

AXIS Q19 Thermal Camera Series

AXIS Q1971-E Thermal Camera

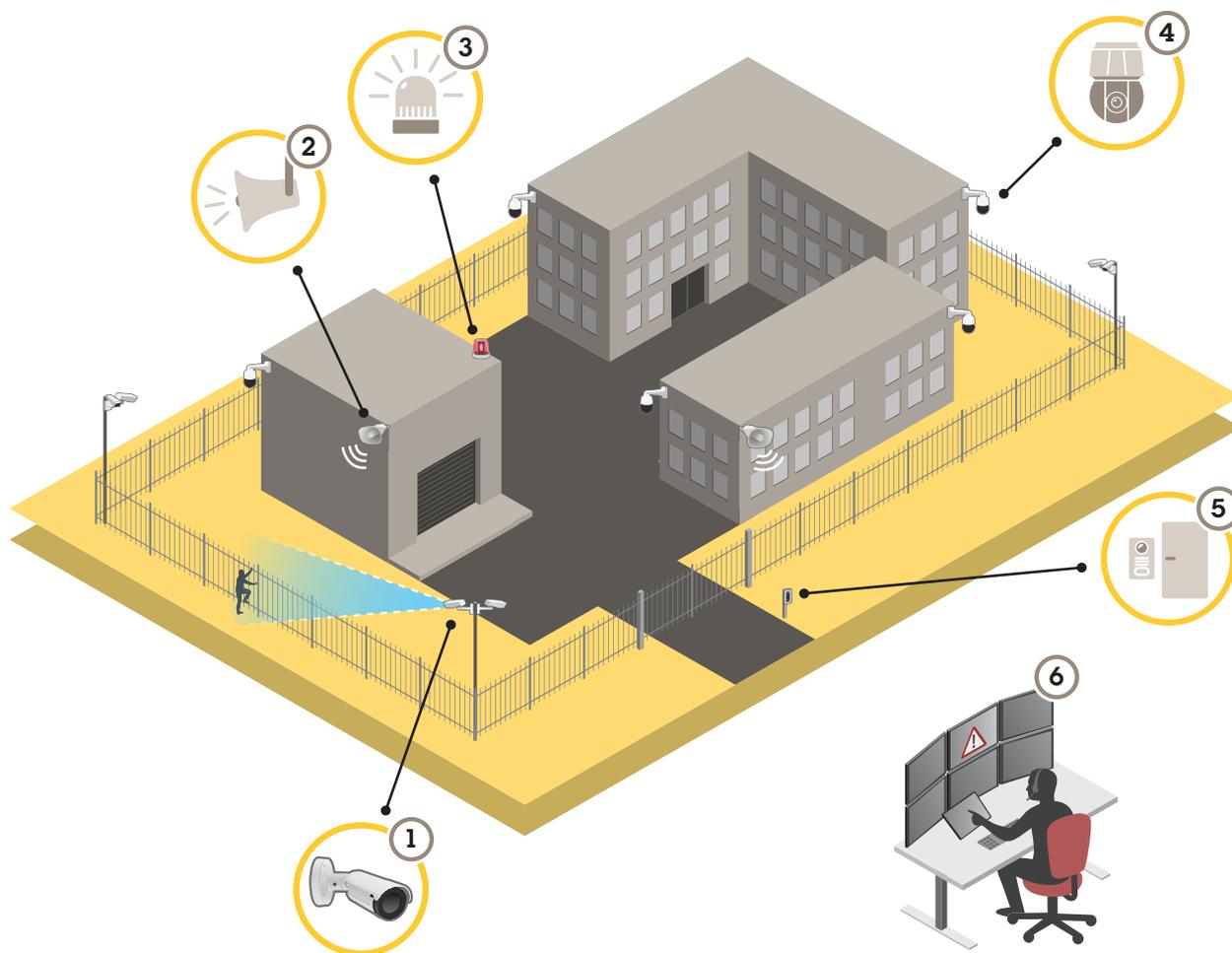
AXIS Q1972-E Thermal Camera

Table of Contents

Solution overview 4
 4
 Perimeter protection..... 4
 Installation 5
 Preview mode 5
 Get started..... 6
 Find the device on the network..... 6
 Browser support 6
 Open the device's web interface..... 6
 Create an administrator account..... 6
 Secure passwords..... 7
 Make sure that no one has tampered with the device software 7
 Web interface overview 7
 Configure your device..... 8
 Basic settings 8
 Adjust the image..... 8
 Level the camera 8
 Select exposure mode 8
 Handle scenes with strong backlight..... 8
 Stabilize a shaky image with image stabilization..... 8
 Monitor long and narrow areas 9
 Verify the pixel resolution..... 9
 Hide parts of the image with privacy masks..... 10
 Show an image overlay 10
 Show a text overlay 10
 Add street names and compass direction to the image..... 10
 View and record video 11
 Reduce bandwidth and storage 11
 Set up network storage 11
 Record and watch video 11
 Verify that no one has tampered with the video..... 12
 Set up rules for events 12
 Trigger an action 12
 Record video when the camera detects an object..... 12
 Show a text overlay in the video stream when the device detects an object 13
 Provide visual indication of an ongoing event..... 13
 Record video when the camera detects loud noises 14
 Record video when the camera detects impact 15
 Detect tampering with input signal 15
 Set up the intrusion alarm 16
 Send an email automatically if someone spray paints the lens..... 16
 Audio..... 17
 Add audio to your recording 17
 Connect to a network speaker..... 17
 The web interface 18
 Learn more..... 19
 Color palettes 19
 Privacy masks 19
 Overlays 19
 Streaming and storage..... 19
 Video compression formats..... 19
 How do Image, Stream, and Stream profile settings relate to each other? 20
 Bitrate control..... 20

- Edge-to-edge technology..... 22
 - Speaker pairing 22
- Analytics and apps 22
 - AXIS Perimeter Defender 22
- Cybersecurity..... 24
 - Axis Edge Vault 24
 - Signed OS..... 24
 - Secure boot 24
 - Secure keystore 24
 - Axis device ID..... 24
 - Signed video 24
 - Encrypted file system 24
 - Axis security notification service 25
 - Vulnerability management..... 25
 - Secure operation of Axis devices 25
- Specifications..... 26
 - Product overview 26
 - LED indicators..... 26
 - SD card slot..... 26
 - Buttons..... 27
 - Control button 27
 - Connectors 27
 - Network connector 27
 - Audio connector 27
 - I/O connector 27
 - Power connector 28
- Clean your device..... 29
- Troubleshooting..... 30
 - Reset to factory default settings 30
 - AXIS OS options 30
 - Check the current AXIS OS version 30
 - Upgrade AXIS OS..... 30
 - Technical problems and possible solutions 31
 - Performance considerations 33
 - Contact support..... 33

Solution overview



- 1 Thermal camera with AXIS Perimeter Defender
- 2 Horn speaker
- 3 Flashing beacon
- 4 PTZ network camera
- 5 Door controller
- 6 Surveillance center

Perimeter protection

For areas in need of intrusion detection, you can set up perimeter protection using thermal cameras with analytics. The main objective for perimeter protection is to detect a threat or an actual intrusion at the earliest possible stage.

To set up perimeter protection, you need to install an analytics application for perimeter surveillance and protection on your thermal camera. Axis provides the AXIS Perimeter Defender application for this purpose. You can read more about AXIS Perimeter Defender at axis.com/products/axis-perimeter-defender

- To let possible intruders know that your perimeter is protected, use a flashing beacon (3). See .
- To warn and deter, connect a horn speaker (2) that plays a pre-recorded warning message. See .

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

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 6*.

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 7*.
3. Re-enter the password.
4. Accept the license agreement.
5. Click **Add account**.

Important

The device has no default account. If you lose the password for your administrator account, you must reset the device. See *Reset to factory default settings, on page 30*.

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 30*.
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

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.

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 9.

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 19.

Level the camera

To adjust the view in relation to a reference area or an object, use the level grid in combination with a mechanical adjustment of the camera.

1. Go to **Video > Image >** and click  **A**.
2. Click  to show the level grid.
3. Adjust the camera mechanically until the position of the reference area or the object is aligned with the level grid.

Select exposure mode

To improve image quality for specific surveillance scenes, use exposure modes. Exposure modes lets you control aperture, shutter speed, and gain. Go to **Video > Image > Exposure** and select between the following exposure modes:

- For most use cases, select **Automatic** exposure.

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. Use the **Local contrast** slider to adjust the amount of WDR.
3. 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/web-articles/wdr.

Stabilize a shaky image with image stabilization

Image stabilization is suitable in environments where the product is mounted in an exposed location where vibrations can occur, for example, due to wind or passing traffic.

The feature makes the image smoother, steadier, and less blurry. It also reduces the file size of the compressed image and lowers the bitrate of the video stream.

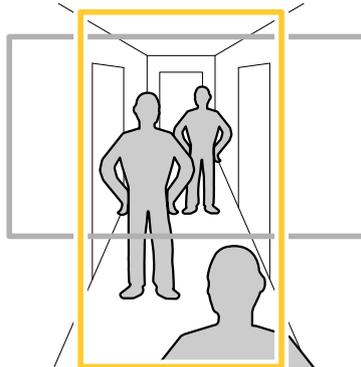
Note

When you turn on image stabilization, the image is slightly cropped, which lowers the maximum resolution.

1. Go to **Video > Installation > Image correction**.
2. Turn on **Image stabilization**.

Monitor long and narrow areas

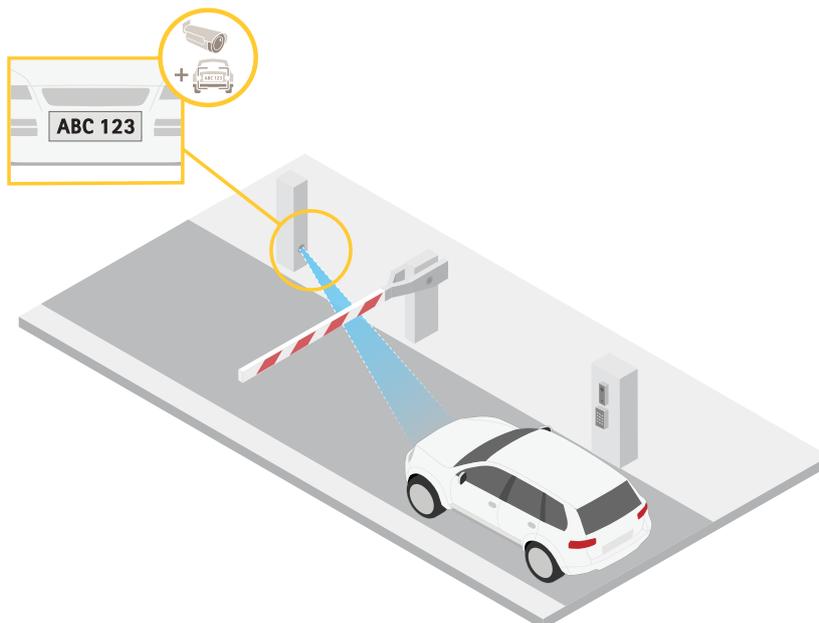
Use corridor format to better utilize the full field of view in a long and narrow area, for example a staircase, hallway, road, or tunnel.



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 license plates, you can use the pixel counter.



1. Go to **Video > Image**.

2. Click .
3. Click  for Pixel counter.
4. In the camera's live view, adjust the size and position of the rectangle around the area of interest, for example where you expect license plates to appear.
5. 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 19*

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.

Add street names and compass direction to the image

Note

The street name and compass direction will be visible on all video streams and recordings.

1. Go to **Apps**.
2. Select **axis-orientationaid**.
3. Click **Open**.

4. To add a street name, click **Add text** and modify the text to fit the street.
5. To add a compass, click **Add compass** and modify the compass to fit the image.

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 19.

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.

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 11*

- To stop recording, click  again.

Watch video

- Go to **Recordings**.
- 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.

- Go to **Video > Stream > General** and turn on **Signed video**.
- Use AXIS Camera Station (5.46 or later) or another compatible video management software to record video. For instructions, see the *AXIS Camera Station user manual*.
- Export the recorded video.
- Use AXIS File Player to play the video. *Download AXIS File Player*.

 indicates that no one has tampered with the video.

Note

To get more information about the video, right-click the video and select **Show digital signature**.

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

- 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.
- Enter a **Name**.
- 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.
- 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.

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 Video Motion Detection is running:

- Go to **Apps > AXIS Video Motion Detection**.
- 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 **VMD4**.
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**.

Show a text overlay in the video stream when the device detects an object

This example explains how to display the text "Motion detected" when the device detects an object.

Make sure that AXIS Video Motion Detection is running:

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

Add the overlay text:

1. Go to **Video > Overlays**.
2. Under **Overlays**, select **Text** and click .
3. Enter #D in the text field.
4. Choose text size and appearance.
5. To position the text overlay, click  and select an option.

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 **VMD4**.
4. In the list of actions, under **Overlay text**, select **Use overlay text**.
5. Select a video channel.
6. In **Text**, type "Motion detected".
7. Set the duration.
8. Click **Save**.

Note

If you update the overlay text it will be automatically updated on all video streams dynamically.

Provide visual indication of an ongoing event

You have the option to connect the AXIS I/O Indication LED to your network camera. This LED can be configured to turn on whenever certain events occur in the camera. For example, to let people know that video recording is in progress.

Required hardware

- AXIS I/O Indication LED
- An Axis network video camera

Note

AXIS I/O Indication LED should be connected to an output port.

Note

For instructions on how to connect the AXIS I/O Indication LED, see the installation guide provided with the product.

The following example shows how to configure a rule that turns on the AXIS I/O Indication LED to indicate that camera is recording.

1. Go to **System > Accessories > I/O ports**.
2. Make sure that the port you connected the AXIS I/O Indication LED to is set to **Output**. Set the normal state to **Circuit open**.
3. Go to **System > Events**.
4. Create a new rule.
5. Select the **Condition** that must be met to trigger the camera to start recording. It can, for example, be a time schedule or motion detection.
6. In the list of actions, select **Record video**. Select a storage space. Select a stream profile or create a new. Also set the **Prebuffer** and **Postbuffer** as required.
7. Save the rule.
8. Create a second rule and select the same **Condition** as in the first rule.
9. In the list of actions, select **Toggle I/O while the rule is active**, and then select the port the AXIS I/O Indication LED is connected to. Set the state to **Active**.
10. Save the rule.

Other scenarios where AXIS I/O Indication LED can be used are for example:

- Configure the LED to turn on when the camera starts, to indicate the presence of the camera. Select **System ready** as a condition.
- Configure the LED to turn on when live stream is active to indicate that a person or a program is accessing a stream from the camera. Select **Live stream accessed** as a condition.

Record video when the camera detects loud noises

This example explains how to set up the camera to start recording to the SD card five seconds before it detects loud noise and to stop two minutes after.

Turn on audio:

1. Set up the stream profile to include audio, see *Add audio to your recording, on page 17*.

Turn on audio detection:

1. Go to **System > Detectors > Audio detection**.
2. Adjust the sound level 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 **Audio**, select **Audio Detection**.
4. In the list of actions, under **Recordings**, select **Record video**.
5. In the list of storage options, select **SD_DISK**.
6. Select the stream profile where audio has been turned on.
7. Set the prebuffer time to 5 seconds.

8. Set the postbuffer time to 2 minutes.
9. Click **Save**.

Record video when the camera detects impact

Shock detection allows the camera to detect tampering caused by vibrations or shock. Vibrations due to the environment or to an object can trigger an action depending on the shock sensitivity range, which can be set from 0 to 100. In this scenario, someone is throwing rocks at the camera after hours and you would like to get a video clip of the event.

Turn on shock detection:

1. Go to **System > Detectors > Shock detection**.
2. Turn on shock detection, and adjust the shock sensitivity.

Create a rule:

3. Go to **System > Events > Rules** and add a rule.
4. Type a name for the rule.
5. In the list of conditions, under **Device status**, select **Shock detected**.
6. Click **+** to add a second condition.
7. In the list of conditions, under **Scheduled and recurring**, select **Schedule**.
8. In the list of schedules, select **After hours**.
9. In the list of actions, under **Recordings**, select **Record video while the rule is active**.
10. Select where to save the recordings.
11. Select a **Camera**.
12. Set the prebuffer time to 5 seconds.
13. Set the postbuffer time to 50 seconds.
14. Click **Save**.

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 27*.

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

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**.

Set up the intrusion alarm

Use the intrusion alarm switch to, for example, send a notification if someone opens the camera housing.

Before you start

- Connect the intrusion alarm switch to pin 1 (ground) and pin 3 (digital input) of the camera's I/O connector.

Configure the input port:

1. Go to **System > Accessories > I/O ports**.
2. For **Port 1**:
 - 2.1. Select **Circuit closed**.

Add an email recipient:

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

Create a rule:

11. Go to **System > Events > Rules** and add a rule.
12. Type a name for the rule.
13. In the list of conditions, under **I/O**, select **Digital input**.
14. In the list of ports, select **Port 1**.
15. In the list of actions, under **Notifications**, select **Send notification to email**.
16. Select a recipient from the list or go to **Recipients** to create a new recipient.
To create a new recipient, click . To copy an existing recipient, click .
17. Type a subject line and message for the email.
18. Click **Save**.

Send an email automatically if someone spray paints the lens

Activate the tampering detection:

1. Go to **System > Detectors > Camera tampering**.
2. Set a value for **Trigger delay**. The value indicates the time that must pass before an email is sent.

Add an email recipient:

3. Go to **System > Events > Recipients** and add a recipient.
4. Type a name for the recipient.
5. Select **Email**.

6. Type an email address to send the email to.
7. The camera doesn't have its own email server, so it has to log into another email server to send mails. Fill in the rest of the information according to your email provider.
8. To send a test email, click **Test**.
9. Click **Save**.

Create a rule:

10. Go to **System > Events > Rules** and add a rule.
11. Type a name for the rule.
12. In the list of conditions, under **Video**, select **Tampering**.
13. In the list of actions, under **Notifications**, select **Send notification to email** and then select the recipient from the list.
14. Type a subject and a message for the email.
15. Click **Save**.

Audio

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.
4. If you make any changes to the input source, click **Apply changes**.

Edit the stream profile that is used for the recording:

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

Connect to a network speaker

Network speaker pairing allows you to use a compatible Axis network speaker as if it is connected directly to the camera. Once paired, the speaker acts as an audio out device where you can play audio clips and transmit sound through the camera.

Important

For this feature to work with a video management software (VMS), you must first pair the camera with the network speaker, then add the camera to your VMS.

Pair camera with network speaker

1. Go to **System > Edge-to-edge > Pairing**.
2. Click  **Add** and select the pairing type **Audio** from the drop-down list.
3. Select **Speaker pairing**.
4. Type the network speaker's IP address, username and password.
5. Click **Connect**. A confirmation message appears.

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

Color palettes

To help the human eye distinguish details in a thermal image, you can apply a color palette to the image. The colors in the palette are artificially created pseudocolors that emphasize temperature differences.

The product has several color palettes to choose from. If an operator watches the video stream, you can choose any of the palettes. If the video stream is only used by applications, select the white-hot palette.

Privacy masks

A privacy mask is a user-defined area that covers a part of the monitored area. In the video stream, privacy masks appear either as blocks of solid color or with a mosaic pattern.

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.

Overlays

Overlays are superimposed over the video stream. They are used to provide extra information during recordings, such as a timestamp, or during product installation and configuration. You can add either text or an image.

The video streaming indicator is another type of overlay. It shows you that the live view video stream is live.

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

Note

To ensure support for the Opus audio codec, the Motion JPEG stream is always sent over RTP.

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.

How do Image, Stream, and Stream profile settings relate to each other?

The **Image** tab contains camera settings that affect all video streams from the product. If you change something in this tab, it immediately affects all video streams and recordings.

The **Stream** tab contains settings for video streams. You get these settings if you request a video stream from the product and don't specify for example resolution, or frame rate. When you change the settings in the **Stream** tab, it doesn't affect ongoing streams, but it will take effect when you start a new stream.

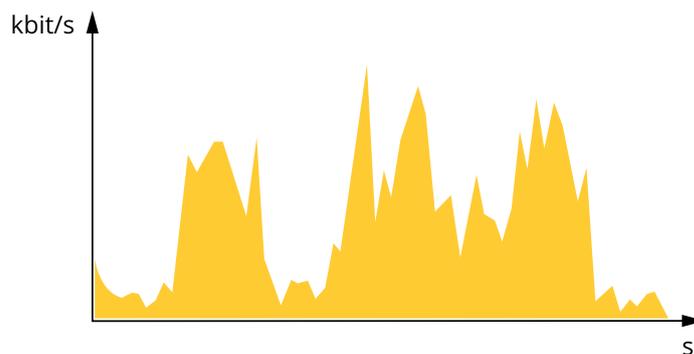
The **Stream profiles** settings override the settings from the **Stream** tab. If you request a stream with a specific stream profile, the stream contains the settings of that profile. If you request a stream without specifying a stream profile, or request a stream profile that doesn't exist in the product, the stream contains the settings from the **Stream** tab.

Bitrate control

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

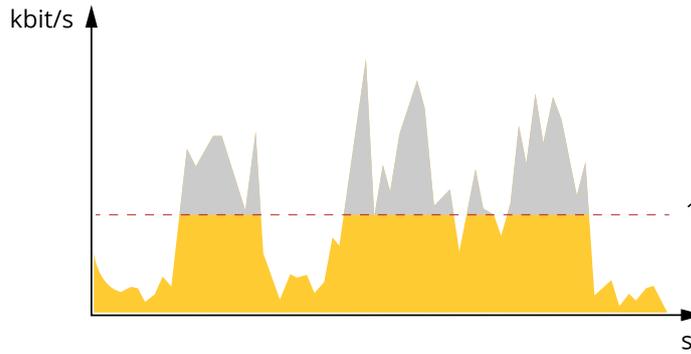
Variable bitrate (VBR)

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.

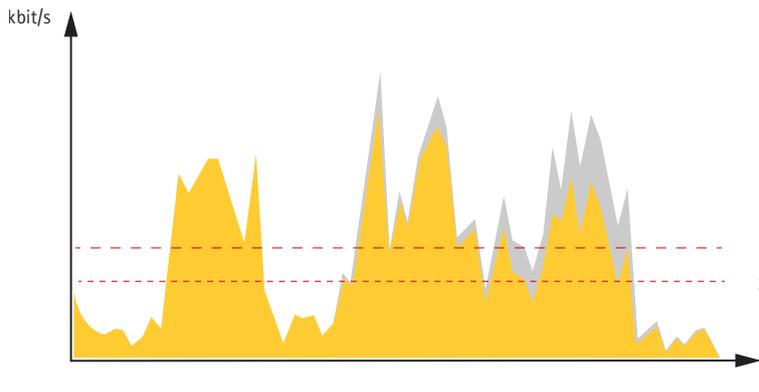


1 Target bitrate

Average bitrate (ABR)

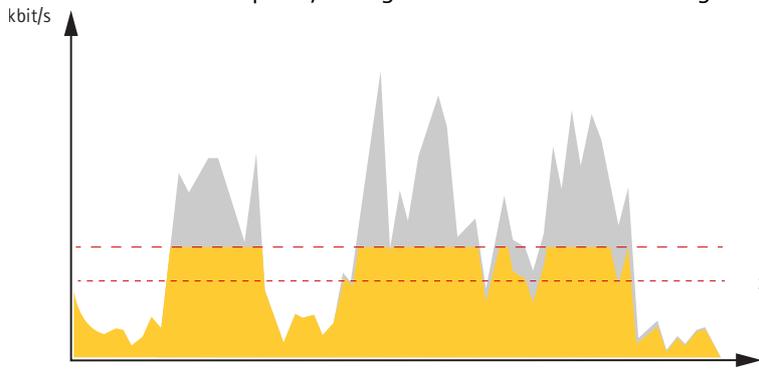
With average bitrate, the bitrate is automatically adjusted over a longer period of time. This is so you can meet the specified target and provide the best video quality based on your available storage. Bitrate is higher in scenes with a lot of activity, compared to static scenes. You are more likely 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

Edge-to-edge technology

Edge-to-edge is a technology that makes IP devices communicate directly with each other. It offers smart pairing functionality between, for example, Axis cameras and Axis audio or radar products.

Note

Make sure the paired devices run the same AXIS OS version.

For more information, see the white paper "Edge-to-edge technology" at whitepapers.axis.com/edge-to-edge-technology.

Speaker pairing

Edge-to-edge speaker pairing allows you to use a compatible Axis network speaker as if it's part of your camera. Once paired, the speaker's features are integrated in the camera's web interface and the network speaker acts as an audio out device where you can play audio clips and transmit sound through the camera.

The camera will identify itself to the VMS as a camera with integrated audio output and redirect any played audio to the speaker.

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.

Note

- Several apps can run at the same time but some apps might not be compatible with each other. Certain combinations of apps might require too much processing power or memory resources when run in parallel. Verify that the apps work together before deployment.

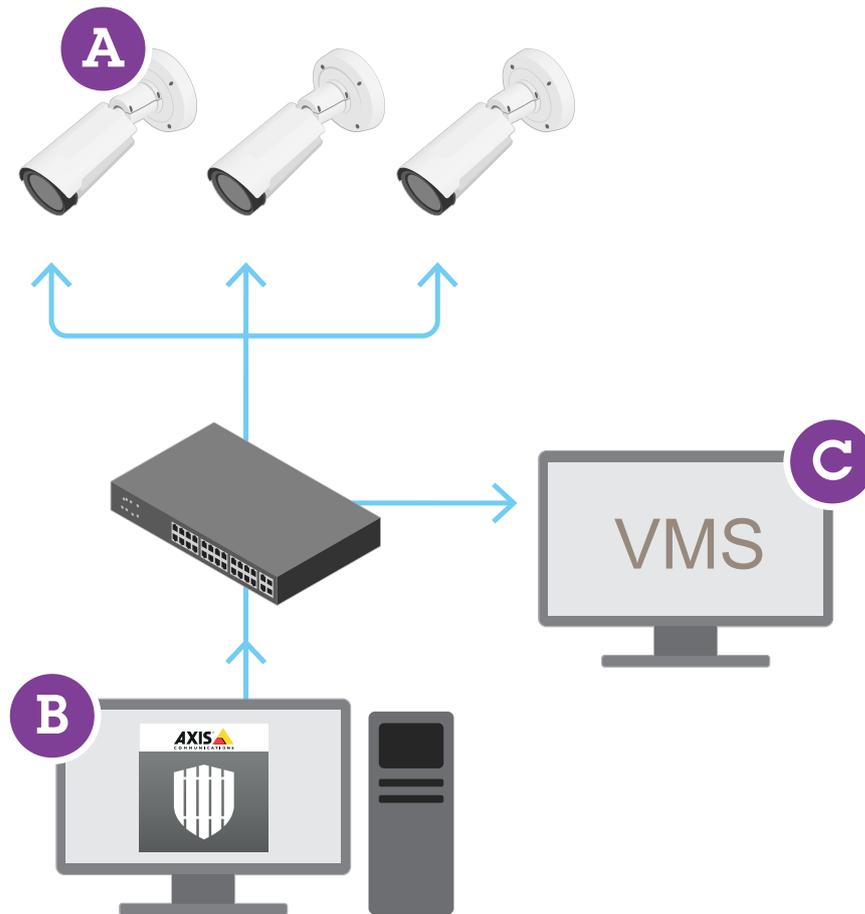
AXIS Perimeter Defender

AXIS Perimeter Defender is an application for perimeter surveillance and protection. It is ideal for high-security perimeter protection where there is a need to strengthen the physical access control system with reliable intrusion detection.

AXIS Perimeter Defender is primarily designed for so-called sterile zone protection, for example along a fence marking a boundary. The term sterile zone refers to an area where people are not supposed to be.

Use AXIS Perimeter Defender in an outdoor environment to:

- Detect moving persons.
- Detect moving vehicles, without discriminating between vehicle types.



This camera can run the application in calibration mode, AI mode, or both modes in combination. If you choose to run it in AI mode only, camera mounting is more flexible and you don't need to calibrate the cameras.

AXIS Perimeter Defender consists of a desktop interface (B), from where you install and set up the application on the cameras (A). You can then configure the system to send alarms to the Video Management Software (C).

AXIS Perimeter Defender PTZ Autotracking is a plugin to the AXIS Perimeter Defender application, using the same desktop interface. With the plugin, you pair a fixed visual or thermal camera with an Axis Q-line PTZ camera. You can then maintain continuous detection coverage of a scene with the fixed camera while the PTZ camera automatically tracks and gives you closer views of detected objects.

Important

AXIS Perimeter Defender PTZ Autotracking requires calibration of both fixed and PTZ cameras.

AXIS Perimeter Defender offers the following types of detection scenarios:

- **Intrusion:** triggers an alarm when a person or a vehicle enters a zone defined on the ground (from any direction and with any trajectory).
- **Loitering:** triggers an alarm when a person or a vehicle remains in a zone defined on the ground for more than a predefined number of seconds.
- **Zone-crossing:** triggers an alarm when a person or a vehicle passes through two or more zones defined on the ground in a given sequence.
- **Conditional:** triggers an alarm when a person or a vehicle enters a zone defined on the ground without first passing through another zone or zones defined on the ground.

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 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.

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.

Secure keystore

A tamper-protected environment for the protection of private keys and secure execution of cryptographic operations. It prevents unauthorized access and malicious extraction in the event of a security breach. Depending on security requirements, an Axis device can have either one or multiple hardware-based cryptographic computing modules, which provide a hardware-protected secure keystore. Depending on security requirements, an Axis device can have either one or multiple hardware-based cryptographic computing modules, like a TPM 2.0 (Trusted Platform Module) or a secure element, and/or a TEE (Trusted Execution Environment), which provide a hardware-protected secure keystore. Furthermore, selected Axis products feature a FIPS 140-2 Level 2-certified secure keystore.

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

Signed video

Signed video ensures that video evidence can be verified as untampered without proving the chain of custody of the video file. Each camera uses its unique video signing key, which is securely stored in the secure keystore, to add a signature into the video stream. When the video is played, the file player shows whether the video is intact. Signed video makes it possible to trace the video back to the camera origin and verifies that the video has not been tampered with after it left the camera.

Encrypted file system

The secure keystore prevents the malicious exfiltration of information and prevents configuration tampering by enforcing strong encryption upon the file system. This ensures no data stored in the file system can be extracted or tampered with when the device is not in use, unauthenticated access to the device is achieved and/or the

Axis device is stolen. During the secure boot process, the read-write filesystem is decrypted and can be mounted and used by the Axis device.

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

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

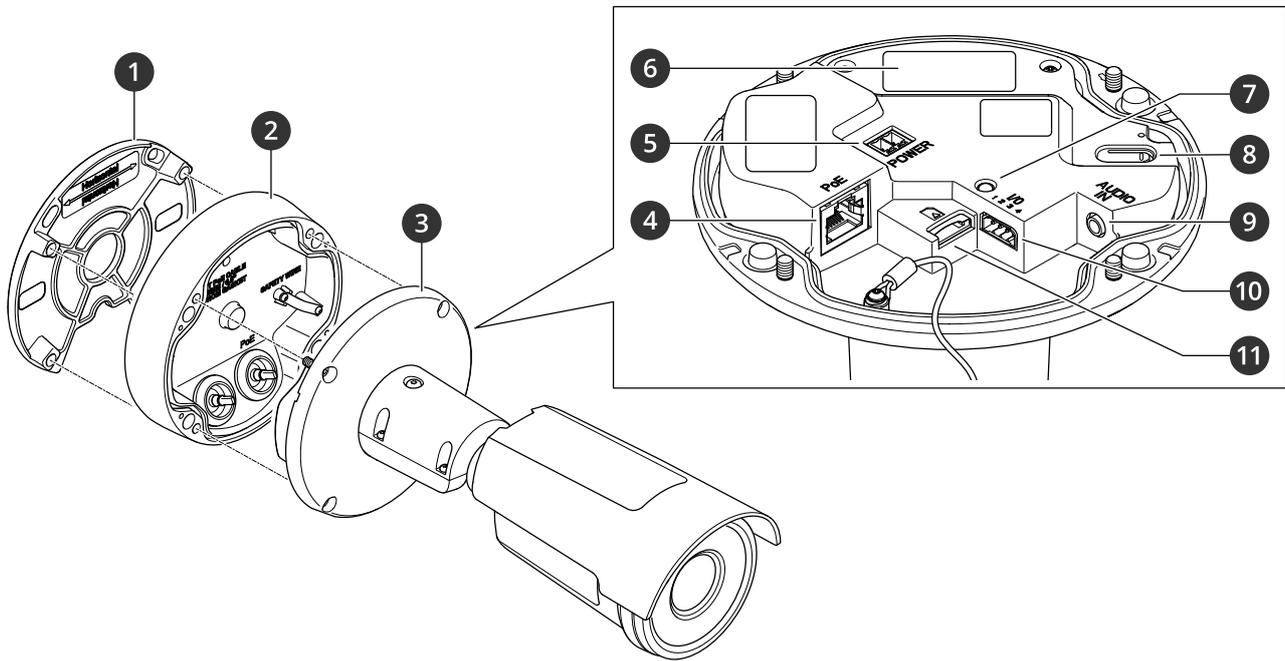
To minimize customers' risk of exposure, Axis, as a **Common Vulnerability and Exposures (CVE) numbering authority (CNA)**, follows industry standards to manage and respond to discovered vulnerabilities in our devices, software, and services. For more information about Axis vulnerability management policy, 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 Mounting bracket
- 2 Connection lid
- 3 Camera unit
- 4 Network connector (PoE)
- 5 Power connector
- 6 Part number (P/N) & serial number (S/N)
- 7 Status LED indicator
- 8 Control button
- 9 Audio connector
- 10 I/O connector
- 11 SD memory card slot

LED indicators

Status LED	Indication
Unlit	Connection and normal operation.
Green	Connection and normal operation.
Amber	Steady during startup. Flashes during device software upgrade or reset to factory default.
Amber/Red	Flashes amber/red if network connection is unavailable or lost.
Red	Device software upgrade failure.

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.



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 30*.
- 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 with Power over Ethernet (PoE).

Audio connector

- **Audio in** – 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 input

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

The external microphone is used when connected.

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.

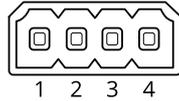
Supervised input – Enables possibility to detect tampering on a digital input.

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.

Note

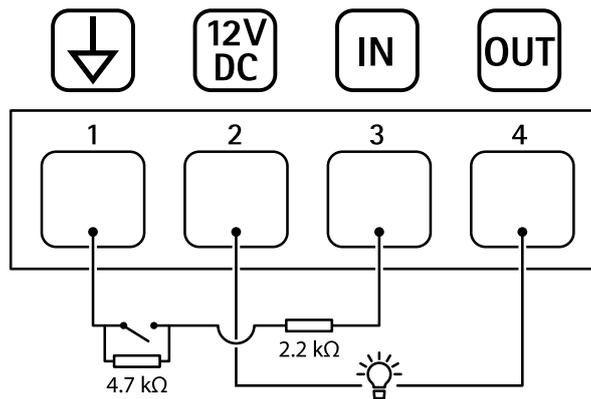
The I/O connector is connected to the housing (fan/heater) on delivery. In case of a fan or heater error, an input signal will be triggered in the camera. Set up an action rule in the camera to configure which action the signal shall trigger.

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 or Supervised Input	3	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	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

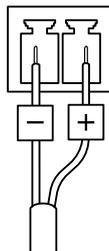
Example:



- 1 DC ground
- 2 DC output 12 V, max 25 mA
- 3 Supervised input
- 4 Digital output

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.



Clean your device

You can clean your device with lukewarm water and mild, nonabrasive soap.

NOTICE

- Harsh chemicals can damage the device. Don't use chemicals such as window cleaner or acetone to clean your device.
 - Don't spray detergent directly on the device. Instead, spray detergent on a nonabrasive cloth and use that to clean the 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 and mild, nonabrasive soap.
 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 26*.
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.

You can use AXIS Device Manager to upgrade multiple devices at the same time. Find out more at 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 30*.

The IP address has been changed by DHCP

IP addresses obtained from a DHCP server are dynamic and could change. If the IP address has been changed, use AXIS IP Utility or AXIS Device Manager to locate the device on the network. Identify the device using its model or serial number, or by the DNS name (if the name has been configured).

If required, you can assign a static IP address manually. For instructions, go to axis.com/support.

Certificate error when using IEEE 802.1X

For authentication to work properly, the date and time settings in the Axis device must be synchronized with an NTP server. Go to **System > Date and time**.

The browser isn't supported

For a list of recommended browsers, see *Browser support, on page 6*.

Can't access the device externally

To access the device externally, we recommend you to use one of the following applications for Windows®:

- AXIS Camera Station Edge: free of charge, ideal for small systems with basic surveillance needs.
- AXIS Camera Station Pro: 90-day trial version free of charge, ideal for small to mid-size systems.

For instructions and download, go to axis.com/vms.

Problems with 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.

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

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.
- Using palettes affects the product's CPU load which in turn affects the frame rate.

Contact support

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

T10209446

2026-02 (M8.2)

© 2024 – 2026 Axis Communications AB