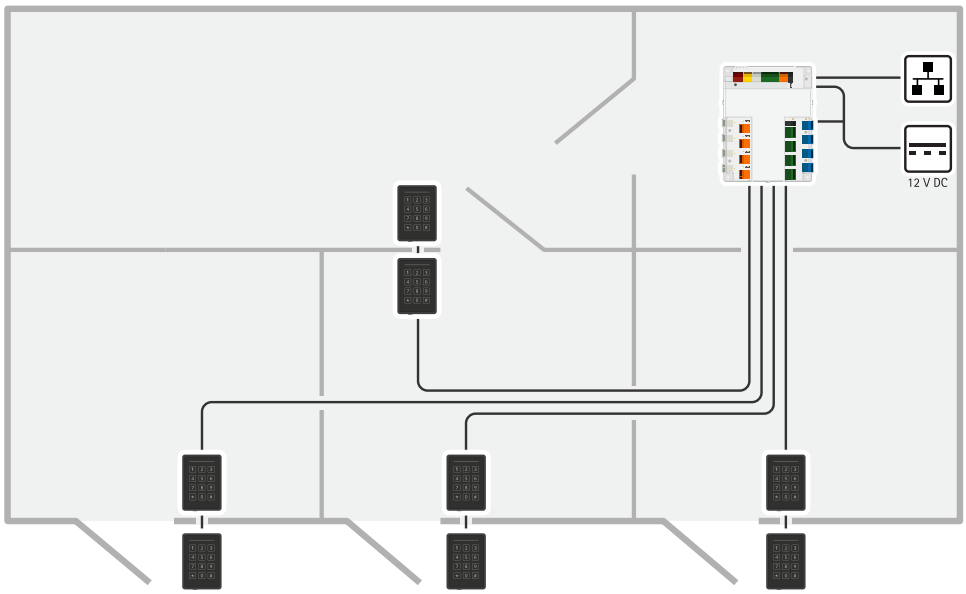
AXIS A1710-B Network Door Controller

User manual

Table of Contents

Solution overview



The network door controller can easily be connected to your existing IP network. Each network door controller can power and control up to 8 readers and 4 locks.

Installation

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 6*.

For descriptions of all the controls and options in the device's web interface, see *The web interface, on page 9*.

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 7*.
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 43*.

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 43*.
   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

For how to configure your device, see *AXIS Camera Station user manual* or third-party solutions.

Add AXIS A9910

- In the door controller's web interface, go to **Device > I/Os and relays**.
- Click **Add encryption key**.
- If you have generated the encryption key before, enter the key and click **OK**.
- To generate an encryption key:
  - Click **Generate key**.
  - Click **Export key** to save the key. If the encryption key is lost, you will lose access to the device.
  - Click **OK**.
- Click **Add AXIS A9910**.
- Enter the name and select the RS485 port and address to use.
- Click **OK**.

Elevator control

With a reader inside the elevator cabin, you can control the floor access by using the door controller and AXIS A9910. See *Add AXIS A9910, on page 8*.

You can connect up to 16 floors linked to a single door controller and AXIS A9910 expansion modules:

- The expansion modules use one reader port on the controller.
- The other reader port is used by the reader placed inside the elevator cabin.

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

Door connection

Door: Shows the status of connected doors.

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 A9910

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 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.

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

Readers

Add reader: Click to add a reader.

AXIS A4612: You can add up to 16 Bluetooth readers to the controller, no license required.

- **Name**: Enter a name for the reader.
- **Reader**: Select a reader from the drop-down list.
- **IP address**: Enter the IP address of the reader manually.
- **Username**: Enter the username of the reader.
- **Password**: Enter the password of the reader.
- **Ignore server certificate verification**: Turn on to ignore verification.
- **I/O ports and relays**: Expand to configure I/O ports and relays.
  - **Port**: Shows the name of the port.
  - **Direction**: Indicates that it is an input or output port.
  - **Normal state**: Click  for open circuit, and  for closed circuit.

AXIS License Plate Verifier (Need to reconfigure in AXIS Camera Station)

- **Name**: Enter a name for the reader.
- **API-key**: Enter the API key.
- **Generate**: Click to generate the API key.
- **Copy API-key**: Click to copy the API key to save it in a safe place.

AXIS Barcode Reader (Need to reconfigure in AXIS Camera Station)

- **Name**: Enter a name for the reader.
- **API-key**: Enter the API key.
- **Generate**: Click to generate the API key.
- **Copy API-key**: Click to copy the API key to save it in a safe place.

Axis intercom reader (Need to reconfigure in AXIS Camera Station)

- **Name**: Enter a name for the reader.
- **Reader**: Select a reader from the drop-down list.
- **IP address**: Enter the IP address of the reader manually.
- **Username**: Enter the username of the reader.
- **Password**: Enter the password of the reader.
- **Ignore server certificate verification**: Turn on to ignore verification.

Edit: Select a reader and click **Edit** to make changes for the selected reader.

Delete: Select the readers and click **Delete** to delete the selected readers.

Wireless locks

You can connect up to 16 ASSA ABLOY Aperio wireless locks using the AH30 Communication Hub. A license is required for the wireless lock.

Note

You must install the AH30 Communication Hub on the secure side.

Connect communication hub: Click to connect the wireless locks.

Upgrade

Upgrade readers: Click to upgrade the reader's software. You can only upgrade supported readers when they are online.

Upgrade converters: Click to upgrade the converter's software. You can only upgrade supported converters when they are online.

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.

Note

AXIS Door Controller Extension ACAP comes preinstalled on the system. It requires a license to use it.

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.

Global proxies

Http proxy: Specify a global proxy host or IP address according to the allowed format.

Https proxy: Specify a global proxy host or IP address according to the allowed format.

Allowed formats for http and https proxies:

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

Note

Restart the device to apply the global proxy settings.

No proxy: Use **No proxy** to bypass global proxies. Enter one of the options in the list, or enter several separated by a comma:

- Leave empty
- Specify an IP address
- Specify an IP address in CIDR format
- Specify a domain name, for example: www.<domain name>.com
- Specify all subdomains in a specific domain, for example .<domain name>.com

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.

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.

Virtual host

Add virtual host: Click to add a new virtual host.

Enabled: Select to use this virtual host.

Server name: Enter the name of the server. Only use numbers 0-9, letters A-Z, and hyphen (-).

Port: Enter the port the server is connected to.

Type: Select the type of authentication to use. Select between **Basic**, **Digest**, **Open ID**, and **Client Credential Grant**.

HTTPS: Select to use HTTPS.

The context menu contains:

- **Update virtual host**
- **Delete virtual host**

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.

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.

Accessories

I/O ports

Use digital input to connect external devices that can toggle between an open and closed circuit, for example, PIR sensors, door or window contacts, and glass break detectors.

Use digital output to connect external devices such as relays and LEDs. You can activate connected devices through the VAPIX® Application Programming Interface or the web interface.

Port

Name: Edit the text to rename the port.

Direction:  indicates that the port is an input port.  indicates that it's an output port. If the port is configurable, you can click the icons to change between input and output.

Normal state: Click  for open circuit, and  for closed circuit.

Current state: Shows the current state of the port. The input or output is activated when the current state is different from the normal state. An input on the device has an open circuit when it's disconnected or when there is a voltage above 1 VDC.

Note

During restart, the output circuit is open. When the restart is complete, the circuit goes back to the normal position. If you change any settings on this page, the output circuits go back to their normal positions regardless of any active triggers.

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.

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.

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
- O3C 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

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 security notification service

Axis provides a notification service with information about vulnerability and other security related matters for Axis devices. To receive notifications, you can subscribe at *axis.com/security-notification-service*.

Vulnerability management

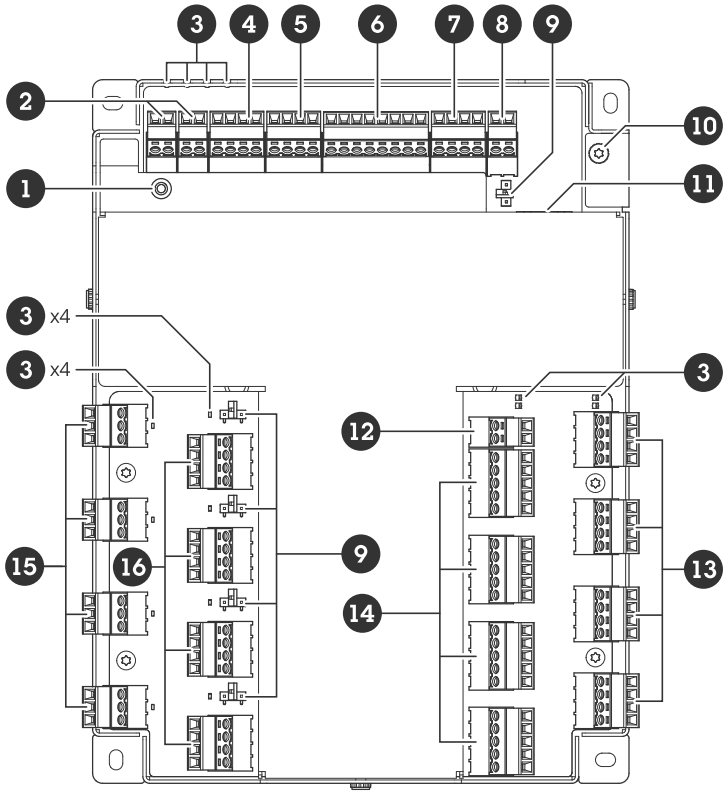
To minimize customers' risk of exposure, Axis, as a **Common Vulnerability and Exposures (CVE) numbering authority (CNA)**, follows industry standards to manage and respond to discovered vulnerabilities in our devices, software, and services. For more information about Axis vulnerability management policy, how to report vulnerabilities, already disclosed vulnerabilities, and corresponding security advisories, see *axis.com/vulnerability-management*.

Secure operation of Axis devices

Axis devices with factory default settings are pre-configured with secure default protection mechanisms. We recommend using more security configuration when installing the device. To learn more about Axis' approach to cybersecurity, including best practices, resources, and guidelines for securing your devices, go to *axis.com/about-axis/cybersecurity*.

Specifications

Product overview



1 *Control button*
2 *Tamper/alarm*
3 *LEDs*
4 *Auxiliary connector*
5 *Output connector*
6 *Input connector*
7 *Relay connector*
8 *Power connector (DC IN)*
9 *Relay jumper*
10 *Grounding position*
11 *Network connector*
12 *Power connector (DC IN DOOR 1–4)*
13 *Reader connector*
14 *Door connector*
15 *AUX relay connector*
16 *Door relay connector*

LED indicators

LED	Color	Indication
Status (STAT)	Green	Steady green for normal operation.
	Amber	Steady during startup and when restoring settings.
	Red	Slow flash for failed upgrade.
Network (NET)	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 (PWR)	Green	Normal operation.
	Amber	Flashes green/amber during firmware upgrade.
Relay (RELAY)	Green	Relay active. (*)
	Unlit	Relay inactive.

LED DOOR 1–4	Color	Indication
Status (STAT)	Green	Blinks (on for 1 second, off for 1 second) when offline.
	Green	Blinks (on for 200 milliseconds, off for 2 seconds) when online.
	Red	Blinks green/red during device software upgrade.
Power (PWR)	Green	Normal operation.
RS485 over current (OC READER)	Red	Over current or under voltage fault on any RS485 port.
Relay over current (OC RELAY)	Red	Over current or under voltage fault on any relay port.
Relay (RELAY)	Green	Relay active. (*)
	Unlit	Relay inactive.
AUX Relay (RELAY)	Green	Relay active. (*)
	Unlit	Relay inactive.

(*) Relay is active when COM is connected to NO.

Buttons

Control button

The control button is used for:

- Resetting the product to factory default settings. See *Reset to factory default settings, on page 43*.

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 30 W Midspan.

Power options

To power the device, you need to connect the following connectors:

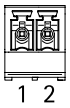
1. PoE or DC IN. See *Power priority, on page 35*.
2. DC IN DOOR 1–4 (required).

Power priority

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

Power connector

Two 2-pin terminal blocks for DC power input. See *Power options, on page 35*.



DC IN

Optional to power the device. You can use PoE instead. See *Power priority, on page 35*.

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

DC IN DOOR 1–4

Required to power the device.

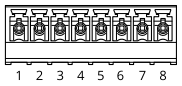
Function	Pin	Notes	Specifications
DC ground (GND)	1		0 V DC
DC input	2	Required to power the device. Note: This pin can only be used as power in.	12 V DC, max 96 W

UL: DC power to be supplied by a UL 294, UL 603, or UL 2610 listed power supply, depending on application, with appropriate ratings.

Input connector

One 8-pin terminal block

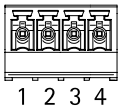
Digital inputs supports supervision with end of line resistors. If the connection is interrupted, an alarm is triggered. To use supervised inputs, install end of line resistors. Use the connection diagram for supervised inputs. See *page 41*.



Function	Pin	Note	Specifications
DC ground (GND)	1, 3, 5, 7		0 V DC
Input	2, 4, 6	Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. Possible to supervise. See *Supervised inputs, on page 41*.	0–30 V DC
+12 V DC	8		Max 190 mA

Output connector

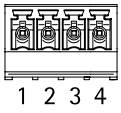
One 4-pin terminal block



Function	Pin	Specifications
DC ground (GND)	1	0 V DC
Output	2,3,4	Open drain, 0–30 V DC, max 100 mA

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.



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.	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.	

Note

The relay is 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	1 900 mA	1000 mA
PoE	150 mA	50 mA
PoE+	920 mA	420 mA

NOTICE

If the lock is non-polarized, we recommend you to add an external flyback diode.

Auxiliary connector

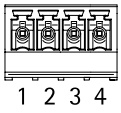
Use the auxiliary connector with external devices in combination with, for example, motion detection, event triggering, and alarm notifications. In addition to the 0 V DC reference point and power (DC output), the auxiliary connector provides the interface to:

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.

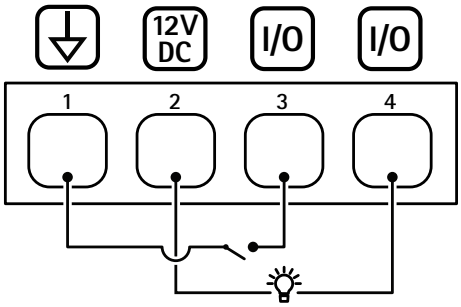
Digital output – For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface or from the product's webpage.

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 = 250 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



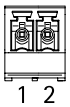
1 *DC ground*
2 *DC output 12 V*
3 *I/O configured as input*
4 *I/O configured as output*

Tamper/Alarm 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
TAMPER	2	Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. Possible to supervise. See *Supervised inputs, on page 41*.	0 to max 30 V DC



Function	Pin	Notes	Specifications
DC ground	1		0 V DC
ALARM	2	Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. Possible to supervise. See *Supervised inputs, on page 41*.	0 to max 30 V DC

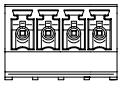
Reader connector

Four 4-pin terminal blocks supporting OSDP protocol for communication with the reader.

It can connect up to eight OSDP readers or Wiegand readers. 2 A at 12 V DC is reserved for readers connected to DOOR 1–4.

Note

Wiegand readers requires AXIS TA1101-B Wiegand to OSDP converter connected between the reader and controller.



Configured for one OSDP reader

Function	Pin	Note	Specifications
DC ground (GND)	1		0 V DC
DC output (+12 V)	2	Supplies power to reader.	12 V DC, combined total of 2 A for all reader connectors.
A	3	Half duplex	
B	4	Half duplex	

Configured for two OSDP readers (multi-drop)

Function	Pin	Note	Specifications
DC ground (GND)	1		0 V DC
DC output (+12 V)	2	Supplies power to both readers.	12 V DC, combined total of 2 A for all reader connectors.
A	3	Half duplex	
B	4	Half duplex	

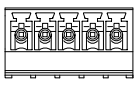
Important

- When the reader is powered by the controller, the qualified cable length is up to 200 m (656 ft) if the following cable requirement is met: AWG 22–14. Verified only for Axis readers.
- When the reader is not powered by the controller, the qualified cable length for reader data is up to 1000 m (3280,8 ft) if the following cable requirements are met: 1 twisted pair, AWG 26–14. Verified only for Axis readers.

Door connector

Four 5-pin terminal blocks for door monitoring devices (digital input).

Door monitor 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 *page 41*.



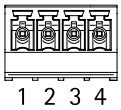
Function	Pin	Notes	Specifications
DC ground (GND)	1, 3		0 V DC
Input	2, 4	For communicating with door monitor. Digital input or Supervised input — Connect to pin 1 or 3 respectively to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC
+12 V DC	5	Supply power to devices such as door sensors.	Combined total of 400 mA for all door connectors

Important

The qualified cable length is up to 200 m (656 ft) if the following cable requirement is met: AWG 24–14.

Door relay connector

Four 4-pin terminal blocks for form C relays that can be used, for example, to control a lock or an interface to a gate.



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.	Max current = 4 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.	

Note

The relay is 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
COM Combined total of 46 W for all door relay connectors	Combined total of 3.8 A for all door relay connectors	Combined total of 1.5 A for all door relay connectors

NOTICE

If the lock is non-polarized, we recommend you to add an external flyback diode.

AUX relay connector

Four 3-pin terminal blocks for form C relays that can be used, for example, to control a lock or an interface to a gate.

Function	Pin	Notes	Specifications
NO	1	Normally open. For connecting relay devices. Connect a fail-secure lock between NO and DC ground.	Max current = 2 A Max voltage = 30 V DC
COM	2	Common	
NC	3	Normally closed. For connecting relay devices. Connect a fail-safe lock between NC and DC ground.	

Note

The relay is galvanically separated from the rest of the circuitry if the jumpers are not used.

NOTICE

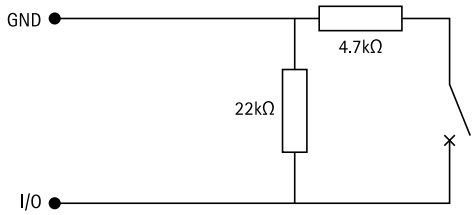
If the lock is non-polarized, we recommend you to add an external flyback diode.

Supervised inputs

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

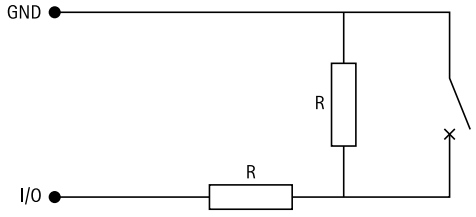
Parallel first connection

The resistor values must be 4.7 kΩ and 22 kΩ.



Serial first connection

The resistor values must be the same and possible values are 1 kΩ, 2.2 kΩ, 4.7 kΩ and 10 kΩ.



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 cable is short circuit to GND.
Cut	The I/O 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 33*.
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*.
- Because the database of users, groups, credentials, and other data are updated after a AXIS OS upgrade, the first start-up could take a few minutes to complete. The time required is dependent on the amount of data.

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.

4. When the product has been restarted, clear the web browser's cache.

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 43*.

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 6*.

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 Edge: free of charge, ideal for small systems with basic surveillance needs.
- 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*.

T10217727

2026-02 (M12.2)