AXIS M5000-G PTZ Camera

User manual

Table of Contents

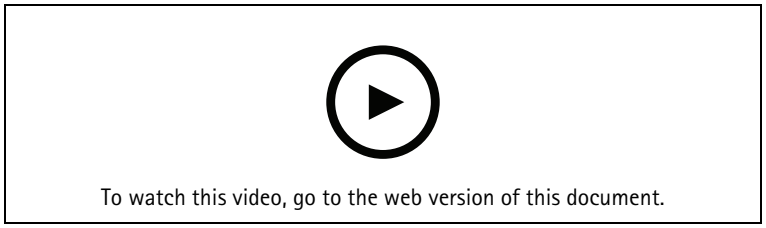
Installation

How to install the product

How to install the product with a ceiling mount

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*.

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 27*.

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 27*.
   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 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 .

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 18*.

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

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**:

Note

When you increase the gain, image noise also increases.

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

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.

Handle scenes with strong backlight

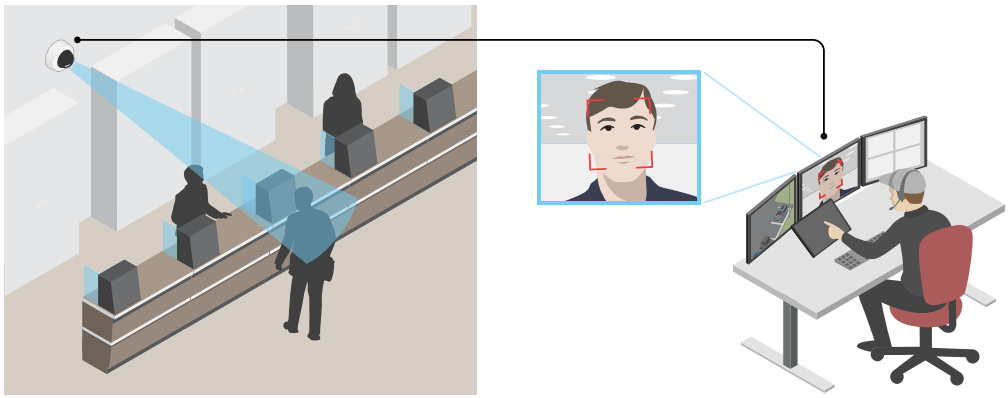
Dynamic range is the difference in light levels in an image. In some cases the difference between the darkest and the brightest areas can be significant. The result is often an image where either the dark or the bright areas are visible. Wide dynamic range (WDR) makes both dark and bright areas of the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

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

Find out more about WDR and how to use it at *axis.com/solutions/wide-dynamic-range-wdr*.

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 18*

Show the pan or tilt position as a text overlay

You can show the pan or tilt position as an overlay in the image.

1. Go to **Video > Overlays** and click  .
2. In the text field, type `#x` to show the pan position.
   Type `#y` to show the tilt position.
3. Choose appearance, text size, and alignment.
4. The current pan and tilt positions show up in the live view image and in the recording.

Adjust the camera view (PTZ)

Limit the pan, tilt, and zoom movements

If there are parts of the scene that you don't want the camera to reach, you can limit the pan, tilt, and zoom movements. 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 movements:

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 20*.

Reduce bandwidth and storage

Important

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

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

View a live video stream on a monitor

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**.

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 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.

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**.

Direct the camera to a preset position when the camera detects motion

This example explains how to set up the camera to go to a preset position when it detects motion in the image.

1. Start the application if it is not already running.
2. Make sure you have set up the application according to your needs.

Add a preset position:

Go to **PTZ** and set where you want the camera to be directed by creating a preset position.

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, select **Go to preset position**.
4. Select the preset position you want the camera to go to.
5. 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**.

Use PIR and audio to deter intruders

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

Before you start:

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

Create a rule:

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

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

Audio

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**.

Set up Z-Wave®

For more information about Z-Wave, go to *Wireless I/O (Z-Wave Plus® v2), on page 19*.

Considerations

Before using wireless I/O with Z-Wave Plus v2, consider the following:

- To do any Z-Wave configurations, you need to be an administrator.
- When performing Z-Wave related actions on the product's web page, such as adding, removing and replacing Z-Wave devices or resetting the Z-Wave network, we recommend that you do not reload the page or move away from it when the action process is ongoing. If done, the action's actual and displayed statuses may differ. To recover, you may need to wait up to several minutes and then reload the page again.
- Replication, i.e. copying network information to another control device, is executed as part of the inclusion process.
- This product ignores all commands in the Basic Command Class.

Turn on Z-Wave

1. Go to **System > Z-Wave**.
2. Go to **Gateway settings wireless I/O** and turn on Z-Wave. You may need to wait for a few minutes for Z-Wave to become active.

Add a Z-Wave device

Though not limited by the Z-Wave Plus v2 protocol, your product's event system allows you to add Z-Wave devices at any given time. If the maximum number is reached, you need to remove a Z-Wave device before you can add a new one. See the product's datasheet for information about maximum number of Z-Wave devices.

1. Go to **System > Z-Wave**.

2. Go to **Device management** and click **+ Add device**. The product starts looking for Z-Wave devices in the Z-Wave network.
3. Set the Z-Wave device to be added into inclusion/exclusion mode as described in its User Manual.
4. If requested, enter the PIN delivered with the Z-Wave device, and click **OK**.
5. Wait until the adding process is finalized as indicated by a notification on the web page.

The added Z-Wave device is now visible in the device management list.

Note

If the Z-Wave device is not found, the adding process is terminated automatically.

To see the detailed status information of the added Z-Wave device, expand the device information in the device management list.

Note

Status information for an added Z-Wave device varies depending on the device type. For more information, see the online help ⓘ.

You can set the product to trigger rules with specified Z-Wave trigger conditions. The available Z-Wave conditions and actions vary depending on the added Z-Wave device type.

Add a Z-Wave device with SmartStart inclusion

You can add a Z-Wave device to the Z-Wave network with SmartStart inclusion. A Z-Wave device added to the SmartStart list is automatically added to the device management list within 10 minutes of being powered on in the network vicinity.

1. Go to **System > Z-Wave**.
2. Go to **SmartStart** and click **+ Add device information**.
3. Type the device specific key and any optional information.
4. Click **OK**.

Remove a Z-Wave device through inclusion/exclusion mode

Note

This is the recommended removal procedure.

1. Go to **System > Z-Wave**.
2. Go to **Device management** and click 🗑. The product starts looking for Z-Wave devices in the Z-Wave network.
3. Set the Z-Wave device to be removed into inclusion/exclusion mode as described in its User Manual.
4. Wait until the removal process is finalized as indicated by a notification on the web page.

The Z-Wave device is now removed from the device management list.

Note

All product-related information in the removed Z-Wave device is deleted.

Note

If the Z-Wave device is not found, the removal process is terminated automatically.

Remove a Z-Wave device through forced process

There may be a communication fail, for example due to drained battery, so you may not be able to remove the Z-Wave device by setting it to inclusion/exclusion mode. You can perform a forced removal of a Z-Wave device that shows the status **Down** in the device management list.

1. Go to **System > Z-Wave**.
2. Go to **Device management** and expand the device information for the Z-Wave device to be removed.
3. Go to **Node > Status** and click −.
4. Wait until the exclusion process is finalized as indicated by a notification on the web page.

The Z-Wave device is now removed from the device management list.

Note

All product-related information in the removed Z-Wave device is retained.

Remove a Z-Wave device from the SmartStart list

Note

A Z-Wave device will not be removed from the device management list if you remove it from the SmartStart list.

1. Go to **System > Z-Wave**.
2. Go to **SmartStart**.
3. Hover over the device in the list to display the trash icon: 🗑.
4. Click 🗑 next to the Z-Wave device to be remove it from the SmartStart list.

Replace a Z-Wave device

There may be a communication fail, for example due to a faulty Z-Wave device, and you want to replace the device with another one. You can perform a forced replacement of a Z-Wave device that shows status **Down** in the device management list.

1. Go to **System > Z-Wave**.
2. Go to **Device management** and expand the device information for the Z-Wave device to be replaced.
3. Go to **Node > Status** and click ⟳. The product starts looking for Z-Wave devices in the Z-Wave network.
4. Set the Z-Wave device that is to replace the existing device into inclusion/exclusion mode as described in its User Manual.
5. Wait until the replacement process is finalized as indicated by a notification on the web page.

The new Z-Wave device with some status information is now visible in the device management list.

Note

Node ID and event action information is handed over to the new Z-Wave device. All other information is deleted.

Note

If the Z-Wave device is not found, the replacement process is terminated automatically.

Reset the Z-Wave network

Important

- This procedure removes all Z-Wave devices from the product.
- After resetting the Z-Wave network, you also need to either remove each Z-Wave device or reset it to factory default before you can add it to any network again.
- Use this procedure only when the network primary controller is missing or otherwise inoperable.

1. Go to **System > Z-Wave**.
2. Go to **Device management** and click ⋮.

3. Select **Reset network** in the drop-down menu.

All added Z-Wave devices are now removed from the product, and the device management list is empty.

Use Z-Wave as I/O

This product doesn't have any physical I/O connectors, but you can use Z-Wave functions in the I/O interface.

You can assign an I/O port number to up to a maximum of six connected Z-Wave devices. To see the port numbers, go to **System > Accessories > I/O ports**. The I/O port number can be changed in the Z-Wave device's information window.

When used as a digital input port event, the Z-Wave device can only use one function. The default function depends on what type of device it is. To change which function to use, go to the device's information window.

For more information about using I/O ports, see the product's built-in help.

The web interface

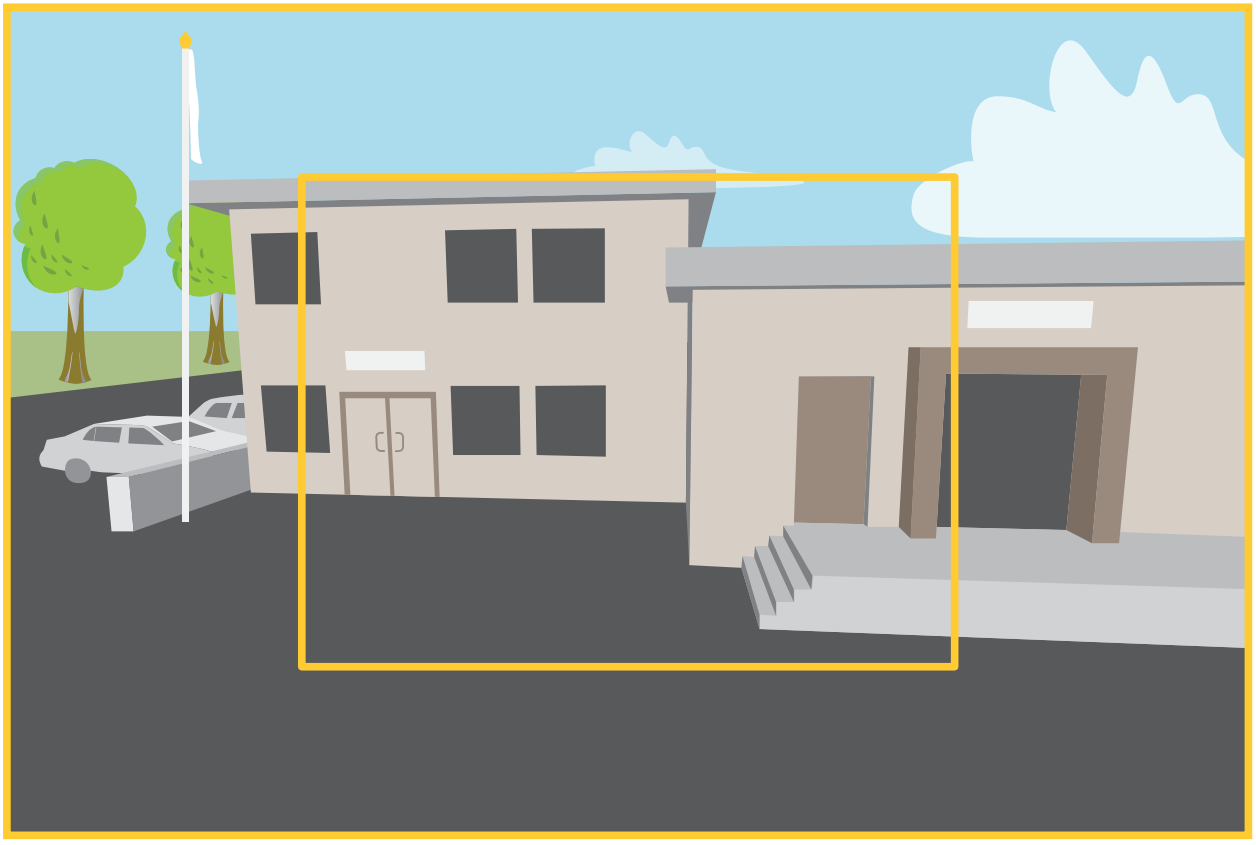
To read about all the features and settings available in the web interface of devices with AXIS OS, go to *AXIS OS web interface help*.

Learn more

Capture modes

A capture mode is a preset configuration that defines how the camera captures images. The capture mode setting can affect the camera's field of view and aspect ratio. The shutter speed can also be affected, which in turn affects the light sensitivity.

The lower resolution capture mode might be sampled from the original resolution, or it might be cropped out from the original, in which case the field of view could also be affected.



The image shows how the field of view and aspect ratio can change between two different 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*.

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.

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.

Overlays

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

Pan, tilt, and zoom (PTZ)

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.

Wireless I/O (Z-Wave Plus® v2)

This is a security enabled Z-Wave Plus® v2 product that can use encrypted Z-Wave Plus v2 messages to communicate with security enabled Z-Wave Plus v2 devices. The product can be operated in any Z-Wave® network with compatible Z-Wave certified devices from other manufacturers. To increase the network reliability, all non-battery operated Z-Wave devices in the network act as repeaters regardless of vendor. This product acts as the control device and the Z-Wave devices added to it act as secondary devices.

Associations

- This product supports one association group with group identifier = 1 (Lifeline).
- Maximum number of devices that can be added to the association group = 1.
- Group identifier 1 is used to send the Device Reset Locally report.

Command classes

This product supports the following command classes:

- COMMAND_CLASS_APPLICATION_STATUS
- COMMAND_CLASS_ASSOCIATION_V3 (secured)
- COMMAND_CLASS_ASSOCIATION_GRP_INFO_V3 (secured)
- COMMAND_CLASS_CRC_16_ENCAP
- COMMAND_CLASS_DEVICE_RESET_LOCALLY (secured)
- COMMAND_CLASS_FIRMWARE_UPDATE_MD_V5 (secured)
- COMMAND_CLASS_INCLUSION_CONTROLLER
- COMMAND_CLASS_INDICATOR_V3 (secured)
- COMMAND_CLASS_MANUFACTURER_SPECIFIC_V2 (secured)
- COMMAND_CLASS_MULTI_CHANNEL_ASSOCIATION_V4 (secured)
- COMMAND_CLASS_MULTI_CMD
- COMMAND_CLASS_NETWORK_MANAGEMENT_BASIC_V2 (secured)
- COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION_V4 (secured)
- COMMAND_CLASS_NETWORK_MANAGEMENT_INSTALLATION_MAINTENANCE_V4 (secured)
- COMMAND_CLASS_NETWORK_MANAGEMENT_PROXY_V4 (secured)
- COMMAND_CLASS_NODE_PROVISIONING (secured)
- COMMAND_CLASS_POWERLEVEL (secured)
- COMMAND_CLASS_SECURITY
- COMMAND_CLASS_SECURITY_2

- COMMAND_CLASS_SUPERVISION
- COMMAND_CLASS_TIME
- COMMAND_CLASS_TRANSPORT_SERVICE_V2
- COMMAND_CLASS_VERSION_V3 (secured)
- COMMAND_CLASS_ZWAVEPLUS_INFO_V2 (secured)

Note

The product supports COMMAND_CLASS_INDICATOR_V3, however there is no visible indicator.

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.

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.

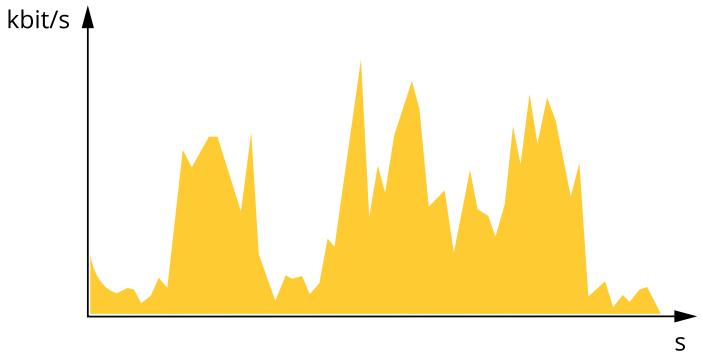
The **Stream** tab contains settings for video streams. You get these settings if you request a video stream from the product and don't specify for example resolution, or frame rate. When you change the settings in the **Stream** tab, it doesn't affect ongoing streams, but it will take effect when you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

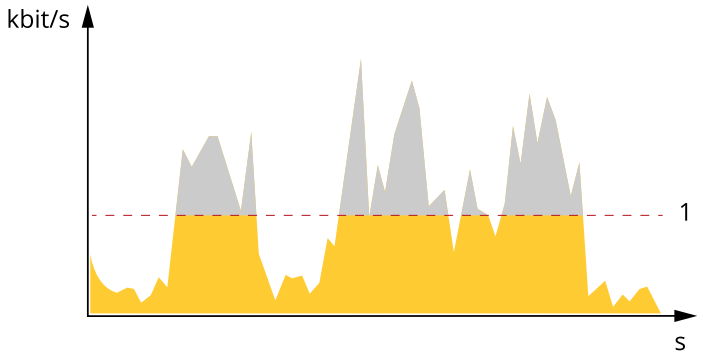
Bitrate control

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.



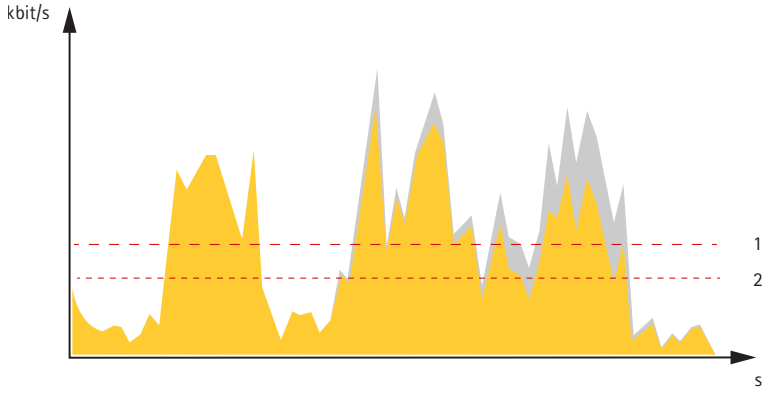
Maximum bitrate (MBR)
Maximum bitrate lets you set a target bitrate to handle bitrate limitations in your system. You might see a decline in image quality or frame rate as the instantaneous bitrate is kept below the specified target bitrate. You can choose to prioritize either image quality or frame 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

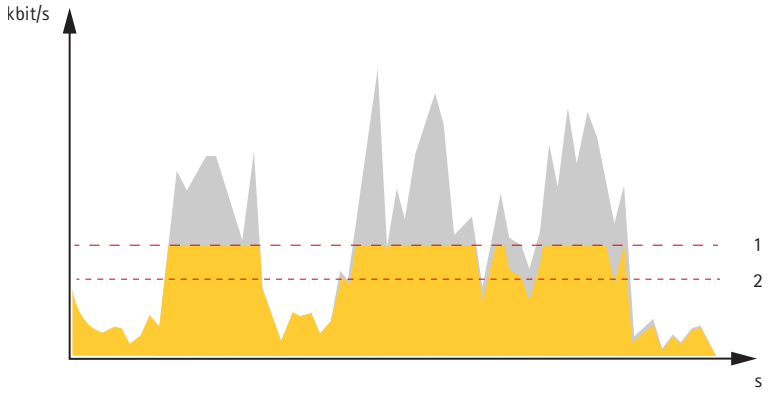
Average bitrate (ABR)
With average bitrate, the bitrate is automatically adjusted over a longer period of time. This is so you can meet the specified target and provide the best video quality based on your available storage. Bitrate is higher in scenes with a lot of activity, compared to static scenes.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

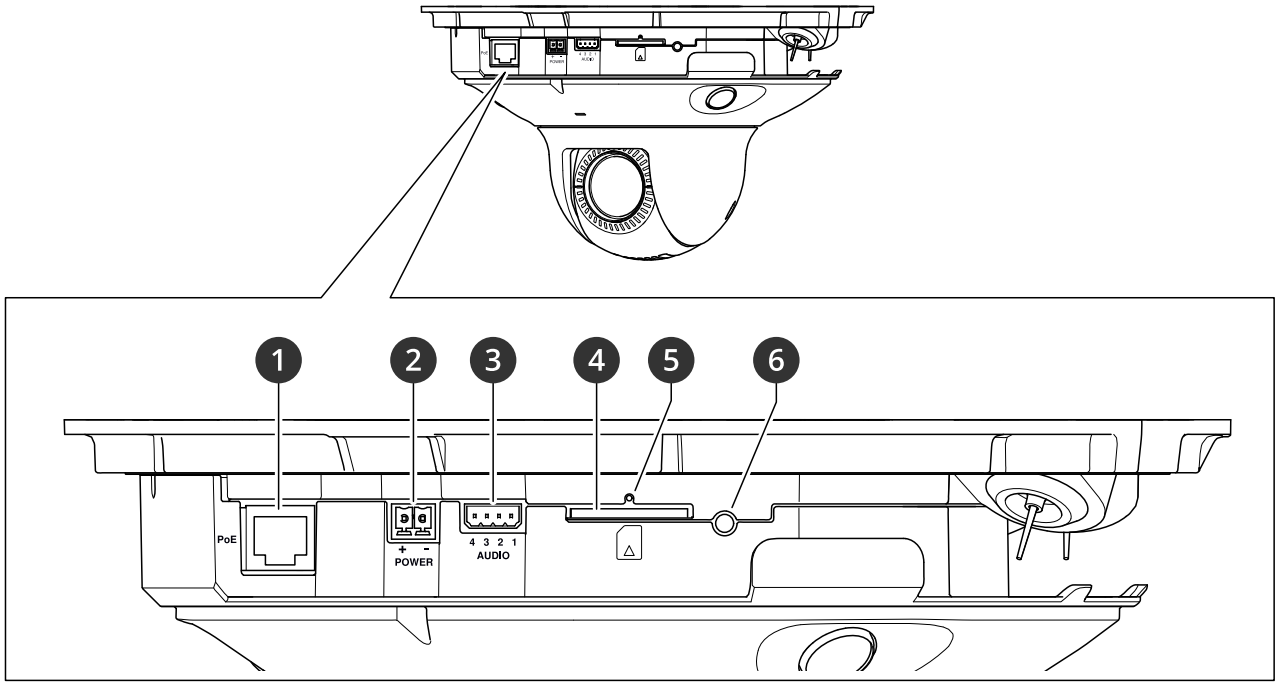
- Several apps can run at the same time but some apps might not be compatible with each other. Certain combinations of apps might require too much processing power or memory resources when run in parallel. Verify that the apps work together before deployment.

Important

AXIS 3D People Counter is an app that is embedded in the device. We don't recommend you to run any other apps on this device since it can affect the performance of the AXIS 3D People Counter.

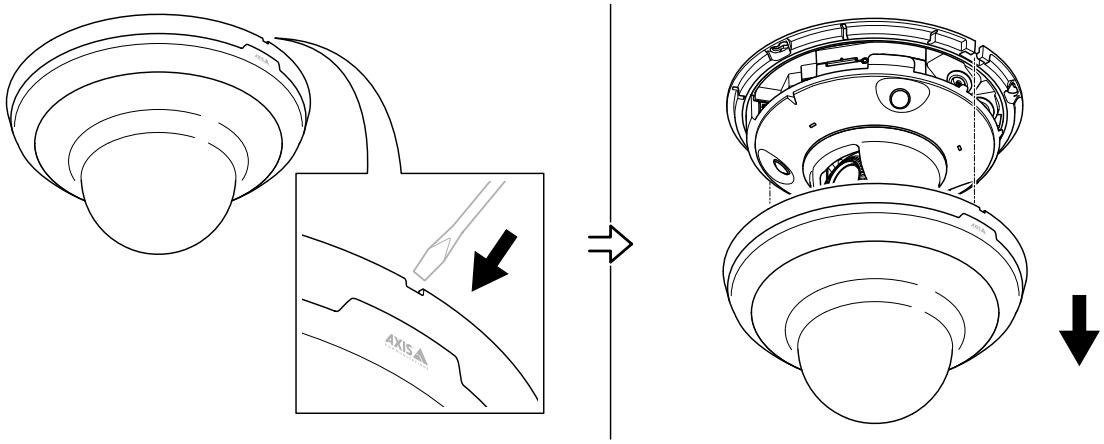
Specifications

Product overview



1 *Network connector (PoE)*
2 *Power connector*
3 *Audio connector*
4 *SD card slot (SD/SDHC/SDXC card)*
5 *Status LED indicator*
6 *Control button*

How to remove the dome



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.

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.

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.

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.

Buttons

Control button

The control button is used for:

- Resetting the product to factory default settings. See *Reset to factory default settings, on page 27*.
- Connecting to a one-click cloud connection (O3C) service over the internet. To connect, press and release the button, then wait for the status LED to flash green three times.

Connectors

Network connector

RJ45 Ethernet connector with Power over Ethernet (PoE).

Audio connector

4-pin terminal block for audio input and output. See *Product overview, on page 23*.

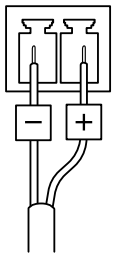
For audio in, the left channel is used from a stereo signal.

Function	Pin	Notes
GND	1	Audio GND
NC	2	Not connected

AUDIO IN	3	Audio line in
AUDIO OUT	4	Audio line out

Power connector

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



Clean your device

You can clean your device with lukewarm water.

NOTICE

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

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

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

Troubleshooting

Reset to factory default settings

Important

If you have a Z-Wave network, you must reset the Z-Wave network before resetting your device to factory default. See *Reset the Z-Wave network, on page 15*.

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

The camera has been preconfigured with AXIS License Plate Verifier. If you reset to factory default, you need to reinstall the license key. See .

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 23*.
3. Keep the control button pressed for 15–30 seconds until the status LED indicator flashes amber.
4. Release the control button. The process is complete when the status LED indicator turns green. If no DHCP server is available on the network, the device IP address will default to one of the following:
   - **Devices with AXIS OS 12.0 and later:** Obtained from the link-local address subnet (169.254.0.0/16)
   - **Devices with AXIS OS 11.11 and earlier:** 192.168.0.90/24
5. Use the installation and management software tools to assign an IP address, set the password, and access the device.
   The installation and management software tools are available from the support pages on *axis.com/support*.

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

AXIS OS options

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

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

Check the current AXIS OS version

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

To check the current AXIS OS version:

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

Upgrade AXIS OS

Important

- When you upgrade the device software, your preconfigured and customized settings are saved. Axis Communications AB can't guarantee that the settings are saved, even if the features are available in the new AXIS OS version.
- Starting from AXIS OS 12.6, you must install every LTS version between your device's current version and the target version. For example, if the currently installed device software version is AXIS OS 11.2, you have to install the LTS version AXIS OS 11.11 before you can upgrade the device to AXIS OS 12.6. For more information, see *AXIS OS 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*.

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 27*.

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 31*.
- 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.

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*.

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*.

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*. 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* 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*. 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* 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* 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.

Secure component verification (SCV)

Your device comes with SCV, a certificate that verifies you've received the correct device, and that your device has not been tampered with since it left the factory. The certificate is signed by the manufacturer and stored in iDRAC.

When you receive your device, use the AXIS Recorder Toolbox to verify your device's SCV certificate. Refer to *dell.com* for more information about SCV.

T10169100

2026-07 (M18.2)