

# AXIS A1710-B Network Door Controller

Table of Contents

Solution overview .....3

Installation .....4

Get started.....5

    Find the device on the network.....5

        Browser support.....5

    Open the device's web interface.....5

    Create an administrator account.....5

    Secure passwords.....6

    Make sure that no one has tampered with the device software .....6

    Web interface overview .....6

Configure your device.....7

    Add AXIS A9910.....7

    Elevator control .....7

    Door override.....7

The web interface .....8

Learn more.....9

    Cybersecurity.....9

        Axis security notification service .....9

        Vulnerability management.....9

        Secure operation of Axis devices .....9

Specifications.....10

    Product overview .....10

    LED indicators.....10

    Buttons.....11

        Control button .....11

Connectors.....11

    Network connector .....11

    Power options .....12

    Power priority .....12

    Power connector .....12

    Input connector.....13

    Output connector .....13

    Relay connector .....13

    Auxiliary connector.....14

    Tamper/Alarm connector .....15

    Reader connector .....16

    Door connector .....16

    Door relay connector.....17

    AUX relay connector .....18

    Supervised inputs .....18

        .....19

Troubleshooting.....20

    Reset to factory default settings .....20

    AXIS OS options.....20

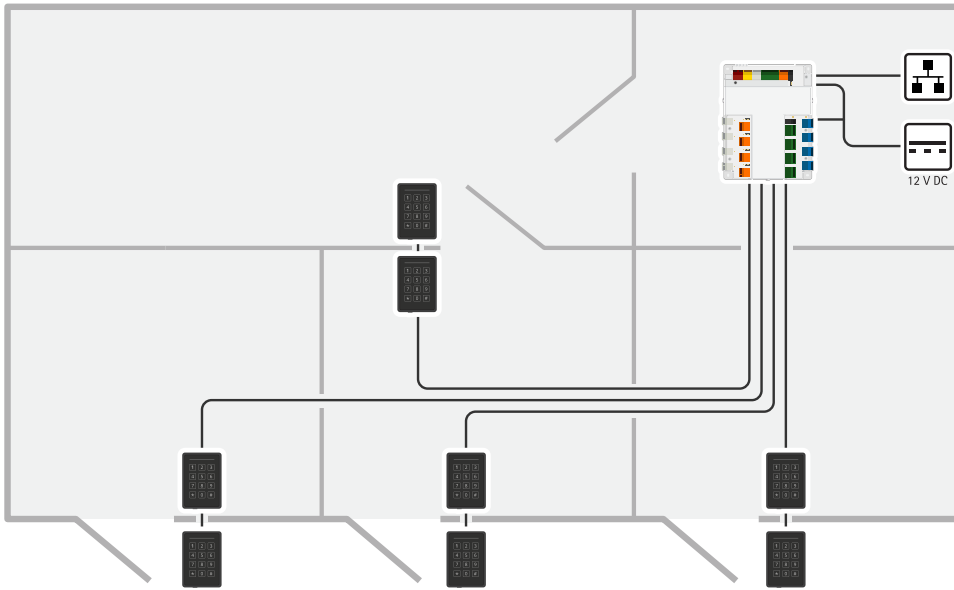
    Check the current AXIS OS version .....20

    Upgrade AXIS OS.....20

    Technical problems and possible solutions .....21

    Contact support .....23

## 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



To watch this video, go to the web version of this document.

## 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](http://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 don't 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 5*.

For descriptions of all features and settings in the web interface of devices with AXIS OS, see *AXIS OS web interface help*.

### 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 6*.
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 20*.

## 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 20*.  
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 7*.

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.

#### Door override

##### Important

This feature takes direct control of the door relays and overrides the relay configuration in AXIS Camera Station. Only use it if Axis support has instructed you to do so.

1. Stop the Secure Entry service in AXIS Camera Station.
2. In the door controller's web interface, go to **Advanced > Door override**.
3. Read the information on the page carefully, then click **I understand**.
4. Turn on **Door override** and click **Enable**.
5. Go to the door relay, click **Lock**, **Unlock**, or **Access** to lock the door, unlock the door, or grant access.
6. Go to the relay you want to configure and click **Activate** or **Deactivate** to activate or deactivate the relay.

## The web interface

To read about all the features and settings available in the web interface of devices with AXIS OS, go to *AXIS OS web interface help*.

### Learn more

#### Cybersecurity

For product-specific information about cybersecurity, see the product's datasheet at [axis.com](https://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](https://axis.com/security-notification-service).

#### Vulnerability management

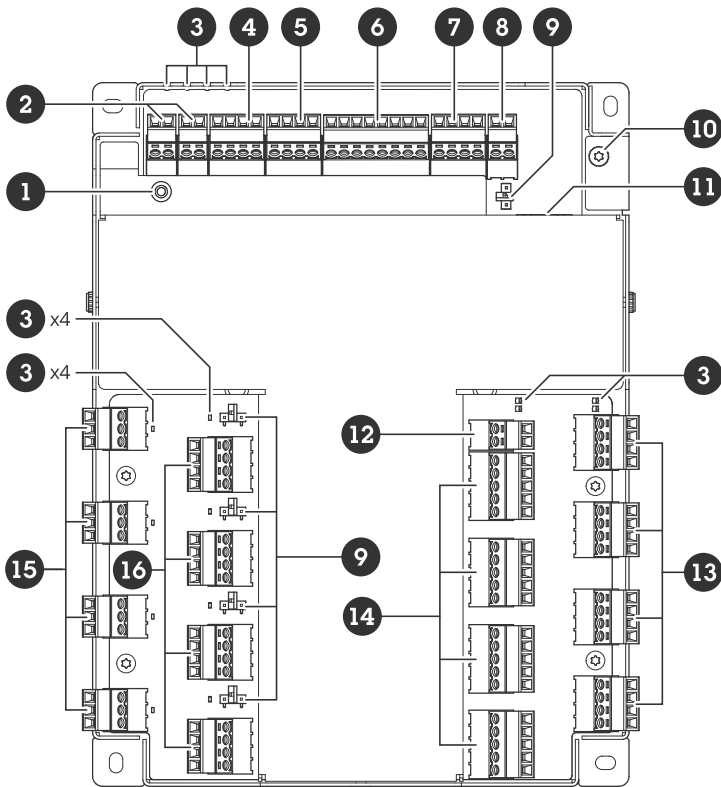
To minimize customers' risk of exposure, Axis, as a **Common Vulnerability and Exposures (CVE) numbering authority (CNA)**, follows industry standards to manage and respond to discovered vulnerabilities in our devices, software, and services. For more information about Axis vulnerability management policy, how to report vulnerabilities, already disclosed vulnerabilities, and corresponding security advisories, see [axis.com/vulnerability-management](https://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](https://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 20*.

## 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:

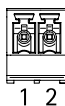
1. PoE or DC IN. See *Power priority*, on page 12.
2. DC IN DOOR 1–4 (required).

## 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 12.



### DC IN

Optional to power the device. You can use PoE instead. See *Power priority*, on page 12.

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.

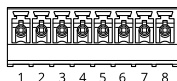
Function	Pin	Notes	Specifications
DC ground (GND)	1		0 V DC
DC input	2	Required to power the device. Note: This pin can only be used as power in.	12 V DC, max 96 W

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

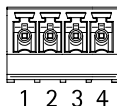
Digital inputs supports supervision with end of line resistors. If the connection is interrupted, an alarm is triggered. To use supervised inputs, install end of line resistors. Use the connection diagram for supervised inputs. See page 18.



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 <i>Supervised inputs, on page 18.</i>	0–30 V DC
+12 V DC	8		Max 190 mA

### Output connector

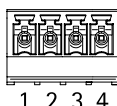
One 4-pin terminal block



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**

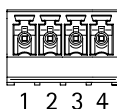
Use the auxiliary connector with external devices in combination with, for example, motion detection, event triggering, and alarm notifications. In addition to the 0 V DC reference point and power (DC output), the auxiliary connector provides the interface to:

**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.

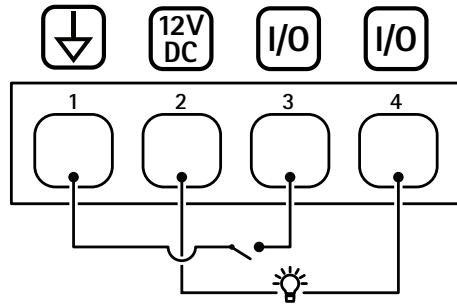
**Digital output** – For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface or from the product's webpage.

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

	<p>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.</p>	<p>0 to max 30 V DC, open drain, 100 mA</p>
--	--	---

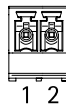


- 1 DC ground
- 2 DC output 12 V
- 3 I/O configured as input
- 4 I/O configured as output

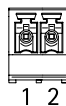
**Tamper/Alarm connector**

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 <i>Supervised inputs</i> , on page 18.	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 <i>Supervised inputs</i> , on page 18.	0 to max 30 V DC

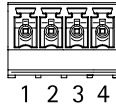
**Reader connector**

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	

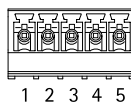
**Important**

- 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 18*.



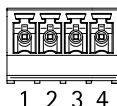
Function	Pin	Notes	Specifications
DC ground (GND)	1, 3		0 V DC
Input	2, 4	For communicating with door monitor. Digital input or Supervised input – Connect to pin 1 or 3 respectively to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC
+12 V DC	5	Supply power to devices such as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

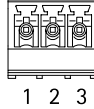
Power source	Max power at 12 V DC	Max power at 24 V DC
COM Combined total of 46 W for all door relay connectors	Combined total of 3.8 A for all door relay connectors	Combined total of 1.5 A for all door relay connectors

**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**

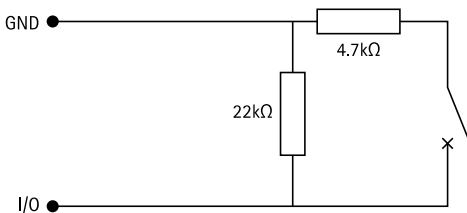
If the lock is non-polarized, we recommend you to add an external flyback diode.

**Supervised inputs**

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

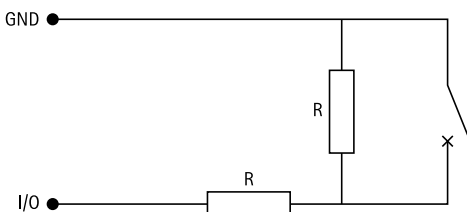
**Parallel first connection**

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 10*.
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](https://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](http://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](http://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 20*.

#### 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](https://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 5*.

#### 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](https://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.

### Problems with operating the device

### Front heater and wiper aren't working

If the front heater or wiper are not turning on, confirm that the top cover is properly fastened to the bottom of the housing unit.

If you can't find what you're looking for here, try the troubleshooting section at [axis.com/support](https://axis.com/support).

### Contact support

If you need more help, go to [axis.com/support](https://axis.com/support).

T10217727

2026-04 (M14.2)

© 2024 – 2026 Axis Communications AB