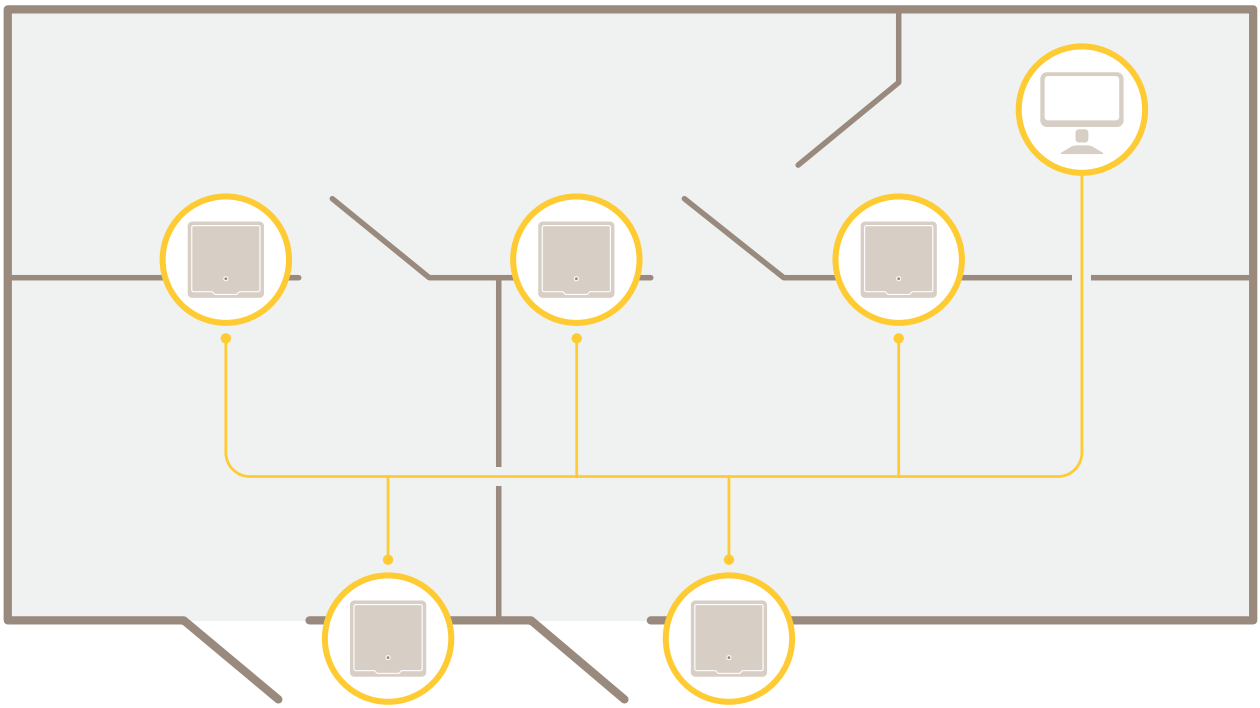
AXIS A1610 Network Door Controller

User manual

Table of Contents

Solution overview 3
Get started 4
Find the device on the network 4
Browser support 4
Open the device's web interface 4
Create an administrator account 4
Secure passwords 5
Make sure that no one has tampered with the device software 5
Web interface overview 5
Configure your device 6
Add AXIS A9910 6
Elevator control 6
Door override 7
OSDP LED profile 7
Card format 9
The web interface 10
Learn more 11
Cybersecurity 11
Signed OS 11
Secure boot 11
Axis Edge Vault 11
Axis device ID 11
Specifications 12
....12
Product overview 12
....12
LED indicators 12
Buttons 13
Control button 13
Connectors 13
Network connector 13
Power priority 13
Reader connector 14
Supervised inputs 15
Door connector 15
Relay connector 16
Auxiliary connector 17
External connector 18
Power connector 18
12 V backup power input 18
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
Performance considerations 22
Contact support 23

Solution overview



The network door controller can easily be connected to and powered by your existing IP network with no need for special cabling.

Each network door controller is an intelligent device that is easily mounted close to a door. It can power and control up to four readers.

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 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 4*.

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 an account.
2. Enter a password. See *Secure passwords, on page 5*.
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 password is the primary protection for your data and services.

To protect your data we strongly recommend that you:

- 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

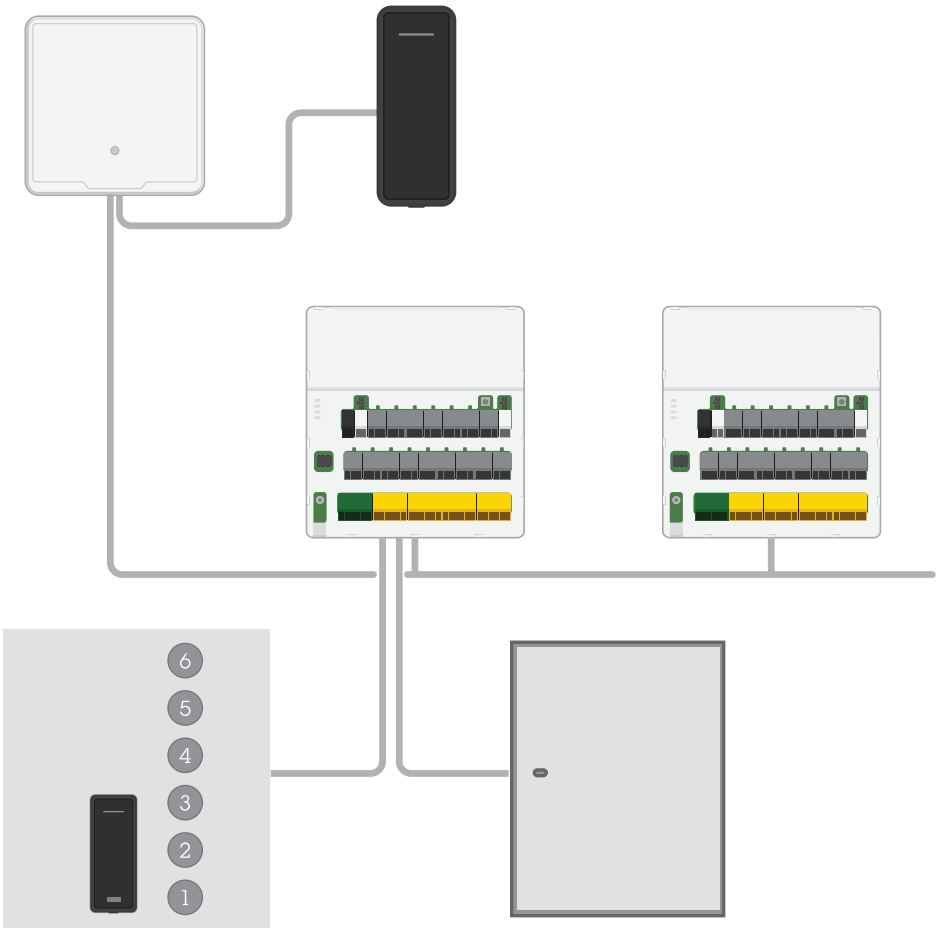
- In the door controller's web interface, go to **Peripherals** > **Expansion I/O module**.
- Click **Add encryption key**.
- If you have generated the encryption key before, enter the key and click **OK**.
- To generate an encryption key:
  - Click **Generate**.
  - Click **Export and add** to save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

Elevator control

With a reader inside the elevator cabin, you can control the floor access by using the door controller and Axis expansion module.

You can connect up to 64 floors linked to a single door controller and Axis 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.

OSDP LED profile

You can customize your OSDP reader's LED profiles to define the lights and sounds that are used for different events. For a full list of profiles, see *LED profiles*.

Set light and audio levels

1. Go to **Peripherals** > **Readers** > **OSDP LED profile**.
2. Expand the **Light and audio levels** drop-down menu.
3. Use the slider to adjust the intensity of the LED stripe, the LED backlight, and sound.

4. Click **Save**.

Note

When you change the light and audio levels, the settings are updated for any readers connected to the controller.

Test OSDP LED settings:

You can use the **OSDP LED test** menu to see the audio and light settings for any of your reader profiles.

To test the settings for your OSDP LED profiles:

1. Go to **Peripherals** > **Readers** > **OSDP LED profile**.
2. Expand the **OSDP LED test** drop-down menu.
3. Choose an LED feedback.
4. Choose the reader you would like to test.
5. Click **Start**.
6. Click **Edit feedback** to change the light and audio settings for your profile.
   - Choose a new color from the **Color** drop-down menu.
   - Choose an audio frequency from the **Audio** drop-down menu, if applicable.
   - You can also reset the profile's settings by clicking **Reset to default values**.
   - Click **Save**.

Change OSDP LED profile settings:

1. Go to **Peripherals** > **Readers** > **OSDP LED profile**.
2. Navigate to **OSDP LED profile**.
3. Click next to the profile you wish to edit.
4. Edit your applicable settings:
   - Choose the behavior your LEDs will follow from the **Behavior** drop-down menu.
   - Choose the color of your LEDs from the **Color** drop-down menu.
   - Set the **Duration on** and **Duration off** for your LEDs.
   - Set the **Recurrence** of the LED response.
   - From the **Audio** drop-down menu, choose the **Beep duration, on** and **Beep duration, off**, and set the **Recurrence** of your buzzer response. Make sure the **Beep duration, on** and **Beep duration, off** are the same duration.
5. Click **Save**.

Import existing settings from another controller

1. Go to **Peripherals** > **Readers** > **OSDP LED profile**.
2. Click on **Import**.
3. Choose the file you want to upload.
4. Click **Import**.

Export current settings

1. Go to **Peripherals** > **Readers** > **OSDP LED profile**.
2. Click on **Export**.
3. Choose where you want to save the json file and click **Save**.

Card format

This feature is for expert use only. As soon as **Card format** is turned on:

- If you are using a 37-bit credential, the last 5 bits are removed.
- If you are using a 64–bit credential (QR code), the first 24-bit sequence is removed.

You can use either the sample data or the card reader to view credentials.

1. Go to **Advanced** > **Card format**.
2. Read the warning and click **I understand** to enable **Card format**.
3. In the **Reader data visualization** drop-down menu, choose your reader.
4. Click **Get reader data** or **Use sample data** to generate a card output. It will be applied to all cardholders on the device.
5. Turn on **Trim reader data** to remove the end bits from card credentials.
6. Click **Enable**.

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.

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

Signed OS

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

Secure boot

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

Axis Edge Vault

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

Axis device ID

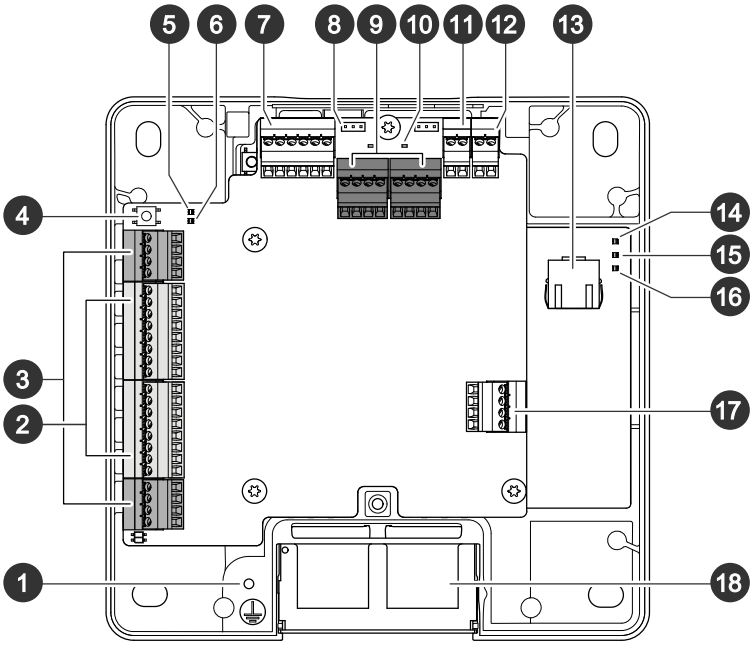
Being able to verify the origin of the device is key to establishing trust in the device identity. During production, devices with Axis Edge Vault are assigned a unique, factory-provisioned, and IEEE 802.1AR-compliant Axis device ID certificate. This works like a passport to prove the origin of the device.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

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

Specifications

Text marked with **UL** is only valid for UL 294 installations.

Product overview



1 *Grounding position*
2 *Reader connector, 2x*
3 *Door connector, 2x*
4 *Control button*
5 *Relay overcurrent LED*
6 *Reader overcurrent LED*
7 *Auxiliary connector*
8 *Relay jumper, 2x*
9 *Relay connector, 2x*
10 *Relay LED, 2x*
11 *12 V backup power input*
12 *Power connector*
13 *Network connector*
14 *Power LED*
15 *Status LED*
16 *Network LED*
17 *External connector*
18 *Reversible cable cover*

LED indicators

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

	Red	Slow flash for failed upgrade.
Power	Green	Normal operation.
	Amber	Flashes green/amber during firmware upgrade.
Relay overcurrent	Red	Steady when short circuited or if overcurrent has been detected.
	Unlit	Normal operation.
Reader overcurrent	Red	Steady when short circuited or if overcurrent has been detected.
	Unlit	Normal operation.
Relay	Green	Relay active.[1]
	Unlit	Relay inactive.

Note

- The Status LED can be configured to flash while an event is active.
- The Status LED can be configured to flash for identifying the unit. Go to **Setup > Additional Controller Configuration > System Options > Maintenance** .

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 supplied by a UL 294 listed Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 3 or Power over Ethernet Plus (PoE+) IEEE 802.3at Type 2 Class 4 power limited injector that provides 44–57 V DC, 15.4 W / 30 W. Power over Ethernet (PoE) has been evaluated by UL with AXIS T8133 Midspan 30 W 1-port.

Power priority

This device can be powered by either PoE or DC input. See *Network connector, on page 13* and *Power connector, on page 18*.

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

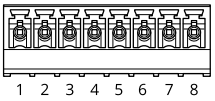
1. *Relay is active when COM is connected to NO.*

Reader connector

Two 8–pin terminal blocks supporting both RS485 and Wiegand protocols for communication with the reader.

The specified power output values are shared between the two reader ports. It means that 500 mA at 12 V DC is reserved for all readers connected to the door controller.

Select which protocol to use in the product's web page.



Configured for RS485

Function	Pin	Note	Specifications
DC ground (GND)	1		0 V DC
DC output (+12 V)	2	Supplies power to reader.	12 V DC, max 500 mA combined for all readers
RX/TX	3–4	Full duplex: RX. Half duplex: RX/TX.	
TX	5–6	Full duplex: TX.	
Configurable (Input or Output)	7–8	Digital input — Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC
		Digital output — If used with an inductive load, e. g., a relay, connect a diode in parallel with the load, to protect against voltage transients.	0 to max 30 V DC, open drain, 100 mA

Important

- When the reader is powered by the controller, the qualified cable length is up to 200 m (656 ft).
- 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 with shield, AWG 20-16.

Configured for Wiegand

Function	Pin	Note	Specifications
DC ground (GND)	1		0 V DC
DC output (+12 V)	2	Supplies power to reader.	12 V DC, max 500 mA combined for all readers
D0	3		
D1	4		
O	5–6	Digital output, open drain	

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

Important

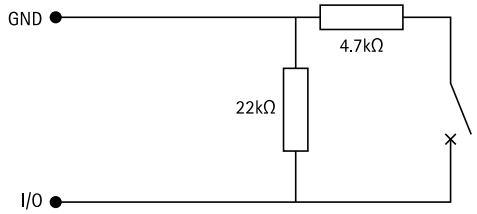
- When the reader is powered by the controller, the qualified cable length is up to 150 m (500 ft).
- When the reader is not powered by the controller, the qualified cable length for reader data is up to 150 m (500 ft) if the following cable requirement is met: AWG 20-16.

Supervised inputs

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

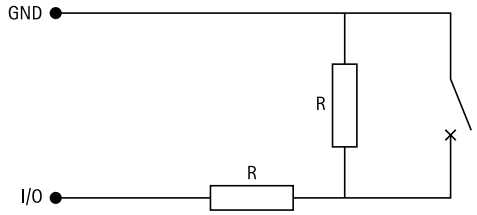
Parallel first connection

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.



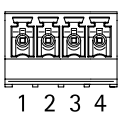
Note

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

Door connector

Two 4-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 *Supervised inputs, on page 15*.



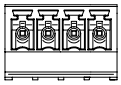
Function	Pin	Notes	Specifications
DC ground	1, 3		0 V DC
Input	2, 4	For communicating with door monitor. Digital input or Supervised input — Connect to pin 1 or 3 respectively to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC

Important

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

Relay connector

Two 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. The two relay pins are galvanically separated from the rest of the circuitry if the jumpers are not used.	Max current = 2 A per relay Max voltage = 30 V DC
COM	3	Common	
NC	4	Normally closed. For connecting relay devices. Connect a fail-safe lock between NC and DC ground. The two relay pins are galvanically separated from the rest of the circuitry if the jumpers are not used.	

Relay power jumper

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

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

Power source	Max power at 12 V DC[2]	Max power at 24 V DC[2]
DC IN	1 800 mA	750 mA
PoE	900 mA	410 mA

NOTICE

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

2. The power is shared between the two relays and AUX I/O 12 V DC.

Auxiliary connector

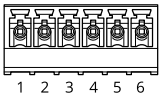
Use the auxiliary connector with external devices in combination with, for example, motion detection, event triggering, and alarm notifications. In addition to the 0 V DC reference point and power (DC output), the auxiliary connector provides the interface to:

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.

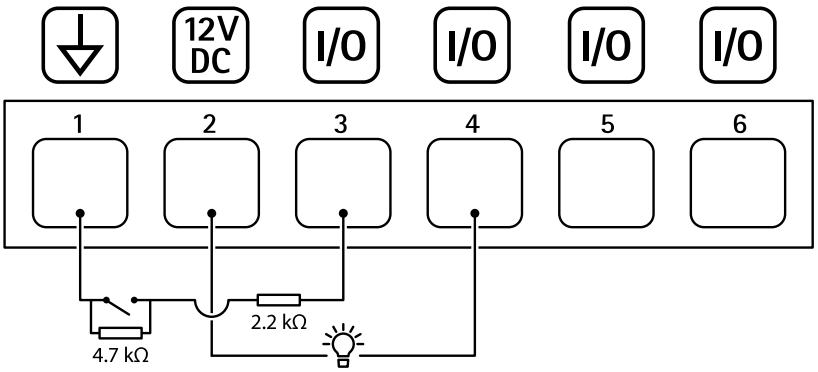
Supervised input – Enables possibility to detect tampering on a digital input.

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.

6–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 and on the secure side since it shares power with the relays.	12 V DC Max load = 50 mA for each I/O
Configurable (Input or Output)	3–6	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. Each I/O is capable of driving 12 V DC, 50 mA (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.	0 to max 30 V DC, open drain, 100 mA



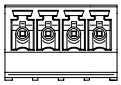
1 *DC ground*
2 *DC output 12 V, max 50 mA*
3 *I/O configured as supervised input*
4 *I/O configured as output*

5 *Configurable I/O*
6 *Configurable I/O*

External connector

4-pin terminal block for external devices, for example glass break or fire detectors.

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



Function	Pin	Notes	Specifications
DC ground	1, 3		0 V DC
Configurable (Input or Output)	2, 4	Digital input – Connect to pin 1 or 3 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC
		Digital output – Connect to pin 1 or 3 to activate, or leave floating (unconnected) to deactivate. If used with an inductive load, e. g., a relay, connect a diode in parallel with the load, to protect against voltage transients.	0 to max 30 V DC, open drain, 100 mA

Note

The USB-A connection port is not functional on this device. You can't use the USB-A port for power, data transfer, or local configuration.

Power connector

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



Function	Pin	Notes	Specifications
0 V DC (-)	1		0 V DC
DC input	2	For powering controller when not using Power over Ethernet. Note: This pin can only be used as power in.	10.5–28 V DC, max 36 W

UL: DC power to be supplied by a UL 294, UL 293 or UL 603 listed power supply, depending on application, with appropriate ratings.

12 V backup power input

For a backup solution using a battery with built-in charger. 12 V DC input.

UL: The connector has not been evaluated by UL.

Important

When the battery input is used, an external 3 A slow blow fuse must be connected in series.



Function	Pin	Notes	Specifications
0 V DC (-)	1		0 V DC
Battery input	2	For powering the door controller when other power sources are unavailable. Note: This pin can only be used as battery power in. For connection to UPS only.	11– 13.7 V DC, max 36 W

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 12*.
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 Lifecycle guide: 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 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*.

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 4*.

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*.

Performance considerations

The most important factors to consider:

- Heavy network utilization due to poor infrastructure affects the bandwidth.

Contact support

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

T10181937

2026-09 (M13.3)

© 2022 – 2026 Axis Communications AB