AXIS XFQ1656

User manual

AXIS XFQ1656

Table of Contents

Installation

Preview mode

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

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

help.axis.com/?&piaId=79189&section=preview-mode

This video demonstrate 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™	Firefox®	Edge™	Safari®
Windows®	recommended	recommended	✓	
macOS®	recommended	recommended	✓	✓
Linux®	recommended	recommended	✓	
Other operating systems	✓	✓	✓	✓*

*To use AXIS OS web interface with iOS 15 or iPadOS 15, go to **Settings > Safari > Advanced > Experimental Features** and disable NSURLSession Websocket.*

If you need more information about recommended browsers, go to *AXIS OS Portal*.

Open the device's web interface

1. Open a browser and type the IP address or host name of the Axis device.

   If you do not 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 set the root password. See *Set a new password for the root account on page 4*.

Set a new password for the root account

The default administrator username is `root`. There's no default password for the root account. You set a password the first time you log in to the device.

1. Type a password. Follow the instructions about secure passwords. See *Secure passwords on page 4*.

2. Retype the password to confirm the spelling.

3. Click **Add user**.

Important

   If you lose the password for the root account, go to *Reset to factory default settings on page 71* and follow the instructions.

Secure passwords

Important

   Axis devices send the initially set password in clear text over the network. To protect your device after the first login, set up a secure and encrypted HTTPS connection and then change the password.

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.

Verify that no one has tampered with the firmware

To make sure that the device has its original Axis firmware, 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 71*.

   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.

help.axis.com/?&piaId=79189&section=web-interface-overview

Axis device web interface

Configure your device

Basic settings

Set the capture mode

1. Go to **Video > Installation > Capture mode**.

2. Click **Change**.

3. Select a capture mode and click **Save and restart**.

   See also *Capture modes on page 50*.

Set the orientation

1. Go to **Video > Installation > Rotate**.

2. Select **0** , **90**, **180** or **270** degrees.

   See also *Monitor long and narrow areas on page 9* .

Adjust the image

This section includes instructions about configuring your device. If you want to learn more about how certain features work, go to *Learn more on page 50*.

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 ⚙ .

2. Click 👁‍🗨 to show the level grid.

3. Adjust the camera mechanically until the position of the reference area or the object is aligned with the level grid.

Adjust the zoom and focus

To adjust the zoom:

1. Go to **Video > Installation** and adjust the zoom slider.

To adjust the focus:

1. Click 👁‍🗨 to show the autofocus area.

2. Adjust the autofocus area to cover the part of the image that you want to be in focus.

   If you don't select an autofocus area, the camera focuses on the entire scene. We recommend that you focus on a static object.

3. Click **Autofocus**.

4. To fine tune the focus, adjust the focus slider.

Configure your device

Select scene profile

A scene profile is a set of predefined image appearance settings including color level, brightness, sharpness, contrast and local contrast. Scene profiles are preconfigured in the product for quick setup to a specific scenario, for example **Forensic** which is optimized for surveillance conditions. For a description of each available setting, see *The device interface on page 17*.

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

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

2. Go to **Scene profile** and select a profile.

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**.

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**.

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 possible, open the aperture.

- 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**:

- Move the **Blur-noise trade-off** slider toward **Low motion blur**.

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.

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.

1. Go to **Video > Image > Wide dynamic range**.

2. Use the **Local contrast** slider to adjust the amount of WDR.

3. Use the **Tone mapping** slider to adjust the amount of WDR.

4. If you still have problems, go to **Exposure** and adjust the **Exposure zone** to cover the area of interest.

Find out more about WDR and how to use it at *axis.com/web-articles/wdr*.

Stabilize a shaky image with electronic image stabilization (EIS)

Electronic Image Stabilization (EIS) can be used in environments where the product is mounted in an exposed location and subject to vibrations, for example, wind or passing traffic.

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

Note

The image is cropped slightly when EIS is enabled, lowering the maximum resolution.

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

2. Turn on **Image stabilization**.

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)**.

3. Use the slider to improve the image.

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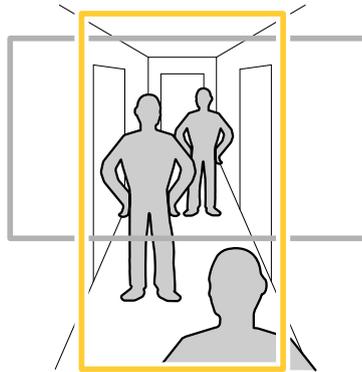
1. Depending on your device, turn the camera or the 3-axis lens in the camera 90° or 270°.

2. If the device doesn't have automatic rotation of the view, go to **Video > Installation**.

3. Rotate the view 90° or 270°.

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 51*

Show an image overlay

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

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

2. Select **Image** and click ✚ .

3. Click **Images**.

4. Drag and drop an image.

5. Click **Upload**.

6. Click **Manage overlay**.

7. 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 in the video stream.

4. Select a position. You can also drag the overlay text field in the live view to change the position.

View and record video

This section includes instructions about configuring your device. To learn more about how streaming and storage works, go to
Streaming and storage on page 51.

Reduce bandwidth and storage

Important

    Reducing the bandwidth can result in loss of details in the image.

1. Go to **Video > Stream**.

2. Click ⚙ in the live view.

3. Select **Video format 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.

   Note

       The **Zipstream** settings are used for both H.264 and H.265.

   - Turn on **Dynamic FPS**.

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

Configure your device

Note

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

Set up network storage

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

1. Go to **System > Storage**.

2. Click **+** **Add network storage** under **Network storage**.

3. Type the IP address of the host server.

4. Type the name of the shared location on the host server under **Network share**.

5. Type the username and password.

6. Select the SMB version or leave it on **Auto**.

7. Select **Add share even if connection fails** 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 > Image**.

2. To start a recording, click ● .

   If you haven't set up any storage, click 🗄 and ⚙ . For instructions on how to set up network storage, see *Set up network storage on page 11*

3. To stop recording, click ● again.

Watch video

1. Go to **Recordings**.

2. Click ▶ for your recording in the list.

Verify that no one has tampered with the video

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

1. Go to **Video > Stream > General** and turn on **Signed video**.

2. Use AXIS Camera Station (5.46 or later) or another compatible video management software to record video. For instructions, see the *AXIS Camera Station user manual*.

3. Export the recorded video.

4. Use AXIS File Player to play the video. *Download AXIS File Player.*

indicates that no one has tampered with the video.

Note

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

Set up rules for events

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

To learn more, check out our guide *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** the device should perform when the conditions are met.

Note

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

Record video when the camera detects an object

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

Before you start:

*   Make sure you have an SD card installed.

Make sure that AXIS Object Analytics is running:

1. Go to **Apps > AXIS Object Analytics**.

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

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

Create a rule:

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

2. Type a name for the rule.

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

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

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

6. Select a camera and a stream profile.

7. Set the prebuffer time to 5 seconds.

8. Set the postbuffer time to 1 minute.

9. Click **Save**.

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:

1. Go to **Apps > AXIS Object Analytics**.

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

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

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 actions, under **Overlay text**, select **Use overlay text**.

5. Select a video channel.

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

7. Set the duration.

8. Click **Save**.

Note

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

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.
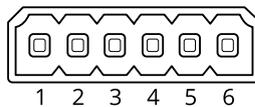
Configure your device

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

Note

> For information on the I/O connector, see *Connectors on page 61*.

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**.

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 62*.

1. Go to **System > Accessories** 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**.

4. Type an email address to send the email to.

5. The camera doesn't have it's own email server, so it has to log into another email server to send mails. Fill in the rest of the information according to your email provider.

6. To send a test email, click **Test**.

7. 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 and a message for the email.

7. Click **Save**.

Audio

Add audio to your recording

Turn on audio:

1. Go to **Video > Stream > Audio** and include audio.

2. If the device has more than one input source, select the correct one in **Source**.

3. Go to **Audio > Device settings** and turn on the correct input source.

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

Edit the stream profile that is used for the recording:

5. Go to **System > Stream profiles** and select the stream profile.

6. Select **Include audio** and turn it on.

7. Click **Save**.

Connect to a network speaker

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

Important

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

Pair camera with network speaker

1. Go to **System > Edge-to-edge > Pairing**.

2. Type the network speaker's IP address, username and password.

3. Select **Speaker pairing**.

4. Click **Connect**. A confirmation message appears.

The device interface

To reach the device interface, type the device's IP address in a web browser.

Note

Support for the features and settings described in this section varies between devices. This icon ⓘ indicates that the feature or setting is only available in some devices.

☰ Show or hide the main menu.

❓ Access the product help.

💬 Change the language.

◐ Set light theme or dark theme.

👤 👤 👤 The user menu contains:

- Information about the user who is logged in.
- 👥 **Change user** : Log out the current user and log in a new user.
- ↪ **Log out** : Log out the current user.

⋮ The context menu contains:

- **Analytics data**: Accept to share non-personal browser data.
- **Feedback**: Share any feedback to help us improve your user experience.
- **Legal**: View information about cookies and licenses.
- **About**: View device information, including firmware version and serial number.
- **Legacy device interface**: Change the device interface to the legacy device interface.

Status

Device info

Shows device information, including firmware version and serial number.

Upgrade firmware: Click to go to the Maintenance page where you can do a firmware upgrade.

Time sync status

Shows NTP synchronization information, including if the device is in sync with an NTP server and the time remaining until the next sync.

NTP settings: Click to go to the Date and time page where you can change the NTP settings.

Security

Shows what kinds of access to the device that are active, and what encryption protocols are in use. Recommendations to the settings are based on the AXIS OS Hardening Guide.

Hardening guide: Click to go to *AXIS OS Hardening guide* where you can learn more about how to apply cybersecurity best practices.

Connected clients

View details: Click to show all clients that are connected to the device.

Ongoing recordings

Recordings: Shows each ongoing recording and its source. For more information, see *Recordings on page 30*

Shows the storage space where the recording is saved.

Video

▶ Click to play the live video stream.

⏸ Click to freeze the live video stream.

📷 Click to take a snapshot of the live video stream. The file is saved in the 'Downloads' folder on your computer. The image file name is [snapshot_YYYY_MM_DD_HH_MM_SS.jpg]. The size of the snapshot depends on the compression that is applied from the specific web-browser engine where the snapshot is received, therefore, the snapshot size may vary from the actual compression setting that is configured in the device.

⌁ ⓘ Click to show I/O output ports. Use the switch to open or close the circuit of a port, for example to test external devices.

IR ⓘ Click to manually turn on or turn off the IR illumination.

💡 ⓘ Click to manually turn on or turn off the white light.

⯐ Click to access onscreen controls:

• **Predefined controls**: Turn on to use the available onscreen controls.

• **Custom controls**: Click ➕ **Add custom control** to add an onscreen control.

🜒 ⓘ Starts the washer. When the sequence starts, the camera moves to the configured position to receive the wash spray. When the whole wash sequence is completed, the camera returns to its previous position. This icon is only visible when the washer is connected and configured.

🜕 ⓘ Starts the wiper.

📍 ⓘ Click and select a preset position to go to that preset position in the live view. Or, click **Setup** to go to the preset position page.

AXIS XFQ1656

The device interface

:diamond-focus-add: :diamond-focus-remove: (i) Adds or removes a focus recall area. When you add a focus recall area, the camera saves the focus settings at that specific pan/tilt range. When you have set a focus recall area and the camera enters that area in the live view, the camera recalls the previously saved focus. It's enough to cover half of the area for the camera to recall the focus.

:shield: (i) Click to select a guard tour, then click **Start** to play the guard tour. Or, click **Setup** to go to the guard tours page.

:heater: (i) Click to manually turn on the heater for a selected period of time.

• Click to start a continuous recording of the live video stream. Click again to stop the recording. If a recording is ongoing, it will resume automatically after a reboot.

:storage: Click to show the storage that is configured for the device. To configure the storage you need to be logged in as an administrator.

:gear: Click to access more settings:

- **Video format**: Select the encoding format to use in the live view.
- **Client stream information**: Turn on to show dynamic information about the video stream used by the browser that shows the live video stream. The bitrate information differs from the information shown in a text overlay, because of different information sources. The bitrate in the client stream information is the bitrate of the last second, and it comes from the encoding driver of the device. The bitrate in the overlay is the average bitrate of the last 5 seconds, and it comes from the browser. Both values cover only the raw video stream and not the additional bandwidth generated when it's transported over the network through UDP/TCP/HTTP.
- **Adaptive stream**: Turn on to adapt the image resolution to the viewing client's actual display resolution, to improve the user experience and help prevent a possible overload of the client's hardware. The adaptive stream is only applied when you view the live video stream in the web interface in a browser. When adaptive stream is turned on, the maximum frame rate is 30 fps. If you take a snapshot while adaptive stream is turned on, it will use the image resolution selected by the adaptive stream.
- **Level grid**: Click :eye-off: to show the level grid. The grid helps you decide if the image is horizontally aligned. Click :eye: to hide it.
- **Pixel counter**: Click :eye-off: to show the pixel counter. Drag and resize the box to contain your area of interest. You can also define the pixel size of the box in the **Width** and **Height** fields.
- **Refresh**: Click :refresh: to refresh the still image in the live view.
- **PTZ controls** (i) : Turn on to display PTZ controls in the live view.

1:1 Click to show the live view at full resolution. If the full resolution is larger than your screen size, use the smaller image to navigate in the image.

:fullscreen: Click to show the live video stream in full screen. Press ESC to exit full screen mode.

Installation

Capture mode (i) : A capture mode is a preset configuration that defines how the camera captures images. When you change the capture mode, it can affect many other settings, such as view areas and privacy masks.

Mounting position (i) : The orientation of the image can change depending on how the camera is mounted.

Power line frequency: Select the frequency that is used in your region to minimize image flicker. The American regions usually use 60 Hz. The rest of the world mostly uses 50 Hz. If you're not sure of your region's power line frequency, check with the local authorities.

Rotate: Select the preferred image orientation.

Zoom: Use the slider to adjust the zoom level.

Focus: Use the slider to set the focus manually.

AF: Click to make the camera focus on the selected area. If you don't select an autofocus area, the camera focuses on the entire scene.

Autofocus area: Click 👁 to show the autofocus area. This area should include the area of interest.

Reset focus: Click to make the focus return to its original position.

Image correction

> **Important**
>
> We recommend you not to use multiple image correction features at the same time, since it can lead to performance issues.

Barrel distortion correction (BDC) (i) : Turn on to get a straighter image if it suffers from barrel distortion. Barrel distortion is a lens effect that makes the image appear curved and bent outwards. The condition is seen more clearly when the image is zoomed out.

Crop (i) : Use the slider to adjust the correction level. A lower level means that the image width is kept at the expense of image height and resolution. A higher level means that image height and resolution are kept at the expense of image width.

Remove distortion (i) : Use the slider to adjust the correction level. Pucker means that the image width is kept at the expense of image height and resolution. Bloat means that image height and resolution are kept at the expense of image width.

Image stabilization (i) : Turn on to get a smoother and steadier image with less blur. We recommend that you use image stabilization in environments where the device is mounted in an exposed location and subject to vibrations due to, for example, wind or passing traffic.

Focal length (i) : Use the slider to adjust the focal length. A higher value leads to higher magnification and a narrower angle of view, while a lower value leads to a lower magnification and a wider angle of view.

Stabilizer margin (i) : Use the slider to adjust the size of the stabilizer margin, which determines the level of vibration to stabilize. If the product is mounted in an environment with a lot of vibration, move the slider towards **Max**. As a result, a smaller scene is captured. If the environment has less vibration, move the slider towards **Min**.
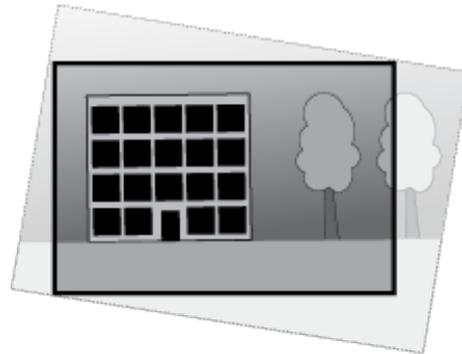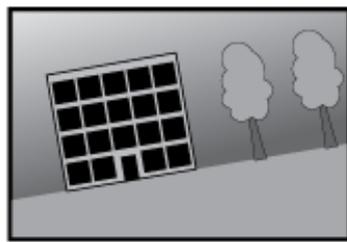
The device interface

Straighten image ⓘ : Turn on and use the slider to straighten the image horizontally by rotating and cropping it digitally. The functionality is useful when it's not possible to mount the camera exactly level. Ideally, straighten the image during installation.

⊞ : Click to show a supporting grid in the image.

▦ : Click to hide the grid.

The image before and after it has been straightened.

Image

Appearance

Scene profile ⓘ : Select a scene profile that suits your surveillance scenario. A scene profile optimizes image settings, including color level, brightness, sharpness, contrast, and local contrast, for a specific environment or purpose.

- **Forensic**: Suitable for surveillance purposes.
- **Indoor** ⓘ : Suitable for indoor environments.
- **Outdoor** ⓘ : Suitable for outdoor environments.
- **Vivid**: Useful for demonstration purposes.
- **Traffic overview**: Suitable for vehicle traffic monitoring.

Saturation: Use the slider to adjust the color intensity. You can for example get a grayscale image.

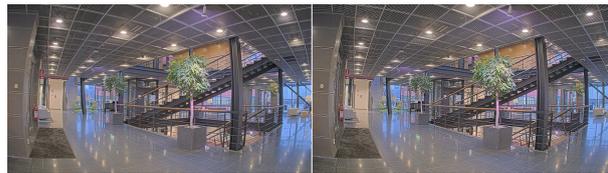**Contrast**: Use the slider to adjust the difference between light and dark.

Brightness: Use the slider to adjust the light intensity. This can make objects easier to see. Brightness is applied after image capture, and doesn't affect the information in the image. To get more details from a dark area, it's usually better to increase gain or exposure time.

Sharpness: Use the slider to make objects in the image appear sharper by adjusting the edge contrast. If you increase the sharpness, it may increase the bitrate and the amount of storage space needed as well.

Wide dynamic range

WDR ⓘ : Turn on to make both bright and dark areas of the image visible.

Local contrast ⓘ : Use the slider to adjust the contrast of the image. A higher value makes the contrast higher between dark and light areas.

Tone mapping ⓘ : Use the slider to adjust the amount of tone mapping that is applied to the image. If the value is set to zero only the standard gamma correction is applied, while a higher value increases the visibility of the darkest and brightest parts in the image.

White balance

The device interface

When the camera detects the color temperature of the incoming light, it can adjust the image to make the colors look more natural. If this is not sufficient, you can select a suitable light source from the list.

The automatic white balance setting reduces the risk of color flicker by adapting to changes gradually. If the lighting changes, or when the camera is first started, it can take up to 30 seconds to adapt to the new light source. If there is more than one type of light source in a scene, that is they differ in color temperature, the dominating light source acts as a reference for the automatic white balance algorithm. This behavior can be overridden by choosing a fixed white balance setting that matches the light source you want to use as a reference.

Light environment:

- **Automatic**: Automatic identification and compensation for the light source color. This is the recommended setting which can be used in most situations.

- **Automatic – outdoors** ⓘ : Automatic identification and compensation for the light source color. This is the recommended setting which can be used in most outdoor situations.

- **Custom – indoors** ⓘ : Fixed color adjustment for a room with some artificial light other than fluorescent lighting and good for a normal color temperature around 2800 K.

- **Custom – outdoors** ⓘ : Fixed color adjustment for sunny weather conditions with a color temperature around 5500 K.
- **Fixed – fluorescent 1**: Fixed color adjustment for fluorescent lighting with a color temperature around 4000 K.
- **Fixed – fluorescent 2**: Fixed color adjustment for fluorescent lighting with a color temperature around 3000 K.
- **Fixed – indoors**: Fixed color adjustment for a room with some artificial light other than fluorescent lighting and good for a normal color temperature around 2800 K.
- **Fixed – outdoors 1**: Fixed color adjustment for sunny weather conditions with a color temperature around 5500 K.
- **Fixed – outdoors 2**: Fixed color adjustment for cloudy weather condition with a color temperature around 6500 K.

- **Street light – mercury** ⓘ : Fixed color adjustment for ultraviolet emission in mercury vapor lights common in street lighting.

- **Street light – sodium** ⓘ : Fixed color adjustment that compensates for the yellow orange color of sodium vapor lights common in street lighting.
- **Hold current**: Keep the current settings and do not compensate for light changes.

- **Manual** ⓘ : Fix the white balance with the help of a white object. Drag the circle to an object that you want the camera to interpret as white in the live view image. Use the **Red balance** and **Blue balance** sliders to adjust the white balance manually.

Day-night mode

IR-cut filter:

- **Auto**: Select to automatically turn on and off the IR-cut filter. When the camera is in day mode, the IR-cut filter is turned on and blocks incoming infrared light, and when in night mode, the IR-cut filter is turned off and the camera's light sensitivity increases.
- **On**: Select to turn on the IR-cut filter. The image is in color, but with reduced light sensitivity.
- **Off**: Select to turn off the IR-cut filter. The image is in black and white for increased light sensitivity.

Threshold: Use the slider to adjust the light threshold where the camera changes from day mode to night mode.

- Move the slider towards **Bright** to decrease the threshold for the IR-cut filter. The camera changes to night mode earlier.
- Move the slider towards **Dark** to increase the threshold for the IR-cut filter. The camera changes to night mode later.

IR light ⓘ

If your device doesn't have built-in illumination, these controls are only available when you have connected a supporting Axis accessory.

Allow illumination: Turn on to let the camera use the built-in light in night mode.

The device interface

Synchronize illumination: Turn on to automatically synchronize the illumination with the surrounding light. The synchronization between day and night only works if the IR-cut filter is set to **Auto** or **Off**.

Automatic illumination angle (i) : Turn on to use the automatic illumination angle.

Illumination angle (i) : Use the slider to manually set the illumination angle, for example if the angle needs to be different from the camera's angle of view. If the camera has a wide angle of view, you can set the illumination angle to a narrower angle, which equals a greater tele position. This will result in dark corners in the image.

IR wavelength (i) : Select the desired wavelength for the IR light.

White light (i)

Allow illumination (i) : Turn on to let the camera use white light in night mode.

Synchronize illumination (i) : Turn on to automatically synchronize the white light with the surrounding light.

Exposure

Exposure mode: Select an exposure mode to reduce rapidly changing irregular effects in the image, for example flicker produced by different types of light sources. We recommend you to use the automatic exposure mode, or the same frequency as your power network.

- **Automatic**: The camera adjusts the aperture, gain and shutter automatically.

- **Automatic aperture** (i) : The camera adjusts the aperture and gain automatically. The shutter is fixed.

- **Automatic shutter** (i) : The camera adjusts the shutter and gain automatically. The aperture is fixed.
- **Hold current**: Locks the current exposure settings.

- **Flicker-free** (i) : The camera adjusts the aperture and gain automatically, and uses only the following shutter speeds: 1/50 s (50 Hz) and 1/60 s (60 Hz).

- **Flicker-free 50 Hz** (i) : The camera adjusts the aperture and gain automatically, and uses the shutter speed 1/50 s.

- **Flicker-free 60 Hz** (i) : The camera adjusts the aperture and gain automatically, and uses the shutter speed 1/60 s.

- **Flicker-reduced** (i) : This is the same as flicker-free, but the camera might use shutter speeds faster than 1/100 s (50 Hz) and 1/120 s (60 Hz) for brighter scenes.

- **Flicker-reduced 50 Hz** (i) : This is the same as flicker-free, but the camera might use shutter speeds faster than 1/100 s for brighter scenes.

- **Flicker-reduced 60 Hz** (i) : This is the same as flicker-free, but the camera might use shutter speeds faster than 1/120 s for brighter scenes.

- **Manual** (i) : The aperture, gain and shutter are fixed.

Exposure zone (i) : Use exposure zones to optimize the exposure in a selected part of the scene, for example, the area in front of an entrance door.

The device interface

> Note
>
> The exposure zones are related to the original image (unrotated), and the names of the zones apply to the original image. This means, for example, that if the video stream is rotated 90°, then the **Upper** zone becomes the **Right** zone in the stream, and **Left** becomes **Lower**.

- **Automatic**: Suitable for most situations.
- **Center**: Uses a fixed area in the center of the image to calculate the exposure. The area has a fixed size and position in the live view.
- **Full** ⓘ : Uses the entire live view to calculate the exposure.
- **Upper** ⓘ : Uses an area with a fixed size and position in the upper part of the image to calculate the exposure.
- **Lower** ⓘ : Uses an area with a fixed size and position in the lower part of the image to calculate the exposure.
- **Left** ⓘ : Uses an area with a fixed size and position in the left part of the image to calculate the exposure.
- **Right** ⓘ : Uses an area with a fixed size and position in the right part of the image to calculate the exposure.
- **Spot**: Uses an area with a fixed size and position in the live view to calculate the exposure.
- **Custom**: Uses an area in the live view to calculate the exposure. You can adjust the size and position of the area.

Max shutter: Select the shutter speed to provide the best image. Low shutter speeds (longer exposure) might cause motion blur when there is movement, and a too high shutter speed might affect the image quality. Max shutter works with max gain to improve the image.

Max gain: Select the suitable max gain. If you increase the max gain, it improves the visible level of detail in dark images, but also increases the noise level. More noise can also result in increased use of bandwidth and storage. If you set the max gain to a high value, images can differ a lot if the light conditions are very different from day to night. Max gain works with max shutter to improve the image.

Motion-adaptive exposure ⓘ : Select to reduce motion blur in low-light conditions.

Blur-noise trade-off: Use the slider to adjust the priority between motion blur and noise. If you want to prioritize low bandwidth and have less noise at the expense of details in moving objects, move the slider towards **Low noise**. If you want to prioritize the preservation of details in moving objects at the expense of noise and bandwidth, move the slider towards **Low motion blur**.

> Note
>
> You can change the exposure either by adjusting the exposure time or by adjusting the gain. If you increase the exposure time, it results in more motion blur, and if you increase the gain it results in more noise. If you adjust the **Blur-noise trade-off** towards **Low noise**, the automatic exposure will prioritize longer exposure times over increasing gain, and the opposite if you adjust the trade-off towards **Low motion blur**. Both the gain and exposure time will eventually reach their maximum values in low-light conditions, regardless of the priority set.

Lock aperture ⓘ : Turn on to keep the aperture size set by the **Aperture** slider. Turn off to allow the camera to automatically adjust the aperture size. You can, for example, lock the aperture for scenes with permanent light conditions.

Aperture ⓘ : Use the slider to adjust the aperture size, that is, how much light passes through the lens. To allow more light to enter the sensor and thereby produce a brighter image in low-light conditions, move the slider towards **Open**. An open aperture also reduces the depth of field, which means that objects close to or far from the camera can appear unfocused. To allow more of the image to be in focus, move the slider towards **Closed**.

Exposure level: Use the slider to adjust the image exposure.

Defog ⓘ : Turn on to detect the effects of foggy weather and automatically remove them for a clearer image.

> **Note**
>
> We recommend you not to turn on **Defog** in scenes with low contrast, large light level variations, or when the autofocus is slightly off. This can affect the image quality, for example, by increasing the contrast. Furthermore, too much light can negatively impact the image quality when defog is active.

Optics

Temperature compensation: Turn on if you want the focus position to be corrected based on the temperature in the optics.

IR compensation ⓘ : Turn on if you want the focus position to be corrected when IR-cut filter is off and when there is IR light.

Calibrate zoom and focus: Click to reset the optics and the zoom and focus settings to the factory default position. You need to do this if the optics have lost calibration during transport, or if the device has been exposed to extreme vibrations.

Stream

General

Resolution: Select the image resolution suitable for the surveillance scene. A higher resolution increases bandwidth and storage.

Frame rate: To avoid bandwidth problems on the network or reduce storage size, you can limit the frame rate to a fixed amount. If you leave the frame rate at zero, the frame rate is kept at the highest possible rate under the current conditions. A higher frame rate requires more bandwidth and storage capacity.

Compression: Use the slider to adjust the image compression. High compression results in a lower bitrate and lower image quality. Low compression improves the image quality, but uses more bandwidth and storage when you record.

Signed video ⓘ : Turn on to add the signed video feature to the video. Signed video protects the video from tampering by adding cryptographic signatures to the video.

Zipstream

Zipstream is a bitrate reduction technology, optimized for video surveillance, that reduces the average bitrate in an H.264 or H.265 stream in real time. Axis Zipstream applies a high bitrate in scenes where there are multiple regions of interest, for example in scenes with moving objects. When the scene is more static, Zipstream applies a lower bitrate, and thereby reduces the required storage. To learn more, see *Reducing the bit rate with Axis Zipstream*

Select the bitrate reduction **Strength**:

- **Off**: No bitrate reduction.
- **Low**: No visible quality degradation in most scenes. This is the default option and it can be used in all types of scenes to reduce the bitrate.
- **Medium**: Visible effects in some scenes through less noise and a slightly lower level of detail in regions of lower interest, for example where there's no movement.
- **High**: Visible effects in some scenes through less noise and a lower level of detail in regions of lower interest, for example where there's no movement. We recommend this level for cloud-connected devices and devices that use local storage.
- **Higher**: Visible effects in some scenes through less noise and a lower level of detail in regions of lower interest, for example where there's no movement.
- **Extreme**: Visible effects in most scenes. The bitrate is optimized for smallest possible storage.

Optimize for storage: Optimize settings for storing the stream by minimizing the bitrate while maintaining quality. The optimization is not applied to the stream shown in the web client. Turning on **Optimize for storage** also turns on **Dynamic GOP**.

Dynamic FPS (frames per second): Turn on to allow the bandwidth to vary based on the level of activity in the scene. More activity requires more bandwidth.

Lower limit: Enter a value to adjust the frame rate between minimal fps and the stream default fps based on scene motion. We recommend you to use lower limit in scenes with very little motion, where the fps could drop to 1 or lower.

Dynamic GOP (Group of Pictures): Turn on to dynamically adjust the interval between I-frames based on the level of activity in the scene.

Upper limit: Enter a maximum GOP length, that is, the maximum number of P-frames between two I-frames. An I-frame is a self-contained image frame that is independent of other frames.

P-frames: A P-frame is a predicted image that shows only the changes in the image from the previous frame. Enter the desired number of P-frames. The higher the number, the less bandwidth is required. However, if there are network congestion, there could be a noticeable deterioration in the video quality.

Bitrate control

- **Average**: Select to automatically adjust the bitrate over a longer time period and provide the best possible image quality based on the available storage.
  - ▣ Click to calculate the target bitrate based on available storage, retention time, and bitrate limit.
  - **Target bitrate**: Enter desired target bitrate.
  - **Retention time**: Enter the number of days to keep the recordings.
  - **Storage**: Shows the estimated storage that can be used for the stream.
  - **Maximum bitrate**: Turn on to set a bitrate limit.
  - **Bitrate limit**: Enter a bitrate limit that is higher than the target bitrate.
- **Maximum**: Select to set a maximum instant bitrate of the stream based on your network bandwidth.
  - **Maximum**: Enter the maximum bitrate.
- **Variable**: Select to allow the bitrate to vary based on the level of activity in the scene. More activity requires more bandwidth. We recommend this option for most situations.

Orientation

Mirror: Turn on to mirror the image.

Audio

Include: Turn on to use audio in the video stream.

Source ⓘ : Select what audio source to use.

Stereo ⓘ : Turn on to include built-in audio as well as audio from an external microphone.

Overlays

➕ : Click to add an overlay. Select the type of overlay from the dropdown list:

- **Text**: Select to show a text that is integrated in the live view image and visible in all views, recordings and snapshots. You can enter your own text, and you can also include pre-configured modifiers to automatically show for example time, date, frame rate.
  - 📅 : Click to add the date modifier %F to show yyyy-mm-dd.
  - 🕐 : Click to add the time modifier %X to show hh:mm:ss (24-hour clock).
  - **Modifiers**: Click to select any of the modifiers shown in the list to add them to the text box. For example, %a shows the day of the week.
  - **Size**: Select the desired font size.
  - **Appearance**: Select the text color and background color, for example, white text on a black background (default).

- ⬚ : Select the position of the overlay in the image.
- **Image**: Select to show a static image superimposed over the video stream. You can use .bmp, .png, .jpeg, or .svg files. To upload an image, click **Images**. Before you upload an image, you can choose to:
    - **Scale with resolution**: Select to automatically scale the overlay image to fit the video resolution.
    - **Use transparency**: Select and enter the RGB hexadecimal value for that color. Use the format RRGGBB. Examples of hexadecimal values: FFFFFF for white, 000000 for black, FF0000 for red, 6633FF for blue, and 669900 for green. Only for .bmp images.
- **Streaming indicator** ⓘ : Select to show an animation superimposed over the video stream. The animation indicates that the video stream is live, even if the scene doesn't contain any motion.
    - **Appearance**: Select the animation color and background color, for example, red animation on a transparent background (default).
    - **Size**: Select the desired font size.
    - ⬚ : Select the position of the overlay in the image.

View areas

＋ : Click to create a view area.

⬚ Click the view area to access settings.

Name: Enter a name for the view area. The maximum length is 64 characters.

Aspect ratio: Select desired aspect ratio. The resolution adjusts automatically.

PTZ: Turn on to use pan, tilt, and zoom functionality in the view area.

Privacy masks

＋ : Click to create a new privacy mask. The maximum number of masks depend on the complexity of all masks combined. Each mask can have maximum 10 anchor points.

Privacy masks: Click to change the color of all privacy masks, or to delete all privacy masks permanently.

Cell size: If you choose mosaic color, the privacy masks appear as pixilated patterns. Use the slider to change the size of the pixels.

⬛ **Mask x**: Click to rename, disable, or permanently delete the mask.

Audio

Overview

Locate device: Click to play a sound that helps you identify the speaker. For some products, a LED will flash on the device.

Calibrate ⓘ : Click to calibrate the speaker.

Launch AXIS Audio Manager Edge: Click to launch the application.

Device settings

Input: Turn on or off audio input. Shows the type of input.

Allow stream extraction (i) : Turn on to allow stream extraction.

Input type: Select the type of input, for instance if it's a microphone or line-in.

Power type: Select power type for your input.

Apply changes: Click to apply your selection.

Separate gain controls (i) : Turn on to adjust the gain separately for the different input types.

Automatic gain control (i) : Turn on to dynamically adapt the gain to changes in the sound.

Gain: Use the slider to change the gain. Click the microphone icon to mute or unmute.

Input: Turn on or off audio input. Shows the type of input.

Allow stream extraction (i) : Turn on to allow stream extraction.

Input type (i) : Select the type of input, for instance if it's internal microphone or line-in.

Power type (i) : Select power type for your input.

Apply changes (i) : Click to apply your selection.

Separate gain controls (i) : Turn on to adjust the gain separately for the different input types.

Automatic gain control (i) : Turn on to dynamically adapt the gain to changes in the sound.

Gain: Use the slider to change the gain. Click the microphone icon to mute or unmute.

Output (i) : Shows the type of output.

Gain: Use the slider to change the gain. Click the speaker icon to mute or unmute.

Stream

Encoding: Select the encoding to use for the input source streaming. You can only choose encoding if audio input is turned on. If audio input is turned off, click **Enable audio input** to turn it on.

Audio clips

┼ **Add clip**: Click to add a new audio clip. You can use .au, .mp3, .opus, .vorbis, .wav files.

▶ Click to play the audio clip.

■ Click to stop playing the audio clip.

⋮ The context menu contains:

- **Rename**: Change the name of the audio clip.
- **Create link**: Create a URL which, when used, plays the audio clip on the device. Specify the volume and number of times to play the clip.
- **Download**: Download the audio clip to your computer.
- **Delete**: Delete the audio clip from the device.

Audio enhancement

Input

Ten Band Graphic Audio Equalizer: Turn on to adjust the level of different frequency bands within an audio signal. This feature is for advanced users with audio configuration experience.

Talkback range ⓘ : Choose the operational range to gather audio content. An increase to the operational range cause a reduction of simultaneous two-way communication capabilities.

Voice enhancement ⓘ : Turn on to enhance the voice content in relation to other sounds.

Recordings

Ongoing recordings: Show all ongoing recordings on the camera.

● Select to start a recording on the camera.

▪ Choose which storage device to save to.

● Select to stop a recording on the camera.

Triggered recordings will end both when manually stopped and when the camera is shut down.

Continuous recordings will continue until manually stopped. Even if the camera is shut down, the recording will continue when the camera starts up again.

▶ Click to play the recording.

■ Click to stop playing the recording.

﹀ Click to show more information and options about the recording.

Set export range: If you only want to export part of the recording, enter from when to when.

🗑 Click to delete the recording.

Export: Click to export (part of) the recording.

☰ Click to filter the recordings.

From: Show recordings done after a certain point in time.

To: Show recordings up until a certain point in time.

Source ⓘ : Show recordings based on source.

Event: Show recordings based on events.

Storage: Show recordings based on storage type.

Apps

✚ **Add app**: Click to install a new app.

Find more apps: Click to go to an overview page of Axis apps.

Allow unsigned apps: Turn on to allow installation of unsigned apps.

Allow root-privileged apps: Turn on to allow apps with root privileges full access to the device.

Note

The device's performance might be affected if you run several apps at the same time.

Use the switch next to the app name to start or stop the app.

Open: Click to access the app's settings. The available settings depend on the application. Some applications don't have any settings.

⋮ The context menu can contain one or more of the following options:

- **Open-source license**: Click to view information about open-source licenses used in the app.
- **App log**: Click to view a log of the app events. The log is helpful when you contact support.
- **Activate license with a key**: If the app requires a license, you need to activate it. Use this option if your device doesn't have internet access.
  If you don't have a license key, go to *axis.com/products/analytics*. You need a license code and the Axis product serial number to generate a license key.
- **Activate license automatically**: If the app requires a license, you need to activate it. Use this option if your device has internet access. You need a license code to activate the license.

- **Deactivate the license**: Deactivate the license to use it in another device. If you deactivate the license, you also remove it from the device. To deactivate the license requires internet access.
- **Settings**: Configure the parameters.
- **Delete**: Delete the app permanently from the device. If you don't deactivate the license first, it remains active.

System

Date and time

The time format depends on the web browser's language settings.

Note

We recommend you to synchronize the device's date and time with an NTP server.

Synchronization: Select an option for synchronizing the device's date and time.

- **Automatic date and time (manual NTS KE servers)**: Synchronize with the secure NTP key establishment servers connected to the DHCP server.
  - **Manual NTS KE servers**: Enter the IP address of one or two NTP servers. When you use two NTP servers, the device synchronizes and adapts its time based on input from both.
- **Automatic date and time (NTP servers using DHCP)**: Synchronize with the NTP servers connected to the DHCP server.
  - **Fallback NTP servers**: Enter the IP address of one or two fallback servers.
- **Automatic date and time (manual NTP servers)**: Synchronize with NTP servers of your choice.
  - **Manual NTP servers**: Enter the IP address of one or two NTP servers. When you use two NTP servers, the device synchronizes and adapts its time based on input from both.
- **Custom date and time**: Manually set the date and time. Click **Get from system** to fetch the date and time settings once from your computer or mobile device.

Time zone: Select which time zone to use. Time will be automatically adjusted for daylight saving time and standard time.

Note

The system uses the date and time settings in all recordings, logs and system settings.

Regional settings

Sets the system of measurement to be used in all system settings.

Metric (m, km/h): Select for distance to be measured in meters and speed to be measured in kilometers per hour.

U.S. customary (ft, mph): Select for distance to be measured in feet and speed to be measured in miles per hour.

Network

IPv4

Assign IPv4 automatically: Select to let the network router assign an IP address to the device automatically. We recommend automatic IP (DHCP) for most networks.

IP address: Enter a unique IP address for the device. Static IP addresses can be assigned at random within isolated networks, provided that each address is unique. To avoid conflicts, we recommend you to contact your network administrator before you assign a static IP address.

Subnet mask: Enter the subnet mask to define what addresses are inside the local area network. Any address outside the local area network goes through the router.

Router: Enter the IP address of the default router (gateway) used to connect devices that are attached to different networks and network segments.

Fallback to static IP address if DHCP isn't available: Select if you want to add a static IP address to use as fallback if DHCP is unavailable and can't assign an IP address automatically.

IPv6

Assign IPv6 automatically: Select to turn on IPv6 and to let the network router assign an IP address to the device automatically.

Hostname

Assign hostname automatically: Select to let the network router assign a hostname to the device automatically.

Hostname: Enter the hostname manually to use as an alternative way of accessing the device. The hostname is used in the server report and in the system log. Allowed characters are A–Z, a–z, 0–9 and -.

DNS servers

Assign DNS automatically: Select to let the DHCP server assign search domains and DNS server addresses to the device automatically. We recommend automatic DNS (DHCP) for most networks.

Search domains: When you use a hostname that is not fully qualified, click **Add search domain** and enter a domain in which to search for the hostname used by the device.

DNS servers: Click **Add DNS server** and enter the IP address of the DNS server. This provides the translation of hostnames to IP addresses on your network.

HTTP and HTTPS

Allow access through: Select if a user is allowed to connect to the device through the **HTTP**, **HTTPS**, or both **HTTP and HTTPS** protocols.

HTTPS is a protocol that provides encryption for page requests from users and for the pages returned by the web server. The encrypted exchange of information is governed by the use of an HTTPS certificate, which guarantees the authenticity of the server.

To use HTTPS on the device, you must install an HTTPS certificate. Go to **System > Security** to create and install certificates.

Note

> If you view encrypted web pages through HTTPS, you might experience a drop in performance, especially when you request a page for the first time.

HTTP port: Enter the HTTP port to use. Port 80 or any port in the range 1024-65535 are allowed. If you are logged in as an administrator, you can also enter any port in the range 1-1023. If you use a port in this range, you get a warning.

HTTPS port: Enter the HTTPS port to use. Port 443 or any port in the range 1024-65535 are allowed. If you are logged in as an administrator, you can also enter any port in the range 1-1023. If you use a port in this range, you get a warning.

Certificate: Select a certificate to enable HTTPS for the device.

Network discovery protocols

Bonjour®: Turn on to allow automatic discovery on the network.

Bonjour name: Enter a friendly name to be visible on the network. The default name is the device name and MAC address.

UPnP®: Turn on to allow automatic discovery on the network.

UPnP name: Enter a friendly name to be visible on the network. The default name is the device name and MAC address.

WS-Discovery: Turn on to allow automatic discovery on the network.

One-click cloud connection

One-click cloud connection (O3C) together with an O3C service provides easy and secure internet access to live and recorded video from any location. For more information, see *axis.com/end-to-end-solutions/hosted-services*.

Allow O3C:

- **One-click**: The default setting. Press and hold the control button on the device to connect to an O3C service over the internet. You need to register the device with the O3C service within 24 hours after you press the control button. Otherwise, the device disconnects from the O3C service. Once you have registered the device, **Always** is enabled and the device stays connected to the O3C service.
- **Always**: The device constantly attempts to connect to an O3C service over the internet. Once you have registered the device, it stays connected to the O3C service. Use this option if the control button on the device is out of reach.
- **No**: Disables the O3C service.

Proxy settings: If needed, enter the proxy settings to connect to the proxy server.

Host: Enter the proxy server's address.

Port: Enter the port number used for access.

Login and **Password**: If needed, enter username and password for the proxy server.

Authentication method:

- **Basic**: This method is the most compatible authentication scheme for HTTP. It's less secure than the **Digest** method because it sends the username and password unencrypted to the server.
- **Digest**: This method is more secure because it always transfers the password encrypted across the network.
- **Auto**: This option lets the device select the authentication method depending on the supported methods. It prioritizes the **Digest** method over the **Basic** method.

Owner authentication key (OAK): Click **Get key** to fetch the owner authentication key. This is only possible if the device is connected to the internet without a firewall or proxy.

SNMP

The Simple Network Management Protocol (SNMP) allows remote management of network devices.

SNMP: Select the version of SNMP to use.

- **v1 and v2c**:
    - **Read community**: Enter the community name that has read-only access to all supported SNMP objects. The default value is **public**.
    - **Write community**: Enter the community name that has read/write access to all supported SNMP objects (except read-only objects). The default value is **write**.
    - **Activate traps**: Turn on to activate trap reporting. The device uses traps to send messages for important events or status changes to a management system. In the device interface, you can set up traps for SNMP v1 and v2c. Traps are automatically turned off if you change to SNMP v3 or turn off SNMP. If you use SNMP v3, you can set up traps through the SNMP v3 management application.
    - **Trap address**: Enter the IP address or host name of the management server.
    - **Trap community**: Enter the community to use when the device sends a trap message to the management system.
    - **Traps**:
    - **Cold start**: Sends a trap message when the device starts.
    - **Warm start**: Sends a trap message when you change an SNMP setting.
    - **Link up**: Sends a trap message when a link changes from down to up.
    - **Authentication failed**: Sends a trap message when an authentication attempt fails.

Note

All Axis Video MIB traps are enabled when you turn on SNMP v1 and v2c traps. For more information, see *AXIS OS Portal > SNMP*.

- **v3**: SNMP v3 is a more secure version, which provides encryption and secure passwords. To use SNMP v3, we recommend you to activate HTTPS, as the password is then sent through HTTPS. This also prevents unauthorized

parties to access unencrypted SNMP v1 and v2c traps. If you use SNMP v3, you can set up traps through the SNMP v3 management application.

- **Password for the account "initial"**: Enter the SNMP password for the account named "initial". Although the password can be sent without activating HTTPS, we don't recommend it. The SNMP v3 password can only be set once, and preferably only when HTTPS is enabled. Once the password is set, the password field is no longer displayed. To set the password again, you must reset the device to factory default settings.

Security

Certificates

Certificates are used to authenticate devices on a network. The device supports two types of certificates:

- **Client/server certificates**
  A client/server certificate validates the device's identity, and can be self-signed or issued by a Certificate Authority (CA). A self-signed certificate offers limited protection and can be used before a CA-issued certificate has been obtained.
- **CA certificates**
  You can use a CA certificate to authenticate a peer certificate, for example to validate the identity of an authentication server when the device connects to a network protected by IEEE 802.1X. The device has several pre-installed CA certificates.

These formats are supported:

- Certificate formats: .PEM, .CER, and .PFX
- Private key formats: PKCS#1 and PKCS#12

Important

If you reset the device to factory default, all certificates are deleted. Any pre-installed CA certificates are reinstalled.

Filter the certificates in the list.

Add certificate : Click to add a certificate.

The context menu contains:

- **Certificate information**: View an installed certificate's properties.
- **Delete certificate**: Delete the certificate.
- **Create certificate signing request**: Create a certificate signing request to send to a registration authority to apply for a digital identity certificate.

IEEE 802.1x

IEEE 802.1x is an IEEE standard for port-based network admission control providing secure authentication of wired and wireless network devices. IEEE 802.1x is based on EAP (Extensible Authentication Protocol).

To access a network protected by IEEE 802.1x, network devices must authenticate themselves. The authentication is performed by an authentication server, typically a RADIUS server (for example FreeRADIUS and Microsoft Internet Authentication Server).

Certificates

When configured without a CA certificate, server certificate validation is disabled and the device tries to authenticate itself regardless of what network it is connected to.

When using a certificate, in Axis' implementation, the device and the authentication server authenticate themselves with digital certificates using EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).

To allow the device to access a network protected through certificates, a signed client certificate must be installed on the device.

Client certificate: Select a client certificate to use IEEE 802.1x. The authentication server uses the certificate to validate the client's identity.

CA certificate: Select a CA certificate to validate the authentication server's identity. When no certificate is selected, the device tries to authenticate itself regardless of what network it is connected to.

EAP identity: Enter the user identity associated with the client certificate.

EAPOL version: Select the EAPOL version that is used in the network switch.

Use IEEE 802.1x: Select to use the IEEE 802.1x protocol.

Prevent brute-force attacks

Blocking: Turn on to block brute-force attacks. A brute-force attack uses trial-and-error to guess login info or encryption keys.

Blocking period: Enter the number of seconds to block a brute-force attack.

Blocking conditions: Enter the number of authentication failures allowed per second before the block starts. You can set the number of failures allowed both on page level and device level.

IP address filter

Use filter: Select to filter which IP addresses that are allowed to access the device.

Policy: Choose whether to **Allow** access or **Deny** access for certain IP addresses.

Addresses: Enter the IP numbers that are either allowed or denied access to the device. You can also use the CIDR format.

Custom-signed firmware certificate

To install test firmware or other custom firmware from Axis on the device, you need a custom-signed firmware certificate. The certificate verifies that the firmware is approved by both the device owner and Axis. The firmware can only run on a specific device which is identified by its unique serial number and chip ID. Custom-signed firmware certificates can only be created by Axis, since Axis holds the key to sign them.

Click **Install** to install the certificate. You need to install the certificate before you install the firmware.

Users

╋ **Add user**: Click to add a new user. You can add up to 100 users.

Username: Enter a unique username.

New password: Enter a password for the user. Passwords must be 1 to 64 characters long. Only ASCII printable characters (code 32 to 126) are allowed in the password, for example letters, numbers, punctuation, and some symbols.

Repeat password: Enter the same password again.

Role:

- **Administrator**: Has full access to all settings. Administrators can also add, update, and remove other users.
- **Operator**: Has access to all settings except:
    - All **System** settings.
    - Adding apps.
- **Viewer**: Has access to:
    - Watch and take snapshots of a video stream.
    - Watch and export recordings.
    - With PTZ user access: pan, tilt, and zoom.

⋮ The context menu contains:

Update user: Edit the user's properties.

Delete user: Delete the user. You can't delete the root user.

Anonymous users

Allow anonymous viewers: Turn on to allow anyone to access the device as a viewer without having to log in with a user account.

Allow anonymous PTZ operators: Turn on to allow anonymous users to pan, tilt, and zoom the image.

Events

Rules

A rule defines the conditions that must be met for the product to perform an action. The list shows all the currently configured rules in the product.

> Note
>
> You can create up to 256 action rules.

✚ **Add a rule**: Click to create a rule.

Name: Enter a name for the rule.

Wait between actions: Enter the minimum time (hh:mm:ss) that must pass between rule activations. It is useful if the rule is activated by for example day-night mode conditions, to avoid that small light changes during sunrise and sunset activate the rule repeatedly.

Condition: Select a condition from the list. A condition must be met for the device to perform an action. If multiple conditions are defined, all of them must be met to trigger the action. For information about specific conditions, see *Get started with rules for events*.

Use this condition as a trigger: Select to make this first condition function only as a starting trigger. It means that once the rule is activated it remains active for as long as all the other conditions are met, no matter the state of the first condition. If you don't select this option, the rule will simply be active whenever all the conditions are met.

Invert this condition: Select if you want the condition to be the opposite of your selection.

✚ **Add a condition**: Click to add an additional condition.

Action: Select an action from the list and enter its required information. For information about specific actions, see *Get started with rules for events*.

Your product may have some of the following pre-configured rules:

Front-facing LED Activation: LiveStream: When the microphone is turned on and a live stream is received, then the front-facing LED on the audio device will turn green.

Front-facing LED Activation: Recording : When the microphone is turned on and a recording is ongoing, then the front-facing LED on the audio device will turn green.

Front-facing LED Activation: SIP : When the microphone is turned on and a SIP call is active, then the front-facing LED on the audio device will turn green. SIP must be enabled on the audio device before this event can be triggered.

Pre-announcement tone: Play tone on incoming call: When a SIP call is made to the audio device, then a pre-defined audio clip is played. SIP must be enabled for the audio device. For the SIP caller to hear a ring tone while the audio clip is played, the SIP account for the audio device must be configured to not answer the call automatically.

Pre-announcement tone: Answer call after incoming call-tone: When the audio clip has ended, the incoming SIP-call is answered. SIP must be enabled for the audio device.

Loud ringer : When a SIP call is made to the audio device, a pre-defined audio clip is played as long as the rule is active. SIP must be enabled for the audio device.

Recipients

You can set up your device to notify recipients about events or send files. The list shows all the recipients currently configured in the product, along with information about their configuration.

Note

    You can create up to 20 recipients.

➕ **Add a recipient**: Click to add a recipient.

Name: Enter a name for the recipient.

Type: Select from the list:

- FTP
    - **Host**: Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
    - **Port**: Enter the port number used by the FTP server. The default is 21.
    - **Folder**: Enter the path to the directory where you want to store files. If this directory doesn't already exist on the FTP server, you will get an error message when uploading files.
    - **Username**: Enter the username for the login.
    - **Password**: Enter the password for the login.
    - **Use temporary file name**: Select to upload files with temporary, automatically generated filenames. The files get renamed to the desired names when the upload completes. If the upload is aborted/interrupted, you don't get any corrupt files. However, you probably still get the temporary files. This way you know that all files that have the desired name, are correct.
    - **Use passive FTP**: Under normal circumstances the product simply requests the target FTP server to open the data connection. The device actively initiates both the FTP control and data connections to the target server. This is normally needed if there is a firewall between the device and the target FTP server.
- HTTP
    - **URL**: Enter the network address to the HTTP server and the script that will handle the request. For example: http://192.168.254.10/cgi-bin/notify.cgi.
    - **Username**: Enter the username for the login.
    - **Password**: Enter the password for the login.
    - **Proxy**: Turn on and enter the required information if a proxy server must be passed to connect to the HTTP server.
- HTTPS
    - **URL**: Enter the network address to the HTTPS server and the script that will handle the request. For example: https://192.168.254.10/cgi-bin/notify.cgi.

- **Validate server certificate**: Select to validate the certificate that was created by HTTPS server.
- **Username**: Enter the username for the login.
- **Password**: Enter the password for the login.
- **Proxy**: Turn on and enter the required information if a proxy server must be passed to connect to the HTTPS server.

- **Network storage**
  You can add network storage such as a NAS (Network Attached Storage) and use it as a recipient to store files.
  The files are stored in the Matroska (MKV) file format.
    - **Host**: Enter the IP address or hostname for the network storage.
    - **Share**: Enter the name of the share on the host.
    - **Folder**: Enter the path to the directory where you want to store files.
    - **Username**: Enter the username for the login.
    - **Password**: Enter the password for the login.

- **SFTP**
    - **Host**: Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
    - **Port**: Enter the port number used by the SFTP server. The default is 22.
    - **Folder**: Enter the path to the directory where you want to store files. If this directory doesn't already exist on the SFTP server, you will get an error message when uploading files.
    - **Username**: Enter the username for the login.
    - **Password**: Enter the password for the login.
    - **SSH host public key type (MD5)**: Enter the fingerprint of the remote host's public key (a 32-digit hexadecimal string). The SFTP client supports SFTP servers using SSH-2 with RSA, DSA, ECDSA, and ED25519 host key types. RSA is the preferred method during negotiation, followed by ECDSA, ED25519, and DSA. Make sure to enter the right MD5 host key that is used by your SFTP server. While the Axis device supports both MD5 and SHA-256 hash keys, we recommend using SHA-256 due to stronger security over MD5. For more information on how to configure an SFTP server with an Axis device, go to the *AXIS OS Portal*.
    - **SSH host public key type (SHA256)**: Enter the fingerprint of the remote host's public key (a 43-digit Base64 encoded string). The SFTP client supports SFTP servers using SSH-2 with RSA, DSA, ECDSA, and ED25519 host key types. RSA is the preferred method during negotiation, followed by ECDSA, ED25519, and DSA. Make sure to enter the right MD5 host key that is used by your SFTP server. While the Axis device supports both MD5 and SHA-256 hash keys, we recommend using SHA-256 due to stronger security over MD5. For more information on how to configure an SFTP server with an Axis device, go to the *AXIS OS Portal*.
    - **Use temporary file name**: Select to upload files with temporary, automatically generated filenames. The files get renamed to the desired names when the upload completes. If the upload is aborted/interrupted, you don't get any corrupt files. However, you probably still get the temporary files. This way you know that all files that have the desired name, are correct.

- **SIP or VMS** ⓘ :
  SIP: Select to make a SIP call.
  VMS: Select to make a VMS call.
    - **From SIP account**: Select from the list.
    - **To SIP address**: Enter the SIP address.
    - **Test**: Click to test that your call settings works.

- **Email**
    - **Send email to**: Enter the email address to send emails to. To enter multiple addresses, use commas to separate them.
    - **Send email from**: Enter the email address of the sending server.
    - **Username**: Enter the username for the mail server. Leave this field empty if the mail server does not require authentication.
    - **Password**: Enter the password for the mail server. Leave this field empty if the mail server does not require authentication.
    - **Email server (SMTP)**: Enter the name of the SMTP server, for example smtp.gmail.com, smtp.mail.yahoo.com.
    - **Port**: Enter the port number for the SMTP server, using values in the range 0-65535. The default value is 587.
    - **Encryption**: To use encryption, select either SSL or TLS.
    - **Validate server certificate**: If you use encryption, select to validate the identity of the device. The certificate can be self-signed or issued by a Certificate Authority (CA).
    - **POP authentication**: Turn on to enter the name of the POP server, for example pop.gmail.com.

> Note
>
> Some email providers have security filters that prevent users from receiving or viewing large amount of attachments, from receiving scheduled emails and similar. Check the email provider's security policy to avoid your email account being locked or missing out on your expected emails.

- **TCP**
  - **Host**: Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
  - **Port**: Enter the port number used to access the server.

Test: Click to test the setup.

⋮ The context menu contains:

View recipient: Click to view all the recipient details.

Copy recipient: Click to copy a recipient. When you copy, you can make changes to the new recipient.

Delete recipient: Click to delete the recipient permanently.

Schedules

Schedules and pulses can be used as conditions in rules. The list shows all the schedules and pulses currently configured in the product, along with information about their configuration.

✚ **Add schedule**: Click to create a schedule or pulse.

Manual triggers

The manual trigger is used to manually trigger a rule. The manual trigger can for example be used to validate actions during product installation and configuration.

MQTT

MQTT (Message Queuing Telemetry Transport) is a standard messaging protocol for the Internet of Things (IoT). It was designed for simplified IoT integration and is used in a wide variety of industries to connect remote devices with a small code footprint and minimal network bandwidth. The MQTT client in Axis device firmware can simplify integration of data and events produced in the device to systems which are not video management systems (VMS).

Set up the device as an MQTT client. MQTT communication is based on two entities, the clients and the broker. The clients can send and receive messages. The broker is responsible for routing messages between clients.

You can learn more about MQTT in *AXIS OS Portal*.

ALPN

ALPN is a TLS/SSL extension that allows for the selection of an application protocol during the handshake phase of the connection between the client and server. This is used to enable MQTT traffic over the same port that is used for other protocols, such as HTTP. In some cases, there might not be a dedicated port open for MQTT communication. A solution in such cases is to use ALPN to negotiate the use of MQTT as the application protocol on a standard port, allowed by the firewalls.

MQTT client

Connect: Turn on or off the MQTT client.

Status: Shows the current status of the MQTT client.

Broker

Host: Enter the hostname or IP address of the MQTT server.

Protocol: Select which protocol to use.

Port: Enter the port number.

- 1883 is the default value for **MQTT over TCP**
- 8883 is the default value for **MQTT over SSL**
- 80 is the default value for **MQTT over WebSocket**
- 443 is the default value for **MQTT over WebSocket Secure**

ALPN protocol: Enter the ALPN protocol name provided by your MQTT broker provider. This is only applicable with MQTT over SSL and MQTT over WebSocket Secure.

Username: Enter the username that the client will use to access the server.

Password: Enter a password for the username.

Client ID: Enter a client ID. The client identifier is sent to the server when the client connects to it.

Clean session: Controls the behavior at connection and disconnection time. When selected, the state information is discarded at connect and disconnect.

Keep alive interval: The keep alive interval enables the client to detect when the server is no longer available without having to wait for the long TCP/IP timeout.

Timeout: The time interval in seconds to allow a connect to complete. Default value: 60

Device topic prefix: Used in the default values for the topic in the connect message and LWT message on the **MQTT client** tab, and in the publication conditions on the **MQTT publication** tab.

Reconnect automatically: Specifies whether the client should reconnect automatically after a disconnect.

Connect message

Specifies if a message should be sent out when a connection is established.

Send message: Turn on to send messages.

Use default: Turn off to enter your own default message.

Topic: Enter the topic for the default message.

Payload: Enter the content for the default message.

Retain: Select to keep the state of client on this **Topic**

QoS: Change the QoS layer for the packet flow.

Last Will and Testament message

The Last Will Testament (LWT) lets a client provide a testament along with its credentials when connecting to the broker. If the client disconnects ungracefully at some point later (maybe because his power source died), it can let the broker deliver a message to other clients. This LWT message has the same form as an ordinary message and gets routed via the same mechanics.

Send message: Turn on to send messages.

Use default: Turn off to enter your own default message.

Topic: Enter the topic for the default message.

Payload: Enter the content for the default message.

Retain: Select to keep the state of client on this **Topic**

QoS: Change the QoS layer for the packet flow.

MQTT publication

Use default topic prefix: Select to use the default topic prefix, that is defined in the device topic prefix in the **MQTT client** tab.

Include topic name: Select to include the topic that describes the condition in the MQTT topic.

Include topic namespaces: Select to include ONVIF topic namespaces in the MQTT topic.

Include serial number: Select to include the device's serial number in the MQTT payload.

✛ **Add condition**: Click to add a condition.

Retain: Defines which MQTT messages are sent as retained.

- **None**: Send all messages as non-retained.
- **Property**: Send only stateful messages as retained.
- **All**: Send both stateful and stateless messages as retained.

QoS: Select the desired level for the MQTT publication.

MQTT subscriptions

✛ **Add subscription**: Click to add a new MQTT subscription.

Subscription filter: Enter the MQTT topic that you want to subscribe to.

Use device topic prefix: Add the subscription filter as prefix to the MQTT topic.

Subscription type:

- **Stateless**: Select to convert MQTT messages into a stateless message.
- **Stateful**: Select to convert MQTT messages into a condition. The payload is used as the state.

QoS: Select the desired level for the MQTT subscription.

MQTT overlays

Note

Connect to an MQTT broker before you add MQTT overlay modifiers.

✛ **Add overlay modifier**: Click to add a new overlay modifier.

Topic filter: Add the MQTT topic that contains the data you want to show in the overlay.

Data field: Specify the key for the message payload that you want to show in the overlay, assuming the message is in JSON format.

Modifier: Use the resulting modifier when you create the overlay.

- Modifiers that start with **#XMP** show all of the data received from the topic.
- Modifiers that start with **#XMD** show the data specified in the data field.

Storage

Network storage

Ignore: Turn on to ignore network storage.

Add network storage: Click to add a network share where you can save recordings.

- **Address**: Enter the IP address or host name of the host server, typically a NAS (Network Attached Storage). We recommend you to configure the host to use a fixed IP address (not DHCP since a dynamic IP address can change) or that you use DNS. Windows SMB/CIFS names are not supported.
- **Network share**: Enter the name of the shared location on the host server. Several Axis devices can use the same network share, since each device gets its own folder.
- **User**: If the server requires a login, enter the username. To log in to a specific domain server, type DOMAIN\username.
- **Password**: If the server requires a login, enter the password.
- **SMB version**: Select the SMB storage protocol version to connect to the NAS. If you select **Auto**, the device tries to negotiate one of the secure versions SMB: 3.02, 3.0, or 2.1. Select 1.0 or 2.0 to connect to older NAS that don't support higher versions. You can read more about SMB support in Axis devices *here*.
- **Add share even if connection test fails**: Select to add the network share even if an error is discovered during the connection test. The error can be, for example, that you didn't enter a password even though the server requires one.

Remove network storage: Click to unmount, unbind and remove the connection to the network share. This removes all settings for the network share.

Unbind: Click to unbind and disconnect the network share.
Bind: Click to bind and connect the network share.

Unmount: Click to unmount the network share.
Mount: Click to mount the network share.

Write protect: Turn on to stop writing to the network share and protect recordings from being removed. You can't format a write-protected network share.

Retention time: Select how long to keep recordings, to limit the amount of old recordings or to comply with regulations regarding data storage. If the network storage becomes full, old recordings are removed before the selected time period has passed.

Tools

- **Test connection**: Test the connection to the network share.
- **Format**: Format the network share, for example when you need to quickly erase all data. CIFS is the available file system option.

Click **Use tool** to activate the selected tool.

Onboard storage

Important

Risk of data loss and corrupted recordings. Do not remove the SD card while the device is running. Unmount the SD card before you remove it.

Unmount: Click to safely remove the SD card.

Write protect: Turn on to stop writing to the SD card and protect recordings from being removed. You can't format a write-protected SD card.

Autoformat: Turn on to automatically format a newly inserted SD card. It formats the file system into ext4.

Ignore: Turn on to stop storing recordings on the SD card. When you ignore the SD card, the device no longer recognizes that the card exists. The setting is only available for administrators.

Retention time: Select how long to keep recordings, to limit the amount of old recordings or to comply with regulations regarding data storage. If the SD card becomes full, old recordings are removed before the selected time period has passed.

Tools

- **Check**: Check for errors on the SD card. This only works for the ext4 file system.
- **Repair**: Repair errors in the ext4 file system. To repair an SD card with the VFAT file system, eject the SD card, insert it in a computer and perform a disk repair.
- **Format**: Format the SD card, for example when you need to change the file system or quickly erase all data. VFAT and ext4 are the two available file system options. The recommended format is ext4, due to its resilience against data loss if the card is ejected or if there is an abrupt power loss. However, you need a third-party ext4 driver or application to access the file system from Windows®.
- **Encrypt**: Use this tool to format the SD card and enable encryption. **Encrypt** deletes all data stored on the SD card. After using **Encrypt** data that's stored on the SD card is protected using encryption.
- **Decrypt**: Use this tool to format the SD card without encryption. **Decrypt** deletes all data stored on the SD card. After using **Decrypt** data that's stored on the SD card is not protected using encryption.
- **Change password**: Change the password required to encrypt the SD card.

Click **Use tool** to activate the selected tool.

Wear trigger: Set a value for the SD card wear level at which you want to trigger an action. The wear level ranges from 0–200%. A new SD card that has never been used has a wear level of 0%. A wear level of 100% indicates that the SD card is close to its expected lifetime. When the wear-level reaches 200% there is a high risk of the SD card malfunctioning. We recommend setting the wear trigger between 80–90%. This gives you time to download any recordings as well as replace the SD card in time before it potentially wears out. The wear trigger allows you to set up an event and get a notification when the wear level reaches your set value.

Stream profiles

A stream profile is a group of settings that affect the video stream. You can use stream profiles in different situations, for example when you create events and use rules to record.

Click ➕ to create a new stream profile.

Preview: A preview of the video stream with the stream profile settings you select. The preview updates when you change the settings on the page. If your device has different view areas, you can change the view area in the drop-down in the bottom left corner of the image.

Name: Add a name for your profile.

Description: Add a description of your profile.

Video codec: Select the video codec that should apply for the profile.

Resolution: See *Stream on page 26* for a description of this setting.

Frame rate: See *Stream on page 26* for a description of this setting.

Compression: See *Stream on page 26* for a description of this setting.

Zipstream ⓘ : See *Stream on page 26* for a description of this setting.

Optimize for storage ⓘ : See *Stream on page 26* for a description of this setting.

Dynamic FPS ⓘ : See *Stream on page 26* for a description of this setting.

Dynamic GOP ⓘ : See *Stream on page 26* for a description of this setting.

Mirror ⓘ : See *Stream on page 26* for a description of this setting.

GOP length ⓘ : See *Stream on page 26* for a description of this setting.

Bitrate control: See *Stream on page 26* for a description of this setting.

Include overlays: Select what type of overlays to include. See *Overlays on page 27* for information about how to add overlays.

Include audio ⓘ : See *Stream on page 26* for a description of this setting.

ONVIF

ONVIF users

ONVIF (Open Network Video Interface Forum) is a global interface standard that makes it easier for end-users, integrators, consultants, and manufacturers to take advantage of the possibilities offered by network video technology. ONVIF enables interoperability between different vendor products, increased flexibility, reduced cost and future-proof systems.

When you create an ONVIF user, you automatically enable ONVIF communication. Use the username and password for all ONVIF communication with the device. For more information see the Axis Developer Community at *axis.com*.

✚ **Add user**: Click to add a new ONVIF user.

Username: Enter a unique username.

New password: Enter a password for the user. Passwords must be 1 to 64 characters long. Only ASCII printable characters (code 32 to 126) are allowed in the password, for example letters, numbers, punctuation, and some symbols.

Repeat password: Enter the same password again

Role:

- **Administrator**: Has full access to all settings. Administrators can also add, update, and remove other users.
- **Operator**: Has access to all settings except:
    - All **System** settings.
    - Adding apps.
- **Media user**: Allows access to the video stream only.

⋮ The context menu contains:

Update user: Edit the user's properties.

Delete user: Delete the user. You can't delete the root user.

ONVIF media profiles

An ONVIF media profile consists of a set of configurations that you can use to change media stream settings.

✚ **Add media profile**: Click to add a new ONVIF media profile.

profile_x: Click a profile to edit.

Analytics metadata

Metadata producers

Metadata producers lists the channels used by apps and the metadata they are streaming from the device.

Producer: The app producing the metadata.

Channel: The channel used by the app. Check to enable the metadata stream. Uncheck to disable the stream for compatibility or resources management reasons.

Detectors

Camera tampering

The camera tampering detector generates an alarm when the scene changes, for example because the lens is covered, sprayed or severely put out of focus, and the time in **Trigger delay** has passed. The tampering detector only activates when the camera has not moved for at least 10 seconds. During this period the detector sets up a scene model to use as a comparison to detect tampering in current images. For the scene model to be set up properly, make sure that the camera is in focus, the lighting conditions are correct, and the camera doesn't point at a scene that lacks contours, for example a blank wall. Camera tampering can be used as a condition to trigger actions.

Trigger delay: Enter the minimum time that the tampering conditions must be active before the alarm triggers. This can help prevent false alarms for known conditions that affect the image.

Trigger on dark images: It is very difficult to generate alarms when the camera lens is sprayed, since it is impossible to distinguish that event from other situations where the image turns dark in a similar way, for example when the lighting conditions change. Turn on this parameter to generate alarms for all cases where the image turns dark. When it's turned off, the device doesn't generate any alarm when the image turns dark.

Note

For detection of tampering attempts in static and non-crowded scenes.

Audio detection

These settings are available for each audio input.

Sound level: Adjust the sound level to a value from 0–100, where 0 is the most sensitive and 100 the least sensitive. Use the activity indicator as a guide when you set the sound level. When you create events, you can use the sound level as a condition. You can choose to trigger an action if the sound level rises above, falls below or passes the set value.

Shock detection

Shock detector: Turn on to generate an alarm if the device is hit by an object or if it is tampered with.

Sensitivity level: Move the slider to adjust the sensitivity level at which the device should generate an alarm. A low value means that the device only generates an alarm if the hit is powerful. A high value means that the device generates an alarm even with mild tampering.

Accessories

PTZ

Select PTZ mode: Select a PTZ mode that suits your type of installation. See available modes below.

- **Digital**: Select this mode to use digital PTZ and view areas.
- **Mechanical**: Select this mode to connect to an external pan-tilt device.
  - **Driver**: Select the driver for your connected pan-tilt device. The driver is required for the connected device to function correctly.
  - **Device type**: Select the type of device you're connecting to from the drop-down list. The device type is driver dependent.
  - **Device id**: Type the id, or address, of the connected device. You can find the address in the documentation of the device.

For more information about PTZ drivers, see *PTZ drivers on page 66.*

I/O ports

Use digital input to connect external devices that can toggle between an open and closed circuit, for example PIR sensors, door or window contacts, and glass break detectors.

Use digital output to connect external devices such as relays and LEDs. You can activate connected devices through the VAPIX® Application Programming Interface or in the device interface.

Port

Name: Edit the text to rename the port.

Direction: ⟴ indicates that the port is an input port. ⟵ indicates that it's an output port. If the port is configurable, you can click the icons to change between input and output.

Normal state: Click ⟋• open circuit, and •—• for closed circuit.

Current state: Shows the current state of the port. The input or output is activated when the current state is different from the normal state. An input on the device has an open circuit when it's disconnected or when there is a voltage above 1 V DC.

Note

> During restart the output circuit is open. When the restart is complete, the circuit goes back to the normal position. If you change any settings on this page, the output circuits go back to their normal positions regardless of any active triggers.

Supervised ⓘ : Turn on to make it possible to detect and trigger actions if someone tampers with the connection to digital I/O devices. In addition to detecting if an input is open or closed, you can also detect if someone has tampered with it (that is, cut or shorted). To supervise the connection requires additional hardware (end-of-line resistors) in the external I/O loop.

Edge-to-edge

Pairing

Pairing allows you to use a compatible Axis network speaker or microphone as if it's part of the camera. Once paired, the network speaker acts as an audio out device where you can play audio clips and transmit sound through the camera. The network microphone will take up sounds from the surrounding area and make it available as an audio input device, usable in media streams and recordings.

Important

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

Address: Enter host name or IP address to the network speaker.

Username: Enter username.

Password: Enter password for the user.

Speaker pairing: Select to pair a network speaker.

Microphone pairing: Select to pair a microphone.

Clear fields: Click to clear all fields.

Connect: Click to establish connection to the speaker or microphone.

Logs

Reports and logs

Reports

- **View the device server report**: Click to show information about the product status in a pop-up window. The Access Log is automatically included in the Server Report.
- **Download the device server report**: Click to download the server report. It creates a .zip file that contains a complete server report text file in UTF–8 format, as well as a snapshot of the current live view image. Always include the server report .zip file when you contact support.
- **Download the crash report**: Click to download an archive with detailed information about the server's status. The crash report contains information that is in the server report as well as detailed debug information. This report might contain sensitive information such as network traces. It can take several minutes to generate the report.

Logs

- **View the system log**: Click to show information about system events such as device startup, warnings and critical messages.
- **View the access log**: Click to show all failed attempts to access the device, for example when a wrong login password is used.

Network trace

Important

A network trace file might contain sensitive information, for example certificates or passwords.

A network trace file can help you troubleshoot problems by recording activity on the network.

Trace time: Select the duration of the trace in seconds or minutes, and click **Download**.

Remote system log

Syslog is a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, which indicates the software type generating the message, and assigned a severity level.

✚   **Server**: Click to add a new server.

Host: Enter the hostname or IP address of the server.

Format: Select which syslog message format to use.

- RFC 3164
- RFC 5424

Protocol: Select the protocol and port to use:

- UDP (Default port is 514)

- TCP (Default port is 601)
- TLS (Default port is 6514)

Severity: Select which messages to send when triggered.

CA certificate set: See the current settings or add a certificate.

Plain config

Plain config is for advanced users with experience of Axis device configuration. Most parameters can be set and edited from this page.

Maintenance

Restart: Restart the device. This does not affect any of the current settings. Running applications restart automatically.

Restore: Return *most* settings to the factory default values. Afterwards you must reconfigure the device and apps, reinstall any apps that didn't come preinstalled, and recreate any events and PTZ presets.

Important

> The only settings saved after restore are:
>
> - Boot protocol (DHCP or static)
>
> - Static IP address
>
> - Default router
>
> - Subnet mask
>
> - 802.1X settings
>
> - O3C settings

Factory default: Return *all* settings to the factory default values. Afterwards you must reset the IP address to make the device accessible.

Note

> All Axis device firmware is digitally signed to ensure that you only install verified firmware on your device. This further increases the overall minimum cybersecurity level of Axis devices. For more information, see the white paper "Signed firmware, secure boot, and security of private keys" at *axis.com*.

Firmware upgrade: Upgrade to a new firmware version. New firmware releases can contain improved functionality, bug fixes, and completely new features. We recommend you to always use the latest release. To download the latest release, go to *axis.com/support*.

When you upgrade, you can choose between three options:

- **Standard upgrade**: Upgrade to the new firmware version.
- **Factory default**: Upgrade and return all settings to the factory default values. When you choose this option, you can't revert to the previous firmware version after the upgrade.
- **Autorollback**: Upgrade and confirm the upgrade within the set time. If you don't confirm, the device reverts to the previous firmware version.

Firmware rollback: Revert to the previously installed firmware version.

Learn more

View area

A view area is a cropped part of the full view. You can stream and store view areas instead of the full view to minimize bandwidth and storage needs. If you enable PTZ for a view area, you can pan, tilt and zoom within it. By using view areas you can remove parts of the full view, for example, the sky.

When you set up a view area, we recommend you to set the video stream resolution to the same size as or smaller than the view area size. If you set the video stream resolution larger than the view area size it implies digitally scaled up video after sensor capture, which requires more bandwidth without adding image information.

Capture modes

A capture mode is a preset configuration that defines how the camera captures images. The selected mode can affect the maximum resolution and maximum frame rate available in the device. If you use a capture mode with a lower resolution than the maximum, the field of view might be reduced. The capture mode also affects the shutter speed, which in turn affects the light sensitivity – a capture mode with a high maximum frame rate has a reduced light sensitivity, and vice versa. Note that with certain capture modes you might not be able to use WDR.

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*.

Remote focus and zoom

The remote focus and zoom functionality allows you to make focus and zoom adjustments to your camera from a computer. It is a convenient way to ensure that the scene's focus, viewing angle and resolution are optimized without having to visit the camera's installation location.

Privacy masks

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

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

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

Important

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

You can create several privacy masks. The maximum number of masks depends on the complexity of all the masks combined. The more anchor points in each mask, the fewer masks you can create. Each mask can have 3 to 10 anchor points.

Important

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

Overlays

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

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

Streaming and storage

Video compression formats

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

Motion JPEG

Note

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

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

H.264 or MPEG-4 Part 10/AVC

Note

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

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

H.265 or MPEG-H Part 2/HEVC

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

Note

- H.265 is licensed technology. The Axis product includes one H.265 viewing client license. Installing additional unlicensed copies of the client is prohibited. To purchase additional licenses, contact your Axis reseller.

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

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

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

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

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

Bitrate control

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

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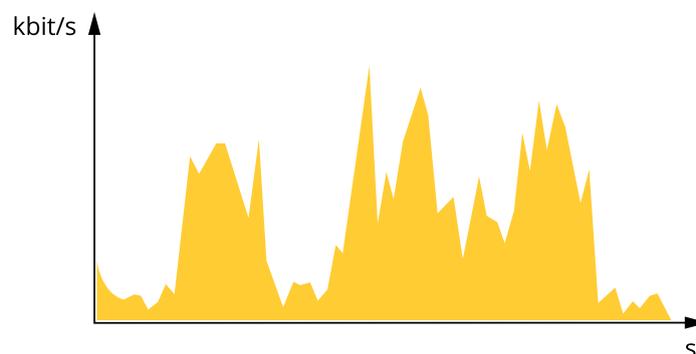

Maximum bitrate (MBR)
Maximum bitrate lets you set a target bitrate to handle bitrate limitations in your system. You might see a decline in image quality or frame rate as the instantaneous bitrate is kept below the specified target bitrate. You can choose to prioritize either image quality

or frame rate. We recommend that you configure the target bitrate to a higher value than the expected bitrate. This gives you a margin in case there is a high level of activity in the scene.
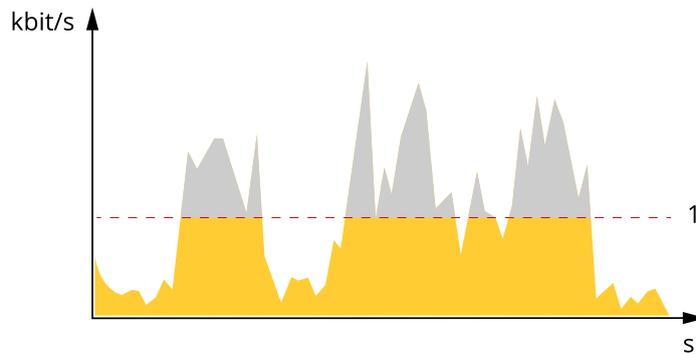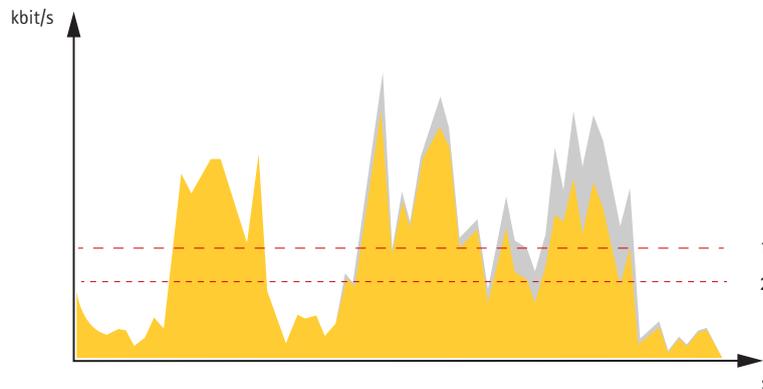

    1   Target bitrate

Average bitrate (ABR)

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

- To calculate the estimated storage need, set the target bitrate and the retention time.

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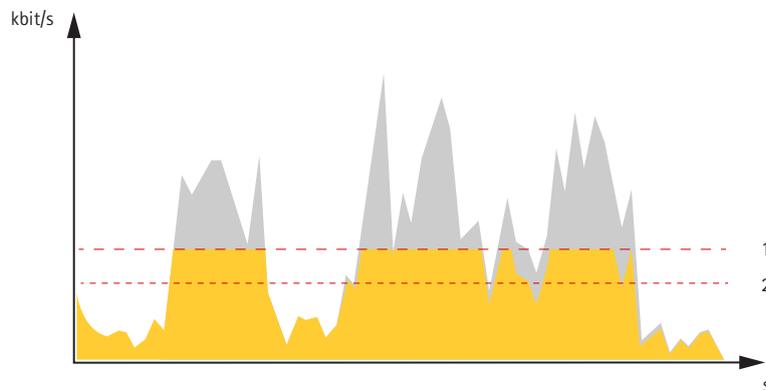

    1   Target bitrate
    2   Actual average bitrate

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

Learn more

1   Target bitrate
2   Actual average bitrate

Applications

With applications 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 applications for Axis devices. Applications can be preinstalled on the device, available for download for free, or for a license fee.

To find the user manuals for Axis applications, go to *help.axis.com*.

Note

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

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*.

PPE monitoring[BETA]

One feature within the AXIS Object Analytics application is PPE monitoring[BETA]. This feature can be used to enhance safety in hazardous environments where a hard hat is required to keep safe. You can set up the feature to trigger an alarm when a person without a hard hat is detected. Standard hard hats are recognized as approved headgear. Hard hats with other shapes, for example climbing helmets, are more difficult to detect and can trigger false alarms. As this is a beta feature, the detection behavior for other types of headgear is uncertain.

Learn more

Object size and movement

Only moving objects are detected and can trigger alarms. The objects must also be large enough to be detected. Objects that are too small don't trigger any alarms, or they can trigger false alarms. Go to your scenario and click **Visualize**. Use this feature to make sure that objects in the scene are large enough to be detected.

Objects are too small to be detected

A person without a hard hat is detected

Smoke alert

Important

        The smoke alert feature does not replace a certified fire detection solution. It's not allowed to link smoke alert to a fire alarm center.

Smoke alert is a video analytics feature for smoke and flame detection. It enables the camera to detect and locate fire incidents through continuous real time analysis of the video stream. Upon detection, smoke alert can push live video to security staff, activate speakers, start a video recording, or respond in whatever way the user has set up.

To minimize the risk for false alarms, there are a few things to consider:

- Make sure there are sufficient contrasts in the scene. Avoid white walls or large areas without contrast.

- Avoid a combination of extreme dark spots and extreme bright spots in the scene.

- Avoid direct sunlight or bright reflections of the sun falling straight into the lens.

- Smoke detection require some light in the scene. Flame detection works good in complete dark environment.

Turn on smoke alert

1. Go to **Apps**.

2. Go to **Smoke alert** and turn on smoke alert. You may need to wait for a few minutes for smoke alert to calibrate.

Set up smoke and flame detection

1. Go to **Apps** > **Smoke alert** and click **Open**.

2. Go to **Settings**.

3. Go to **Smoke alarm** or **Flame alarm** and turn on one or both alarms.

4. Set the smoke and flame sensitivity to match your environment. The sensitivity level determines how easily an alarm is triggered. The higher the value, the more sensitive the detection becomes.

5. To avoid false alarms due to short disturbances in the scene, set the alarm delay to match your environment. An alarm will be triggered after it has been identified for the specified amount of time.

6. Click **Save**.

Add an overlay to show smoke alert status

You can add a text overlay that shows the smoke alert status in the video stream.

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

2. Select **Text** and click ╋ .

3. In the text field, type #D1 to show the smoke alert status.
   Type %F %X to show the date and time.

4. Select a position for your overlay. You can also drag the overlay text field in the live view to change the position.

Add an overlay to indicate where the smoke or flames are

You can add an overlay to the video stream to indicate where the smoke or flames are. The overlay is shown as a bounding box that dynamically changes as the incident zone grows or shrinks.

1. Go to **Apps** > **Smoke alert** and click **Open**.

2. Go to **Settings**.

3. Go to **General** and turn on **Overlay**.

4. Click **Save**.

Set up a detection zone

To limit the detection to certain zones, you can set up one or more detection zones.

> Note
>
> To set up a detection zone, the camera must be in a preset position.

1. Click ⋮ and select **Legacy device interface**.

2. Go to **PTZ > Preset positions**.

3. Click ➕ to create a preset position.

4. Go to **Apps > Smoke alert** and click **Open**.

5. Go to **DetectionZone**.

6. Draw a polygon detection zone with a minimum of three points. Left-click to add a point. Right-click to close the polygon. You can add one or more detection zones.

7. Click **Save**.

Security

Signed firmware

Signed firmware is implemented by the software vendor signing the firmware image with a private key. When a firmware has this signature attached to it, a device will validate the firmware before accepting to install it. If the device detects that the firmware integrity is compromised, the firmware 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 firmware, secure boot ensures that a device can boot only with authorized firmware.

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.

TPM module

The TPM (Trusted Platform Module) is a component that provides cryptographic features to protect information from unauthorized access. It is always activated and there are no settings you can change.

Axis device ID

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

Signed video

Signed video ensures that video evidence can be verified as untampered without proving the chain of custody of the video file. Each camera uses its unique video signing key, which is securely stored in the secure keystore, to add a signature into the video stream. When the video is played, the file player shows whether the video is intact. Signed video makes it possible to trace the video back to the camera origin and verifies that the video has not been tampered with after it left the camera.
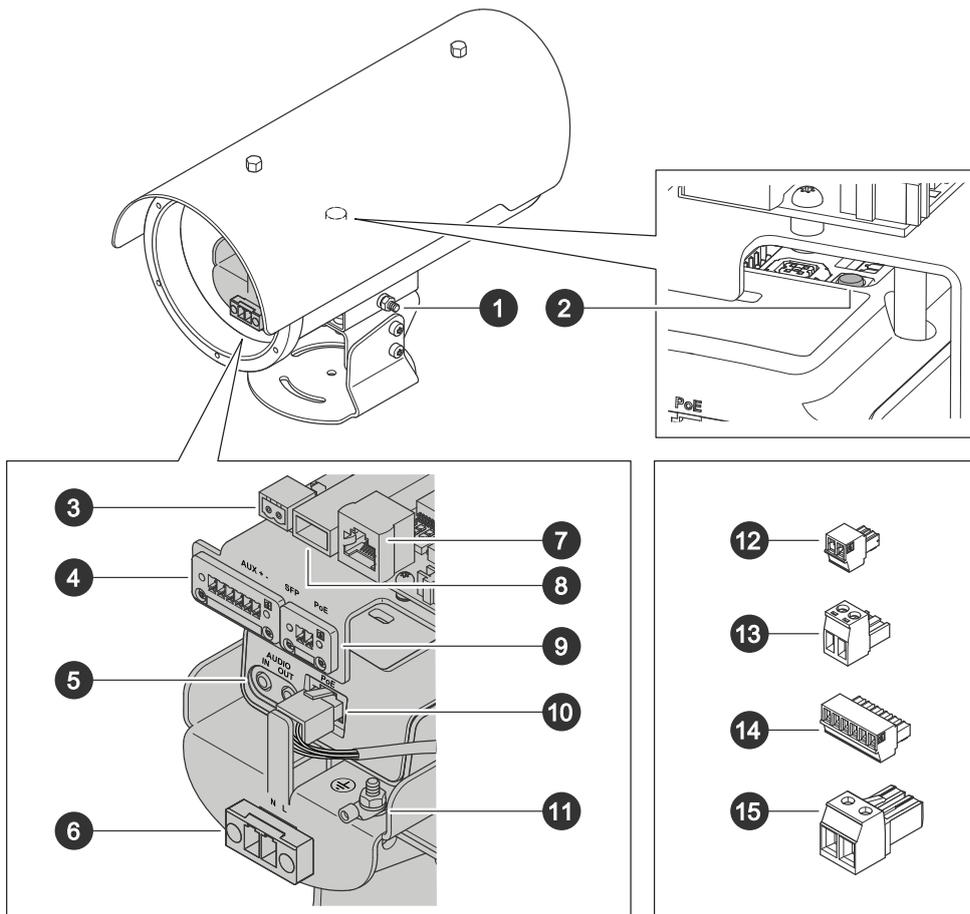
To learn more about Axis Edge Vault and cybersecurity features in Axis devices, go to *axis.com/learning/white-papers* and search for cybersecurity.

Specifications

Specifications

Product overview

1   Earth supplemental bonding
2   Control button
3   Auxiliary OUT connector
4   I/O connector
5   Audio connectors
6   AC mains IN connector
7   Network connector RJ45 (PoE)
8   SFP connector
9   RS485 BA connector
10   Internal wiring — Don't modify!
11   Earth stud
12   RS485 terminal
       Pin1: A
       Pin 2: B
13   Auxiliary OUT terminal
       Pin +: Auxiliary OUT +48 V DC 14.4 W max
       Pin –: Auxiliary OUT 0 V DC

Specifications

14 I/O terminal
Pin 1: DC ground, 0 V DC
Pin 2: DC output. 12 V. max load 50 mA
Pin 3–4: Digital input or supervised input, 0 to max 30 V DC
Pin 5–6: Digital output, 0 to max 30 V DC, open drain, 100 mA

15 AC mains IN terminal
Pin N: Supply neutral
Pin L: Supply live

LED indicators

Note

The Status LED can be configured to flash while an event is active.

Status LED	Indication
Unlit	Connection and normal operation.
Green	Shows steady green for 10 seconds for normal operation after startup completed.
Amber	Steady during startup. Flashes during firmware upgrade or reset to factory default.
Amber/Red	Flashes amber/red if network connection is unavailable or lost.
Red	Firmware upgrade failure.

SD card slot

NOTICE

- Risk of damage to SD card. Don't use sharp tools, metal objects, or excessive force when inserting or removing the SD card. Use your fingers to insert and remove the card.

- Risk of data loss and corrupted recordings. Unmount the SD card from the device's web interface before removing it. Don't remove the SD card while the product is running.

This device supports microSD/microSDHC/microSDXC cards.

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

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

Buttons

Control button

The control button is used for:

- Resetting the product to factory default settings. See *Reset to factory default settings on page 71*.

- Connecting to a one-click cloud connection (O3C) service over the internet. To connect, press and hold the button for about 3 seconds until the status LED flashes green.

Specifications

Connectors

Network connector

RJ45 Ethernet connector with Power over Ethernet (PoE).

USB connector

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

Audio connector

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

- **Audio 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 input

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

Audio output

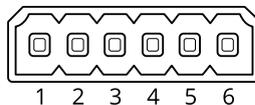| 1 Tip	2 Ring	3 Sleeve
Channel 1, unbalanced line, mono	Channel 1, unbalanced line, mono	Ground

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 V DC 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.

6-pin terminal block

AXIS XFQ1656

Specifications

| Function	Pin	Notes	Specifications
DC ground	1		0 V DC
DC output	2	Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	12 V DC 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 V DC
		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 V DC, open drain, 100 mA

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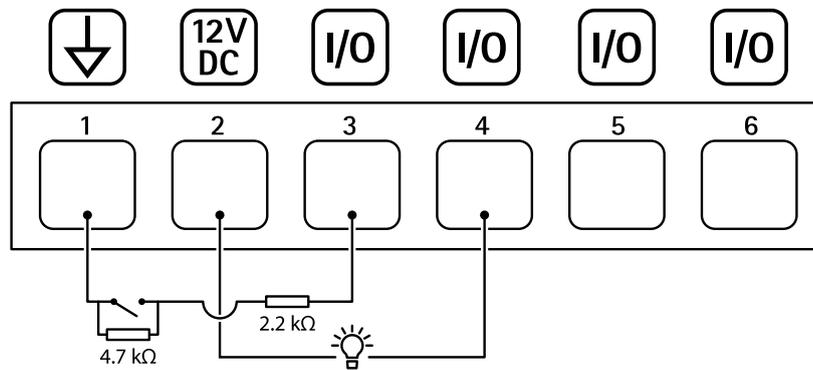
1   DC ground
2   DC output 12 V, max 50 mA
3   I/O configured as supervised input
4   I/O configured as output
5   Configurable I/O
6   Configurable I/O

Function	Pin	Notes	Specifications
DC ground	1		0 V DC
DC output	2	Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	12 V DC Max load = 125 mA
Configurable (Input or Output)	3–6	Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC
		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, a diode must be connected in parallel with the load, for protection against voltage transients.	0 to max 30 V DC, open drain, 100 mA

Connection example

AXIS XFQ1656

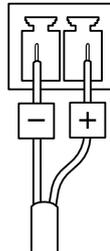## Specifications
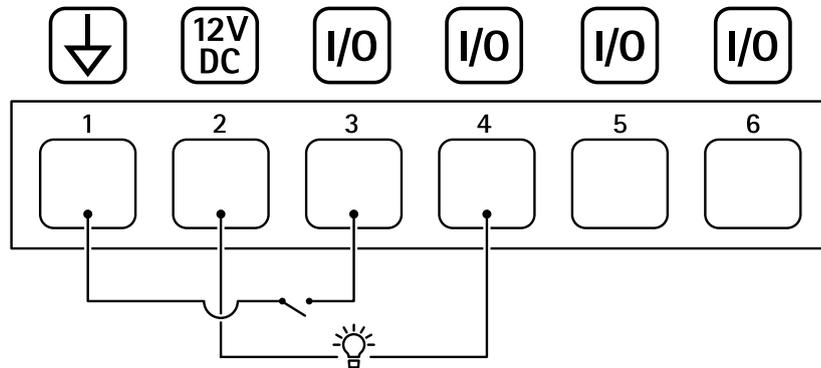
1   DC ground
2   DC output 12 V, max 125 mA
3   I/O configured as input
4   I/O configured as output
5   Configurable I/O
6   Configurable I/O

Power connector

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

RS485/RS422 connector

Two 2-pin terminal blocks for RS485/RS422 serial interface used to control auxiliary equipment such as pan-tilt devices.

The serial port can be configured to support:

- Two-wire RS485 half duplex

- Four-wire RS485 full duplex

- Two-wire RS422 simplex

- Four-wire RS422 full duplex point to point communication
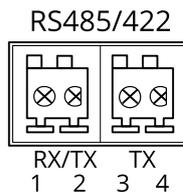
AXIS XFQ1656

Specifications

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

Important

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

PTZ drivers

APTP

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

Important

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

Supported models with RS485 2-wire interface:

- AXIS T99A Positioning Unit Series.

    For information about compatible Axis products, see *axis.com*.

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

Technical information

DEFAULT capabilities for PTZ driver:

Driver	APTP
Version	1.1.0

DEFAULT serial configuration:

PortMode	RS485
BaudRate	115200
DataBits	8
StopBits	1
Parity	None

DEFAULT supported capabilities in this PTZ driver:

Note

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

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

Connection

For the RS485/RS422 pin assignment on your device, see *RS485/RS422 connector on page 64*.

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

Pelco

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

Important

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

PTZ drivers

Supported models:

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

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

Technical information

DEFAULT capabilities for PTZ driver:

Driver	Pelco
Version	4.17

DEFAULT serial configuration:

PortMode	RS485
BaudRate	2400
DataBits	8
StopBits	1
Parity	None

DEFAULT supported capabilities in this PTZ driver:

Note

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

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

AutoIris	yes
AutoFocus	yes
IrCutFilter	no
BackLight	yes
OSDMenu	yes

Connection

For the RS485/RS422 pin assignment on your device, see *RS485/RS422 connector on page 64*.

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

Visca

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

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

Supported models with RS422 4-wire interface:

- Sony EVI-D70/D70P

- WISKA DCP-27 (PT-head)

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

- Axis EVI-D30/D31

- Sony EVI-G20/G21

- Sony EVI-D30/D31

- Sony EVI-D100/D100P

- Sony EVI-D70/D70P

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

Technical information

DEFAULT capabilities for PTZ driver:

Driver	Visca/EVI
Version	4.11

DEFAULT serial configuration:

PortMode	RS422
BaudRate	9600
DataBits	8
StopBits	1
Parity	None

DEFAULT supported capabilities in this PTZ driver:

PTZ drivers

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

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

AutoIris	yes
AutoFocus	yes
IrCutFilter	yes
BackLight	yes
OSDMenu	no

Connection

For the RS485/RS422 pin assignment on your device, see *RS485/RS422 connector on page 64*.

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

Cleaning recommendations

> **NOTICE**
>
> Never use harsh detergent, for example gasoline, benzene, or acetone.

1. Use a can of compressed air to remove any dust or loose dirt from the device.

2. If necessary, clean the lens with a soft cloth dampened with lukewarm water.

Note

Avoid cleaning in direct sunlight or at elevated temperatures, as this may cause stains when the water droplets dry.

Troubleshooting

Reset to factory default settings

Important

Reset to factory default should be used with caution. A reset to factory default resets all settings, including the IP address, to the factory default values.

To reset the product to the factory default settings:

1. Disconnect power from the product.

2. Press and hold the control button while reconnecting power. See *Product overview on page 60*.

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. The product has been reset to the factory default settings. If no DHCP server is available on the network, the default IP address is 192.168.0.90.

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**.

Firmware options

Axis offers product firmware 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 firmware 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 product firmware strategy, go to *axis.com/support/firmware*.

Check the current firmware version

Firmware is the software that determines the functionality of network devices. When you troubleshoot a problem, we recommend you to start by checking the current firmware version. The latest firmware version might contain a correction that fixes your particular problem.

To check the current firmware:

1. Go to the device's web interface > **Status**.

2. See the firmware version under **Device info**.

Upgrade the firmware

Important

- Preconfigured and customized settings are saved when you upgrade the firmware (provided that the features are available in the new firmware) although this is not guaranteed by Axis Communications AB.

- Make sure the device remains connected to the power source throughout the upgrade process.

Note

When you upgrade the device with the latest firmware 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 the firmware. To find the latest firmware and the release notes, go to *axis.com/support/firmware*.

1. Download the firmware file to your computer, available free of charge at *axis.com/support/firmware*.

2. Log in to the device as an administrator.

3. Go to **Maintenance > Firmware 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 issues, clues, and solutions

If you can't find what you're looking for here, try the troubleshooting section at *axis.com/support*.

Problems upgrading the firmware

Firmware upgrade failure	If the firmware upgrade fails, the device reloads the previous firmware. The most common reason is that the wrong firmware file has been uploaded. Check that the name of the firmware file corresponds to your device and try again.
Problems after firmware upgrade	If you experience problems after a firmware upgrade, roll back to the previously installed version from the **Maintenance** page.

Problems setting the IP address

The device is located on a different subnet	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 cannot set the IP address. Contact your network administrator to obtain an IP address.
The IP address is being used by another device	Disconnect the Axis device from the network. Run the ping command (in a Command/DOS window, type `ping` and the IP address of the device): - If you receive: `Reply from <IP address>:  bytes=32; time=10...` this means that the IP address may already be in use by another device on the network. Obtain a new IP address from the network administrator and reinstall the device. - 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.
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 may be problems accessing the device.

The device can't be accessed from a browser

Can't log in	When HTTPS is enabled, ensure that the correct protocol (HTTP or HTTPS) is used when attempting to log in. You may need to manually type `http` or `https` in the browser's address field. If the password for the user root is lost, the device must be reset to the factory default settings. See *Reset to factory default settings on page 71*.

The IP address has been changed by DHCP	IP addresses obtained from a DHCP server are dynamic and may 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, a static IP address can be assigned 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 device is accessible locally but not externally

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

- AXIS Companion: free of charge, ideal for small systems with basic surveillance needs.
- AXIS Camera Station: 30-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. Go to the adapter's documentation for more information.
Lower frame rate than expected	- See *Performance considerations on page 74.* - 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.

Can't connect over port 8883 with MQTT over SSL

The firewall blocks traffic using port 8883 as it's deemed insecure.	In some cases the server/broker might not provide a specific port for MQTT communication. It may 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 the image	
Image degradation or image loss	Check the devices server report for the number of times you have lost the link to the sensor unit.
	Check that the connector cable between the sensor unit and the main unit is tight.
	Change to a new sensor unit cable.

The device turns itself off	
Device shutdown	Disconnect and reconnect power to the device.
	Check if **Delayed shutdown** is turned on. If it's on, the main unit turns off according to the set delay time. You have 300 s to turn off **Delayed shutdown** before the device turns itself off again.

Performance considerations

When setting up your system, it is important to consider how various settings and situations affect the performance. Some factors affect the amount of bandwidth (the bitrate) required, others can affect the frame rate, and some affect both. If the load on the CPU reaches its maximum, this also affects the frame rate.

The following factors are the most important 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 or unicast H.264 clients affects the bandwidth.

- Access by large numbers of Motion JPEG or unicast H.265 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 Motion JPEG and H.264 video streams simultaneously affects both frame rate and bandwidth.

- Accessing Motion JPEG and H.265 video streams simultaneously affects both frame rate and bandwidth.

- 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

Contact support at *axis.com/support*.