

# AXIS Q1715 Block Camera

Table of Contents

Installation ..... 4  
 Preview mode ..... 4  
 Get started..... 5  
 Find the device on the network..... 5  
     Browser support ..... 5  
 Open the device's web interface..... 5  
 Create an administrator account..... 5  
 Secure passwords..... 6  
 Make sure that no one has tampered with the device software ..... 6  
 Web interface overview ..... 6  
 Configure your device..... 7  
 Basic settings ..... 7  
 Adjust the image..... 7  
     Level the camera ..... 7  
     Adjust the focus ..... 7  
     Select scene profile..... 8  
     Reduce image processing time with low latency mode..... 8  
     Select exposure mode ..... 9  
     Reduce noise in low-light conditions ..... 9  
     Handle scenes with strong backlight..... 9  
     Stabilize a shaky image with image stabilization..... 10  
     Monitor long and narrow areas ..... 10  
     Verify the pixel resolution..... 10  
     Hide parts of the image with privacy masks..... 11  
     Show an image overlay ..... 11  
 Adjust the camera view (PTZ)..... 11  
     Limit the zoom movements..... 12  
     Create a guard tour with preset positions..... 12  
 View and record video ..... 12  
     Reduce bandwidth and storage ..... 12  
     Set up network storage ..... 13  
     Record and watch video ..... 13  
 Set up rules for events ..... 13  
     Record video when the camera detects an object..... 13  
     Show a text overlay in the video stream when the device detects an object ..... 14  
     Record video when the camera detects loud noises ..... 14  
     Zoom in on a specific area automatically with gatekeeper ..... 15  
     Record video when the camera detects impact ..... 15  
     Set up the intrusion alarm ..... 16  
     Detect tampering with input signal ..... 16  
     Trigger a notification when the camera lens is tampered ..... 17  
 Audio..... 18  
     Add audio to your recording ..... 18  
     Connect to a network speaker..... 18  
     Add audio capability to your product using portcast..... 18  
 Connect to a strobe siren ..... 19  
 The web interface ..... 20  
 Learn more..... 21  
     Capture modes..... 21  
     Privacy masks ..... 21  
     Overlays ..... 21  
     Pan, tilt, and zoom (PTZ) ..... 21  
         Preset positions..... 21

Guard tours.....	21
Streaming and storage.....	22
Video compression formats.....	22
How do Image, Stream, and Stream profile settings relate to each other?.....	22
Bitrate control.....	22
Analytics and apps .....	24
AXIS Object Analytics.....	24
Metadata visualization.....	24
Edge-to-edge technology.....	24
Network pairing .....	24
Clean your device.....	25
Specifications.....	26
Product overview .....	26
.....	26
LED indicators.....	26
SD card slot.....	26
Buttons.....	27
Control button .....	27
PoE class switch .....	27
Connectors.....	27
BNC connector.....	27
HDMI connector.....	27
Network connector.....	27
Audio connector.....	27
I/O connector.....	27
Power connector .....	28
RS485/RS422 connector.....	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.....	34
PTZ drivers .....	35
AFTP.....	35
Pelco .....	35
Visca.....	37
Cybersecurity .....	39
Vulnerability management .....	39
Security notifications.....	39
Secure product lifecycle.....	39

## Installation



*Installation video for the product.*

## 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.



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

For more information about how to find and assign IP addresses, go to *How to assign an IP address and access your device*.

### Browser support

You can use the device with the following browsers:

	Chrome™	Edge™	Firefox®	Safari®
Windows®	✓	✓	*	*
macOS®	✓	✓	*	*
Linux®	✓	✓	*	*
Other operating systems	*	*	*	*

✓: Recommended

\*: Supported with limitations

### Open the device's web interface

1. Open a browser and type the IP address or host name of the Axis device. If you don't know the IP address, use AXIS IP Utility or AXIS Device Manager to find the device on the network.
2. Type the username and password. If you access the device for the first time, you must create an administrator account. See *Create an administrator account, on page 5*.

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

### Create an administrator account

The first time you log in to your device, you must create an administrator account.

1. Enter a username.
2. Enter a password. See *Secure passwords, on page 6*.
3. Re-enter the password.
4. Accept the license agreement.
5. Click **Add account**.

#### Important

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

### Basic settings

#### Set the capture mode

1. Go to **Video > Installation > Capture mode**.
2. Click **Change**.
3. Select a capture mode and click **Save and restart**.  
See also *Capture modes, on page 21*.

#### 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 10*.

### 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 21*.

#### 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.

#### Adjust the focus

This product can have four focus modes:


- **Auto:** The camera automatically adjusts focus based on the entire image.
- **Area:** The camera automatically adjusts focus based on a selected area of the image.
- **Manual:** The focus is set manually at a fixed distance.
- **Spot:** The focus is set to a fixed area in the center of the image.



Spot focus

To turn off autofocus and adjust the focus manually:

1. In the live view window, if the **Zoom** slider is visible, click **Zoom** and select **Focus**.

2. Click  and use the slider to set the focus.

### Select scene profile

A scene profile is a set of predefined image appearance settings including color level, brightness, sharpness, contrast and local contrast. Scene profiles are preconfigured in the product for quick setup to a specific scenario, for example **Forensic** which is optimized for surveillance conditions. For a description of each available setting, see *The web interface, on page 20*.

You can select a scene profile during the initial setup of the camera. You can also select or change scene profile later.

1. Go to **Video > Image > Appearance**.
2. Go to **Scene profile** and select a profile.

### Reduce image processing time with low latency mode

You can optimize the image processing time of your live stream by turning on low latency mode. The latency in your live stream is reduced to a minimum. When you use low latency mode, the image quality is lower than usual.

1. Go to **System > Plain config**.
2. Select **ImageSource** from the drop-down list.
3. Go to **ImageSource/I0/Sensor > Low latency mode** and select **On**.
4. Click **Save**.

## 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.
- For environments with certain artificial lighting, for example fluorescent lighting, select **Flicker-free**. Select the same frequency as the power line frequency.
- For environments with certain artificial light and bright light, for example outdoors with fluorescent lighting at night and sun during daytime, select **Flicker-reduced**. Select the same frequency as the power line frequency.
- To lock the current exposure settings, select **Hold current**.

## Reduce noise in low-light conditions

To reduce noise in low-light conditions, you can adjust one or more of the following settings:

- Adjust the trade-off between noise and motion blur. Go to **Video > Image > Exposure** and move the **Blur-noise trade-off** slider toward **Low noise**.
- Set the exposure mode to automatic.

### Note

A high max shutter value can result in motion blur.

- To slow down the shutter speed, set max shutter to the highest possible value.

### Note

When you reduce the max gain, the image can become darker.

- Set the max gain to a lower value.
- If there is an **Aperture** slider, move it towards **Open**.

## 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.



*Image without WDR.*



*Image with WDR.*

### Note

- WDR can cause artifacts in the image.
  - WDR may not be available for all capture modes.
1. Go to **Video > Image > Wide dynamic range**.
  2. Turn on WDR.
  3. Use the **Local contrast** slider to adjust the amount of WDR.
  4. Use the **Tone mapping** slider to adjust the amount of WDR.
  5. 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](https://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.

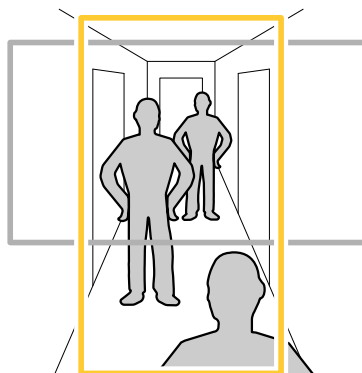
### Note

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

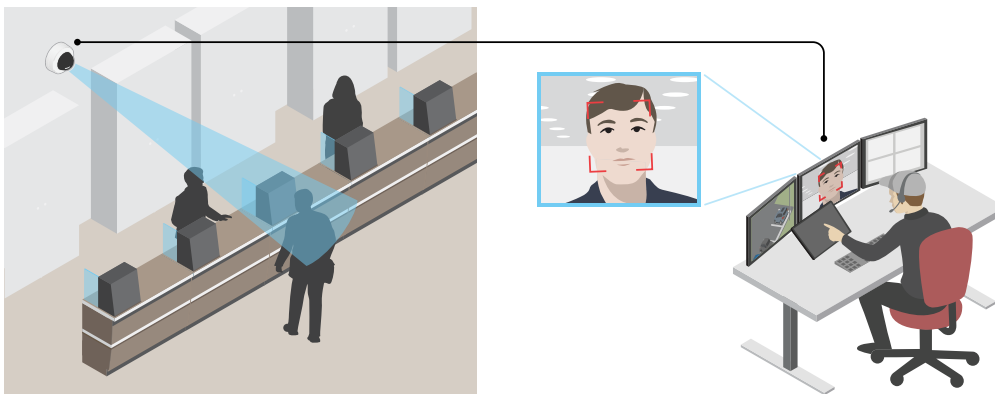
Use corridor format to better utilize the full field of view in a long and narrow area, for example a staircase, hallway, road, or tunnel.





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 the face of a person, you can use the pixel counter.



1. Go to **Video > Image** and click .
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 21*

### 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.

### Adjust the camera view (PTZ)

To learn more about different pan, tilt, and zoom settings, see *Pan, tilt, and zoom (PTZ), on page 21*.

## Limit the zoom movements


If there are parts of the scene that you don't want the camera to be able to zoom in on, you can limit the maximum zoom level. For example, you want to protect the privacy of residents in an apartment building, which is located close to a parking lot that you intend to monitor.

To limit the maximum zoom level:

1. Go to **PTZ > Limits**.
2. Set the limits as needed.

## Create a guard tour with preset positions

A guard tour displays the video stream from different preset positions either in a predetermined or random order, and for configurable periods of time.

1. Go to **PTZ > Guard tours**.
2. Click  **Guard tour**.
3. Select **Preset position** and click **Create**.
4. Under **General settings**:
  - Enter a name for the guard tour and specify the pause length between each tour.
  - If you want the guard tour to go to the preset positions in a random order, turn on **Play guard tour in random order**.
5. Under **Step settings**:
  - Set the duration for the preset.
  - Set the move speed, which controls how fast to move to the next preset.
6. Go to **Preset positions**.
  - 6.1. Select the preset positions that you want in your guard tour.
  - 6.2. Drag them to the **View order** area, and click **Done**.
7. To schedule the guard tour, go to **System > Events**.


## 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 22.

## Reduce bandwidth and storage

### Important

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

1. Go to **Video > Stream**.
2. Click  **A** 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 13*

3. To stop recording, click  again.

### Watch video

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

## 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*.

## 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.

1. Start the application if it is not already running.
2. 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 actions, under **Recordings**, select **Record video while the rule is active**.
4. In the list of storage options, select **SD\_DISK**.
5. Select a camera and a stream profile.
6. Set the prebuffer time to 5 seconds.
7. Set the postbuffer time to 1 minute.
8. 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.

1. Start the application if it is not already running.
2. 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 actions, under **Overlay text**, select **Use overlay text**.
4. Select a video channel.
5. In **Text**, type "Motion detected".
6. Set the duration.
7. Click **Save**.

### 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.

#### Note

The following instructions require that a microphone is connected to audio-in.

Turn on audio:

1. Set up the stream profile to include audio, see *Add audio to your recording, on page 18*.

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**.

### Zoom in on a specific area automatically with gatekeeper

This example explains how to use the gatekeeper functionality to make the camera zoom in automatically on the license plate of a car that passes through a gate. When the car has passed, the camera zooms out to the home position.

Create the preset positions:

1. Go to **PTZ > Preset positions**.
2. Create the home position that includes the entrance of the gate.
3. Create the zoomed-in preset position so that it covers the area in the image where you assume that the license plate will appear.

Create a rule:

1. Go to **System > Events** and add a rule.
2. Name the rule "Gatekeeper".
3. In the list of actions, under **Preset positions**, select **Go to preset position**.
4. Select a **Video channel**.
5. Select the **Preset position**.
6. To make the camera wait a while before it returns to the home position, set a time for **Home timeout**.
7. 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**.

## Set up the intrusion alarm

### Before you start

- Connect the intrusion alarm switch to pin 1 (ground) and pin 3 (digital I/O) 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 **Input**.
  - 2.2. 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**.

## 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** for the relevant port.

### Add an email recipient:

1. Go to **System > Events > Recipients** and add a recipient.

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

### Create a rule:

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

### Trigger a notification when the camera lens is tampered

This example explains how to set up an email notification when the camera lens gets either spray painted, covered, or blurred.

### 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.
3. Turn on **Trigger on dark images** to detect if the lens is sprayed, covered, or rendered severely out of focus.

### Add an email recipient:

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

### Create a rule:

12. Go to **System > Events > Rules** and add a rule.
13. Type a name for the rule.
14. In the list of conditions, under **Video**, select **Tampering**.
15. In the list of actions, under **Notifications**, select **Send notification to email** and then select the recipient from the list.
16. Type a subject line and message for the email.
17. 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.

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**.


### 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

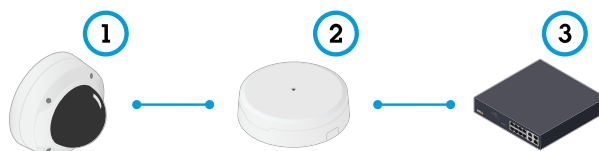
1. Go to **System > Edge-to-edge > Pairing**.
2. Click  **Add** and select the pairing type **Audio** from the drop-down list.
3. Select **Speaker pairing**.
4. Type the network speaker's IP address, username and password.
5. Click **Connect**. A confirmation message appears.

### Add audio capability to your product using portcast

With portcast technology, you can add audio capability to your product. It allows audio and I/O communication digitally over the network cable between the camera and the interface.

To add audio capability to your Axis network video device, connect the portcast compatible Axis audio device and I/O Interface between your device and the PoE switch which provides power.

1. Connect the Axis network video device (1) and the Axis portcast device (2) with a PoE cable.
2. Connect the Axis portcast device (2) and the PoE switch (3) with a PoE cable.



- 1 Axis network video device
- 2 Axis portcast device
- 3 Switch


Once the devices are connected, an audio tab becomes visible in the settings for your Axis network video device. Go to the audio tab and turn on **Allow audio**.

See your Axis portcast device's user manual for more information.

## Connect to a strobe siren

Network pairing allows you to pair a camera with a compatible Axis device with light and siren functionality. Once paired, the camera can configure and maintain both devices.

Pair the camera with a strobe siren:

1. Go to **System > Edge-to-edge > Pairing**.
2. Click  **Add** and select the pairing type **Network pairing** from the drop-down list.
3. Type the IP address, username and password of the strobe siren.
4. Click **Connect**. A confirmation message appears.

To find devices directly on the network, click **Discover devices**.

### Note

- The list shows all Axis devices that are found, not only devices that can be paired.
- An info icon is shown for devices that have already been paired. Hover over the icon to get information about pairings that are already active.
- Make sure the paired devices run the same AXIS OS version.

### Important

- It's only possible to discover devices where Bonjour is enabled. To enable Bonjour for a device, open its web interface and go to **System > Network > Network discovery protocols**.

## 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

### Capture modes

What capture mode to choose depends on the requirements for the frame rate and resolution of the specific surveillance setup. For specifications about available capture modes, see the product's datasheet at [axis.com](http://axis.com).

### 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

#### Note

Image and text overlay will not be displayed on video stream over HDMI .

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.

### Pan, tilt, and zoom (PTZ)

#### Preset positions

A preset position is a saved view that can be used to quickly move the camera view to a specific position.

A preset position can consist of the following values:

- Zoom position
- Focus position (manual or automatic)
- Iris position (manual or automatic)

The preset positions can be reached at any time:

- from the drop-down list in the live view window
- as actions in the event system
- as triggers in the event system
- when setting up a guard tour

#### Guard tours

A guard tour displays the video stream from different preset positions either in a predetermined or random order, and for configurable periods of time. Once started, a guard tour continues to run until stopped, even when there are no clients (web browsers) viewing the images.

## 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.

### 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.

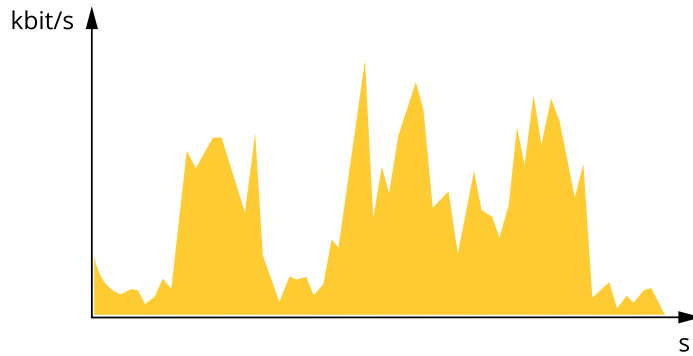
The **Stream profiles** settings override the settings from the **Stream** tab. If you request a stream with a specific stream profile, the stream contains the settings of that profile. If you request a stream without specifying a stream profile, or request a stream profile that doesn't exist in the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

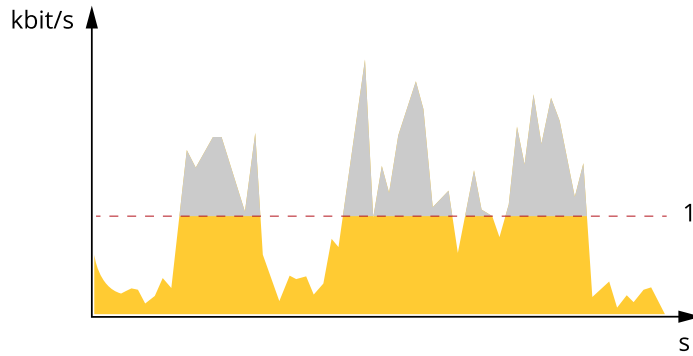
#### Variable bitrate (VBR)

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.

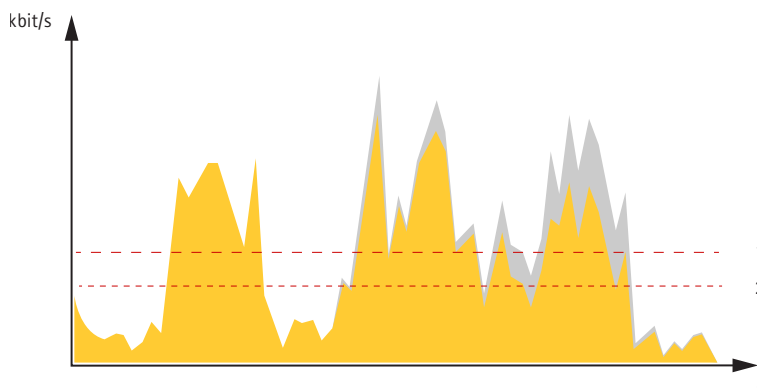


1 Target bitrate

**Average bitrate (ABR)**

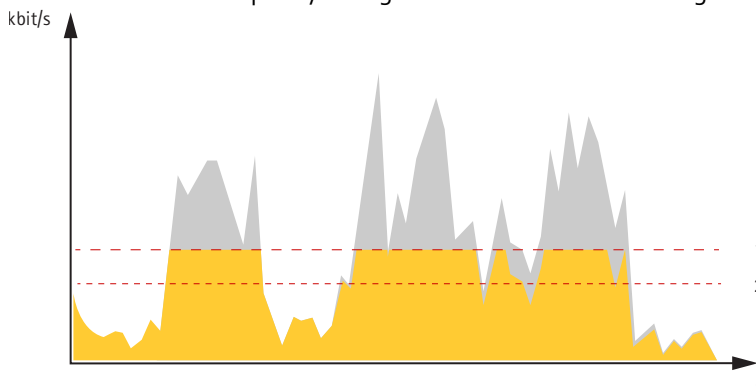
With average bitrate, the bitrate is automatically adjusted over a longer period of time. This is so you can meet the specified target and provide the best video quality based on your available storage. Bitrate is higher in scenes with a lot of activity, compared to static scenes. You are more likely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

## 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*.

## 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*.

## 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](http://whitepapers.axis.com/edge-to-edge-technology).

## Network pairing

With edge-to-edge network pairing, you can connect your camera to a compatible Axis device with light and siren or illuminator light functionality and benefit from its integrated features.

## Clean your device

You can clean your device with lukewarm water.

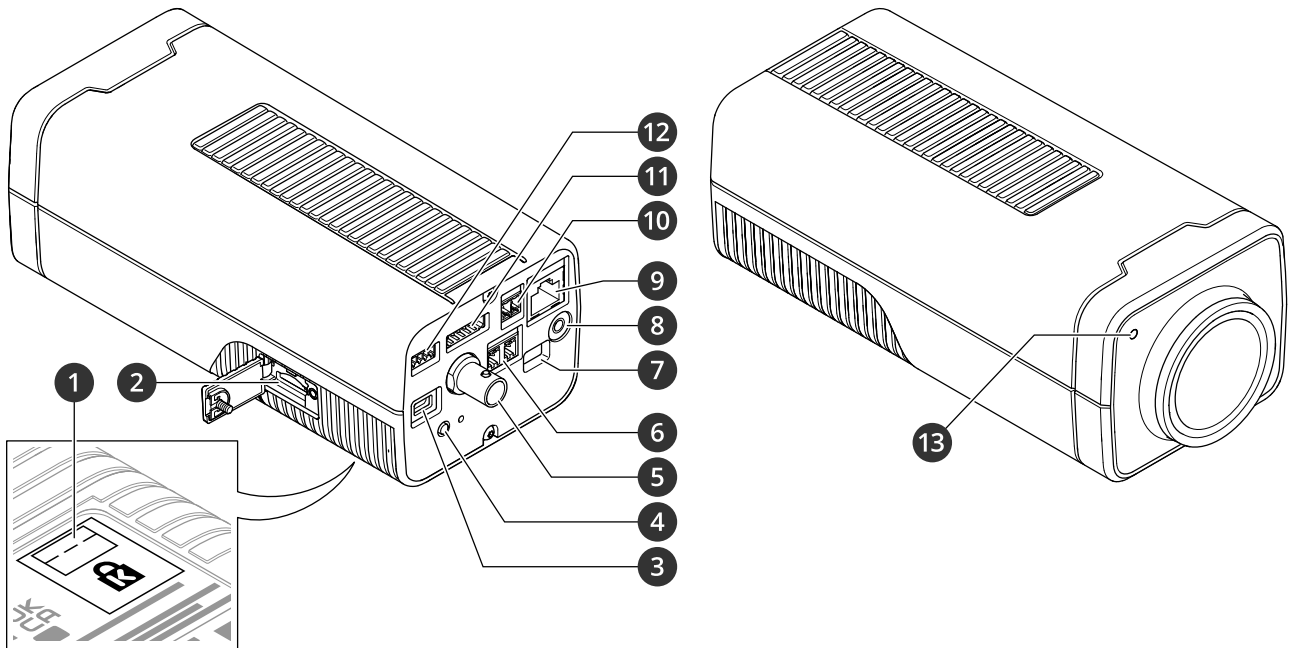
### **NOTICE**

- 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*.

## Specifications

### Product overview



- 1 Security lock slot
- 2 microSD card slot
- 3 HDMI connector
- 4 Control button
- 5 SDI connector
- 6 RS-485/422 connector
- 7 PoE class switch
- 8 Audio in (analogue/digital)
- 9 Network connector (PoE)
- 10 Power connector (DC)
- 11 I/O connector
- 12 I2C connector (camera housing communication connector)
- 13 Status LED

### 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 device software upgrade or reset to factory default.
Amber/Red	Flashes amber/red if network connection is unavailable or lost.


### 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 30*.

### PoE class switch

Use the switch to select the PoE class you want the device to use. Select PoE class 3 if you're mounting the camera in an outdoor housing that supports it.

#### Important

When using PoE class 3, HDMI and SDI are turned off.

## Connectors

### BNC connector

The BNC connector is used for connecting broadcast equipment using SDI. Connect a 75 Ohm coaxial SDI cable.

#### CAUTION

The connector may be hot during normal operation in elevated ambient temperatures.

### HDMI connector

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

#### Note

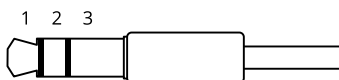
Make sure that the camera is set to PoE class 4 for the HDMI™ to function properly.

### Network connector

RJ45 Ethernet connector with Power over Ethernet (PoE).

### Audio connector

- Audio in – 3.5 mm input for a mono microphone, or a line-in mono signal (left channel is used from a stereo signal).



Audio input

1 Tip	2 Ring	3 Sleeve
-------	--------	----------

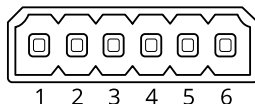
### I/O connector


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.

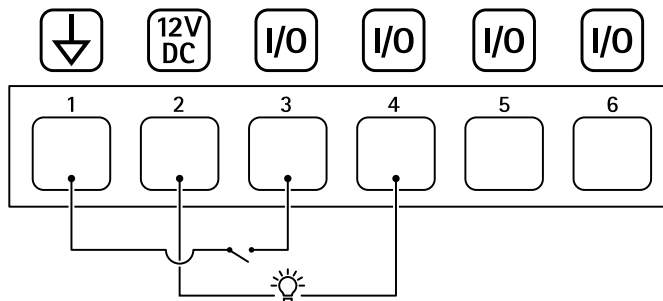
**Digital output** – For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface, through an event or from the device's web interface.

6-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 = 50 mA
Configurable (Input or Output)	3-6	Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 VDC
		Digital output – Internally connected to pin 1 (DC ground) when active, and floating (unconnected) when inactive. If used with an inductive load, e.g., a relay, connect a diode in parallel with the load, to protect against voltage transients.	0 to max 30 VDC, open drain, 100 mA

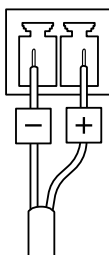
Example:



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

**Power connector**

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

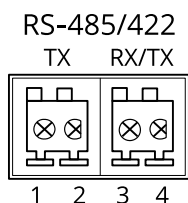


**RS485/RS422 connector**

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

The serial port can be configured to support:

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



Function	Pin	Notes
RS485/RS422 TX(B)	1	TX pair for RS422 and 4-wire RS485
RS485/RS422 TX(A)	2	
RS485B alt RS485/422 RX(B)	3	RX pair for all modes (combined RX/TX for 2-wire RS485)
RS485A alt RS485/422 RX(A)	4	

**Important**

The maximum cable length is 30 m (98 ft).

## 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](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](https://axis.com/support/device-software).
1. Download the AXIS OS file to your computer, available free of charge at [axis.com/support/device-software](https://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](https://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](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 5*.

**Can't access the device externally**

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

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

For instructions and download, go to [axis.com/vms](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 33.
- 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.

## Problems with operating the device

### Front heater and wiper aren't working

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

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

## 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).

## PTZ drivers

### APTP

This is a list of models supported by this driver. The physical installation depends on your Axis product and the PTZ unit.

#### Important

Check what serial communication your Axis product and the PTZ unit will support.

Supported models with RS485 2-wire interface:

- AXIS T99A Positioning Unit Series.  
For information about compatible Axis products, see *axis.com*.

Other models may be supported but this has not been verified by Axis.

### Technical information

DEFAULT capabilities for PTZ driver:

Driver	APTP
Version	1.1.0

DEFAULT serial configuration:

PortMode	RS485
BaudRate	115,200
DataBits	8
StopBits	1
Parity	None

DEFAULT supported capabilities in this PTZ driver:

#### Note

Different PTZ units may have other capabilities (both less and more).

Movement	Absolute	Relative	Continuous
Pan	yes	yes	yes
Tilt	yes	yes	yes

### Connection

For the RS485/RS422 pin assignment on your device, see *RS485/RS422 connector, on page 29*.

To change serial port settings, go to **System > Plain config > Serial** in the device's web interface.

### Pelco

This is a list of models supported by this driver. The physical installation depends on your Axis product and the PTZ unit.

#### Important

Check what serial communication your Axis product and the PTZ unit will support.

Supported models:

- Pelco DD5-C
- Pelco Esprit ES30C/ES31C
- Pelco LRD41C21
- Pelco LRD41C22
- Pelco Spectra III
- Pelco Spectra IV
- Pelco Spectra Mini
- Videotec DTRX3/PTH310P
- Videotec ULISSE
- PTK AMB
- YP3040

Other models may be supported but this has not been verified by Axis.

**Technical information**

DEFAULT capabilities for PTZ driver:

Driver	Pelco
Version	4.17

DEFAULT serial configuration:

PortMode	RS485
BaudRate	2,400
DataBits	8
StopBits	1
Parity	None

DEFAULT supported capabilities in this PTZ driver:

**Note**

Different PTZ units may have other capabilities (both less and more).

Movement	Absolute	Relative	Continuous
Pan	no	yes	yes
Tilt	no	yes	yes
Zoom	no	yes	yes
Focus	no	yes	yes
Iris	no	yes	yes

AutoIris	yes
AutoFocus	yes
IrCutFilter	no

BackLight	yes
OSDMenu	yes

**Connection**

For the RS485/RS422 pin assignment on your device, see *RS485/RS422 connector, on page 29*.

To change serial port settings, go to **System > Plain config > Serial** in the device's web interface.

**Visca**

This is a list of models supported by this driver. The physical installation depends on your Axis product and the PTZ unit.

**Important**

Check what serial communication your Axis product and the PTZ unit will support.

Supported models with RS422 4-wire interface:

- Sony EVI-D70/D70P
- WISKA DCP-27 (PT-head)

Supported models with RS232 interface (may require external RS422-4-wire/RS232 converter):

- Axis EVI-D30/D31
- Sony EVI-G20/G21
- Sony EVI-D30/D31
- Sony EVI-D100/D100P
- Sony EVI-D70/D70P

Other models may be supported but this has not been verified by Axis.

**Technical information**

DEFAULT capabilities for PTZ driver:

Driver	Visca/EVI
Version	4.11

DEFAULT serial configuration:

PortMode	RS422
BaudRate	9,600
DataBits	8
StopBits	1
Parity	None

DEFAULT supported capabilities in this PTZ driver:

**Note**

Different PTZ units may have other capabilities (both less and more).

Movement	Absolute	Relative	Continuous
Pan	yes	yes	yes
Tilt	yes	yes	yes
Zoom	yes	yes	yes
Focus	yes	yes	yes
Iris	yes	yes	no

AutoIris	yes
AutoFocus	yes
IrCutFilter	yes
BackLight	yes
OSDMenu	no

### Connection

For the RS485/RS422 pin assignment on your device, see *RS485/RS422 connector, on page 29*.

To change serial port settings, go to **System > Plain config > Serial** in the device's web interface.

## 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.

T10168073

2026-07 (M21.2)

© 2021 – 2026 Axis Communications AB