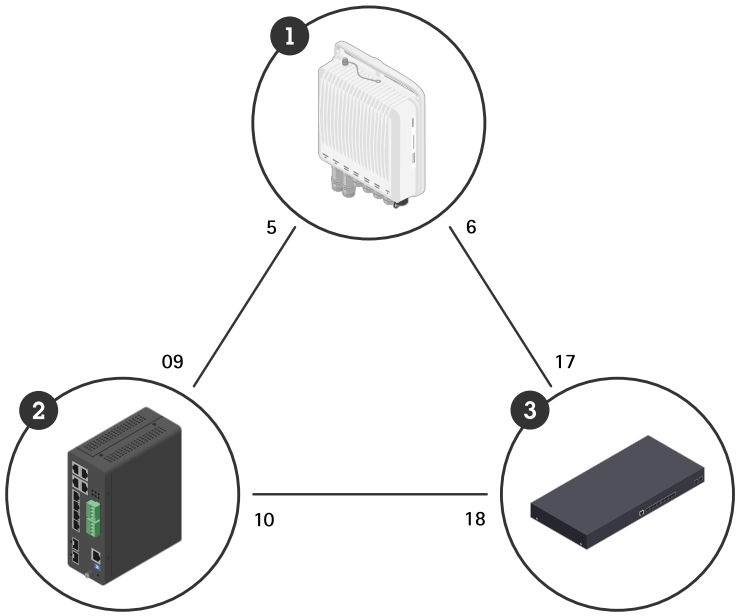
Reserve an IP address based on MAC address

1. Go to **Advanced** > **DHCP** > **Server** > **Configuration** > **Pool**.
2. Click **Add New Pool**.
3. Enter a name for the pool and click **Save**. No spaces are allowed in the name.
4. To access the pool settings, click the added name.
5. In the **Type** drop-down menu, select **Host**.
6. Enter other required settings, such as **IP** address, **Subnet Mask** and **Default Router**.
7. In the **Client Identifier** drop-down menu, select **MAC**.
8. In the **Hardware Address** field, enter the MAC address of the device.
9. Click **Save**.

Create redundant links between switches for network redundancy

If network redundancy is required, you can create redundant links between switches using spanning tree configuration.

Example:
In this example, the switches AXIS D8204-E (1), AXIS D8208-R (2), and AXIS T8516 (3) are connected by a redundant link, and no extra VLANs. If any of the uplinks between the switches should fail, the redundant link is activated and provides network connectivity.



Device name	Model name	CIST ports
Switch - 01	AXIS D8204-E	5, 6
Switch - 02	AXIS D8208-R	9, 10
Switch - 03	AXIS T8516	17, 18

To create a redundant link on each switch's web page:

1. Go to **Advanced** > **Spanning Tree** > **Configuration** > **Bridge Settings**.
2. Under **Basic Settings** in the **Protocol Version** drop-down menu, select **RSTP**, and click **Save**.
3. Go to **Advanced** > **Spanning Tree** > **Configuration** > **CIST Port**.
4. Under **CIST Normal Port Configuration**, make sure that **STP Enabled** is selected for the switch's ports as follows:

- Switch – 01: ports 5 and 6
- Switch – 02: ports 9 and 10
- Switch – 03: ports 17 and 18

5. Click **Save**.

Note

If you want to make sure that a certain port is used as a primary communication link, enter **Path Cost** for that port under **CIST Normal Port Configuration**. If not specified, the switch selects the port automatically. For example, if you want to use port 17 as the primary communication link, enter **Path Cost** value 10 to port 6 and **Path Cost** value 50 to port 18.

Use VAPIX to turn PoE on or off for a port

You can use the following commands in VAPIX to turn PoE on or off for a specific port:

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

Configure MACsec

MACsec configuration establishes a secure relationship between two MACsec-capable devices, to ensure that the communication between your devices are confidential, authenticated, and protected against replay attacks.

Static CAK

A Connectivity Association Key (CAK) is a cryptographic key that ensures secure communication between devices . It must be 32 hexadecimal characters for a 128-bit key or 64 hexadecimal characters for a 256-bit key.

A Connectivity Key Name (CKN) identifies the key to establish a secure MACsec connection between devices and allows only authorized devices to participate in the secure communication. The CKN must be between 2 and 64 hexadecimal characters and the character length must be an even number. The CKN identifies which CAK to use and both the CAK and CKN must match on both ends of the link to establish MACsec communication.

You can create CAK and CKN manually or generate them with OpenSSL.

Generate CAK and CKN with OpenSSL

1. Open a command prompt on a computer with OpenSSL installed.
2. To generate a CAK:
   - Type `openssl rand -hex 16`.
   - Press Enter.
3. To generate a CKN:
   - Type `openssl rand -hex 8`.
   - Press Enter.
4. Save the CAK and CKN. You need them later.

Configure AXIS OS device

1. In the device's web interface, go to **System** > **Security** > **Network access control and encryption**.
2. For **Authentication method**, select **IEEE 802.1AE MACsec (Static CAK/Pre-Shared Key)**.
3. For **Key agreement connectivity association key name**, type the CKN.
4. For **Key agreement connectivity association key**, type the CAK.
5. Click **Save**.

Configure the switch

1. In the switch's web interface, go to **Advanced** > **Security** > **MACsec** > **Configuration** > **Policies**.
2. Click **Add Policy**.
3. Enter a name for the policy.
4. Select **Enable** and type the CAK and CKN that you generated.
5. Click **Save**.
6. Go to **Advanced** > **Security** > **MACsec** > **Configuration** > **Interfaces**.
   - For the **Interface** connected to the device, select the new policy from the drop-down list.
   - Click **Save**.

Verify the connection

1. In the switch's web interface, go to **System** > **Security** > **MACsec** > **Status** > **Status**.
2. Check that **State** has a green status indicator.

Dynamic CAK

The CAK is derived through an authentication and key management process using IEEE 802.1X and an authentication server. With this, you can generate and manage keys dynamically so you don't need to configure long-term keys manually.

Note

- Make sure a RADIUS server is configured and accessible on the network.
- Install the *Axis device ID CA certificate* on the RADIUS server.

Configure the connected device

1. In the device's web interface, go to **System** > **Security** > **Network access control and encryption**.
2. For **Authentication method**, select **IEEE 802.1X EAP-TLS / IEEE 802.1AE MACsec (Dynamic CAK)**.
3. For **Client certificate**, select the Axis device ID certificate that the RADIUS server trusts<. The authentication server uses the certificate to validate the client's identity.
4. For **CA certificates**, when no certificate is selected, the device authenticates itself regardless of what network it is connected to.
5. For **EAP Identity**, type the user identity associated with the client certificate. The EAP Identity must match the Common Name (CN) field in the selected client certificate.
6. In the **EAPOL Version** list, select the version that the network switch uses.
7. Turn on **Use IEEE 802.1X** to use the IEEE 802.1X protocol.
8. Click **Save**.

Configure 802.1X on the switch

1. In the switch's web interface, go to **Advanced** > **Security** > **Radius** > **Configuration**.
2. Click **Add new server** and type the hostname and password.
3. Click **Save**.

4. Go to **Advanced** > **Spanning Tree** > **Configuration** > **CIST Ports**.
5. Clear the **STP Enabled** box for the port connected to your device.
6. Click **Save**.
7. Go to **Advanced** > **Security** > **802.1X** > **Configuration**.
8. In the **Mode** list, select **Enabled**.
9. For the relevant port, set **Admin state** to **Port-based 802.1X** .
10. Click **Save**.

Verify the 802.1x connection

1. In the device's web interface, go to **System** > **Security**.
2. Check that **802.1X Authorized** has a green status indicator.

Configure MACsec on the switch

1. In the switch's web interface, go to **Advanced** > **Security** > **MACsec** > **Configuration** > **Policies**.
2. Click **Add policy** and type a name for the policy.
3. Click **Save**.
4. Go to **Advanced** > **Security** > **MACsec** > **Configuration** > **Interfaces**.
5. For the interface connected to the device, select the newly created policy from the list.
6. Click **Save**.

Verify the MACsec connection

1. Go to **System** > **Security** > **MACsec** > **Status** > **Status**.
2. Check that **State** has a green status indicator.

Note

If the connection status stays pending, restart the device.

Connect a 1Gbps SFP module

1. Go to **Advanced** > **Ports** > **Configuration**.
2. For the port that you connected the module to (5 or 6), set **Configured** to **1 Gbps FDX**.

Note

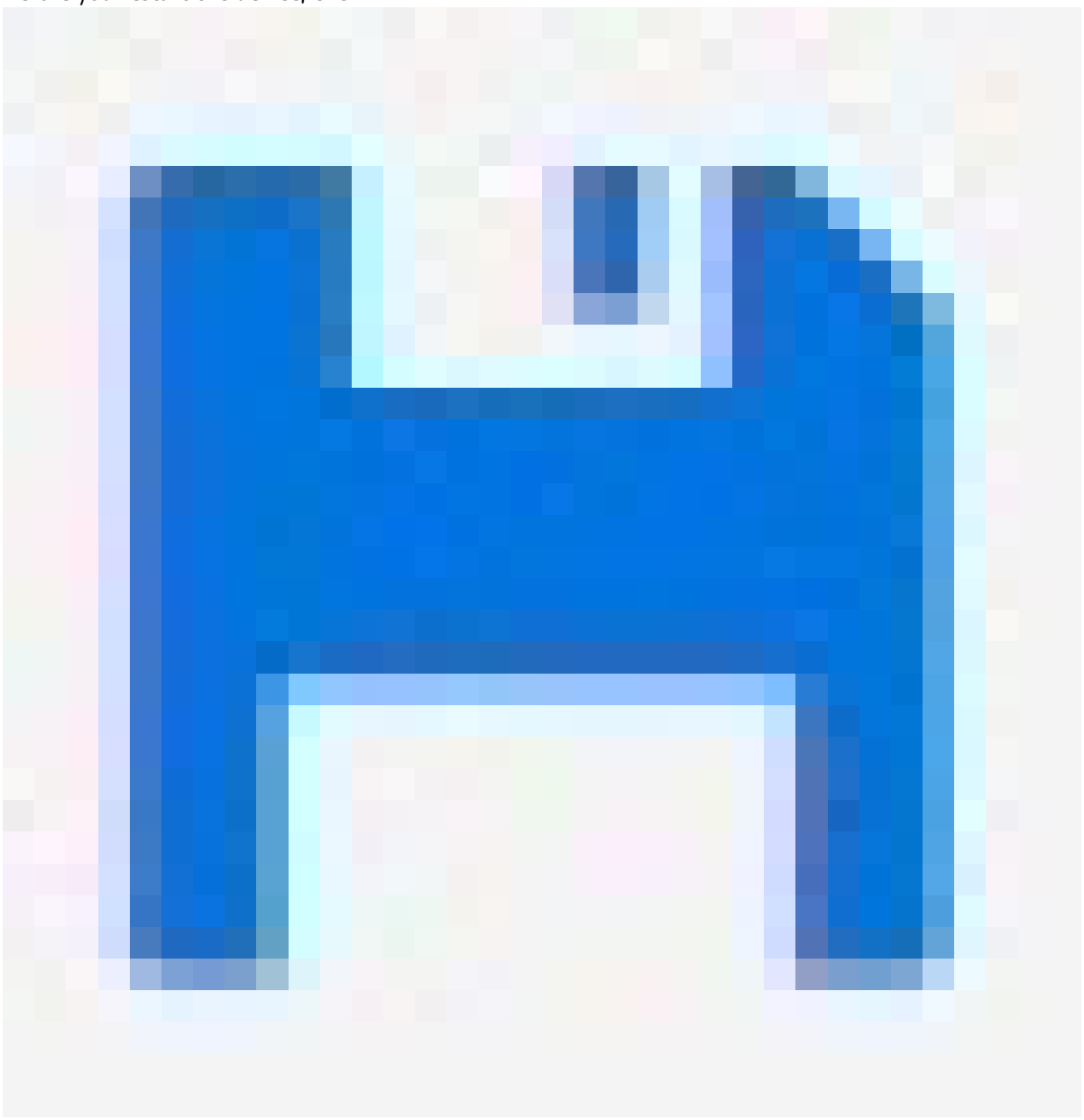
If you set the port to **Auto**, both SFP and SFP+ will work.

Maintain your system

Restart the product

Note

- The traffic through the product is affected during restart.
- Before you restart the device, click



to save your settings to the start-up configuration file.

1. Go to **Advanced** > **Maintenance** > **Restart Device**.
2. Click **Yes**. After restart, the product will boot normally.

Reset to factory default settings

Important

Any saved configuration will be restored to factory default values.

1. Go to **Advanced** > **Maintenance** > **Factory Defaults**.
2. Click **Yes**.

Follows these steps for factory default if you've lost the password:

1. Disconnect everything from the switch, including power.
2. Connect an RJ45 cable between ports 1 and 2.
3. Connect the power cable and power up the switch.
4. After 5 minutes, disconnect the RJ45 cable. The power cable should stay connected.
5. Connect the unit to the computer and the IP should return to the default IP address, 192.168.0.254.
6. Go to **Advanced** > **Maintenance** > **Factory Defaults**.
7. Click **Yes**.

Upgrade the device software

Important

The software upgrade takes up to 10 minutes. Do not restart or power off the device during this time.

Note

The traffic through the product is affected during upgrade.

1. Go to **Advanced** > **Maintenance**> **Device Software** > **Software Upgrade**.
2. To select the software file from a specified location, click **Select file...**.
3. Click **Upgrade**.

After software upgrade, the product will restart normally.

Revert to alternate software image

You can choose to use the alternate (backup) software image instead of the active (primary) software image in the product. Information tables on both images are shown under **Advanced > Maintenance > Device Software > Software Selection**.

Note

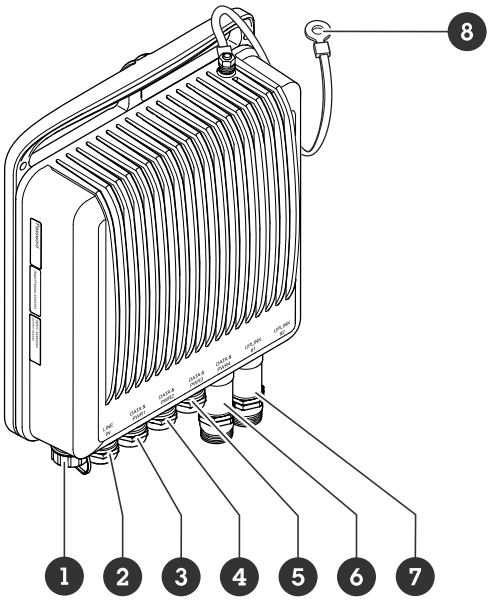
- If the active image is already set as the alternate image, only the **Active Image** table is shown, and the **Activate Alternate Image** button is disabled.
- If the alternate image is already set as the active image (either manually or due to a corrupted primary image), and a new software image is uploaded to the product, the new image will automatically be set as the active image.
- Software version and date information may be empty for older software releases. This is normal.

To set the alternate image as the active image:

1. Go to **Advanced > Maintenance > Device Software > Software Selection**.
2. Click **Activate Alternate Image**.

Specifications

Product overview



1 Power connector port
2 – 5. RJ45 PoE port
6 – 7. SFP slot
8 Grounding cable

Troubleshooting

Problems accessing the device

Can't log in when accessing the device from a browser

When HTTPS is enabled, make sure that you use the correct protocol (HTTP or HTTPS) when you try to log in. You might need to manually type `http` or `https` in the browser's address field.

If you've lost the password for the root account, you must reset the device to the factory default settings. For instructions, see *Reset to factory default settings, on page 12*.

The IP address has been changed by DHCP

IP addresses obtained from a DHCP server are dynamic and could change. If the IP address has been changed, use AXIS IP Utility or AXIS Device Manager to locate the device on the network. Identify the device using its model or serial number, or by the DNS name (if the name has been configured).

If you need more help, go to *axis.com/support* or *Axis Network Switches Configuration Guide*.

Cybersecurity

Cybersecurity supports a successful product lifecycle with minimized risks. You can find in-depth information and documentation about our cybersecurity approach at *axis.com/about-axis/cybersecurity*. Follow the cybersecurity guidelines below to receive product security notifications from Axis and to configure your product for a secure lifecycle and decommissioning.

At *Axis Trust Center*, you can find information about how Axis implements security compliance, transparency, data protection, and privacy.

Vulnerability management

Axis is a *Common Vulnerability and Exposures (CVE) Numbering Authority (CNA)*. To minimize your risk of exposure, we follow industry standards when identifying and resolving vulnerabilities in our devices, software, and services. Refer to *axis.com/vulnerability-management* for information about our vulnerability management policy or to report a vulnerability.

Security notifications

Subscribe to Axis security notification emails at *axis.com/security-notification-service*. We will send you information about vulnerabilities, corresponding security advisories, and other security-related matters for your Axis product.

Secure product lifecycle

Axis minimizes risks throughout the lifetime of our products through secure lifecycle management. Use our hardening guides at *help.axis.com* to more securely configure and operate your Axis products and to find information about:

Secure first-use – Axis products are pre-configured with high default protection to allow for secure initialization and encrypted communication from the very start.

Intended use and common configuration mistakes – Our guides provide information about the intended usage of Axis products, including common security-relevant misuse and configuration mistakes that should be avoided.

Managing vulnerabilities and supply chain transparency – A Software Bill of Material (SBOM) is published with every software release on *axis.com* to disclose vulnerabilities and improve supply chain transparency.

Decommissioning and the secure erasure of data – To securely decommission a product when it reaches the end of its lifecycle, reset it to factory default settings. This erases your configurations, stored data, and sensitive information.

T10231182

2026-11 (M1.17)

© 2025 – 2026 Axis Communications AB