

AXIS A9210 Network I/O Relay Module

Get started

Find the device on the network

To find Axis devices on the network and assign them IP addresses in Windows®, use AXIS IP Utility or AXIS Device Manager. Both applications are free and can be downloaded from axis.com/support.

For more information about how to find and assign IP addresses, go to *How to assign an IP address and access your device*.

Browser support

You can use the device with the following browsers:

	Chrome™	Edge™	Firefox®	Safari®
Windows®	✓	✓	*	*
macOS®	✓	✓	*	*
Linux®	✓	✓	*	*
Other operating systems	*	*	*	*

✓: Recommended

*: Supported with limitations

Open the device's web interface

1. Open a browser and type the IP address or host name of the Axis device.
If you do not know the IP address, use AXIS IP Utility or AXIS Device Manager to find the device on the network.
2. Type the username and password. If you access the device for the first time, you must create an administrator account. See *Create an administrator account, on page 2*.

For descriptions of all the controls and options in the device's web interface, see *The web interface, on page 5*.

Create an administrator account

The first time you log in to your device, you must create an administrator account.

1. Enter a username.
2. Enter a password. See *Secure passwords, on page 3*.
3. Re-enter the password.
4. Accept the license agreement.
5. Click **Add account**.

Important

The device has no default account. If you lose the password for your administrator account, you must reset the device. See *Reset to factory default settings, on page 42*.

Secure passwords

Important

Use HTTPS (which is enabled by default) to set your password or other sensitive configurations over the network. HTTPS enables secure and encrypted network connections, thereby protecting sensitive data, such as passwords.

The device password is the primary protection for your data and services. Axis devices do not impose a password policy as they may be used in various types of installations.

To protect your data we strongly recommend that you:

- Use a password with at least 8 characters, preferably created by a password generator.
- Don't expose the password.
- Change the password at a recurring interval, at least once a year.

Make sure that no one has tampered with the device software

To make sure that the device has its original AXIS OS, or to take full control of the device after a security attack:

1. Reset to factory default settings. See *Reset to factory default settings, on page 42*.
After the reset, secure boot guarantees the state of the device.
2. Configure and install the device.

Web interface overview





This video gives you an overview of the device's web interface.



Axis device web interface


Configure your device

Configure an I/O port


1. Go to **Device > I/Os and relays > AXIS A9210 > I/Os**.
2. Click  to expand the I/O port settings.
3. Rename the port.
4. Configure the normal state. Click  for open circuit, or  for closed circuit.
5. To configure the I/O port as input:
 - 5.1. Under **Direction**, click .
 - 5.2. To monitor the input state, turn on **Supervised**. See *Supervised inputs*, on page 40.

Note

In APIs, the supervised I/O ports work differently from the supervised input ports. For more information, go to the *VAPIX® Library*.

6. To configure the I/O port as output:
 - 6.1. Under **Direction**, click .
 - 6.2. To view the URLs to activate and deactivate connected devices, go to **Toggle port URL**.

Configure a relay

1. Go to **Device > I/Os and relays > AXIS A9210 > Relays**.
2. Click  to expand the relay settings.
3. Turn on **Relay**.
4. Rename the relay.
5. To view the URLs to activate and deactivate the relay, go to **Toggle port URL**.

Set up rules for events

To learn more, see *Get started with rules for events*.

Trigger an action

1. Go to **System > Events** and add a rule. The rule defines when the device will perform certain actions. You can set up rules as scheduled, recurring, or manually triggered.
2. Enter a **Name**.
3. Select the **Condition** that must be met to trigger the action. If you specify more than one condition for the rule, all of the conditions must be met to trigger the action.
4. Select which **Action** to perform when the conditions are met.

Note

- If you make changes to an active rule, the rule must be turned on again for the changes to take effect.

The web interface

To reach the device's web interface, type the device's IP address in a web browser.

Note

Support for the features and settings described in this section varies between devices. This icon  indicates that the feature or setting is only available in some devices.



Show or hide the main menu.



Access the release notes.



Access the product help.



Change the language.



Set light theme or dark theme.



The user menu contains:

- Information about the user who is logged in.
-  **Change account** : Log out from the current account and log in to a new account.
-  **Log out** : Log out from the current account.



The context menu contains:

- **Analytics data**: Accept to share non-personal browser data.
- **Feedback**: Share any feedback to help us improve your user experience.
- **Legal**: View information about cookies and licenses.
- **About**: View device information, including AXIS OS version and serial number.

Status

Device info

Shows information about the device, including AXIS OS version and serial number.

Upgrade AXIS OS: Upgrade the software on your device. Takes you to the Maintenance page where you can do the upgrade.

Time sync status

Shows NTP synchronization information, including if the device is in sync with an NTP server and the time remaining until the next sync.

NTP settings: View and update the NTP settings. Takes you to the **Time and location** page where you can change the NTP settings.

Security

Shows what kind of access to the device that is active, what encryption protocols are in use, and if unsigned apps are allowed. Recommendations to the settings are based on the AXIS OS Hardening Guide.

Hardening guide: Link to *AXIS OS Hardening guide* where you can learn more about cybersecurity on Axis devices and best practices.

Connected clients

Shows the number of connections and connected clients.

View details: View and update the list of connected clients. The list shows IP address, protocol, port, state, and PID/process of each connection.



Device

I/Os and relays



AXIS A9210

I/Os





Input

- **Name:** Edit the text to rename the port.
- **Direction:** Indicates that it is an input port.
- **Normal state:** Click  for open circuit, and  for closed circuit.
- **Supervised:** Turn on to make it possible to detect and trigger actions if someone tampers with the connection to digital I/O devices. In addition to detecting if an input is open or closed, you can also detect if someone has tampered with it (that is, cut or shorted). To supervise the connection requires additional hardware (end-of-line resistors) in the external I/O loop.
 - To use parallel first connection, select **Parallel first connection with a 22 K Ω parallel resistor and a 4.7 K Ω serial resistor**.
 - To use serial first connection, select **Serial first connection** and select a resistor value from the **Resistor values** drop-down list.

Output: Turn on to activate connected devices.

- **Name:** Edit the text to rename the port.
- **Direction:** Indicates that it is an output port.
- **Normal state:** Click  for open circuit, and  for closed circuit.
- **Toggle port URL:** Shows the URLs to activate and deactivate connected devices through the VAPIX® Application Programming Interface.

I/O: Turn on to activate connected devices when the port is configured as output.

- **Name:** Edit the text to rename the port.
- **Direction:** Click  or  to configure it as input or output.
- **Normal state:** Click  for open circuit, and  for closed circuit.
- **Supervised:** Turn on to make it possible to detect and trigger actions if someone tampers with the connection to digital I/O devices. In addition to detecting if an input is open or closed, you can also detect if someone has tampered with it (that is, cut or shorted). To supervise the connection requires additional hardware (end-of-line resistors) in the external I/O loop. It appears only when the port is configured as input.
 - To use parallel first connection, select **Parallel first connection with a 22 K Ω parallel resistor and a 4.7 K Ω serial resistor**.
 - To use serial first connection, select **Serial first connection** and select a resistor value from the **Resistor values** drop-down list.
- **Toggle port URL:** Shows the URLs to activate and deactivate connected devices through the VAPIX® Application Programming Interface. It appears only when the port is configured as output.

Relays

- **Relay:** Turn on or off the relay.
- **Name:** Edit the text to rename the relay.
- **Direction:** Indicates that it is an output relay.
- **Toggle port URL:** Shows the URLs to activate and deactivate the relay through the VAPIX® Application Programming Interface.

AXIS A9910

You can connect up to 16 AXIS A9910 to one AXIS A9210 to support 128 I/Os, 64 relays and 64 Modbus sensors. The max distance from AXIS A9210 to the last AXIS A9910 is 1000 m.



Add encryption key: Click to set up an encryption key to ensure encrypted communication.







Add AXIS A9910: Click to add an expansion module.

- **Name:** Edit the text to rename the expansion module.
- **Address:** Shows the address that the expansion module is connected to.
- **Device software version:** Shows the current software version of the expansion module.
- **Upgrade device software:** Click to upgrade the expansion module software. You can choose to upgrade to the version bundled with the door controller or upload a version of your choice.

I/Os

I/O: Turn on to activate connected devices when the port is configured as output.


- **Name:** Edit the text to rename the port.
- **Direction:** Click  or  to configure it as input or output.
- **Normal state:** Click  for open circuit, and  for closed circuit.
- **Supervised:** Turn on to make it possible to detect and trigger actions if someone tampers with the connection to digital I/O devices. In addition to detecting if an input is open or closed, you can also detect if someone has tampered with it (that is, cut or shorted). To supervise the connection requires additional hardware (end-of-line resistors) in the external I/O loop. It appears only when the port is configured as input.
 - To use parallel first connection, select **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor**.
 - To use serial first connection, select **Serial first connection** and select a resistor value from the **Resistor values** drop-down list.
- **Toggle port URL:** Shows the URLs to activate and deactivate connected devices through the VAPIX® Application Programming Interface. It appears only when the port is configured as output.


Relays


- **Relay:** Turn on or off the relay.
- **Name:** Edit the text to rename the relay.
- **Direction:** Indicates that it is an output relay.
- **Toggle port URL:** Shows the URLs to activate and deactivate the relay through the VAPIX® Application Programming Interface.

Alarms

Device motion: Turn on to trigger an alarm in your system when it detects a movement of the device.




Casing open  : Turn on to trigger an alarm in your system when it detects an open door controller case. Turn off this setting for barebone door controllers.


External tamper  : Turn on to trigger an alarm in your system when it detects an external tamper. For example, when someone opens or closes the external cabinet.

- **Supervised input**  : Turn on to monitor the input state and configure the end-of-line resistors.
 - To use parallel first connection, select **Parallel first connection with a 22 K Ω parallel resistor and a 4.7 K Ω serial resistor**.
 - To use serial first connection, select **Serial first connection** and select a resistor value from the **Resistor values** drop-down list.

Power monitoring

Main unit

- **Power in:** Shows the status of power in including PoE, DC, DC Door 1–4, and DC Door 5–8 if applicable.
- **Power out**  : Shows the power out of all RS485 and all relays.
- **Temperature:** Shows the core temperature of the device.
- **Door 1–4**  : Shows the status and power usage of DC input Door 1–4 including power usage of all relays, all readers, and all REX.
- **Door 5–8**  : Shows the status and power usage of DC input Door 5–8 including power usage of all relays, all readers, and all REX.

Connected devices  : Shows the status, name, address, and the power usage of the connected devices including power usage of all relays, all RS485, and all AUX.

Peripherals

Sensors

Shows an overview of your connected sensors to AXIS A9210. You can connect up to 8 Modbus sensors directly on the RS485 port, or extend to 16 AXIS A9910 to have 64 Modbus sensors on a single AXIS A9210.



Add: Click to add a sensor.

Name: Enter a name for the sensor.

Sensor: Select the device the sensor is connected to.

RS485 port: Select the port the sensor is connected to.

Address: Enter the address of the sensor. If multidrop is used, enter the unique address between 1–247.

Type:

- Select **Custom**.
 - **Export template:** Click to download a JSON file. You can edit the file and upload it to the device later.
 - **Select configuration file:** Click to select a configuration file or drag it. You can edit, copy, download or print the configuration file.
- Select **Hugo** or **Tibbo**.
 - **Read data:** Set how often to read data from the sensor.
 - **Thresholds:** Set threshold values for available sensor features such as temperature, humidity, dew point, atmospheric pressure, or luminance.

Save: Click to save the configuration.

In the list of sensors:

- **Name:** Edit the text to rename the sensor.
- **Device/Port:** The Modbus ID and port number where the sensor is connected.
- **Type:** The type of measurement or function performed by the sensor, such as temperature, humidity, or luminance.
- **Model:** The model name of the sensor.
- **Last value:** The most recent reading from the sensor.
- **Last event:** The reason for the last triggered event, such as above or below the set limit for the selected parameter.
- **Status:** Indicates whether the sensor is currently online or offline.

Apps



Add app: Install a new app.

Find more apps: Find more apps to install. You will be taken to an overview page of Axis apps.



Allow unsigned apps : Turn on to allow installation of unsigned apps.



View the security updates in AXIS OS and ACAP apps.

Note

The device's performance might be affected if you run several apps at the same time.

Use the switch next to the app name to start or stop the app.

Open: Access the app's settings. The available settings depend on the application. Some applications don't have any settings.



The context menu can contain one or more of the following options:

- **Open-source license:** View information about open-source licenses used in the app.
- **App log:** View a log of the app events. The log is helpful when you contact support.
- **Activate license with a key:** If the app requires a license, you need to activate it. Use this option if your device doesn't have internet access.
If you don't have a license key, go to axis.com/products/analytics. You need a license code and the Axis product serial number to generate a license key.
- **Activate license automatically:** If the app requires a license, you need to activate it. Use this option if your device has internet access. You need a license code to activate the license.
- **Deactivate the license:** Deactivate the license to replace it with another license, for example, when you change from a trial license to a full license. If you deactivate the license, you also remove it from the device.
- **Settings:** Configure the parameters.
- **Delete:** Delete the app permanently from the device. If you don't deactivate the license first, it remains active.

System

Time and location

Date and time

The time format depends on the web browser's language settings.

Note

We recommend you synchronize the device's date and time with an NTP server.

Synchronization: Select an option for the device's date and time synchronization.

- **Automatic date and time (PTP):** Synchronize using the precision time protocol.
- **Automatic date and time (manual NTS KE servers):** Synchronize with the secure NTP key establishment servers connected to the DHCP server.
 - **Manual NTS KE servers:** Enter the IP address of one or two NTP servers. When you use two NTP servers, the device synchronizes and adapts its time based on input from both.
 - **Trusted NTS KE CA certificates:** Select the trusted CA certificates to use for secure NTS KE time synchronization, or leave at none.
 - **Max NTP poll time:** Select the maximum amount of time the device should wait before it polls the NTP server to get an updated time.
 - **Min NTP poll time:** Select the minimum amount of time the device should wait before it polls the NTP server to get an updated time.
- **Automatic date and time (NTP servers using DHCP):** Synchronize with the NTP servers connected to the DHCP server.
 - **Fallback NTP servers:** Enter the IP address of one or two fallback servers.
 - **Max NTP poll time:** Select the maximum amount of time the device should wait before it polls the NTP server to get an updated time.
 - **Min NTP poll time:** Select the minimum amount of time the device should wait before it polls the NTP server to get an updated time.
- **Automatic date and time (manual NTP servers):** Synchronize with NTP servers of your choice.
 - **Manual NTP servers:** Enter the IP address of one or two NTP servers. When you use two NTP servers, the device synchronizes and adapts its time based on input from both.
 - **Max NTP poll time:** Select the maximum amount of time the device should wait before it polls the NTP server to get an updated time.
 - **Min NTP poll time:** Select the minimum amount of time the device should wait before it polls the NTP server to get an updated time.
- **Custom date and time:** Manually set the date and time. Click **Get from system** to fetch the date and time settings once from your computer or mobile device.

Time zone: Select which time zone to use. Time will automatically adjust to daylight saving time and standard time.

- **DHCP:** Adopts the time zone of the DHCP server. The device must be connected to a DHCP server (v4 or v6) before you can select this option. If both versions are available, the device prefers IANA time zones over POSIX, and DHCPv4 over DHCPv6.
 - DHCPv4 uses Option 100 for POSIX time zones and Option 101 for IANA time zones.
 - DHCPv6 uses Option 41 for POSIX and Option 42 for IANA.
- **Manual:** Select a time zone from the drop-down list.

Note

The system uses the date and time settings in all recordings, logs, and system settings.

Device location

Enter where the device is located. Your video management system can use this information to place the device on a map.

- **Latitude:** Positive values are north of the equator.
- **Longitude:** Positive values are east of the prime meridian.
- **Heading:** Enter the compass direction that the device is facing. 0 is due north.
- **Label:** Enter a descriptive name for your device.
- **Save:** Click to save your device location.

Network

IPv4

Assign IPv4 automatically: Select IPv4 automatic IP (DHCP) to let the network assign your IP address, subnet mask, and router automatically, without manual configuration. We recommend using automatic IP assignment (DHCP) for most networks.

IP address: Enter a unique IP address for the device. Static IP addresses can be assigned at random within isolated networks, provided that each address is unique. To avoid conflicts, we recommend you contact your network administrator before you assign a static IP address.

Subnet mask: Enter the subnet mask to define what addresses are inside the local area network. Any address outside the local area network goes through the router.

Router: Enter the IP address of the default router (gateway) used to connect devices that are attached to different networks and network segments.

Fallback to static IP address if DHCP isn't available: Select if you want to add a static IP address to use as fallback if DHCP is unavailable and can't assign an IP address automatically.

Note

If DHCP isn't available and the device uses a static address fallback, the static address is configured with a limited scope.

IPv6

Assign IPv6 automatically: Select to turn on IPv6 and to let the network router assign an IP address to the device automatically.

Hostname

Assign hostname automatically: Select to let the network router assign a hostname to the device automatically.

Hostname: Enter the hostname manually to use as an alternative way of accessing the device. The server report and system log use the hostname. Allowed characters are A–Z, a–z, 0–9 and –.

Enable dynamic DNS updates: Allow your device to automatically update its domain name server records whenever its IP address changes.

Register DNS name: Enter a unique domain name that points to your device's IP address. Allowed characters are A–Z, a–z, 0–9 and –.

TTL: Time to Live (TTL) sets how long a DNS record stays valid before it needs to be updated.

DNS servers

Assign DNS automatically: Select to let the DHCP server assign search domains and DNS server addresses to the device automatically. We recommend automatic DNS (DHCP) for most networks.

Search domains: When you use a hostname that is not fully qualified, click **Add search domain** and enter a domain in which to search for the hostname the device uses.

DNS servers: Click **Add DNS server** and enter the IP address of the DNS server. This provides the translation of hostnames to IP addresses on your network.

Note

If DHCP is disabled, features that rely on automatic network configuration, such as hostname, DNS servers, NTP, and others, may stop working.

HTTP and HTTPS

HTTPS is a protocol that provides encryption for page requests from users and for the pages returned by the web server. The encrypted exchange of information is governed by the use of an HTTPS certificate, which guarantees the authenticity of the server.

To use HTTPS on the device, you must install an HTTPS certificate. Go to **System > Security** to create and install certificates.

Allow access through: Select if a user is allowed to connect to the device through the HTTP, HTTPS, or both HTTP and HTTPS protocols.

Note

If you view encrypted web pages through HTTPS, you might experience a drop in performance, especially when you request a page for the first time.

HTTP port: Enter the HTTP port to use. The device allows port 80 or any port in the range 1024–65535. If you are logged in as an administrator, you can also enter any port in the range 1–1023. If you use a port in this range, you get a warning.

HTTPS port: Enter the HTTPS port to use. The device allows port 443 or any port in the range 1024–65535. If you are logged in as an administrator, you can also enter any port in the range 1–1023. If you use a port in this range, you get a warning.

Certificate: Select a certificate to enable HTTPS for the device.

Network discovery protocols

Bonjour®: Turn on to allow automatic discovery on the network.

Bonjour name: Enter a friendly name to be visible on the network. The default name is the device name and MAC address.

UPnP®: Turn on to allow automatic discovery on the network.

UPnP name: Enter a friendly name to be visible on the network. The default name is the device name and MAC address.

WS-Discovery: Turn on to allow automatic discovery on the network.

LLDP and CDP: Turn on to allow automatic discovery on the network. Turning LLDP and CDP off can impact the PoE power negotiation. To resolve any issues with the PoE power negotiation, configure the PoE switch for hardware PoE power negotiation only.

One-click cloud connection

One-click cloud connection (O3C) together with an O3C service provides easy and secure internet access to live and recorded video from any location. For more information, see axis.com/end-to-end-solutions/hosted-services.

Allow O3C:

- **One-click:** This is the default option. To connect to O3C, press the control button on the device. Depending on the device model, either press and release or press and hold, until the status LED flashes. Register the device with the O3C service within 24 hours to enable **Always** and stay connected. If you don't register, the device will disconnect from O3C.
- **Always:** The device continuously attempts to connect to an O3C service over the internet. Once you register the device, it stays connected. Use this option if the control button is out of reach.
- **No:** Disconnects the O3C service.

Proxy settings: If needed, enter the proxy settings to connect to the proxy server.

Host: Enter the proxy server's address.

Port: Enter the port number used for access.

Login and Password: If needed, enter username and password for the proxy server.

Authentication method:

- **Basic:** This method is the most compatible authentication scheme for HTTP. It's less secure than the **Digest** method because it sends the username and password unencrypted to the server.
- **Digest:** This method is more secure because it always transfers the password encrypted across the network.
- **Auto:** This option lets the device select the authentication method depending on the supported methods. It prioritizes the **Digest** method over the **Basic** method.

Owner authentication key (OAK): Click **Get key** to fetch the owner authentication key. This is only possible if the device is connected to the internet without a firewall or proxy.

SNMP

The Simple Network Management Protocol (SNMP) allows remote management of network devices.

SNMP: Select the version of SNMP to use.

- **v1 and v2c:**
 - **Read community:** Enter the community name that has read-only access to all supported SNMP objects. The default value is **public**.
 - **Write community:** Enter the community name that has read or write access to all supported SNMP objects (except read-only objects). The default value is **write**.
 - **Activate traps:** Turn on to activate trap reporting. The device uses traps to send messages for important events or status changes to a management system. In the web interface, you can set up traps for SNMP v1 and v2c. Traps are automatically turned off if you change to SNMP v3 or turn off SNMP. If you use SNMP v3, you can set up traps through the SNMP v3 management application.
 - **Trap address:** Enter the IP address or host name of the management server.
 - **Trap community:** Enter the community to use when the device sends a trap message to the management system.
 - **Traps:**
 - **Cold start:** Sends a trap message when the device starts.
 - **Link up:** Sends a trap message when a link changes from down to up.
 - **Link down:** Sends a trap message when a link changes from up to down.
 - **Authentication failed:** Sends a trap message when an authentication attempt fails.

Note

All Axis Video MIB traps are enabled when you turn on SNMP v1 and v2c traps. For more information, see *AXIS OS Portal > SNMP*.

- **v3:** SNMP v3 is a more secure version, which provides encryption and secure passwords. To use SNMP v3, we recommend you to activate HTTPS, as the password is then sent through HTTPS. This also prevents unauthorized parties' access to unencrypted SNMP v1 and v2c traps. If you use SNMP v3, you can set up traps through the SNMP v3 management application.
 - **Privacy:** Select what encryption to use for protecting your SNMP data.
 - **Password for the account "initial":** Enter the SNMP password for the account named "initial". Although the password can be sent without activating HTTPS, we don't recommend it. The SNMP v3 password can only be set once, and preferably only when HTTPS is enabled. Once the password is set, the password field is no longer displayed. To set the password again, you must reset the device to factory default settings.

Security

Certificates

Certificates are used to authenticate devices on a network. The device supports two types of certificates:

- **Client/server certificates**
A client/server certificate validates the device's identity, and can be self-signed or issued by a Certificate Authority (CA). A self-signed certificate offers limited protection and can be used before a CA-issued certificate has been obtained.
- **CA certificates**
You can use a CA certificate to authenticate a peer certificate, for example to validate the identity of an authentication server when the device connects to a network protected by IEEE 802.1X. The device has several pre-installed CA certificates.

These formats are supported:


- Certificate formats: .PEM, .CER, and .PFX
- Private key formats: PKCS#1 and PKCS#12

Important

If you reset the device to factory default, all certificates are deleted. Any pre-installed CA certificates are reinstalled.



Add certificate : Click to add a certificate. A step-by-step guide opens up.



- **More**  : Show more fields to fill in or select.
- **Secure keystore**: Select to use **Trusted Execution Environment (SoC TEE)**, **Secure element** or **Trusted Platform Module 2.0** to securely store the private key. For more information on which secure keystore to select, go to help.axis.com/axis-os#cryptographic-support.
- **Key type**: Select the default or a different encryption algorithm from the drop-down list to protect the certificate.



The context menu contains:

- **Certificate information**: View an installed certificate's properties.
- **Delete certificate**: Delete the certificate.
- **Create certificate signing request**: Create a certificate signing request to send to a registration authority to apply for a digital identity certificate.

Secure keystore  :

- **Trusted Execution Environment (SoC TEE)**: Select to use SoC TEE for secure keystore.
- **Secure element (CC EAL6+, FIPS 140-3 Level 3)**  : Select to use secure element for secure keystore.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Level 2)**  : Select to use TPM 2.0 for secure keystore.

Network access control and encryption

IEEE 802.1x

IEEE 802.1x is an IEEE standard for port-based network admission control providing secure authentication of wired and wireless network devices. IEEE 802.1x is based on EAP (Extensible Authentication Protocol).

To access a network protected by IEEE 802.1x, network devices must authenticate themselves. The authentication is performed by an authentication server, typically a RADIUS server (for example, FreeRADIUS and Microsoft Internet Authentication Server).

IEEE 802.1AE MACsec

IEEE 802.1AE MACsec is an IEEE standard for media access control (MAC) security that defines connectionless data confidentiality and integrity for media access independent protocols.

Certificates

When configured without a CA certificate, server certificate validation is disabled and the device tries to authenticate itself regardless of what network it is connected to.

When using a certificate, in Axis' implementation, the device and the authentication server authenticate themselves with digital certificates using EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).

To allow the device to access a network protected through certificates, you must install a signed client certificate on the device.

Authentication method: Select an EAP type used for authentication.

Client certificate: Select a client certificate to use IEEE 802.1x. The authentication server uses the certificate to validate the client's identity.

CA certificates: Select CA certificates to validate the authentication server's identity. When no certificate is selected, the device tries to authenticate itself regardless of what network it is connected to.

EAP identity: Enter the user identity associated with the client certificate.

EAPOL version: Select the EAPOL version that is used in the network switch.

Use IEEE 802.1x: Select to use the IEEE 802.1x protocol.

These settings are only available if you use **IEEE 802.1x PEAP-MSCHAPv2** as the authentication method:

- **Password:** Enter the password for your user identity.
- **Peap version:** Select the Peap version that is used in the network switch.
- **Label:** Select 1 to use client EAP encryption; select 2 to use client PEAP encryption. Select the Label that the network switch uses when using Peap version 1.

These settings are only available if you use **IEEE 802.1ae MACsec (Static CAK/Pre-Shared Key)** as the authentication method:

- **Key agreement connectivity association key name:** Enter the connectivity association name (CKN). It must be 2 to 64 (divisible by 2) hexadecimal characters. The CKN must be manually configured in the connectivity association and must match on both ends of the link to initially enable MACsec.
- **Key agreement connectivity association key:** Enter the connectivity association key (CAK). It should be either 32 or 64 hexadecimal characters long. The CAK must be manually configured in the connectivity association and must match on both ends of the link to initially enable MACsec.

Prevent brute-force attacks

Blocking: Turn on to block brute-force attacks. A brute-force attack uses trial-and-error to guess login info or encryption keys.

Blocking period: Enter the number of seconds to block a brute-force attack.

Blocking conditions: Enter the number of authentication failures allowed per second before the block starts. You can set the number of failures allowed both on page level and device level.

Firewall

Firewall: Turn on to activate the firewall.

Default Policy: Select how you want the firewall to handle connection requests not covered by rules.

- **ACCEPT:** Allows all connections to the device. This option is set by default.
- **DROP:** Blocks all connections to the device.

To make exceptions to the default policy, you can create rules that allows or blocks connections to the device from specific addresses, protocols, and ports.

+ New rule: Click to create a rule.

Rule type:

- **FILTER:** Select to either allow or block connections from devices that match the criteria defined in the rule.
 - **Policy:** Select **Accept** or **Drop** for the firewall rule.
 - **IP range:** Select to specify a range of addresses to allow or block. Use IPv4/IPv6 in **Start** and **End**.
 - **IP address:** Enter an address that you want to allow or block. Use IPv4/IPv6 or CIDR format.
 - **Protocol:** Select a network protocol (TCP, UDP, or Both) to allow or block. If you select a protocol, you must also specify a port.
 - **MAC:** Enter the MAC address of a device that you want to allow or block.
 - **Port range:** Select to specify the range of ports to allow or block. Add them in **Start** and **End**.
 - **Port:** Enter a port number that you want to allow or block. Port numbers must be between 1 and 65535.
 - **Traffic type:** Select a traffic type that you want to allow or block.
 - **UNICAST:** Traffic from a single sender to a single recipient.
 - **BROADCAST:** Traffic from a single sender to all devices on the network.
 - **MULTICAST:** Traffic from one or more senders to one or more recipient.
- **LIMIT:** Select to accept connections from devices that match the criteria defined in the rule but apply limits to reduce excessive traffic.
 - **IP range:** Select to specify a range of addresses to allow or block. Use IPv4/IPv6 in **Start** and **End**.
 - **IP address:** Enter an address that you want to allow or block. Use IPv4/IPv6 or CIDR format.
 - **Protocol:** Select a network protocol (TCP, UDP, or Both) to allow or block. If you select a protocol, you must also specify a port.
 - **MAC:** Enter the MAC address of a device that you want to allow or block.
 - **Port range:** Select to specify the range of ports to allow or block. Add them in **Start** and **End**.
 - **Port:** Enter a port number that you want to allow or block. Port numbers must be between 1 and 65535.
 - **Unit:** Select the type of connections to allow or block.
 - **Period:** Select the time period related to **Amount**.
 - **Amount:** Set the maximum number of times a device is allowed to connect within the set **Period**. The maximum amount is 65535.
 - **Burst:** Enter the number of connections allowed to exceed the set **Amount** once during the set **Period**. Once the number has been reached, only the set amount during the set period is allowed.
 - **Traffic type:** Select a traffic type that you want to allow or block.
 - **UNICAST:** Traffic from a single sender to a single recipient.
 - **BROADCAST:** Traffic from a single sender to all devices on the network.

- **MULTICAST:** Traffic from one or more senders to one or more recipient.

Test rules: Click to test the rules that you have defined.

- **Test time in seconds:** Set a time limit for testing the rules.
- **Roll back:** Click to roll back the firewall to its previous state, before you have tested the rules.
- **Apply rules:** Click to activate the rules without testing. We don't recommend that you do this.

Custom signed AXIS OS certificate

To install test software or other custom software from Axis on the device, you need a custom signed AXIS OS certificate. The certificate verifies that the software is approved by both the device owner and Axis. The software can only run on a specific device which is identified by its unique serial number and chip ID. Only Axis can create custom signed AXIS OS certificates, since Axis holds the key to sign them.

Install: Click to install the certificate. You need to install the certificate before you install the software.



The context menu contains:

- **Delete certificate:** Delete the certificate.

Accounts

Accounts



Add account: Click to add a new account. You can add up to 100 accounts.

Account: Enter a unique account name.

New password: Enter a password for the account. Passwords must be 1 to 64 characters long. Only ASCII printable characters (code 32 to 126) are allowed in the password, for example, letters, numbers, punctuation, and some symbols.

Repeat password: Enter the same password again.

Privileges:

- **Administrator:** Has full access to all settings. Administrators can also add, update, and remove other accounts.
- **Operator:** Has access to all settings except:
 - All **System** settings.
- **Viewer:** Doesn't have access to change any settings.



The context menu contains:

Update account: Edit the account properties.

Delete account: Delete the account. You can't delete the root account.

Anonymous access

Allow anonymous viewing: Turn on to allow anyone access the device as a viewer without logging in with an account.

Allow anonymous PTZ operating  : Turn on to allow anonymous users to pan, tilt, and zoom the image.

SSH accounts



Add SSH account: Click to add a new SSH account.

- **Enable SSH:** Turn on to use SSH service.

Account: Enter a unique account name.

New password: Enter a password for the account. Passwords must be 1 to 64 characters long. Only ASCII printable characters (code 32 to 126) are allowed in the password, for example, letters, numbers, punctuation, and some symbols.

Repeat password: Enter the same password again.

Comment: Enter a comment (optional).



The context menu contains:

Update SSH account: Edit the account properties.

Delete SSH account: Delete the account. You can't delete the root account.

OpenID Configuration

Important

If you can't use OpenID to sign in, use the Digest or Basic credentials you used when you configured OpenID to sign in.

Client ID: Enter the OpenID username.

Outgoing Proxy: Enter the proxy address for the OpenID connection to use a proxy server.

Admin claim: Enter a value for the admin role.

Provider URL: Enter the web link for the API endpoint authentication. Format should be https://[insert URL]/well-known/openid-configuration

Operator claim: Enter a value for the operator role.

Require claim: Enter the data that should be in the token.

Viewer claim: Enter the value for the viewer role.

Remote user: Enter a value to identify remote users. This assists to display the current user in the device's web interface.

Scopes: Optional scopes that could be part of the token.

Client secret: Enter the OpenID password

Save: Click to save the OpenID values.

Enable OpenID: Turn on to close current connection and allow device authentication from the provider URL.

Events

Rules

A rule defines the conditions that triggers the product to perform an action. The list shows all the currently configured rules in the product.

Note

You can create up to 256 action rules.



Add a rule: Create a rule.

Name: Enter a name for the rule.

Wait between actions: Enter the minimum time (hh:mm:ss) that must pass between rule activations. It is useful if the rule is activated by, for example, day-night mode conditions, to avoid that small light changes during sunrise and sunset activate the rule repeatedly.

Condition: Select a condition from the list. A condition must be met for the device to perform an action. If multiple conditions are defined, all of them must be met to trigger the action. For information about specific conditions, see *Get started with rules for events*.

Use this condition as a trigger: Select to make this first condition function only as a starting trigger. It means that once the rule is activated, it remains active for as long as all the other conditions are met, no matter the state of the first condition. If you don't select this option, the rule will simply be active whenever all the conditions are met.

Invert this condition: Select if you want the condition to be the opposite of your selection.



Add a condition: Click to add an additional condition.

Action: Select an action from the list and enter its required information. For information about specific actions, see *Get started with rules for events*.

Recipients

You can set up your device to notify recipients about events or send files.

Note

If you set up your device to use FTP or SFTP, don't change or remove the unique sequence number that's added to the file names. If you do that, only one image per event can be sent.

The list shows all the recipients currently configured in the product, along with information about their configuration.

Note



You can create up to 20 recipients.



Add a recipient: Click to add a recipient.

Name: Enter a name for the recipient.

Type: Select from the list:

- **FTP** 
 - **Host:** Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
 - **Port:** Enter the port number used by the FTP server. The default is 21.
 - **Folder:** Enter the path to the directory where you want to store files. If this directory doesn't already exist on the FTP server, you will get an error message when uploading files.
 - **Username:** Enter the username for the login.
 - **Password:** Enter the password for the login.
 - **Use temporary file name:** Select to upload files with temporary, automatically generated filenames. The files get renamed to the desired names when the upload completes. If the upload is aborted/interrupted, you don't get any corrupt files. However, you probably still get the temporary files. This way you know that all files that have the desired name are correct.
 - **Use passive FTP:** Under normal circumstances, the product simply requests the target FTP server to open the data connection. The device actively initiates both the FTP control and data connections to the target server. This is normally needed if there is a firewall between the device and the target FTP server.
- **HTTP**
 - **URL:** Enter the network address to the HTTP server and the script that will handle the request. For example, `http://192.168.254.10/cgi-bin/notify.cgi`.
 - **Username:** Enter the username for the login.
 - **Password:** Enter the password for the login.
 - **Proxy:** Turn on and enter the required information if a proxy server must be passed to connect to the HTTP server.
- **HTTPS**
 - **URL:** Enter the network address to the HTTPS server and the script that will handle the request. For example, `https://192.168.254.10/cgi-bin/notify.cgi`.
 - **Validate server certificate:** Select to validate the certificate that was created by HTTPS server.
 - **Username:** Enter the username for the login.
 - **Password:** Enter the password for the login.
 - **Proxy:** Turn on and enter the required information if a proxy server must be passed to connect to the HTTPS server.
- **Network storage** 

You can add network storage such as NAS (network-attached storage) and use it as a recipient to store files. The files are stored in the Matroska (MKV) file format.

 - **Host:** Enter the IP address or hostname for the network storage.
 - **Share:** Enter the name of the share on the host.
 - **Folder:** Enter the path to the directory where you want to store files.
 - **Username:** Enter the username for the login.
 - **Password:** Enter the password for the login.

- **SFTP** 
 - **Host:** Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
 - **Port:** Enter the port number used by the SFTP server. The default is 22.
 - **Folder:** Enter the path to the directory where you want to store files. If this directory doesn't already exist on the SFTP server, you will get an error message when uploading files.
 - **Username:** Enter the username for the login.
 - **Password:** Enter the password for the login.
 - **SSH host public key type (MD5):** Enter the fingerprint of the remote host's public key (a 32-digit hexadecimal string). The SFTP client supports SFTP servers using SSH-2 with RSA, DSA, ECDSA, and ED25519 host key types. RSA is the preferred method during negotiation, followed by ECDSA, ED25519, and DSA. Make sure to enter the right MD5 host key that is used by your SFTP server. While the Axis device supports both MD5 and SHA-256 hash keys, we recommend using SHA-256 due to stronger security over MD5. For more information on how to configure an SFTP server with an Axis device, go to the *AXIS OS Portal*.
 - **SSH host public key type (SHA256):** Enter the fingerprint of the remote host's public key (a 43-digit Base64 encoded string). The SFTP client supports SFTP servers using SSH-2 with RSA, DSA, ECDSA, and ED25519 host key types. RSA is the preferred method during negotiation, followed by ECDSA, ED25519, and DSA. Make sure to enter the right MD5 host key that is used by your SFTP server. While the Axis device supports both MD5 and SHA-256 hash keys, we recommend using SHA-256 due to stronger security over MD5. For more information on how to configure an SFTP server with an Axis device, go to the *AXIS OS Portal*.
 - **Use temporary file name:** Select to upload files with temporary, automatically generated filenames. The files get renamed to the desired names when the upload completes. If the upload is aborted or interrupted, you don't get any corrupt files. However, you probably still get the temporary files. This way, you know that all files that have the desired name are correct.
- **SIP or VMS**  :
 - SIP:** Select to make a SIP call.
 - VMS:** Select to make a VMS call.
 - **From SIP account:** Select from the list.
 - **To SIP address:** Enter the SIP address.
 - **Test:** Click to test that your call settings works.
- **Email**
 - **Send email to:** Enter the email address to send emails to. To enter multiple addresses, use commas to separate them.
 - **Send email from:** Enter the email address of the sending server.
 - **Username:** Enter the username for the mail server. Leave this field empty if the mail server does not require authentication.
 - **Password:** Enter the password for the mail server. Leave this field empty if the mail server does not require authentication.
 - **Email server (SMTP):** Enter the name of the SMTP server, for example, smtp.gmail.com, smtp.mail.yahoo.com.
 - **Port:** Enter the port number for the SMTP server, using values in the range 0-65535. The default value is 587.
 - **Encryption:** To use encryption, select either SSL or TLS.
 - **Validate server certificate:** If you use encryption, select to validate the identity of the device. The certificate can be self-signed or issued by a Certificate Authority (CA).

- **POP authentication:** Turn on to enter the name of the POP server, for example, pop.gmail.com.

Note

Some email providers have security filters that prevent users from receiving or viewing large amount of attachments, from receiving scheduled emails and similar. Check the email provider's security policy to avoid your email account being locked or missing out on your expected emails.

- **TCP**
 - **Host:** Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
 - **Port:** Enter the port number used to access the server.

Test: Click to test the setup.



The context menu contains:

View recipient: Click to view all the recipient details.

Copy recipient: Click to copy a recipient. When you copy, you can make changes to the new recipient.

Delete recipient: Click to delete the recipient permanently.

Schedules

Schedules and pulses can be used as conditions in rules. The list shows all the schedules and pulses currently configured in the product, along with information about their configuration.



Add schedule: Click to create a schedule or pulse.

Manual triggers

You can use the manual trigger to manually trigger a rule. The manual trigger can, for example, be used to validate actions during product installation and configuration.

MQTT

MQTT (Message Queuing Telemetry Transport) is a standard messaging protocol for the Internet of Things (IoT). It was designed for simplified IoT integration and is used in a wide variety of industries to connect remote devices with a small code footprint and minimal network bandwidth. The MQTT client in Axis device software can simplify integration of data and events produced in the device to systems which are not video management software (VMS).

Set up the device as an MQTT client. MQTT communication is based on two entities, the clients and the broker. The clients can send and receive messages. The broker is responsible for routing messages between clients.

You can learn more about MQTT in *AXIS OS Knowledge base*.

ALPN

ALPN is a TLS/SSL extension that allows for the selection of an application protocol during the handshake phase of the connection between the client and server. This is used to enable MQTT traffic over the same port that is used for other protocols, such as HTTP. In some cases, there might not be a dedicated port open for MQTT communication. A solution in such cases is to use ALPN to negotiate the use of MQTT as the application protocol on a standard port, allowed by the firewalls.

MQTT client

Connect: Turn on or off the MQTT client.

Status: Shows the current status of the MQTT client.

Broker

Host: Enter the hostname or IP address of the MQTT server.

Protocol: Select which protocol to use.

Port: Enter the port number.

- 1883 is the default value for **MQTT over TCP**
- 8883 is the default value for **MQTT over SSL**
- 80 is the default value for **MQTT over WebSocket**
- 443 is the default value for **MQTT over WebSocket Secure**

ALPN protocol: Enter the ALPN protocol name provided by your MQTT broker provider. This is only applicable with MQTT over SSL and MQTT over WebSocket Secure.

Username: Enter the username that the client will use to access the server.

Password: Enter a password for the username.

Client ID: Enter a client ID. The client identifier is sent to the server when the client connects to it.

Clean session: Controls the behavior at connection and disconnection time. When selected, the state information is discarded at connect and disconnect.

HTTP proxy: A URL with a maximum length of 255 bytes. You can leave the field empty if you don't want to use an HTTP proxy.

HTTPS proxy: A URL with a maximum length of 255 bytes. You can leave the field empty if you don't want to use an HTTPS proxy.

Keep alive interval: Enables the client to detect when the server is no longer available without having to wait for the long TCP/IP timeout.

Timeout: The time interval in seconds to allow a connect to complete. Default value: 60

Device topic prefix: Used in the default values for the topic in the connect message and LWT message on the MQTT client tab, and in the publication conditions on the **MQTT publication** tab.

Reconnect automatically: Specifies whether the client should reconnect automatically after a disconnect.

Connect message

Specifies if a message should be sent out when a connection is established.

Send message: Turn on to send messages.

Use default: Turn off to enter your own default message.

Topic: Enter the topic for the default message.

Payload: Enter the content for the default message.

Retain: Select to keep the state of client on this Topic

QoS: Change the QoS layer for the packet flow.

Last Will and Testament message

The Last Will Testament (LWT) lets a client provide a testament along with its credentials when connecting to the broker. If the client disconnects ungracefully at some point later (maybe because his power source died), it

can let the broker deliver a message to other clients. This LWT message has the same form as an ordinary message and gets routed via the same mechanics.

Send message: Turn on to send messages.

Use default: Turn off to enter your own default message.

Topic: Enter the topic for the default message.

Payload: Enter the content for the default message.

Retain: Select to keep the state of client on this Topic

QoS: Change the QoS layer for the packet flow.

MQTT publication

Use default topic prefix: Select to use the default topic prefix, that is defined in the device topic prefix in the MQTT client tab.

Include condition: Select to include the topic that describes the condition in the MQTT topic.

Include namespaces: Select to include ONVIF topic namespaces in the MQTT topic.

Include serial number: Select to include the device's serial number in the MQTT payload.



Add condition: Click to add a condition.

Retain: Defines which MQTT messages are sent as retained.

- **None:** Send all messages as non-retained.
- **Property:** Send only stateful messages as retained.
- **All:** Send both stateful and stateless messages as retained.

QoS: Select the desired level for the MQTT publication.

MQTT subscriptions



Add subscription: Click to add a new MQTT subscription.

Subscription filter: Enter the MQTT topic that you want to subscribe to.

Use device topic prefix: Add the subscription filter as prefix to the MQTT topic.

Subscription type:

- **Stateless:** Select to convert MQTT messages into a stateless message.
- **Stateful:** Select to convert MQTT messages into a condition. The payload is used as the state.

QoS: Select the desired level for the MQTT subscription.

Logs

Reports and logs

Reports

- **View the device server report:** View information about the product status in a pop-up window. The Access Log is automatically included in the Server Report.
- **Download the device server report:** It creates a .zip file that contains a complete server report text file in UTF-8 format, as well as a snapshot of the current live view image. Always include the server report .zip file when you contact support.
- **Download the crash report:** Download an archive with detailed information about the server's status. The crash report contains information that is in the server report as well as detailed debug information. This report might contain sensitive information such as network traces. It can take several minutes to generate the report.

Logs

- **View the system log:** Click to show information about system events such as device startup, warnings, and critical messages.
- **View the access log:** Click to show all failed attempts to access the device, for example, when a wrong login password is used.
- **View the audit log:** Click to show information about user and system activities, for example, successful or failed authentications and configurations.

Network trace

Important

A network trace file might contain sensitive information, for example certificates or passwords.

A network trace file can help you troubleshoot problems by recording activity on the network.

Trace time: Select the duration of the trace in seconds or minutes, and click **Download**.

Remote system log

Syslog is a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, which indicates the software type generating the message, and assigned a severity level.



Server: Click to add a new server.

Host: Enter the hostname or IP address of the server.

Format: Select which syslog message format to use.

- Axis
- RFC 3164
- RFC 5424

Protocol: Select the protocol to use:

- UDP (Default port is 514)
- TCP (Default port is 601)
- TLS (Default port is 6514)

Port: Edit the port number to use a different port.

Severity: Select which messages to send when triggered.

Type: Select the type of logs you want to send.

Test server setup: Send a test message to all servers before you save the settings.

CA certificate set: See the current settings or add a certificate.

Plain config

Plain config is for advanced users with experience of Axis device configuration. Most parameters can be set and edited from this page.

Maintenance

Restart: Restart the device. This does not affect any of the current settings. Running applications restart automatically.

Restore: Return most settings to the factory default values. Afterwards you must reconfigure the device and apps, reinstall any apps that didn't come preinstalled, and recreate any events and presets.

Important

The only settings saved after restore are:

- Boot protocol (DHCP or static)
- Static IP address
- Default router
- Subnet mask
- 802.1X settings
- QoS settings
- DNS server IP address

Factory default: Return all settings to the factory default values. Afterwards you must reset the IP address to make the device accessible.

Note

All Axis device software is digitally signed to ensure that you only install verified software on your device. This further increases the overall minimum cybersecurity level of Axis devices. For more information, see the white paper "Axis Edge Vault" at axis.com.

AXIS OS upgrade: Upgrade to a new AXIS OS version. New releases can contain improved functionality, bug fixes, and completely new features. We recommend you to always use the latest AXIS OS release. To download the latest release, go to axis.com/support.

When you upgrade, you can choose between three options:

- **Standard upgrade:** Upgrade to the new AXIS OS version.
- **Factory default:** Upgrade and return all settings to the factory default values. When you choose this option, you can't revert to the previous AXIS OS version after the upgrade.
- **Automatic rollback:** Upgrade and confirm the upgrade within the set time. If you don't confirm, the device reverts to the previous AXIS OS version.

AXIS OS rollback: Revert to the previously installed AXIS OS version.

Learn more

Analytics and apps

With analytics and apps you can get more out of your Axis device. AXIS Camera Application Platform (ACAP) is an open platform that makes it possible for third parties to develop analytics and other apps for Axis devices. Apps can be preinstalled on the device, available for download for free, or for a license fee.

To find the user manuals for Axis analytics and apps, go to help.axis.com.

AXIS Door Monitoring

This application monitors the door status, showing whether the door is open or closed, and if it stays open for too long. For example, use this application on a fire safety door that doesn't require a lock but where you need to know if it is open.

A regular door has a door position sensor, REX, along with locks and readers, which requires a door controller.

A monitoring door requires only a door position sensor and REX, and can be monitored using a network I/O relay module. Each network I/O relay module can connect up to five monitoring doors.

Limitations

The application is only available on AXIS A9210. REX can only be connected to I/O 1 and I/O 2, not possible to configure REX on I 3, I 4, or I 5.

AXIS Monitoring Door Configuration

Name	Description
Door	The number of the door.
DPS input	The DPS input for the door.
REX input	The REX input for the door.
Door open too long time (sec)	The number of seconds the door is allowed to stay open.
Access time (sec)	The number of seconds the door shall remain unlocked after access has been granted.
State	The state of the door.

Cybersecurity

For product-specific information about cybersecurity, see the product's datasheet at axis.com.

For in-depth information about cybersecurity in AXIS OS, read the *AXIS OS Hardening guide*.

Axis Edge Vault

Axis Edge Vault provides a hardware-based cybersecurity platform that safeguards the Axis device. It offers features to guarantee the device's identity and integrity and to protect your sensitive information from unauthorized access. It builds on a strong foundation of cryptographic computing modules (secure element and TPM) and SoC security (TEE and secure boot), combined with expertise in edge device security.

Signed OS

Signed OS is implemented by the software vendor signing the AXIS OS image with a private key. When the signature is attached to the operating system, the device will validate the software before installing it. If the device detects that the integrity of the software is compromised, the AXIS OS upgrade will be rejected.

Secure boot

Secure boot is a boot process that consists of an unbroken chain of cryptographically validated software, starting in immutable memory (boot ROM). Being based on the use of signed OS, secure boot ensures that a device can boot only with authorized software.

Secure keystore

A tamper-protected environment for the protection of private keys and secure execution of cryptographic operations. It prevents unauthorized access and malicious extraction in the event of a security breach. Depending on security requirements, an Axis device can have either one or multiple hardware-based cryptographic computing modules, which provide a hardware-protected secure keystore. Depending on security requirements, an Axis device can have either one or multiple hardware-based cryptographic computing modules, like a TPM 2.0 (Trusted Platform Module) or a secure element, and/or a TEE (Trusted Execution Environment), which provide a hardware-protected secure keystore. Furthermore, selected Axis products feature a FIPS 140-2 Level 2-certified secure keystore.

Axis device ID

Being able to verify the origin of the device is key to establishing trust in the device identity. During production, devices with Axis Edge Vault are assigned a unique, factory-provisioned, and IEEE 802.1AR-compliant Axis device ID certificate. This works like a passport to prove the origin of the device. The device ID is securely and permanently stored in the secure keystore as a certificate signed by Axis root certificate. The device ID can be leveraged by the customer's IT infrastructure for automated secure device onboarding and secure device identification

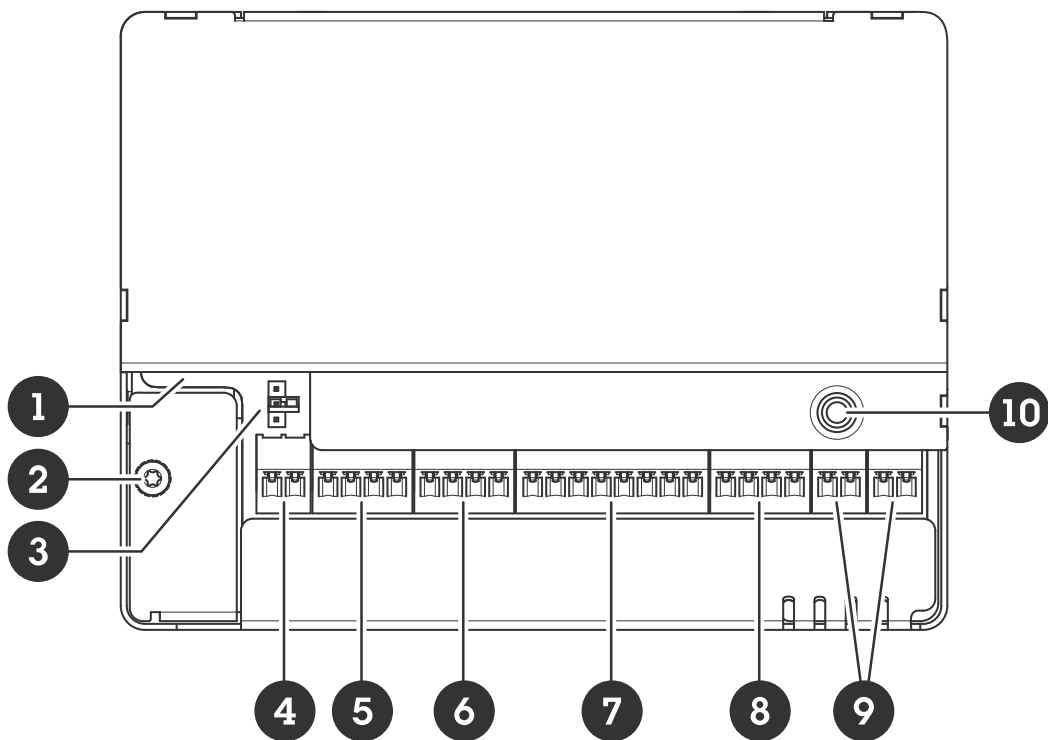
Encrypted file system

The secure keystore prevents the malicious exfiltration of information and prevents configuration tampering by enforcing strong encryption upon the file system. This ensures no data stored in the file system can be extracted or tampered with when the device is not in use, unauthenticated access to the device is achieved and/or the Axis device is stolen. During the secure boot process, the read-write filesystem is decrypted and can be mounted and used by the Axis device.

To learn more about the cybersecurity features in Axis devices, go to axis.com/learning/white-papers and search for cybersecurity.

Specifications

Product overview



- 1 Network connector
- 2 Grounding position
- 3 Relay jumper
- 4 Power connector
- 5 Relay connector
- 6 Input 1 connector
- 7 RS485 and I/O connector
- 8 I/O connector
- 9 Input 2 connector
- 10 Control button

LED indicators

LED	Color	Indication
Status	Green	Steady green for normal operation.
	Amber	Steady during startup and when restoring settings.
	Red	Slow flash for failed upgrade.
Network	Green	Steady for connection to a 100 MBit/s network. Flashes for network activity.
	Amber	Steady for connection to a 10 MBit/s network. Flashes for network activity.
	Unlit	No network connection.
Power	Green	Normal operation.

	Amber	Flashes green/amber during firmware upgrade.
Relay	Green	Relay active. ¹
	Unlit	Relay inactive.

Buttons

Control button

The control button is used for:

- Resetting the product to factory default settings. See *Reset to factory default settings, on page 42*.
- Connecting to a one-click cloud connection (O3C) service over the internet. To connect, press and release the button, then wait for the status LED to flash green three times.

Connectors

Network connector

RJ45 Ethernet connector with Power over Ethernet Plus (PoE+).

UL: Power over Ethernet (PoE) shall be over Ethernet IEEE 802.3af/802.3at Type 1 Class 3 or Power over Ethernet Plus (PoE+) IEEE 802.3at Type 2 Class 4 power limited injector that provides 44–57 V DC, 15.4 W / 30 W. Power over Ethernet (PoE) has been evaluated by UL with AXIS T8133 Midspan 30 W 1-port.

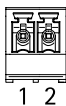
Power priority

This device can be powered by either PoE or DC input. See *Network connector, on page 36* and *Power connector, on page 36*.

- When PoE and DC are both connected before the device is powered, PoE is used for powering.
- PoE and DC are both connected and PoE is currently powering. When PoE is lost, the device uses DC for powering without restart.
- PoE and DC are both connected and DC is currently powering. When DC is lost, the device restarts and uses PoE for powering.
- When DC is used during startup and PoE is connected after the device has started, DC is used for powering.
- When PoE is used during startup and DC is connected after the device has started, PoE is used for powering.

Power connector

2-pin terminal block for DC power input. Use a Safety Extra Low Voltage (SELV) compliant limited power source (LPS) with either a rated output power limited to ≤ 100 W or a rated output current limited to ≤ 5 A.



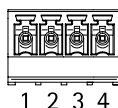
1. Relay is active when COM is connected to NO.

Function	Pin	Notes	Specifications
DC ground (GND)	1		0 V DC
DC input	2	For powering the device when not using Power over Ethernet. Note: This pin can only be used as power in.	12 V DC, max 36 W

UL: DC power to be supplied by a UL 603 listed power supply, depending on application, with appropriate ratings.

Relay connector

One 4-pin terminal block for form C relays that can be used, for example, to control a lock or an interface to a gate. If used with an inductive load, for example a lock, connect a diode in parallel with the load to protect against voltage transients.



Function	Pin	Notes	Specifications
DC ground (GND)	1		0 V DC
NO	2	Normally open. For connecting relay devices. Connect a fail-secure lock between NO and DC ground. The two relay pins are galvanically separated from the rest of the circuitry if the jumpers are not used.	Max current = 2 A Max voltage = 30 V DC
COM	3	Common	
NC	4	Normally closed. For connecting relay devices. Connect a fail-safe lock between NC and DC ground. The two relay pins are galvanically separated from the rest of the circuitry if the jumpers are not used.	

Relay power jumper

When the relay power jumper is fitted, it connects 12 V DC or 24 V DC to the relay COM pin.

It can be used to connect a lock between the GND and NO, or GND and NC pins.

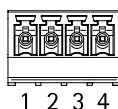
Power source	Max power at 12 V DC	Max power at 24 V DC
DC IN	2 000 mA	1 000 mA

PoE	350 mA	150 mA
PoE+	1100 mA	500 mA

Input 1 connector

One 4-pin terminal block for input.

It supports supervision with end of line resistors. If the connection is interrupted, an alarm is triggered. To use supervised inputs, install end of line resistors. Use the connection diagram for supervised inputs. See *Supervised inputs*, on page 40.



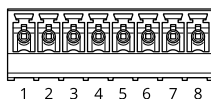
Function	Pin	Notes	Specifications
DC ground	1, 3		0 V DC
Input	2, 4	Digital input or supervised input – Connect to pin 1 or 3 respectively to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC

Important

The qualified cable length is up to 200 m (656 ft) if the following cable requirement is met: AWG 24.

RS485 and I/O connector

One 8-pin terminal block including 4-pin RS485 and 4-pin I/O.



RS485

Function	Pin	Note	Specifications
DC ground (GND)	1		0 V DC
DC output (+12 V)	2	Supplies power to auxiliary devices, for example, Modbus sensors.	12 V DC, max 200 mA
A	3		
B	4		

I/O

Function	Pin	Note	Specifications
Digital output	5	If used with an inductive load, for example a relay, connect a diode in parallel with the load to protect against voltage transients.	0 to max 30 V DC, open drain, 100 mA

Digital output	6	If used with an inductive load, for example a relay, connect a diode in parallel with the load to protect against voltage transients.	0 to max 30 V DC, open drain, 100 mA
Input	7	Digital input or supervised input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC
Digital output	8	If used with an inductive load, for example a relay, connect a diode in parallel with the load to protect against voltage transients.	0 to max 30 V DC, open drain, 100 mA

Important

- The qualified cable length for RS485 is up to 1000 m (3281 ft) if the following cable requirements are met: 1 twisted pair with shield, AWG 24, 120 ohm impedance.
- The qualified cable length for I/O is up to 200 m (656 ft).

I/O connector

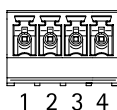
Use the auxiliary connector with external devices in combination with, for example, motion detection, event triggering, and alarm notifications. In addition to the 0 V DC reference point and power (DC output), the auxiliary connector provides the interface to:

Digital input – For connecting devices that can toggle between an open and closed circuit, for example PIR sensors, door/window contacts, and glass break detectors.

Supervised input – Enables possibility to detect tampering on a digital input.

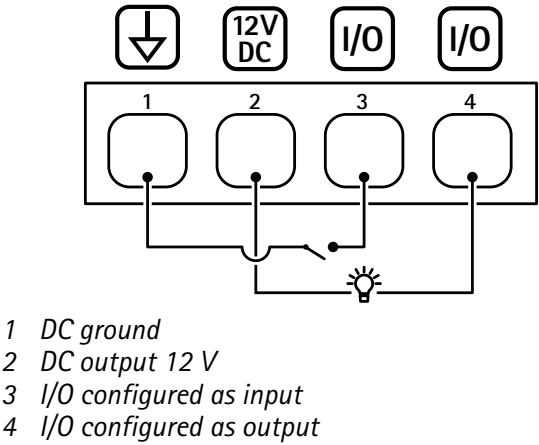
Digital output – For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface or from the product's webpage.

4-pin terminal block



Function	Pin	Notes	Specifications
DC ground	1		0 V DC
DC output	2	Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	12 V DC Max load = 50 mA in total
Configurable (Input or Output)	3–4	Digital input or supervised input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. To use supervised input, install end-of-line resistors. See connection diagram for information about how to connect the resistors.	0 to max 30 V DC

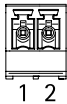
		Digital output – Internally connected to pin 1 (DC ground) when active, and floating (unconnected) when inactive. If used with an inductive load, e.g., a relay, connect a diode in parallel with the load, to protect against voltage transients. I/Os are capable of driving 12 V DC, 50 mA (combined max) external load, if internal 12 V DC output (pin 2) is used. In the case of using open drain connections in combination with an external power supply, then the I/Os can manage DC supply of 0–30 V DC, 100 mA each.	0 to max 30 V DC, open drain, 100 mA
--	--	---	--------------------------------------



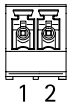
Input 2 connector

Two 2-pin terminal blocks for external devices, for example glass break or fire detectors.

UL: The connector has not been evaluated by UL for burglar or fire alarm use.



Function	Pin	Notes	Specifications
DC ground	1		0 V DC
Input	2	Digital input or supervised input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC



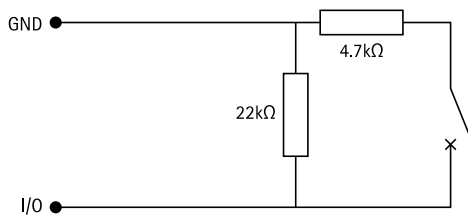
Function	Pin	Notes	Specifications
DC ground	1		0 V DC
Input	2	Digital input or supervised input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC

Supervised inputs

To use supervised inputs, install end of line resistors according to the diagram below.

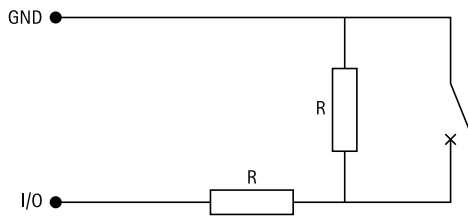
Parallel first connection

The resistor values must be 4.7 k Ω and 22 k Ω .



Serial first connection

The resistor values must be the same and possible values are 1 k Ω , 2.2 k Ω , 4.7 k Ω and 10 k Ω , 1%, 1/4 watt standard.



Note

It is recommended to use twisted and shielded cables. Connect shielding to 0 V DC.

Status	Description
Open	The supervised switch is in open mode.
Closed	The supervised switch is in closed mode.
Short	The I/O or Input 1-5 cable is short circuit to GND.
Cut	The I/O or Input 1-5 cable is cut and left open with no current path to GND.

Troubleshooting

Reset to factory default settings

Important

Reset to factory default should be used with caution. A reset to factory default resets all settings, including the IP address, to the factory default values.

To reset the product to the factory default settings:

1. Disconnect power from the product.
2. Press and hold the control button while reconnecting power. See *Product overview*, on page 35.
3. Keep the control button pressed for 25 seconds until the status LED indicator turns amber for the second time.
4. Release the control button. The process is complete when the status LED indicator turns green. If no DHCP server is available on the network, the device IP address will default to one of the following:
 - Devices with AXIS OS 12.0 and later: Obtained from the link-local address subnet (169.254.0.0/16)
 - Devices with AXIS OS 11.11 and earlier: 192.168.0.90/24
5. Use the installation and management software tools, assign an IP address, set the password, and access the product.

You can also reset parameters to factory default through the device's web interface. Go to **Maintenance > Factory default** and click **Default**.

AXIS OS options

Axis offers device software management according to either the active track or the long-term support (LTS) tracks. Being on the active track means continuously getting access to all the latest product features, while the LTS tracks provide a fixed platform with periodic releases focused mainly on bug fixes and security updates.

Using AXIS OS from the active track is recommended if you want to access the newest features, or if you use Axis end-to-end system offerings. The LTS tracks are recommended if you use third-party integrations, which are not continuously validated against the latest active track. With LTS, the products can maintain cybersecurity without introducing any significant functional changes or affecting any existing integrations. For more detailed information about Axis device software strategy, go to axis.com/support/device-software.

Check the current AXIS OS version

AXIS OS determines the functionality of our devices. When you troubleshoot a problem, we recommend that you to start by checking the current AXIS OS version. The latest version might contain a correction that fixes your particular problem.

To check the current AXIS OS version:

1. Go to the device's web interface > **Status**.
2. Under **Device info**, see the AXIS OS version.

Upgrade AXIS OS

Important

- When you upgrade the device software, your preconfigured and customized settings are saved. Axis Communications AB can't guarantee that the settings are saved, even if the features are available in the new AXIS OS version.
- Starting from AXIS OS 12.6, you must install every LTS version between your device's current version and the target version. For example, if the currently installed device software version is AXIS OS 11.2, you

have to install the LTS version AXIS OS 11.11 before you can upgrade the device to AXIS OS 12.6. For more information, see *AXIS OS Portal: Upgrade path*.

- Make sure the device remains connected to the power source throughout the upgrade process.

Note

- When you upgrade the device with the latest AXIS OS version in the active track, the product receives the latest functionality available. Always read the upgrade instructions and release notes available with each new release before you upgrade. To find the latest AXIS OS version and the release notes, go to axis.com/support/device-software.
1. Download the AXIS OS file to your computer, available free of charge at axis.com/support/device-software.
 2. Log in to the device as an administrator.
 3. Go to **Maintenance > AXIS OS upgrade** and click **Upgrade**.

When the upgrade has finished, the product restarts automatically.

Technical problems and possible solutions

Problems upgrading AXIS OS

AXIS OS upgrade failed

If the upgrade fails, the device reloads the previous version. The most common reason is that the wrong AXIS OS file has been uploaded. Check that the name of the AXIS OS file corresponds to your device and try again.

Problems after AXIS OS upgrade

If you experience problems after the upgrade, roll back to the previously installed version from the **Maintenance** page.

Problems setting the IP address

Can't set the IP address

- If the IP address intended for the device and the IP address of the computer used to access the device are located on different subnets, you can't set the IP address. Contact your network administrator to obtain an IP address.
- The IP address could be in use by another device. To check:
 1. Disconnect the Axis device from the network.
 2. In a Command/DOS window, type `ping` and the IP address of the device.
 3. If you receive: `Reply from <IP address>: bytes=32; time=10...` this means that the IP address might already be in use by another device on the network. Obtain a new IP address from the network administrator and reinstall the device.
 4. If you receive: `Request timed out`, this means that the IP address is available for use with the Axis device. Check all cabling and reinstall the device.
- There could be a possible IP address conflict with another device on the same subnet. The static IP address in the Axis device is used before the DHCP server sets a dynamic address. This means that if the same default static IP address is also used by another device, there could be problems accessing the device.

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 42*.

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 required, you can assign a static IP address manually. For instructions, go to axis.com/support.

Certificate error when using IEEE 802.1X

For authentication to work properly, the date and time settings in the Axis device must be synchronized with an NTP server. Go to **System > Date and time**.

The browser isn't supported

For a list of recommended browsers, see *Browser support, on page 2*.

Can't access the device externally

To access the device externally, we recommend you to use one of the following applications for Windows®:

- AXIS Camera Station Pro: 90-day trial version free of charge, ideal for small to mid-size systems.

For instructions and download, go to axis.com/vms.

Problems with MQTT

Can't connect over port 8883 with MQTT over SSL

The firewall blocks traffic that uses port 8883 since it's regarded insecure.

In some cases the server/broker might not provide a specific port for MQTT communication. It might still be possible to use MQTT over a port normally used for HTTP/HTTPS traffic.

- If the server/broker supports WebSocket/WebSocket Secure (WS/WSS), typically on port 443, use this protocol instead. Check with the server/broker provider to see if WS/WSS is supported and which port and basepath to use.
- If the server/broker supports ALPN, the use of MQTT can be negotiated over an open port, such as 443. Check with your server/broker provider to see if ALPN is supported and which ALPN protocol and port to use.

If you can't find what you're looking for here, try the troubleshooting section at axis.com/support.

Contact support

If you need more help, go to axis.com/support.

T10202445

2026-02 (M6.2)

© 2023 Axis Communications AB