

# **AXIS P3265-LVE-3 License Plate Verifier Kit**

## Get started

### Find the device on the network

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

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

### Browser support

You can use the device with the following browsers:

|                         | Chrome™ | Edge™ | Firefox® | Safari® |
|-------------------------|---------|-------|----------|---------|
| Windows®                | ✓       | ✓     | *        | *       |
| macOS®                  | ✓       | ✓     | *        | *       |
| Linux®                  | ✓       | ✓     | *        | *       |
| Other operating systems | *       | *     | *        | *       |

✓: Recommended

\*: Supported with limitations

### Open the device's web interface

1. Open a browser and type the IP address or host name of the Axis device.  
If you do not know the IP address, use AXIS IP Utility or AXIS Device Manager to find the device on the network.
2. Type the username and password. If you access the device for the first time, you must create an administrator account. See .

For descriptions of all the controls and options in the device's web interface, see .

### Create an administrator account

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

1. Enter a username.
2. Enter a password. See .
3. Re-enter the password.
4. Accept the license agreement.
5. Click **Add account**.

#### Important

The device has no default account. If you lose the password for your administrator account, you must reset the device. See .

## **Secure passwords**

### **Important**

Use HTTPS (which is enabled by default) to set your password or other sensitive configurations over the network. HTTPS enables secure and encrypted network connections, thereby protecting sensitive data, such as passwords.

The device password is the primary protection for your data and services. Axis devices do not impose a password policy as they may be used in various types of installations.

To protect your data we strongly recommend that you:

- Use a password with at least 8 characters, preferably created by a password generator.
- Don't expose the password.
- Change the password at a recurring interval, at least once a year.

## **Make sure that no one has tampered with the device software**

To make sure that the device has its original AXIS OS, or to take full control of the device after a security attack:

1. Reset to factory default settings. See .  
After the reset, secure boot guarantees the state of the device.
2. Configure and install the device.

## **Web interface overview**

This video gives you an overview of the device's web interface.



*Axis device web interface*

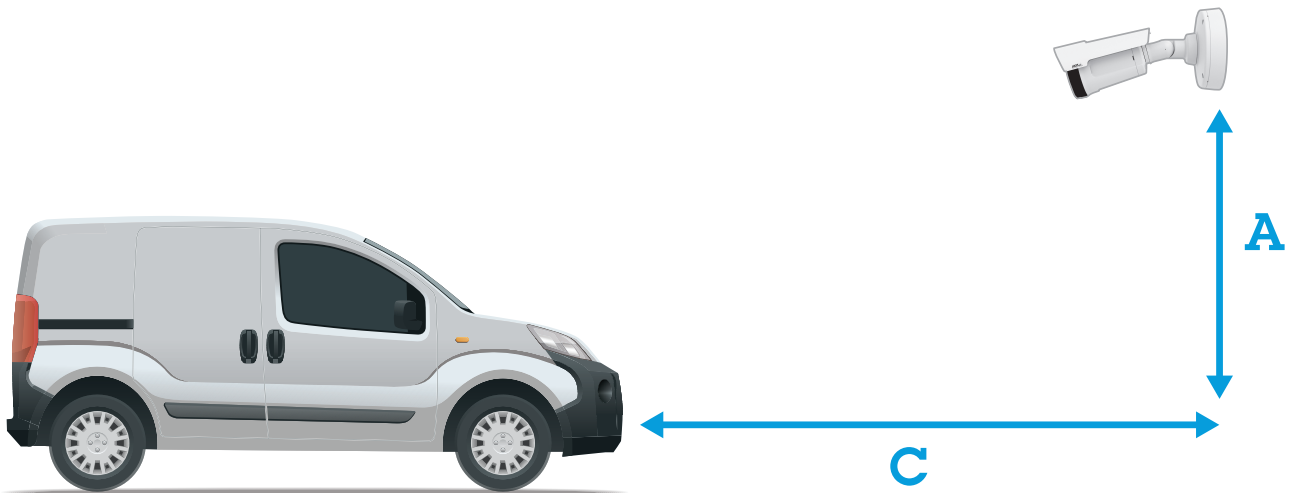
## Basic setup

These setup instructions are valid for all scenarios:

- 1.
- 2.
- 3.
- 4.
- 5.

## Camera mounting recommendations

- When you select the mounting location, remember that direct sunlight can distort the image, for example, during sunrise and sunset.
- The mounting height for a camera in a **Access control** scenario should be half of the distance of that between the vehicle and the camera.
- The mounting height for camera in a **Free flow** (slow traffic license plate recognition) scenario should be less than half of the distance of that between the vehicle and the camera.



**Access control** capture distance: 2–7 m (6.6–23 ft). This example is based on the AXIS P3265–LVE–3 License Plate Verifier kit.

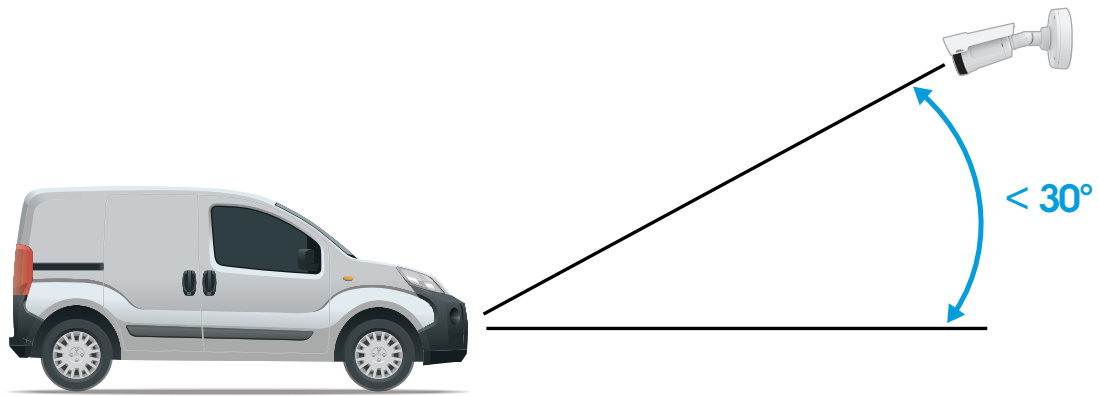
| Capture distance: (C) | Mounting height (A) |
|-----------------------|---------------------|
| 2.0 m (6.6 ft)        | 1.0 m (3.3 ft)      |
| 3.0 m (9.8 ft)        | 1.5 m (4.9 ft)      |
| 4.0 m (13 ft)         | 2.0 m (6.6 ft)      |
| 5.0 m (16 ft)         | 2.5 m (8.2 ft)      |
| 7.0 m (23 ft)         | 3.5 m (11 ft)       |

**Free flow** capture distance: 7–20m (23–65 ft). This example is based on the AXIS P1465–LE–3 License Plate Verifier kit.

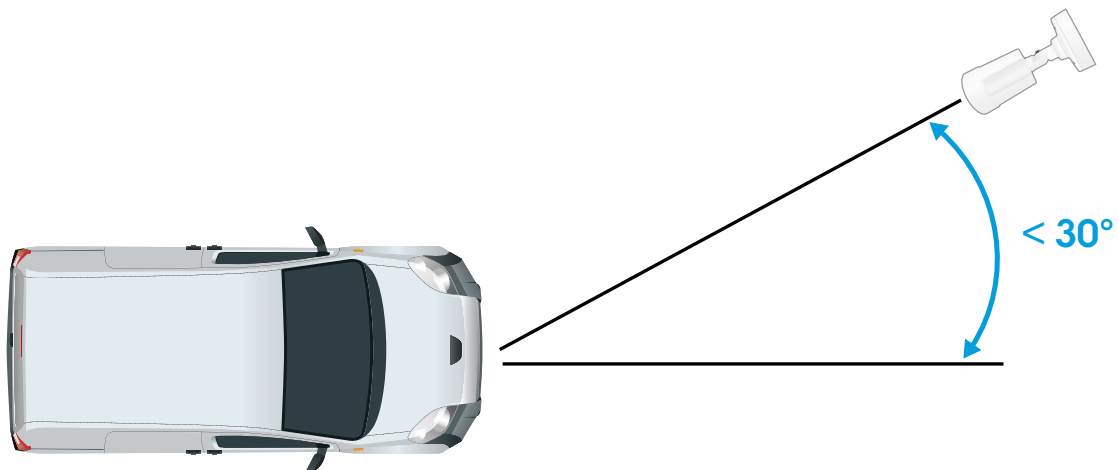
| Capture distance (C) | Mounting height (A) |
|----------------------|---------------------|
| 7.0 m (23 ft)        | 3.0 m (9.8 ft)      |
| 10.0 m (33 ft)       | 4.0 m (13 ft)       |

|                |                 |
|----------------|-----------------|
| 15.0 m (49 ft) | 6.0 m (19.5 ft) |
| 20.0 m (65 ft) | 10.0 m (33 ft)  |

- The camera's mounting angle should not be larger than 30° in any direction.

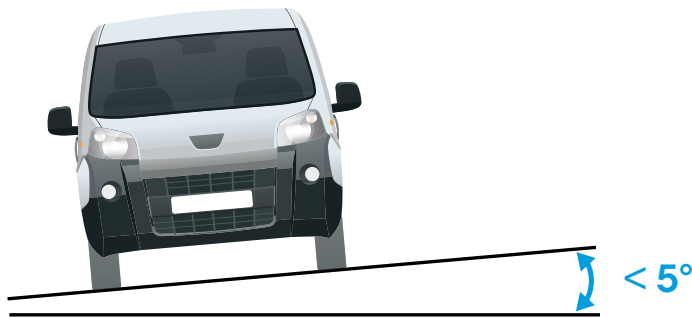


*Mounting angle from the side.*



*Mounting angle from above.*

- The image of the license plate should not tilt more than 5° horizontally. If the image is tilted more than 5°, we recommended that you adjust the camera so that the license plate is displayed horizontally in the live stream.



*Roll angle.*

## **Setup assistant**

When you first run the application, set up **Free flow** or **Access control** using the setup assistant. If you want to make changes later on, it can be found in the **Settings** tab under **Setup assistant**.

### **Free flow**

In **Free flow**, the application can detect and read license plates in slow speed traffic on larger access roads, city centers and enclosed areas like campuses, ports or airports. This allows for LPR-forensic search and LPR triggered events in a VMS.

1. Select **Free flow** and click **Next**.
2. Select the image rotation that corresponds to how your camera is mounted.
3. Select the number of areas of interest. Note that one area can detect plates in both directions.
4. Select the region where the camera is located.
5. Select capture type.
  - **License plate crop** saves only the license plate.
  - **Vehicle crop** saves the entire captured vehicle.
  - **Frame downsized 480x270** saves the entire image and reduces the resolution to 480x270.
  - **Full frame** saves the entire image at full resolution.
6. Drag the anchor points to adjust the area of interest. See .
7. Adjust the direction of the area of interest. Click the arrow and rotate to set the direction. The direction determines how the application registers vehicles entering or exiting the area.
8. Click **Next**
9. In the **Protocol** drop-down list, select one of the following protocols:
  - **TCP**
  - **HTTP POST**
10. In the **Server URL** field, type the server address and port in the following format: 127.0.0.1:8080
11. In the **Device ID** field, type the name of the device or leave as is.
12. Under **Event types**, select one or more of the following options:
  - **New** means the first detection of a license plate.

- **Update** is either a correction of a character on a previously detected license plate, or when a direction is detected as the plate moves and is tracked across the image.
  - **Lost** is the last tracked event of the license plate before it exits the image. It also contains the direction of the license plate.
13. To turn on the feature, select **Send event data to server**.
  14. To reduce bandwidth when using HTTP POST, you can select **Do not to send images through HTTP POST**.
  15. Click **Next**.
  16. If you already have a list of registered plates, choose to import as either a **blocklist** or **allowlist**.
  17. Click **Finish**.

## Access control

Use the setup wizard for quick and easy configuration. You can choose to **Skip** to leave the guide at any time.

1. Select **Access control** and click **Next**.
2. Select the type of access control to use:
  - **Internal I/O** if you want keep list management in the camera. See .
  - **Controller** if you want to connect a Door controller. See .
  - **Relay** if you want to connect to a relay module. See .
3. In the **Barrier mode** drop-down list, under **Open from lists**, select **Allowlist**.
4. In the **Vehicle direction** drop-down list, select **out**.
5. In the **ROI** drop-down-list, select the area of interest you would like to use, or if you would like to use all.
6. Click **Next**.

On the **Image settings** page:

1. Select the number of areas of interest.
2. Select the region where the camera is located.
3. Select capture type. See .
4. Drag the anchor points to adjust the area of interest. See .
5. Adjust the direction of the area of interest. The direction determines how the application registers vehicles entering or exiting the area.
6. Click **Next**

On the **Event data** page:

### Note

For detailed settings see: .

1. In the **Protocol** drop-down list, select one of the following protocols:
  - **TCP**
  - **HTTP POST**
2. In the **Server URL** field, type the server address and port in the following format: 127.0.0.1:8080.
3. In the **Device ID** field, type the name of the device or leave as is.
4. Under **Event types**, select one or more of the following options:
  - **New** means the first detection of a license plate.
  - **Update** is either a correction of a character on a previously detected license plate, or when a direction is detected as the plate moves and is tracked across the image.

- **Lost** is the last tracked event of the license plate before it exits the image. It also contains the direction of the license plate.
- 5. To turn on the feature, select **Send event data to server**.
- 6. To reduce bandwidth when using HTTP POST, you can select **Do not to send images through HTTP POST**.
- 7. Click **Next**

On the **Import list from a .csv file** page:

1. If you already have a list of registered plates, choose to import as either a **blocklist** or **allowlist**.
2. Click **Finish**.

## **Access the application settings**

1. In the camera's web interface, go to **Apps**, start the application and click **Open**.

## **Adjust the area of interest**

The area of interest is the area in the live view where the application looks for license plates. For optimal performance, keep the area of interest as small as possible. To adjust the area of interest, do the following:

1. Go to **Settings**.
2. Click **Edit area of interest**.
3. To improve verification and captured images, go to **Zoom** and adjust the slider to your needs.
4. To have the camera automatically focus on the vehicles, click **Autofocus**. To set the focus manually, go to **Focus** and adjust it with the slider.
5. To move the area of interest, click anywhere in the area and drag it to where the license plates are most visible. If you place the area of interest outside the live view, it will automatically jump back to default position. Make sure the region of interest stays in position after you have saved the settings.
6. To adjust the area of interest, click anywhere in the area and drag the anchor points highlighted in blue.
  - To reset the area of interest, right click within the area and select **Reset**.
  - To add anchor points, click the on one of the yellow anchor points. The anchor point will turn blue, showing it can be manipulated. New yellow points are automatically added next to the blue anchor point. The maximum number of blue anchor points is eight.
7. Click anywhere outside the area of interest to save your changes.
8. To get the correct direction feedback in the **Event log**, you need to turn the arrow to match the driving direction.
  - 8.1. Click the arrow icon.
  - 8.2. Select the anchor point and rotate the arrow so it aligns with the driving direction.
  - 8.3. Click outside the area of interest to save the changes.

Note that one area can detect plates in both directions. The direction feedback shows up in the **Direction** column.

- To add a second area of interest, select **2** in the **Area of interest** drop-down menu.



*Example with one area of interest.*

**Note**

- If you are using a standalone camera, you can have the app set the recommended settings for license plate recognition.
  1. Click **Recommended LPR settings**. You will see a table where the current settings and the recommended settings differ.
  2. Click **Update settings** to have the app change the settings their recommended values.

## Select region

1. Go to **Settings > Image**.
2. In the **Region** drop-down list, select your region.

## Adjust the image capture settings

1. Go to **Settings > Image**.
2. To change the resolution of captured images, go to **Resolution**
3. To change the rotation of the captured image, go to **Image rotation**
4. To change how you save your captured images, go to **Save full frame**:
  - **License plate crop** saves only the license plate.
  - **Vehicle crop** saves the entire captured vehicle.
  - **Frame downsized 480x270** saves the entire image and reduces the resolution to 480x270.
  - **Full frame** saves the entire image at full resolution.

## Set up event storage

An event consists of the captured image, the license plate, the area of interest number, vehicle direction, access, and the date and time.

This example use case explains how to store events of allowlisted license plate numbers for 30 days.

Requirements:

- Camera physically installed and connected to the network.

- AXIS License Plate Verifier up and running on the camera.
  - Internal storage or an SD card installed in the camera.
1. Go to **Settings > Events**.
  2. Under **Save events**, select **Allowlisted**.
  3. Under **Delete events after**, select **30 days**.

### **Note**

To detect an inserted SD card when the app is running, you need to restart the app. If an SD card is installed in the camera, the app will automatically choose the SD card as the default storage.

AXIS License Plate Verifier uses the cameras internal memory to save up to 1,000 events, using license plate crops as the frame. If you use larger frames, it will vary the amount of events you can save.

To change the image capture settings, go to **Settings > Image**. An SD card can save up to 100,000 events using any type of frame.

### **Installation**

#### **Preview mode**

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



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

*This video demonstrates how to use preview mode.*

## Configure your device

### For users of AXIS Camera Station

#### Set up AXIS License Plate Verifier

When a device is configured with AXIS License Plate Verifier, it is considered as an external data source in the video management system. You can connect a view to the data source, search for the license plates that are captured by the device, and view the related image.

##### Note

- It requires AXIS Camera Station 5.38 or later.
  - AXIS License Plate Verifier requires a license.
1. Download and install the application on your device.
  2. Configure the application. See *AXIS License Plate Verifier user manual*.
  3. For an existing AXIS Camera Station installation, renew your server certificate that is used to communicate with the client. See *Certificate renewal*.
  4. Turn on time synchronization to use AXIS Camera Station server as the NTP server. See *Server settings*.
  5. Add the device to AXIS Camera Station. See *Add devices*.
  6. When the first event is received, a data source is automatically added under **Configuration > Devices > External data sources**.
  7. Connect the data source to a view. See *External data sources*.
  8. Search for license plates that are captured by the device. See *Data search*.
  9. Click  to export the search results to a .txt file.

### Basic settings

#### Set the mounting position

1. Go to **Video > Installation > Mounting position**.
2. Click **Change**.
3. Select a mounting position and click **Save and restart**.

#### Set the power line frequency

1. Go to **Video > Installation > Power line frequency**.
2. Click **Change**.
3. Select a power line frequency and click **Save and restart**.

### Adjust the image

This section includes instructions about configuring your device.

#### Reduce image processing time with low latency mode

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

1. Go to **System > Plain config**.
2. Select **ImageSource** from the drop-down list.
3. Go to **ImageSource/I0/Sensor > Low latency mode** and select **On**.

4. Click **Save**.

## Select exposure mode

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

- For most use cases, select **Automatic** exposure.
- For environments with certain artificial lighting, for example fluorescent lighting, select **Flicker-free**. Select the same frequency as the power line frequency.
- For environments with certain artificial light and bright light, for example outdoors with fluorescent lighting at night and sun during daytime, select **Flicker-reduced**. Select the same frequency as the power line frequency.
- To lock the current exposure settings, select **Hold current**.

## Compensate for barrel distortion

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

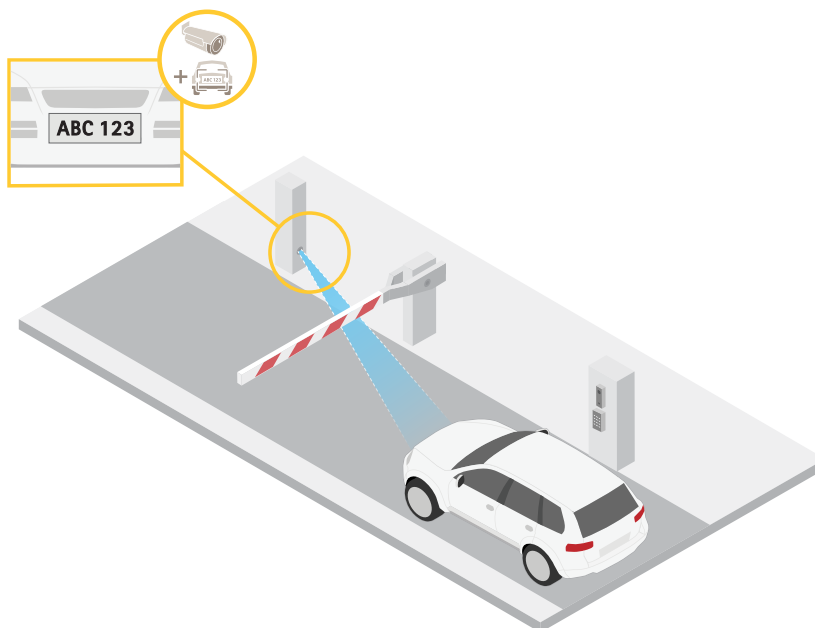
### Note

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

1. Go to **Video > Installation > Image correction**.
2. Turn on **Barrel distortion correction (BDC)**.

## Verify the pixel resolution

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



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

3. Click  for **Pixel counter**.
4. In the camera's live view, adjust the size and position of the rectangle around the area of interest, for example where you expect license plates to appear.
5. You can see the number of pixels for each of the rectangle's sides, and decide if the values are enough for your needs.

## View and record video

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

### Reduce bandwidth and storage

#### Important

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

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

#### Note

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

- Select the Zipstream **Strength** that you want to use.
- Turn on **Optimize for storage**. This can only be used if the video management software supports B-frames.
- Turn on **Dynamic FPS**.
- Turn on **Dynamic GOP** and set a high **Upper limit GOP length** value.

#### Note

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

### Set up network storage

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

1. Go to **System > Storage**.
2. Click  **Add network storage** under **Network storage**.
3. Type the IP address of the host server.
4. Type the name of the shared location on the host server under **Network share**.
5. Type the username and password.
6. Select the SMB version or leave it on **Auto**.
7. Select **Add share without testing** if you experience temporary connection issues, or if the share is not yet configured.
8. Click **Add**.

### Record and watch video

Record video directly from the camera

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

2. To start a recording, click .

If you haven't set up any storage, click  and . For instructions on how to set up network storage, see

3. To stop recording, click  again.

#### Watch video

1. Go to **Recordings**.

2. Click  for your recording in the list.

#### Verify that no one has tampered with the video

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

1. Go to **Video > Stream > General** and turn on **Signed video**.
2. Use AXIS Camera Station (5.46 or later) or another compatible video management software to record video. For instructions, see the *AXIS Camera Station user manual*.
3. Export the recorded video.
4. Use AXIS File Player to play the video. *Download AXIS File Player*.

 indicates that no one has tampered with the video.

#### Note

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

#### Set up rules for events

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

To learn more, check out our guide *Get started with rules for events*.

#### Record video when the camera detects a license plate

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

Before you start:

- Make sure you have an SD card installed.

Make sure that AXIS Licence Plate Verifier is running:

1. Go to **Apps > AXIS License Plate Verifier**.
2. Start the application if it is not already running.
3. Make sure you have set up the application according to your needs.

Create a rule:

1. Go to **System > Events** and add a rule.
2. Type a name for the rule.
3. In the list of conditions, under **Application**, select **ALPV.PlateInView**.
4. In the list of actions, under **Recordings**, select **Record video while the rule is active**.
5. In the list of storage options, select **SD\_DISK**.

6. Select a camera and a stream profile.
7. Set the prebuffer time to 5 seconds.
8. Set the postbuffer time to 1 minute.
9. Click **Save**.

### **Trigger a notification when the camera lens is tampered**

This example explains how to set up an email notification when the camera lens gets either spray painted, covered, or blurred.

#### **Activate the tampering detection:**

1. Go to **System > Detectors > Camera tampering**.
2. Set a value for **Trigger delay**. The value indicates the time that must pass before an email is sent.
3. Turn on **Trigger on dark images** to detect if the lens is sprayed, covered, or rendered severely out of focus.

#### **Add an email recipient:**

4. Go to **System > Events > Recipients** and add a recipient.
5. Type a name for the recipient.
6. Select **Email** as the notification type.
7. Type the recipient's email address.
8. Type the email address that you want the camera to send notifications from.
9. Provide the login details for the sending email account, along with the SMTP hostname and port number.
10. To test your email setup, click **Test**.
11. Click **Save**.

#### **Create a rule:**

12. Go to **System > Events > Rules** and add a rule.
13. Type a name for the rule.
14. In the list of conditions, under **Video**, select **Tampering**.
15. In the list of actions, under **Notifications**, select **Send notification to email** and then select the recipient from the list.
16. Type a subject line and message for the email.
17. Click **Save**.

## **Audio**

### **Add audio to your recording**

#### **Turn on audio:**

1. Go to **Video > Stream > Audio** and include audio.
2. If the device has more than one input source, select the correct one in **Source**.
3. Go to **Audio > Device settings** and turn on the correct input source.
4. If you make any changes to the input source, click **Apply changes**.

#### **Edit the stream profile that is used for the recording:**

5. Go to **System > Stream profiles** and select the stream profile.
6. Select **Include audio** and turn it on.
7. Click **Save**.

## **Add audio capability to your product using portcast**

With portcast technology, you can add audio capability to your product. It allows audio and I/O communication digitally over the network cable between the camera and the interface.

To add audio capability to your Axis network video device, connect the portcast compatible Axis audio device and I/O Interface between your device and the PoE switch which provides power.

1. Connect the Axis network video device (1) and the Axis portcast device (2) with a PoE cable.
2. Connect the Axis portcast device (2) and the PoE switch (3) with a PoE cable.



- 1 *Axis network video device*
- 2 *Axis portcast device*
- 3 *Switch*

Once the devices are connected, an audio tab becomes visible in the settings for your Axis network video device. Go to the audio tab and turn on **Allow audio**.

See your Axis portcast device's user manual for more information.

## Manage lists

### Add detected license plate to list

A license plate can be added directly to a list after being detected by the application.

1. Click the **Event log** tab.
2. Go to **Latest Event**.
3. Click **Add to list** next to the license plate that you'd like to add.
4. Select the list you would like to add the license plate in the list drop down menu.
5. Click **Append**.

#### Note

Make sure the symbols **<**, **>** and **&** aren't used in either license plates or descriptions.

### Add descriptions to license plates

To add a description to a license plate in the list:

- Go to **List management**.
- Select the license plate you want to edit and click the pen icon.
- Type the relevant information in the **Description** field at the top of the list .
- Click the disk icon to save.

#### Note

Make sure the symbols **<**, **>** and **&** aren't used in either license plates or descriptions.

### Customize list names

You can change the name of any of the lists to fit your specific use case.

1. Go to **List management**.
2. Go to the list menu of the list you want to change.
3. Select **Rename**.
4. Type the name of the list.

The new list name will be updated in any existing configurations.

### Import allowlisted license plate numbers

You can import allowlisted license plate numbers from a .csv file on the computer. In addition to the license plate number, you can also add comments for each license plate number in the .csv file.

The structure of the .csv file must look like this: `license plate,date,description`

#### Example:

Only license plate: `AXIS123`

License plate + description: `AXIS123, , John Smith`

License plate + date + description: `AXIS123, 2022-06-08, John Smith`

#### Note

Make sure the symbols **<**, **>** and **&** aren't used in either license plates or descriptions.

1. Go to **List management**
2. Go to the context menu next to **Allowlist** and select **Import from file**.

3. Browse to select a .csv file on the computer.
4. Click **OK**.
5. Check that the imported license plate numbers appear in the **Allowlist**.

### **Share license plate lists with other cameras**

You can share the license plate lists with other cameras on the network. The synchronization will override all current license plate lists in the other cameras.

1. Go to **List management**.
2. Under **Camera synchronization**, type the IP address, username and password.
3. Click **+**.
4. Click **Camera synchronization**.
5. Check that the date and time under **Last sync** updates accordingly.

### **Schedule lists**

Lists can be scheduled to only be active during certain times during certain days of the week. To schedule a list:

- Go to **List management**.
- Go to the list menu of the list you want to schedule.
- Select **Schedule** in the pop-up menu.
- Select the start and end time, and the day when the list should be active.
- Click the button next to **Enabled**.
- Click **Save**.

## Additional settings

### Configure text overlay

A text overlay shows the following event information in the live view: `weekday`, `month`, `time`, `year`, `license plate number`.

1. Go to **Settings > Image**.
2. Activate **Text overlay**.
3. Set **Overlay duration** to a value between 1 and 9 seconds.
4. Select either date, time and license plate (**Datetime + LP**), or just the license plate (**LP**).
5. Check that the overlay appears in the live view.

### Detect license plates in low-light conditions

Each detection gets a score by the algorithm, this is called the sensitivity level (confidence parameter). Detections that have a lower score than the selected level will not show up in the list of events.

For scenes with low lighting you can lower the sensitivity level.

1. Go to **Settings > Detection parameters**.
2. Adjust the slider under **Sensitivity level**. To avoid false detections, we recommend that you lower the threshold value with 0.05 at a time.
3. Check that the algorithm detects the license plates as expected.

### Allow fewer characters on license plates

The application has a default minimum number of characters for a license plate to be detected. The default minimum number of characters is five. You can configure the application to detect license plates with fewer characters.

1. Go to **Settings > Detection parameters**.
2. In the **Minimum number of characters** field, type the minimum number of characters you want to allow.
3. Check that the application detects license plates as expected.

### Allow only exact matches of license plates

The matching algorithm automatically allows a deviation of one character when matching the detected license plate against the allowlist or blocklist. However, some scenarios need an exact match of all characters of the license plate.

1. Go to **List management**.
2. Click to activate **Strict matching**.
3. Check that the application matches the license plates as expected.

### Allow more than one character deviation when matching license plates

The matching algorithm automatically allows a deviation of one character when matching the detected license plate against the allowlist or blocklist. However, you can allow more than one character deviation.

1. Go to **Settings > Detection parameters**.
2. Under **Allowed character deviation**, select the number of characters that are allowed to be different.
3. Check that the application matches the license plates as expected.

## **Give limited access to operators**

Operators can be given a limited access to the app using an URL. This way they only have access to the Event log and List management. The URL can be found under **Settings > User rights**.

## **Set up secure connection**

To protect communication and data between devices, for example between the camera and the door controller, set up a secure connection with HTTPS using certificates.

1. Go to **Settings > Security**.
2. Under HTTPS, **Enable HTTPS**.
3. Select either **Self-signed** or **CA-signed**.

### **Note**

Find out more about HTTPS and how to use it at .

## **Backup and restore app settings**

You can backup and restore settings made in the app related to image capture, security, detection and integration. If something should go wrong, you can now restore the settings you have backed up.

To backup app settings:

- Go to **Settings > Maintenance**.
- Click **Backup configuration**.

A JSON file will be downloaded to you downloads folder.

To restore app settings:

- Go to **Settings > Maintenance**.
- Click **Restore configuration**.

Select the JSON file containing the backup.

The setting are restored automatically.

## **Clear all events**

After you set up the app, it can be a good idea to clear the records of any images or captured plates from the setup process.

To clear all images and plates from the database:

Go to **Settings > Maintenance**.

- Click **Clear all recognition results**.
- Click **Yes**.

## **Use virtual ports to trigger actions**

Virtual ports can be used together with access control to trigger any kind of action. This example explains how to set up AXIS License Plate Verifier together with the camera's I/O port to display a text overlay using a virtual port.

Requirements:

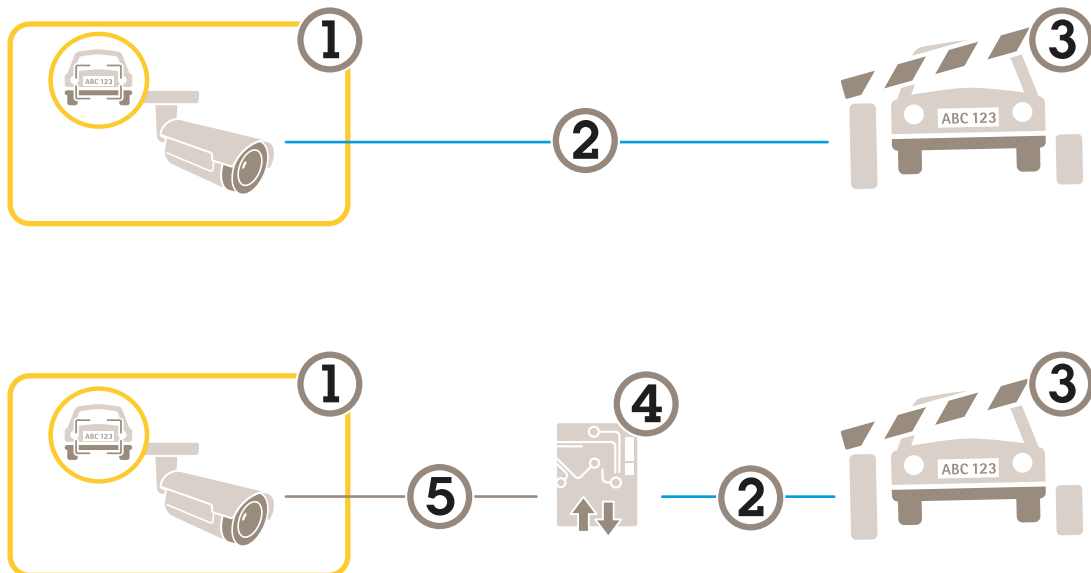
- Camera physically installed and connected to the network.
  - AXIS License Plate Verifier up and running on the camera.
  - Cables connected between the barrier and the camera's I/O port.
  - Basic setup done. See .
1. Go to the application's webpage and select the **Settings** tab.

2. Go to **Access control**.
3. Under **Access control** , select the **Type** drop-down list, select **Internal I/O**.
4. Select the **I/O output #**.
5. Select a port in the **Virtual port** drop-down list.
6. In the **Barrier mode** drop-down list, select **Open to all**.
7. In the **Vehicle direction** drop-down list, select **any**.
8. In the **ROI** drop-down-list, select the area of interest you would like to use, or if you would like to use all.
9. In the camera's webpage, go to **System > Events**.
10. Click **Add rule**.
11. Under **Condition** select **Virtual input is active** and the port number you have selected.
12. Under **Action**, select **Use overlay text**.
13. Select **Video channels**.
14. Type the text you want displayed.
15. Add the duration of the text.
16. Click **Save**.
17. Go to **Video > Overlays**.
18. Go to **Overlays**.
19. Select **Text** in the drop-down menu and click **+**.
20. Type **#D** or select the modifier in the **Modifiers** drop-down list.
21. Check that the text overlay is displayed when a vehicle enters the region of interest in the live view.

## Vehicle entry and exit scenario

In the scenario for vehicle entry and exit, the application reads the vehicle license plate captured by the camera and verifies the license plate against a list of authorized or unauthorized license plate numbers stored in the camera.

This scenario requires the application embedded in a camera with I/O support or a connected I/O relay module to open and close the barrier.



Two possible setups for the vehicle entry and exit scenario.

- 1 Axis camera with AXIS License Plate Verifier
- 2 I/O communication
- 3 Barrier
- 4 Axis I/O relay module
- 5 IP communication

## Open a barrier for known vehicles using a relay module

This example use case explains how to set up AXIS License Plate Verifier together with a relay module to open a barrier for a known vehicle driving through a specific region of interest (ROI) into, let's say a parking area.

### Requirements:

- Camera physically installed and connected to the network.
  - AXIS License Plate Verifier up and running on the camera.
  - Cables connected between the barrier and the relay module.
  - Basic setup done. See .
1. Go to the camera's webpage, select **Settings** and open AXIS License Plate Verifier.
  2. Go to the relay module's webpage and make sure the relay port is connected to the camera's I/O port.
  3. Copy the relay module's IP address.
  4. Go back to AXIS License Plate Verifier.
  5. Go to **Settings > Access control**.
  6. Go to **Type** and select **Relay** in the drop-down list.
  7. In the **I/O output** drop-down list, select the I/O port that is connected to the barrier.
  8. In the **Barrier mode** drop-down list, select **Open from lists** and then check **Allowlist**.
  9. In the **Vehicle direction** drop-down list, select **in**.
  10. In the **ROI** drop-down list, select the area of interest that covers the traffic lane.

11. Enter the following information:
  - the IP address for the relay module in format 192.168.0.0
  - the username for the relay module
  - the password for the relay module
12. To make sure the connection works, click **Connect**.
13. To activate the connection, click **Turn on integration**.
14. Go to the **List management** tab
15. Enter the license plate number in the **Allowlist** field.

**Note**

The physical input ports 1 to 8 on the relay module correspond to ports 1 to 8 in the drop-down list. However, the relay ports 1 to 8 on the relay module correspond to ports 9 to 16 in the drop-down list. This is valid even if the relay module only has 8 ports.

16. Check that the application identifies the license plate number in the allowlist as a known vehicle and that the barrier opens as expected.

## Open a barrier for known vehicles using the camera's I/O

This example explains how to set up AXIS License Plate Verifier together with the camera's I/O port to open a barrier for a known vehicle entering, for example, a parking area.

**Requirements:**

- Camera physically installed and connected to the network.
- AXIS License Plate Verifier up and running on the camera.
- Cables connected between the barrier and the camera's I/O port.
- Basic setup done. See .



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

*Open a barrier for known vehicles using the camera's I/O*

1. Go to the application's webpage and select the **Event log** tab and add detected license plates to a list. See
2. To edit the lists directly, go to the **List management** tab.
3. Enter the authorized license plate numbers in the **Allowlist** field.
4. Go to the **Settings** tab.
5. Under **Access control** , select the **Type** drop-down list, select **Internal I/O**.
6. Select the **I/O output #**.
7. In the **Barrier mode** drop-down list, select **Open from lists** and then check **Allowlist**.
8. In the **Vehicle direction** drop-down list, select **in**.
9. In the **ROI** drop-down-list, select the area of interest you would like to use, or if you would like to use all.
10. Check that the application identifies the license plate number in the allowlist as a known vehicle and that the barrier opens as expected.

**Note**

You can change the name of any of the lists to fit your specific use case.

## **Get notified about an unauthorized vehicle**

This example explains how to set up the application so that an event that triggers a notification can be created in the camera.

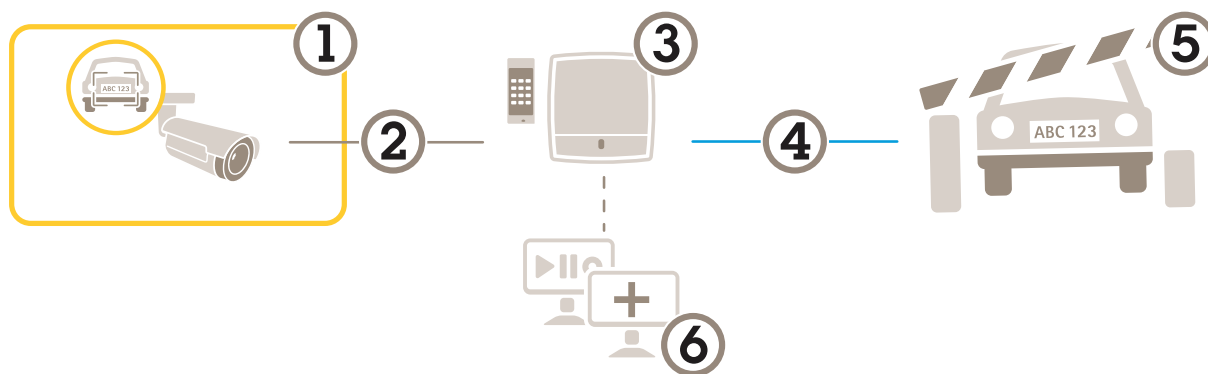
Requirements:

- Basic setup done. See .
- 1. Go to **List management**.
- 2. Enter the license plate number in the **Blocklist** field.
- 3. Go to the camera's webpage.
- 4. Go to **Settings > Events** and set up an action rule with the application as a condition and with a notification as an action.
- 5. Check that the application identifies the added license plate number as an unauthorized vehicle and that the action rule runs as expected.

## Vehicle access control scenario

In the scenario for vehicle access control, the application can be connected to an Axis network door controller to configure access rules, create schedules for access times, and handle vehicle access not only for employees, but also, for example, visitors and suppliers.

For backup, use an access system involving a door controller and card reader. To set up the door controller and the card reader, see the user documentation at [axis.com](http://axis.com)



- 1 Axis camera with AXIS License Plate Verifier
- 2 IP communication
- 3 Axis network door controller with card reader
- 4 I/O communication
- 5 Barrier
- 6 Optional third-party software

## Connect to a door controller

In this example we connect the camera to a network door controller which means the camera works as a sensor. The camera forwards the information to the controller which in turn analyzes the information and triggers the events.

### Note

When switching between the AXIS License Plate Verifier and AXIS Entry Manager, make sure to refresh the webpages to get access to all parameters.

### Requirements:

- Camera and door controller physically installed and connected to the network.
- AXIS License Plate Verifier up and running on the camera.
- Basic setup done. See .



*How to get the application up and running with AXIS A1001 Door Controller.*

### Hardware configuration in AXIS Entry Manager

1. Go to AXIS Entry Manager and start a new hardware configuration under **Setup**.
2. In the hardware configuration, rename the network door controller to "Gate controller".
3. Click **Next**.
4. In **Configure locks connected to this controller**, clear the **Door monitor** option.
5. Click **Next**.

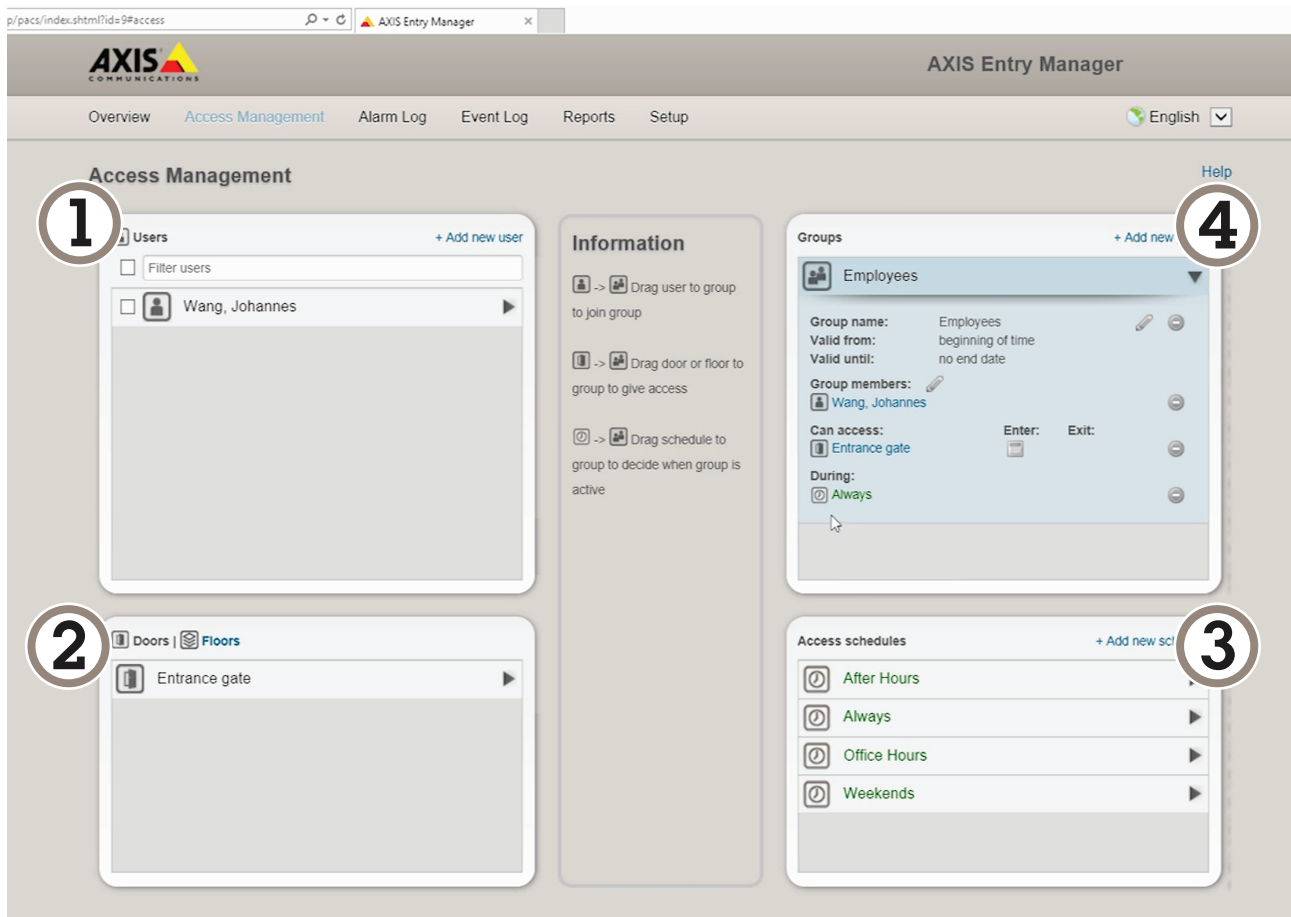
6. In **Configure readers connected to this controller**, clear the **Exit reader** option.
7. Click **Finish**.

#### Configuration in AXIS License Plate Verifier

1. Go to the **AXIS License Plate Verifier** webpage.
2. Go to the **Settings > Access control**.
3. Go to **Type** and select **Controller** in the drop-down list.
4. Enter the following information:
  - the IP address for the controller in format **192.168.0.0**
  - the username for the controller
  - the password for the controller
5. Click **Connect**.
6. If the connection is successful, "Gatecontroller" shows up in the **Network Door Controller name** drop-down list. Select "Gatecontroller".
7. In the **Reader name** drop-down list, select the reader connected to the door "Gatecontroller", for example "Reader entrance". These names can be changed in **AXIS Entry Manager**.
8. To activate the connection, select **Turn on integration**.
9. Enter one of the user's license plate number, or use the default, in the test field and click **Test integration**. Check that the test was successful.

#### Configure users, groups, doors, and schedules in AXIS Entry Manager

1. Go to **AXIS Entry Manager**.
2. Go to **Access Management**.
3. Go to **Doors > Add identification type**.
4. In the **Credentials needed** drop-down list, select **License plate only**.
5. To set limits for when the identification type can be used, drag and drop a **Schedule** to the door.
6. Add users and, for each user, add the credential **License plate**.
7. Click **Add credential** again and enter the license plate information.
8. Click **Add new group** and enter the information.
9. To add users to a group, drag and drop **Users** to the user group.
10. To give users access, drag and drop the **Door** to the user group.
11. To limit the access time, drag and drop a **Schedule** to the user group.



Overview of AXIS Entry Manager user interface.

- 1 Users
- 2 Doors
- 3 Schedules
- 4 User groups

## Connect to AXIS Secure Entry

This example describes connecting an Axis door controller in AXIS Camera Station and AXIS Secure Entry with AXIS Licence Plate Verifier.

### Requirements:

- Camera and door controller physically installed and connected to the network.
- AXIS License Plate Verifier up and running on the camera.
- AXIS Camera Station client version 5.49.449 and up.
- Basic setup done. See .

In **AXIS Camera Station**, see *Add a reader*.

In the **AXIS License Plate Verifier** app:

1. In the **Settings** tab, go to **Configuration wizard** and click **Start**.
2. Select **Access Control**.
3. Select **Secure Entry**, and click **Next**.

In **AXIS Camera Station**:

4. Type the IP address of the door controller, available in the device list in **AXIS Camera Station > Configuration > Other Devices**.
5. To add a Authentication key, go to **AXIS Camera Station > Configuration > Encrypted communication**.
6. Go to **External Peripheral Authentication Key** and click **Show authentication key**.

7. Click **Copy** key.

In the **AXIS License Plate Verifier** app:

8. Go to **Authentication key** in the configuration wizard and paste the key.
9. Click **Connect**.
10. Select the **Door controller name** in the drop-down menu.
11. Select the **Reader name** in the drop-down menu.
12. Check **Turn on integration**.
13. Click **Next**.
14. Adjust the area of interest. See .
15. Click **Next** twice and then **Finish**.

## Free flow scenario with speed measurement

In a free flow scenario with speed measurement, the camera is paired with an Axis radar through the edge-to-edge technology. The camera covers two lanes and reads the license plates of the passing vehicles, and the paired radar covers the same two lanes to measure the speed of the vehicles. Additionally, the application *AXIS Speed Monitor* can visualize the maximum speed in each lane through overlays in the camera's live view.

To find out more about edge-to-edge, see .

### Requirements:

- An Axis license plate verifier camera kit and *AXIS D2210-VE Radar* installed and connected to the network

## Set up the scenario

Set up the scenario in four steps: first configure the camera, then pair and configure the radar, and finally use *AXIS Speed Monitor* to add overlays.

### Before you start:

- Make sure that the camera and radar are directed towards the same area of interest.
- Make sure that the camera and radar are time synced. To check the status, go to **Installation > Time sync status** in each device.
- Make sure that the camera's second view area (**View area 2**) isn't used, since the radar will use it after pairing.

### Configure the camera:

1. Set up the camera according to the instructions in .
2. Make sure to select free flow when you follow the setup assistant. For more information, see .

### Pair the camera with a radar:

1. In the camera's web interface, go to **System > Edge-to-edge > Radar pairing**.
2. Enter the host name, user name, and password of the radar.
3. Click **Connect** to pair the devices.  
When the connection is established, the radar settings will be available in the camera's web interface.

### Note

The default resolution of the paired radar is 1280x720. Keep the default resolution of the radar in the camera's web interface, and if you add it to a VMS.

### Configure the radar:

1. In the camera's web interface, go to **Radar > Scenarios**.
2. Add one radar scenario that covers one lane, and another radar scenario that covers the other lane.
3. For both scenarios, select **Movement in area**, trigger on **Vehicles**, and set a **Speed limit**.  
For more information, go to *Add scenarios* in *AXIS D2210-VE Radar* user manual.

### Note

If you want to add overlays containing license plate information through *AXIS License Plate Verifier*, make sure to add these before you add any overlays in *AXIS Speed Monitor*.

### Use *AXIS Speed Monitor* to add speed overlays:

1. Download and install *AXIS Speed Monitor* on your camera.
2. Add one overlay for each lane, which will show the maximum speed in the camera's live view.  
For installation and configuration instructions, go to *AXIS Speed Monitor user manual*.

## Search for specific events

Use the search feature to search for events using a number of criteria.

1. Go to the application's webpage and select the **Event log** tab.
2. Select the date in the **Start time** and **End time** calendar menus.
3. Enter the license plate in the **Plate** field, if you want to search for a plate.
4. Click the **ROI** drop down menu to select which region of interest, or if both should be relevant in the search.
5. select **Direction** to filter by entry or exit.
6. To filter out license plates that belong to either the allow- or blocklist, click the **Access** drop down menu.
7. Click **Search**.

To go back to the live updated log, click **Live**.

### Note

Once a search has completed you can see a brief summary of statistics pertaining to that search.

To show any description related to the license plates, click the settings icon and check **Show description**.

## Export and share search results

To export any search result as a CSV file with the statistics at that time, click **Export** to save the results as a CSV file

To copy the API as a link which can be used to export data to third party systems, click **Copy search link**.

## Integration

### Use profiles to push events to multiple servers

With profiles, you can push an event to different servers using different protocols at the same time. To use profiles:

1. Select a profile in the **Profiles** drop-down menu.
2. Configure the rule. See .
3. Click **Save**.
4. Select a new profile in the **Profiles** drop-down menu.

### Push event information to third-party software

#### Note

The application sends the event information in JSON format. For more information, *log in using your MyAxis account*, go to the *AXIS VAPIX Library* and select **AXIS License Plate Verifier**

With this feature you can integrate third-party software by pushing the event data through TCP or HTTP POST.

Before you start:

- The camera must be physically installed and connected to the network.
  - AXIS License Plate Verifier must up and running on the camera.
1. Go to **Integration > Push events**.
  2. In the **Protocol** drop-down list, select one of the following protocols:
    - TCP
    - HTTP POST
      - Type the user name and password.
  3. In the **Server URL** field, type the server address and port in the following format: 127.0.0.1:8080
  4. In the **Device ID** field, type the name of the device or leave as is.
  5. Under **Event types**, select one or more of the following options:
    - **New** means the first detection of a license plate.
    - **Update** is either a correction of a character on a previously detected license plate, or when a direction is detected as the plate moves and is tracked across the image.
    - **Lost** is the last tracked event of the license plate before it exits the image. It also contains the direction of the license plate.
  6. To turn on the feature, select **Send event data to server**.
  7. To reduce bandwidth when using HTTP POST, you can select **Do not to send images through HTTP POST**.
  8. Click **Save**.

#### Note

To push events using HTTP POST, you can use an authorization header instead of a user name and password, go to the **Auth-Header** field, and add a path to an authentication API.

### Send images of license plates to a server

With this feature you can push images of the license plates to a server through FTP.

Before you start:

- The camera must be physically installed and connected to the network.
  - AXIS License Plate Verifier must up and running on the camera.
1. Go to **Integration > Push events**.

2. In the **Protocol** drop-down list, select **FTP**.
3. In the **Server URL** field, type the server address in the following format: `ftp://10.21.65.77/LPR`.
4. In the **Device ID** field, type the name of the device. A folder with this name will be created for the images. Images are created using the following format: `timestamp_area of interest_direction_carID_license plate text_country.jpg`.
5. Type the username and password for the FTP server.
6. Select the path and name modifiers for the filenames.
7. Click **Done**.
8. Under **Event types**, select one or more of the following options:
  - **New** means the first detection of a license plate.
  - **Update** is either a correction of a character on a previously detected license plate, or when a direction is detected as the plate moves and is tracked across the image.
  - **Lost** is the last tracked event of the license plate before it exits the image. It also contains the direction of the license plate.

**Note**

Direction is only included in the filename when **Lost** or **Update** is selected.

9. To turn on the feature, select **Send event data to server**.
10. Click **Save**.

**Note**

Note that the image varies depending on what type of capture mode you have selected, see .

**Note**

If push events fail, the app will resend up to the first 100 failed events to the server.  
 When using FTP in push events to a Windows server, do not use %c for naming of images that gives you date and time. This is due to the fact that Windows does not accept the naming set by the function %c for date and time. Note that this is not an issue when using a Linux server.

## Direct integration with 2N

This example describes direct integration with a 2N IP device.

Set up an account in your 2N device:

1. Go to 2N IP Verso.
2. Go to **Services > HTTP API > Account 1**.
3. Select **Enable account**.
4. Select **Camera access**.
5. Select **License plate recognition**.
6. Copy the IP address.

In the AXIS License Plate Verifier app:

1. Go to **Integration > Direct integration**.
2. Add the IP address or URL to the 2N device.
3. Select **Connection type**.
4. Select what the **Barrier** is used for.
5. Type your username and password.
6. Click **Enable integration**.
7. Click **Save**.

To check in the integration is working:

1. Go to 2N IP Verso.
2. Go to **Status > Events**.

## **Integrate with Genetec Security Center**

This example describes setting up a direct integration with Genetec Security Center.

In Genetec Security Center:

1. Go to **Overview**.
2. Make sure that **Database, Directory and License** are online. If they're not, run all Genetec and SQLEXPRESS services in Windows.
3. Go to **Genetec Config Tool > Plugins**.
4. Click **Add an entity**.
5. Go to **Plugin** and select **LPR plugin**.
6. Click **Next**.
7. Click **Next**.
8. Click **Next**.
9. Select the LPR plugin you've added and go to **Data sources**.

Under **ALPR reads API**:

10. Check **Enabled**.
11. In **Name**, type: **Plugin REST API**.
12. In **API path prefix**, type: **lpr**.
13. In **REST port**, select **443**.
14. In **WebSDK host**, type: **localhost**.
15. In **WebSDK port**, select **443**.
16. Check **Allow self signed certificates**.

Under **Security Center events data source**:

17. Check **Enabled**.
18. In **Name**, type **Security Center Lpr Events**.
19. In **Processing frequency**, select **5 sec** in the drop-down menu.
20. Go to the **Data sinks** tab.
21. Click **+**.
22. In **Type**, select **Database**.
23. **Select and configure the database:**
  - Check **Enabled**.
  - In **Source**, check **Plugin REST API and Native ALPR Events**.
  - In **Name**, type **Reads DB**.
  - In **Include**, check **Reads, Hits and Images**.
  - Go to the **Resources** tab.
  - Click **Delete the database** and then **Create a database**.

Create an API user:

24. Go to **Config Tool > User Management**.
25. Click **Add an entity**.

26. Select **User**.
27. Type a username and password. Leave the other fields unchanged.
28. Select the added user and go to the **Privileges** tab.
29. Check to allow everything under **Application privileges**.
30. Check to allow **Third-party ALPR reads API**.
31. Click **Apply**.

In the **AXIS License Plate Verifier** app:

1. Go to the **Integration** tab.
2. Select **Genetec Security Center** in the drop-down list.
3. In **URL/IP**, type your address according to this template: `https://server-address/api/V1/lpr/lpringestion/reads`.
4. Type in your Genetec username and password.
5. Click **Enable integration**.
6. Go to the **Settings** tab.
7. Under **Security > HTTPS**.
8. Select **Self-signed**, or **CA-signed** depending on the settings in Genetec Security Center.

In Genetec Security Center:

1. Go to **Genetec Security desk**.
2. Under **Investigation**, click **Reads**.
3. Go to the **Reads** tab.
4. Filter the result to your needs.
5. Click **Generate report**.

**Note**

You can also read Genetec's documentation on integrating third party ALPR plugins. *You can do that here (requires registration).*

## The web interface

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

### Note

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



Show or hide the main menu.



Access the release notes.



Access the product help.



Change the language.



Set light theme or dark theme.



The user menu contains:

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



The context menu contains:

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

## Status

### Device info

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

**Upgrade AXIS OS:** Upgrade the software on your device. Takes you to the Maintenance page where you can do the upgrade.

### Time sync status

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

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

## Security

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

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

### 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.

### Ongoing recordings

Shows ongoing recordings and their designated storage space.

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



Shows the storage space where the recording is saved.

### 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.

## Video



Click to play the live video stream.



Click to freeze the live video stream.



Click to take a snapshot of the live video stream. The file is saved in the 'Downloads' folder on your computer. The image file name is [snapshot\_YYYY\_MM\_DD\_HH\_MM\_SS.jpg]. The size of the snapshot depends on the compression that 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 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 full screen. Press ESC to exit full screen mode.

## Installation

**Capture mode** 

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

**Mounting position** 

: The orientation of the image can change depending on how you mount the camera.

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

**Rotate:** Select the preferred image orientation.

**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.

## Image correction

### Important

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

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

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

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

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

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

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

**Focus breathing correction** ⓘ : Turn on to keep the angle of view constant while you change the focus. You might not be able to zoom in as much with this function activated.

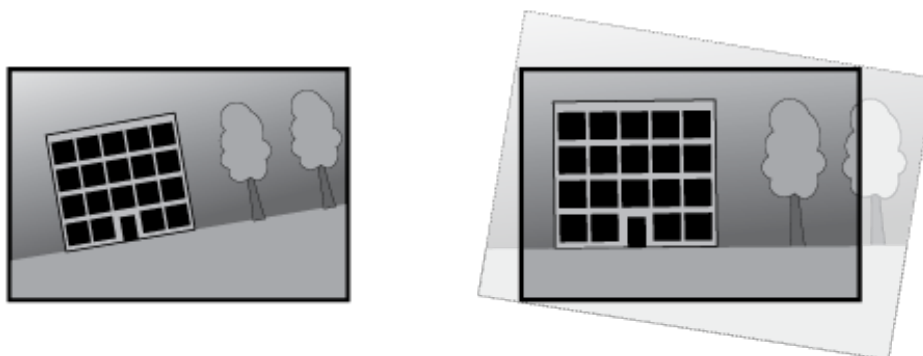
**Straighten image** ⓘ : Turn on and use the slider to straighten the image horizontally by rotating and cropping it digitally. The functionality is useful when it's not possible to mount the camera exactly level. Ideally, straighten the image during installation.



: Click to show a supporting grid in the image.



: Click to hide the grid.



*The image before and after it has been straightened.*

## Image

### Appearance

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

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

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



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



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



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



### Wide dynamic range

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

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

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

### White balance

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

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

#### Light environment:

- **Automatic:** Automatic identification and compensation for the light source color. This is the recommended setting which can be used in most situations.
- **Automatic – outdoors**  : Automatic identification and compensation for the light source color. This is the recommended setting which can be used in most outdoor situations.
- **Custom – indoors**  : Fixed color adjustment for a room with some artificial light other than fluorescent lighting and good for a normal color temperature around 2800 K.
- **Custom – outdoors**  : Fixed color adjustment for sunny weather conditions with a color temperature around 5500 K.
- **Fixed – fluorescent 1:** Fixed color adjustment for fluorescent lighting with a color temperature around 4000 K.
- **Fixed – fluorescent 2:** Fixed color adjustment for fluorescent lighting with a color temperature around 3000 K.
- **Fixed – indoors:** Fixed color adjustment for a room with some artificial light other than fluorescent lighting and good for a normal color temperature around 2800 K.
- **Fixed – outdoors 1:** Fixed color adjustment for sunny weather conditions with a color temperature around 5500 K.
- **Fixed – outdoors 2:** Fixed color adjustment for cloudy weather condition with a color temperature around 6500 K.
- **Street light – mercury**  : Fixed color adjustment for ultraviolet emission in mercury vapor lights common in street lighting.
- **Street light – sodium**  : Fixed color adjustment that compensates for the yellow orange color of sodium vapor lights common in street lighting.
- **Hold current:** Keep the current settings and do not compensate for light changes.
- **Manual**  : Fix the white balance with the help of a white object. Drag the circle to an object that you want the camera to interpret as white in the live view image. Use the **Red balance** and **Blue balance** sliders to adjust the white balance manually.

#### Day-night mode

#### IR-cut filter:

- **Auto:** Select to automatically turn on and off the IR-cut filter. When the camera is in day mode, the IR-cut filter is turned on and blocks incoming infrared light, and when in night mode, the IR-cut filter is turned off and the camera's light sensitivity increases.

#### Note

- Some devices have IR-pass filters in night mode. The IR-pass filter increases IR-light sensitivity but blocks visible light.
- **On:** Select to turn on the IR-cut filter. The image is in color, but with reduced light sensitivity.
- **Off:** Select to turn off the IR-cut filter. The image is in black and white for increased light sensitivity.

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

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

#### IR light

If your device doesn't have built-in illumination, these controls are only available when you connect a supported Axis illuminator.

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

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

**Automatic illumination angle**  : Turn on to use the automatic illumination angle. Turn off to set the illumination angle manually.

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

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

**White light** 

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

**Synchronize illumination**  : Turn on to automatically synchronize the white light with the surrounding light.

#### Exposure

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

#### Exposure mode:

- **Automatic:** The camera adjusts the aperture, gain, and shutter automatically.
- **Automatic aperture** ⓘ : The camera adjusts the aperture and gain automatically. The shutter is fixed.
- **Automatic shutter** ⓘ : The camera adjusts the shutter and gain automatically. The aperture is fixed.
- **Hold current:** Locks the current exposure settings.
- **Flicker-free** ⓘ : The camera adjusts the aperture and gain automatically, and uses only the following shutter speeds: 1/50 s (50 Hz) and 1/60 s (60 Hz).
- **Flicker-free 50 Hz** ⓘ : The camera adjusts the aperture and gain automatically, and uses the shutter speed 1/50 s.
- **Flicker-free 60 Hz** ⓘ : The camera adjusts the aperture and gain automatically, and uses the shutter speed 1/60 s.
- **Flicker-reduced** ⓘ : This is the same as flicker-free, but the camera might use shutter speeds faster than 1/100 s (50 Hz) and 1/120 s (60 Hz) for brighter scenes.
- **Flicker-reduced 50 Hz** ⓘ : This is the same as flicker-free, but the camera might use shutter speeds faster than 1/100 s for brighter scenes.
- **Flicker-reduced 60 Hz** ⓘ : This is the same as flicker-free, but the camera might use shutter speeds faster than 1/120 s for brighter scenes.
- **Manual** ⓘ : The aperture, gain, and shutter are fixed.

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

#### Note

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

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

- **Right**  : Uses an area with a fixed size and position in the right part of the image to calculate the exposure.
- **Spot**: Uses an area with a fixed size and position in the live view to calculate the exposure.
- **Custom**: Uses an area in the live view to calculate the exposure. You can adjust the size and position of the area.

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

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

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

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

#### Note

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

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

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

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

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

#### Note

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

## Optics

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

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

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

## Stream

### General

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

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

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

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

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

### Zipstream

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

Select the bitrate reduction **Strength**:

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

**Optimize for storage**: Turn on to minimize the bitrate while maintaining quality. The optimization does not apply to the stream shown in the web client. This can only be used if your VMS supports B-frames. Turning on **Optimize for storage** also turns on **Dynamic GOP**.

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

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

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

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

## Bitrate control

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

## Orientation

**Mirror**: Turn on to mirror the image.

## Audio

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

**Source**  : Select what audio source to use.

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

## Overlays



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

- **Text:** Select to show a text that is integrated in the live view image and visible in all views, recordings and snapshots. You can enter your own text, and you can also include pre-configured modifiers to automatically show, for example, time, date, and frame rate.
  -  : Click to add the date modifier %F to show yyyy-mm-dd.
  -  : Click to add the time modifier %X to show hh:mm:ss (24-hour clock).
  - **Modifiers:** Click to select any of the modifiers shown in the list to add them to the text box. For example, %a shows the day of the week.
  - **Size:** Select the desired font size.
  - **Appearance:** Select the text color and background color, for example, white text on a black background (default).
  -  : Select the position of the overlay in the image 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. You can use .bmp, .png, .jpeg, or .svg files.  
To upload an image, click **Manage images**. Before you upload an image, you can choose to:
  - **Scale with resolution:** Select to automatically scale the overlay image to fit the video resolution.
  - **Use transparency:** Select and enter the RGB hexadecimal value for that color. Use the format RRGGBB. Examples of hexadecimal values: FFFFFFFF for white, 000000 for black, FF0000 for red, 6633FF for blue, and 669900 for green. Only for .bmp images.
- **Scene annotation**  : Select to show a text overlay in the video stream that stays in the same position, even when the camera pans or tilts in another direction. You can choose to only show the overlay within certain zoom levels.
  -  : Click to add the date modifier %F to show yyyy-mm-dd.
  -  : Click to add the time modifier %X to show hh:mm:ss (24-hour clock).
  - **Modifiers:** Click to select any of the modifiers shown in the list to add them to the text box. For example, %a shows the day of the week.
  - **Size:** Select the desired font size.
  - **Appearance:** Select the text color and background color, for example, white text on a black background (default).
  -  : Select the position of the overlay in the image or click and drag the overlay to move it around in the live view. The overlay is saved and remains in the pan and tilt coordinates of this position.
  - **Annotation between zoom levels (%):** Set the zoom levels which the overlay will be shown within.
  - **Annotation symbol:** Select a symbol that appears instead of the overlay when the camera is not within the set zoom levels.
- **Streaming indicator**  : Select to show an animation superimposed over the video stream. The animation indicates that the video stream is live, even if the scene doesn't contain any motion.

- **Appearance:** Select the animation color and background color, for example, red animation on a transparent background (default).
- **Size:** Select the desired font size.
-  : Select the position of the overlay in the image 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.

## View areas



: Click to create a view area.



Click the view area to access settings.

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

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

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

## Privacy masks



: Click to create a new privacy mask.

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



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

## Analytics

### 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.

## 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.

## 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.

## Audio

### Device settings

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

Allow stream extraction  : Turn on to allow stream extraction.

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

Power type  : Select power type for your input.

Apply changes  : Apply your selection.

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

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

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

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

Output: Shows the type of output.

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

Automatic volume control  : Turn on to make the device automatically and dynamically adjust the gain based on the ambient noise level. Automatic volume control affects all audio outputs, including line and telecoil.

### Stream

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

## 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.

## Audio enhancement

### Input

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

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

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

## Recordings



**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.

**Ongoing recordings:** Show all ongoing recordings on the device.

- Start a recording on the device.



Choose which storage device to save to.

- Stop a recording on the device.

**Triggered recordings** will end when manually stopped or when the device is shut down.

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



Play the recording.



Stop playing the recording.



Show or hide information and options about the recording.

**Set export range:** If you only want to export part of the recording, enter a time span. Note that if you work in a different time zone than the location of the device, the time span is based on the device's time zone.

**Encrypt:** Select to set a password for exported recordings. It will not be possible to open the exported file without the password.



Click to delete a recording.

**Export:** Export the whole or a part of the recording.

## 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.



View the security updates in AXIS OS and ACAP apps.

### Note

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

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

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



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

- **Open-source license:** View information about open-source licenses used in the app.
- **App log:** View a log of the app events. The log is helpful when you contact support.
- **Activate license with a key:** If the app requires a license, you need to activate it. Use this option if your device doesn't have internet access.  
If you don't have a license key, go to [axis.com/products/analytics](https://axis.com/products/analytics). You need a license code and the Axis product serial number to generate a license key.
- **Activate license automatically:** If the app requires a license, you need to activate it. Use this option if your device has internet access. You need a license code to activate the license.
- **Deactivate the license:** Deactivate the license to replace it with another license, for example, when you change from a trial license to a full license. If you deactivate the license, you also remove it from the device.
- **Settings:** Configure the parameters.
- **Delete:** Delete the app permanently from the device. If you don't deactivate the license first, it remains active.

## System

### Time and location

#### Date and time

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

### Note

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

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

- **Automatic date and time (manual NTS KE servers):** Synchronize with the secure NTP key establishment servers connected to the DHCP server.
  - **Manual NTS KE servers:** Enter the IP address of one or two NTP servers. When you use two NTP servers, the device synchronizes and adapts its time based on input from both.
  - **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 before you can select this option.
- **Manual:** Select a time zone from the drop-down list.

**Note**

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

## Device location

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

- **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.

## Network

### IPv4

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

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

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

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

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

#### Note

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

### IPv6

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

### Hostname

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

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

**Enable dynamic DNS updates:** Allow your device to automatically update its domain name server records whenever its IP address changes.

**Register DNS name:** Enter a unique domain name that points to your device's IP address. Allowed characters are A–Z, a–z, 0–9 and –.

**TTL:** Time to Live (TTL) sets how long a DNS record stays valid before it needs to be updated.

### DNS servers

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

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

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

## HTTP and HTTPS

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

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

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

### Note

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

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

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

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

## Network discovery protocols

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

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

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

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

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

**LLDP and CDP:** Turn on to allow automatic discovery on the network. Turning LLDP and CDP off can impact the PoE power negotiation. To resolve any issues with the PoE power negotiation, configure the PoE switch for hardware PoE power negotiation only.

## Global proxies

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

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

Allowed formats for http and https proxies:

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

**Note**

Restart the device to apply the global proxy settings.

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

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

### One-click cloud connection

One-click cloud connection (O3C) together with an O3C service provides easy and secure internet access to live and recorded video from any location. For more information, see [axis.com/end-to-end-solutions/hosted-services](http://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.
  - **Password for the account "initial":** Enter the SNMP password for the account named "initial". Although the password can be sent without activating HTTPS, we don't recommend it. The SNMP v3 password can only be set once, and preferably only when HTTPS is enabled. Once the password is set, the password field is no longer displayed. To set the password again, you must reset the device to factory default settings.

## Security

### Certificates

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

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

These formats are supported:

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

#### Important

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



**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](http://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+)**: 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.

## 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

### Accounts



**Add account:** Click to add a new account. You can add up to 100 accounts.

**Account:** Enter a unique account name.

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

**Repeat password:** Enter the same password again.

**Privileges:**

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



The context menu contains:

**Update account:** Edit the account properties.

**Delete account:** Delete the account. You can't delete the root account.

### Anonymous access

**Allow anonymous viewing:** Turn on to allow anyone access the device as a viewer without logging in with an account.

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

## SSH accounts

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

- **Enable SSH:** Turn on to use SSH service.

**Account:** Enter a unique account name.

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

**Repeat password:** Enter the same password again.

**Comment:** Enter a comment (optional).

⋮ The context menu contains:

**Update SSH account:** Edit the account properties.

**Delete SSH account:** Delete the account. You can't delete the root account.

## Virtual host

 **Add virtual host:** Click to add a new virtual host.

**Enabled:** Select to use this virtual host.

**Server name:** Enter the name of the server. Only use numbers 0-9, letters A-Z, and hyphen (-).

**Port:** Enter the port the server is connected to.

**Type:** Select the type of authentication to use. Select between **Basic**, **Digest**, and **Open ID**.

⋮ The context menu contains:

- **Update:** Update the virtual host.
- **Delete:** Delete the virtual host.

**Disabled:** The server is disabled.

## 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*.

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

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

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



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

**Retain:** Defines which MQTT messages are sent as retained.

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

**QoS:** Select the desired level for the MQTT publication.

## MQTT subscriptions



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

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

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

**Subscription type:**

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

**QoS:** Select the desired level for the MQTT subscription.

## SIP

### Settings

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

**SIP setup assistant:** Click to set up and configure SIP step by step.

**Enable SIP:** Check this option to make it possible to initiate and receive SIP calls.

**Allow incoming calls:** Check this option to allow incoming calls from other SIP devices.

#### Call handling

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

#### Ports

A port number must be between 1024 and 65535.

- **SIP port:** The network port used for SIP communication. The signaling traffic through this port is non-encrypted. The default port number is 5060. Enter a different port number if required.
- **TLS port:** The network port used for encrypted SIP communication. The signaling traffic through this port is encrypted with Transport Layer Security (TLS). The default port number is 5061. Enter a different port number if required.
- **RTP start port:** The network port used for the first RTP media stream in a SIP call. The default start port number is 4000. Some firewalls block RTP traffic on certain port numbers.

#### NAT traversal

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

##### Note

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

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

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

#### Audio and video

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

##### Note

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

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

#### Additional

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

## Accounts

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

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

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



**Add account:** Click to create a new SIP account.

- **Active:** Select to be able to use the account.
- **Make default:** Select to make this the default account. There must be a default account, and there can only be one default account.
- **Answer automatically:** Select to automatically answer an incoming call.
- **Prioritize IPv6 over IPv4**  : Select to prioritize IPv6 addresses over IPv4 addresses. This is useful when you connect to peer-to-peer accounts or domain names that resolve in both IPv4 and IPv6 addresses. You can only prioritize IPv6 for domain names that are mapped to IPv6 addresses.
- **Name:** Enter a descriptive name. This can, for example, be a first and last name, a role, or a location. The name is not unique.
- **User ID:** Enter the unique extension or phone number assigned to the device.
- **Peer-to-peer:** Use for direct calls to another SIP device on the local network.
- **Registered:** Use for calls to SIP devices outside the local network, through a SIP server.
- **Domain:** If available, enter the public domain name. It will be shown as part of the SIP address when calling other accounts.
- **Password:** Enter the password associated with the SIP account for authenticating against the SIP server.
- **Authentication ID:** Enter the authentication ID used for authenticating against the SIP server. If it is the same as the user ID, you don't need to enter the authentication ID.
- **Caller ID:** The name which is presented to the recipient of calls from the device.
- **Registrar:** Enter the IP address for the registrar.
- **Transport mode:** Select the SIP transport mode for the account: UDP, 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.

## Storage

### Network storage

**Ignore:** Turn on to ignore network storage.

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

- **Address:** Enter the IP address or host name of the host server, typically a NAS (network-attached storage). We recommend you to configure the host to use a fixed IP address (not DHCP since a dynamic IP address can change) or that you use DNS. Windows SMB/CIFS names are not supported.
- **Network share:** Enter the name of the shared location on the host server. Several Axis devices can use the same network share since each device gets its own folder.
- **User:** If the server requires a login, enter the username. To log in to a specific domain server, type DOMAIN\username.
- **Password:** If the server requires a login, enter the password.
- **SMB version:** Select the SMB storage protocol version to connect to the NAS. If you select **Auto**, the device tries to negotiate one of the secure versions SMB: 3.02, 3.0, or 2.1. Select 1.0 or 2.0 to connect to older NAS that don't support higher versions. You can read more about SMB support in Axis devices [here](#).
- **Add share without testing:** Select to add the network share even if an error is discovered during the connection test. The error can be, for example, that you didn't enter a password even though the server requires one.

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

**Unbind:** Click to unbind and disconnect the network share.

**Bind:** Click to bind and connect the network share.

**Unmount:** Click to unmount the network share.

**Mount:** Click to mount the network share.

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

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

#### Tools

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

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

### Onboard storage

#### Important

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

**Unmount:** Click to safely remove the SD card.

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

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

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

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

#### Tools

- **Check:** Check for errors on the SD card.
- **Repair:** Repair errors in the file system.
- **Format:** Format the SD card to change the file system and erase all data. You can only format the SD card to the ext4 file system. You need a third-party ext4 driver or application to access the file system from Windows®.
- **Encrypt:** Use this tool to format the SD card and enable encryption. This erases all data stored on the SD card. Any new data you store on the SD card will be encrypted.
- **Decrypt:** Use this tool to format the SD card without encryption. This erases all data stored on the SD card. Any new data you store on the SD card will not be encrypted.
- **Change password:** Change the password required to encrypt the SD card.

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

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

## Stream profiles

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



**Add stream profile:** Click to create a new stream profile.

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

**Name:** Add a name for your profile.

**Description:** Add a description of your profile.

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

**Resolution:** See for a description of this setting.

**Frame rate:** See for a description of this setting.

**Compression:** See for a description of this setting.

**Zipstream**  : See for a description of this setting.

**Optimize for storage**  : See for a description of this setting.

**Dynamic FPS**  : See for a description of this setting.

**Dynamic GOP**  : See for a description of this setting.

**Mirror**  : See for a description of this setting.

**GOP length**  : See for a description of this setting.

**Bitrate control:** See for a description of this setting.

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

**Include audio**  : See for a description of this setting.

## ONVIF

### 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](https://axis.com).



**Add accounts:** Click to add a new ONVIF account.

**Account:** Enter a unique account name.

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

**Repeat password:** Enter the same password again.

**Role:**

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



The context menu contains:

**Update account:** Edit the account properties.

**Delete account:** Delete the account. You can't delete the root account.

## ONVIF media profiles

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



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

**Profile name:** Add a name for the media profile.

**Video source:** Select the video source for your configuration.

- **Select configuration:** Select a user-defined configuration from the list. The configurations in the drop-down list correspond to the device's video channels, including multiviews, view areas and virtual channels.

**Video encoder:** Select the video encoding format for your configuration.

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

#### Note

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

**Audio source**  : Select the audio input source for your configuration.

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

**Audio encoder**  : Select the audio encoding format for your configuration.

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

**Audio decoder**  : Select the audio decoding format for your configuration.

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

**Audio output**  : Select the audio output format for your configuration.

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

**Metadata:** Select the metadata to include in your configuration.

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

**PTZ**  : Select the PTZ settings for your configuration.

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

**Create:** Click to save your settings and create the profile.

**Cancel:** Click to cancel the configuration and clear all settings.

**profile\_x:** Click on the profile name to open and edit the preconfigured profile.

## Detectors

### Camera tampering

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

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

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

#### Note

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

### Audio detection

These settings are available for each audio input.

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

## 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.

## 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.

**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.

## Edge-to-edge

### Pairing

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 where you can play audio clips and transmit sound through the camera. The network microphone will take up sounds from the surrounding area and make it available as an audio input device, usable in media streams and recordings.

### Important

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

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.



**Add:** Add a device to pair with.

**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 will show all Axis devices that are found, not only devices that can be paired.

Only devices with **Bonjour** enabled can be found. To enable **Bonjour** for a device, open the device's web interface and go to **System > Network > Network discovery protocols**.

**Note**

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.



To pair a device from the list, click .

**Select pairing type:** Select from the drop-down list.

**Speaker pairing:** Select to pair a network speaker.

**Microphone pairing**  : Select to pair a microphone.

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

**Username:** Enter username.

**Password:** Enter password for the user.

**Close:** Click to clear all fields.

**Connect:** Click to establish connection to the device to pair with.

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



**Add:** Add a device to pair with.

**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 will show all Axis devices that are found, not only devices that can be paired.

Only devices with **Bonjour** enabled can be found. To enable **Bonjour** for a device, open the device's web interface and go to **System > Network > Network discovery protocols**.

**Note**

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.



To pair a device from the list, click .

**Select pairing type:** Select from the drop-down list.

**Address:** Enter the host name or IP address of the radar.

**Username:** Enter the username of the radar.

**Password:** Enter the password for the radar.

**Close:** Click to clear all fields.

**Connect:** Click to connect to the radar.

When connected, the radar settings will be available in the main menu. For more information about radar settings, see the paired radar's user manual.

## Logs

### Reports and logs

#### Reports

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

#### Logs

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

**Reset PTR**  : Reset PTR if for some reason the **Pan**, **Tilt**, or **Roll** settings aren't working as expected. The PTR motors are always calibrated in a new camera. But calibration can be lost, for example, if the camera loses power or if the motors are moved by hand. When you reset PTR, the camera is re-calibrated and returns to its factory default position.

**Calibration**  : Click **Calibrate** to recalibrate the pan, tilt, and roll motors to their default positions.

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

**Port check**: To verify connectivity from the device to a specific IP address and TCP/UDP port, enter the hostname or IP address and port number you want to check and click **Start**.

### Network trace

#### Important

A network trace file might contain sensitive information such as certificates or passwords.

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

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

## Learn more

### Edge-to-edge technology

Edge-to-edge is a technology that makes IP devices communicate directly with each other. It offers smart pairing functionality between, for example, Axis cameras and Axis audio or radar products.

For more information, see the white paper "Edge-to-edge technology" at [whitepapers.axis.com/edge-to-edge-technology](http://whitepapers.axis.com/edge-to-edge-technology).

### Radar pairing

With edge-to-edge radar pairing, you can connect your camera to a compatible Axis radar and benefit from integrated radar features, such as speed detection.

Radar pairing is a one-way setup where you pair one camera with one radar and use the camera to configure and maintain both devices. When paired, you can access the radar's settings and create rules for radar-specific events directly in the camera's web interface. The camera will also identify itself to a VMS as a camera with integrated radar functionality.

Additionally, the radar stream is visualized in the camera's second view area, called **view area 2**. The metadata produced by the radar is available through the camera's second metadata producer channel, called **channel 2**.

### Speaker pairing

Edge-to-edge speaker pairing allows you to use a compatible Axis network speaker as if it's part of your camera. Once paired, the speaker's features are integrated in the camera's web interface and the network speaker acts as an audio out device where you can play audio clips and transmit sound through the camera.

The camera will identify itself to the VMS as a camera with integrated audio output and redirect any played audio to the speaker.

### View area

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

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

#### Note

If you pair the camera with a radar through edge-to-edge, the radar stream is visualized in the camera's second view area.

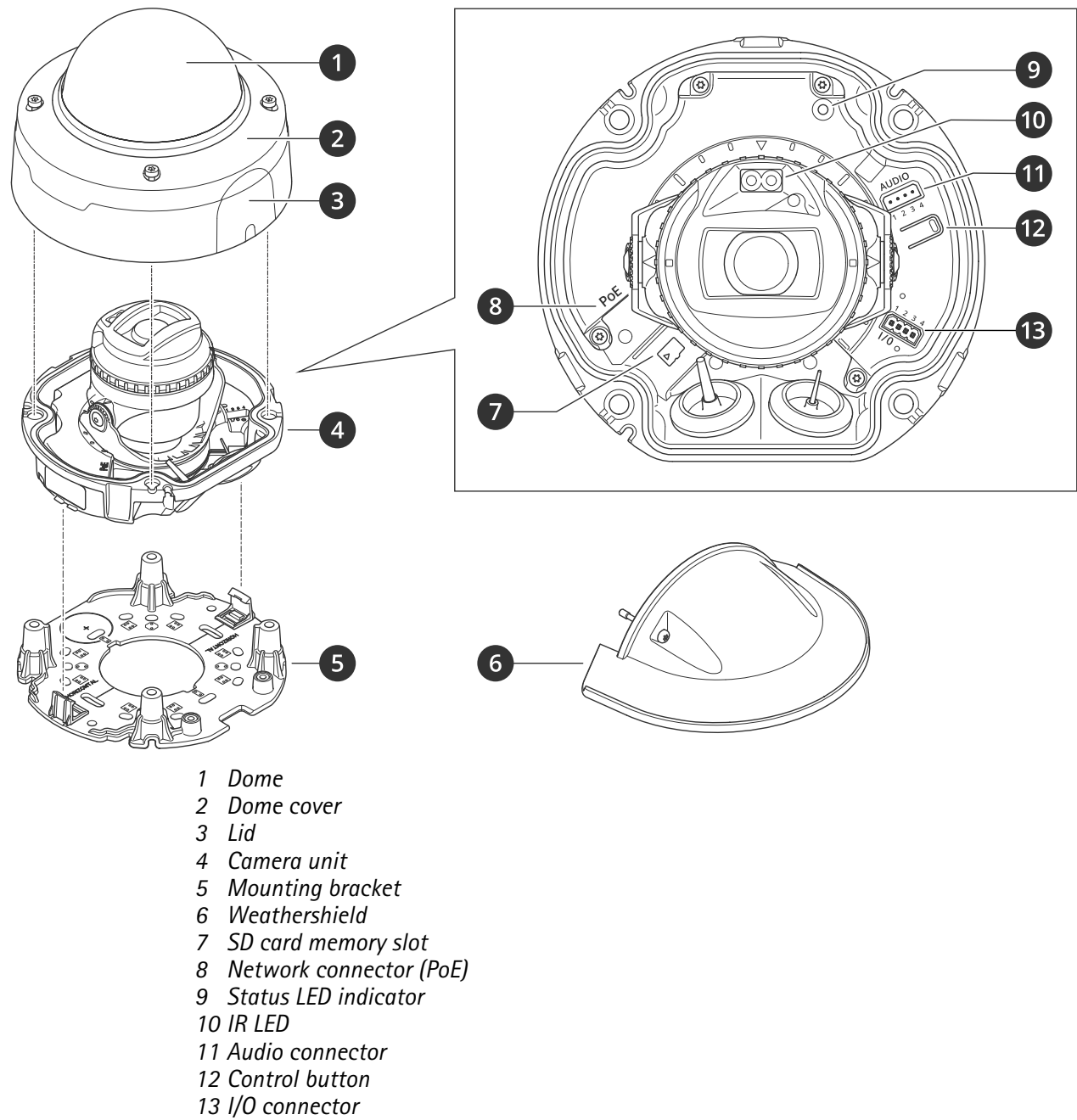
### AXIS Image Health Analytics

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

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

Specifications

Product overview



LED indicators

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

## SD card slot

### NOTICE

- Risk of damage to SD card. Don't use sharp tools, metal objects, or excessive force when inserting or removing the SD card. Use your fingers to insert and remove the card.
- Risk of data loss and corrupted recordings. Unmount the SD card from the device's web interface before removing it. Don't remove the SD card while the product is running.

This device supports microSD/microSDHC/microSDXC cards.

For SD card recommendations, see [axis.com](http://axis.com).



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

## Buttons

### Control button

The control button is used for:

- Resetting the product to factory default settings. See .

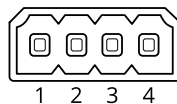
## Connectors

### Network connector

RJ45 Ethernet connector with Power over Ethernet (PoE).

### Audio connector

4-pin terminal block for audio input and output.



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

### I/O connector

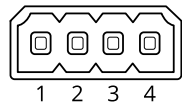
Use the I/O connector with external devices in combination with, for example, motion detection, event triggering, and alarm notifications. In addition to the 0 VDC reference point and power (12 V DC output), the I/O connector provides the interface to:

**Digital input** – For connecting devices that can toggle between an open and closed circuit, for example PIR sensors, door/window contacts, and glass break detectors.

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

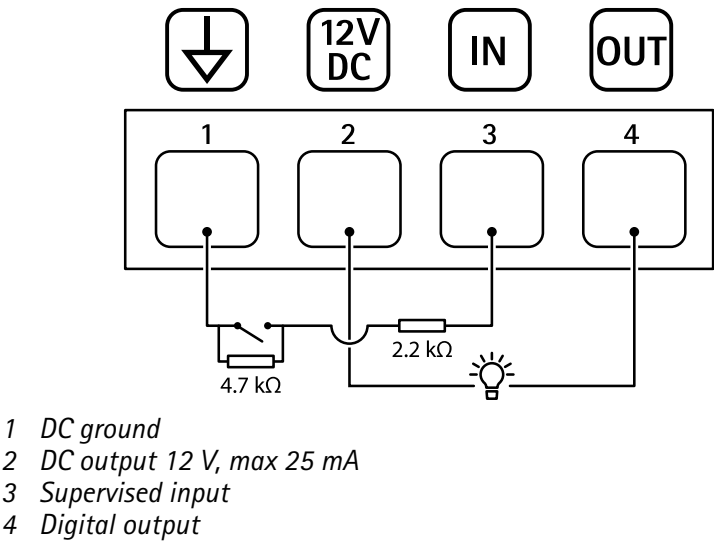
**Digital output** – For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface, through an event or from the device's web interface.

4-pin terminal block



| Function                          | Pin | Notes                                                                                                                                                                                                                             | Specifications                      |
|-----------------------------------|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| DC ground                         | 1   |                                                                                                                                                                                                                                   | 0 VDC                               |
| DC output                         | 2   | <div>⚠</div> Can be used to power auxiliary equipment.<br>Note: This pin can only be used as power out.                                                                                                                           | 12 VDC<br>Max load = 25 mA          |
| Digital Input or Supervised Input | 3   | Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. To use supervised input, install end-of-line resistors. See connection diagram for information about how to connect the resistors.                   | 0 to max 30 VDC                     |
| Digital Output                    | 4   | Internally connected to pin 1 (DC ground) when active, and floating (unconnected) when inactive. If used with an inductive load, e.g., a relay, connect a diode in parallel with the load, to protect against voltage transients. | 0 to max 30 VDC, open drain, 100 mA |

Example:



## Troubleshooting

### Reset to factory default settings

#### ⚠ WARNING

⚠ Possibly hazardous optical radiation is emitted from this product. It can be harmful to the eyes. Do not stare at the operating lamp.

#### Important

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

#### Note

The camera has been preconfigured with AXIS License Plate Verifier. If you reset to factory default, you will keep the license key. You will not need to reinstall the application after a factory reset.

To reset the product to the factory default settings:

1. Disconnect power from the product.
2. Press and hold the control button while reconnecting power. See .
3. Keep the control button pressed for 15–30 seconds until the status LED indicator flashes amber.
4. Release the control button. The process is complete when the status LED indicator turns green. The product has been reset to the factory default settings. If no DHCP server is available on the network, the default IP address is 192.168.0.90.
5. Use the installation and management software tools to assign an IP address, set the password, and access the device.  
The installation and management software tools are available from the support pages on [axis.com/support](https://axis.com/support).

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

### AXIS OS options

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

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

### Check the current AXIS OS version

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

To check the current AXIS OS version:

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

## Upgrade AXIS OS

### Important

- Preconfigured and customized settings are saved when you upgrade the device software (provided that the features are available in the new AXIS OS) although this is not guaranteed by Axis Communications AB.
- Make sure the device remains connected to the power source throughout the upgrade process.

### Note

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

1. Download the AXIS OS file to your computer, available free of charge at [axis.com/support/device-software](https://axis.com/support/device-software).
2. Log in to the device as an administrator.
3. Go to **Maintenance > AXIS OS upgrade** and click **Upgrade**.

When the upgrade has finished, the product restarts automatically.

You can use AXIS Device Manager to upgrade multiple devices at the same time. Find out more at [axis.com/products/axis-device-manager](https://axis.com/products/axis-device-manager).

## Technical issues, clues, and solutions

If you can't find what you're looking for here, try the troubleshooting section at [axis.com/support](https://axis.com/support).

### Problems upgrading AXIS OS

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

### Problems setting the IP address

|                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The device is located on a different subnet                         | If the IP address intended for the device and the IP address of the computer used to access the device are located on different subnets, you cannot set the IP address. Contact your network administrator to obtain an IP address.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| The IP address is being used by another device                      | <p>Disconnect the Axis device from the network. Run the ping command (in a Command/DOS window, type <code>ping</code> and the IP address of the device):</p> <ul style="list-style-type: none"> <li>• If you receive: <code>Reply from &lt;IP address&gt;: bytes=32; time=10...</code> this means that the IP address may already be in use by another device on the network. Obtain a new IP address from the network administrator and reinstall the device.</li> <li>• If you receive: <code>Request timed out</code>, this means that the IP address is available for use with the Axis device. Check all cabling and reinstall the device.</li> </ul> |
| Possible IP address conflict with another device on the same subnet | The static IP address in the Axis device is used before the DHCP server sets a dynamic address. This means that if the same default static IP address is also used by another device, there may be problems accessing the device.                                                                                                                                                                                                                                                                                                                                                                                                                          |

### The device can't be accessed from a browser

---

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Can't log in                             | <p>When HTTPS is enabled, ensure that the correct protocol (HTTP or HTTPS) is used when attempting to log in. You may need to manually type <code>http</code> or <code>https</code> in the browser's address field.</p> <p>If the password for the root account is lost, the device must be reset to the factory default settings. See .</p>                                                                                                                   |
| The IP address has been changed by DHCP  | <p>IP addresses obtained from a DHCP server are dynamic and may change. If the IP address has been changed, use AXIS IP Utility or AXIS Device Manager to locate the device on the network. Identify the device using its model or serial number, or by the DNS name (if the name has been configured).</p> <p>If required, a static IP address can be assigned manually. For instructions, go to <a href="https://axis.com/support">axis.com/support</a>.</p> |
| Certificate error when using IEEE 802.1X | For authentication to work properly, the date and time settings in the Axis device must be synchronized with an NTP server. Go to <b>System &gt; Date and time</b> .                                                                                                                                                                                                                                                                                           |

### The device is accessible locally but not externally

---

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

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

For instructions and download, go to [axis.com/vms](https://axis.com/vms).

### Problems with streaming

---

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

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Lower frame rate than expected           | <ul style="list-style-type: none"> <li>• See .</li> <li>• Reduce the number of applications running on the client computer.</li> <li>• Limit the number of simultaneous viewers.</li> <li>• Check with the network administrator that there is enough bandwidth available.</li> <li>• Lower the image resolution.</li> <li>• Log in to the device's web interface and set a capture mode that prioritizes frame rate. If you change the capture mode to prioritize frame rate it might lower the maximum resolution, depending on the device used and capture modes available.</li> </ul> |
| Can't select H.265 encoding in live view | Web browsers don't support H.265 decoding. Use a video management system or application that supports H.265 decoding.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

#### Can't connect over port 8883 with MQTT over SSL

|                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The firewall blocks traffic using port 8883 as it's deemed insecure. | <p>In some cases the server/broker might not provide a specific port for MQTT communication. It may still be possible to use MQTT over a port normally used for HTTP/HTTPS traffic.</p> <ul style="list-style-type: none"> <li>• If the server/broker supports WebSocket/WebSocket Secure (WS/WSS), typically on port 443, use this protocol instead. Check with the server/broker provider to see if WS/WSS is supported and which port and basepath to use.</li> <li>• If the server/broker supports ALPN, the use of MQTT can be negotiated over an open port, such as 443. Check with your server/broker provider to see if ALPN is supported and which ALPN protocol and port to use.</li> </ul> |
|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Unknown vehicles are marked as accepted

If the application lets in vehicles with license plates that are not in the allowlist, one probable reason is that the comparison allows a deviation of one character.

For example, if **AXI S1234** is in the allowlist the application accepts **AXI SI234**.

Similarly, if **AXIS 1234** is in the allowlist the application accepts **AXI 1234**.

Go to to set the characters allowed.

#### The connection between the application and controller or relay module doesn't work

Make sure the controller, or relay module, allows data traffic through HTTP. To find out how to change this setting, go to the user manual for the corresponding device.

#### Problems with radar pairing

|                                        |                                                                                                                                                                                                                                                                         |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| I can't pair the camera with the radar | <p>Make sure the camera's second view area (<b>View area 2</b>) isn't used since the radar will be assigned to this automatically.</p> <p>If the second view area is used, go to <b>Video &gt; View areas</b> to remove it, and then try to pair the devices again.</p> |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The moving vehicles in the camera view are not in sync with the speed overlays, or with the tracks in the radar view | <p>Make sure the camera and radar are time synced.</p> <p>To check the status, go to <b>Status &gt; Time sync status</b> in the web interface of each device. If the status shows <b>Synchronized: No</b>, click on <b>NTP settings</b> and select a time source for synchronizing the device. Make sure to use the same time source for both devices.</p>             |
| The camera's second view area doesn't show the radar stream correctly                                                | <p>The default resolution of the radar after edge-to-edge pairing is 1280x720, both in the camera's web interface and in a VMS. If you select another resolution, the radar stream will appear incorrectly.</p> <p>To adjust the resolution of the radar, go to <b>Video &gt; Stream &gt; General</b> in the camera's web interface and select <b>View area 2</b>.</p> |

| Problems with overlays                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The overlays I have added through the camera's web interface disappear after radar pairing | <p>If you have added more than one view area in the camera, any previously added overlays will disappear from the camera's web interface. Since the radar will occupy the second view area after radar pairing, all existing overlays in the camera's web interface will disappear.</p> <p>The overlays will only disappear from the web interface. You can still request a stream containing the overlays, for example in a VMS.</p> |
| The license plate overlays I have added in AXIS License Plate Verifier don't appear        | <p>If you have added overlays that show the vehicle speed in AXIS Speed Monitor, and then turn on license plate overlays in AXIS License Plate Verifier, the license plate overlays won't appear.</p> <p>Make sure to turn on the overlays in AXIS License Plate Verifier first, before you add any speed overlays through AXIS Speed Monitor.</p>                                                                                    |

## Performance considerations

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

The following factors are the most important to consider:

- High image resolution or lower compression levels result in images containing more data which in turn affects the bandwidth.
- Rotating the image in the GUI can increase the product's CPU load.
- Access by large numbers of Motion JPEG clients or unicast H.264/H.265/AV1 clients affects the bandwidth.
- Simultaneous viewing of different streams (resolution, compression) by different clients affects both frame rate and bandwidth.  
Use identical streams wherever possible to maintain a high frame rate. Stream profiles can be used to ensure that streams are identical.
- Accessing video streams with different codecs simultaneously affects both frame rate and bandwidth. For optimal performance, use streams with the same codec.
- Heavy usage of event settings affects the product's CPU load which in turn affects the frame rate.
- Using HTTPS may reduce frame rate, in particular if streaming Motion JPEG.
- Heavy network utilization due to poor infrastructure affects the bandwidth.
- Viewing on poorly performing client computers lowers perceived performance and affects frame rate.
- Running multiple AXIS Camera Application Platform (ACAP) applications simultaneously may affect the frame rate and the general performance.

## Contact support

If you need more help, go to [axis.com/support](https://axis.com/support).

T10191705

2025-09 (M14.2)

© 2023 – 2025 Axis Communications AB