AXIS D3110 Mk II Connectivity Hub

User manual

Solution overview

This device enables sensor and audio integration into network video systems that don't have such capabilities or need additional ones. Ideal in an Axis end-to-end solution, it helps you increase scene awareness without compromising network security.

If you are using an audio or video management software, you can use that software for configuring the device. The following management software are available for controlling your audio system:

- **AXIS Audio Manager Edge** — Audio management software for small systems. Comes pre-installed on all audio devices with a firmware equal to or higher than 10.0.
  - *AXIS Audio Manager Edge user manual*
- **AXIS Audio Manager Pro** — Advanced audio management software for large systems.
  - *AXIS Audio Manager Pro user manual*
- **AXIS Audio Manager Center** — Cloud service for remote access and management of multi-site systems.
  - *AXIS Audio Manager Center user manual*

For more information, see *Audio management software*.

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 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 a username.
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 17*.

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 17*.
   After the reset, secure boot guarantees the state of the device.
2. Configure and install the device.

Configure your device

This section covers all the important configurations that an installer needs to do to get the product up and running after the hardware installation has been completed.

Set up rules for events

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

Trigger an action

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

Note

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

Detect tampering with input signal

This example explains how to send an email when the input signal is cut or short-circuited. For more information about the I/O connector, see *page 13*.

1. Go to **System > Accessories > I/O ports** and turn on **Supervised** for the relevant port.

Add an email recipient:

1. Go to **System > Events > Recipients** and add a recipient.
2. Type a name for the recipient.
3. Select **Email** as the notification type.
4. Type the recipient's email address.
5. Type the email address that you want the camera to send notifications from.
6. Provide the login details for the sending email account, along with the SMTP hostname and port number.
7. To test your email setup, click **Test**.
8. Click **Save**.

Create a rule:

1. Go to **System > Events > Rules** and add a rule.
2. Type a name for the rule.
3. In the list of conditions, under **I/O**, select **Supervised input tampering is active**.
4. Select the relevant port.
5. In the list of actions, under **Notifications**, select **Send notification to email** and then select the recipient from the list.
6. Type a subject line and message for the email.
7. Click **Save**.

Activate a lamp when the window is opened

This example explains how to connect a window contact to a connectivity hub, and how to set up an event to activate a lamp when a window with a contact on it is opened.

Prerequisites

- Connect a 2-wire cable (ground, I/O) to the window contact and to the I/O connector on the connectivity hub.
- Connect the lamp to power and to the relay connector on the connectivity hub.

Configure the I/O ports in the connectivity hub

1. Go to **System > Accessories**.
2. Enter the following information in **Port 1**:
   - **Name**: Window sensor
   - **Direction**: **Input**
   - **Normal state**: **Closed circuit**
3. Enter the following information in **Port 2**:
   - **Name**: Lamp
   - **Direction**: **Output**
   - **Normal state**: **Open circuit**

Create two rules in the connectivity hub

1. Go to **System > Events** and add a rule.
2. Enter the following information:
   - **Name**: Window sensor
   - **Condition**: **Digital input**
     Select **Use this condition as a trigger**
   - **Port**: **Window sensor**
   - **Action**: **Toggle I/O while the rule is active**
   - **Port**: **Lamp**
   - **State**: **Active**
3. Click **Save**.

Activate connectivity hub over MQTT when camera detects motion

Prerequisites

- Configure a device for the I/O port 1 in the connectivity hub.
- Set up an MQTT broker and get the broker's IP address, username and password.
- Set up AXIS Motion Guard in the camera.

Set up the MQTT client in the camera

1. In the camera's device interface, go to **System > MQTT > MQTT client > Broker** and enter the following information:
   - **Host**: Broker IP address
   - **Client ID**: For example Camera 1
   - **Protocol**: The protocol the broker is set to
   - **Port**: The port number used by the broker
   - The broker **Username** and **Password**
2. Click **Save** and **Connect**.

Create two rules in the camera for MQTT publishing

1. Go to **System > Events > Rules** and add a rule.
2. Enter the following information:
   - **Name**: Motion detected
   - **Condition**: **Applications > Motion alarm**

- **Action**: **MQTT > Send MQTT publish message**
- **Topic**: Motion
- **Payload**: On
- **QoS**: 0, 1 or 2

3. Click **Save**.
4. Add another rule with the following information:
   - **Name**: No motion
   - **Condition**: **Applications > Motion alarm**
     - Select **Invert this condition.**
   - **Action**: **MQTT > Send MQTT publish message**
   - **Topic**: Motion
   - **Payload**: Off
   - **QoS**: 0, 1 or 2
5. Click **Save**.

Set up the MQTT client in the connectivity hub

1. In the connectivity hub's device interface, go to **System > MQTT > MQTT client > Broker** and enter the following information:
   - **Host**: Broker IP address
   - **Client ID**: Port 1
   - **Protocol**: The protocol the broker is set to
   - **Port**: The port number used by the broker
   - **Username** and **Password**
2. Click **Save** and **Connect**.
3. Go to **MQTT subscriptions** and add a subscription.
   Enter the following information:
   - **Subscription filter**: Motion
   - **Subscription type**: Stateful
   - **QoS**: 0, 1 or 2
4. Click **Save**.

Create a rule in the connectivity hub for MQTT subscriptions

1. Go to **System > Events > Rules** and add a rule.
2. Enter the following information:
   - **Name**: Motion detected
   - **Condition**: **MQTT > Stateful**
   - **Subscription filter**: **Motion**
   - **Payload**: On
   - **Action**: **I/O > Toggle I/O while the rule is active**
   - **Port**: I/O 1.
3. Click **Save**.

Open a lock when a button is pressed

This example explains how to connect a relay to the connectivity hub and how to set up an event to open a lock when someone presses a button connected to the connectivity hub.

Prerequisites

- Connect a 2-wire cable (COM, NO) to the lock and to the relay connector on the connectivity hub.
- Connect a 2-wire cable (ground, I/O) to the button and to the I/O connector on the connectivity hub.

Configure the I/O ports in the connectivity hub

1. Go to **System > Accessories**.
2. Enter the following information in **Port 1**:
   - **Name**: Button
   - **Direction**: **Input**
   - **Normal state**: **Open circuit**
3. Enter the following information in **Port 9**:
   - **Name**: Lock
   - **Normal state**: **Open circuit**

Create a rule in the connectivity hub

1. Go to **System > Events** and add a rule.
2. Enter the following information:
   - **Name**: Open lock
   - **Condition**: **I/O > Digital input is active**
     Select **Use this condition as a trigger**
   - **Port**: **Button**
   - **Action**: **I/O > Toggle I/O once**
   - **Port**: **Lock**
   - **State**: **Active**
   - **Duration:** 10 s
3. Click **Save**.

Audio

Record audio to SD card

This example explains how to set up recording from two microphones to an SD card.

Before you start

- Connect two microphones and insert one microSD card into the connectivity hub.

1. Go to **Audio > Device settings** and turn on **Input 0: IN 1** and **Input 1: IN 2**.
2. Select **Input type** and **Power type**.
3. If you expect the sound levels to vary across the room, turn on **Automatic gain control**.
4. Go to **System > Storage > Onboard storage** and set **Retention time**.
5. Go to **Audio > Stream** and select **Encoding**.

Note

To keep the CPU load low when running multiple streams (for example recording and live stream from the same source), use the same encoding for both streams.

6. Go to **Audio > Listen and record** and click  .
7. Click  .

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

Analytics and apps

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

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

AXIS Audio Analytics

AXIS Audio Analytics detects sudden increases in sound volume and specific types of sounds such as screams or shouts within range of the device it's installed on. These detections can be configured to trigger a response, such as recording video, playing an audio message, or alerting security staff. To find out more about how the application works, see *AXIS Audio Analytics user manual*.

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

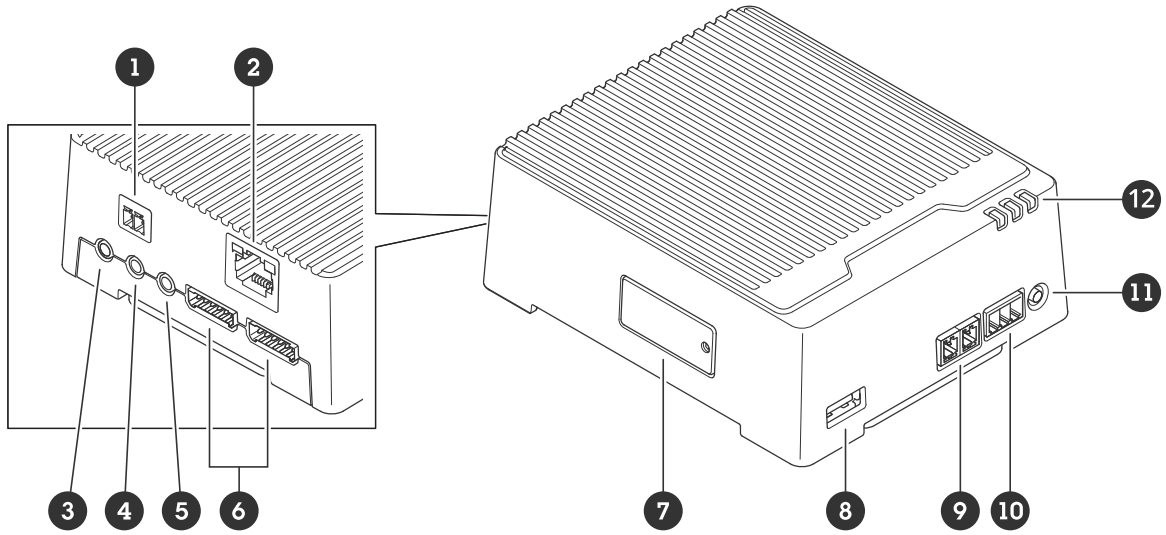
To minimize customers' risk of exposure, Axis, as a **Common Vulnerability and Exposures (CVE) numbering authority (CNA)**, follows industry standards to manage and respond to discovered vulnerabilities in our devices, software, and services. For more information about Axis vulnerability management policy, 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 *Power connector*
2 *RJ45 ethernet connector*
3 *Microphone port 2 (analog)*
4 *Microphone port 1 (digital and analog)*
5 *Audio out*
6 *2x I/O connectors (6-pin)*
7 *MicroSD card slot*
8 *USB port*
9 *RS485/RS422 connector*
10 *Relay connector*
11 *Control button*
12 *Status LED*

SD card slot

For SD card recommendations, see *axis.com*.

microSD, microSDHC, and microSDXC Logos are trademarks of SD-3C LLC. microSD, microSDHC, microSDXC are trademarks or registered trademarks of SD-3C, LLC in the United States, other countries or both.

Buttons

Control button

The control button is used for:

- Resetting the product to factory default settings. See *Reset to factory default settings, on page 17*.
- Connecting to a one-click cloud connection (O3C) service over the internet. To connect, press and release the button, then wait for the status LED to flash green three times.

Connectors

Network connector

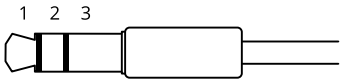
RJ45 Ethernet connector.

Input: RJ45 Ethernet connector with Power over Ethernet (PoE).

Output: RJ45 Ethernet connector with Power over Ethernet (PoE).

Audio connector

- **Audio in** (microphone port 1) – 3.5 mm input for a digital microphone, an analog mono microphone, or a line-in mono signal (left channel is used from a stereo signal).
- **Audio in** (microphone port 2) – 3.5 mm input for an analog mono microphone, or a line-in mono signal (left channel is used from a stereo signal).
- **Audio out** – 3.5 mm output for audio (line level) that can be connected to a public address (PA) system or an active speaker with a built-in amplifier. A pair of headphones can also be attached. A stereo connector must be used for audio out.



Audio input

1 Tip	2 Ring	3 Sleeve
Unbalanced microphone (with or without electret power) or line-in	Electret power if selected	Ground
Balanced microphone (with or without phantom power) or line-in, "hot" signal	Balanced microphone (with or without phantom power) or line-in, "cold" signal	Ground
Digital signal	Ring power if selected	Ground

Audio output

1 Tip	2 Ring	3 Sleeve
Channel 1, unbalanced line, mono	Channel 1, unbalanced line, mono	Ground

I/O connector

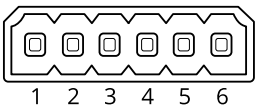
Use the I/O connector with external devices in combination with, for example, motion detection, event triggering, and alarm notifications. In addition to the 0 VDC reference point and power (12 V DC output), the I/O connector provides the interface to:

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, through an event or from the device's web interface.

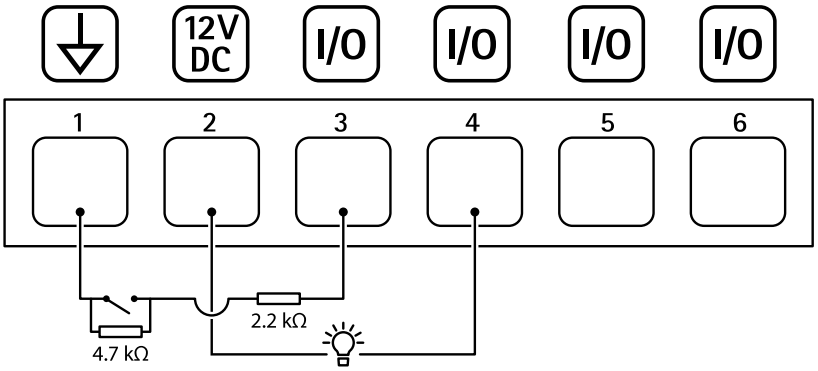
6-pin terminal block



Function	Pin	Notes	Specifications
DC ground	1		0 VDC
DC output	2	⚠	12 VDC

		Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	Max load = 50 mA
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 VDC
		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.	0 to max 30 VDC, open drain, 100 mA

Example:



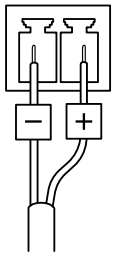
1 *DC ground*
2 *DC output 12 V, max 50 mA*
3 *I/O configured as supervised input*
4 *I/O configured as output*
5 *Configurable I/O*
6 *Configurable I/O*

Electrical design specification for digital I/O

Parameter	Value
Minimum input voltage durability	-30 V DC
Maximum input voltage durability	+30 V DC
Maximum digital input low voltage	+0.50 V at 25 °C +0.40 V at 85 °C
Minimum digital input high voltage	+1.5 V
Maximum output low voltage at 100 mA	+0.6 V
Maximum output low voltage at 10 mA	+0.06 V
Maximum rise time (including delay from GPIO) at 10 kHz	5 us
Maximum fall time (including delay from GPIO) at 10 kHz	5 us
Maximum output sink current	100 mA
Maximum I/O leakage current	100 µA at 12 V DC

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.

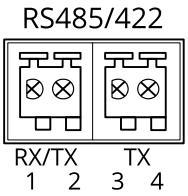


RS485/RS422 connector

Two 2-pin terminal blocks for RS485/RS422 serial interface.

The serial port can be configured to support:

- Two-wire RS485 half duplex
- Four-wire RS485 full duplex
- Two-wire RS422 simplex
- Four-wire RS422 full duplex point to point communication



Function	Pin	Notes
RS485/RS422 RX/TX A	1	(RX) For full duplex RS485/RS422 (RX/TX) For half duplex RS485
RS485/RS422 RX/TX B	2	
RS485/RS422 TX A	3	(TX) For full duplex RS485/RS422
RS485/RS422 TX B	4	

Clean your device

You can clean your device with lukewarm water.

NOTICE

- Harsh chemicals can damage the device. Don't use chemicals such as window cleaner or acetone to clean your device.
- Avoid cleaning in direct sunlight or elevated temperatures, since this can cause stains.

1. Use a can of compressed air to remove dust and loose dirt from the device.
2. If necessary, clean the device with a soft microfiber cloth dampened with lukewarm water.
3. To avoid stains, dry the device with a clean, nonabrasive cloth.

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 15–30 seconds until the status LED indicator flashes amber.
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 to assign an IP address, set the password, and access the device.
   The installation and management software tools are available from the support pages on *axis.com/support*.

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

AXIS OS options

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

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

Check the current AXIS OS version

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

To check the current AXIS OS version:

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

Upgrade AXIS OS

Important

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

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

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

Note

- When you upgrade the device with the latest AXIS OS version in the active track, the product receives the latest functionality available. Always read the upgrade instructions and release notes available with each new release before you upgrade. To find the latest AXIS OS version and the release notes, go to *axis.com/support/device-software*.

1. Download the AXIS OS file to your computer, available free of charge at *axis.com/support/device-software*.
2. Log in to the device as an administrator.
3. Go to **Maintenance > AXIS OS upgrade** and click **Upgrade**.

When the upgrade has finished, the product restarts automatically.

Technical problems and possible solutions

Problems upgrading AXIS OS

AXIS OS upgrade failed

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

Problems after AXIS OS upgrade

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

Problems setting the IP address

Can't set the IP address

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

Problems accessing the device

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

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

If you've lost the password for the root account, you must reset the device to the factory default settings. For instructions, see *Reset to factory default settings, on page 17*.

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.

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*.

Performance considerations

The following factors are the most important to consider:

- Heavy network utilization due to poor infrastructure affects the bandwidth.
- Running multiple activities at the same time can affect the audio performance.

Contact support

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

T10208737

2026-02 (M6.2)