AXIS OS

User manual

Table of Contents

Device settings 5
Status 5
..... 6
..... 7
Sequences 7
Device 9
I/Os and relays 9
Alarms 10
Power monitoring 10
Peripherals 11
Readers 11
LED profiles 12
Wireless locks 12
Expansion I/O module 12
Sensors 13
Upgrade 14
Advanced 14
Door override 14
Video 15
Installation 17
Fusion alignment 22
Image 22
Stream 28
Overlays 31
View areas 33
Night mode 33
Privacy masks 35
Picture in picture 35
Air quality monitor 35
Dashboard 35
Settings 40
Statistics 43
Communication 43
VMS calls 43
Contact list 43
Recipients 43
Calls 47
Display 48
Configuration 48
Display settings 49
Pages 51
Clock 52
General 52
Screensaver 53
Thermometry 53
Temperature reading 53
Temperature detection 54
Deviation detection 55
Radar 57
Settings 58
Stream 60
Map calibration 62
Lanes 62

Exclusion zones 63
Scenarios 64
Overlays 65
Dynamic LED strip 67
Radar PTZ autotracking 68
Autocalibration 68
PTZ 69
PTZ channels 69
Preset positions 70
Guard tours 70
Limits 72
Motion 73
OSDI zones 73
Orientation aid 74
Gatekeeper 74
Control queue 74
Settings 74
Reader 75
Connection 75
Output format 77
Chip types 77
PIN 78
Entry list 78
Audio 79
AXIS Audio Manager Edge 79
Device settings 79
Stream 80
Audio clips 80
Listen and record 80
Audio enhancement 80
Speaker test 81
Sources 81
Light 82
Overview 82
Profiles 83
Recordings 85
Media 86
Cellular routing 86
Apps 88
System 88
Time and location 88
WLAN 90
Configuration check 90
Network 91
Network ports 95
Modem 95
Security 96
Accounts 102
Events 106
MQTT 110
SIP 113
Storage 118
Stream profiles 122
ONVIF 123
Detectors 124
Z-Wave 125

Video input 129
Video out 129
Power settings 132
Power meter 132
Indicators 132
Accessories 133
Edge-to-edge 134
Logs 135
Plain config 136
Maintenance 137
Maintenance 137
Troubleshoot 138
Analytics 139
AXIS Object Analytics 139
Autotracking 139
AXIS Image Health Analytics 141
AXIS Audio Analytics 141
..... 142
AXIS Live Privacy Shield 142
Metadata visualization 142
..... 142
Metadata configuration 143

Device settings

This is an overview of all features and settings available in the web interface of devices with AXIS OS.

Note

No single device contains all settings listed here.

To reach the device's web interface, type the device's IP address in a web browser. For more information, see *AXIS OS Knowledge base* or the user manual for your device at *help.axis.com*.

: Switch between **Device settings** and the **Analytics** overview.

: Show or hide the main menu.

Help: Access product help, release notes and lifecycle guide.

Information:

- **About**: View device information, including AXIS OS version and serial number.
- **Legal**: View information about cookies and licenses.
- **Feedback**: Share any feedback to help us improve your user experience.
- **Analytics data**: Accept to share non-personal browser data.
- **Device server report**: Download the device server report.

Administrator:

- : Information about the user who is logged in.
- : Change the language.
- : Set light theme or dark theme.
- **Change account**: Log out from the current account and log in to a new account.
- **Log out**: Log out from the current account.

Status

Audio system info

This information is only shown for devices that belong to an AXIS Audio Manager Edge site.

AXIS Audio Manager Edge: Launch AXIS Audio Manager Edge.

AXIS Image Health Analytics

Shows the status of the preinstalled application AXIS Image Health Analytics and if the application has detected any issues.

Go to apps: Go to the **Apps** page where you can manage your installed applications.

Open application: Open AXIS Image Health Analytics in a new browser tab.

Cellular network

Shows the signal strength of the cellular network as well as the IP address that your back box has on the cellular network. If you are not connected to a cellular network while staging the back box, no IP address will be displayed.

Modem settings: Click to go to the modem page where you can view and change the settings.

Configuration

Shows the setup assistant configurations, including installation type, lens selection, installation focus, PTZ information.

Start setup assistant: Configure the setup assistant.

View setup assistant: View and update the setup assistant.

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.

Device info

Shows information about the device, 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.

Door connection

Door: Shows the status of connected doors.

Locate device

Shows the locate device information, including serial number and IP address.

Locate device: Plays a sound that helps you identify the speaker. For some products, the device will flash a LED.

Network ports

Shows the status of network ports and power information including allocated power and total PoE consumption.

Network ports settings: Click to go to the Network ports page where you can change the settings.

Ongoing recordings

Shows ongoing recordings and their designated storage space.

Recordings: View ongoing and filtered recordings and their source. For more information, see *Recordings, on page 85*

 Shows the storage space where the recording is saved.

Power status

Shows power status information, including current power, average power, and max power.

Power settings: View and update the power settings for the device. Takes you to the Power settings page where you can change the power 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.

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.

Speaker test

Shows whether the speaker has been calibrated or not.

Speaker test: Calibrate the speaker. Takes you to the **Speaker test** page where you can do the calibration and run the speaker test.

Storage

Shows the storage status and information including free space and disk temperature.

Storage settings: Click to go to the Onboard storage page where you can change the settings.

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, as well as the PTP status.

NTP settings: View and update the NTP settings. Takes you to the **Time and location** page where you can change the NTP settings.

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.

Sequences

Monitor

Shows information about the sequence.

USB

To activate USB functionality, turn on USB ports in **System > Accessories** and restart the device.

Allow USB input: Turn on to let the device use the USB input.

Invert joystick axes: Select if you want to invert the joystick axes:

- **Horizontal:** X axis
- **Vertical:** Y axis

Always play audio when a single segment is selected: Turn on to play audio when a single segment is selected.

Sequences

Important

To avoid problems with multi-stream playbacks, follow the recommendations in the web interface.

Add sequence: Click to add a sequence.

Name: Enter a name for the sequence.

: Click to select how many sources you want to display.

: Click to add one more .

: Click to play the sequence.

The context menu contains:

Edit sequence

Delete sequence

Set as default sequence

Fallback

Add fallback image: Click to add an image that can be displayed if the camera stream is lost.

Device

I/Os and relays

Input

- **Name**: Edit the text to rename the port.
- **Direction**: Indicates that it is an input port.
- **Normal state**: Click  for open circuit, and  for closed circuit.
- **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.
  - To use parallel first connection, select **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor**.
  - To use serial first connection, select **Serial first connection** and select a resistor value from the **Resistor values** drop-down list.

Output.

- **Name**: Edit the text to rename the port.
- **Direction**: Indicates that it is an output port.
- **Normal state**: Click  for open circuit, and  for closed circuit.
- **Output state**: Turn on to activate the output.

I/O:

- **Name**: Edit the text to rename the port.
- **Direction**: Click  or  to configure it as input or output.
- **Normal state**: Click  for open circuit, and  for closed circuit.
- **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. It appears only when the port is configured as input.
  - To use parallel first connection, select **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor**.
  - To use serial first connection, select **Serial first connection** and select a resistor value from the **Resistor values** drop-down list.
- **Output state**: Turn on to activate the output. It appears only when the port is configured as output.

Relays

- **Name**: Edit the text to rename the relay.
- **Direction**: Indicates that it is an output relay.
- **Relay**: Turn on or off the relay.
- **Toggle port URL**: Shows the URLs to activate and deactivate the relay through the VAPIX® Application Programming Interface.

Alarms

Device motion: Turn on to trigger an alarm in your system when it detects a movement of the device.

Casing open: Turn on to trigger an alarm in your system when it detects an open door controller case. Turn off this setting for barebone door controllers.

External tamper: Turn on to trigger an alarm in your system when it detects an external tamper. For example, when someone opens or closes the external cabinet.

- **Normal state**: Click  for open circuit, and  for closed circuit.
- **Supervised input**: Turn on to monitor the input state and configure the end-of-line resistors.
  - To use parallel first connection, select **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor**.
  - To use serial first connection, select **Serial first connection** and select a resistor value from the **Resistor values** drop-down list.

Power monitoring

Main unit

- **Power in**: Shows the status of power in including PoE, DC, DC Door 1–4, and DC Door 5–8 if applicable.
- **Power out**: Shows the power out of all RS485 and all relays.
- **Temperature**: Shows the core temperature of the device.
- **Door 1–4**: Shows the status and power usage of DC input Door 1–4 including power usage of all relays, all readers, and all REX.
- **Door 5–8**: Shows the status and power usage of DC input Door 5–8 including power usage of all relays, all readers, and all REX.

Connected devices: Shows the status, name, address, and the power usage of the connected devices including power usage of all relays, all RS485, and all AUX.

Peripherals

Readers

Add: Click to add a reader.

Axis network readers: You can add up to 16 Bluetooth readers to the controller, no license required.

- **Name**: Enter a name for the reader.
- **Reader**: Select a reader from the drop-down list.
- **IP address**: Enter the IP address of the reader manually.
- **Username**: Enter the username of the reader.
- **Password**: Enter the password of the reader.
- **Ignore server certificate verification**: Turn on to ignore verification.
- **I/O ports and relays**: Expand to configure I/O ports and relays.
  - **Port**: Shows the name of the port.
  - **Direction**: Indicates that it is an input or output port.
  - **Normal state**: Click for open circuit, and for closed circuit.

Axis network intercoms (Need to reconfigure in AXIS Camera Station)

- **Name**: Enter a name for the reader.
- **Reader**: Select a reader from the drop-down list.
- **IP address**: Enter the IP address of the reader manually.
- **Username**: Enter the username of the reader.
- **Password**: Enter the password of the reader.
- **Ignore server certificate verification**: Turn on to ignore verification.

AXIS License Plate Verifier (Need to reconfigure in AXIS Camera Station)

- **Name**: Enter a name for the reader.
- **API-key**: Enter the API key.
- **Generate**: Click to generate the API key.
- **Copy API-key**: Click to copy the API key to save it in a safe place.

AXIS Barcode Reader (Need to reconfigure in AXIS Camera Station)

- **Name**: Enter a name for the reader.
- **API-key**: Enter the API key.
- **Generate**: Click to generate the API key.
- **Copy API-key**: Click to copy the API key to save it in a safe place.

Edit: Select a reader and click **Edit** to make changes for the selected reader.

Delete: Select the readers and click **Delete** to delete the selected readers.

LED profiles

Your OSDP reader has customizable LED profiles:

- **Access granted**: Activates when a user's credential check is successful and they're authorized to enter.
- **Access denied**: Activates when a user's credential check is unsuccessful and they aren't authorized to enter.
- **Alarm**: Triggered by a forced door or an external trigger. This is different than the **Door open too long** alarm.
- **Door locked**: Activates when the lock reengages after an authorized entry.
- **Door unlocked**: Activates when the lock is released and the door can be opened.
- **Door open too long**: Triggered when the door is held open longer than the specified amount of time.
- **Idle**: Resting state of the reader.
- **Require PIN**: Activates in a multifactor authentication system when you need to enter your second authentication factor, such as your PIN.

Note

You can only customize the sound and light behaviors for certain profiles.

Wireless locks

You can connect up to 16 ASSA ABLOY Aperio wireless locks using the AH30 Communication Hub. A license is required for the wireless lock.

Note

You must install the AH30 Communication Hub on the secure side.

Connect communication hub: Click to connect the wireless locks.

Expansion I/O module

You can connect up to 16 AXIS A9910 to one AXIS A9210 to support 128 I/Os, 64 relays and 64 Modbus sensors. The max distance from AXIS A9210 to the last AXIS A9910 is 1000 m.

Add encryption key: Click to set up an encryption key to ensure encrypted communication.

Add: Click to add an expansion module.

- **Name**: Enter a name for the expansion module.
- **RS485 port**: Select the port to use.
- **Address**: Select the address that the expansion module is connected to.

Edit: Select an expansion module and click to edit.

Select an I/O port and click **Edit**:

- **Name**: Edit the text to rename the port.
- **Direction**: Click  or  to configure it as input or output.
- **Normal state**: Click  for open circuit, and  for closed circuit.
- **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. It appears only when the port is configured as input.
  - To use parallel first connection, select **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor**.
  - To use serial first connection, select **Serial first connection** and select a resistor value from the **Resistor values** drop-down list.
- **Output state**: Turn on to activate the output. It appears only when the port is configured as input.

Select a relay and click **Edit**:

- **Name**: Edit the text to rename the relay.
- **Direction**: Indicates that it is an output relay.
- **Relay**: Turn on or off the relay.
- **Toggle port URL**: Shows the URLs to activate and deactivate the relay through the VAPIX® Application Programming Interface.

Upgrade: Click to upgrade the expansion module software. You can choose to upgrade to the version bundled with the door controller or upload a version of your choice.

- **Use bundled device software**: Turn on to upgrade to the version bundled with the device.
- **Select devices**: Select the expansion I/O modules you want to upgrade.

Sensors

Shows an overview of your connected sensors to AXIS A9210. You can connect up to 8 Modbus sensors directly on the RS485 port, or extend to 16 AXIS A9910 to have 64 Modbus sensors on a single AXIS A9210.

Add: Click to add a sensor.

Name: Enter a name for the sensor.
Sensor: Select the device the sensor is connected to.
RS485 port: Select the port the sensor is connected to.
Address: Enter the address of the sensor. If multidrop is used, enter the unique address between 1–247.
Type:

- Select **Custom**.
  - **Export template**: Click to download a JSON file. You can edit the file and upload it to the device later.
  - **Select configuration file**: Click to select a configuration file or drag it. You can edit, copy, download or print the configuration file.
- Select **Hugo** or **Tibbo**.
  - **Read data**: Set how often to read data from the sensor.
  - **Thresholds**: Set threshold values for available sensor features such as temperature, humidity, dew point, atmospheric pressure, or luminance.

Save: Click to save the configuration.

In the list of sensors:

- **Name:** Edit the text to rename the sensor.
- **Device/Port:** The Modbus ID and port number where the sensor is connected.
- **Type:** The type of measurement or function performed by the sensor, such as temperature, humidity, or luminance.
- **Model:** The model name of the sensor.
- **Last value:** The most recent reading from the sensor.
- **Last event:** The reason for the last triggered event, such as above or below the set limit for the selected parameter.
- **Status:** Indicates whether the sensor is currently online or offline.

Upgrade

Upgrade readers: Click to upgrade the reader's software. You can only upgrade supported readers when they are online.

Upgrade converters: Click to upgrade the converter's software. You can only upgrade supported converters when they are online.

Advanced

Door override

Important

It takes direct control of the door relays and overrides the relay configuration in AXIS Camera Station. Only turn on this setting if Axis support has instructed you to do so.

I understand: Click to make it possible to turn on door override.

Door override: Click to turn on door override.

Door relays: Click **Lock**, **Unlock**, or **Access** to lock the door, unlock the door, or grant access.

Available relays: Click **Activate** or **Deactivate** to activate or deactivate the relay.

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. Enable groups of onscreen controls to make the settings in each group available when users right-click the live stream in the video management software.

- **Predefined controls**: Lists the default onscreen controls.
- **Custom controls**: Click **Add custom control** to create customized onscreen controls.

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 autotracking settings. More settings are available if you click the icon from **Analytics > Autotracking**.

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.

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 expanded full screen. Click again to exit the expanded full screen mode.

Click to show the live video stream in full screen. Press Esc to exit full screen mode.

Installation

Camera: Select the sensor you want to view in the drop-down menu. The number after **Camera** indicates the individual sensors.

Group view: Select to show all sensors next to each other.

Quad view: Select to show all sensors next to each other.

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.

Leveling assistant

Overlay: Turn on to add an overlay to assist you when you want to level the image.

Buzzer: Turn on to hear the buzzer when you want to level the image.

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

Pan: Use the slider to adjust the pan angle.

Tilt: Use the slider to adjust the tilt angle.

Troubleshoot: Click to get to **Reset pan and tilt**.

Close-up reach: Click to show the close-up reach areas.

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.

Autofocus: 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.

Roll: Use the slider to adjust the angle to make the image horizontal.

Preset Position: A preset position is a saved position you can use to quickly move the camera view to a set position. With a preset position, you can save pan, tilt, roll, zoom, and focus positions. You can use the saved preset positions in the live view.



Add new preset: Create a new preset position. You can add up to five PTRZ preset positions.

- **Name**: Type a name for the preset position.
- **Description**: Add a description for the preset position.



: Click to delete a preset position.

Load selected preset: Select a preset position and click to move the camera to the preset position.

Spot focus: Use to set the focus to a fixed area in the center of the image.

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.

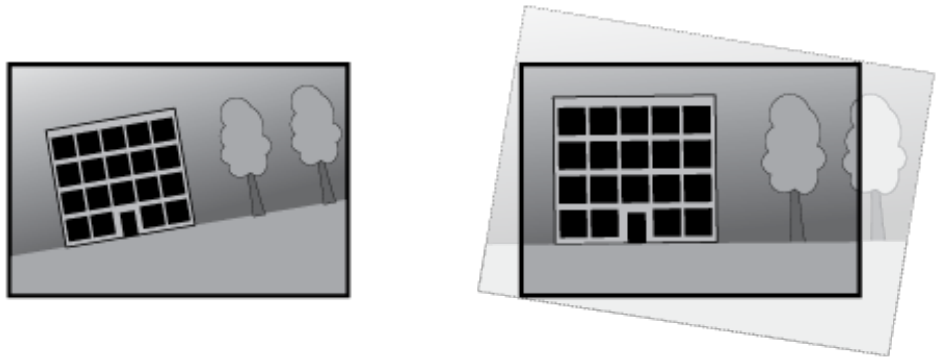
Stabilizer margin: Use the slider to adjust the size of the stabilizer margin, which determines the level of vibration to stabilize. If the product is mounted in an environment with a lot of vibration, move the slider towards **Max**. As a result, a smaller scene is captured. If the environment has less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

Horizon straightening

Horizon straightening compensates for any tilt of the camera, which would otherwise bend the horizon. It provides an image that is perceived to be straight and aligned with the horizon.

Horizon position: Use the slider to move the yellow center line to the position of the horizon. You can also move the center line directly in the live view image.

Stretch: Turn on to stretch the image in order to fit the whole window.

Zoom synchronization

Shows whether zoom synchronization between visual and thermal channels is turned on or turned off.

Traffic camera installation assistance

Traffic camera installation assistance is a tool you can use to get camera setting recommendations based on your specific installation environment.

Surveillance mode

Select a surveillance mode to define the primary purpose of your traffic camera:

- **License plate capture**: Capture clear images of license plates.
- **Traffic overview**: Monitor overall traffic flow and conditions.

Capture settings

Provide the following information to get accurate recommendations for your camera settings:

- **Camera height**: Distance between the camera and the ground.
- **Road distance**: Distance between the camera and the middle of the road.
- **Max car speed**: Maximum speed of cars on the road.
- **Automatic distance**: Turn on to automatically calculate the distance between the camera and cars on the road.
- **Car distance**: Distance between the camera and cars on the road.

Installation overview

Displays a visual representation of your camera's position and angle, indicating if any adjustments are needed.

- **Vertical angle**: Tilt position angle.
- **Horizontal angle**: Pan position angle.
- **Roll angle**: Rotation angle.
- **Car distance**: Recommended distance between the camera and moving vehicles.

Image settings

Shows you the recommended image settings for optimal performance. Apply the recommended settings by leaving the boxes checked. To keep your current settings, uncheck the boxes.

- **Scene profile**: A predefined scene profile that suits your surveillance scenario.
- **Max shutter**: Maximum recommended shutter time to prevent motion blur.
- **Zoom**: Recommended zoom level for optimal license plate resolution.

Apply settings: Click to update your camera's settings with the selected values. Once the new settings are applied, review the camera's direction and adjust it if needed.

Fusion alignment

Fusion opacity

Image order: Select which image appears on top when the thermal and visual image are combined.

Image opacity: Drag the slider or enter a percentage to adjust how transparent the top layer appears.

Align fusion view

Fine tune alignment: Use the arrow buttons to shift the images in small increments until they align.

Factory reset: Resets the alignment to factory settings.

Image

Scene intelligence

Uses object classification to make it easier to identify objects in the scene and to reduce bitrate.

Background appearance: Sharpness and saturation reduction can help increase object visibility, especially in scenes with high levels of detail.

Sharpness reduction: Turn on to set sharpness reduction.

Saturation reduction: Turn on to set saturation reduction.

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.
- **Traffic overview (low bandwidth)**: Suitable for vehicle traffic monitoring at low bandwidth.
- **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 is not sufficient, you can select a suitable light source from the list.

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

Light environment:

- **Automatic**: Automatic identification and compensation for the light source color. This is the recommended setting which can be used in most situations.
- **Automatic – outdoors**: Automatic identification and compensation for the light source color. This is the recommended setting which can be used in most outdoor situations.
- **Custom – indoors**: Fixed color adjustment for a room with some artificial light other than fluorescent lighting and good for a normal color temperature around 2800 K.
- **Custom – outdoors**: Fixed color adjustment for sunny weather conditions with a color temperature around 5,500 K.
- **Fixed – fluorescent 1**: Fixed color adjustment for fluorescent lighting with a color temperature around 4,000 K.
- **Fixed – fluorescent 2**: Fixed color adjustment for fluorescent lighting with a color temperature around 3,000 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 2,800 K.
- **Fixed – outdoors 1**: Fixed color adjustment for sunny weather conditions with a color temperature around 5,500 K.
- **Fixed – outdoors 2**: Fixed color adjustment for cloudy weather condition with a color temperature around 6,500 K.
- **Street light – mercury**: Fixed color adjustment for ultraviolet emission in mercury vapor lights common in street lighting.
- **Street light – sodium**: Fixed color adjustment that compensates for the yellow orange color of sodium vapor lights common in street lighting.
- **Hold current**: Keep the current settings and do not compensate for light changes.
- **Manual**: Fix the white balance with the help of a white object. Drag the circle to an object that you want the camera to interpret as white in the live view image. Use the **Red balance** and **Blue balance** sliders to adjust the white balance manually.

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.

Max gain: Select the suitable max gain. If you increase the max gain, it improves the visible level of detail in low contrast images, but also increases the noise level. More noise can also result in increased use of bandwidth and storage.

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.

Filters

The privacy filter creates a black and white view that looks drawn and aims to protect the privacy of people and happenings.

Pencil: Creates a view with the pencil privacy filter.

Threshold: Use the slider or text box to set the threshold value for luminance per pixel. Some details below the threshold value will be removed and is dependent on the lighting conditions of the scene.

Kernel size: Use the slider or text box to set the size of the kernel in the view. Larger kernels emphasizes larger edges and smaller kernels emphasizes smaller edges.

Video input

Deinterlacing: Select a method to improve the video stream image quality from analog devices.

- **None**: No deinterlacing.
- **Blending**: Improves the image quality without putting too much load on the processor.
- **Adaptive interpolation**: Applies different filters to the image. Can in rare cases give better results than motion-adaptive interpolation.
- **Motion-adaptive interpolation**: Applies different filters to different parts of the video stream image, depending on the level of motion in different parts of the scene. This option usually gives the best image quality.

Video termination: Turn off when the device is connected alongside other equipment. If you leave video termination on, it can affect the image quality. We recommend you to only keep video termination turned on for the last device in the video signal chain.

X offset: Enter a value to horizontally adjust the image orientation.

Y offset: Enter a value to vertically adjust the image orientation.

General

Name: Enter a name for the selected camera.

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.

Stitching

The different sensor images are stitched together to appear as one complete image.

Blending: The slider softens the line between the different sensor images.

Distance: The slider sets the distance (in meters) between the camera and the objects of interest in the scene. At the set distance, you get the optimal stitching of the images.

Stream

General

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

Palette: Select a palette to color the image with different colors depending on temperature. The palette can improve visibility of fine details.

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, H.265, or AV1 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.

Lossless zoom

- **Include lossless icon in the stream**: Turn on to display lossless zoom icon in the video stream.
- **Display duration**: Enter how long the icon should appear in the video stream.

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

Manage images: Click to add an image file. Upload or drag and drop the image. You can use .bmp, .png, .jpeg or .svg files. 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 settings: Click to turn on or off **PTZ mouse control** and **Background overlays**.

Add overlay: Select the type of overlay from the dropdown list and then click + :

- **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.
  - **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.
  - : 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).
  - **Templates**: Choose a template from this list of predefined and reusable templates.
  - : Select the text color, background color and the outline color, for example, white text on a black background (default).
  - **Size**: Select the desired font size.
  - : Select the position of the overlay in the image or click and drag the overlay to move it around in the live view.
- **Image**: Select to show a static image superimposed over the video stream.
  - : Select the position of the overlay in the image or click and drag the overlay to move it around in the live view.
- **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.
  - : Select the animation color and background color, for example, red animation on a transparent background (default).
  - **Size**: Select the desired size.
  - : Select the position of the overlay in the image or click and drag the overlay to move it around in the live view.
- **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 or click and drag the overlay to move it around in the live view.
  - **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 or click and drag the overlay to move it around in the live view.
  - **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.
- **Widget: Speed visualizer (radar data)**: Show a text overlay with real-time information about radar tracks that interact with scenarios, for example when entering or leaving a zone.
  - **Scenario**: Select the scenario to show information for.
  - **Text**: You can enter your own text, and you can also include pre-configured modifiers to automatically show, for example, maximum speed and violations.
  - **Modifiers**: Click to select any of the modifiers shown in the list to add them to the text box. For example, `%a` shows the average speed the last 15 minutes.

- : Select the text color, background and outline color.
- **Size**: Select the desired font size.
- : Select the position of the overlay in the image or click and drag the overlay to move it around in the live view.
- **Visible on all channels**: Turn off to show only on your currently selected channel. Turn on to show on all active channels.

- **Scene annotation: Ground plane**: Select to show a 3D grid projected onto the video to represent the ground surface. Before you create the ground plane, set the camera's installation height in the device location settings.
  - **Roll**: Drag the slider or enter a number to rotate the ground plane to the left or right.
  - **Tilt**: Drag the slider or enter a number to tilt the ground plane forward or backward.
  - **Rotation**: Drag the slider or enter a number to rotate the ground plane clockwise or counterclockwise.
  - **Distance from ground**: Drag the slider or enter a number to set the ground plane distance from the ground.
  - **Plane color**: Select the grid line color.
- **Scene annotations: 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.
  - **Text**: Enter an annotation text.
  - : Select the text color, outline color, background color and transparency.
  - **Size**: Select the desired font size.
  - **Icon and alignment**:
    - : Click to select any of the icons shown in the list to add them to the text box.
    - : Click to select the icon color, backplate color and transparency.
    - Click to select the position of the backplate in the image.
  - **Zoom range visiblility**: Set the zoom levels which the overlay will be shown within.

View areas

Add a view area: Click to create a view area.

Click the view area to access settings.

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

Go to: PTZ channels: Link to **PTZ** > **PTZ channels**. PTZ channels and view areas share the same pool.

Night mode

Basic IR settings

Night mode

Switch between nigh and day mode:

- **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.
- **Auto advanced**:
  - **Day to night threshold**: Use the slider to adjust the light threshold where the camera changes from day mode to night mode.
  - **Day-to-night delay**: Set a delay time to reduce unintended switching from day-to-night mode due to short light changes. For example, flickering lights in a hallway.
  - **Night-to-day delay**: Set a delay time to reduce unintended switching from night-to-day mode due to short light changes. For example, lights from a car driving by.
- **Always day**: Select to turn on the IR-cut filter. The image is in color, but with reduced light sensitivity.
- **Always night**: Select to turn off the IR-cut filter. The image is in black and white for increased light sensitivity.
  - **IR pass filter**: Turn on to block visible light and only allow near infrared light to pass through.

Internal IR controls

IR light

If your device doesn't have built-in illumination, this feature is only available when you connect a supported Axis illuminator.

Allow IR: Turn on to let the device use the built-in light in night mode.

Synchronized strobe: Turn on to automatically sync the IR light with the camera's frame rate. Use this when you need to light up a scene only for the brief moment when the image sensor captures an image.

- **Automatic illumination angle**: Select to use the automatic illumination angle.
- **Manual illumination angle**: Select to manually set the **Illumination angle** using the slider. 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.
- **Automatic intensity**: Select to automatically set the IR light intensity.
- **Manual intensity**: Select to manually adjust the **IR light** intensity using the slider.

IR wavelength: Select the desired wavelength for the IR light.

Manual IR on/off

Light: Turn on or off IR light manually.

White light

Internal white light controls

Allow white light: Turn on to let the device use white light in night mode.

- **Automatic intensity**: Select to automatically set the white light intensity.
- **Manual intensity**: Select to manually adjust the **White light** intensity using the slider.

Manual white light on/off

Light: Turn on or off white light manually.

Adaptive illumination

Motion adaptive illumination: To get access to these settings, go to **Basic IR settings** > **Internal IR controls**, turn on **Allow IR** and select **Automatic intensity**.

Adaptive IR illumination: Turn on to use full illumination when the camera detects motion. When there's no motion, the IR light dims to save power.

- **Movement sensitivity threshold**: Use the slider to set motion sensitivity.

IR power reduction

Minimum IR intensity: Use the slider to set the IR intensity when IR light is dimmed.

IR power reduction delay: Set a time how long the IR light stays at full power after motion stops.

Privacy masks

Mask settings: Click to change the color of all privacy masks or to delete them permanently.

Add a privacy mask: Click to create a new privacy mask.

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

Mask x: Click an individual mask to rename it, turn it off, or delete it permanently.

Use zoom level: Turn on to make this privacy mask appear only when it reaches the zoom level at which it was created. Zooming out in the image hides the mask again.

Picture in picture

: Click to create a new picture in picture.

Visible: Turn on to show picture in picture in the live view.

Resolution: Select size of picture in picture. Small, medium or large.

Transparency: Use the slider to adjust the transparency.

Note

Click and drag the image to move it around in the live view.

Air quality monitor

Dashboard

Real-time sensor data

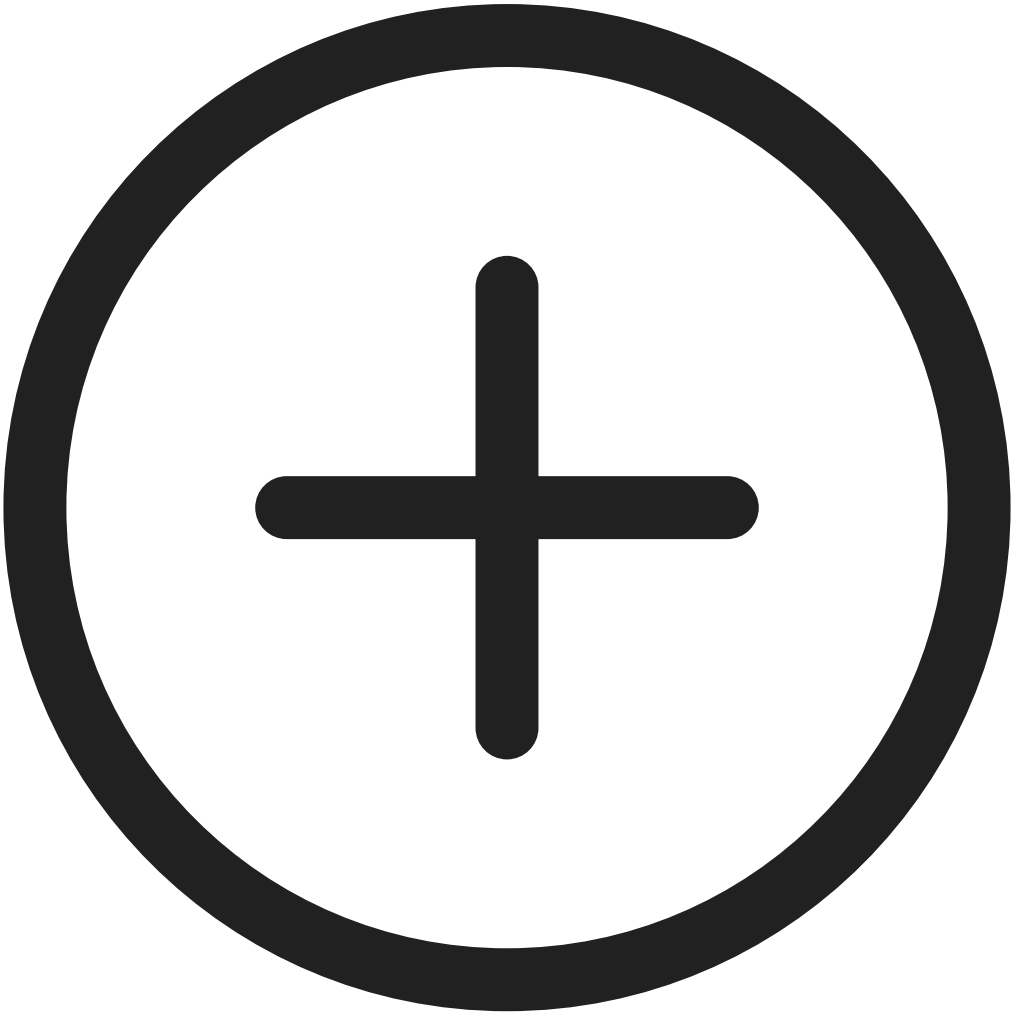
Shows the real-time sensor data.

Note

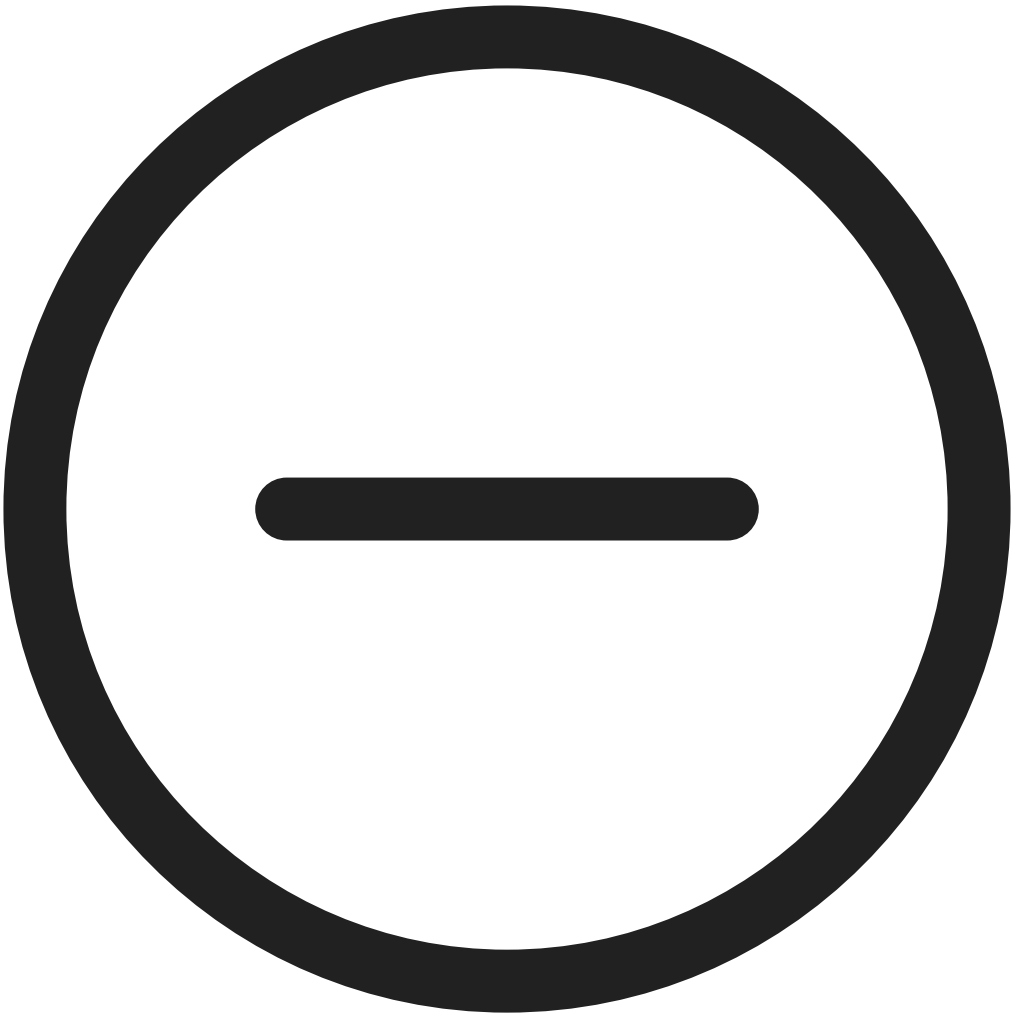
- Full CO2 accuracy takes 2 days the first time the device runs.
- The AQI (Air Quality Index) requires 12 hours to be functional the first time the device runs. The AQI will show **Calculating** until it has enough data. The calibration time is required whenever the device reboots.
- Full VOC accuracy is obtained after the device has been running for one hour. The calibration time is required whenever the device reboots.
- Full NOx accuracy is obtained after the device has been running for 6 hours. The calibration time is required whenever the device reboots.

: Click to set the name of the dashboard.

Edit: Click to show or hide the data.



: Click to add data to the dashboard.



: Click to remove data from the dashboard.

Temperature: View the real-time temperature from the air quality sensor.

Humidity: View the real-time humidity from the air quality sensor.

CO2: View the real-time carbon dioxide.

The color meanings of the CO2 status bars are as follows:

- **Green (0–1,000 ppm)**: **Good**. The data is considered satisfactory.
- **Orange (1,001–2,000 ppm)**: **Unhealthy for sensitive groups**. Members of sensitive groups may experience health effects. The general public is less likely to be affected.
- **Red (2,001–5,000 ppm)**: **Unhealthy**. Everyone may begin to experience health effects; members of sensitive groups may experience more serious health effects.
- **Purple (5,001–40,000 ppm)**: **Very unhealthy**. Health warnings of emergency conditions. The entire population is more likely to be affected.

NOx: View the real-time nitric oxide and nitrogen dioxide.

The color meanings of the NOx status bars are as follows:

- **Green (0–30): Good.** The data is considered satisfactory.
- **Yellow (31–150): Moderate.** The data is acceptable. There may be a moderate health concern for a very small number of people who are unusually sensitive.
- **Orange (151–300): Unhealthy for sensitive group.** Everyone may begin to experience health effects; members of sensitive groups may experience more serious health effects.
- **Red (301–500): Unhealthy.** Everyone may begin to experience health effects; members of sensitive groups may experience more serious health effects.

PM 1.0: View the real-time particle matter 1.0.

PM 2.5: View the real-time particle matter 2.5.

The color meanings of the PM 2.5 status bars are as follows:
- **Green (0–9 µg/m³): Good.** The data is considered satisfactory.
- **Yellow (9.1–35.4 µg/m³): Moderate.** The data is acceptable. There may be a moderate health concern for a very small number of people who are unusually sensitive.
- **Orange (35.5–55.4 µg/m³): Unhealthy for sensitive group.** Everyone may begin to experience health effects; members of sensitive groups may experience more serious health effects.
- **Red (55.5–125.4 µg/m³): Unhealthy.** Everyone may begin to experience health effects; members of sensitive groups may experience more serious health effects.
- **Purple (125.5–225.4 µg/m³): Very unhealthy.** Health warnings of emergency conditions. The entire population is more likely to be affected.
- **Maroon (225.5–1,000 µg/m³): Hazardous.** Emergency conditions. The entire population is more likely to be affected.

PM 4.0: View the real-time particle matter 4.0.

PM 10.0: View the real-time particle matter 10.0.

The color meanings of the PM 10.0 status bars are as follows:
- **Green (0–54 µg/m³): Good.** The data is considered satisfactory.
- **Yellow (55–154 µg/m³): Moderate.** The data is acceptable. There may be a moderate health concern for a very small number of people who are unusually sensitive.
- **Orange (155–254 µg/m³): Unhealthy for sensitive group.** Everyone may begin to experience health effects; members of sensitive groups may experience more serious health effects.
- **Red (255–354 µg/m³): Unhealthy.** Everyone may begin to experience health effects; members of sensitive groups may experience more serious health effects.
- **Purple (355–424 µg/m³): Very unhealthy.** Health warnings of emergency conditions. The entire population is more likely to be affected.
- **Maroon (425–1,000 µg/m³): Hazardous.** Emergency conditions. The entire population is more likely to be affected.

Vaping/Smoking: View the vaping or smoking detected or undetected.

The color meanings of the Vaping/Smoking status bars are as follows:
- **Green: Undetected.** The suspected vaping or smoking activity is not detected.
- **Red: Detected.** The suspected vaping or smoking activity is detected.

VOC: View volatile organic compounds index.

The color meanings of the VOC status bars are as follows:
- **Green (0–200): Good.** The data is considered satisfactory.
- **Yellow (201–300): Moderate.** The data is acceptable. There may be a moderate health concern for a very small number of people who are unusually sensitive.

- **Orange (301–400)**: **Unhealthy for sensitive group**. Everyone may begin to experience health effects; members of sensitive groups may experience more serious health effects.
- **Red (401–500)**: **Unhealthy**. Everyone may begin to experience health effects; members of sensitive groups may experience more serious health effects.

AQI: View air quality index.

The color meanings of the air quality index status bars are as follows:
- **Green (0–50)**: **Good**. The data is considered satisfactory.
- **Yellow (51–100)**: **Moderate**. The data is acceptable. There may be a moderate health concern for a very small number of people who are unusually sensitive.
- **Orange (101–150)**: **Unhealthy for sensitive group**. Everyone may begin to experience health effects; members of sensitive groups may experience more serious health effects.
- **Red (151–200)**: **Unhealthy**. Everyone may begin to experience health effects; members of sensitive groups may experience more serious health effects.
- **Purple (201–300)**: **Very unhealthy**. Health warnings of emergency conditions. The entire population is more likely to be affected.
- **Maroon (301–500)**: **Hazardous**. Emergency conditions. The entire population is more likely to be affected.

Humidex: View the real-time humidity index from the air quality sensor.

The color meaning of the humidex status bars are as follows:
- **Green (<30 °C)**: **Comfortable**. There is little to no discomfort and conditions are not unsafe.
- **Yellow (30–39 °C)**: **Caution**. Everyone may experience some discomfort and should be cautious during physical activity.
- **Orange (40–45 °C)**: **Warning**. Everyone may experience great discomfort and should avoid physical exertion.
- **Red (>45 °C)**: **Danger**. Conditions are dangerous and everyone may be at risk of heat stroke.

Heat index: View the real-time heat index from the air quality sensor.

The color meaning of the heat index status bars are as follows:
- **Green (<27 °C)**: **Normal**. There is little to no discomfort and conditions are not unsafe.
- **Yellow (27–32 °C)**: **Caution**. Prolonged physical activity can cause heat cramps and fatigue.
- **Orange (33–39 °C)**: **Danger**. Prolonged physical activity can cause heat cramps, heat exhaustion, and heat stroke.
- **Red (>39 °C)**: **Extreme**. Prolonged physical actively is likely to cause heat cramps and heat exhaustion, while heat stroke is probable.

Settings

Threshold

Sets up the air quality sensor data.

Temperature: Set temperature **Min** and **Max** within the range **-10 to 45**.

Humidity : Set humidity **Min** and **Max** within the range **0 to 100**.

CO2 : Set carbon dioxide **Min** and **Max** within the range **0 to 40000**.

NOx : Set nitric oxide and nitrogen dioxide **Min** and **Max** within the range **0 to 500**.

PM1.0 : Set particle matter 1.0 **Min** and **Max** within the range **0 to 1000**.

PM2.5 : Set particle matter 2.5 **Min** and **Max** within the range **0 to 1000**.

PM4.0 : Set particle matter 4.0 **Min** and **Max** within the range **0 to 1000**.

PM10.0 : Set particle matter 10.0 **Min** and **Max** within the range **0 to 1000**.

VOC : Set volatile organic compounds index **Min** and **Max** within the range **0 to 500**.

AQI : Set air quality index **Min** and **Max** within the range **0 to 500**.

Heat index: Set heat index **Min** and **Max** within the range **0 to 153**.

Humidex: Set humidex **Min** and **Max** within the range **0 to 96**.

Temperature units

Show temperature in : **Celsius** or **Fahrenheit**

Vaping detect sensitivity

Sets up the vaping detect sensitivity.

Low sensitivity, High sensitivity: Use the slider to adjust the difference between low sensitivity and high sensitivity at which the device should generate an alarm. High sensitivity means the device will detect even small amounts of smoking or vaping and is more likely to trigger an alert; low sensitivity means it will only respond to larger amounts of smoking or vaping, reducing the chance of false alarms.

Storage setting

To change the storage settings for your device:

1. Go to **Air quality monitor** > **Settings**.
2. Navigate to **Storage settings**.
3. Select your preferred storage from the available options.

Note

Changing the storage option will erase existing data.

Variable metadata

Variable metadata is used by third-party platforms that want to subscribe to sensor metadata with an adjustable transmission frequency. The variable metadata includes all the sensor data shown on the dashboard.

Variable metadata: Turn on to use variable metadata.

Note

By default this function is disabled; no metadata for the topic is sent. After enabling, metadata for the topic is transmitted at the frequency range set below.

Set frequency range (00:00:01 – 23:59:59): Enter a value to set the frequency range.

Validation period

You can set a validation period for below air quality settings. The validation period acts as a time threshold, and the reading must stay above the limit of the validation period range to trigger an alarm.

Example

If CO_2 validation period is 5 s, the CO_2 level must stay above the limit for the full 5 s to trigger the alarm.

Set validation period range (0s-60s) for the below data:

- **Temperature**
- **Humidity**
- **CO2**
- **NOx**
- **PM1.0**
- **PM2.5**
- **PM4.0**
- **PM10.0**
- **VOC**
- **AQI**
- **Vaping or smoking**
- **Heat index**
- **Humidex**

Modbus

Modbus is disabled by default. When enabled, you can use Modbus to send data from the air quality sensor.

Important

Enabling Modbus functionality may make your system insecure.

Modbus TCP Registers

Register Address	Name	Scale	Unit	Comments
0	Temperature	0.1	°C	0x00FF (225) –> 25.5 °C
1	Humidity	0.1	%RH	0x00FF (225) –> 25.5 %RH
2	CO_2	1	ppm	0x01F4 (500) –> 500 ppm
3	VOC	1	- -	0x0064 (100) –> 100
4	NO_X	1	- -	0x0002 (2) –> 2
5	AQI	1	- -	0x0001 (1) –> 1
6	Vaping	1	- -	0x0001 (1) –> 1
7	PM1.0	0.1	µg/m^3	0x0019 (25) –> 2.5 µg/m^3
8	PM2.5	0.1	µg/m^3	0x0019 (25) –> 2.5 µg/m^3
9	PM4.0	0.1	µg/m^3	0x0019 (25) –> 2.5 µg/m^3

10	PM10.0	0.1	µg/m^3	0x0019 (25) –> 2.5 µg/m^3
11	Humidex	1	°C	0x0019 (25) –> 25 °C
12	Heat Index	1	°C	0x0019 (25) –> 25 °C

Statistics

Sensor data statistics

You can export up to 365 days of sensor statistics to a CSV file for use in applications such as Microsoft® Excel.

- **Predefined date range**: to select the pre defined date range you'd like to download from the list.
- **From** and **To**: to select customized range you'd like to download. You can download the data up to 365 days.

Note

If both a custom and a predefined range are selected, the custom range takes precedence.

Note

The maximum download range is limited by the retention time configured in *Storage setting, on page 41*.

- **Select a source**: to select the desired source you'd like to download.
- **Download data**: to select **Download selected sensor data** from the drop down menu.
- **Download data for all sources**: to export data for all sources within the chosen time span.

The file is downloaded to your downloads folder. Download could take a while depending on the file size.

Communication

VMS calls

VMS calls

Allow calls in the video management software (VMS): Select to allow calls from the device to the VMS. You can make VMS calls even if SIP is turned off.

Call timeout: Set the maximum duration of an attempted call if no one answers.

Contact list

Recipients

Devices

Add device: Click to add a new device to the list of recipients.

- **Name**: Enter a name for the device.
- **Location**: Enter a location for the device.
- **SIP**: Select SIP as protocol.
  - **SIP address**: If you use SIP, enter the device's IP address or extension.
  - **SIP account**: If you use SIP, select the SIP account to use when calling from AXIS C6110 Network Paging Console to the recipient device.
- **VAPIX**: Select VAPIX as protocol.
  - **IP**: Enter the device's IP address or extension.
  - **Username**: Enter username.
  - **Password**: Enter password.
- **Use external video source**: Select to activate a video stream from a specific source when calling or receiving a call from a specific contact or device.
  - **URI**: Enter the address to the video source.
  - **Use AXIS template**: Click to use a template that makes it easier to write the address.
  - **Username**: Enter username.
  - **Password**: Enter password.
  - **Validate server certificate**: Select to validate the certificate that was created by HTTPS server.

The context menu contains:

- **Edit device**: Edit the device's properties.
- **Delete device**: Delete the device.

Contacts

For intercom devices:

Click to download the contact list as a json file.

Click to import a contact list (json).

Add contact: Click to add a new contact to the contact list.

Upload image: Click to upload an image to represent the contact.

First name: Enter the contact's first name.

Last name: Enter the contact's last name.

Speed dial: Enter an available speed dial number for the contact. This number is used to call the contact from the device.

SIP address: If you use SIP, enter the contact's IP address or extension.

: Click to make a test call. The call will automatically end when answered.

SIP account: If you use SIP, select the SIP account to use for the call from the device to the contact.

Availability: Select the contact's availability schedule. You can add or adjust schedules in **System > Events > Schedules**. If a call is attempted when the contact isn't available, the call is canceled unless there's a fallback contact.

Fallback: If applicable, select a fallback contact from the list.

Notes: Add optional information about the contact.

The context menu contains:

Edit contact: Edit the contact's properties.

Delete contact: Delete the contact.

For AXIS C6110 Paging Console:

Add contact: Click to add a new contact to the list of recipients.

- **Name**: Enter a first name for the contact.
- **Last name**: Enter a last name for the contact.
- **Location**: Enter a location for the contact.
- **SIP**: Select SIP as protocol.
  - **SIP address**: If you use SIP, enter the contact's IP address or extension.
  - **SIP account**: If you use SIP, select the SIP account to use when calling from AXIS C6110 Network Paging Console to the recipient contact.
- **VAPIX**: Select VAPIX as protocol.
  - **IP**: Enter the contact's IP address or extension.
  - **User name**: Enter user name.
  - **Password**: Enter password.
- **Use external video source**: Select to activate a video stream from a specific source when calling or receiving a call from a specific contact or device.
  - **URI**: Enter the address to the video source.
  - **Use AXIS template**: Click to use a template that makes it easier to write the address.
  - **Username**: Enter username.
  - **Password**: Enter password.
  - **Validate server certificate**: Select to validate the certificate that was created by HTTPS server.

The context menu contains:

- **Edit contact**: Edit the contact's properties.
- **Delete contact**: Delete the contact.

Groups

For intercom devices:

Click to download the contact list as a json file.

Click to import a contact list (json).

Add group: Click to create a new group of existing contacts.

Upload image: Click to upload an image to represent the group.

Name: Enter a name for the group.

Use for group calls only: Turn on if you want to use the group only for group calls. Turn off if you want to add individual contacts in a group but not use the group for group calls.

Speed dial: Enter an available speed dial number for the group. This number is used to call the group from the device. Only for group call groups.

Recipients: Select the contacts to include in the group. Calls will be placed to all recipients at the same time. The maximum number of recipients is six.

Fallback: If applicable, select a fallback contact from the list. Only for group call groups.

Notes: Add optional information about the group.

The context menu contains:

Edit group: Edit the group's properties.

Delete group: Delete the group.

For AXIS C6110 Paging Console:

For paging a group of Axis devices using VAPIX.

Add group: Click to create a new group of existing recipients.

- **Name**: Enter a name for the group.
- **Recipients**: Select recipients for the group.

The context menu contains:

- **Edit group**: Edit the group's properties.
- **Delete group**: Delete the group.

Calls

Call button

Use call button: Turn on to make it possible to use the call button.

Button functionality during a call: Select the functionality of the call button once a call has been started from the device.

- **End the call**: When a visitor presses the call button during an outgoing call, the call ends. Use this option to allow visitors to end a call at any time.
- **No functionality until the call has ended**: When a visitor presses the call button during an outgoing call, nothing happens. Use this option to prohibit visitors from ending calls.
- **Delay before you can end the call**: When a visitor presses the call button within the time set in **Delay (seconds)** after they have started a call, nothing happens. If the delay time has passed, pressing the call button ends the call. Use this option to prevent visitors from accidentally ending calls due to double presses.
  - **Delay (seconds)**: Enter the time that must pass before a second press of the call button ends the call.

Standby light: Select an option for the built-in light around the call button.

- **Auto**: The device turns the built-in light on and off based on the surrounding light.
- **On**: The built-in light is always turned on when the device is in standby mode.
- **Off**: The built-in light is always turned off when the device is in standby mode.

Recipients: Select or create one or more contacts to call when someone presses the call button. If you add more than one recipient, the call will be placed to all of them at the same time. The maximum number of SIP call recipients is six, while you can have an unlimited number of VMS call recipients.

Fallback: Add a fallback contact from the list in case none of the recipients replies.

General

Audio

Note

- The selected audio clip is only played when a call is made.
- If you change the audio clip or gain during an ongoing call, it doesn't take effect until the next call.

Ringtone: Select the audio clip to play when someone makes a call to the device. Use the slider to adjust the gain.

Ringback tone: Select the audio clip to play when someone makes a call from the device. Use the slider to adjust the gain.

Display

Configuration

Home

⋮ The context menu contains:

- **Rename title**: Change the title of the home view.

Buttons

Click a button to configure it.

- **Action**: Select to make the button an action.
  - **Use an existing action**: Select to choose an action that already exists.
  - **Create a new action**: Select to create a new action.
  - **Action**: Select an action for the button.
- **Folder**: Select to make the button a folder that can contain further buttons.
  - **Name**: Name the folder.

Actions

+ Add action: Click to create an action that can be used for the buttons. Available action types:

- **Play a file**: Select to make an announcement (play an audio file to a person or a device).
- **Two-way**: Select to initiate two-way call to a contact (a person or a device).
- **Clear call history**: Select to clear the call history.
- **HTTP request**: Select to make an HTTP request.
- **One-way**: Select to page a contact (one-way communication to a person or device).
- **Home**: Select to go to the home screen.
- **Show call history**: Select to show the call history.
- **Show contacts**: Select to show the list of contacts that are added as persons (see Add contacts)

Folder: Select to create a folder that can contain further buttons or folders.

Display settings

Display

Brightness

- **Adaptive brightness**: Select for automatic adjustment of the brightness.
- **Level**: Select a brightness level manually.

Timers

- **Low power mode**: Select a time to wait for activity before activation a mode of low power consumption.
- **Return to home**: Select a time to wait before returning to the home screen.

Presence detection

- **Turn on display when presence is detected**: Turn on to make the display activate itself when it detects presence.
- **Distance**: Set the distance for presence detection.

Display lock

Display lock

- **Use display lock**: Select to use the display lock.
- **PIN**: Enter the four digit code that will be used to unlock the display lock.
- **Auto-lock time**: Select the time of inactivity that will activate the display lock.
- **Save**: Click to save your changes.

Localization

Display language

Display language
- **Language**: Select the language to use on the display.

Status bar clock
- **Off/On**: Turn on to show the clock, and turn off to hide the clock.
- **24-hour clock**: Turn on to use a 24-hour format, and turn off to use a 12-hour format.

Pages

Add: Create a new page for the display.

Name: Give the page a name to help you identify it.

Background image: Select an image from the media library to use as a background. The optimal image resolution is 480x800 pixels. The maximum image resolution allowed is 2048x2048 pixels.

Add: Add a widget, such as a button, text, or image to the page. A widget is a graphical element.

Type: Select a widget type.

- **Button – Button type**: Select a type of button.
  - **Contact**
    - **Contact**: Assign a contact to the button. Visitors press the button to make a call to the contact.
    - **Size**: Select the size of the contact button.
  - **Custom**
    - **Text**: Type a text to show on the button.
    - **Name**: Give the button a name to help you identify it when you create a rule in the events system.
    - **Size**: Select the size of the button.
- **Image**
  - **Name**: Give the image a name.
  - **Image scaling**
    - **Auto**: Let the system optimize the scaling of the image.
    - **Fit**: Adjust the scaling so the image fits in the display.
    - **Fill**: Adjust the scaling so the image fills the display.
  - **Image**: Select an image from the media library. The maximum image resolution allowed is 2048x2048 pixels.
- **Text**
  - **Text**: Type a text to show on the display.
  - **Styling**: Choose how to format the text.

Save: Save the page to be able to show it on the display and to create rules for the widgets.

The context menu contains:

Edit: Adjust the page.

Reset: Undo unsaved changes to the page.

Duplicate: Create a copy of the page.

Set as default homepage: Make this page the one to show when no scheduled page is active. You must save a page before you can set it as homepage.

Schedule: Select to show the page according to one of the schedules defined in **System > Events > Schedules**.

Delete: Delete the page. You can't delete the page set as default homepage.

Clock

Preview

The preview shows what the display will look like with the current settings.

Appearance

Use 24 hour clock: Turn on to show the clock with 24-hour format, e.g. 14:30. Turn off to show the clock with 12-hour format, e.g. 2:30 pm.

Show seconds: Turn on to show both hours, minutes and seconds. Turn off to show only hours and minutes.

Show date: Turn on to show the date and off to hide the date.

Font color: Set the color of the text that is shown on the display.

Background color: Set the color of the display background.

Availability

Off: Select to hide the clock. Messages triggered by rules will still appear on the display.

Always on: Select to keep the display on all the time.

Turn on display when presence is detected: Select to activate the display when presence is detected. If no presence is detected for the chosen standby time, the display will be turned off.

Turn on display according to schedule: Select to activate the display according to a schedule.

Invert schedule: Select to invert the schedule. For instance, if you schedule an event to play between 8.00 – 12.00 and invert the schedule, the event will play between 12.00 – 8.00 instead.

General

Device language: Select the language for default texts on the display.

Show keypad on homepage: Turn on to show a keypad button on the default homepage. Visitors can press the button to open a keypad and use their credentials to unlock the door.

Screensaver

Add: Click to create a new screensaver. The screensaver can be a page or an image.

Duration: Select the amount of time to show the screensaver.

Edit: Select a screensaver from the list and click to adjust it.

Remove: Select one or more screensavers from the list and click to delete them.

Settings: Click to adjust general screensaver settings.

Start screensaver when inactive: Set the allowed time of inactivity before the screensaver starts. If you set a time that is longer than the time set in **Turn off display when inactive**, the screensaver never starts.

Turn off display when inactive: Set the allowed time of inactivity before the display is turned off. This time includes the time of the screensaver.

Screensaver sequence: Select in what order to show the screensavers, if there is more than one. Each screensaver is shown for the time set in **Duration** before switching to the next one. If you have only one screensaver it will be shown repeatedly.

- **Listed**: Show screensavers in the listed order.
- **Random**: Show screensavers in a randomized order.

Wake-up trigger: Select how to wake up the display while the screensaver is active or the display is turned off.

- **Touch**: Wake up the display when someone touches it.
- **Touch or presence detection**: Wake up the display when someone touches it or when the device detects someone in front of it.

Show tap-to-unlock icon: Show a hand icon to indicate that users need to touch the display to wake it up.

Thermometry

Temperature reading

Palettes

The colors in the palette emphasize temperature differences. Palettes with names that start with Iso are isothermal. Isothermal palettes make it possible to isolate specific colors to specific temperature levels. The low level indicates where the colored part of the palette starts. If you select an isothermal palette, a vertical bar in the image shows the user-defined temperature levels.

Palette: Select a palette to color the image and improve visibility of fine details.

High level: Type the temperature where the high level temperature range starts. The vertical bar indicates what color represents the high level temperature.

Mid level: Type the temperature where the mid level temperature range starts. The vertical bar indicates what color represents the mid level temperature.

Low level: Type the temperature where the low level temperature range starts. The vertical bar indicates what color represents the low level temperature.

Min level: Type the temperature where the min level temperature range starts. The vertical bar indicates what color represents the min level temperature.

Show palette: Select to show the palette's color scale as a vertical bar in the image.

Spot meter

Measure spot temperature: Turn on to be able to click anywhere in the image to measure and show the temperature at that spot.

Temperature units

Choose if you want to show temperatures in Celsius or Fahrenheit.

Temperature detection

With temperature detection, you can define up to ten areas in the scene where you want to monitor the temperature. In **System > Events**, you can use the detection areas as conditions when you create rules.

Temperature detection: Click to be able to delete all detection areas permanently.

Preset positions: Select a preset position to create, update, or delete temperature detection areas.

Pause guard tour on alarm: Turn on to pause the guard tour when an alarm is triggered.

Resume guard tour after alarm: Turn on to continue playing the guard tour when the alarm condition is no long met.

Add detection area: Click to create a new detection area. Turn off the guard tour before you create or edit a detection area.

Name: Type a descriptive name for the detection area.

Use area: Turn on to make it possible to use the detection area and its settings when you create rules.

Conditions for detection: Set the conditions for detecting high or low temperatures or temperature changes.

Temperature in the area:

- **Warmest spot**: Select to trigger an action based on the temperature in the warmest spot inside the detection area.
- **Average**: Select to trigger an action based on the detection area's average temperature.
- **Coolest spot**: Select to trigger an action based on the temperature in the coolest spot inside the detection area.

Select what type of temperature change should trigger an action:

- **Above**: Select to trigger an action when the temperature rises above a certain value for a certain amount of time. The default time is 5 seconds, and allowed values are 0–300 seconds.
- **Below**: Select to trigger an action when the temperature drops below a certain value for a certain amount of time. The default time is 5 seconds, and allowed values are 0–300 seconds.

For **Above** and **Below**, type the threshold temperature and for how long the temperature must be above or below the threshold temperature.

- **Increase rate**: Select to trigger an action when the temperature has increased by a certain number of degrees at the end of a certain time span. To determine the increase rate, the temperature at the end of the time span is compared to the temperature at the start. The default time span is 5 seconds, and allowed values are 0–300 seconds.
- **Decrease rate**: Select to trigger an action when the temperature has decreased by a certain number of degrees at the end of a certain time span. To determine the decrease rate, the temperature at the end of the time span is compared to the temperature at the start. The default time span is 5 seconds, and allowed values are 0–300 seconds.

For **Increase rate** and **Decrease rate**, type the number of degrees the temperature has to change and the time span for the change.

Include detection area in video stream:

- **Never**: Select to never show the detection area in the video stream.
- **Always**: Select to always show the detection area in the video stream.
- **If triggered**: Select to show the detection area in the video stream when an action gets triggered.

Include temperature: Select to show the temperature in the video stream.

Deviation detection

With deviation detection, you can monitor if the temperature difference between two or more areas becomes too big. The areas are defined by using overlays created under **Temperature detection**. In **System > Events**, you can use **Temperature deviation** as conditions when you create rules.

Add deviation group: Click to create a new deviation group.

Group name: Enter a name for the group.

Use group: Turn on to make it possible to use deviation detection when you create rules.

Add areas to group: Select the areas to group.

Area temperatures to compare: Select a method for comparing:

- **Warmest spots**: Compare the warmest spots inside the areas.
- **Averages**: Compare the average temperatures of the areas.
- **Coolest spots**: Compare the coolest spots inside the areas.
- **Inherit from area settings**: Use the temperatures that are set for the areas. This makes it possible, for instance, to compare the maximal temperature of one area with the minimal temperature of the other area.

Max deviation: Enter the deviation limit for temperature and time delay.

Include: Turn on to show the overlay when the alarm has triggered.

Radar

Click to play the live radar stream.

Click to freeze the live radar stream.

Click to take a snapshot of the live radar stream. The file is saved in the 'Downloads' folder on your computer. The 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 start a continuous recording of the live radar 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 controls to pan and zoom the radar view.

Click to access onscreen controls. Enable groups of onscreen controls to make the settings in each group available when users right-click the live stream in the video management software.

- **Custom controls**: Click **Add custom control** to create customized onscreen controls.

Click to access more settings:

- **Video format**: Select the encoding format to use in the live view.
- **Autoplay**: Turn on to autoplay a muted radar stream whenever you open the device in a new session.
- **Client stream information**: Turn on to show dynamic information about the radar stream used by the browser that shows the live radar 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 radar 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 radar 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.
- **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.
- **Level grid**: Click to show the level grid. The grid helps you decide if the image is horizontally aligned. Click to hide it.

- **Refresh**: Click to refresh the still image in the live view.

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 radar stream in expanded full screen. Click again to exit the expanded full screen mode.

Click to show the live radar stream in full screen. Press Esc to exit full screen mode.

Settings

Operation

Transmission

Radar transmission: Use this to turn off the radar module completely.

Channel: If you have problems with multiple devices interfering with each other, select the same channel for up to four devices that are close to each other. For most installations, select **Auto** to let the devices automatically negotiate which channel to use.

Installation

Mounting height: Enter the mounting height for the product.

Note

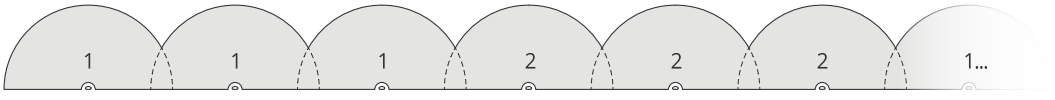
Be as specific as you can when you enter the mounting height. This helps the device visualize the radar detection in the correct position in the image.

Number of neighboring radars: Select the number of neighboring radars that are mounted within the same coexistence zone. This helps avoid interference.

Coexistence

Number of neighboring radars: Select the number of neighboring radars that are mounted within the same coexistence zone. This will help to avoid interference. The coexistence radius is 350 m (1,148 ft).

- **0–1**: Select this option if you mount one to two radars in the same coexistence zone.
- **2**: Select this option if you mount three radars in the same coexistence zone.
- **3–5**: Select this option if you mount four to six radars in the same coexistence zone.
  - **Groups**: Select a group (**Group 1** or **Group 2**) for your radar. This will also help to avoid interference. We recommend that you add three radars in each group, and that you add the radars that are closest to each other in the same group.



Detection

Detection sensitivity: Select how sensitive the radar should be. A higher value means that you get a longer detection range, but there is also a higher risk of false alarms. A lower sensitivity decreases the number of false alarms, but it may shorten the detection range.

Radar profile: Select a profile that suits your area of interest.

- **Area monitoring**: Detect both large and small objects that move at lower speeds in open areas.
- **Two-directional road monitoring**: Detect vehicles that travel in both directions at speeds up to 200 km/h (125 mph) in urban zones and on suburban roads.
- **One-directional road monitoring**: Detect oncoming vehicles that travel at speeds up to 300 km/h (186 mph).

Radar image stabilization: Turn on to stabilize the image if the device is exposed to vibrations.

Small objects filter: Turn on to minimize false alarms from small objects, such as cats or rabbits.

Ignore stationary rotating objects: Turn on to minimize false alarms from stationary objects with rotating movements, such as fans or turbines.

Swaying object filter: Turn on to minimize false alarms from swaying objects, such as trees, bushes, or flagpoles.

Unknown object filter: Turn on to minimize false alarms caused by objects that the radar can't classify.

Speed statistics

Collect statistics: Turn on to collect and store speed statistics from vehicles.

Select time period for downloading statistics (.csv format): Select the period to download statistics for.

Download: Click to download speed statistics for the selected period to your computer as a comma separated file.

Traffic assistant

Status: Shows the status of the configuration.

Configure: Click to open the setup assistant that guides you through the calibration step by step.

Visualization

View

Information legend: Turn on to show a legend containing the object types the radar can detect and track. Drag and drop to move the information legend.

Zone opacity: Select how opaque or transparent the coverage zone should be.

Grid opacity: Select how opaque or transparent the grid should be.

Color scheme: Select a theme for the radar visualization.

Rotation: Select the preferred orientation of the radar image.

Object visualization

Trail lifetime: Select how long the trail of a tracked object is visible in the radar view.

Icon style: Select the icon style of the tracked objects in the radar view. For plain triangles, select **Triangle**. For representative symbols, select **Symbol**. The icons will point in the direction the tracked objects are moving, regardless of style.

Show information with icon: Select which information to display next to the icon of the tracked object:

- **Object type**: Show the object type that the radar has detected.
- **Classification probability**: Show how sure the radar is that the object classification is correct.
- **Velocity**: Show how fast the object is moving.

Stream

General

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

Palette: Select a palette to color the image with different colors depending on temperature. The palette can improve visibility of fine details.

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, H.265, or AV1 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.

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.

Map calibration

Use map calibration to upload and calibrate a reference map. The result of the calibration is a reference map that displays the radar coverage in the appropriate scale, which makes it easier to see where objects are moving.

Setup assistant: Click to open the setup assistant that guides you through the calibration step by step.

Reset calibration: Click to remove the current map image and radar position on the map.

Map

Upload map: Select or drag and drop the map image you want to upload.

Download map: Click to download the map.

Rotate map: Use the slider to rotate the map image.

Scale and distance on map

Distance: Add the distance between the two points you have added to the map.

Pan and zoom map

Mouse controls: Turn on to use the mouse to pan and zoom the map image. Scroll to zoom. Click and drag to pan. You can also press and hold SHIFT to activate mouse controls.

Pan: Click on the buttons to pan the map image.

Zoom: Click on the buttons to zoom in or out on the map image.

Reset pan and zoom: Click to remove the pan and zoom settings.

Radar position

Position: Click on the buttons to move the radar on the map.

Rotation: Click on the buttons to rotate the radar on the map.

Lanes

Lanes improve the radar's performance and ability to track vehicles when monitoring lanes on a road. Add one lane in the radar for each actual lane you are monitoring.

Add lane: Click to add a new lane. Use the mouse to modify the shape of the lane you have added.

: Click to expand and edit the name of the lane.

: Click to delete the lane.

Lanes enabled: Turn on to activate the lanes you have added.

Exclusion zones

An **exclusion zone** is an area in which moving objects are ignored. Use exclusion zones if there are areas inside a scenario that trigger a lot of unwanted alarms.

 : Click to create a new exclusion zone.

To modify an exclusion zone, select it in the list.

Track passing objects: Turn on to track objects that pass through the exclusion zone. The passing objects keep their track IDs and are visible throughout the zone. Objects that appear from within the exclusion zone will not be tracked.

Zone shape presets: Select the initial shape of the exclusion zone.

- **Cover everything**: Select to set an exclusion zone that covers the entire radar coverage area.
- **Reset to box**: Select to place a rectangular exclusion zone in the middle of the coverage area.

To modify the shape of the zone, drag and drop any of the points on the lines. To remove a point, right-click on it.

Scenarios

A scenario is a combination of triggering conditions, as well as scene and detection settings.

: Click to create a new scenario. You can create up to 20 scenarios.

Triggering conditions: Select the condition that will trigger alarms.

- **Movement in area**: Select if you want the scenario to trigger on objects moving in an area.
- **Line crossing**: Select if you want to the scenario to trigger on objects crossing one, or two, lines.

Scene: Define the area or lines in the scenario where moving objects will trigger alarms.

- For **Movement in area**, select one of the shape presets to modify the area.
- For **Line crossing**, drag and drop the line in the scene. To create more points on a line, click and drag anywhere on it. To remove a point, right-click on it.
  - **Require crossing of two lines**: Turn on if the object must pass two lines before the scenario triggers an alarm.
  - **Change direction:** Turn on if you want the scenario to trigger an alarm when objects cross the line in the other direction.

Detection settings: Define the trigger criteria for the scenario.

- For **Movement in area**:
  - **Ignore short-lived objects**: Set the delay in seconds from when the radar detects the object to when the scenario triggers an alarm. This can help to reduce false alarms.
  - **Trigger on object type**: Select the type of objects (human, vehicle, unknown) you want the scenario to trigger on.
  - **Speed limit**: Trigger on objects moving at speeds within a specific range.
    - **Invert**: Select if you want to trigger on speeds above and below the set speed limit.
- For **Line crossing**:
  - **Ignore short-lived objects**: Set the delay in seconds from when the radar detects the object to when the scenario triggers an action. This can help to reduce false alarms. This option is not available for objects crossing two lines.
  - **Max time between crossings**: Set the max time between crossing the first line and the second line. This option is only available for objects crossing two lines.
  - **Trigger on object type**: Select the type of objects (human, vehicle, unknown) you want the scenario to trigger on.
  - **Speed limit**: Trigger on objects moving at speeds within a specific range.
    - **Invert**: Select if you want to trigger on speeds above and below the set speed limit.

Alarm settings: Define the criteria for the alarm.

- **Minimum trigger duration**: Set the minimum duration for the triggered alarm.

Overlays

Manage images: Click to add an image file. Upload or drag and drop the image. You can use .bmp, .png, .jpeg or .svg files. 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 settings: Click to turn on or off **PTZ mouse control** and **Background overlays**.

Add overlay: Select the type of overlay from the dropdown list and then click + :

- **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.
  - **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.
  - : 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).
  - **Templates**: Choose a template from this list of predefined and reusable templates.
  - : Select the text color, background color and the outline color, for example, white text on a black background (default).
  - **Size**: Select the desired font size.
  - : Select the position of the overlay in the image or click and drag the overlay to move it around in the live view.
- **Image**: Select to show a static image superimposed over the video stream.
  - : Select the position of the overlay in the image or click and drag the overlay to move it around in the live view.
- **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.
  - : Select the animation color and background color, for example, red animation on a transparent background (default).
  - **Size**: Select the desired size.
  - : Select the position of the overlay in the image or click and drag the overlay to move it around in the live view.
- **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 or click and drag the overlay to move it around in the live view.
  - **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 or click and drag the overlay to move it around in the live view.
  - **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.
- **Widget: Speed visualizer (radar data)**: Show a text overlay with real-time information about radar tracks that interact with scenarios, for example when entering or leaving a zone.
  - **Scenario**: Select the scenario to show information for.
  - **Text**: You can enter your own text, and you can also include pre-configured modifiers to automatically show, for example, maximum speed and violations.
  - **Modifiers**: Click to select any of the modifiers shown in the list to add them to the text box. For example, `%a` shows the average speed the last 15 minutes.

- : Select the text color, background and outline color.
- **Size**: Select the desired font size.
- : Select the position of the overlay in the image or click and drag the overlay to move it around in the live view.
- **Visible on all channels**: Turn off to show only on your currently selected channel. Turn on to show on all active channels.

- **Scene annotation: Ground plane**: Select to show a 3D grid projected onto the video to represent the ground surface. Before you create the ground plane, set the camera's installation height in the device location settings.
  - **Roll**: Drag the slider or enter a number to rotate the ground plane to the left or right.
  - **Tilt**: Drag the slider or enter a number to tilt the ground plane forward or backward.
  - **Rotation**: Drag the slider or enter a number to rotate the ground plane clockwise or counterclockwise.
  - **Distance from ground**: Drag the slider or enter a number to set the ground plane distance from the ground.
  - **Plane color**: Select the grid line color.
- **Scene annotations: 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.
  - **Text**: Enter an annotation text.
  - : Select the text color, outline color, background color and transparency.
  - **Size**: Select the desired font size.
  - **Icon and alignment**:
    - : Click to select any of the icons shown in the list to add them to the text box.
    - : Click to select the icon color, backplate color and transparency.
    - Click to select the position of the backplate in the image.
  - **Zoom range visiblility**: Set the zoom levels which the overlay will be shown within.

Dynamic LED strip

Dynamic LED strip patterns

Use this page to test the patterns of the dynamic LED strip.

Pattern: Select the pattern you want to test.

Duration: Specify the duration of the test.

Test: Click to start the pattern you want to test.

Stop: Click to stop the test. If you leave the page when a pattern plays, it will stop automatically.

To activate a pattern for indication or deterrence purposes, go to **System > Events** and create a rule. For an example, see .

Radar PTZ autotracking

Pair the radar with a PTZ camera to use radar autotracking. To establish the connection, go to **System > Edge-to-edge**.

Configure initial settings:

Camera mounting height: The distance from the ground to the height of the mounted PTZ camera.

Pan alignment: Pan the PTZ camera so that it points in the same direction as the radar. Click on the IP address of the PTZ camera to access it.

Save pan offset: Click to save the pan alignment.

Ground incline offset: Use the ground incline offset to fine tune the camera's tilt. If the ground is sloped, or if the camera is not mounted horizontally, the camera may aim too high or too low when tracking an object.

Done: Click to save your settings and continue with the configuration.

Configure PTZ autotracking:

Track: Select if you want to track humans, vehicles and/or unknown objects.

Tracking: Turn on to start tracking objects with the PTZ camera. The tracking automatically zooms in on an object, or a group of objects, to keep them in the view of the camera.

Object switching: If the radar detects multiple objects that won't fit in the PTZ camera's view, the PTZ camera tracks the object that the radar gives the highest priority, and ignores the others.

Object hold time: Determines for how many seconds the PTZ camera should track each object.

Return to home: Turn on to make the PTZ camera return to its home position when the radar no longer tracks any objects.

Return to home timeout: Determines how long the PTZ camera should stay at the tracked objects last known position before returning to home.

Zoom: Use the slider to fine tune the zoom of the PTZ camera.

Reconfigure installation: Click to clear all settings and go back to the initial configuration.

Autocalibration

Calibration finalized: Turn on when calibration has reached a satisfactory level and you want to freeze it.

Elevation

Autocalibration of elevation improves the vertical placement of radar bounding boxes. It doesn't affect the detection of objects, only the presentation.

Status: Shows if calibration data is available or not, and if calibration is still ongoing or not. The camera and radar collects calibration data continuously unless you turn on **Calibration finalized**.

Autocalibration: Turn on to autocalibrate the scene. The autocalibration occurs as soon as calibration data is available. Check the status for availability.

Smoothing: Smooths out differences in elevation.

- **High**: Set smoothing to **High** in scenes with small differences in elevation.
- **Low**: Set smoothing to **Low** in scenes with more significant differences in elevation, for example where there are hills or stairs.

Reset: Resets the autocalibration and the gathered calibration data.

Show elevation pattern: Turn on to visualize the calibration. Shows the vertical distance from the ground up to the camera in a pattern of colored dots. The pattern is only visible on this page, not in the video or radar stream.

Show color legend: Turn on to show a legend containing the colors of the elevation pattern and the vertical distance that each color represent. The legend is only visible on this page, not in the video or radar stream.

Color: Select the colors for the elevation pattern.

Show reference area: Turn on to show the area which the calibration is based on. The area is only visible on this page, not in the video or radar stream.

Azimuth

Autocalibration of azimuth improves the horizontal placement of radar bounding boxes. It doesn't affect the detection of objects, only the presentation.

Status: Shows if calibration data is available or not, and if calibration is still ongoing or not. The camera and radar collects calibration data continuously unless you turn on **Calibration finalized**.

Autocalibration: Turn on to autocalibrate the scene. The autocalibration occurs as soon as calibration data is available. Check the status for availability.

Reset: Resets the autocalibration and the gathered calibration data.

PTZ

PTZ channels

Add a PTZ channel: Click to create a new PTZ channel.

Click the PTZ channel to access settings.

Name: Enter a name for the PTZ channel. The maximum length is 64 characters.

Delete PTZ channel: Click to delete the selected PTZ channel.

PTZ: If you turn off PTZ for your camera's default view, it will turn on the view area for the channel.

Go to: View Areas: Link to **Video** > **View areas**. PTZ channels and view areas share the same pool.

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.

Guard tours

Guard tour: Create a guard tour.

- **Preset position**: Select to create a guard tour with preset positions.
- **Recorded**: Select to create a recorded guard tour.

Preset position

A guard tour with preset positions continuously streams footage from a selection of preset positions in a random or fixed sequence. You can choose how long the camera should stay at each preset position before moving on to the next. The guard tour will continue to run in an endless loop until you stop it, even when there are no clients (web browsers) streaming the footage.

Settings

- General settings
  - **Name**: Enter a name for the guard tour.
  - **Play guard tour in random order**: Turn on to make the camera move unpredictably between the preset positions during the guard tour.
  - **Pause between runs**: Enter your desired time interval between guard tours. You can enter any interval from 0 minutes to 2 hours and 45 minutes.
- Step settings
  - **Duration**: Choose how long you want the camera to stay at each preset position. The default value is 10 seconds, and the maximum allowed value is 60 minutes.
  - **Move speed**: Choose how quickly you want the camera to move to the next preset position. The default value is 70, but you can select any value from 1–100.

Preset positions: To select multiple preset positions, press shift while selecting the preset positions. Click and drag the preset positions to the **View order** area.

View order: Displays the preset positions included in the guard tour.

- **Import all preset positions**: Add all preset positions in the order they were created, starting from the oldest one.
- : Start the guard tour.

Recorded

A recorded tour replays a sequence of recorded pan/tilt/zoom movements, including their variable speeds and lengths.

General settings

- **Name**: Enter a name for the guard tour.
- **Pause between runs**: Enter your desired time interval between guard tours. You can enter any interval from 0 minutes to 2 hours and 45 minutes.

Recorded tour

- **Start recording tour**: Start recording the pan/tilt/zoom movements you want the guard tour to replicate.
- **Stop recording tour**: Stop recording the pan/tilt/zoom movements you want the guard tour to replicate.
- **Re-record**: Start a new recording of pan/tilt/zoom movements. This will overwrite your most recent recording.
- Start the recorded tour.
- Pause the recorded tour.
- Stop the recorded tour.

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 1,000 to limit the pan and tilt speed. Max proportional speed is defined as a percentage, where the value 1,000 equals 1,000%.
  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.
  - **Use cookie**: Select to allow the camera to recognize and separate users within the same user group.

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.

Settings

Use PTZ: Turn on to allow PTZ functionality in the selected view.

Reader

Connection

External reader (Input)

Use external OSDP reader: Turn on to use the device with an external reader. Connect the reader to the reader connector (IO1, IO2, 12V and GND).

Status:

- **Connected**: The device is connected to the active external reader.
- **Connecting**: The device is trying to connect to the external reader.
- **Not connected**: OSDP is turned off.

Reader protocol

Reader protocol type: Select the protocol to use for the reader functionality.

- **VAPIX reader**: Can only be used with an Axis door controller.
  - **Protocol**: Select **HTTPS** or **HTTP**.
  - **Door controller address**: Enter the IP address for the door controller.
  - **User name**: Enter the username of the door controller.
  - **Password**: Enter the password of the door controller.
  - **Connect**: Click to connect to the door controller.
  - **Select reader**: Select the entrance reader for the appropriate door.
- **OSDP**:
  - **OSDP address**: Enter the OSDP reader address. 0 is the default and most common address for single readers.
- **Wiegand**:
  - **Beeper**: Turn on to activate the beeper input.
  - **Input for beeper**: Select the I/O port used for the beeper.
  - **Input used for LED control**: Select how many I/O ports to use for controlling LED feedback on the device.
  - **Input for LED1/LED2**: Select which I/O ports to use for LED input.
  - **Standby color**: If no I/O port is used to control the LED, you can select a static color to show on the card reader indicator stripe.
  - **Color for state low/high**: If one I/O port is used for LED control, select the color to show for state low and state high respectively.
  - **Standby color/LED1 color/LED2 color/LED1 + LED2 color**: If two I/O ports are used for LED control, select the colors to show for idle, LED1, LED2, and LED1 + LED2 respectively.
  - **Keypress format**: Select how to format the PIN when it's sent to the access control unit.
    - **FourBit**: PIN `1234` is encoded and sent as 0x1 0x2 0x3 0x4. This is the default and most common behaviour.
    - **EightBitZeroPadded**: PIN `1234` is encoded and sent as 0x01 0x02 0x03 0x04.
    - **EightBitInvertPadded**: PIN `1234` is encoded and sent as 0xE1 0xD2 0xC3 0xB4.
    - **Wiegand26**: The PIN is encoded in Wiegand26 format with an 8 bit facility code and a 16 bit id.
    - **Wiegand34**: The PIN is encoded in a Wiegand34 format with a 16 bit facility code and a 16 bit id.
    - **Wiegand37**: The PIN is encoded in a Wiegand37 format (H10302) with a 35 bit id.
    - **Wiegand37FacilityCode**: The PIN is encoded in a Wiegand37 format (H10304) with a 16 bit facility code and a 19 bit id.
  - **Facility code**: Enter the facility code to be sent. This option is only available for some keypress formats.

Output format

Select data format: Select in which format to send card data to the access control unit.

- **Raw**: Transmits the card data as it is.
- **Wiegand26**: Encodes the card data in Wiegand26 format with an 8 bit facility code and a 16 bit id.
- **Wiegand34**: Encodes the card data in Wiegand34 format with a 16 bit facility code and a 16 bit id.
- **Wiegand37**: Encodes the card data in Wiegand37 format (H10302) with a 35 bit id.
- **Wiegand37FacilityCode**: Encodes the card data in Wiegand37 format (H10304) with a 16 bit facility code and a 19 bit id.
- **Custom**: Define your own formatting.

Facility code override mode: Select an option for overriding the facility code.

- **Auto**: Doesn't override the facility code, and creates a facility code from the input data auto detection. Either uses the card's original facility code, or forges it from excess bits of a card number.
- **Optional**: Uses the facility code from the input data, or overrides with a configured optional value.
- **Override**: Always overrides with a specified facility code.

Chip types

Chip types

Activate chip type: Select a chip type from the list to activate it.

Active chip types shows a list of all active chip types and whether they use default or custom data sets.

⋮ The context menu contains:

- **Deactivate**: Click to remove the chip type from the list of active chip types.

Data sets

Invert byte order for all chip types using the full card serial number (CSN): Turn on to reverse the byte order of the card serial number. The card serial number is the default data.

Invert byte order for all chip types using secure card data: Turn on to reverse the byte order of the secure card data for chip types that use a custom data set.

Add data set: Select a chip type and click to add a data set. For custom data.

- **Name of data set**: Rename the data set to help you identify the data. The name must be unique. It works as an ID in, for example, the API.
- **Enabled**: Turn off to stop using the data set without deleting it.
- **Required data**: If secure card data for some reason isn't accessible, the device doesn't send any data to the door controller when this setting is turned on. Turn off to send CSN to the door controller in case secure card data isn't accessible.
- **Use as authenticator**: Turn off if you don't want to use secure card data for authentication, but only send it as metadata valid for VAPIX protocol.
- **Offset (bits)**: Enter the start position of the data. 0 means that the start position is the first bit.
- **Length (bits)**: Enter the length of the data. 0 means that any length of data will be read.
- **Use data on card**: Turn on to use secure card data. Turn off to use CSN instead of secure card data.

The remaining settings are chip type specific, and are used to define how to read secure card data.

PIN

The PIN settings must match the ones configured in the access control unit.

Length (0–32): Enter the number of digits in the PIN. If users aren't required to use a PIN when they use the reader, set the length to 0.

Timeout (seconds, 3–50): Enter the number of seconds that need to pass before the device returns to idle mode when no PIN is received.

Entry list

With Entry list, you can set up the device to allow credential holders to use their card, PIN or a QR Code® to perform different actions, such as opening a door. You store the credentials locally in the device. You can also combine this functionality with an external door controller.

QR Code is a registered trademark of Denso Wave Incorporated in Japan and other countries.

Credential holders

Use Entry list: Turn on to use the Entry list functionality.

Use connected door controller: Turn on if the device is already connected to a door controller. If someone presents a credential that doesn't exist in Entry list, we'll send the request to the connected door controller. We don't send credentials that are available in Entry list.

Add credential holder: Click to add a new credential holder.

First name: Enter a first name.

Last name: Enter a last name.

Credential type:

- **PIN**:
  - **PIN**: Enter a unique PIN or click **Generate** to create one automatically.
- **Card**:
  - **UID**: Enter the card's UID and bit length, or click **Get latest** to fetch the data from the latest card swipe.
- **QR Code®**

Event condition: Select one or more conditions to trigger when the credential holder uses their credential. To set up the resulting action, go to **System > Events** and create a rule, using the same condition you select here.

Valid from: Select **Current device time** to activate the credential immediately. Clear to specify when to activate the credential.

Valid to:

- **No end date**: Credential is valid indefinitely.
- **End date**: Specify the date and time when the credential becomes invalid.
- **Number of times**: Specify how many times the credential holder can use the credential. The value in the field reduces as the credential is used, to show the remaining uses.

Notes: Enter optional information.

Suspend: Select to make the credential temporarily invalid.

Download QR Code when saving: If you selected QR Code as credential type, select this checkbox to download the QR code when you click **Save**.

Event log

The event log shows a list of entry list events. The maximum size of the log file is 2 MB, which equals approximately 6000 events.

Export all: Click to export all events in the list. To export only a subset, select the events that you are interested in. The events are exported into a CSV file.

Filter: Click to show events that occurred during a specific time range.

: Type to search for all matching content in the list.

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.

Microphone: Select the microphone that will be used for audio input.

Power type: Select power type for your input.

Apply changes: Apply your selection.

Noise cancellation: Turn on to improve audio quality by removing background noise.

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.

Audio out

Enable Output: Turn on or off audio from the audio out connector.

Audio out synchronization: Set a time to match the delay difference between the audio out (3.5 mm) port and video stream.

Stream

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

Audio clips

Add clip: 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.

Sources

Devices

Add camera source: Click to add a new camera source.

- **Network discovery**: Search for an IP address manually or select an Axis device from the list.
  - **Streaming protocol**: Select which protocol to use
  - **Port**: Enter the port number used for streaming video.
    - 554 is the default value for **RTSPT**
    - 80 is the default value for **RTSP over HTTP**
    - 443 is the default value for **RTSP over HTTPS**
  - **API port**: Enter the port number for sending HTTP requests to the device. This is only used if **Connect to cameras through secure connections** is turned off.
    - 80 is the default value.
  - **Secure API port**: Enter the port number for sending HTTPS requests to the device.
    - 443 is the default value.
  - **Account**: Enter the username for the device.
  - **Password**: Enter the password for the device.
  - **Include motion events**: Select to allow using motion detected by the camera as an event condition. This setting is only available for Axis cameras.
- **Manual**: Add a device manually.
  - **Name**: Enter the video source's name.
  - **Address or hostname**: Enter the device's IP address or hostname.
  - **Account**: Enter the username for the device.
  - **Password**: Enter the password for the device.
  - **Include motion events**: Select to allow using motion detected by the camera as an event condition. This setting is only available for Axis cameras.

The context menu contains:

Edit: Edit the properties of the video source.

Delete: Delete the video source.

Media

Add: Click to add a new media source.

- Upload or drag and drop a media file. You can use .mp4, .mkv, .jpeg or .png files.
- **Storage location**: Select the location from the drop-down list.

Light

Overview

Light status

Shows the different light activities that run on the device. You can have up to 10 activities in the light status list at the same time. When two or more activities run at the same time, the activity with the highest priority shows the light status. That row will be highlighted in green in the status list.

Signaling LED status

Shows the different signaling LED activities that run on the device. You can have up to 10 activities in the signaling LED status list at the same time. When two or more activities run at the same time, the activity with the highest priority shows the signaling LED status. That row will be highlighted in the status list.

Siren status

Shows the different siren activities that run on the device. You can have up to 10 activities in the siren status list at the same time. When two or more activities run at the same time, the activity with the highest priority will run. That row will be highlighted in the status list.

Audio LED status

Shows the different audio LED activities that run on the device. You can have up to 10 activities in the audio LED status list at the same time. When two or more activities run at the same time, the activity with the highest priority will run. That row will be highlighted in green in the status list.

Audio speaker status

Shows the different audio speaker activities that run on the device. You can have up to 10 activities in the audio speaker status list at the same time. When two or more activities run at the same time, the activity with the highest priority will run. That row will be highlighted in green in the status list.

Maintenance

Maintenance mode: Turn on to pause the light and siren activities during the device maintenance. When you turn on maintenance mode, the device shows a white pulsating light pattern in a triangle and the siren is silent. It protects the installer from hearing damage and dazzling bright light.

Maintenance has priority 11. Only system specific activities with higher priority can disrupt the maintenance mode.

Maintenance mode survives a reboot. For example, if you set the time to 2 hours, turn off the device and restart it one hour later, the device will be in maintenance mode for another hour.

When you do a default reset, the device returns to maintenance mode.

Duration

- **Continuous**: Select to let the device stay in maintenance mode until you turn it off.
- **Time**: Select to set a time when the maintenance mode will turn off.

Health check

Check: Do a health check of the device to make sure the light and siren work fine. It turns on each light section one after another and plays a test tone to check that the device works fine. If the health check doesn't pass, go to the system logs for more information.

Profiles

Profiles

A profile is a collection of set configurations. You can have up to 30 profiles with different priorities and patterns. The profiles are listed to give an overview of name, priority, and light and siren settings.

Create: Click to create a profile.

- **Preview/Stop preview**: Start or stop a preview of the profile before you save it.

Note

You can't have two profiles with the same name.

- **Name**: Enter a name of the profile.
- **Description**: Enter a description of the profile.
- **Light**: Select from the drop-down menu what kind of **Pattern**, **Speed**, **Intensity**, and **Color** of the light you want.
- **Siren**: Select from the drop-down menu what kind of **Pattern** and **Intensity** of the siren you want.
- Start or stop a preview of only the light or siren.
- **Duration**: Set the duration of the activities.
  - **Continuous**: Once started, it runs until it's stopped.
  - **Time**: Set a specified time for how long the activity will last.
  - **Repetitions**: Set how many times the activity should repeat itself.
- **Priority**: Set the priority of an activity to a number between 1 and 10. Activities with priority numbers higher than 10 can't be removed from the status list. There are three activities with higher priority than 10; **Maintenance** (11), **Identify** (12), and **Health check** (13).
- **Resume on startup**: Select to automatically resume an active profile after restart.

Import: Add one or more profiles with predefined configuration.

- **Add**: Add new profiles.
- **Delete and add**: The old profiles are deleted, and you can upload new profiles.
- **Overwrite**: Updated profiles overwrite the existing profiles.

To copy a profile and save it to other devices, select one or more profiles and click **Export**. A .json file is exported.

Start a profile. The profile and its activities appear in the status list.

Choose to **Edit**, **Copy**, **Export**, or **Delete** the profile.

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 all or part of a recording. You can export to **Matroska** or **MP4** format.

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.

Media

+ Add: Click to add a new file.

Storage location: Select to store the file in the internal memory or in the onboard storage (SD card, if available).

⋮ The context menu contains:

- **Information**: View information about the file.
- **Copy link**: Copy the link to the file's location on the device.
- **Delete**: Delete the file from the storage location.

Cellular routing

Main mode

Enable forwarding to connected device: Click to forward the network ports to the connected device.

Note

When forwarding the network ports, the connected camera will only be accessible over the wireless IP address. To reach the back box after forwarding, you can access it through the back box management ports.

Configurations in connected mode

Back box management ports

http: Enter the management port number for http.

https: Enter the management port number for https.

rtsp: Enter the management port number for rtsp.

ssh: Enter the management port number for ssh.

Advanced port mapping: Click to configure the port mapping.

Port map mode

- **Connected device as primary**: Select Connected device as primary to make the connected camera use the standard ports.
- **Back box as primary**: Select Back box as primary to make the back box use the standard ports.

Connected device ports

Base port number: Enter the starting port number for the secure port of the first LAN host.

Base port alignment: Enter the alignment for the starting source port for every LAN host port range.

Advanced DHCP configuration: Configure the cellular routing Dynamic Host Configuration Protocol (DHCP).

Check DHCP server presence: Turn on to prevent conflicts and disable the back box DHCP server if an existing DHCP server is detected on the network.

Lease MAC address: Enter the MAC address of the device that should be primary if multiple devices are connected.

DHCP server mode: Select if the DHCP server mode should be in local or passthrough mode.

- **Local**: Select Local to assign a private IP address that is separate from the cellular network.
- **Passthrough**: Select passthrough to receive the cellular IP address.

Local private network configuration

Starting IP address: Enter the first IP address in the DHCP allocation range.

Ending IP address: Enter the last IP address in the DHCP allocation range.

Auto recovery: Turn on to automatically attempt to recover the cellular network connection.

Apps

: View the security updates in AXIS OS and ACAP 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.

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 (PTP)**: Synchronize using the precision time protocol.
- **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.
  - **Trusted NTS KE CA certificates**: Select the trusted CA certificates to use for secure NTS KE time synchronization, or leave at none.
  - **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 be connected to a DHCP server (v4 or v6) before you can select this option. If both versions are available, the device prefers IANA time zones over POSIX, and DHCPv4 over DHCPv6.
  - DHCPv4 uses Option 100 for POSIX time zones and Option 101 for IANA time zones.
  - DHCPv6 uses Option 41 for POSIX and Option 42 for IANA.
- **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.

Time sync status: Shows NTP synchronization information and PTP state.

Network time synchronized capture: Turn on to allow multiple cameras to capture images simultaneously.

Device location

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

- **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

Interactive device image: Click the buttons in the image to simulate real key presses. This allows you to try out configurations or troubleshoot the hardware without having physical access to the device.

Latest credentials: Shows information about the credentials that were last registered.

Show the latest credentials data.

The context menu contains:

- **Reverse UID**: Invert the byte order of the UID.
- **Revert UID**: Revert the byte order of the UID back to the original order.
- **Copy to clipboard**: Copy the UID.

Check credentials: Enter a UID or a PIN and submit to check the credentials. The system will respond in the same way as if you used the credentials at the device. If both UID and PIN is required, start by entering the UID.

Network

Network

IPv4

Assign IPv4 automatically: Select IPv4 automatic IP (DHCP) to let the network assign your IP address, subnet mask, and router automatically, without manual configuration. We recommend using automatic IP assignment (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.

Note

If DHCP is disabled, features that rely on automatic network configuration, such as hostname, DNS servers, NTP, and others, may stop working.

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

Network discovery protocols

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

LLDP and CDP: Select to allow automatic discovery on the network. If LLDP and CDP are not allowed, it can affect the PoE power negotiation. To resolve any issues with the PoE power negotiation, configure the PoE switch for hardware PoE power negotiation only.

Neighbors: Click to show information about neighboring devices connected to the same network.

One-click cloud connection

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

Allow O3C:

- **One-click**: This is the default option. To connect to O3C, press the control button on the device. Depending on the device model, either press and release or press and hold, until the status LED flashes. Register the device with the O3C service within 24 hours to enable **Always** and stay connected. If you don't register, the device will disconnect from O3C.
- **Always**: The device continuously attempts to connect to an O3C service over the internet. Once you register the device, it stays connected. Use this option if the control button is out of reach.
- **No**: Disconnects 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.
    - **Link up**: Sends a trap message when a link changes from down to up.
    - **Link down**: Sends a trap message when a link changes from up to down.
    - **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.
  - **Privacy**: Select what encryption to use for protecting your SNMP data.
  - **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. Note that the password must comply with the password policy, see *Accounts, on page 102*.

Network ports

Power over Ethernet

- **Allocated power**: Number of watts (W) that are currently allocated.
- **Total PoE consumption**: Number of watts (W) that are consumed.
- **Keep PoE active during device restart**: Turn on to supply power to connected devices during a restart of the recorder.

Click to show or hide the ports image.

- Click a port in the image to see the port details in the port list.

Port list

- **Port**: The port number.
- **PoE**: Turn on or off PoE for the port.
- **Network**: Turn on or off network for the port.
- **Security**: Select the required type of network security for each port.

  Note

  We recommend that you only connect one device directly to the PoE port if you want to use 802.1x authentication or MACsec security feature. This security feature only supports the authentication of the Axis device ID certificate.

  - **Disabled**: Security check is off.
  - **Not required**: 802.1x authentication is optional.
  - **Authentication required**: 802.1x authentication is mandatory.
  - **MACSec secured required**: Both 802.1x and MACSec are mandatory.
- **Status**: Shows if there is device connected to this port.
- **Friendly name**: The friendly name is set in **Network settings**. The default name is a combination of the model and the media access control address (MAC address) of the connected device.
- **Power consumption**: Number of watts (W) that are currently consumed and allocated by the connected device.

Modem

Cellular network

Access point name (APN): Enter the name of the access point.

Test cellular connection

Address: To check if the device can reach a specific address, enter the hostname or IP address of the host you want to test and click **Start**.

Port: If needed, change the port number.

Radio parameters

Here you can see the current radio parameters of the cellular network that you are currently connected to, including radio generation, radio band, cell connection information, and signal strength metrics. This information is refreshed every 10 seconds.

This information is valuable for network integrators when they determine the optimal placement for fixed device installations (such as the AXIS TP3604–E Cellular Back Box). It is also useful for troubleshooting to determine whether performance degradation is caused by network conditions or other factors.

SIM management

If you insert a SIM card with its PIN protection enabled into the back box, enter the SIM PIN and click **Unlock with SIM PIN** to unlock it.

SIM PIN: Enter a valid SIM PIN for the SIM card that is inserted in the back box.

Enable SIM PIN: Turn on or turn off the SIM PIN protection on the SIM card.

Change SIM PIN: If the PIN code is required for use, you can change the PIN. Enter the current SIM PIN and a new SIM PIN. Click **Save**.

The SIM card will be blocked after three incorrect PIN attempts and cannot be used until it is unblocked. To unblock the SIM card, click **Unblock SIM** and enter the PUK (Personal Unblocking Key) code provided by the cellular network provider, and a new PIN code.

SIM PIN: Enter the SIM PIN.

SIM PUK: Enter the PUK from the SIM card provider. You have ten attempts to enter the correct PUK.

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.

Add certificate : Click to add a certificate. A step-by-step guide opens up.

- **More** : Show more fields to fill in or select.
- **Secure keystore**: Select to use **Trusted Execution Environment (SoC TEE)**, **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/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:

- **Trusted Execution Environment (SoC TEE)**: Select to use SoC TEE for secure keystore.
- **Secure element (CC EAL6+, FIPS 140-3 Level 3)**: 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.

Enrollment over Secure Transport

You can configure and enable certificate enrollment. Once certificate enrollment is enabled, certificates used by TLS-based applications, such as HTTPS and 802.1X, will rotate their certificates automatically.

- **URL**: Enter the URL (HTTPS) to the enrollment server.
- **Services**: Select one or several services for the certificates.
- **Client certificate**: Select a client certificate for the authentication towards the EST server.
- **CA certificates**: Select the CA certificates from the EST server HTTPS endpoint so that the Axis device trusts the configured EST server.
  - **Clear all**: Click to clear the selection of CA certificates.
- **Reset**: Click to clear all selections.
- **Connect**: This button is visible if you are not connected to the server. Click to connect to the server. The EST server needs to trust this certificate for certificate enrollment.
- **Enroll**: This button is visible if you are connected to the server. Click to start certificate enrollment.

Cryptographic policy

The cryptographic policy defines how encryption is used to protect data.

Active: Select which cryptographic policy to apply to the device:

- **Default — OpenSSL**: Balanced security and performance for general use.
- **FIPS — Policy to comply with FIPS 140–2**: Encryption compliant with FIPS 140-2 for regulated industries.

Network access control and encryption

IEEE 802.1x

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

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

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.

Prevent brute-force attacks

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

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

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

Firewall

Firewall: Turn on to activate the firewall.

Default Policy: Select how you want the firewall to handle connection requests not covered by rules.

- **ACCEPT:** Allows all connections to the device. This option is set by default.
- **DROP:** Blocks all connections to the device.

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

+ New rule: Click to create a rule.

Rule type:

- **FILTER**: Select to either allow or block connections from devices that match the criteria defined in the rule.
  - **Policy**: Select **Accept** or **Drop** for the firewall rule.
  - **IP range**: Select to specify a range of addresses to allow or block. Use IPv4/IPv6 in **Start** and **End**.
  - **IP address**: Enter an address that you want to allow or block. Use IPv4/IPv6 or CIDR format.
  - **Protocol**: Select a network protocol (TCP, UDP, or Both) to allow or block. If you select a protocol, you must also specify a port.
  - **MAC**: Enter the MAC address of a device that you want to allow or block.
  - **Port range**: Select to specify the range of ports to allow or block. Add them in **Start** and **End**.
  - **Port**: Enter a port number that you want to allow or block. Port numbers must be between 1 and 65535.
  - **Traffic type**: Select a traffic type that you want to allow or block.
    - **UNICAST**: Traffic from a single sender to a single recipient.
    - **BROADCAST**: Traffic from a single sender to all devices on the network.
    - **MULTICAST**: Traffic from one or more senders to one or more recipient.
- **LIMIT**: Select to accept connections from devices that match the criteria defined in the rule but apply limits to reduce excessive traffic.
  - **IP range**: Select to specify a range of addresses to allow or block. Use IPv4/IPv6 in **Start** and **End**.
  - **IP address**: Enter an address that you want to allow or block. Use IPv4/IPv6 or CIDR format.
  - **Protocol**: Select a network protocol (TCP, UDP, or Both) to allow or block. If you select a protocol, you must also specify a port.
  - **MAC**: Enter the MAC address of a device that you want to allow or block.
  - **Port range**: Select to specify the range of ports to allow or block. Add them in **Start** and **End**.
  - **Port**: Enter a port number that you want to allow or block. Port numbers must be between 1 and 65535.
  - **Unit**: Select the type of connections to allow or block.
  - **Period**: Select the time period related to **Amount**.
  - **Amount**: Set the maximum number of times a device is allowed to connect within the set **Period**. The maximum amount is 65535.
  - **Burst**: Enter the number of connections allowed to exceed the set **Amount** once during the set **Period**. Once the number has been reached, only the set amount during the set period is allowed.
  - **Traffic type**: Select a traffic type that you want to allow or block.
    - **UNICAST**: Traffic from a single sender to a single recipient.
    - **BROADCAST**: Traffic from a single sender to all devices on the network.

- **MULTICAST**: Traffic from one or more senders to one or more recipient.

Test rules: Click to test the rules that you have defined.

- **Test time in seconds**: Set a time limit for testing the rules.
- **Roll back**: Click to roll back the firewall to its previous state, before you have tested the rules.
- **Apply rules**: Click to activate the rules without testing. We don't recommend that you do this.

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

Device 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**: Doesn't have access to change any 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.

Password policy

Choose the complexity of passwords for all accounts connecting to this device

- **None**: No password complexity requirements
- **Length**: Passwords must be at least 15 characters long. No additional complexity requirements are required. This policy follows U.S. NIST 800-63B and Japan JC-Star.
- **Complexity**: Passwords must be at least 12 characters long and include one uppercase letter, one lowercase letter, one numeric digit, and one special character. This policy follows South Korea NIS, German BSI, France ANSSI and Singapore CLS among others.

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.

ONVIF accounts

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.

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.
  - 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.

SSH accounts

Add SSH account: Click to add a new SSH account.

- **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.

Authentication

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**, **Open ID**, and **Client Credential Grant**.

HTTPS: Select to use HTTPS.

The context menu contains:

- **Update virtual host**
- **Delete virtual host**

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.

Client Credentials Grant Configuration

Admin claim: Enter a value for the admin role.

Verification URI: Enter the web link for the API endpoint authentication.

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.

Save: Click to save the values.

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*.

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

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

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

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

Pre-announcement tone: Play tone on incoming call: When a SIP call is made to the audio device, then the device plays a pre-defined audio clip. You must enable SIP for the audio device. For the SIP caller to hear a ring tone while the audio device plays the audio clip, you must configure the SIP account for the device to not answer the call automatically.

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

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

Recipients

You can set up your device to notify recipients about events or send files.

Note

If you set up your device to use FTP or SFTP, don't change or remove the unique sequence number that's added to the file names. If you do that, only one image per event can be sent.

The list shows all the recipients currently configured in the product, along with information about their configuration.

Note

You can create up to 20 recipients.

Add a recipient: Click to add a recipient.

Name: Enter a name for the recipient.

Type: Select from the list:

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

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

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

Note

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

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

Test: Click to test the setup.

⋮ The context menu contains:

View recipient: Click to view all the recipient details.

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

Delete recipient: Click to delete the recipient permanently.

Schedules

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

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

Manual triggers

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

MQTT

MQTT (Message Queuing Telemetry Transport) is a standard messaging protocol for the Internet of Things (IoT). It was designed for simplified IoT integration and is used in a wide variety of industries to connect remote devices with a small code footprint and minimal network bandwidth. The MQTT client in Axis device 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 Knowledge base*.

ALPN

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

MQTT client

Connect: Turn on or off the MQTT client.

Status: Shows the current status of the MQTT client.

Broker

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

Protocol: Select which protocol to use.

Port: Enter the port number.

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

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

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

Password: Enter a password for the username.

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

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

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

Include 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.

Note

If you edit the subscription filter, make sure to update the connected events.

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

- **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.

- **Show video in call**: Show the incoming video stream on the device's display.

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.
- **Registrar**: Enter the IP address of the SIP server. The IP address identifies the server component that receives and stores the current contact location of a SIP user.
- **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.

Protocols

Select 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.

Multicast controller

User multicast controller: Turn on to activate multicast controller.

Audio codec: Select an audio codec.

Source: Add a new multicast controller source.

- **Label**: Enter the name of a label that is not already used by a source.
- **Source**: Enter a source.
- **Port**: Enter a port.
- **Priority**: Select a priority.
- **Profile**: Select a profile.
- **SRTP key**: Enter an SRTP key.

The context menu contains:

Edit: Edit the multicast controller source.

Delete: Delete the multicast controller source.

Storage

Format disk: Appears when an onboard storage isn't formatted. Click **Format disk** and follow the step-by-step guide to format your storage.

Network storage

Network storage: Turn on to use 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

For devices with SD card

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.

For devices with hard drive

Hard drive

- **Free**: The amount of free disk space.
- **Status**: If the disk is mounted or not.
- **File system**: The file system used by the disk.
- **Encrypted**: If the disk is encrypted or not.
- **Temperature**: The current temperature of the hardware.
- **Overall heath test**: The result after checking the health of the disk.

Tools

- **Check**: Check the storage device for errors and tries to repair it automatically.
- **Repair**: Repair the storage device. Active recordings will pause during the repair. Repairing a storage device may result in lost data.
- **Format**: Erase all recordings and format the storage device. Choose a file system.
- **Encrypt**: Encrypt stored data.
- **Decrypt**: Decrypt stored data. The system will erase all files on the storage device.
- **Change password**: Change the password for the disk encryption. Changing the password doesn't disrupt ongoing recordings.
- **Use tool**: Click to run the selected tool

Unmount: Click before you disconnect the device from the system. This will stop all ongoing recordings.

Write protect: Turn on to protect the storage device from being overwritten.

Autoformat: The disk will automatically format using the ext4 file system.

For devices with RAID

RAID

- **Free**: The amount of free disk space.
- **Status**: If the disk is mounted or not.
- **File system**: The file system that is used by the disk.
- **Encrypted**: If the disk is encrypted or not.
- **Temperature**: The current temperature of the hardware.
- **Overall heath test**: The result after checking the health of the disk.
- **RAID level**: The RAID level used for the storage. Supported RAID levels are 0, 1, 5, 6, 10.
- **RAID status**: The RAID status of the storage. Possible values are **Online**, **Degraded**, **Syncing**, and **Failed**. The syncing process may take several hours.

Tools

Note

When you run the following tools, make sure to wait until the operation is done before closing the page.

- **Check**: Check the storage device for errors and tries to repair it automatically.
- **Repair**: Repair the storage device. Active recordings will pause during the repair. Repairing a storage device may result in lost data.
- **Format**: Erase all recordings and format the storage device. Choose a file system.
- **Encrypt**: Encrypt data that is stored. All files on the storage device will be erased.
- **Decrypt**: Decrypt data that is stored. All files on the storage device will be erased.
- **Change password**: Change the password for the disk encryption. Changing the password doesn't disrupt ongoing recordings.
- **Change RAID level**: Erase all recordings and change the RAID level for the storage.
- **Use tool**: Click to run the selected tool.

Hard drive status: Click to view the hard drive status, capacity, and serial number.

Write protect: Turn on write protection to protect the storage device from being overwritten.

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 28* for a description of this setting.

Frame rate: See *Stream, on page 28* for a description of this setting.

Compression: See *Stream, on page 28* for a description of this setting.

Zipstream: See *Stream, on page 28* for a description of this setting.

Optimize for storage: See *Stream, on page 28* for a description of this setting.

Dynamic FPS: See *Stream, on page 28* for a description of this setting.

Dynamic GOP: See *Stream, on page 28* for a description of this setting.

Mirror: See *Stream, on page 28* for a description of this setting.

GOP length: See *Stream, on page 28* for a description of this setting.

Bitrate control: See *Stream, on page 28* for a description of this setting.

Include overlays: Select what type of overlays to include. See *Overlays, on page 31* for information about how to add overlays.

Include audio: See *Stream, on page 28* for a description of this setting.

ONVIF

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.

Z-Wave

Z-Wave configuration

Gateway settings wireless I/O

- **Z-Wave**: Turn on to use Z-Wave on your device.

Device management

The settings vary according to device, read the manual of the Z-Wave device.

Add device: Add a Z-Wave device. The Axis device looks for Z-Wave devices in the Z-Wave network that you can add according to its user manual.

Remove the device. The Axis device looks for Z-Wave devices in the Z-Wave network that you can remove according to its user manual..

Status: The status of the device is color coded.

- **Alive**: The device is active and working.
- **Sleeping**: The device is in a low-power state in a controlled manner. Notifications happen instantly, but if you change settings these don't take affect until the device wakes up.
- **Down**: The node is currently unresponsive and there can be an error in the network.
- **Unavailable**: The device is not available on the network.

Device name: The name of the device. This is the name you give the device when it is added.

Device type: What type of device it is.

State: Shows the condition of the Z-Wave device such as sensor value, current setting, or if the device is turned on or off. This depends on the connected device.

I/O port: Shows a number between 1–6 depending on what port the device is connected to. When connected, these devices can also be used in the video management system.

Battery level: Shows how much battery is left in the connected device, if the device is run on batteries. When the battery is low, it is indicated by an icon that shows a drained battery, replace the battery as soon as possible

Endpoint

Name: Give the sensor a user friendly name.

Location: Enter the location to more easily identify the device, for example Front door.

Endpoint type: This information is provided by the Z-Wave device.

Sensor data: Available sensors and current show other units by changing the settings. For example change temperature units from Celsius to Fahrenheit depending on the sensor data available,

Temperature threshold: Set and edit events that are triggered when the temperature is above or below the threshold.

Binary Switch: Use the toggle to turn the binary switch On or Off.

Multilevel sensor

A Z-Wave device supporting more than one sensor, for example a combination of temperature sensor, motion sensor, and light sensor. To change the units in the live view, click and choose **View settings**.

Troubleshooting

Use the **Advanced settings** to help troubleshoot or refine the Z-Wave device settings.

Advanced settings

The settings vary according to device, read the manual of the Z-Wave device. The settings are device specific and are found under **Device management**, extend the device information of the node required, then click **Advanced settings** to see the settings for that device, examples are detailed below.

Anti-theft unlock

The device is currently locked by another device and can be unlocked by entering the Magic Code for the device.

Association: One device controls another device.

In order to control a different device, the controlling device has to maintain a list of devices that will receive commands. These lists are called association groups and they are always related to certain events, for example, button pressed and sensor triggers. In case an event happens, all devices stored in the respective association group will receive the same command.

Basic

Here you can set which command should be used, for example on/off. Check the manual of the Z-Wave device to see which valid values that can be set. Trigger a Set by changing the value and clicking outside the input field

Examples:

- `0`: off
- `255`: on
- `1-99`: 1 to 99%

Central scene

Settings vary according to device, check the manual of the Z-Wave device. Use this feature to set different codes, button presses for different scenes or scenarios. For example, a garage door could have one scene to open the door and a different scene to close the door.

Configuration

Settings vary according to device, check the manual of the Z-Wave device.

Software update

Update the software on your Z-Wave device. Save the software on your Axis device in the temp file and then the Axis device will upgrade the Z-Wave device (sleeping nodes will need manual triggers). For more information on software updates, see your Z-Wave device manual.

Indicator

Configure different indicators to represent different things, for example you can set an LED indicator to flash a 3 times, or a buzzer to sound.

Supported indicators: A list displaying the supported indicators. Settings vary according to device, check the manual of the Z-Wave device.

Meter

Settings here can vary according to device, check the manual of the Z-Wave device.

- **Meter type**: For example, Electric meter.
- **Units**: Measuring unit. For example, kWh, W, V, A
- **Rate type**: For example, import (Consumed measurement)

Meter reading

- **Preferred unit**: A list of available options will be displayed here.

Reset meter: This operation will reset all accumulated values stored in the meter device. You must first confirm you have read understood the actions of resetting the meter.

Notification

Settings here can vary according to device, check the manual of the Z-Wave device.

Supported notifications: Details of supported notifications will be listed here.

Fetch notification report:

- **Type**: Available types will display here.
- **Event**: List of configured events will display here.

Control notification status:

- **Type**: Available types will display here.
- **Activated**: Current status is displayed here.

Wake-up

Allows a sleeping node (one that sends data only when it needs to) to receive data by notify an always-listening device that it is awake and ready to receive data, does not require the node to be manually triggered.

Maximum interval: Time in seconds, for example `86400` seconds.

Minimum interval: Time in seconds, for example `600` seconds.

Default interval: Time in seconds, for example `14400` seconds.

Interval step: Time in seconds, for example `600` seconds.

Configure wake-up interval:

- **Wake-up interval**: The number of seconds it takes before the gateway will synchronize with the device, for example `4200` seconds. The **Wake-up interval must** be devisable by the number of seconds in the interval step. Furthermore the value needs to be within the range defined by the minimum and maximum interval, see the examples given.
- **Node ID**: The ID of the node to be notified on wake-up, use 255 to broadcast to all nodes.

SmartStart

You can add a Z-Wave device to the provisioning list with SmartStart inclusion. A Z-Wave device added to the provisioning list is automatically added to the device management list as soon as the device is powered on.

Note

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

+ **Add device information**: When a device is found follow the instructions as per your Z-Wave device installation manual. Manually add **Device name** and **Device location**, these will be displayed in the **Device management** table.

: Hover over a device in the list to show the icon. Click the icon to delete it from the list.

Status: The status of the device are color coded.

- **Alive**: The device is active and working.
- **Sleeping**: The device is in a low-power state in a controlled manner. Notifications happen instantly, but if you change settings these don't take affect until the device wakes up.
- **Down**: The node is currently unresponsive and there can be an error in the network.
- **Unavailable**: The device is not available on the network.

Device Specific Key: The DSK string code that is found on the package or the device.

Device name: The name of the device. This is the name you give the device when it is added.

Device type: What type of device it is.

Device location: The location where the device is positioned. You enter this manually.

Video input

Each video input is terminated using a coax/BNC connector and displayed as a numbered channel.

Connect a 75 Ohm coaxial video cable; the recommended maximum length is 250 m (800 ft).

Automatic: The default setting. The encoder detects the video standard and resolution automatically.

Manual: Lock the channel to the selected video standard and resolution.

Reload: Click to restore to the current encoder settings.

Mark as configured: Click to acknowledge the video input settings. The video input is shown as configured in the Status page.

Save changes & restart: Click to save the changes and restart the device. If you restart the device, it will affect ongoing recordings.

Video out

Video out

You can connect an external monitor to the device through an HDMI cable or, for some devices, an SDI cable.

Output: Select an output port.

Outputs: Shows the type of video outputs currently enabled on the device.

Display mode: Select your preferred mode from the list and go to **Maintenance** and click **Restart**. Your device reboots to apply the changes.

Scan mode: Select the scan mode that applies to your hardware configuration.

- **Progressive**: The default option. Select this option for all modern hardware such as LCD computer monitors and HDTVs.
- **Interlaced**: A legacy option for older hardware.

SDI level (SMPTE 424): Select the SDI level that applies to your hardware configuration.

HDMI

You can connect an external monitor to the device through an HDMI cable.

Single source

A stream from an individual camera or group view is displayed on the external monitor.

- **Source**: Select what do display on the external monitor.
- **Rotate image 180°**: Turn on to rotate the image.
- **Mirror image**: Turn on to flip the image.
- **Dynamic overlays**: Turn on to overlay.

Quad view

View streams from four separate cameras at the same time on the external monitor.

- **Source**: Select a different camera from each of the four drop-down lists. The image beside the source shows where the video from that camera will be displayed on the screen.

Playlist

Single streams from multiple cameras alternate on the external monitor.

- **Rotate image 180°**: Turn on to rotate the image.
- + **Add**: Click to add a camera to the playlist.
- **Source**: Select the desired camera.
- **Duration**: Set how long (in mm:ss) the playlist will stream from this camera in each rotation.
- **Create**: Click to save.

Picture-in-picture

Two streams are displayed on the external monitor at the same time. One stream fills the display and the other is a smaller picture. **Position**, **picture size** and **borders** are customizable.

- **Picture-in-picture**

– **Source**: Select the camera or group view that will stream as the smaller picture.
– **Rotate image 180°**: Turn on to rotate the image.
– **Mirror image**: Turn on to flip the image.
– **Position**: Select where on the screen the picture should appear.
– **Picture size**: Drag the slider to set the size (% of screen) of the picture.
– **Border**: Click to toggle borders for the picture on or off.
– : Drag the slider to set the thickness for the entire border.
– : Drag the slider to set the thickness for the top border.
– : Drag the slider to set the thickness for the right border.
– : Drag the slider to set the thickness for the bottom border.
– : Drag the slider to set the thickness for the left border.
– **Border color**: Select a border color.

- **Main view**

– **Source**: Select the camera or group view that will stream on the full display.
– **Rotate image 180°**: Turn on to rotate the image.
– **Mirror image**: Turn on to flip the image.

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 or conditions that the device will be used in:

- **Full power (default)**: Select when there's a risk of colder temperatures and ice formation. This is when heaters are used, and power consumption is high.
- **Cold climate**: Select when there's a risk of colder temperatures and ice formation. Improved pan heater performance, which activates after a device restart. Power consumption is high while the heaters are in use.
- **Low power**: Select to reduce power consumption. The heater is turned off.
- **Housing**: Select when the device is inside the housing unit.

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 warning overlay: Turn on to show a power warning overlay when the device doesn't have enough power.

I/O port power: Turn on to supply 12 V power to external devices connected to the I/O ports. Leave off to prioritize internal functions, such as IR, heating, and cooling. As a result, devices and sensors that require 12 V power will stop working properly.

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.

Port

Name: Edit the text to rename the port.

Usage: The default option for the relay port is **Door**. For devices with indicator icons,  turns green when the state changes and the door is unlocked. If you use the relay for something other than a door and don't want the icon to light up when the state changes, you can select one of the other options for 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.

PTZ

Select PTZ mode: Select a PTZ mode that suits your type of installation.

- **Digital**: Select this mode to use digital PTZ and view areas.
- **Mechanical**: Select this mode to connect to an external PTZ device.
  - **Driver**: Select the driver for your connected PTZ device. The driver is required for the connected device to function correctly.
  - **Device type**: Select the type of device you're connecting to from the drop-down list. The device type is driver dependent.
  - **Device id**: Type the id or address of the connected PTZ device. You can find the address in the documentation of the device.
- **Optical zoom for installation**: Select this mode to use optical zoom and focus during installation, and to create view areas with or without digital PTZ.
- **Optical zoom for monitoring**: Select this mode to use optical zoom for monitoring activities. View areas are not available in this mode.

USB configuration

By default, the USB port is turned off and won't respond to any connections. When turned on, your device can connect to external USB devices, such as memory sticks, Axis control boards and other compatible accessories.

- To turn on the USB port, toggle the switch and go to **Maintenance** and click **Restart**. Your device will reboot to apply the changes.

Washer

Lock nozzle position: First, pan and tilt the camera until the nozzle is in the center of the image. Then, turn on **Lock nozzle position** to save the camera position as the washer position. When you turn it on, the washer button appears in the live view. Each time you click the washer button, the camera moves to the locked position.

Pump time: Set the duration of the wash spray sequence in seconds.

Wiper time: Set the duration of the wiper sequence in seconds.

Pump connection: Select the washer pump pin that the washer is connected to. Go to **System > Accessories > I/O ports** and check that the selected pin is configured as an output.

Edge-to-edge

Edge-to-edge pairing allows you to use a compatible Axis device as if it were part of the main device.

Audio pairing allows you to pair with network speaker or microphone. Once paired, the network speaker acts as an audio out device. The network microphone will take up sounds from the surrounding area and make it available as an audio input device.

Important

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

Set a 'Wait between actions (hh:mm:ss)' limit in the event rule when you use a network paired audio device in an event rule with 'Audio detection' as condition and 'Play audio clip' as action. This will help you avoid a looping detection if the capturing microphone picks up audio from the speaker.

PTZ pairing allows you to pair a radar with a PTZ camera to use autotracking. Radar PTZ autotracking makes the PTZ camera track objects based on information from the radar about the objects' positions.

Radar pairing allows you to pair a camera with a compatible Axis radar, and use the camera to configure both devices.

Network pairing allows you to pair with a device with light and siren or illuminator light functionality.

Camera pairing allows you to pair an Axis intercom with a compatible Axis camera, to include the camera's live stream in SIP and VMS calls.

Pair device: Click to add a device to pair with.

- **Select pairing type**: Select from the drop-down list.
- **Address**: Enter host name or IP address of the paired device.
- **Username**: Enter username. Enter the username of the PTZ camera, radar, camera.
- **Password**: Enter password for the user. Enter the password for the PTZ camera, radar, camera.
- **Common name (CN)**: Enter the common name of the device you are connecting to. To find the common name, go to **System > Security > Certificates > Certificate information**.
- **Name**: Enter the name of the device you are connecting to.
- **Description**: Enter a description.
- **Supported features**: Select at least one feature to finalize the pairing.
- **Streaming protocol**: Select **RTSP** to stream over HTTP from a device that supports HTTP. Select **SRTSP** to stream over HTTPS from a device that supports HTTPS. You may need valid certificates for these protocols. To add them, go to **System > Security > Certificates**.
- **Verify certificate**: Select to strictly check TLS certificates. SRTSP data is always encrypted.
- **Close**: Click to clear all fields.
- **Connect**: Click to establish connection to the device to pair with.
- **Configure radar autotracking**: Click to open and configure autotracking. You can also go to **Radar > Radar PTZ autotracking** to configure
- **Video channel**: Select the video channel or view area to display.

Discover devices: Click to find devices on the network. When the network has been scanned a list of available devices is shown.

Note

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

Important

- It's only possible to discover devices where Bonjour is enabled. To enable Bonjour for a device, open its web interface and go to **System > Network > Network discovery protocols**.
- It's only possible to discover devices with AXIS OS 11.4 or later.

: Click to configure your paired device.

- **Name**: Enter a name for the device.
- **Description**: Enter a description.
- **Supported features**: Select the features you want to enable.

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. To include the snapshot of the current live view image, select **Include 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.
- **View the audit log**: Click to show information about user and system activities, for example, successful or failed authentications and configurations.

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.

Type: Select the type of logs you want to send.

Test server setup: Send a test message to all servers before you save the settings.

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.
- **Automatic rollback**: 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

Calibration: Click **Calibrate** to reset the focus and zoom settings or pan, tilt, and roll motors to their default positions. Calibration can be lost during transport, if the device is exposed to extreme vibration, if the camera loses power, or if the motors are moved by hand.

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**.

Analytics

The Analytics space gives you an overview of all Axis analytics applications installed and running on your device. It includes a dashboard with metadata visualization. If your camera supports it, you can also view a heat map.

AXIS Object Analytics

Start: Click to start AXIS Object Analytics. The application will run in the background, and you can create rules for events based on the application's current settings.

Open: Click to open AXIS Object Analytics. The application opens up in a new browser tab where you can configure its settings.

- **Not installed**: AXIS Object Analytics is not installed on this device. Upgrade AXIS OS to the latest version to get the latest version of the application.

Autotracking

Settings

These settings apply to all tracking profiles. You can override some of the settings in each profile.

Active: Turn on to start tracking, automatically through enabled profiles, or manually by clicking objects in the image.

Video objects: Turn on to show bounding boxes around objects that have been confirmed by the camera. When turned on, you can also click an object to start tracking it.

Virtual areas and lines: Turn on to show inclusion areas, exclusion areas, and virtual lines.

Max tracking time: Set the maximum time the camera should track an object. Turn off to keep tracking an object indefinitely.

Timeout: Set the time the camera should wait until it returns to its home position in case it loses the tracked object. If there is a timeout set in the profile, it overrides this timeout.

Settings when paired with a radar:

Active: Turn on to start tracking, automatically through enabled profiles, or manually by clicking objects in the image.

Object type verification: For tracking profiles that require the camera to confirm the radar classification to track objects and trigger connected events. Set the time the camera is given for the verification in **Verification time**.

Multi-object behavior: Control the camera's tracking behavior if several objects simultaneously fulfill the tracking criteria of one profile, or if several profiles with the same priority are triggered simultaneously by different objects.

- **Select one object to track**: Track only one object based on the set **Selection condition**:
  - **Earliest object**: Track the object that fulfilled the tracking criteria first.
  - **Most recent object**: Track the object that fulfilled the tracking criteria most recently.
  - **Object closest to camera**: Track the object that is closest to the camera.
  - **Object furthest from camera**: Track the object that is furthest away from the camera.
  - **Slowest object**: Track the slowest-moving object.
  - **Fastest object**: Track the fastest-moving object.
- **Alternate between objects**: Switch between the objects at a regular interval. Set the interval in **Time per object**.

Visual confirmation: Show overlays on confirmed objects.

- **Video objects**: Show bounding boxes around objects that have been confirmed by the camera.
- **Radar objects**: Show bounding boxes around objects that have been confirmed by the radar.

Use illumination only during autotracking: Turn on to save power by using IR light only when the radar detects an object. When you turn this on, a rule with the same name is automatically created in **Events > Rules**.

Elevation variation

- **Low**: Select if the terrain is mostly flat.
- **Medium**: Select if the terrain has some elevation differences.
- **High**: Select if the terrain has dramatic elevation changes with steep hills.

Tracking profiles

+ Create: Click to create a new tracking profile.

AXIS Object Analytics scenario: Select the scenario that you want to use to trigger autotracking to start. One scenario can be used only for one tracking profile. In the scenario, detection must be restricted to one preset position.

Tracking profile name: The profile name will be based on the scenario name, but you can update it if you want to.

Timeout: Set the time the camera should wait until it returns to its home position in case it loses the tracked object. This setting overrides the timeout in the Settings page.

Use profile: Turn on to enable the profile.

Settings when paired with a radar:

+ Create: Click to create a new tracking profile.

Radar scenario: Select the scenario that you want to use to trigger autotracking to start. One scenario can be used only for one tracking profile.

Tracking profile name: The profile name will be based on the scenario name, but you can update it if you want to.

Tracking criteria: Select the criteria that needs to be fulfilled to track an object.

- **Object detected by radar or camera**: Track the object as long as either the radar or the camera detects it, regardless of which detects it first.
- **Object detected by radar**: Track the object as long as the radar detects it, even if it exits the inclusion area of the radar scenario.
- **Object triggers radar scenario**: Track the object as long as it moves inside the inclusion area of the radar scenario and fulfills the scenario's triggering conditions. This option is only available for movement in area-scenarios.

Object type verification: Turn on to track and trigger events only for objects classified by both the radar and the camera.

Priority: Set the priority of the tracking profile. The priority is used when objects are detected in several profiles at the same time.

AXIS Image Health Analytics

Start: Click to start AXIS Image Health Analytics. The application will run in the background, and you can create rules for events based on the application's current settings.

Open: Click to open AXIS Image Health Analytics. The application opens up in a new browser tab where you can configure its settings.

Not installed: AXIS Image Health Analytics is not installed on this device. Upgrade AXIS OS to the latest version to get the latest version of the application.

AXIS Audio Analytics

Audio analytics: Turn on to allow audio analytics.

Sound pressure level

Show threshold and events in graph: Turn on to show in the graph when a sound spike was detected.

Threshold: Adjust the threshold values for detection. The application will register an audio event for any sounds that fall outside the threshold values.

Adaptive audio detection

Show events in graph: Turn on to show in the graph when a sound spike was detected.

Threshold: Move the slider to adjust the threshold for detection. The minimum threshold will register even slight spikes in sound as a detection, while the maximum threshold will only register significant spikes in sound as a detection.

Test alarms: Click **Test** to trigger a detection event for testing purposes.

Audio classification

Show events in graph: Turn on to show in the graph when a specific type of sound was detected.

Classifications: Select which types of sounds you want the application to detect.

Test alarms: Click **Test** to trigger a detection event of a specific sound for testing purposes.

Directional audio detection: Turn on to help identify the direction of a sound.

Trigger level

Audio pointer: Turn on to see where detected sound is coming from.

Threshold: Move the slider to adjust the threshold for the detected sound. Sounds louder than the set threshold value above the background noise are detected as potential audio events.

Duration: Set a time interval for other audio events to be ignored after the detection of the first audio event.

Audio detection multi-view

View area timeout: Set how long it takes before an event is considered outdated.

Audio event log

Live update log: Turn on to show information about audio events live.

PTZ

Set default tilt: Click after manually adjusting the tilt of the PTZ camera. The default tilt value is used when audio detection can't find any tilt information.

PTZ movement: Turn on to make the PTZ camera move towards the sound.

AXIS Live Privacy Shield

Start: Click to start AXIS Live Privacy Shield. The application allows you to remotely monitor activities while safeguarding privacy.

Open: Click to open AXIS Live Privacy Shield.

- **Not installed**: AXIS Live Privacy Shield is not installed on this device. Upgrade AXIS OS to the latest version to get the latest version of the application.

Metadata visualization

The camera detects moving objects and classes them according to object type. In the view, a classified object has a colored bounding box around it along with its assigned id.

Id: A unique identification number for the identified object and the type. This number is shown in both the list and the view.

Type: Classifies a moving object as Human, Face, Car, Bus, Truck, Bike, or License Plate. The color of the bounding box depends on the type classification.

Confidence: The bar indicates the level of confidence in the classification of the object type.

Metadata configuration

RTSP metadata producers

View and manage the data channels that stream metadata and the channels they use.

Note

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

Producer: A data channel that uses Real-Time Streaming Protocol (RTSP) to send metadata.

Channel: The channel used to send metadata from a producer. Turn on to enable the metadata stream. Turn off for compatibility or resource management reasons.

MQTT

Configure the producers that generate and stream metadata over MQTT (Message Queuing Telemetry Transport).

- **Create**: Click to create a new MQTT producer.
  - **Key**: Select a predefined identifier from the dropdown list to specify the source of the metadata stream.
  - **MQTT topic**: Enter a name for the MQTT topic.
  - **QoS (Quality of Service)**: Set the level of message delivery assurance (0-2).

Retain messages: Choose whether to retain the last message on the MQTT topic.

Use MQTT client device topic prefix: Choose whether to add a prefix to the MQTT topic to help identify the source device.

The context menu contains:

- **Update**: Modify the settings of the selected producer.
- **Delete**: Delete the selected producer.

Object snapshot: Turn on to include a cropped image of each detected object.

Additional crop margin: Turn on to add extra margin around cropped images of detected objects.

T10233729

2026-10 (M21.2)

© 2026 Axis Communications AB