AXIS M32 Dome Camera Series

AXIS M3215-LVE Dome Camera
AXIS M3216-LVE Dome Camera

User manual

Table of Contents

Installation

For instructions on how to install the product, see the installation guide on the product's support page on *axis. com*.

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 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 35*.

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 35*.
   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.

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

Axis device web interface

Configure your device

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 22*.

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.

- For fast moving objects that require a fast or fixed shutter, select **Automatic aperture**.

- To maintain a longer depth of field or focus range, select **Automatic shutter**.

- 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.

- If you need full control of all parameters, select **Manual**. This is mostly useful for scenes with little change in lighting.

- To lock the current exposure settings, select **Hold current**.

Benefit from IR light in low-light conditions by using night mode

Your camera uses visible light to deliver color images during the day. But as the visible light diminishes, color images become less bright and clear. If you switch to night mode when this happens, the camera uses both visible and near-infrared light to deliver bright and detailed black-and-white images instead. You can set the camera to switch to night mode automatically.

1. Go to **Video > Image > Day-night mode**, and make sure that the **IR-cut filter** is set to **Auto**.

2. To set at what light level you want the camera to switch to night mode, move the **Threshold** slider toward **Bright** or **Dark**.

3. To use the built-in IR light when the camera is in night mode, turn on **Allow illumination** and **Synchronize illumination**.

4. If you use an accessory IR illuminator, turn on **Allow illumination** and **Synchronize illumination** to use IR light when the camera is in night mode.

Note

If you set the switch to night mode to occur when it's brighter, the image remains sharper as there is less low-light noise. If you set the switch to occur when it's darker, the image colors are maintained for longer, but there is more image blur due to low-light noise.

Optimize IR illumination

Depending on the installation environment and the conditions around the camera, for example external light sources in the scene, you can sometimes improve the image quality if you manually adjust the intensity of the LEDs. If you have problems with reflections from the LEDs, you can try to reduce the intensity.

1. Go to **Video > Image > Day-night mode**.

2. Turn on **Allow illumination**.

3. Click IR in the live view and select **Manual**.

4. Adjust the intensity.

You can also reduce the reflections by changing the illumination angle.

1. Go to **Video > Image > Day-night mode**.

2. Turn off **Automatic illumination angle**.

3. Adjust the illumination angle slider.

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**.

- Reduce sharpness in the image, under **Video > Image > Appearance**.

If the above settings do not improve the image sufficiently, change to a lens with a lower f-value.

Reduce motion blur in low-light conditions

To reduce motion blur in low-light conditions, adjust one or more of the following settings in **Video > Image > Exposure**:
- Set **Exposure mode** to **Automatic** and turn on **Motion-adaptive exposure**.

Note

When you increase the gain, image noise also increases.

- Set **Max shutter** to a shorter time, and **Max gain** to a higher value.

Note

When you open the aperture, the depth of field gets shallower.

- Move the **Aperture** slider toward **Open**.

If you still have problems with motion blur:
- Increase the light level in the scene.

- Mount the camera so that objects move toward it or away from it rather than sideways.

Note

If you use a lens with a larger aperture, the depth of field gets shallower.

- Change to a lens with a larger aperture.

Maximize the details in an image

Important

If you maximize the details in an image, the bitrate will probably increase and you might get a reduced frame rate.

- Make sure to select the capture mode that has the highest resolution.

- Go to **Video > Stream > General** and set the compression as low as possible.

- Below the live view image, click ⚙ and in **Video format**, select **MJPEG**.

- Go to **Video > Stream > Zipstream** and select **Off**.

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. To set the amount of WDR, select Low, Medium or High from the **WDR level** list.
6. 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*.

Compensate for barrel distortion

Barrel distortion is a phenomenon where straight lines appear increasingly bent closer to the edges of the frame. A wide field of view often creates barrel distortion in an image. Barrel distortion correction compensates for this distortion.

Note

Barrel distortion correction affects the image resolution and field of view.

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

2. Turn on **Barrel distortion correction (BDC)**.

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.
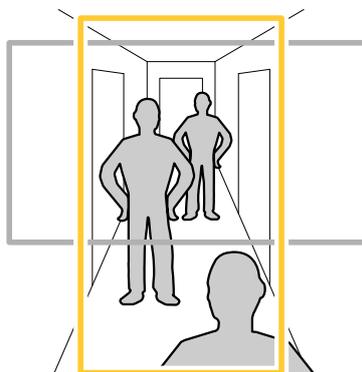
1. Depending on your device, turn the camera or the 3-axis lens in the camera 90° or 270°.

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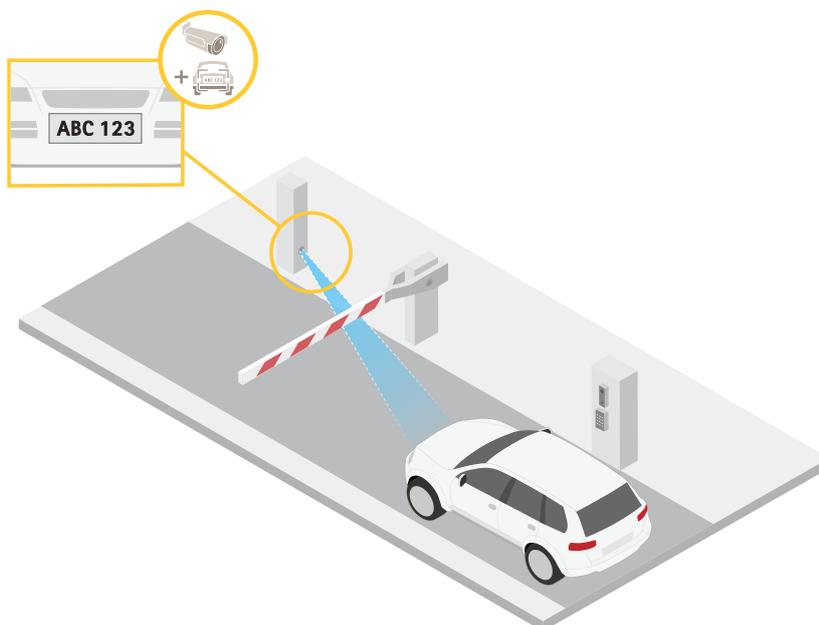
1. Go to **Video > Image**.

2. Click ![icon].

3. Click ![icon] 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 22*

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.

Straighten a skewed image

You can straighten a skewed image by rotating and cropping it digitally. Due to the cropping, a part of the original image is lost. The functionality is useful during installation.
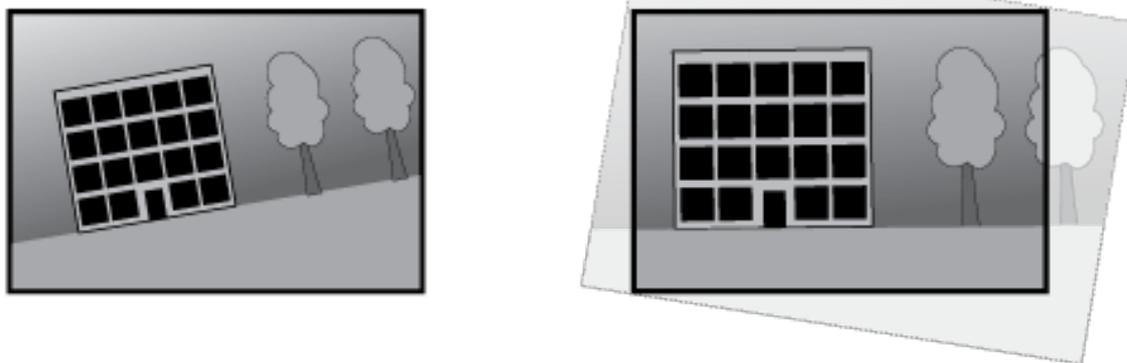
The illustration shows before and after an image has been straightened.

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

2. Turn on **Straighten image**.

3. Use the controls to adjust 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 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 ![icon] in the live view.

3. Select **Video format AV1** if your device supports it. Otherwise select **H.264**.

4. Go to **Video > Stream > General** and increase **Compression**.

5. Go to **Video > Stream > Zipstream** and do one or more of the following:
    Note
    The **Zipstream** settings are used for all video encodings except MJPEG.

    –   Select the Zipstream **Strength** that you want to use.

    –   Turn on **Optimize for storage**. This can only be used if the video management software supports B-frames.

    –   Turn on **Dynamic FPS**.

    –   Turn on **Dynamic GOP** and set a high **Upper limit** GOP length value.

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

View a live video stream on a monitor

Your camera can transmit a live video stream to a monitor even without a network connection. Connect the camera and the monitor using the RCA connectors. Use the monitor for surveillance purposes or for public viewing, for example in a store.

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

1. Connect an external monitor using the HDMI connector.

2. Go to **System > Video out** and turn on **HDMI**.

3. Select a **Source**. Rotate the image if needed.

Important

To view the video stream via the HDMI connector, make sure to select a capture mode that supports HDMI.

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*.

Trigger an action

1. Go to **System > Events** and add a rule. The rule defines when the device will perform certain actions. You can set up rules as scheduled, recurring, or manually triggered.

2. Enter a **Name**.

3. Select the **Condition** that must be met to trigger the action. If you specify more than one condition for the rule, all of the conditions must be met to trigger the action.

4. Select which **Action** to perform when the conditions are met.

Note

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

- If you change the definition of a stream profile that is used in a rule, you need to restart all the rules that use that stream profile.

Record video when the camera detects an object

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

Before you start:

- Make sure you have an SD card installed.

Make sure that AXIS Object Analytics is running:
Make sure that AXIS Video Motion Detection is running:
1. Go to **Apps > AXIS Object Analytics**.

2. Go to **Apps > AXIS Video Motion Detection**.

3. Start the application if it is not already running.

4. Make sure you have set up the application according to your needs.

Create a rule:
1. Go to **System > Events** and add a rule.

2. Type a name for the rule.

3. In the list of conditions, under **Application**, select **Object Analytics**.

4. In the list of conditions, under **Application**, select **VMD4**.

5. In the list of actions, under **Recordings**, select **Record video while the rule is active**.

6. In the list of storage options, select **SD_DISK**.

7. Select a camera and a stream profile.

8. Set the prebuffer time to 5 seconds.

9. Set the postbuffer time to 1 minute.

10. 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 Object Analytics is running:
Make sure that AXIS Video Motion Detection is running:
1. Go to **Apps > AXIS Object Analytics**.

2. Go to **Apps > AXIS Video Motion Detection**.

3. Start the application if it is not already running.

4. 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 **Object Analytics**.

4. In the list of conditions, under **Application**, select **VMD4**.

5. In the list of actions, under **Overlay text**, select **Use overlay text**.

6. Select a video channel.

7. In **Text**, type "Motion detected".

8. Set the duration.

9. Click **Save**.

Note

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

Record video when a PIR detector senses motion

This example explains how to connect a PIR detector (normally closed) to the device, and to start recording video when the detector senses motion.

Required hardware

- 3-wire cable (ground, power, I/O)

- PIR detector, normally closed

NOTICE

Disconnect the device from power before connecting the wires. Reconnect to power after all connections are done.

Connect the wires to the device's I/O connector

Note

For information on the I/O connector, see *Connectors, on page 29.*

1. Connect the ground wire to pin 1 (GND/-).

2. Connect the power wire to pin 2 (12V DC output).

3. Connect the I/O wire to pin 3 (I/O input).

Connect the wires to the PIR detector's I/O connector
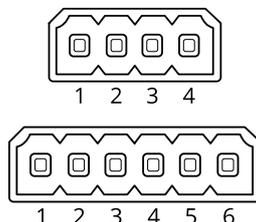
1. Connect the other end of the ground wire to pin 1 (GND/-).

2. Connect the other end of the power wire to pin 2 (DC input/+).

3. Connect the other end of the I/O wire to pin 3 (I/O output).

Configure the I/O port in the device web interface

1. Go to **System > Accessories > I/O ports**.

2. Click to set the direction to input for port 1.

3. Give the input module a descriptive name, for example "PIR detector".

4. If you want to trigger an event whenever the PIR detector senses motion, click to set the normal state to circuit closed.

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, select **PIR detector**.

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**.

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. For the port that you connected the AXIS I/O Indication LED to, click to set the direction to **Output**, and click to set the normal state to **Circuit open**.
   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.

16

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.

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 19*.

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**.

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 32*.

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

2. 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 enclosure is opened

This example explains how to set up an email notification when the housing or casing of the device is opened.

Add an email recipient:
1. Go to **System > Events > Recipients** and click **Add 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:
9. Go to **System > Events > Rules** and click **Add a rule**.

10. Type a name for the rule.

11. In the list of conditions, select **Casing open**.

12. In the list of actions, select **Send notification to email**.

13. Select a recipient from the list.

14. Type a subject line and message for the email.

15. 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

Note

To connect the audio device, this product requires a multicable.

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**.

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 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

Privacy masks

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

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

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.

A privacy mask is a user-defined area that covers part of the monitored area. In the video stream, privacy masks can appear as blocks of solid color, mosaic patterns, or in chameleon mode, which dynamically adapts to the scene to enhance privacy protection.

The privacy mask is relative to the pan, tilt, and zoom coordinates, so regardless of where you point the camera, the privacy mask covers the same place or object.

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.

> **Important**
>
> Set the zoom and focus before you create a privacy mask.

> **Note**
>
> You can't add privacy masks to the quad stream, but it will show all privacy masks configured on the individual channels.

> **Note**
>
> Privacy masks may appear warped in some view modes.

Overlays

> **Note**
>
> Overlays are not included in the video stream when using SIP calls.

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

> **Note**
>
> Image and text overlay will not be displayed on video stream over SDI.

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.

AV1

AV1 (AOMedia Video 1) is a license -free video coding format optimized for streaming media. AV1 enables high-quality video streaming even in bandwidth-constrained environments. By reducing a video's bitrate, AV1 preserves video quality while minimizing data usage.

AV1 supports all major browsers, computer operating systems and mobile platforms.

Note

AV1 requires more processing power for encoding and decoding compared to some other codecs.

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.
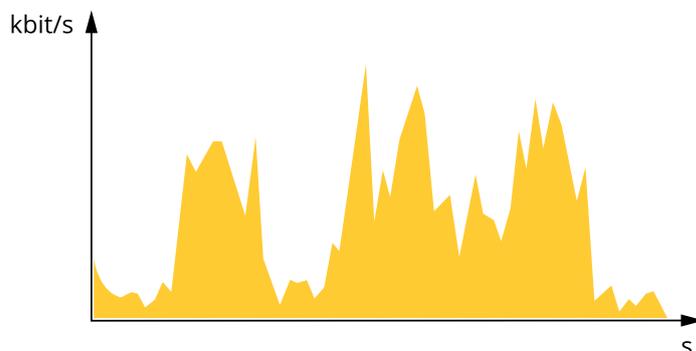
Maximum bitrate (MBR)

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.
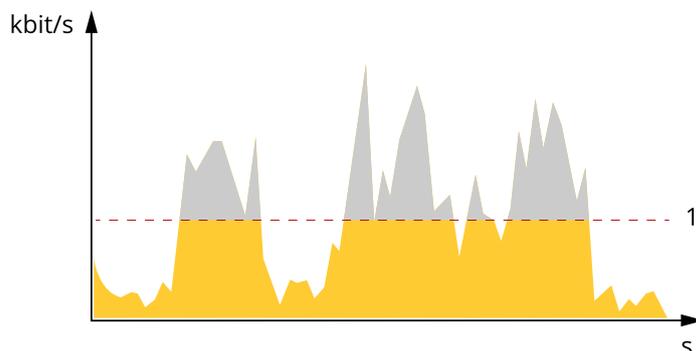
1   Target bitrate

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.
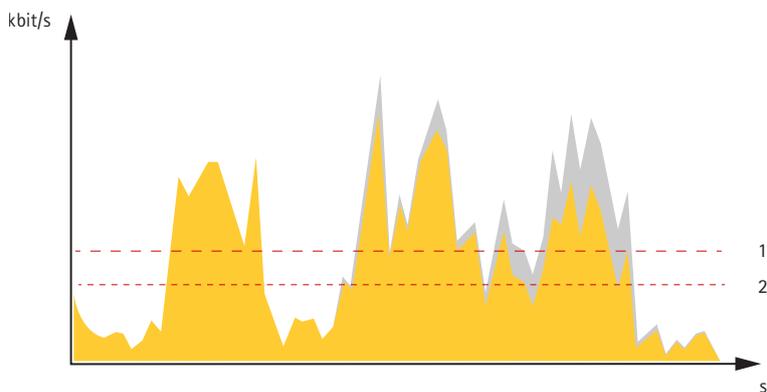
1   Target bitrate
2   Actual average bitrate

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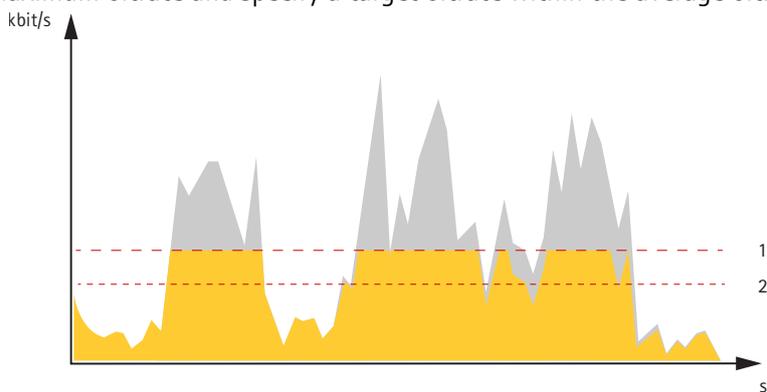
1   Target bitrate
2   Actual average bitrate

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*.

Note

* We recommended running one app at a time.

* 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.

* Avoid running apps when the built-in motion detection is active.

* Apps are supported on channel 1.

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*.

AXIS Image Health Analytics

AXIS Image Health Analytics is an AI-based application that can be used to detect image degradations or tampering attempts. The application analyzes and learns the behavior of the scene to detect blurriness or underexposure in the image, or to detect an obstructed or redirected view. You can set up the application to send events for any of these detections, and trigger actions through the camera's event system or third-party software.

To find out more about how the application works, see *AXIS Image Health Analytics user manual*.

Cybersecurity

For product-specific information about cybersecurity, see the product's datasheet at axis.com.

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

Signed OS

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

Secure boot

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

Axis Edge Vault

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

Axis device ID

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

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

Specifications

Product overview
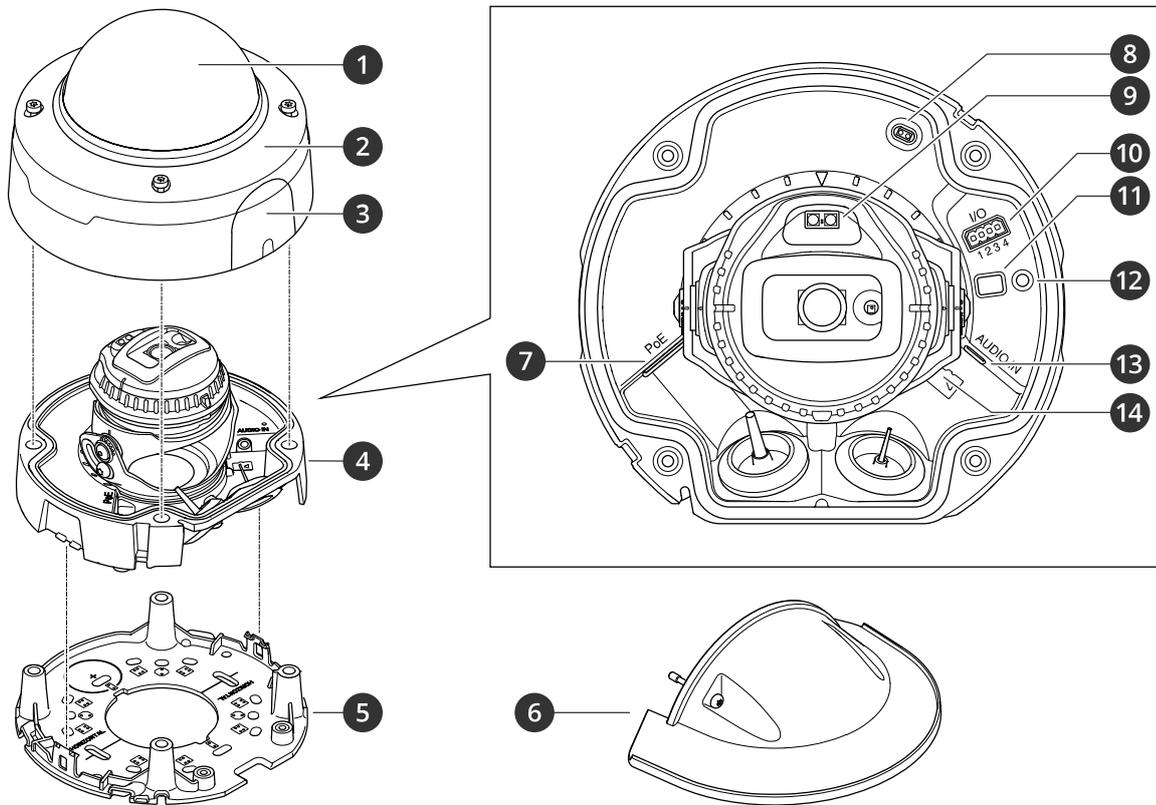
1 Dome
2 Dome cover
3 Lid
4 Camera unit
5 Mounting bracket
6 Weathershield
7 Network connector (PoE)
8 Case open detector
9 IR LED
10 I/O connector
11 Control button
12 Status LED indicator
13 Audio connector
14 SD card memory slot

LED indicators

Note
- The Status LED can be configured to flash while an event is active.
- The LEDs turn off when you close the casing.

Status LED	Indication
Unlit	Connection and normal operation.
Green	Shows steady green for 10 seconds for normal operation after startup completed. Flashes green during wireless network pairing. Steady green for normal operation.

	Flashes before startup if the temperature is below –20 °C and heating is required. The product starts when it reaches operating temperature.
Amber	Steady during startup. Flashes during device software upgrade or reset to factory default.
	Steady during startup. Flashes when restoring settings.
Amber/Red	Flashes amber/red if network connection is unavailable or lost.
Red	Device software upgrade failure.

Network LED	Indication
Green	Steady for connection to a 100 Mbit/s network. Flashes for network activity.
	Steady for connection to a 1 Gbit/s network. Flashes for network activity.
Amber	Steady for connection to a 10 Mbit/s network. Flashes for network activity.
	Steady for connection to a 10/100 Mbit/s network. Flashes for network activity.
Unlit	No network connection.

Power LED	Indication
Green	Normal operation.
Amber	Flashes green/amber during device software upgrade.

Microphone power LED	Indication
Unlit	Phantom power off.
Blue	Phantom power on.
	Steady when the phantom power is on and the microphone is connected.
	Flashes when the phantom power is on and the microphone is disconnected.

Wireless LED	Indication
Unlit	Wired mode.
Green	Steady for connection to a wireless network. Flashes for network activity.
Red	Steady for no wireless network connection. Flashes while scanning for wireless networks.
Amber	Steady or flashing during wireless network pairing.

Note
- The tally LED (indication LED) only indicates network transmission. If video or audio is only transmitted through HDMI or SDI the tally LED will be unlit.

Tally LED	Indication
Unlit	Camera idle.
Red	Active network transmission or recording.

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 SD/SDHC/SDXC cards.

This device supports microSD/microSDHC/microSDXC cards.

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

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

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:
- Enabling the Focus Assistant. Press and very quickly release the Control button.

- Resetting the product to factory default settings. See *Reset to factory default settings, on page 35*.

- Ensuring the camera is level. Press the button for not more than two seconds to start the leveling assistant and press again to stop. The status LED and buzzer signal (see) assist leveling of the camera. The camera is level when the buzzer beeps continuously.

- Ensuring the camera is level. Press the button for not more than two seconds to start the leveling assistant and press again to stop. The buzzer signal (see) assist leveling of the camera. The camera is level when the buzzer beeps continuously.

- Connecting to an AXIS Video Hosting System service. To connect, press and hold the button for about 3 seconds until the status LED flashes green.

- 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

The Axis device is available in two variants with different network connectors:

RJ45 Ethernet connector.

RJ45 Ethernet connector with Power over Ethernet (PoE).

RJ45 Ethernet connector with Power over Ethernet Plus (PoE+).

RJ45 with High Power over Ethernet (High PoE).

RJ45 Push-pull Connector (IP66) with High Power over Ethernet (High PoE).

RJ45 Ethernet service port.

D-coded M12 connector with Power over Ethernet (PoE).

SFP connector.

NOTICE

To comply with the IP66-rated design of the camera and maintain the IP66 protection, the supplied RJ45 Push-pull Connector (IP66) shall be used. Alternatively, use the RJ45 IP66-rated cable with premounted connector which is available from your Axis reseller. Don't remove the plastic network connector shield from the camera.

Audio connector

3.5 mm 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 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 in** – 3.5 mm input for two mono microphones, or two line-in mono signals (using the supplied stereo-to-mono adapter).

- **Audio in** – 3.5 mm input for a stereo microphone, or a line-in stereo signal.

- **Audio out** – 3.5 mm output for audio (line level) that can be connected to a public address (PA) system or an active speaker with a built-in amplifier. A stereo connector must be used for audio out.

- **Audio out** – 3.5 mm output for audio (line level) that can be connected to a public address (PA) system or an active speaker with balanced input and a built-in amplifier. A balanced connector must be used for audio out.

- **Audio out** – 3.5 mm output for audio (line level) that can be connected to a public address (PA) system or an active speaker with a built-in amplifier. A pair of headphones can also be attached. A stereo connector must be used for audio out.


Audio input

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

Audio output

1 Tip	2 Ring	3 Sleeve
Channel 1, unbalanced line, mono	Channel 1, unbalanced line, mono	Ground
Balanced line, "hot" signal	Balanced line, "cold" signal	Ground
Stereo unbalanced line, "left"	Stereo unbalanced line, "right"	Ground
Channel 1, unbalanced line	Channel 2, unbalanced line	Ground

4-pin terminal block for audio input and output.
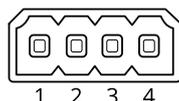
Function	Pin	Notes
GND	1	Ground
Ring power	2	12 V for external source
Microphone/Line in	3	Microphone (analog or digital) or line in (mono). 5 V microphone bias is available.
Line out	4	Line level audio output (mono). Can be connected to a public address (PA) system or an active speaker with a built-in amplifier.

2-pin terminal block for line out.
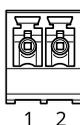
Function	Pin	Notes
Line out (+)	1	Line audio out
0 V DC (–)	2	

2-pin terminal block for amplifier out.
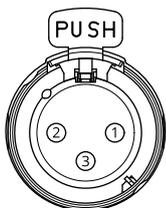
Function	Pin
Amplifier out (+)	1
Amplifier out (–)	2

The internal microphone is used by default; the external microphone is used when connected. You can disable the internal microphone by connecting a plug to the microphone input.

The external microphone is used when connected.

XLR connector

- **Left** – 3-pin XLR connector for balanced audio input. Use left connector for mono.
- **Right** – 3-pin XLR connector for balanced audio input.

Pin	1	2	3
Function	Ground	Balanced Microphone Hot (+) In	Balanced Microphone Cold (–) In

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.

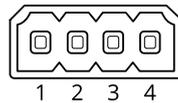**Supervised input –** Enables possibility to detect tampering on a digital input.

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.

A digital light sensor – For receiving a value of the ambient light intensity from an external light sensor. This is used to control the device's day and night functionality.
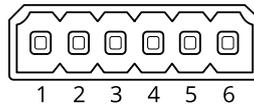
Note

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

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 = 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

Function	Pin	Notes	Specifications
DC ground	1		0 VDC
DC output	2	⚠️ Can be used to power auxiliary equipment.	12 VDC Max load = 50 mA

		Note: This pin can only be used as power out.	
Configurable (Input or Output)	3–4	Digital input or Supervised input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. To use supervised input, install end-of-line resistors. See connection diagram for information about how to connect the resistors.	0 to max 30 VDC
		Digital output – Internally connected to pin 1 (DC ground) when active, and floating (unconnected) when inactive. If used with an inductive load, e.g., a relay, connect a diode in parallel with the load, to protect against voltage transients.	0 to max 30 VDC, open drain, 100 mA

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 or Supervised input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. To use supervised input, install end-of-line resistors. See connection diagram for information about how to connect the resistors.	0 to max 30 VDC
		Digital output – Internally connected to pin 1 (DC ground) when active, and floating (unconnected) when inactive. If used with an inductive load, e.g., a relay, connect a diode in parallel with the load, to protect against voltage transients.	0 to max 30 VDC, open drain, 100 mA

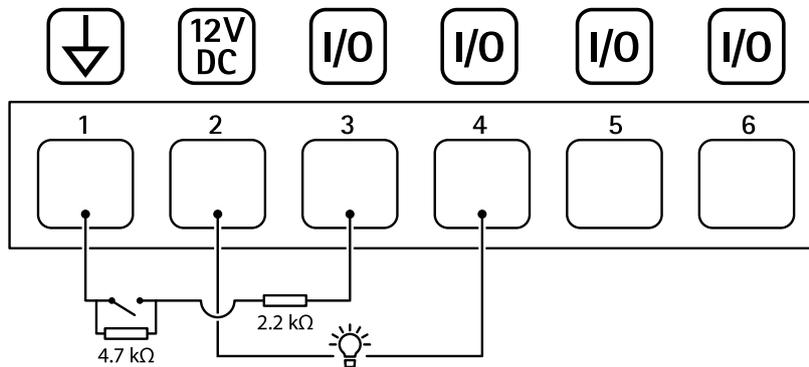**Example:**
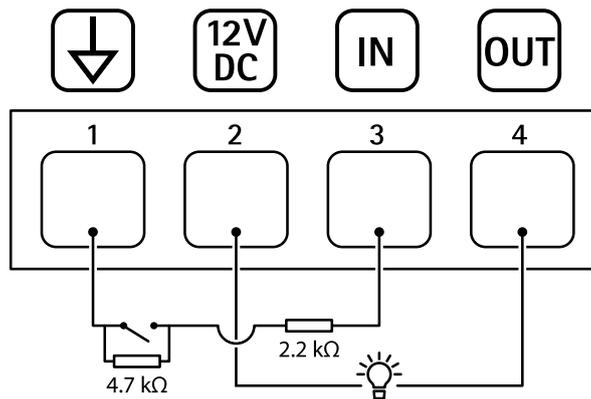
1   DC ground
2   DC output 12 V, max 25 mA
3   Supervised input
4   Digital output
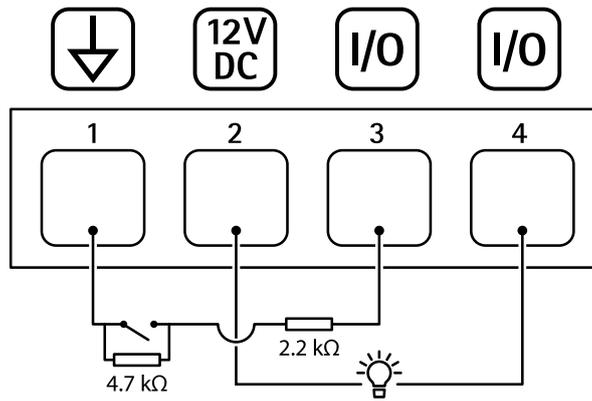
33

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

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

Troubleshooting

Reset to factory default settings

⚠ WARNING

☀ Possibly hazardous optical radiation is emitted from this product. It can be harmful to the eyes. Don't stare at the operating lamp.

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.

Note

For products with multiple IP addresses and AXIS OS 11.11 or earlier, channel 1 will have the address 192.168.0.90, channel 2 will have the address 192.168.0.91 and so on. Products with AXIS OS 12.0 and later will obtain a distinct IP address obtained from the link-local address subnet for each channel (169.254.x.x).

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 27*.

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*.

6. Refocus the product.

1. Press and hold the control button and the restart button at the same time.

2. Release the restart button but continue to hold down the control button for 15–30 seconds until the status LED indicator flashes amber.

3. 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

4. Use the installation and management software tools to assign an IP address, set the password and access the video stream.

5. Release the restart button and hold the control button.

6. Keep the control button pressed until the power LED indicator turns green and the 4 status LED indicators turn amber (this may take up to 15 seconds).

7. Keep the control button pressed until the power LED indicator turns green and the 6 status LED indicators turn amber (this may take up to 15 seconds).

8. Release the control button. When the status LED indicators display green (which can take up to 1 minute) the process is complete and the unit has been reset.

9. The process is now complete. If no DHCP server is available on the network, the device IP addresses will default to either of the following:
   - **Devices with AXIS OS 12.0 and later:** Obtained from the link-local address subnet (169.254.x.x)

–   **Devices with AXIS OS 11.11 and earlier:** 192.168.0.90 to 192.168.0.93

10. The process is now complete. If no DHCP server is available on the network, the device IP addresses will default to either of the following:

    –   **Devices with AXIS OS 12.0 and later:** Obtained from the link-local address subnet (169.254.x.x)

    –   **Devices with AXIS OS 11.11 and earlier:** 192.168.0.90 to 192.168.0.95

11. Use the installation and management software tools to assign the IP addresses, set the password and access the video stream.

Note

To reset a single channel to the original factory default settings, log in to the device's web interface and use the provided button.

1. Press and hold the control button and the power button for 15–30 seconds until the status LED indicator flashes amber. See *Product overview, on page 27*.

2. Release the control button but continue to hold down the power button until the status LED indicator turns green.

3. Release the power button and assemble the product.

4. The process is now complete. The product has been reset to the factory default settings. 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. Using the installation and management software tools to assign an IP address, set the password and access the video stream.

1. Press and hold the control button and the power button. See *Product overview, on page 27*.

2. Release the power button but continue to hold down the control button for 15–30 seconds until the status LED indicator flashes amber.

3. Release the control button.

4. The process is now complete. The product has been reset to the factory default settings. 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. Using the installation and management software tools, assign an IP address, set the password and access the video stream.

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.

- Make sure the cover is attached during upgrade to avoid installation failure.

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 35*.

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 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*.

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 41.*
- 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.
- Log in to the device's web interface and set a capture mode that prioritizes frame rate. If you change the capture mode to prioritize frame rate it might lower the maximum resolution, depending on the device used and capture modes available.
- The maximum frames per second is dependent on the utility frequency (60/50 Hz) of the Axis device.

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 retrieving additional video streams

I get an error message:

- in AXIS Camera Station Edge: 'Video Error', or

- in Chrome/Firefox: 'Stream: Error. Something went wrong. Maybe there are too many viewers.', or

- in Quick Time: '503 service unavailable', or

- AXIS Camera Station 5 or Pro: 'Camera not available', or

- in browser when using the Java applet: 'Error reading video stream'

The reason is that the camera is designed to deliver up to four different streams. If a fifth unique stream is requested, the camera can't provide it, and you get an error message. The error message depends on the way the stream is requested. The streams are used on a first come, first served basis. Examples of instances that use a stream are:

- live viewing in a web browser or other application

- while recording - continuous or motion triggered recording

- an event that uses images on the camera, for example an event that sends an e-mail with an image every hour

- an installed and running application, such as AXIS Object Analytics, always consumes a video stream whether it's used or not. A stopped application doesn't consume a video stream.

The camera can deliver more than four simultaneous streams provided the configuration of any additional stream is identical to any of the first four streams. Identical configuration implies exactly the same resolution, frame rate, compression, video format, rotation etc.

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*.

The image is blurry

The focus is set when the camera is manufactured. But the image can become blurry for different reasons. Try solving the issue in the following order:

1. Clean the dome. See notice below for more information.

2. Clean the lens. See notice below for more information.

3. Turn the focus ring, see image below.

4. Use the focus adjustment tool if you need more precision in turning the focus ring. You can *download the focus adjustment tool* and 3D print it.

5. If the image is still blurry, contact Axis support. See *Contact support, on page 42.*
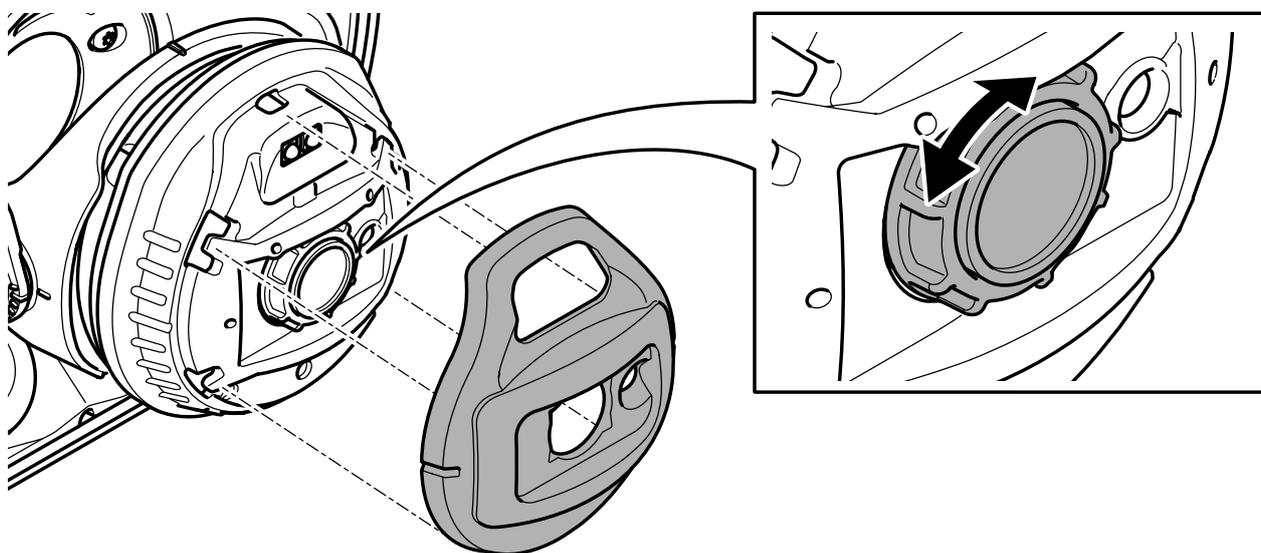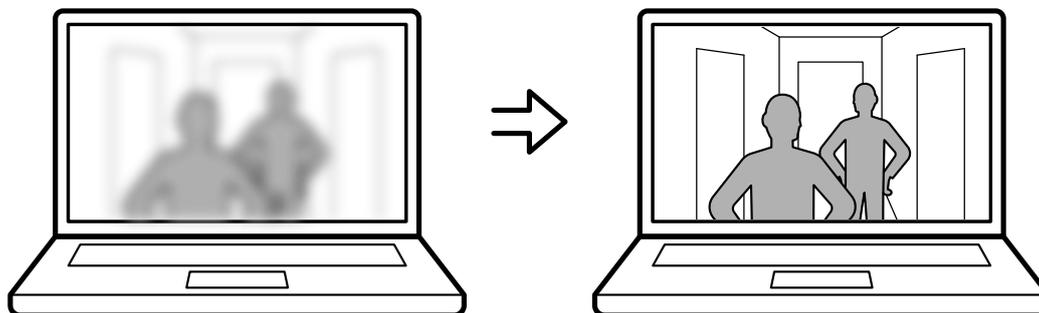
Set focus using the focus ring.

NOTICE

- Be careful not to scratch, damage or leave fingerprints on the dome or the lens because this can decrease image quality. If possible, keep the protective plastic on the dome until the installation is complete.

- Do not clean a dome or a lens that looks clean to the eye. Excessive cleaning could damage the surface.

- Never polish the dome or the lens.

- For general cleaning of the dome we recommend to use a non-abrasive, solvent-free neutral soap or detergent mixed with pure water and a soft, clean cloth. Rinse well with pure lukewarm water. Dry with a soft, clean cloth to prevent water spotting.

- For general cleaning of the lens we recommend to use a soft, clean cloth.

- Never use harsh detergents, gasoline, benzene, acetone, or similar chemicals.

- Avoid cleaning the dome in direct sunlight or at elevated temperatures.

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.

- Removing or attaching the cover will restart the camera.

- 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*.