AXIS V5938 PTZ Network Camera

User manual

AXIS V5938 PTZ Network Camera

Table of Contents

Installation

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

help.axis.com/?&piaId=58263&section=install

Installation video for the product.

Preview mode

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

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

help.axis.com/?&piaId=58263&section=preview-mode

This video demonstrates how to use preview mode.

Get started

Find the device on the network

To find Axis devices on the network and assign them IP addresses in Windows®, use AXIS IP Utility or AXIS Device Manager. Both applications are free and can be downloaded from *axis.com/support*.

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

Browser support

You can use the device with the following browsers:

	Chrome™	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 create an administrator account. See *Create an administrator account on page 4* .

For descriptions of all the controls and options in the device's web interface, see *The web interface on page 21*.

Create an administrator account

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

1. Enter a username.

2. Enter a password. See *Secure passwords on page 5* .

3. Re-enter the password.

4. Accept the license agreement.

5. Click **Add account**.

Important

> The device has no default account. If you lose the password for your administrator account, you must reset the device. See *Reset to factory default settings on page 62.*

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.

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=58263&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 .

Set the mounting position

1. Go to **Video > Installation > Mounting position**.

2. Click **Change**.

3. Select a mounting position and click **Save and restart**.

Set the power line frequency

1. Go to **Video > Installation > Power line frequency**.

2. Click **Change**.

3. Select a power line frequency and click **Save and restart**.

Set the orientation

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

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

   See also .

Replace the lens

1. Stop all recordings and disconnect power from the device.

2. Disconnect the lens cable and remove the standard lens.

3. Attach the new lens and connect the lens cable.

4. Reconnect the power.

5. For the changes to take effect, you need to restart the device. Go to **Maintenance** and click **Restart**.

6. Adjust the zoom and focus.

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 57*.

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 ![icon] .

2. Click ![icon] 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

Adjust the focus

This product can have four focus modes:

- **Auto**: The camera automatically adjusts focus based on the entire image.

- **Area**: The camera automatically adjusts focus based on a selected area of the image.

- **Manual**: The focus is set manually at a fixed distance.

- **Spot**: The focus is set to a fixed area in the center of the image.
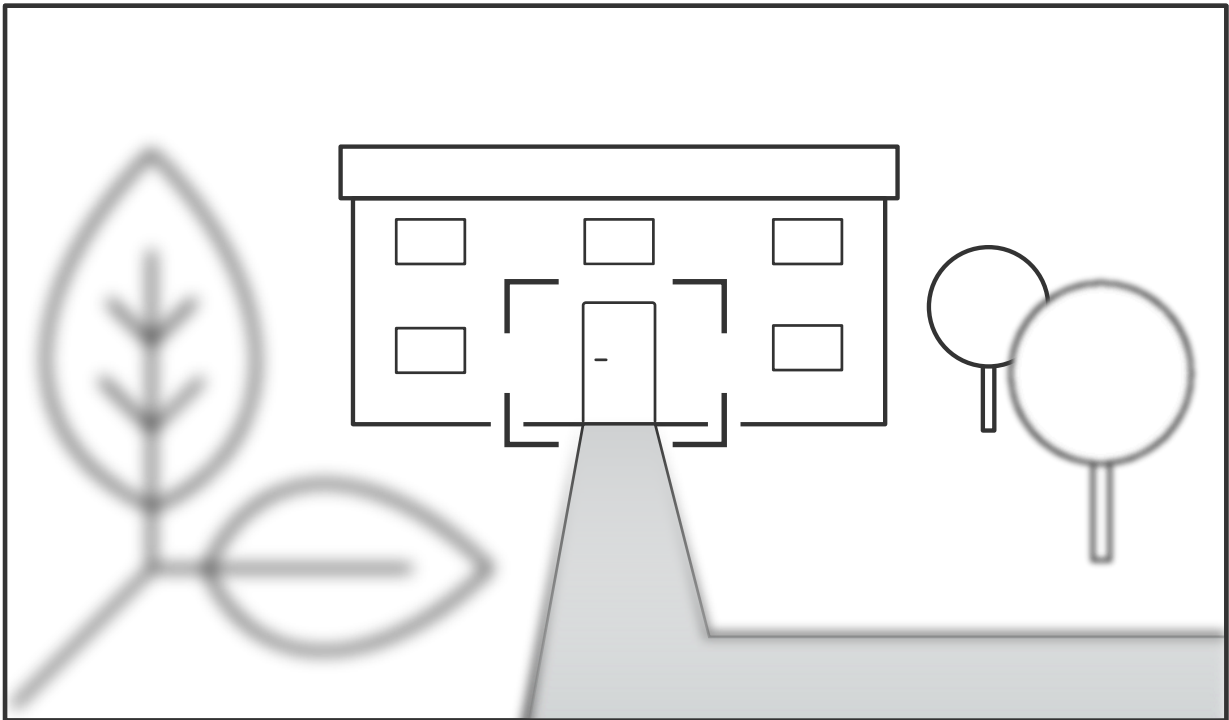
Spot focus

To turn off autofocus and adjust the focus manually:

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

2. Click ![M icon] and use the slider to set the focus.

Configure your device

Adjust the focus faster with focus recall areas

To save the focus settings at a specific pan/tilt range, add a focus recall area. Each time the camera moves into that area it recalls the previously saved focus. It's enough to cover half of the focus recall area in the live view.

We recommend the focus recall feature in the following scenarios:

- When there is a lot of manual operation in live view, for example with a joystick.

- Where PTZ preset positions with manual focus are not efficient, for example movements where the focus setting changes continuously.

- In low-light scenarios, where the autofocus is challenged by the lighting conditions.

Important

- The focus recall overrides the camera's autofocus at the specific pan/tilt range.
- A preset position overrides the focus setting saved in the focus recall area.
- The maximum number of focus recall areas is 20.

Create a focus recall area

1. Pan, tilt, and zoom into the area where you would like to have focus.

   As long as the focus recall button shows a plus , you can add a focus recall area in that position.

2. Adjust the focus.

3. Click the focus recall button.

Delete a focus recall area

1. Pan, tilt, and zoom into the focus recall area you want to delete.

   The focus recall button toggles to minus when the camera detects a focus recall area: .

2. Click the focus recall button.

Reduce image processing time with low latency mode

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

1. Go to **System > Plain config**.

2. Select **ImageSource** from the drop-down list.

3. Go to **ImageSource/I0/Sensor > Low latency mode** and select **On**.

4. Click **Save**.

Select exposure mode

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

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

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

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

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

Note

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

Optimize IR illumination

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

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

2. Turn on **Allow illumination**.

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

4. Adjust the intensity.

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**.

Note

> A high max shutter value can result in motion blur.

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

Note

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

- Set the max gain to a lower value.

- If there is an **Aperture** slider, move it towards **Open**.

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

Reduce motion blur in low-light conditions

To reduce motion blur in low-light conditions, adjust one or more of the following settings in **Video > Image > Exposure**:

Note

> When you increase the gain, image noise also increases.

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

If you still have problems with motion blur:

- Increase the light level in the scene.

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

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

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

Stabilize a shaky image with image stabilization

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

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

Note

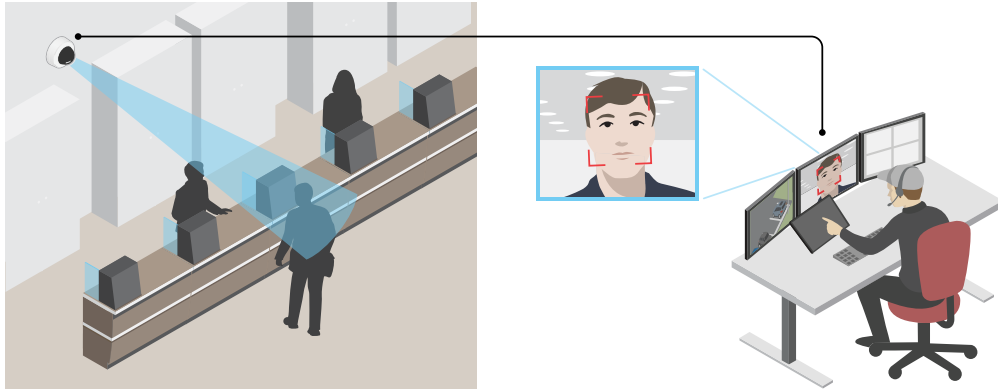When you turn on image stabilization, the image is slightly cropped, which lowers the maximum resolution.

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

2. Turn on **Image stabilization**.

Verify the pixel resolution

To verify that a defined part of the image contains enough pixels to, for example, recognize the face of a person, you can use the pixel counter.

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

2. Click 👁️‍🗨️ for **Pixel counter**.

3. In the camera's live view, adjust the size and position of the rectangle around the area of interest, for example where you expect faces to appear.

    You can see the number of pixels for each of the rectangle's sides, and decide if the values are enough for your needs.

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.

Show the pan or tilt position as a text overlay

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

1. Go to **Video > Overlays** and click ╈ .

2. In the text field, type #x to show the pan position.

   Type #y to show the tilt position.

3. Choose appearance, text size, and alignment.

4. The current pan and tilt positions show up in the live view image and in the recording.

Adjust the camera view (PTZ)

Limit the pan, tilt, and zoom movements

If there are parts of the scene that you don't want the camera to reach, you can limit the pan, tilt, and zoom movements. For example, you want to protect the privacy of residents in an apartment building, which is located close to a parking lot that you intend to monitor.

To limit the movements:

1. Go to **PTZ > Limits**.

2. Set the limits as needed.

Control the camera with VISCA

There are two ways to control this camera with VISCA:

VISCA over IP – Select this to communicate over the Ethernet.

VISCA over serial – Select this to communicate over serial connection.

Control the camera with VISCA over IP

Note

Using the IP protocol for PTZ control increases the risk of unauthorized access. It enables UDP on ports 52380 and 52381, which allows anyone on the network to change settings without having to log in to the camera.

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

2. Turn on **VISCA**.

3. Select **VISCA over IP**.

Control the camera with VISCA over serial

1. Connect a serial cable to the RS232 connector.

2. Go to **Settings > System > Accessories**.

3. Turn on **VISCA**.

4. Select **VISCA over serial**.

5. Select the camera's **Position in series**.

   - Select **Point to point** if the device is directly connected to the VISCA controller.

   - Select **Endpoint** if the device is the last device in the daisy chain.

   - Select **In-chain (daisy chain)** if the device is in the middle of the daisy chain.

6. Select **Baud rate**.

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 57*.

Reduce bandwidth and storage

Important

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

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

2. Click in the live view.

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

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

5. Go to **Video > Stream > Zipstream** and do one or more of the following:

   Note

      The **Zipstream** settings are used for all video encodings except MJPEG.

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

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

   - Turn on **Dynamic FPS**.

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

Note

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

Set up network storage

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

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

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

3. Type the IP address of the host server.

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

5. Type the username and password.

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

7. Select **Add share without testing** if you experience temporary connection issues, or if the share is not yet configured.

8. Click **Add**.

Record and watch video

Record video directly from the camera

1. Go to **Video > 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 13*

3. To stop recording, click   again.

Watch video

1. Go to **Recordings**.

2. Click   for your recording in the list.

Set up rules for events

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

To learn more, 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.

Note

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

Record video when the camera detects an object

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

AXIS V5938 PTZ Network Camera

Configure your device

Before you start:

- Make sure you have an SD card installed.

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

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

Create a rule:

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

2. Type a name for the rule.

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

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

5. Select a camera and a stream profile.

6. Set the prebuffer time to 5 seconds.

7. Set the postbuffer time to 1 minute.

8. Click **Save**.

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

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

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

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

Add the overlay text:

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

2. Under **Overlays**, select **Text** and click ➕ .

3. Enter #D in the text field.

4. Choose text size and appearance.

5. To position the text overlay, click ⊞ and select an option.

Create a rule:

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

2. Type a name for the rule.

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

4. Select a video channel.

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

6. Set the duration.

7. Click **Save**.

Record video when a PIR detector senses motion

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

Required hardware

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

- PIR detector, normally closed

NOTICE

Disconnect the device from power before connecting the wires. Reconnect to power after all connections are done.
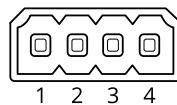
Connect the wires to the device's I/O connector

Note

For information on the I/O connector, see *Connectors on page 67*.

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**.

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

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

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

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

Add a preset position:

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

Create a rule:

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

2. Type a name for the rule.

3. In the list of actions, select **Go to preset position**.

4. Select the preset position you want the camera to go to.

5. Click **Save**.

Provide visual indication of an ongoing event

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

Required hardware

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

Note

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

Note

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

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

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

2. Make sure that the port you connected the AXIS I/O Indication LED to is set to **Output**. Set the normal state to **Circuit open**.

3. Go to **System > Events**.

4. Create a new rule.

5. Select the **Condition** that must be met to trigger the camera to start recording. It can, for example, be a time schedule or motion detection.

6. In the list of actions, select **Record video**. Select a storage space. Select a stream profile or create a new. Also set the **Prebuffer** and **Postbuffer** as required.

7. Save the rule.

8. Create a second rule and select the same **Condition** as in the first rule.

9. In the list of actions, select **Toggle I/O while the rule is active**, and then select the port the AXIS I/O Indication LED is connected to. Set the state to **Active**.

10. Save the rule.

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

- Configure the LED to turn on when the camera starts, to indicate the presence of the camera. Select **System ready** as a condition.

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

Direct the camera and open the lock to a gate when someone is nearby

This example explains how to direct the camera and open a gate when someone wants to enter during daytime. This is done by connecting a PIR detector to the product's input port and a switch relay to the product's output port.

Required hardware

- Mounted PIR detector

- Switch relay connected to the gate lock, in this case the switch is normally closed (NC)

- Connecting wires

Physical connection

1. Connect the wires from the PIR detector to the input pin, see *I/O connector on page 68*.

2. Connect the wires from the switch to the output pin, see *I/O connector on page 68*

Configure I/O ports

You need to connect the switch relay to the camera from the camera's web interface. First, configure the I/O ports:

Set the PIR detector to an input port

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 open.

Set the switch relay to an output port

1. Click ↗ to set the direction to output for port 2.

2. Give the output module a descriptive name, for example "Gate switch".

3. If you want to open the gate whenever an event is triggered, click ⟋ to set the normal state to circuit closed.

Create the preset position

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

2. Create the preset position that covers the entrance of the gate and name it, for example, "Gate entrance".

Create rules

For the camera to open the gate when the PIR detector senses someone nearby, you need to create a rule in the camera:

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

2. Type a name for the rule, for example "Open gate".

3. In the list of conditions, select **PIR detector**.

4. In the list of actions, select **Toggle I/O once**.

5. In the list of ports, select **Gate switch**.

6. Set state to **Active**.

7. Set the duration.

8. Click **Save**.

9. Create another rule with the name "Direct the camera to the gate".

10. Select the same input signal as before, but as action select the previously created "Gate entrance" preset position.

11. Click **Save**.

Record video when the camera detects loud noises

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

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

Turn on audio:

1. Set up the stream profile to include audio, see *Add audio to your recording on page 20*.

Turn on audio detection:

1. Go to **System > Detectors > Audio detection**.

2. Adjust the sound level according to your needs.

Create a rule:

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

2. Type a name for the rule.

3. In the list of conditions, under **Audio**, select **Audio Detection**.

4. In the list of actions, under **Recordings**, select **Record video**.

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

6. Select the stream profile where audio has been turned on.

7. Set the prebuffer time to 5 seconds.

8. Set the postbuffer time to 2 minutes.

9. Click **Save**.

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.
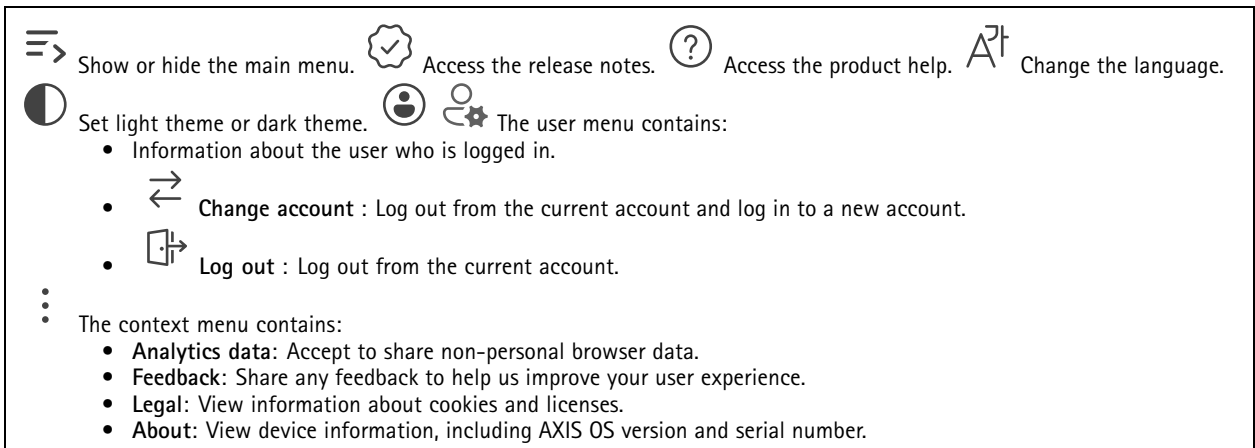
7. Click **Save**.

The web interface

To reach the device's web 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 release notes. ⑦ Access the product help. A̅ᵗ Change the language.

◑ Set light theme or dark theme. 😊 ⚙ The user menu contains:
   • Information about the user who is logged in.

   • ⇄ **Change account** : Log out from the current account and log in to a new account.

   • ⬆ **Log out** : Log out from the current account.

⋮ 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 AXIS OS version and serial number.

Status

Device info

Shows the device information, including AXIS OS version and serial number.

Upgrade AXIS OS: Upgrade the software on your device. Takes you to the Maintenance page where you can do the 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: View and update the NTP settings. Takes you to the **Time and location** page where you can change the NTP settings.

Security

Shows what kind of access to the device that is active, what encryption protocols are in use, and if unsigned apps are allowed. Recommendations to the settings are based on the AXIS OS Hardening Guide.

Hardening guide: Link to *AXIS OS Hardening guide* where you can learn more about cybersecurity on Axis devices and best practices.

Video input

Shows video input information, including if video input is configured and detailed information for each channel.

Video input settings: Update the video input settings. Takes you to the Video input page where you can change the video input settings.

PTZ

Shows the PTZ status and the time of the last test.

Test: Start a test of the PTZ mechanics. During the test, there are no video streams available. When the test is finished, the device restores to its home position.

Connected clients

Shows the number of connections and connected clients.

View details: View and update the list of connected clients. The list shows IP address, protocol, port, state, and PID/process of each connection.

Video

Click-and-drag to pan and tilt in the live view.**Zoom** Use the slider to zoom in and out.**Focus** Use this setting to set focus in the shown area. Depending on the device, different focus modes are available.
- **Auto**: The camera automatically adjusts focus based on the entire image.
- **Manual**: Set the focus manually at a fixed distance.
- **Area**: The camera automatically adjusts focus for a selected area of the image.
- **Spot**: The camera automatically adjusts focus for the center of the image.

Brightness Use this setting to adjust the light intensity in the image, for example, to make objects easier to see. Brightness is applied after image capture, and does not affect the information in the image. To get more details in a dark area, it is sometimes better to try to increase gain or increase exposure time.

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 the specific web-browser engine where the snapshot is received applies, 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. 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. 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. Click to select a guard tour, then click **Start** to play the guard tour. Or, click **Setup** to go to the guard tours page. 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. ⬭ Click to show the storage that is configured for the device. To configure the storage, you need to be logged in as an administrator. ⚙ Click to access more settings:

- **Video format**: Select the encoding format to use in the live view.

- ▷ **Autoplay**: Turn on to autoplay a muted video stream whenever you open the device in a new session.
- **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 👁̸ to show the level grid. The grid helps you decide if the image is horizontally aligned. Click 👁 to hide it.
- **Pixel counter**: Click 👁̸ 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 ↻ to refresh the still image in the live view.
- **PTZ controls** ⓘ : 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. ⌐⌐ Click to show the live video stream in full screen. Press ESC to exit full screen mode.

Installation

Capture mode ⓘ : 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** ⓘ : The orientation of the image can change depending on how you mount the camera. **Power line frequency**: To minimize image flicker, select the frequency your region uses. 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.

P-Iris lens: Select the installed and supported lens. Restart the camera for the changes to take effect.

Zoom: Use the slider to adjust the zoom level. **Autofocus after zooming**: Turn on to enable autofocus after zooming. **Focus**: Use the slider to manually set the focus. **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.

Note

In cold environments, it can take several minutes for the zoom and focus to become available.

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) : 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** : 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** : 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** : 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** : 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** : 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**.**Focus breathing correction** : Turn on to keep the angle of view constant while you change the focus. You might not be able to zoom in as much with this function activated.**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.
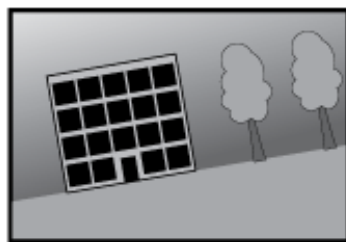
The image before and after it has been straightened.

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.

- **License plate** ⓘ : Suitable for capturing license plates.

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

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 isn't 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. To override this behavior, choose 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.
- **One-Push**: Manually correct the white balance when the shown colors differ from reality. Make sure a white object, in current lighting conditions, occupies more than half the image and click **Set**. The white balance setting becomes fixed and you have to manually change the white balance when the lightning changes.

- **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 don't 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.

Note
- Some devices have IR-pass filters in night mode. The IR-pass filter increases IR-light sensitivity but blocks visible light.

- **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 connect a supporting Axis accessory.**Allow illumination**: Turn on to let the camera use the built-in light in night mode.**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** ⓘ : Turn on to use the automatic illumination angle. Turn off to set the illumination angle manually.**Illumination angle** ⓘ : 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** ⓘ : Select the desired wavelength for the IR light.**White light** ⓘ **Allow illumination** ⓘ : Turn on to let the camera use white light in night mode.**Synchronize illumination** ⓘ : Turn on to automatically synchronize the white light with the surrounding light.

Exposure

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.

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

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

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

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

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

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

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

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

> **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.

General

Name: Enter a name for the selected camera.

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.**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 is network congestion, there could be a noticeable deterioration in the video quality.**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: Turn on to minimize the bitrate while maintaining quality. The optimization does not apply to the stream shown in the web client. This can only be used if your VMS supports B-frames. 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.

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, and 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.
- **Scene annotation** ⓘ : Select to show a text overlay in the video stream that stays in the same position, even when the camera pans or tilts in another direction. You can choose to only show the overlay within certain zoom levels.

    - ▦ : 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. The overlay is saved and remains in the pan and tilt coordinates of this position.

- **Annotation between zoom levels (%)**: Set the zoom levels which the overlay will be shown within.

- **Annotation symbol**: Select a symbol that appears instead of the overlay when the camera is not within the set zoom levels.

- **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.

- **Widget: Linegraph** ⓘ : Show a graph chart that displays how a measured value changes over time.

  - **Title**: Enter a title for the widget.

  - **Overlay modifier**: Select an overlay modifier as data source. If you have created MQTT overlays, they will be located at the end of the list.

  - ⊞ : Select the position of the overlay in the image.

  - **Size**: Select the size of the overlay.

  - **Visible on all channels**: Turn off to show only on your currently selected channel. Turn on to show on all active channels.

  - **Update interval**: Choose the time between data updates.

  - **Transparency**: Set the transparency of the entire overlay.

  - **Background transparency**: Set the transparency only of the background of the overlay.

  - **Points**: Turn on to add a point to the graph line when data is updated.

  - **X axis**

  - **Label**: Enter the text label for the x axis.

  - **Time window**: Enter how long time the data is visualized.

  - **Time unit**: Enter a time unit for the x axis.

  - **Y axis**

  - **Label**: Enter the text label for the y axis.

  - **Dynamic scale**: Turn on for the scale to automatically adapt to the data values. Turn off to manually enter values for a fixed scale.

  - **Min alarm threshold** and **Max alarm threshold**: These values will add horizontal reference lines to the graph, making it easier to see when the data value becomes too high or too low.

- **Widget: Meter** ⓘ : Show a bar chart that displays the most recently measured data value.

  - **Title**: Enter a title for the widget.

  - **Overlay modifier**: Select an overlay modifier as data source. If you have created MQTT overlays, they will be located at the end of the list.

  - ⊞ : Select the position of the overlay in the image.

  - **Size**: Select the size of the overlay.

  - **Visible on all channels**: Turn off to show only on your currently selected channel. Turn on to show on all active channels.

  - **Update interval**: Choose the time between data updates.

  - **Transparency**: Set the transparency of the entire overlay.

  - **Background transparency**: Set the transparency only of the background of the overlay.

  - **Points**: Turn on to add a point to the graph line when data is updated.

  - **Y axis**

  - **Label**: Enter the text label for the y axis.

  - **Dynamic scale**: Turn on for the scale to automatically adapt to the data values. Turn off to manually enter values for a fixed scale.

  - **Min alarm threshold** and **Max alarm threshold**: These values will add horizontal reference lines to the bar chart, making it easier to see when the data value becomes too high or too low.

View areas

$+$: Click to create a view area. $\square$ 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.

Analytics

Metadata configuration

RTSP metadata producers

Lists the apps that stream metadata and the channels they use.

Note

These settings are for the RTSP metadata stream that use ONVIF XML. Changes made here don't affect the Metadata visualization page.

Producer: The app that produces the metadata. Below the app is a list of the types of metadata the app streams from the device.**Channel**: The channel that the app uses. Select to enable the metadata stream. Deselect for compatibility or resource management reasons.

PTZ

Preset positions

A preset position is a specific pan, tilt, and zoom position stored in your camera's memory. You can use preset positions to quickly navigate between different fields of view. If your device supports guard tours, you can use preset positions to create automated guard tours.

Preset positions

- $+$ **Create preset position**: Create a new preset position based on the current position of your camera.
  - **Thumbnail**: Turn on to add a thumbnail image for the preset position.
  - **Name**: Enter a name for the preset position.
  - **Home position**: Turn on to set this position as your camera's default field of view. The home position is marked with 🏠 . Your camera will always have a home position.

Settings
- **Return to home position when inactive**: Turn on to make the camera return to its home position after a specified period of inactivity.
- **Use thumbnails**: Turn on to automatically add a thumbnail to any new preset position you create.

⋮ The context menu contains:

- **Create thumbnails** ⓘ : Create a thumbnail for all your preset positions.
- **Refresh thumbnails**: Replace the thumbnails for your preset positions with new and updated thumbnails.
- **Delete all preset positions**: Remove all your preset positions. This will also create a new home position automatically.

Limits

To narrow down the area under surveillance, you can limit the PTZ movements.**Save as Pan 0**: Click to set the current position as zero-point for pan coordinates.**Pan-tilt limits**: The camera uses the coordinates of the center of the image when you set pan-tilt limits.

- **Left pan limit**: Click to limit the camera's pan movements to the left. Click again to remove the limit.

- **Right pan limit**: Click to limit the camera's pan movements to the right. Click again to remove the limit.

- **Top tilt limit**: Click to limit the camera's tilt movements to the top. Click again to remove the limit.

- **Bottom tilt limit**: Click to limit the camera's tilt movements to the bottom. Click again to remove the limit.

Auto-flip : Enables the camera head to instantly reverse 360° and continue to pan beyond its mechanical limit.**E-flip** : Automatically corrects the camera view by flipping the image 180° when the camera tilts beyond -90°.**Nadir-flip** : Enables the camera to pan 180° when tilting beyond -90°, and then continue upwards.**Zoom limit**: Select a value to limit the camera's maximum zoom level. Optical or digital (e.g. 480x D) values can be selected. When using a joystick, only digital zoom levels can be used to set the zoom limit.**Near focus limit**: Select a value to prevent the camera from autofocusing on objects close to the camera. This way, the camera can ignore objects such as overhead wires, streetlights, or other nearby objects. To make the camera focus on the areas of interest, set the near focus limit to a value greater than the distance at which the objects of no interest tend to appear.

Motion

Proportional speed : Turn on to set the maximum proportional speed.

- **Max proportional speed** : Set a value between 1 and 1000 to limit the pan and tilt speed. Max proportional speed is defined as a percentage, where the value 1000 equals 1000%.
 This is useful when the joystick is pushed all the way out. For example, if the image is approximately 44 degrees wide when fully zoomed out and the max proportional speed is set to 100 (100%), the maximum speed is about 44 degrees/second. If the image is then zoomed in from 44 to 10 degrees wide, the maximum speed reaches about 10 degrees/second, which is probably too fast for easy viewing. To limit the speed, set the max proportional speed to 50 (50%). This way, the maximum speed only reaches 50% of the maximum for the currently selected zoom level. This means that when the image is 44 degrees wide, the greatest possible speed is limited to about 22 degrees/second, and when the view is zoomed in to 10 degrees the speed is limited to about 5 degrees/second.

Adjustable zoom speed: Turn on to use variable speeds when controlling the zoom with a joystick or a mouse wheel. The zoom speed is automatically set through the command `continuouszoommove` in the VAPIX® Application Programming Interface (API). Turn off to use the highest zoom speed which is the same speed for moving to presets.**Freeze image on PTZ**
- **Off**: Never freeze image.
- **All movements**: Freeze the image while the camera is moving. Once the camera reaches its new position, the view from that position is shown.
- **Preset positions**: Freeze the image only when the camera moves between preset positions.

Pan-tilt speed: Select the speed of the camera's pan and tilt movements.

OSDI zones

On-screen direction indicator (OSDI) gives information of the direction the camera is pointing at in the text overlay. The camera uses the coordinates of the center of the image when you set the lower left and upper right zone area. ✛ **Create OSDI zone**: Click to create an OSDI zone.

- **Name**: Enter a name for the zone.
- **Active**: Turn on to display the zone in the live view.
- **Zone limits**

    - ↙ : Navigate to your desired position, and click the icon to set the lower left point of the zone. Click again to unset the lower left point.

    - ↗ : Navigate to your desired position, and click the icon to set the upper right point of the zone. Click again to unset the upper right point.

    - **Go to**: Click to go to the lower left point or the upper right point of the zone.

⋮ The context menu contains:
  - **Create multiple zones**: Click to create multiple zones. Enter a name for the zone, and specify the coordinates for lower left and upper right of the zone.
    - **Add zone coordinates**: Click to specify the parameters for another zone.
  - **Delete all zones**: Click to delete all zones.

Orientation aid

Orientation aid: Turn on to activate overlays of user-defined points of interest at the correct bearing and a 2D-compass synchronized to the cameras movements, including a field of view.**Direction**
  - **Set north**: Position the camera at north, and click **Set north**.
Preset positions: Select the preset positions used for orientation aid.
  - To select an individual preset position, click the preset position.

  - To select all preset positions, click ☑ .

Gatekeeper

A gatekeeper monitors an area such as an entrance gate. When motion is detected in the monitored area, the gatekeeper steers the camera to a selected preset position. Using a zoomed-in preset position can make it possible to, for example, read a license plate or identify a person. When motion is no longer detected, the camera returns to its home position after a defined time.

Control queue

User control queue
  - **PTZ control queue**: Turn on to place PTZ control requests in a queue. This displays the users status and position in the queue. To use the PTZ controls in AXIS Camera Station, turn off this setting.
    - **Enter queue**: Click to add your request for PTZ control to the queue.
    - **Release control**: Click to release the PTZ control.
  - The user groups are listed in a prioritized order with the highest priority on top. To change the priority of a user group, click ═ and drag the user group up or down.
    For each user group:
    - **Timeout duration**: Set the amount of time to wait before timeout. The default value is 1 minute, and allowed values are from 1 second to 60 minutes.
    - **Timeout type**
    - **Timespan**: Time out after reaching the set duration.
    - **Activity**: Time out after reaching the set duration since the last activity.
    - **Infinity**: Never to time out until a user with higher priority takes control.
Settings
  - **Limit number of users in queue**: Set the maximum number of users allowed in a queue. The default number is 20, and allowed values are 1–100.

- **Control queue poll time**: Set how often to poll the camera to update the place of the users or user groups in the queue. The default value is 20 seconds, and allowed values are from 5 seconds to 60 minutes.

Autotracking

AutotrackingWith autotracking, the camera automatically zooms in on and tracks moving objects, for example a vehicle or a person. You can manually select an object to track, or set up trigger areas and let the camera detect moving objects. The application is best suited for open areas with no obscuring objects and where movement is unusual. When the camera doesn't track an object, it returns to its connected preset position.

Audio

AXIS Audio Manager Edge

AXIS Audio Manager Edge: Launch the application.

Audio site security

CA certificate: Select the certificate to use when you add devices to the audio site. You have to enable TLS authentication in AXIS Audio Manager Edge. **Save**: Activate and save your selection.

Device settings

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

Allow stream extraction ⓘ : Turn on to allow stream extraction.**Input type** ⓘ : Select the type of input, for instance, if it's internal microphone or line.**Power type** ⓘ : Select power type for your input.**Apply changes** ⓘ : Apply your selection.**Echo cancellation** ⓘ : Turn on to remove echoes during two-way communication.**Separate gain controls** ⓘ : Turn on to adjust the gain separately for the different input types.**Automatic gain control** ⓘ : 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: Shows the type of output.

Gain: Use the slider to change the gain. Click the speaker icon to mute or unmute.**Automatic volume control** ⓘ : Turn on to make the device automatically and dynamically adjust the gain based on the ambient noise level. Automatic volume control affects all audio outputs, including line and telecoil.

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.

Echo cancellation: Turn on to remove echoes during two-way communication.

Audio clips

┼ **Add clip**: Add a new audio clip. You can use .au, .mp3, .opus, .vorbis, .wav files. ▷ Play the audio clip. ☐ Stop playing the audio clip. ⋮ The context menu contains:
- **Rename**: Change the name of the audio clip.
- **Create link**: Create a URL that, 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.

Listen and record

▷ Click to listen. ● Start a continuous recording of the live audio stream. Click again to stop the recording. If a recording is ongoing, it will resume automatically after a reboot.

Note

You can only listen and record if input is turned on for the device. Go to **Audio > Device settings** to make sure you turn on input.

🗄 Shows the configured storage for the device. To configure the storage, you need to be logged in as an administrator.

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.

Speaker test

You can use the speaker test to verify remotely that the speaker works as intended. **Calibrate**: You need to calibrate the speaker before its first test. During calibration, the speaker plays a series of test tones that are registered by the built-in microphone. When you calibrate the speaker, it must be installed in its final position. If you move the speaker later, or if its surroundings change, for example, if a wall is built or removed, you need to recalibrate the speaker. **Run the test**: Play the same series of test tones that were played during calibration, and compare them with the calibration's registered values.

Recordings

Ongoing recordings: Show all ongoing recordings on the device. ● Start a recording on the device. ▭ Choose which storage device to save to. ● Stop a recording on the device. **Triggered recordings** will end when manually stopped or when the device is shut down. **Continuous recordings** will continue until manually stopped. Even if the device is shut down, the recording will continue when the device starts up again.

▷ Play the recording. ☐ Stop playing the recording. ⌄ ⌃ Show or hide information and options about the recording.**Set export range**: If you only want to export part of the recording, enter a time span. Note that if you work in a different time zone than the location of the device, the time span is based on the device's time zone.**Encrypt**: Select to set a password for exported recordings. It will not be possible to open the exported file without the password. 🗑 Click to delete a recording.**Export**: Export the whole or a 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. The source refers to the sensor.**Event**: Show recordings based on events.**Storage**: Show recordings based on storage type.

Apps

┼ **Add app**: Install a new app.**Find more apps**: Find more apps to install. You will be taken 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. 🔔 View the security updates in AXIS OS and ACAP apps.

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**: 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**: View information about open-source licenses used in the app.
- **App log**: 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 replace it with another license, for example, when you change from a trial license to a full license. If you deactivate the license, you also remove it from the device.
- **Settings**: Configure the parameters.
- **Delete**: Delete the app permanently from the device. If you don't deactivate the license first, it remains active.

System

Time and location

Date and time

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

Note

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

Synchronization: Select an option for the device's date and time synchronization.
  - **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.
    - **Max NTP poll time**: Select the maximum amount of time the device should wait before it polls the NTP server to get an updated time.
    - **Min NTP poll time**: Select the minimum amount of time the device should wait before it polls the NTP server to get an updated time.
  - **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.
    - **Max NTP poll time**: Select the maximum amount of time the device should wait before it polls the NTP server to get an updated time.
    - **Min NTP poll time**: Select the minimum amount of time the device should wait before it polls the NTP server to get an updated time.
  - **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.
    - **Max NTP poll time**: Select the maximum amount of time the device should wait before it polls the NTP server to get an updated time.
    - **Min NTP poll time**: Select the minimum amount of time the device should wait before it polls the NTP server to get an updated time.
  - **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 automatically adjust to daylight saving time and standard time.
  - **DHCP**: Adopts the time zone of the DHCP server. The device must connected to a DHCP server before you can select this option.
  - **Manual**: Select a time zone from the drop-down list.

Note

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

Device location

Enter where the device is located. Your video management system can use this information to place the device on a map.

  - **Format**: Select the format to use when you enter your device's latitude and longitude.
  - **Latitude**: Positive values are north of the equator.
  - **Longitude**: Positive values are east of the prime meridian.
  - **Heading**: Enter the compass direction that the device is facing. 0 is due north.
  - **Label**: Enter a descriptive name for your device.
  - **Save**: Click to save your device location.

Regional settings

Sets the system of measurement to use in all system settings.

Metric (m, km/h): Select for distance measurement to be in meters and speed measurement to be in kilometers per hour.**U.S. customary (ft, mph)**: Select for distance measurement to be in feet and speed measurement to be in miles per hour.

WLAN

With a wireless USB adapter, the device can connect to a wireless network.

Country: To improve the driver's ability to locate network access points, select the country where the device is located. ┼ **Add network**: Add a wireless network that doesn't broadcast its SSID (name). Enter the SSID and all the required settings for the network. Contact your network administrator to get the required settings. ↻ **Refresh**: Update the list of available wireless networks. ⋮ The context menu contains:

- **Info**: Show the signal strength, channel, and type of network security.
- **Configure**: Change the network settings.

Configuration check

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 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.

Note

> If DHCP isn't available and the device uses a static address fallback, the static address is configured with a limited scope.

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 server report and system log use the hostname. Allowed characters are A–Z, a–z, 0–9 and -.**Enable dynamic DNS updates**: Allow your device to automatically update its domain name server records whenever its IP address changes.**Register DNS name**: Enter a unique domain name that points to your device's IP address. Allowed characters are A–Z, a–z, 0–9 and -.**TTL**: Time to Live (TTL) sets how long a DNS record stays valid before it needs to be updated.

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 the device uses.**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

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.

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

> 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. The device allows port 80 or any port in the range 1024-65535. 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. The device allows port 443 or any port in the range 1024-65535. 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.**LLDP and CDP**: Turn on to allow automatic discovery on the network. Turning LLDP and CDP off can impact the PoE power negotiation. To resolve any issues with the PoE power negotiation, configure the PoE switch for hardware PoE power negotiation only.

Global proxies

Http proxy: Specify a global proxy host or IP address according to the allowed format.**Https proxy**: Specify a global proxy host or IP address according to the allowed format.

Allowed formats for http and https proxies:

- **http(s)://host:port**
- **http(s)://user@host:port**
- **http(s)://user:pass@host:port**

> Note
>
> Restart the device to apply the global proxy settings.

No proxy: Use **No proxy** to bypass global proxies. Enter one of the options in the list, or enter several separated by a comma:

- Leave empty
- Specify an IP address
- Specify an IP address in CIDR format
- Specify a domain name, for example: **www.<domain name>.com**
- Specify all subdomains in a specific domain, for example **.<domain name>.com**

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**: This is 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 register 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 register 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 or 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 web 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' access to 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.

<hr>

+
    Add certificate : Click to add a certificate.

- **More** ⌄ : Show more fields to fill in or select.
- **Secure keystore**: Select to use **Secure element** or **Trusted Platform Module 2.0** to securely store the private key. For more information on which secure keystore to select, go to *help.axis.com/en-us/axis-os#cryptographic-support*.
- **Key type**: Select the default or a different encryption algorithm from the drop-down list to protect the 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.

Secure keystore ⓘ :

- **Secure element (CC EAL6+)**: Select to use secure element for secure keystore.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Level 2)**: Select to use TPM 2.0 for secure keystore.

<hr>

Network access control and encryption

<hr>

IEEE 802.1xIEEE 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).**IEEE 802.1AE MACsec**IEEE 802.1AE MACsec is an IEEE standard for media access control (MAC) security that defines connectionless data confidentiality and integrity for media access independent protocols.**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, you must install a signed client certificate on the device.**Authentication method**: Select an EAP type used for authentication.**Client certificate**: Select a client certificate to use IEEE 802.1x. The authentication server uses the certificate to validate the client's identity.**CA certificates**: Select CA certificates 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.These settings are only available if you use **IEEE 802.1x PEAP-MSCHAPv2** as the authentication method:

- **Password**: Enter the password for your user identity.
- **Peap version**: Select the Peap version that is used in the network switch.
- **Label**: Select 1 to use client EAP encryption; select 2 to use client PEAP encryption. Select the Label that the network switch uses when using Peap version 1.

These settings are only available if you use **IEEE 802.1ae MACsec (Static CAK/Pre-Shared Key)** as the authentication method:

- **Key agreement connectivity association key name**: Enter the connectivity association name (CKN). It must be 2 to 64 (divisible by 2) hexadecimal characters. The CKN must be manually configured in the connectivity association and must match on both ends of the link to initially enable MACsec.
- **Key agreement connectivity association key**: Enter the connectivity association key (CAK). It should be either 32 or 64 hexadecimal characters long. The CAK must be manually configured in the connectivity association and must match on both ends of the link to initially enable MACsec.

<hr>

Prevent brute-force attacks

<hr>

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.

<hr>

Firewall

Activate: Turn on the firewall.
Default Policy: Select the default state for the firewall.

- **Allow:** Allows all connections to the device. This option is set by default.
- **Deny:** Denies all connections to the device.

To make exceptions to the default policy, you can create rules that allows or denies connections to the device from specific addresses, protocols, and ports.

- **Address**: Enter an address in IPv4/IPv6 or CIDR format that you want to allow or deny access to.
- **Protocol**: Select a protocol that you want to allow or deny access to.
- **Port**: Enter a port number that you want to allow or deny access to. You can add a port number between 1 and 65535.
- **Policy**: Select the policy of the rule.

┿ : Click to create another rule.
Add rules: Click to add the rules that you have defined.

- **Time in seconds:** Set a time limit for testing the rules. The default time limit is set to **300** seconds. To activate the rules straight away, set the time to **0** seconds.
- **Confirm rules:** Confirm the rules and their time limit. If you have set a time limit of more than 1 second, the rules will be active during this time. If you have set the time to **0**, the rules will be active straight away.

Pending rules: An overview of the latest tested rules that you are yet to confirm.

Note

> The rules that have a time limit appear under **Active rules** until the displayed timer runs out, or until you confirm them. If you don't confirm them, they will appear under **Pending rules** once the timer runs out, and the firewall will revert to the previously defined settings. If you confirm them, they will replace the current active rules.

Confirm rules: Click to activate the pending rules.**Active rules**: An overview of the rules you are currently running on the device.

🗑 : Click to delete an active rule. 🛍 : Click to delete all rules, both pending and active.

Custom signed AXIS OS certificate

To install test software or other custom software from Axis on the device, you need a custom signed AXIS OS certificate. The certificate verifies that the software is approved by both the device owner and Axis. The software can only run on a specific device which is identified by its unique serial number and chip ID. Only Axis can create custom signed AXIS OS certificates, since Axis holds the key to sign them.**Install**: Click to install the certificate. You need to install the certificate before you install the software. ⋮ The context menu contains:

- **Delete certificate**: Delete the certificate.

Accounts

Accounts

┿ **Add account**: Click to add a new account. You can add up to 100 accounts.**Account**: Enter a unique account name.**New password**: Enter a password for the account. 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.**Privileges**:

- **Administrator**: Has full access to all settings. Administrators can also add, update, and remove other accounts.
- **Operator**: Has access to all settings except:
  - All **System** settings.
- **Viewer**: Has access to:
  - Watch and take snapshots of a video stream.
  - Watch and export recordings.
  - Pan, tilt, and zoom; with **PTZ account** access.

⋮ The context menu contains:**Update account**: Edit the account properties.**Delete account**: Delete the account. You can't delete the root account.

Anonymous access

Allow anonymous viewing: Turn on to allow anyone access the device as a viewer without logging in with an account.**Allow anonymous PTZ operating** : Turn on to allow anonymous users to pan, tilt, and zoom the image.

SSH accounts

Add SSH account: Click to add a new SSH account.
- **Restrict root access**: Turn on to restrict functionality that requires root access.
- **Enable SSH**: Turn on to use SSH service.

Account: Enter a unique account name.**New password**: Enter a password for the account. 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.**Comment**: Enter a comment (optional). The context menu contains:**Update SSH account**: Edit the account properties.**Delete SSH account**: Delete the account. You can't delete the root account.

Virtual host

Add virtual host: Click to add a new virtual host.**Enabled**: Select to use this virtual host.**Server name**: Enter the name of the server. Only use numbers 0-9, letters A-Z, and hyphen (-).**Port**: Enter the port the server is connected to.**Type**: Select the type of authentication to use. Select between **Basic**, **Digest**, and **Open ID**. The context menu contains:
- **Update**: Update the virtual host.
- **Delete**: Delete the virtual host.

Disabled: The server is disabled.

OpenID Configuration

Important

If you can't use OpenID to sign in, use the Digest or Basic credentials you used when you configured OpenID to sign in.

Client ID: Enter the OpenID username.**Outgoing Proxy**: Enter the proxy address for the OpenID connection to use a proxy server.**Admin claim**: Enter a value for the admin role.**Provider URL**: Enter the web link for the API endpoint authentication. Format should be https://[insert URL]/.well-known/openid-configuration**Operator claim**: Enter a value for the operator role.**Require claim**: Enter the data that should be in the token.**Viewer claim**: Enter the value for the viewer role.**Remote user**: Enter a value to identify remote users. This assists to display the current user in the device's web interface.**Scopes**: Optional scopes that could be part of the token.**Client secret**: Enter the OpenID password **Save**: Click to save the OpenID values.**Enable OpenID**: Turn on to close current connection and allow device authentication from the provider URL.

Events

Rules

A rule defines the conditions that triggers 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**: 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*.

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 software can simplify integration of data and events produced in the device to systems which are not video management software (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.**BrokerHost**: 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.**HTTP proxy**: A URL with a maximum length of 255 bytes. You can leave the field empty if you don't want to use an HTTP proxy.**HTTPS proxy**: A URL with a maximum length of 255 bytes. You can leave the field empty if you don't want to use an HTTPS proxy.**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.

SIP

Settings

Session Initiation Protocol (SIP) is used for interactive communication sessions between users. The sessions can include audio and video.

SIP setup assistant: Click to set up and configure SIP step by step.**Enable SIP**: Check this option to make it possible to initiate and receive SIP calls.**Allow incoming calls**: Check this option to allow incoming calls from other SIP devices.
Call handling

- **Calling timeout**: Set the maximum duration of an attempted call if no one answers.
- **Incoming call duration**: Set the maximum time an incoming call can last (max 10 min).
- **End calls after**: Set the maximum time that a call can last (max 60 minutes). Select **Infinite call duration** if you don't want to limit the length of a call.
Ports

A port number must be between 1024 and 65535.

- **SIP port**: The network port used for SIP communication. The signaling traffic through this port is non-encrypted. The default port number is 5060. Enter a different port number if required.
- **TLS port**: The network port used for encrypted SIP communication. The signaling traffic through this port is encrypted with Transport Layer Security (TLS). The default port number is 5061. Enter a different port number if required.

- **RTP start port**: The network port used for the first RTP media stream in a SIP call. The default start port number is 4000. Some firewalls block RTP traffic on certain port numbers.

NAT traversal

Use NAT (Network Address Translation) traversal when the device is located on an private network (LAN) and you want to make it available from outside of that network.

Note

For NAT traversal to work, the router must support it. The router must also support UPnP®.

Each NAT traversal protocol can be used separately or in different combinations depending on the network environment.

- **ICE**: The ICE (Interactive Connectivity Establishment) protocol increases the chances of finding the most efficient path to successful communication between peer devices. If you also enable STUN and TURN, you improve the ICE protocol's chances.
- **STUN**: STUN (Session Traversal Utilities for NAT) is a client-server network protocol that lets the device determine if it is located behind a NAT or firewall, and if so obtain the mapped public IP address and port number allocated for connections to remote hosts. Enter the STUN server address, for example, an IP address.
- **TURN**: TURN (Traversal Using Relays around NAT) is a protocol that lets a device behind a NAT router or firewall receive incoming data from other hosts over TCP or UDP. Enter the TURN server address and the login information.

Audio and video

- **Audio codec priority**: Select at least one audio codec with the desired audio quality for SIP calls. Drag-and-drop to change the priority.

Note

The selected codecs must match the call recipient codec, since the recipient codec is decisive when a call is made.

- **Audio direction**: Select allowed audio directions.
- **H.264 packetization mode**: Select which packetization mode to use.
    - **Auto**: (Recommended) The device decides which packetization mode to use.
    - **None**: No packetization mode is set. This mode is often interpreted as mode 0.
    - **0**: Non-interleaved mode.
    - **1**: Single NAL unit mode.
- **Video direction**: Select allowed video directions.

Additional

- **UDP-to-TCP switching**: Select to allow calls to switch transport protocols from UDP (User Datagram Protocol) to TCP (Transmission Control Protocol) temporarily. The reason for switching is to avoid fragmentation, and the switch can take place if a request is within 200 bytes of the maximum transmission unit (MTU) or larger than 1300 bytes.
- **Allow via rewrite**: Select to send the local IP address instead of the router's public IP address.
- **Allow contact rewrite**: Select to send the local IP address instead of the router's public IP address.
- **Register with server every**: Set how often you want the device to register with the SIP server for the existing SIP accounts.
- **DTMF payload type**: Changes the default payload type for DTMF.
- **Max retransmissions**: Set the maximum number of times the device tries to connect to the SIP server before it stops trying.
- **Seconds until failback**: Set the number of seconds until the device tries to reconnect to the primary SIP server after it has failed over to a secondary SIP server.

Accounts

All current SIP accounts are listed under **SIP accounts**. For registered accounts, the colored circle lets you know the status.

● The account is successfully registered with the SIP server.

● There is a problem with the account. Possible reasons can be authorization failure, that the account credentials are wrong, or that the SIP server can't find the account.

The **peer to peer (default)** account is an automatically created account. You can delete it if you create at least one other account and set that account as default. The default account is always used when a VAPIX® Application Programming Interface (API) call is made without specifying which SIP account to call from.

Add account: Click to create a new SIP account.

- **Active**: Select to be able to use the account.
- **Make default**: Select to make this the default account. There must be a default account, and there can only be one default account.
- **Answer automatically**: Select to automatically answer an incoming call.
- **Prioritize IPv6 over IPv4**   : Select to prioritize IPv6 addresses over IPv4 addresses. This is useful when you connect to peer-to-peer accounts or domain names that resolve in both IPv4 and IPv6 addresses. You can only prioritize IPv6 for domain names that are mapped to IPv6 addresses.
- **Name**: Enter a descriptive name. This can, for example, be a first and last name, a role, or a location. The name is not unique.
- **User ID**: Enter the unique extension or phone number assigned to the device.
- **Peer-to-peer**: Use for direct calls to another SIP device on the local network.
- **Registered**: Use for calls to SIP devices outside the local network, through a SIP server.
- **Domain**: If available, enter the public domain name. It will be shown as part of the SIP address when calling other accounts.
- **Password**: Enter the password associated with the SIP account for authenticating against the SIP server.
- **Authentication ID**: Enter the authentication ID used for authenticating against the SIP server. If it is the same as the user ID, you don't need to enter the authentication ID.
- **Caller ID**: The name which is presented to the recipient of calls from the device.
- **Registrar**: Enter the IP address for the registrar.
- **Transport mode**: Select the SIP transport mode for the account: UPD, TCP, or TLS.
- **TLS version** (only with transport mode TLS): Select the version of TLS to use. Versions **v1.2** and **v1.3** are the most secure. **Automatic** selects the most secure version that the system can handle.
- **Media encryption** (only with transport mode TLS): Select the type of encryption for media (audio and video) in SIP calls.
- **Certificate** (only with transport mode TLS): Select a certificate.
- **Verify server certificate** (only with transport mode TLS): Check to verify the server certificate.
- **Secondary SIP server**: Turn on if you want the device to try to register on a secondary SIP server if registration on the primary SIP server fails.
- **SIP secure**: Select to use Secure Session Initiation Protocol (SIPS). SIPS uses the TLS transport mode to encrypt traffic.
- **Proxies**
    - **Proxy**: Click to add a proxy.
    - **Prioritize**: If you have added two or more proxies, click to prioritize them.
    - **Server address**: Enter the IP address of the SIP proxy server.
    - **Username**: If required, enter the username for the SIP proxy server.
    - **Password**: If required, enter the password for the SIP proxy server.
- **Video**
    - **View area**: Select the view area to use for video calls. If you select none, the native view is used.
    - **Resolution**: Select the resolution to use for video calls. The resolution affects the required bandwidth.
    - **Frame rate**: Select the number of frames per second for video calls. The frame rate affects the required bandwidth.
    - **H.264 profile**: Select the profile to use for video calls.

DTMF

╋ **Add sequence**: Click to create a new dual-tone multifrequency (DTMF) sequence. To create a rule that is activated by touch-tone, go to **Events > Rules**.**Sequence**: Enter the characters to activate the rule. Allowed characters: 0–9, A-D, #, and *.**Description**: Enter a description of the action to be triggered by the sequence.**Accounts**: Select the accounts that will use the DTMF sequence. If you choose **peer-to-peer**, all peer-to-peer accounts will share the same DTMF sequence.

ProtocolsSelect the protocols to use for each account. All peer-to-peer accounts share the same protocol settings.**Use RTP (RFC2833)**: Turn on to allow dual-tone multifrequency (DTMF) signaling, other tone signals and telephony events in RTP packets.**Use SIP INFO (RFC2976)**: Turn to include the INFO method to the SIP protocol. The INFO method adds optional application layer information, generally related to the session.

Test call

SIP account: Select which account to make the test call from.**SIP address**: Enter a SIP address and click ☏ to make a test call and verify that the account works.

Access list

Use access list: Turn on to restrict who can make calls to the device.
Policy:

- **Allow**: Select to allow incoming calls only from the sources in the access list.
- **Block**: Select to block incoming calls from the sources in the access list.

╋ **Add source**: Click to create a new entry in the access list.**SIP source**: Type the caller ID or SIP server address of the source.

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 without testing**: 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 passes. **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.

Use tool: Click 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 to administrators.**Retention time**: Select how long to keep recordings to limit the amount of old recordings or comply with data storage regulations. When the SD card is full, it deletes old recordings before their retention time has passed.**Tools**

- **Check**: Check for errors on the SD card.
- **Repair**: Repair errors in the file system.
- **Format**: Format the SD card to change the file system and erase all data. You can only format the SD card to the ext4 file system. 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. This erases all data stored on the SD card. Any new data you store on the SD card will be encrypted.
- **Decrypt**: Use this tool to format the SD card without encryption. This erases all data stored on the SD card. Any new data you store on the SD card will not be encrypted.
- **Change password**: Change the password required to encrypt the SD card.

Use tool: Click 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.

Add stream profile: 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 29* for a description of this setting.**Frame rate**: See *Stream on page 29* for a description of this setting.**Compression**: See *Stream on page 29* for a description of this setting.**Zipstream** : See *Stream on page 29* for a description of this setting.**Optimize for storage** : See *Stream on page 29* for a description of this setting.**Dynamic FPS** : See *Stream on page 29* for a description of this setting.**Dynamic GOP** : See *Stream on page 29* for a description of this setting.**Mirror** : See *Stream on page 29* for a description of this setting.**GOP length** : See *Stream on page 29* for a description of this setting.**Bitrate control**: See *Stream on page 29* for a description of this setting.**Include overlays** : Select what type of overlays to include. See *Overlays on page 30* for information about how to add overlays.**Include audio** : See *Stream on page 29* for a description of this setting.

ONVIF

ONVIF accounts

50

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 account, you automatically enable ONVIF communication. Use the account name and password for all ONVIF communication with the device. For more information see the Axis Developer Community at *axis.com*.

Add accounts: Click to add a new ONVIF account.**Account**: Enter a unique account name.**New password**: Enter a password for the account. 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 accounts.
- **Operator**: Has access to all settings except:
  - All **System** settings.
  - Adding apps.
- **Media account**: Allows access to the video stream only.

The context menu contains:**Update account**: Edit the account properties.**Delete account**: Delete the account. You can't delete the root account.

ONVIF media profiles

An ONVIF media profile consists of a set of configurations that you can use to change media stream settings. You can create new profiles with your own set of configurations or use preconfigured profiles for a quick setup.

Add media profile: Click to add a new ONVIF media profile.**Profile name**: Add a name for the media profile.**Video source**: Select the video source for your configuration.
- **Select configuration**: Select a user-defined configuration from the list. The configurations in the drop-down list correspond to the device's video channels, including multiviews, view areas and virtual channels.

Video encoder: Select the video encoding format for your configuration.
- **Select configuration**: Select a user-defined configuration from the list and adjust the encoding settings. The configurations in the drop-down list act as identifiers/names of the video encoder configuration. Select user 0 to 15 to apply your own settings, or select one of the default users if you want to use predefined settings for a specific encoding format.

Note

Enable audio in the device to get the option to select an audio source and audio encoder configuration.

Audio source ⓘ : Select the audio input source for your configuration.
- **Select configuration**: Select a user-defined configuration from the list and adjust the audio settings. The configurations in the drop-down list correspond to the device's audio inputs. If the device has one audio input, it's user0. If the device has several audio inputs, there will be additional users in the list.

Audio encoder ⓘ : Select the audio encoding format for your configuration.
- **Select configuration**: Select a user-defined configuration from the list and adjust the audio encoding settings. The configurations in the drop-down list act as identifiers/names of the audio encoder configuration.

Audio decoder ⓘ : Select the audio decoding format for your configuration.
- **Select configuration**: Select a user-defined configuration from the list and adjust the settings. The configurations in the drop-down list act as identifiers/names of the configuration.

Audio output ⓘ : Select the audio output format for your configuration.
- **Select configuration**: Select a user-defined configuration from the list and adjust the settings. The configurations in the drop-down list act as identifiers/names of the configuration.

Metadata: Select the metadata to include in your configuration.
- **Select configuration**: Select a user-defined configuration from the list and adjust the metadata settings. The configurations in the drop-down list act as identifiers/names of the metadata configuration.

PTZ ⓘ : Select the PTZ settings for your configuration.
- **Select configuration**: Select a user-defined configuration from the list and adjust the PTZ settings. The configurations in the drop-down list correspond to the device's video channels with PTZ support.

Create: Click to save your settings and create the profile.**Cancel**: Click to cancel the configuration and clear all settings.**profile_x**: Click on the profile name to open and edit the preconfigured profile.

Detectors

Camera tampering

The camera tampering detector generates an alarm when the scene changes, for example, when 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.

PIR sensor

The PIR sensor measures IR light radiating from objects in its field of view.**Sensitivity level**: Adjust the level to a value from 0–100, where 0 is the least sensitive and 100 is the most sensitive.

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.

Power settings

Power status

Shows power status information. Information varies depending on the product.

Power profiles

Select a power profile according to the temperature range that the device will be used in:
- **Full power (default)**: The product can be used in low temperatures, but will consume more power.
- **Low power**: The product can not be used in low temperatures, but will consume less power.

Note

The low power profile turns off the heater or heaters to save power.

Power settings

Delayed shutdown ⓘ : Turn on if you want to set a delay time before the power turns off.**Delay time** ⓘ : Set a delay time between 1 and 60 minutes.**Power saving mode** ⓘ : Turn on to put the device into power saving mode. When you turn on power saving mode, the IR illumination range reduces.**Set power configuration** ⓘ : Change the power configuration by selecting a different PoE class option. Click **Save and restart** to save the change.

Note

> If you set the power configuration to PoE class 3, we recommend you select **Low power profile** if your device has that option.

Dynamic power mode: Turn on to reduce power consumption when the device is inactive. ⓘ

Power meter

Energy usage

Shows the current power usage, average power usage, maximum power usage, and power consumption over time. ⋮ The context menu contains:
- **Export**: Click to export the chart data.

Indicators

Indicators

Tally LED: Use the tally LED to indicate when someone looks at the video stream.**On**: The LED is always on, even if no one streams video from the device.**Off**: The LED is always off, even if someone streams video from the device.**Auto**: The LED is on when someone streams video from the device.

Accessories

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 the web interface.

PortName: 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 ⌐ for 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 VDC.

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.

Logs

Reports and logs

Reports
- **View the device server report**: View 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**: 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**: 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.
- Axis
- RFC 3164
- RFC 5424

Protocol: Select the protocol to use:
- UDP (Default port is 514)
- TCP (Default port is 601)
- TLS (Default port is 6514)

Port: Edit the port number to use a different port.**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

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 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
> - DNS server IP address

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 software is digitally signed to ensure that you only install verified software on your device. This further increases the overall minimum cybersecurity level of Axis devices. For more information, see the white paper "Axis Edge Vault" at *axis.com*.

AXIS OS upgrade: Upgrade to a new AXIS OS version. New releases can contain improved functionality, bug fixes, and completely new features. We recommend you to always use the latest AXIS OS 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 AXIS OS 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 AXIS OS 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 AXIS OS version.

AXIS OS rollback: Revert to the previously installed AXIS OS version.

Troubleshoot

Reset PTR : Reset PTR if for some reason the **Pan**, **Tilt**, or **Roll** settings aren't working as expected. The PTR motors are always calibrated in a new camera. But calibration can be lost, for example, if the camera loses power or if the motors are moved by hand. When you reset PTR, the camera is re-calibrated and returns to its factory default position.**Calibration** : Click **Calibrate** to recalibrate the pan, tilt, and roll motors to their default positions.**Ping**: To check if the device can reach a specific address, enter the hostname or IP address of the host you want to ping and click **Start.Port check**: To verify connectivity from the device to a specific IP address and TCP/UDP port, enter the hostname or IP address and port number you want to check and click **Start.Network trace**

Important

> A network trace file might contain sensitive information such as 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**.

Learn more

Capture modes

Capture mode defines the maximum resolution and maximum frame rate available in the Axis product. The capture mode also affects light sensitivity. A capture mode with a high maximum frame rate has reduced light sensitivity and vice versa.

Which capture mode to choose depends on the requirements of frame rate and resolution for the specific surveillance setup. For specifications about available capture modes, see the product's datasheet at *axis.com*.

Overlays

Note

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

Note

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

Note

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

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

Streaming and storage

Video compression formats

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

Motion JPEG

Note

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

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

The Motion JPEG stream uses considerable amounts of bandwidth, but provides excellent image quality and access to every image contained in the stream.

H.264 or MPEG-4 Part 10/AVC

Note

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

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

H.265 or MPEG-H Part 2/HEVC

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

Note

- H.265 is licensed technology. The Axis product includes one H.265 viewing client license. Installing additional unlicensed copies of the client is prohibited. To purchase additional licenses, contact your Axis reseller.
- Most web browsers don't support H.265 decoding and because of this the camera doesn't support it in its web interface. Instead you can use a video management system or application supporting H.265 decoding.

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

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

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

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

Bitrate control

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

Variable bitrate (VBR)
Variable bitrate allows the bandwidth consumption to vary depending on the level of activity in the scene. The more activity, the more bandwidth you need. With variable bitrate you are guaranteed constant image quality, but you need to make sure you have storage margins.
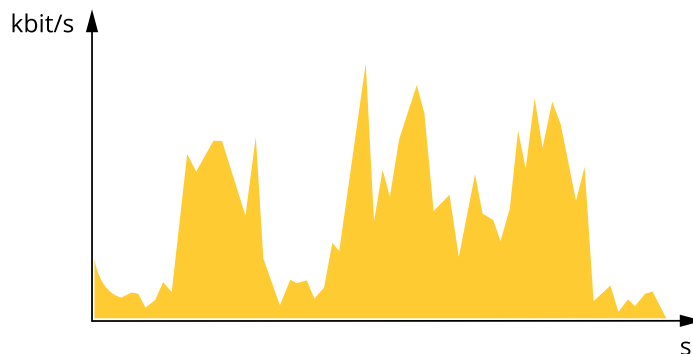
Maximum bitrate (MBR)
Maximum bitrate lets you set a target bitrate to handle bitrate limitations in your system. You might see a decline in image quality or frame rate as the instantaneous bitrate is kept below the specified target bitrate. You can choose to prioritize either image quality or frame rate. We recommend that you configure the target bitrate to a higher value than the expected bitrate. This gives you a margin in case there is a high level of activity in the scene.
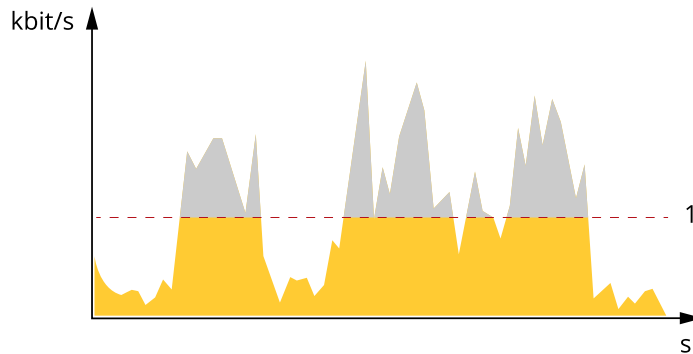
1   Target bitrate

Average bitrate (ABR)

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

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

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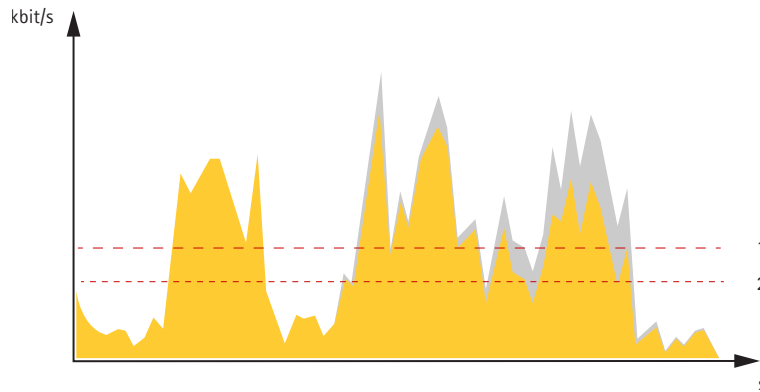
1   Target bitrate
2   Actual average bitrate

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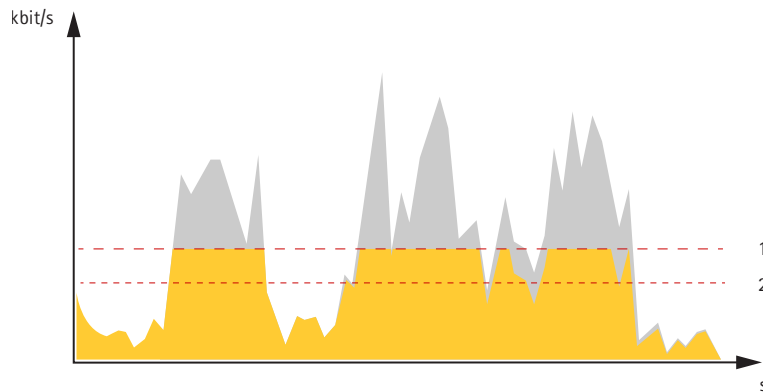
1   Target bitrate
2   Actual average bitrate

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.

Autotracking

With autotracking, the camera automatically zooms in on and tracks moving objects, for example a vehicle or a person. You can manually select an object to track, or set up trigger areas and let the camera detect moving objects. The application is best suited for open areas with no obscuring objects and where movement is unusual. When the camera doesn't track an object, it returns to its connected preset position.

Important
- Autotracking is designed for areas with a limited amount of movement.

Clean your device

You can clean your device with lukewarm water.

NOTICE

- Harsh chemicals can damage the device. Don't use chemicals such as window cleaner or acetone to clean your device.

- Avoid cleaning in direct sunlight or elevated temperatures, since this can cause stains.

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

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

3. To avoid stains, dry the device with a clean, nonabrasive cloth.

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 66*.

3. Keep the control button pressed for 15–30 seconds until the status LED indicator flashes amber.

4. Release the control button. The process is complete when the status LED indicator turns green. If no DHCP server is available on the network, the device IP address will default to one of the following:

   - **Devices with AXIS OS 12.0 and later:** Obtained from the link-local address subnet (169.254.0.0/16)

   - **Devices with AXIS OS 11.11 and earlier:** 192.168.0.90/24

5. Use the installation and management software tools to assign an IP address, set the password, and access the device.

   The installation and management software tools are available from the support pages on *axis.com/support*.

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

AXIS OS options

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

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

Check the current AXIS OS version

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

To check the current AXIS OS version:

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

2. Under **Device info**, see the AXIS OS version.

Upgrade AXIS OS

Important

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

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

When you upgrade the device with the latest AXIS OS version in the active track, the product receives the latest functionality available. Always read the upgrade instructions and release notes available with each new release before you upgrade. To find the latest AXIS OS version and the release notes, go to *axis.com/support/device-software*.

1. Download the AXIS OS file to your computer, available free of charge at *axis.com/support/device-software*.

2. Log in to the device as an administrator.

3. Go to **Maintenance > AXIS OS upgrade** and click **Upgrade**.

When the upgrade has finished, the product restarts automatically.

You can use AXIS Device Manager to upgrade multiple devices at the same time. Find out more at *axis.com/products/axis-device-manager*.

Technical 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 AXIS OS

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

Problems setting the IP address

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 root account is lost, the device must be reset to the factory default settings. See *Reset to factory default settings on page 62*.

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 Camera Station Edge: free of charge, ideal for small systems with basic surveillance needs.
- AXIS Camera Station 5: 30-day trial version free of charge, ideal for small to mid-size systems.
- AXIS Camera Station Pro: 90-day trial version free of charge, ideal for small to mid-size systems.

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

Problems with streaming

Multicast H.264 only accessible by local clients	Check if your router supports multicasting, or if you need to configure the router settings between the client and the device. You might need to increase the TTL (Time To Live) value.
No multicast H.264 displayed in the client	Check with your network administrator that the multicast addresses used by the Axis device are valid for your network.Check with your network administrator to see if there is a firewall that prevents viewing.
Poor rendering of H.264 images	Ensure that your graphics card uses the latest driver. You can usually download the latest drivers from the manufacturer's website.
Color saturation is different in H.264 and Motion JPEG	Modify the settings for your graphics adapter. Go to the adapter's documentation for more information.
Lower frame rate than expected	- See *Performance considerations on page 64*. - 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.

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.

AXIS V5938 PTZ Network Camera

Troubleshooting

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 clients or unicast H.264/H.265/AV1 clients affects the bandwidth.

- Simultaneous viewing of different streams (resolution, compression) by different clients affects both frame rate and bandwidth.

  Use identical streams wherever possible to maintain a high frame rate. Stream profiles can be used to ensure that streams are identical.

- Accessing video streams with different codecs simultaneously affects both frame rate and bandwidth. For optimal performance, use streams with the same codec.

- Heavy usage of event settings affects the product's CPU load which in turn affects the frame rate.

- Using HTTPS may reduce frame rate, in particular if streaming Motion JPEG.

- Heavy network utilization due to poor infrastructure affects the bandwidth.

- Viewing on poorly performing client computers lowers perceived performance and affects frame rate.

- Running multiple AXIS Camera Application Platform (ACAP) applications simultaneously may affect the frame rate and the general performance.
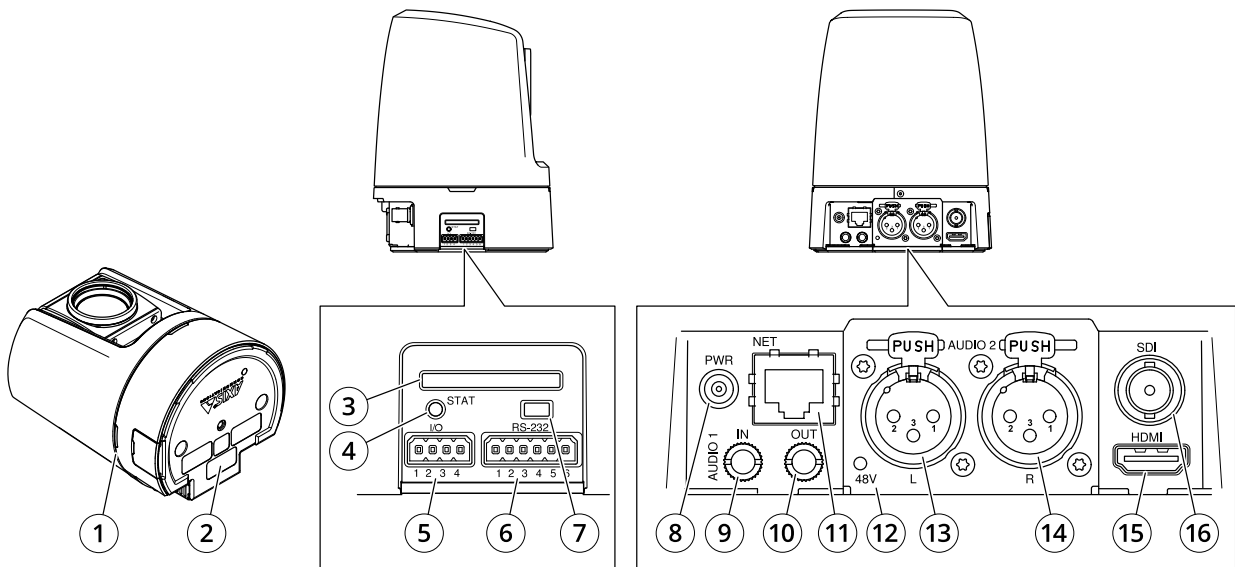
Contact support

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

Specifications

Product overview

1   Tally LED (3x)
2   Part number (P/N) & Serial number (S/N)
3   SD card slot (SDHC)
4   Status LED indicator
5   I/O connector
6   VISCA connector (RS-232)
7   Control button
8   Power connector
9   3.5 mm, unbalanced audio in
10   3.5 mm, unbalanced audio out
11   Network connector
12   Microphone phantom power LED (XLR)
13   XLR, balanced audio in (left)
14   XLR, balanced audio in (right)
15   HDMI connector
16   BNC connector (SDI)

LED indicators

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

Microphone power LED	Indication
Unlit	Phantom power off.
Blue	Phantom power on.

Note

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

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

SD card slot

NOTICE

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

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

This device supports SD/SDHC/SDXC cards.

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

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

Buttons

Control button

The control button is used for:

- Resetting the product to factory default settings. See *Reset to factory default settings on page 62*.

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

Connectors

BNC connector

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

⚠CAUTION

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

HDMI connector

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

Specifications

Network connector

RJ45 Ethernet connector.

Audio connector

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

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


Audio input

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

Audio output

1 Tip	2 Ring	3 Sleeve
Stereo unbalanced line, "left"	Stereo unbalanced line, "right"	Ground

XLR connector

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

- **Right** – 3-pin XLR connector for balanced audio input.
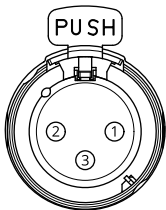
Pin	1	2	3
Function	Ground	Balanced Microphone Hot (+) In	Balanced Microphone Cold (–) In

I/O connector

Use the I/O connector with external devices in combination with, for example, motion detection, event triggering, and alarm notifications. In addition to the 0 VDC reference point and power (12 V DC output), the I/O connector provides the interface to:
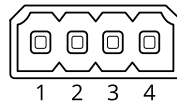
Digital input – For connecting devices that can toggle between an open and closed circuit, for example PIR sensors, door/window contacts, and glass break detectors.

Specifications

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.

4-pin terminal block

Function	Pin	Notes	Specifications
DC ground	1		0 VDC
DC output	2	Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	12 VDC Max load = 25 mA
Digital Input	3	Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 VDC
Digital Output	4	Internally connected to pin 1 (DC ground) when active, and floating (unconnected) when inactive. If used with an inductive load, e.g., a relay, connect a diode in parallel with the load, to protect against voltage transients.	0 to max 30 VDC, open drain, 100 mA

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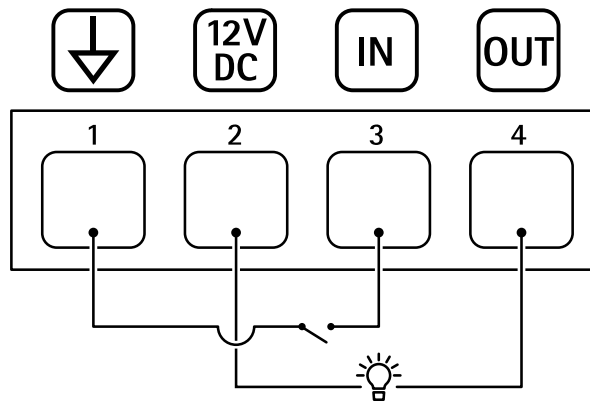
1   DC ground
2   DC output 12 V, max 25 mA
3   Digital input
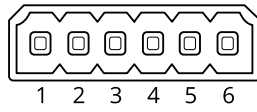4   Digital output

Power connector

DC connector. Use the supplied adapter.

VISCA connector (RS–232)

6-pin terminal block for the RS232 serial interface. This is used to control the camera using the VISCA protocol.

Specifications

Function	Pin	Notes
TXD1	1	VISCA input
RXD1	2	
GND	3	Ground
TXD2	4	VISCA output
RXD2	5	
GND	6	Ground