

# AXIS M1075-L Mk II Box Camera User Manual EN

## Installation

### Preview mode

Preview mode is ideal for installers when fine tuning the camera view during the installation. No login is required to access the camera view in preview mode. It is available only in factory defaulted state for a limited time from powering up the device.



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

*This video demonstrates how to use preview mode.*

## Get started

### Connect the camera to a wireless network

Before you start:


- Find out more about the camera's buttons and connectors. See .
- Connect the wireless adapter to the camera's USB connector.

### Configure the camera through WLAN connection

1. Connect the power injector to the camera.
2. When the camera flashes yellow/red, press the WLAN setup button until status LED is steady blue. The camera is now in access point mode.
3. Connect to the camera's access point with your computer or mobile phone. Use the SSID and password printed on the label on the back of the camera.
4. To get to the WLAN settings page, open a browser and type the IP address 192.168.0.1.

#### Note

To get directly to the WLAN settings page, you can also scan the barcode located next to the SSID and password on the label.

5. Go to the wireless network you will use, click  and configure it according to your needs.
6. Click **Save**. The camera's access point shuts down and the camera connects to the configured access point.


#### Important

Due to security risks, you must do a factory default reset if you want to redo the procedure once you are connected to the WLAN.


### Configure the camera through wired connection

1. Connect the device to the network with a network cable.
2. Log in to the device's webpage. See *Find the device on the network, on page 4*.
3. Go to **System > WLAN**.

If there is a wireless network up and running:

1. Go to the wireless network you will use, click  and configure it according to your needs.
2. Click **Save**.
3. Disconnect the network cable from the camera. Connect the power injector.

If there is no wireless network available:

1. Click  **Add network**.
2. In the list of authentication methods, select **WPA™Personal**.

#### Note

To configure the network with a security method other than WPA™Personal, see *Advanced wireless settings, on page 14*.

3. Enter the SSID and password for the access point.
4. Click **Save**.
5. Disconnect the network cable from the camera. Connect the power injector.

## 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 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 4*.
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 21*.

## 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 21*.  
After the reset, secure boot guarantees the state of the device.
2. Configure and install the device.

## Configure your device

### Basic settings

Set the power line frequency

1. Go to **Video > Installation > Power line frequency**.
2. Select a power line frequency and click **Save and restart**.

Set the orientation

1. Go to **Video > Installation > Rotate**.
2. Select **0**, **90**, **180** or **270** degrees.  
See also *Monitor long and narrow areas*, on page 6.

### Adjust the image

This section includes instructions about configuring your device. If you want to learn more about how certain features work, go to *Learn more*, on page 12.

### Handle scenes with strong backlight

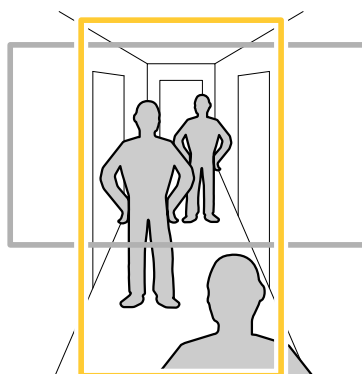
Dynamic range is the difference in light levels in an image. In some cases the difference between the darkest and the brightest areas can be significant. The result is often an image where either the dark or the bright areas are visible. Wide dynamic range (WDR) makes both dark and bright areas of the image visible.

1. Go to **Video > Image > Wide dynamic range**.
2. If you still have problems, go to **Exposure** and adjust the **Exposure zone** to cover the area of interest.

Find out more about WDR and how to use it at [axis.com/solutions/wide-dynamic-range-wdr](http://axis.com/solutions/wide-dynamic-range-wdr).

### Monitor long and narrow areas

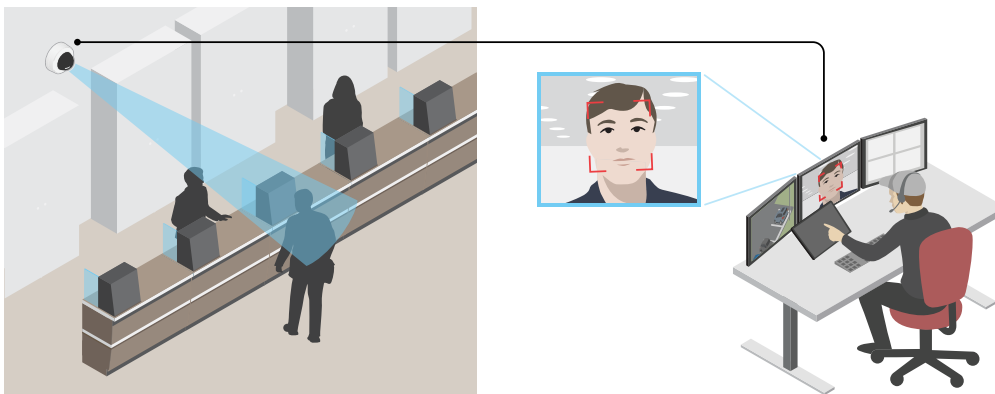
Use corridor format to better utilize the full field of view in a long and narrow area, for example a staircase, hallway, road, or tunnel.





1. Depending on your device, turn the camera or the 3-axis lens in the camera **90°** or **270°**.
2. If the device doesn't have automatic rotation of the view, go to **Video > Installation**.
3. Rotate the view **90°** or **270°**.

### Verify the pixel resolution


To verify that a defined part of the image contains enough pixels to, for example, recognize the face of a person, you can use the pixel counter.



1. Go to **Video > Image** and click  **A**.
2. Click  for **Pixel counter**.
3. In the camera's live view, adjust the size and position of the rectangle around the area of interest, for example where you expect faces to appear.  
You can see the number of pixels for each of the rectangle's sides, and decide if the values are enough for your needs.

### Hide parts of the image with privacy masks


You can create one or several privacy masks to hide parts of the image.

1. Go to **Video > Privacy masks**.
2. Click .
3. Click the new mask and type a name.
4. Adjust the size and placement of the privacy mask according to your needs.
5. To change the color for all privacy masks, click **Privacy masks** and select a color.

See also *Privacy masks, on page 12*

### Show an image overlay


You can add an image as an overlay in the video stream.

1. Go to **Video > Overlays**.
2. Click **Manage images**.
3. Upload or drag and drop an image.
4. Click **Upload**.
5. Select **Image** from the drop-down list and click .
6. Select the image and a position. You can also drag the overlay image in the live view to change the position.

### Show a text overlay

You can add a text field as an overlay in the video stream. This is useful for example when you want to display the date, time or a company name in the video stream.

1. Go to **Video > Overlays**.

2. Select **Text** and click  .
3. Type the text you want to display, or select modifiers to show for example the current date.
4. Select a position. You can also click-and-drag the overlay in the live view to change the position.


## View and record video

This section includes instructions about configuring your device. To learn more about how streaming and storage works, go to *Streaming and storage, on page 12*.

## Reduce bandwidth and storage

### Important

Reducing the bandwidth can lead to loss of detail in the image.

1. Go to **Video > Stream**.
2. Click  in the live view.
3. Select **Video format AV1** if your device supports it. Otherwise select **H.264**.
4. Go to **Video > Stream > General** and increase **Compression**.
5. Go to **Video > Stream > Zipstream** and do one or more of the following:

### Note

The **Zipstream** settings are used for all video encodings except MJPEG.

- Select the **Zipstream Strength** that you want to use.
- Turn on **Optimize for storage**. This can only be used if the video management software supports B-frames.
- Turn on **Dynamic FPS**.
- Turn on **Dynamic GOP** and set a high **Upper limit GOP length** value.

### Note

Most web browsers don't support H.265 decoding and because of this the device doesn't support it in its web interface. Instead you can use a video management system or application that supports H.265 decoding.


## View a live video stream on a monitor

Your camera can transmit a live video stream to an HDMI monitor even without a network connection. Use the monitor for surveillance purposes or for public viewing, for example in a store.

1. Connect an external monitor using the HDMI connector.
2. Go to **System > Video out** and turn on **HDMI**.
3. Select a **Source**. Rotate the image if needed.

## Set up network storage


To store recordings on the network, you need to set up your network storage.

1. Go to **System > Storage**.
2. Click  **Add network storage** under **Network storage**.
3. Type the IP address of the host server.
4. Type the name of the shared location on the host server under **Network share**.
5. Type the username and password.
6. Select the SMB version or leave it on **Auto**.

7. Select **Add share without testing** if you experience temporary connection issues, or if the share is not yet configured.
8. Click **Add**.

## Record and watch video


### Record video directly from the camera

1. Go to **Video > Stream**.
2. To start a recording, click  .

If you haven't set up any storage, click  and . For instructions on how to set up network storage, see *Set up network storage, on page 8*

3. To stop recording, click  again.

### Watch video

1. Go to **Recordings**.
2. Click  for your recording in the list.

## Verify that no one has tampered with the video

With signed video, you can make sure that no one has tampered with the video recorded by the camera.

1. Go to **Video > Stream > General** and turn on **Signed video**.
2. Record video directly on the device, or use AXIS Camera Station Pro or another compatible video management software. For AXIS Camera Station Pro instructions, see the *AXIS Camera Station Pro user manual*.
3. Export the recorded video.
4. Use *Axis signed media verifier* tool to verify the recording.

## Set up rules for events

You can create rules to make your device perform an action when certain events occur. A rule consists of conditions and actions. The conditions can be used to trigger the actions. For example, the device can start a recording or send an email when it detects motion, or show an overlay text while the device is recording.

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.

## Record video when the camera detects an object

This example explains how to set up the camera to start recording to the SD card when the camera detects an object. The recording will include five seconds before detection and one minute after detection ends.

Before you start:

- Make sure you have an SD card installed.

Make sure that AXIS Object Analytics is running:

1. Go to **Apps > AXIS Object Analytics**.
2. Start the application if it is not already running.
3. Make sure you have set up the application according to your needs.

Create a rule:

1. Go to **System > Events** and add a rule.
2. Type a name for the rule.
3. In the list of conditions, under **Application**, select **Object Analytics**.
4. In the list of actions, under **Recordings**, select **Record video while the rule is active**.
5. In the list of storage options, select **SD\_DISK**.
6. Select a camera and a stream profile.
7. Set the prebuffer time to 5 seconds.
8. Set the postbuffer time to 1 minute.
9. Click **Save**.

### Use PIR and audio to deter intruders

This example explains how to set up the camera to play an audio clip with a barking dog when the PIR sensor detects movement outside office hours.

Before you start:

- Add an audio clip with a barking dog to the device. For more information, see .

Create a rule:

1. Go to **System > Events** and add a rule.
2. Enter a name for the rule.
3. In the list of conditions, select **Device status > PIR sensor**.
4. Click **+** to add a second condition.
5. In the list of conditions, select **Scheduled and recurring > Schedule**.
6. In the list of schedules, select **After hours** .
7. In the list of actions, select **Audio clips > Play audio clip**.
8. In the list of clips, select **Dog barking**.
9. Click **Save**.

### Audio

This device has automatic voice enhancement.

### Add audio to your recording

Turn on audio:

1. Go to **Video > Stream > Audio** and include audio.
2. If the device has more than one input source, select the correct one in **Source**.
3. Go to **Audio > Device settings** and turn on the correct input source.

Edit the stream profile that is used for the recording:

4. Go to **System > Stream profiles** and select the stream profile.
5. Select **Include audio** and turn it on.
6. Click **Save**.

## 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

### Privacy masks

A privacy mask is a user-defined area that prevents users from viewing a part of the monitored area. In the video stream, privacy masks appear as blocks of solid color.

You'll see the privacy mask on all snapshots, recorded video, and live streams.

You can use the VAPIX® application programming interface (API) to hide the privacy masks.

#### Important

If you use multiple privacy masks it may affect the product's performance.

You can create several privacy masks. Each mask can have 3 to 10 anchor points.

### Streaming and storage

#### Video compression formats

Decide which compression method to use based on your viewing requirements, and on the properties of your network. The available options are:

##### Motion JPEG

Motion JPEG, or MJPEG, is a digital video sequence that is made up of a series of individual JPEG images. These images are then displayed and updated at a rate sufficient to create a stream that shows constantly updated motion. For the viewer to perceive motion video the rate must be at least 16 image frames per second. Full motion video is perceived at 30 (NTSC) or 25 (PAL) frames per second.

The Motion JPEG stream uses considerable amounts of bandwidth, but provides excellent image quality and access to every image contained in the stream.

##### H.264 or MPEG-4 Part 10/AVC

#### Note

H.264 is a licensed technology. The Axis product includes one H.264 viewing client license. To install additional unlicensed copies of the client is prohibited. To purchase additional licenses, contact your Axis reseller.

H.264 can, without compromising image quality, reduce the size of a digital video file by more than 80% compared to the Motion JPEG format and by as much as 50% compared to older MPEG formats. This means that less network bandwidth and storage space are required for a video file. Or seen another way, higher video quality can be achieved for a given bitrate.

##### H.265 or MPEG-H Part 2/HEVC

H.265 can, without compromising image quality, reduce the size of a digital video file by more than 25% compared to H.264.

#### Note

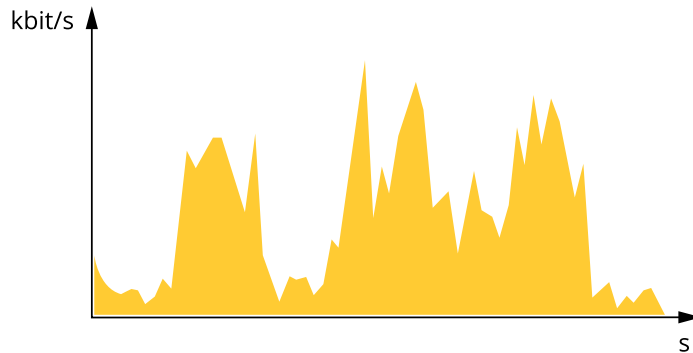
- H.265 is licensed technology. The Axis product includes one H.265 viewing client license. Installing additional unlicensed copies of the client is prohibited. To purchase additional licenses, contact your Axis reseller.
- Most web browsers don't support H.265 decoding and because of this the camera doesn't support it in its web interface. Instead you can use a video management system or application supporting H.265 decoding.

### Bitrate control

Bitrate control helps you to manage the bandwidth consumption of your video stream.

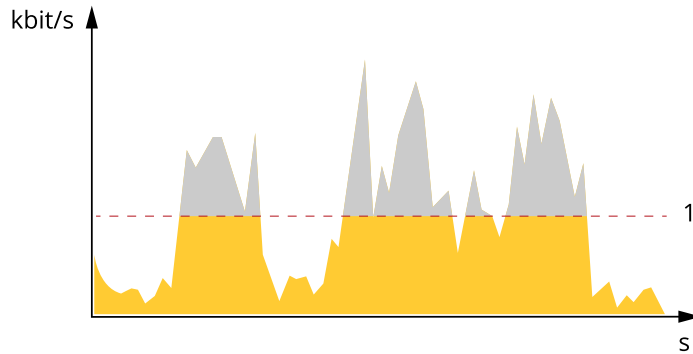
#### Variable bitrate (VBR)

Variable bitrate allows the bandwidth consumption to vary depending on the level of activity in the scene. The more activity, the more bandwidth you need. With variable bitrate you are guaranteed constant image quality, but you need to make sure you have storage margins.



**Maximum bitrate (MBR)**

Maximum bitrate lets you set a target bitrate to handle bitrate limitations in your system. You might see a decline in image quality or frame rate as the instantaneous bitrate is kept below the specified target bitrate. You can choose to prioritize either image quality or frame rate. We recommend that you configure the target bitrate to a higher value than the expected bitrate. This gives you a margin in case there is a high level of activity in the scene.

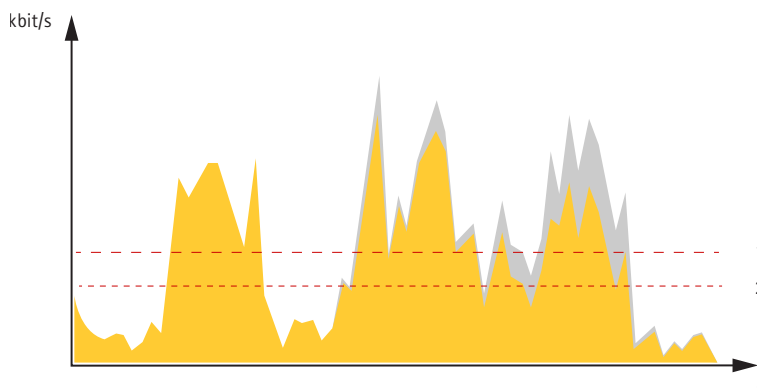


1 Target bitrate

**Average bitrate (ABR)**

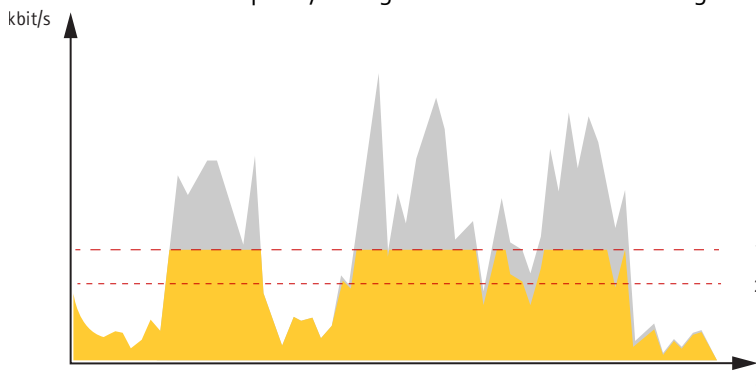
With average bitrate, the bitrate is automatically adjusted over a longer period of time. This is so you can meet the specified target and provide the best video quality based on your available storage. Bitrate is higher in scenes with a lot of activity, compared to static scenes. You are more likely to get better image quality when in scenes with a lot of activity if you use the average bitrate option. You can define the total storage required to store the video stream for a specified amount of time (retention time) when image quality is adjusted to meet the specified target bitrate. Specify the average bitrate settings in one of the following ways:

- To calculate the estimated storage need, set the target bitrate and the retention time.
- To calculate the average bitrate, based on available storage and required retention time, use the target bitrate calculator.



- 1 Target bitrate
- 2 Actual average bitrate

You can also turn on maximum bitrate and specify a target bitrate within the average bitrate option.



- 1 Target bitrate
- 2 Actual average bitrate

## **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](http://help.axis.com).

### **AXIS Object Analytics**

AXIS Object Analytics is an analytic application that comes preinstalled on the camera. It detects objects that move in the scene and classifies them as, for example, humans or vehicles. You can set up the application to send alarms for different types of objects. To find out more about how the application works, see *AXIS Object Analytics user manual*.

### **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*.

### **Metadata visualization**

Analytics metadata is available for moving objects in the scene. Supported object classes are visualized in the video stream through a bounding box surrounding the object, along with information about the object type and confidence level of the classification. To learn more about how to configure and consume analytics metadata, see *AXIS Scene Metadata integration guide*.

## **Advanced wireless settings**

The most common security method is WPA™ Personal. This device also supports WPA™ Enterprise which is a more secure method. All settings must match the settings in the access point.

### **WPA™ Personal**

The security method **WPA Personal** is designed for small networks and does not require an authentication server.

## WPA™ Enterprise

The security method **WPA Enterprise** is designed for large networks and requires an authentication server. The network is protected by EAPoL (Extensible Authentication Protocol Over LAN).

Select the WPA enterprise type used by the access point:

- EAP-TLS. See *page 15*.
- EAP-PEAP/MSCHAPv2. See *page 15*.


### EAP-TLS

The authentication protocol **EAP-TLS** (Extensible Authentication Protocol – Transport Layer Security) allows the client and server to authenticate each other using digital certificates provided by a Certification Authority. To gain access to the protected network, the Axis product presents its certificate to the network access point. Access is granted if the certificate is approved.

#### Important

To ensure successful certificate validation, time synchronization should be performed on all clients and servers prior to configuration.

### Configure the wireless settings with WPA™ Enterprise and EAP-TLS

1. Go to **System > WLAN**.
2. Click  **Add network**.
3. In the list of authentication methods, select **WPA-Enterprise EAP-TLS**.
4. Enter the SSID associated with your certificate.
5. Select the **EAPoL version** (1, 2 or 3) as used in the access point.
6. Select the **CA certificate** and the **Client certificate** to use for wireless authentication.
7. Click **Save**.


### EAP-PEAP/MSCHAPv2

The authentication protocol **EAP-PEAP/MSCHAPv2** (Extensible Authentication Protocol – Protected Extensible Authentication Protocol/Microsoft Challenge Handshake Authentication Protocol) allows the client to authenticate the network using a digital certificate provided by a Certification Authority. The network authenticates the client using an identity and a password. To gain access to the protected network, the Axis product presents its identity and password to the network access point. If these credentials are approved, the access point allows access on a preconfigured port.

#### Important

To ensure successful certificate validation, time synchronization should be performed on all clients and servers prior to configuration.

### Configure the wireless settings with WPA™ Enterprise and EAP-PEAP/MSCHAPv2

1. Go to **System > WLAN**.
2. Click  **Add network**.
3. In the list of authentication methods, select **WPA-Enterprise EAP-PEAP/MSCHAPv2**.
4. Enter the SSID associated with your certificate.
5. Enter the password for your user identity.
6. Select the **EAPoL version** (1, 2 or 3) as used in the access point.

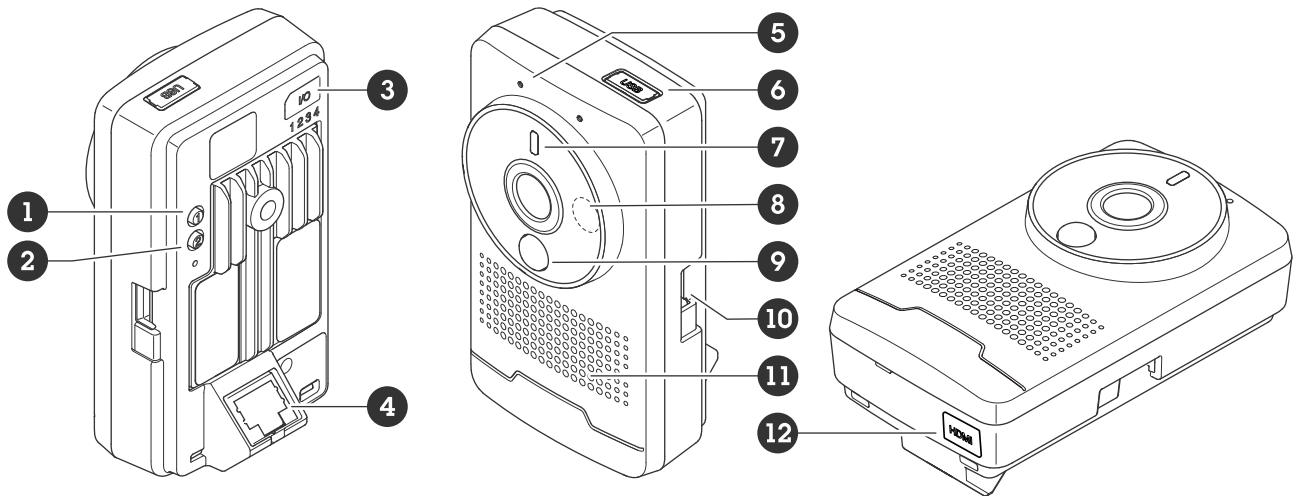
7. Select the **Peap version** (0 or 1) as used in the access point.
8. Select the **Label** that the access point uses when using Peap version 1. Select 1 to use client EAP encryption; select 2 to use client PEAP encryption.
9. Select the **CA certificate** with which to validate the network/AP certificate.
10. Click **Save**.

### **Wireless certificates**

Wireless network certificates are used to authenticate devices on a wireless network. Wireless networks using the WPA™ Enterprise security method are protected by EAPoL (Extensible Authentication Protocol over Lan), which is part of the IEEE 802.1X standard. The client authenticates the server using digital certificates. The server authenticates the client using digital certificates or a password depending on the selected WPA Enterprise type.

## Specifications

### Product overview



- 1 Control button
- 2 WLAN setup button
- 3 I/O connector
- 4 Network connector
- 5 Microphone
- 6 USB connector
- 7 Status LED
- 8 IR LED
- 9 PIR sensor
- 10 SD card slot
- 11 Speaker
- 12 MicroHDMI connector type D

### LED indicators

Status LED	Indication
Unlit	Connection and normal operation.
Green	Shows steady green for 10 seconds for normal operation after startup completed.
Amber	Steady during startup. Flashes during firmware upgrade or reset to factory default.
Amber/Red	Flashes amber/red if network connection is unavailable or lost.
Red	Shows steady red when live stream or recording is on.
Blue	Steady blue during WLAN setup mode.


### SD card slot

#### NOTICE

- Risk of damage to SD card. Don't use sharp tools, metal objects, or excessive force when inserting or removing the SD card. Use your fingers to insert and remove the card.
- Risk of data loss and corrupted recordings. Unmount the SD card from the device's web interface before removing it. Don't remove the SD card while the product is running.

This device supports microSD/microSDHC/microSDXC cards.

For SD card recommendations, see [axis.com](http://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 21*.
- 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.

### WLAN setup button

The WLAN setup button is used for setting up WLAN connection.

## Connectors

### HDMI connector

Use the microHDMI™ connector to connect a display or public view monitor.

### Network connector

RJ45 Ethernet connector with Power over Ethernet (PoE).

### USB connector

Use the USB connector to connect external accessories. See the product's datasheet for supported accessories.

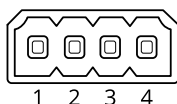
### I/O connector


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.

**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.

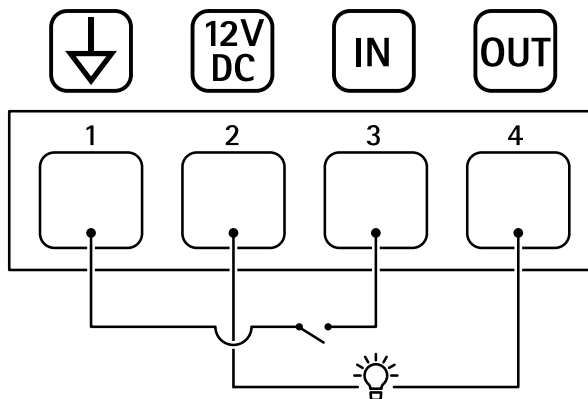
4-pin terminal block



Function	Pin	Notes	Specifications
DC ground	1		0 VDC
DC output	2	 Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	12 VDC Max load = 25 mA

Digital Input	3	Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 VDC
Digital Output	4	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 25 mA
- 3 Digital input
- 4 Digital output

## 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.

For more information about cleaning of Axis devices, see the white paper *Chemical resistance to common cleaning agents*.

## 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 17*.
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](https://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](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 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](http://axis.com/support/device-software).
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.

You can use AXIS Device Manager to upgrade multiple devices at the same time. Find out more at [axis.com/products/axis-device-manager](http://axis.com/products/axis-device-manager).

## 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 21*.

#### 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](http://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](http://axis.com/vms).

### Problems with streaming

#### Multicast H.264 only accessible by local clients

Check if your router supports multicasting, or if you need to configure the router settings between the client and the device. You might need to increase the TTL (Time To Live) value.

#### No multicast H.264 displayed in the client

Check with your network administrator that the multicast addresses used by the Axis device are valid for your network.

Check with your network administrator to see if there is a firewall that prevents viewing.

#### Poor rendering of H.264 images

Ensure that your graphics card uses the latest driver. You can usually download the latest drivers from the manufacturer's website.

#### Color saturation is different in H.264 and Motion JPEG

Modify the settings for your graphics adapter. Check the adapter's documentation for more information.

**Lower frame rate than expected**

- See *Performance considerations, on page 24*.
- Reduce the number of applications running on the client computer.
- Limit the number of simultaneous viewers.
- Check with the network administrator that there is enough bandwidth available.
- Lower the image resolution.

**Can't select H.265 encoding in live view**

Web browsers don't support H.265 decoding. Use a video management system or application that supports H.265 decoding.

**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](https://axis.com/support).

**Performance considerations**

When you set up your system, it's important to consider how different settings and situations affect performance. Some factors affect bandwidth (bitrate), others affect frame rate, and some affect both.

The most important factors to consider:

- High image resolution or lower compression levels result in images containing more data which in turn affects the bandwidth.
- Rotating the image in the GUI can increase the product's CPU load.
- Access by large numbers of Motion JPEG clients or unicast H.264/H.265/AV1 clients affects the bandwidth.
- Simultaneous viewing of different streams (resolution, compression) by different clients affects both frame rate and bandwidth.  
Use identical streams wherever possible to maintain a high frame rate. Stream profiles can be used to ensure that streams are identical.
- Accessing video streams with different codecs simultaneously affects both frame rate and bandwidth. For optimal performance, use streams with the same codec.
- Heavy usage of event settings affects the product's CPU load which in turn affects the frame rate.
- Using HTTPS may reduce frame rate, in particular if streaming Motion JPEG.
- Heavy network utilization due to poor infrastructure affects the bandwidth.
- Viewing on poorly performing client computers lowers perceived performance and affects frame rate.

- Running multiple AXIS Camera Application Platform (ACAP) applications simultaneously may affect the frame rate and the general performance.

### **Contact support**

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

## Cybersecurity

Cybersecurity supports a successful product lifecycle with minimized risks. You can find in-depth information and documentation about our cybersecurity approach at [axis.com/about-axis/cybersecurity](https://axis.com/about-axis/cybersecurity). Follow the cybersecurity guidelines below to receive product security notifications from Axis and to configure your product for a secure lifecycle and decommissioning.

At *Axis Trust Center*, you can find information about how Axis implements security compliance, transparency, data protection, and privacy.

### Vulnerability management

Axis is a *Common Vulnerability and Exposures (CVE) Numbering Authority (CNA)*. To minimize your risk of exposure, we follow industry standards when identifying and resolving vulnerabilities in our devices, software, and services. Refer to [axis.com/vulnerability-management](https://axis.com/vulnerability-management) for information about our vulnerability management policy or to report a vulnerability.

### Security notifications

Subscribe to Axis security notification emails at [axis.com/security-notification-service](https://axis.com/security-notification-service). We will send you information about vulnerabilities, corresponding security advisories, and other security-related matters for your Axis product.

### Secure product lifecycle

Axis minimizes risks throughout the lifetime of our products through secure lifecycle management. Use our hardening guides at [help.axis.com](https://help.axis.com) to more securely configure and operate your Axis products and to find information about:

**Secure first-use** – Axis products are pre-configured with high default protection to allow for secure initialization and encrypted communication from the very start.

**Intended use and common configuration mistakes** – Our guides provide information about the intended usage of Axis products, including common security-relevant misuse and configuration mistakes that should be avoided.

**Managing vulnerabilities and supply chain transparency** – A Software Bill of Material (SBOM) is published with every software release on [axis.com](https://axis.com) to disclose vulnerabilities and improve supply chain transparency.

**Decommissioning and the secure erasure of data** – To securely decommission a product when it reaches the end of its lifecycle, reset it to factory default settings. This erases your configurations, stored data, and sensitive information.



T10229282

2026-07 (M4.2)

© 2025 – 2026 Axis Communications AB