AXIS P3285-LVE Kit License Plate Verifier

User manual

Solution overview

1 *Indoor dome camera*
2 *Outdoor dome camera*
3 *Surveillance center*

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.

Get started

Find the device on the network

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

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

Browser support

You can use the device with the following browsers:

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

✓: Recommended

*: Supported with limitations

Open the device's web interface

1. Open a browser and type the IP address or host name of the Axis device.
   If you don't know the IP address, use AXIS IP Utility or AXIS Device Manager to find the device on the network.
2. Type the username and password. If you access the device for the first time, you must create an administrator account. See *Create an administrator account, on page 4*.

For descriptions of all features and settings in the web interface of devices with AXIS OS, see *AXIS OS web interface help*.

Create an administrator account

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

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

Important

The device has no default account. If you lose the password for your administrator account, you must reset the device. See *Reset to factory default settings, on page 55*.

Secure passwords

Important

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

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

To protect your data we strongly recommend that you:

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

Make sure that no one has tampered with the device software

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

1. Reset to factory default settings. See *Reset to factory default settings, on page 55*.
   After the reset, secure boot guarantees the state of the device.
2. Configure and install the device.

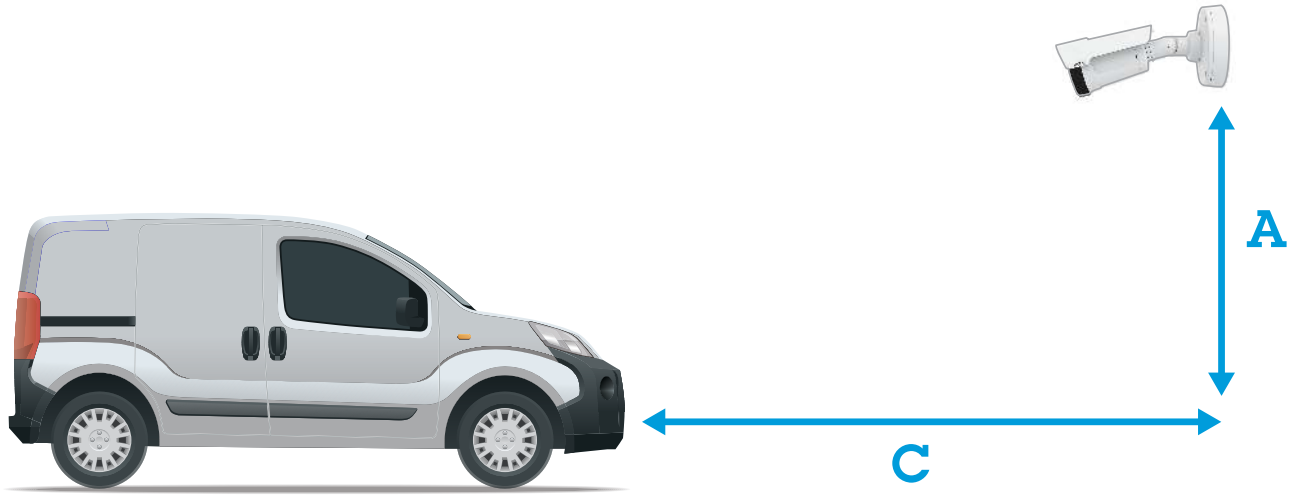
Basic setup

These setup instructions are valid for all scenarios:

1. *Camera mounting recommendations, on page 6*
2. *Setup assistant, on page 8*
3. *Adjust the area of interest, on page 10*
4. *Select region, on page 11*
5. *Set up event storage, on page 11*

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.

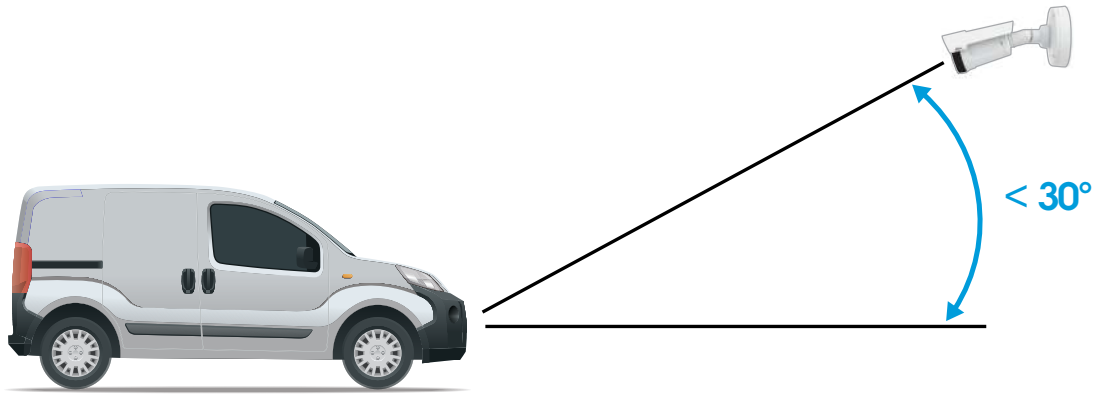
Capture distance: (C)	Mounting height (A)
2.0 m (6.6 ft)	1.0 m (3.3 ft)
3.0 m (9.8 ft)	1.5 m (4.9 ft)
4.0 m (13 ft)	2.0 m (6.6 ft)
5.0 m (16 ft)	2.5 m (8.2 ft)
7.0 m (23 ft)	3.5 m (11 ft)

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

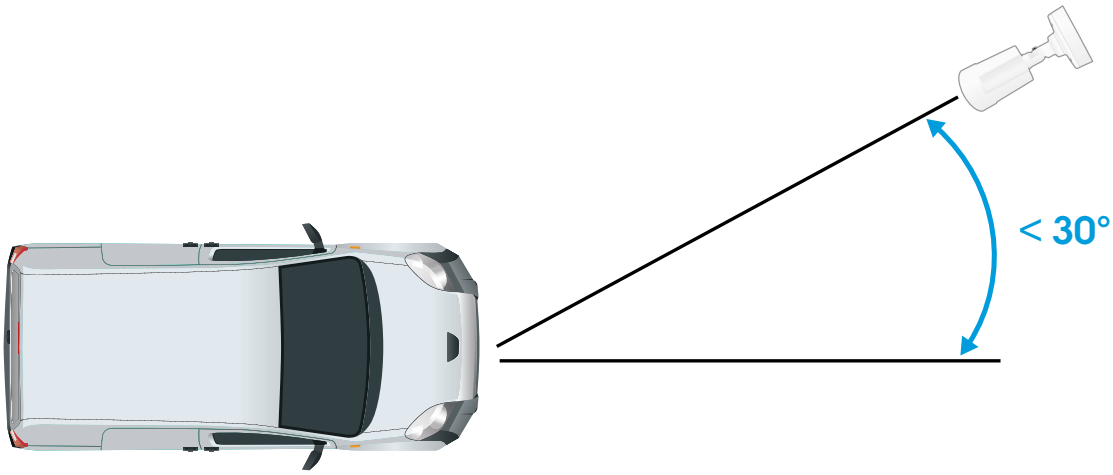
Capture distance (C)	Mounting height (A)
7.0 m (23 ft)	3.0 m (9.8 ft)
10.0 m (33 ft)	4.0 m (13 ft)

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.

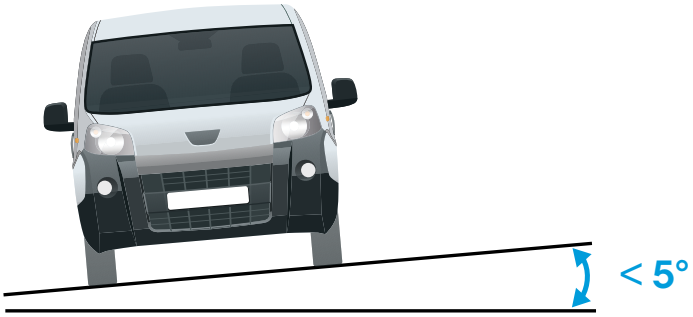


Mounting angle from the side.



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, go to **Settings > Maintenance** and under **Setup assistant** press **Start**.

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 *Adjust the area of interest, on page 10*.
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 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 *Open a barrier for known vehicles using the camera's I/O, on page 32*.
   - **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 *Adjust the image capture settings, on page 11*.
4. Drag the anchor points to adjust the area of interest. See *Adjust the area of interest, on page 10*.
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: *Push event information to third-party software, on page 40*.

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 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 **Image**.
3. Click on 1:1 to zoom in where you want monitor traffic or manage access control.
4. To improve verification and captured images, click on **AF**.
5. To have the camera automatically focus on the vehicles, click **AF**. To set the focus manually, adjust it with the slider.
6. Click on **Area of interest** to see it displayed in the view area.
7. To move the area of interest, click anywhere in the area to select it and drag it to where the license plates are most visible. Make sure the region of interest stays in position after you have saved the settings.
8. To adjust the area of interest, click anywhere in the area to select it and drag the anchor points highlighted in blue.
   - To reset the area of interest, click on the reset button on the lower left corner next to the number icon.
   - To add anchor points, click the on one of the dark anchor points. The anchor point will turn yellow, showing it can be manipulated. New dark points are automatically added next to the yellow anchor point. The maximum amount of yellow anchor points is eight.
9. Click anywhere outside the area of interest to save your changes.
10. To get the correct direction feedback in the **Event log**, you need to turn the arrow to match the driving direction.
    10.1. Click the arrow icon.
    10.2. Select the anchor point and rotate the arrow so it aligns with the driving direction.
    10.3. 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.

11. To check if your area of interest is large enough for the best results, use the pixel counter.
    - To show the pixel counter, click on the calculator icon.
    - To adjust the full size pixel counter area, drag the lower right corner of the area highlighted in yellow.
    - To move the pixel counter area, click anywhere in the area and drag it where you want.

- To add a second area of interest, click on **+** next to **1**.

- If you are using a standalone camera, you can have the app set the recommended settings for license plate recognition.
  1. Click on the magic wand icon and the settings will be optimized for license plate recognition.
  2. Click on the menu button next to the magic wand to see the set values.

Select region

1. Go to **Settings** > **Recognition**.
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 **Image resolution**
3. To change the rotation of the captured image, go to **Rotation**

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** > **Storage**.
2. Under **Retain events**, select **Allowlisted**.
3. Under **Retention period**, select **30 days**.
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.

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.

An SD card can save up to 100,000 events using any type of frame.

Configure your device

This section covers all the important configurations that an installer needs to do to get the product up and running after the hardware installation has been completed.

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.

Basic settings

Set the capture mode

1. Go to **Video > Installation > Capture mode**.
2. Click **Change**.
3. Select a capture mode and click **Save and restart**.
   See also *Capture modes, on page 45*.

Set the orientation

1. Go to **Video > Installation > Rotate**.
2. Select **0** , **90**, **180** or **270** degrees.
   See also *Monitor long and narrow areas, on page 15*.

Adjust the image

This section includes instructions about configuring your device. If you want to learn more about how certain features work, go to *Learn more, on page 45*.

Level the camera

To adjust the view in relation to a reference area or an object, use the level grid in combination with a mechanical adjustment of the camera.

1. Go to **Video > Image >** and click .
2. Click to show the level grid.
3. Adjust the camera mechanically until the position of the reference area or the object is aligned with the level grid.

Adjust the zoom and focus

To adjust the zoom:

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

To adjust the focus:

1. Click to show the autofocus area.
2. Adjust the autofocus area to cover the part of the image that you want to be in focus.
   If you don't select an autofocus area, the camera focuses on the entire scene. We recommend that you focus on a static object.
3. Click **Autofocus**.
4. To fine tune the focus, adjust the focus slider.

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/IO/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**.

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

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

1. Go to **Video > Image > Day-night mode**, and make sure that the **IR-cut filter** is set to **Auto**.
2. To set at what light level you want the camera to switch to night mode, move the **Threshold** slider toward **Bright** or **Dark**.
3. To use the built-in IR light when the camera is in night mode, turn on **Allow illumination** and **Synchronize illumination**.

Note

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

Optimize IR illumination

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

1. Go to **Video > Image > Day-night mode**.
2. Turn on **Allow illumination**.
3. Click IR in the live view and select **Manual**.
4. Adjust the intensity.

Reduce noise in low-light conditions

To reduce noise in low-light conditions, you can adjust one or more of the following settings:

- Adjust the trade-off between noise and motion blur. Go to **Video > Image > Exposure** and move the **Blur-noise trade-off** slider toward **Low noise**.
- Set the exposure mode to automatic.

Note

A high max shutter value can result in motion blur.

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

Note

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

- Set the max gain to a lower value.
- If there is an **Aperture** slider, move it towards **Open**.
- Reduce sharpness in the image, under **Video > Image > Appearance**.

Reduce motion blur in low-light conditions

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

Note

When you increase the gain, image noise also increases.

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

Note

When you open the aperture, the depth of field gets shallower.

- Move the **Aperture** slider toward **Open**.

If you still have problems with motion blur:

- Increase the light level in the scene.
- Mount the camera so that objects move toward it or away from it rather than sideways.

Handle scenes with strong backlight

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

Image without WDR.

Image with WDR.

Note

- WDR can cause artifacts in the image.
- WDR may not be available for all capture modes.

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

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

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.

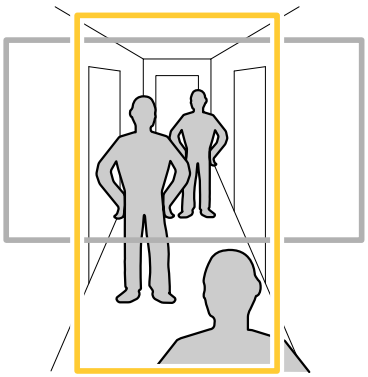
Note

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)**.

Monitor long and narrow areas

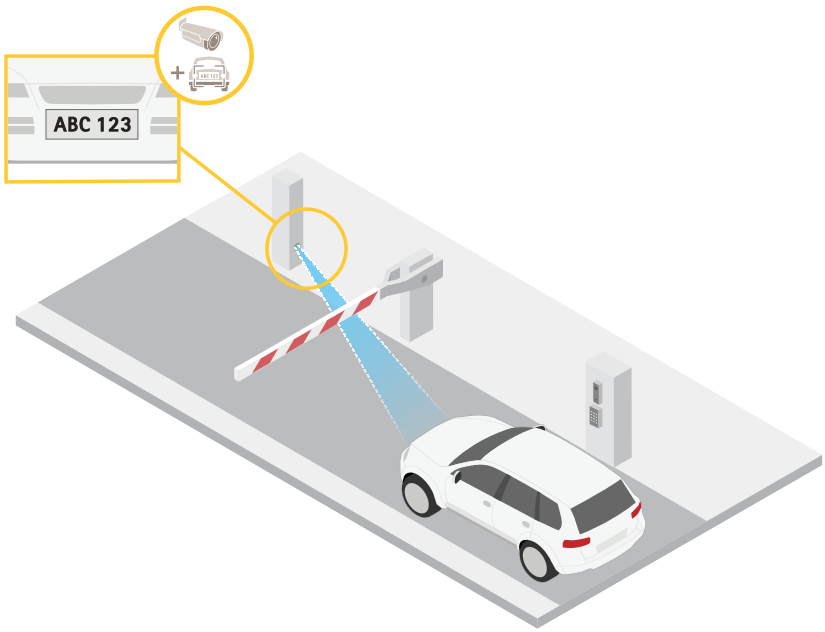
Use corridor format to better utilize the full field of view in a long and narrow area, for example a staircase, hallway, road, or tunnel.



1. Depending on your device, turn the camera or the 3-axis lens in the camera 90° or 270°.
2. If the device doesn't have automatic rotation of the view, go to **Video > Installation**.
3. Rotate the view 90° or 270°.

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.

Hide parts of the image with privacy masks

You can create one or several privacy masks to hide parts of the image.

1. Go to **Video** > **Privacy masks**.
2. Click + .
3. Click the new mask and type a name.
4. Adjust the size and placement of the privacy mask according to your needs.
5. To change the color for all privacy masks, click **Privacy masks** and select a color.

See also *Privacy masks, on page 46*

Show an image overlay

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

1. Go to **Video** > **Overlays**.
2. Click **Manage images**.
3. Upload or drag and drop an image.

4. Click **Upload**.
5. Select **Image** from the drop-down list and click + .
6. Select the image and a position. You can also drag the overlay image in the live view to change the position.

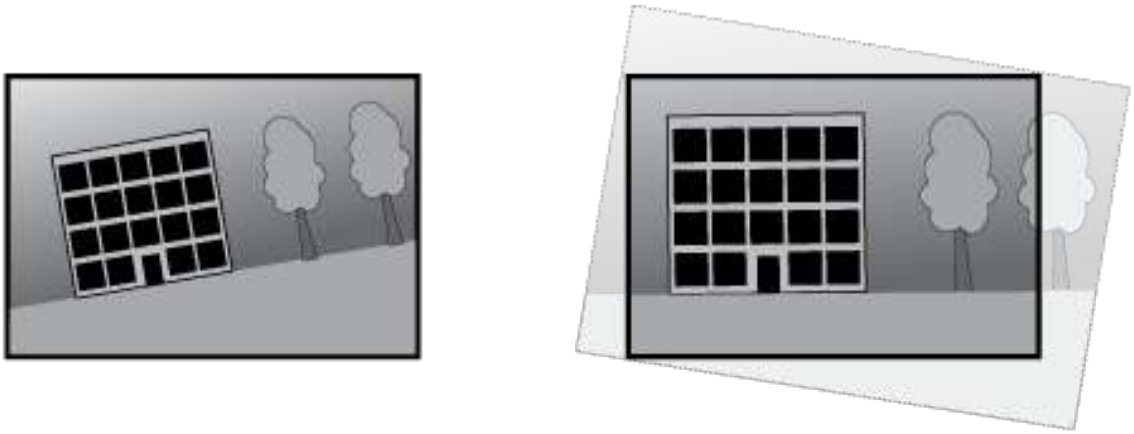
Show a text overlay

You can add a text field as an overlay in the video stream. This is useful for example when you want to display the date, time or a company name in the video stream.

1. Go to **Video > Overlays**.
2. Select **Text** and click + .
3. Type the text you want to display, or select modifiers to show for example the current date.
4. Select a position. You can also click-and-drag the overlay in the live view to change the position.

Straighten a skewed image

You can straighten a skewed image by rotating and cropping it digitally. Due to the cropping, a part of the original image is lost. The functionality is useful during installation.



The illustration shows before and after an image has been straightened.

1. Go to **Video > Installation > Image correction**.
2. Turn on **Straighten image**.
3. Use the controls to adjust the image.

View and record video

This section includes instructions about configuring your device. To learn more about how streaming and storage works, go to *Streaming and storage, on page 46*.

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 *Set up network storage, on page 18*
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. Record video directly on the device, or use AXIS Camera Station Pro or another compatible video management software. For AXIS Camera Station Pro instructions, see the *AXIS Camera Station Pro user manual*.
3. Export the recorded video.
4. Use Axis *signed media verifier* tool to verify the recording.

Set up rules for events

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

To learn more, see *Get started with rules for events*.

Trigger an action

1. Go to **System > Events** and add a rule. The rule defines when the device will perform certain actions. You can set up rules as scheduled, recurring, or manually triggered.
2. Enter a **Name**.
3. Select the **Condition** that must be met to trigger the action. If you specify more than one condition for the rule, all of the conditions must be met to trigger the action.
4. Select which **Action** to perform when the conditions are met.

Record video when the camera detects an object

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

Before you start:

- Make sure you have an SD card installed.

Make sure that AXIS Video Motion Detection is running:

1. Go to **Apps > AXIS Video Motion Detection**.
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 **VMD4**.
4. In the list of actions, under **Recordings**, select **Record video while the rule is active**.
5. In the list of storage options, select **SD_DISK**.
6. Select a camera and a stream profile.
7. Set the prebuffer time to 5 seconds.
8. Set the postbuffer time to 1 minute.
9. Click **Save**.

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

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

Make sure that AXIS Video Motion Detection is running:

1. Go to **Apps > AXIS Video Motion Detection**.

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

Add the overlay text:

1. Go to **Video > Overlays**.
2. Under **Overlays**, select **Text** and click + .
3. Enter `#D` in the text field.
4. Choose text size and appearance.
5. To position the text overlay, click and select an option.

Create a rule:

1. Go to **System > Events** and add a rule.
2. Type a name for the rule.
3. In the list of conditions, under **Application**, select **VMD4**.
4. In the list of actions, under **Overlay text**, select **Use overlay text**.
5. Select a video channel.
6. In **Text**, type "Motion detected".
7. Set the duration.
8. Click **Save**.

Note

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

Provide visual indication of an ongoing event

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

Required hardware

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

Note

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

Note

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

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

1. Go to **System > Accessories > I/O ports**.
2. Make sure that the port you connected the AXIS I/O Indication LED to is set to **Output**. Set the normal state to **Circuit open**.
3. Go to **System > Events**.
4. Create a new rule.
5. Select the **Condition** that must be met to trigger the camera to start recording. It can, for example, be a time schedule or motion detection.

6. In the list of actions, select **Record video**. Select a storage space. Select a stream profile or create a new. Also set the **Prebuffer** and **Postbuffer** as required.
7. Save the rule.
8. Create a second rule and select the same **Condition** as in the first rule.
9. In the list of actions, select **Toggle I/O while the rule is active**, and then select the port the AXIS I/O Indication LED is connected to. Set the state to **Active**.
10. Save the rule.

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

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

Trigger a notification when the enclosure is opened

This example explains how to set up an email notification when the housing or casing of the device is opened.

Add an email recipient:

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

Create a rule:

9. Go to **System > Events > Rules** and click **Add a rule**.
10. Type a name for the rule.
11. In the list of conditions, select **Casing open**.
12. In the list of actions, select **Send notification to email**.
13. Select a recipient from the list.
14. Type a subject line and message for the email.
15. 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**.

Connect to a strobe siren

Network pairing allows you to pair a camera with a compatible Axis device with light and siren functionality. Once paired, the camera can configure and maintain both devices.

Pair the camera with a strobe siren:

1. Go to **System > Edge-to-edge > Pairing**.
2. Click + **Add** and select the pairing type **Network pairing** from the drop-down list.
3. Type the IP address, username and password of the strobe siren.
4. Click **Connect**. A confirmation message appears.

To find devices directly on the network, click **Discover devices**.

Note

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

Important

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

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 on **Home**.
2. Go to **Live**.
3. Click on the arrow icon on the registered plate in the list.
4. Click on **Append plate to list**.
5. Select the list you would like to add the license plate in the dialog.
6. Click **Append**.

Note

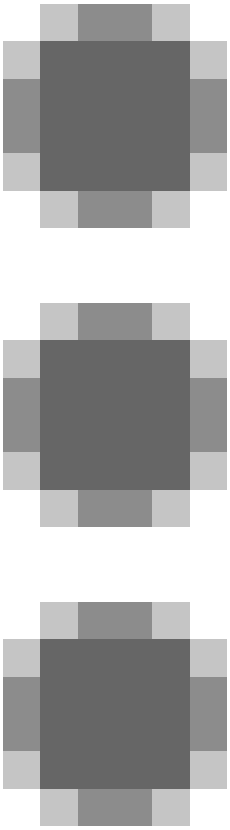
Make sure the symbols **<**, **>** and **&** aren't used in either the license plate or description.

Add descriptions to license plates

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

- Go to **List management**.

- Select the license plate and click



then select **Edit** in the drop-down menu.

- Type the relevant information in the **Description** field.
- Click **Save**.

Note

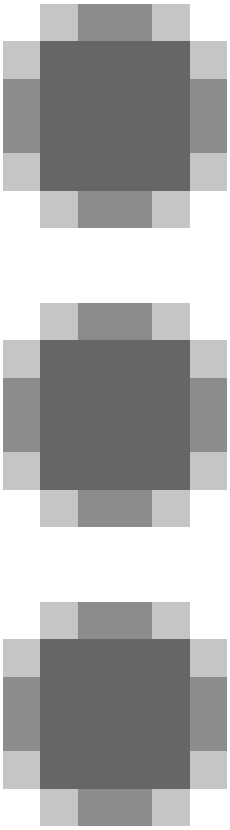
Make sure the symbols **<**, **>** and **&** aren't used in either license plates or descriptions.

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. Click



next to the list you want to change.

3. Select **Edit**.
4. Type the name of the list.
5. Click **Submit**.

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`

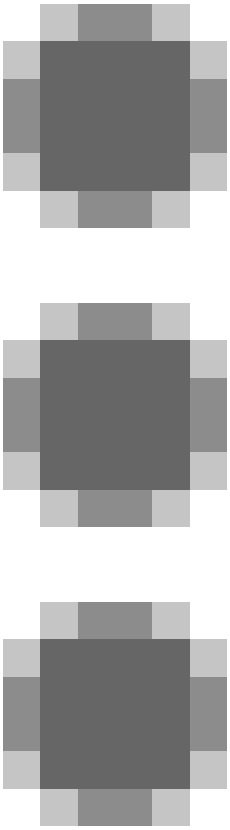
License plate + description: `AXIS123,,John Smith`

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. Click on



next to **Allowlist** and select **Import** in the drop-down menu.

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.

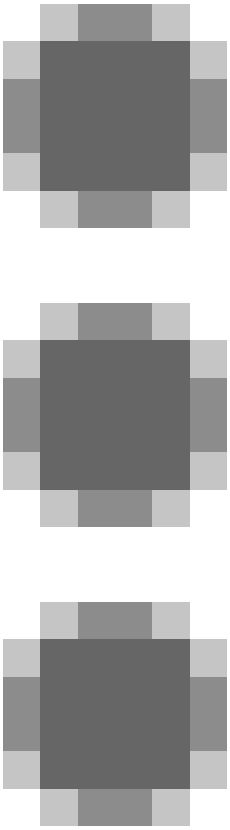
1. Go to **List management > List synchronization**.
2. Under **Remote connected devices**, type the IP address, username and password.
3. Click **Add**.
4. Click **Synchronize list**.

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**.
- Click



next to the list you want to change.
- Select **Schedule** in the drop-down 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. Select either **Timestamp and license plate** or **License plate only**.
4. Set **Overlay duration** to a value between 1 and 9 seconds.
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 confidence threshold. 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 set a lower confidence threshold, which will allow for detection of more plates.

1. Go to **Settings > Recognition**.
2. Adjust the slider under **Confidence threshold**.
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 > Recognition**.
2. Under **Number of characters**, adjust the slider to set 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 > Recognition**.
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, 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 **Download 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 .

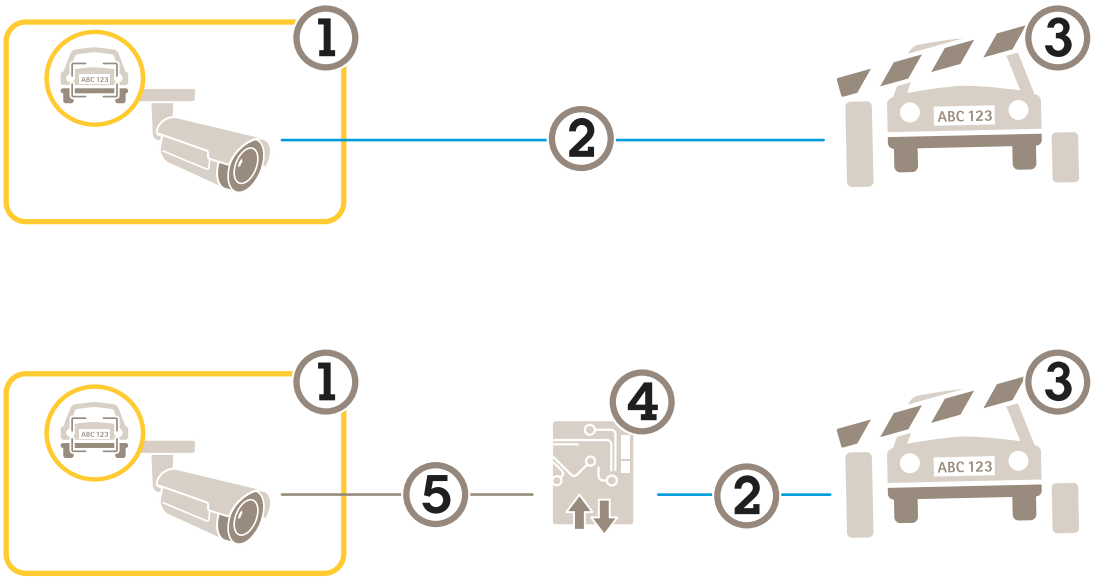
1. Go to the application's webpage and select the **Settings** tab.
2. Go to **Access control**.

3. Under **Access control**, select **Internal I/O**.
4. Select the **I/O output #**.
5. Select a port in the **Virtual port** drop-down list.
6. Under **Barrier mode**, select **Open to all**.
7. Under **Vehicle direction**, select **Any**.
8. Select the **Area of interest** you would like to use.
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 .

1. Go to the application's webpage and go to **Home** and add detected license plates to a list. See *Add detected license plate to list, on page 23*
2. To edit the lists directly, go to **List management** .
3. Enter the authorized license plate numbers in the **Allowlist** field.
4. Go to **Settings**.
5. Under **Access control** , select **Internal I/O**.
6. Select the **I/O output #**.
7. Under **Barrier mode**, select **Open from lists** and then check **Allowlist**.
8. In the **Vehicle direction** drop-down list, select **in**.
9. Under **Area of interest**, 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:

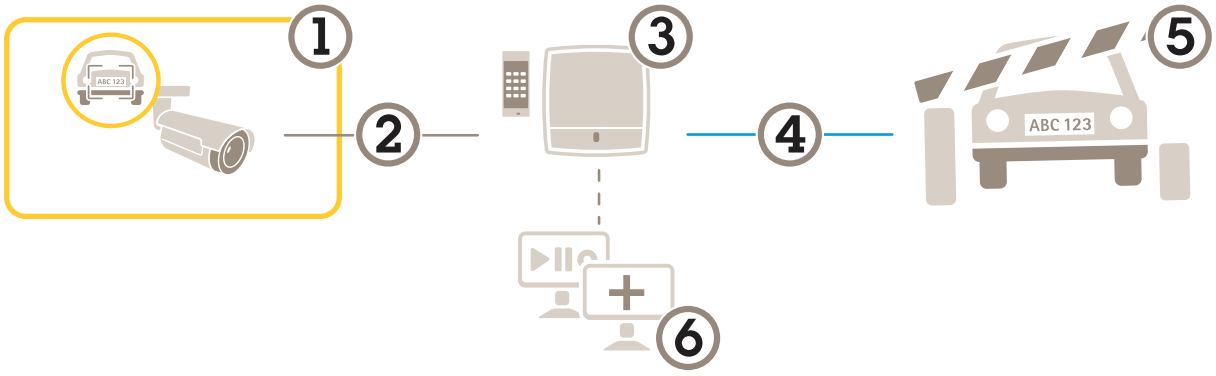
- Basic setup done. See .

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*



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 .

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

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**.

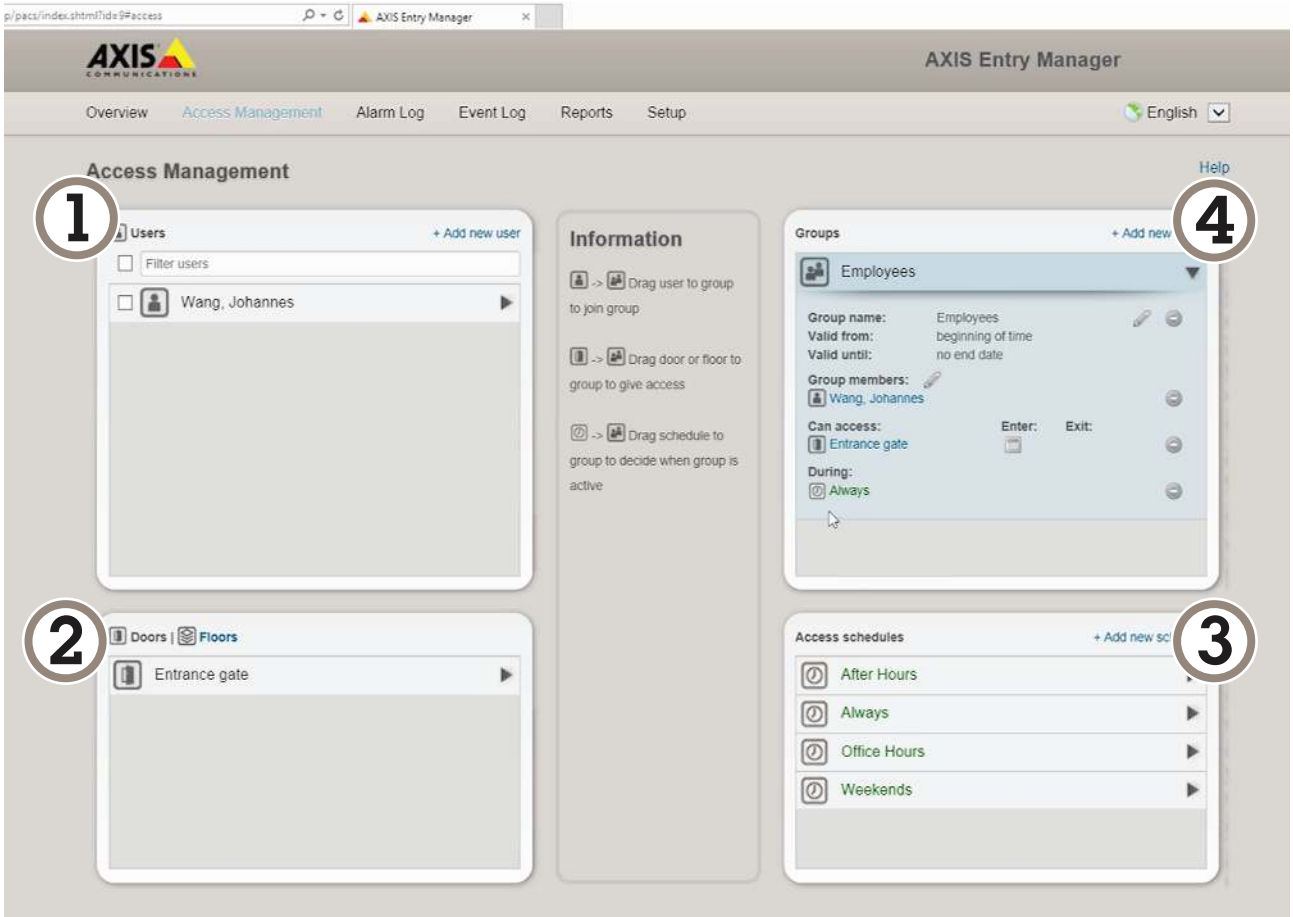
6. In **Configure readers connected to this controller**, clear the **Exit reader** option.
7. Click **Finish**.

Configuration in AXIS License Plate Verifier

1. Go 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 *Adjust the area of interest, on page 10*.
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 *Edge-to-edge technology, on page 49*.

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 *Free flow, on page 8*.

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 **Search** page.
2. Select the date in the **From** and **To** calendar menus.
3. Click the **AOI** drop down menu to select which area of interest should be included in the search.
4. select **Direction** to filter by entry or exit.
5. Enter the license plate in the **Plate** field, if you want to search for a plate.
6. To find license plates that belong to a specific country, select a country in the **Country** drop-down list..
7. To filter out images based on the view of the vehicle, select **Front** or **Rear** in the **Vehicle view** drop-down list.
8. To filter the search results based on the make, model, type or color of the vehicle, select what you are looking for in the **Vehicle details** drop-down menus.
9. Click **Apply filters** to view the search results.

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. Go to **Integration** and the **Push events** page.
2. Select **Profile 1**.
3. Configure the rule. See *Push event information to third-party software, on page 40*.
4. Test the rule.
5. Select a new profile tab to configure a new rule.

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. Select an empty profile
3. In the **Protocol** drop-down list, select **HTTP POST**.
4. In the **Server URL** field, type the server address and port in the following format: `127.0.0.1:8080`
5. Type the user name and password.
6. If you are using a proxy, turn the proxy on and type the hostname, username and password.
7. In the **Device ID** field, type the name of the device or leave as is.
8. Select which direction to trigger push events under **Push conditions**.
9. Under **LPR 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 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.
   - **Conditional** pushes one event for one object when conditions are met.
10. To reduce bandwidth when using HTTP POST, you can select **Do not to send images**.
11. Enable **Event buffer** to buffer events if the server goes down, and send them when the server becomes available.
12. To include the license plate crop in addition to the image if you've chosen under **Retention settings** select **Send two images**.
13. To send the events in mulitpart format instead of base64, select **Multipart**.
14. Click **Test** to test the integration with a virtual license plate.
15. To turn on the feature, select **Activate**.

Note

To push events using HTTP POST, you can use an authorization header instead of a user name and password, go to **Auth-Header** , 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. Type the username and password for the FTP server.
5. Select the path and name modifiers for the filenames.
6. 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.
7. Select which direction to trigger push events under **Push conditions**.
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 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.
   - **Conditional** pushes one event for one object when conditions are met.

   Note

   Direction is only included in the filename when **Lost** or **Update** is selected.
9. Click **Test** to test the integration with a virtual license plate.
10. To turn on the feature, click **Activate**.

Note

Note that the image varies depending on what type of capture mode you have selected, see *Adjust the image capture settings, on page 11*.

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. Select **2N IP Device**.
3. Add the IP address or URL to the 2N device.
4. Type your username and password.
5. Select **Connection type**.
6. Select what the **Barrier is used for**.
7. Click **Enable integration**.
8. Select the direction of the vehicles..
9. To turn on the feature, select **Activate**.

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 **Integration > Direct integration**.
2. Select **Genetec Security Center**.
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. Select **Connection type**.
6. To turn on the feature, select **Activate**.
7. Click **Test** to test the integration with a virtual license plate.
8. If you've chosen HTTPS, go to the **Settings** tab.
9. Under **Security > HTTPS**.
10. 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 read about all the features and settings available in the web interface of devices with AXIS OS, go to *AXIS OS web interface help*.

Learn more

View area

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

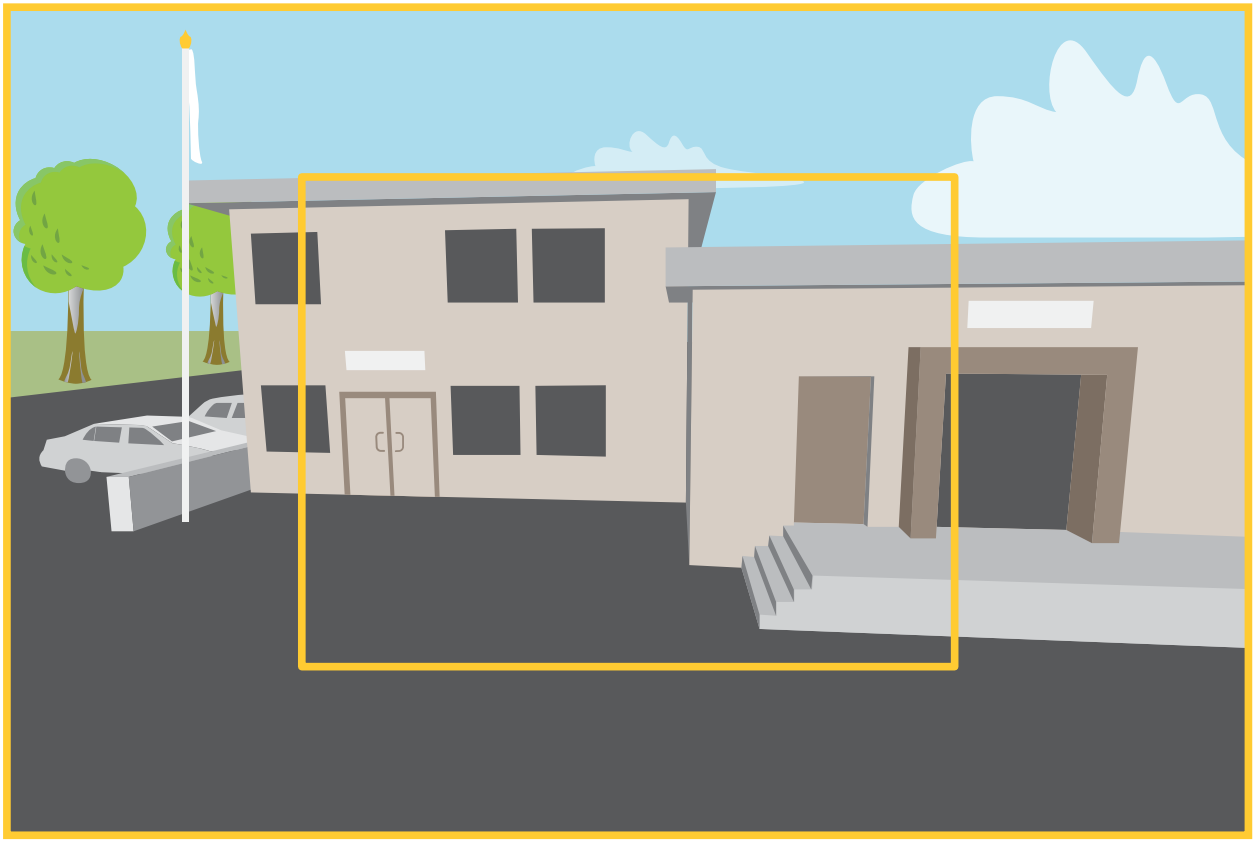
When you set up a view area, we recommend you to set the video stream resolution to the same size as or smaller than the view area size. If you set the video stream resolution larger than the view area size it implies digitally scaled up video after sensor capture, which requires more bandwidth without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

Capture modes

A capture mode is a preset configuration that defines how the camera captures images.

- The capture mode setting can affect the maximum resolution and maximum frame rate available in the device.
- The capture mode with a lower resolution than the maximum can reduce the field of view.
- The capture mode also affects the shutter speed, which in turn affects the light sensitivity. This is because a capture mode with a high maximum frame rate has a reduced light sensitivity, and the other way around.
- With some capture modes you can't use WDR.

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



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

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

Remote focus and zoom

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

Privacy masks

A privacy mask is a user-defined area that prevents users from viewing a part of the monitored area. In the video stream, privacy masks appear as blocks of solid color.

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

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

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

Important

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

You can create several privacy masks. Each mask can have 3 to 10 anchor points.

Important

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

Overlays

Note

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

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

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

Note

Overlays are included in all video streams except SIP calls when the connection is over PoE class 3.

Streaming and storage

Video compression formats

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

Motion JPEG

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

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

H.264 or MPEG-4 Part 10/AVC

Note

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

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

H.265 or MPEG-H Part 2/HEVC

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

Note

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

AV1

AV1 (AOMedia Video 1) is a license -free video coding format optimized for streaming media. AV1 enables high-quality video streaming even in bandwidth-constrained environments. By reducing a video's bitrate, AV1 preserves video quality while minimizing data usage.

AV1 supports all major browsers, computer operating systems and mobile platforms.

Note

AV1 requires more processing power for encoding and decoding compared to some other codecs.

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

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

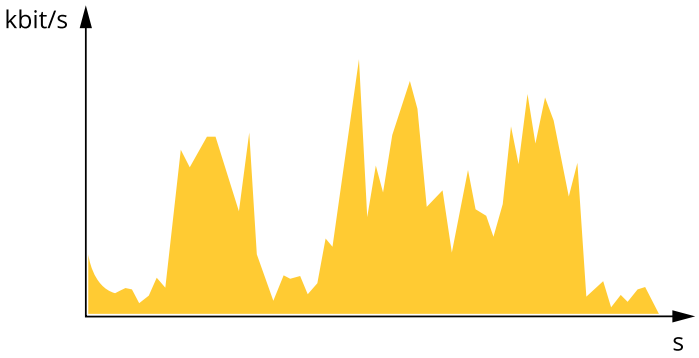
The **Stream** tab contains settings for video streams. You get these settings if you request a video stream from the product and don't specify for example resolution, or frame rate. When you change the settings in the **Stream** tab, it doesn't affect ongoing streams, but it will take effect when you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

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

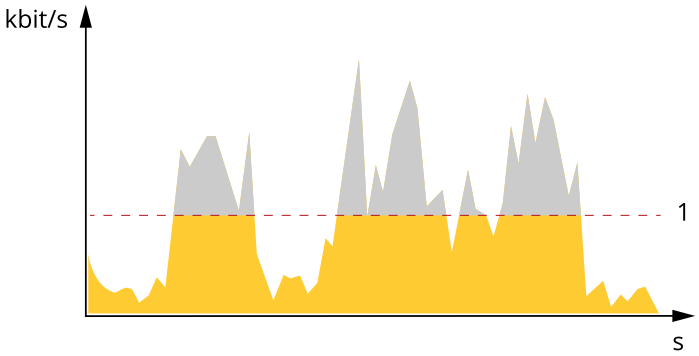
Bitrate control

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

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



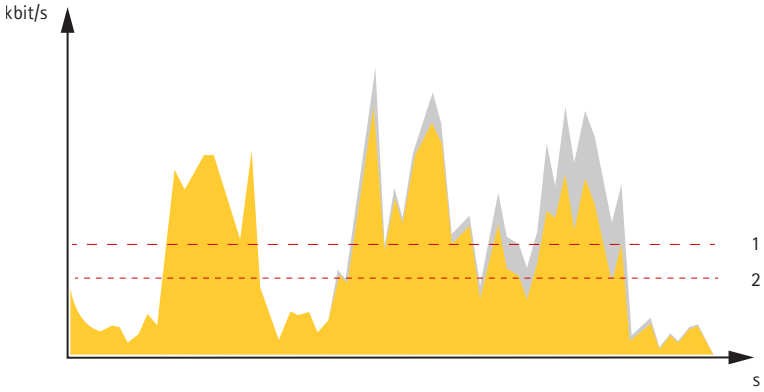
Maximum bitrate (MBR)
Maximum bitrate lets you set a target bitrate to handle bitrate limitations in your system. You might see a decline in image quality or frame rate as the instantaneous bitrate is kept below the specified target bitrate. You can choose to prioritize either image quality or frame rate. We recommend that you configure the target bitrate to a higher value than the expected bitrate. This gives you a margin in case there is a high level of activity in the scene.



1 Target bitrate

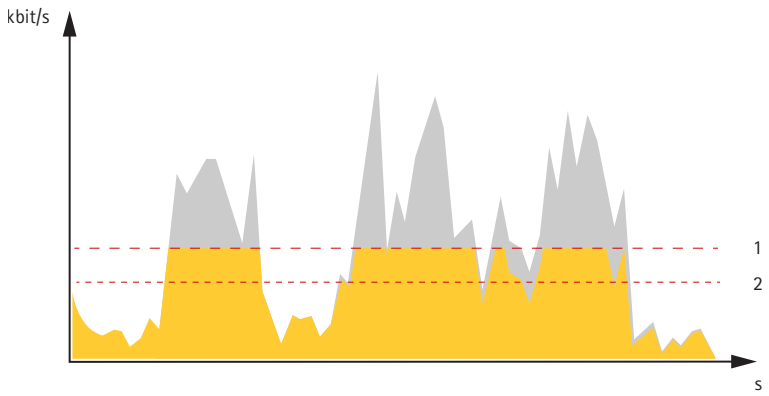
Average bitrate (ABR)
With average bitrate, the bitrate is automatically adjusted over a longer period of time. This is so you can meet the specified target and provide the best video quality based on your available storage. Bitrate is higher in scenes with a lot of activity, compared to static scenes.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

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



1 Target bitrate
2 Actual average bitrate

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



1 *Target bitrate*
2 *Actual average bitrate*

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.

Note

Make sure the paired devices run the same AXIS OS version.

For more information, see the white paper "Edge-to-edge technology" at *whitepapers.axis.com/edge-to-edge-technology*.

Network pairing

With edge-to-edge network pairing, you can connect your camera to a compatible Axis device with light and siren or illuminator light functionality and benefit from its integrated features.

Analytics and apps

With analytics and apps you can get more out of your Axis device. AXIS Camera Application Platform (ACAP) is an open platform that makes it possible for third parties to develop analytics and other apps for Axis devices. Apps can be preinstalled on the device, available for download for free, or for a license fee.

To find the user manuals for Axis analytics and apps, go to *help.axis.com*.

Note

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

AXIS Object Analytics

AXIS Object Analytics is an analytic application that comes preinstalled on the camera. It detects objects that move in the scene and classifies them as, for example, humans or vehicles. You can set up the application to send alarms for different types of objects. To find out more about how the application works, see *AXIS Object Analytics user manual*.

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.

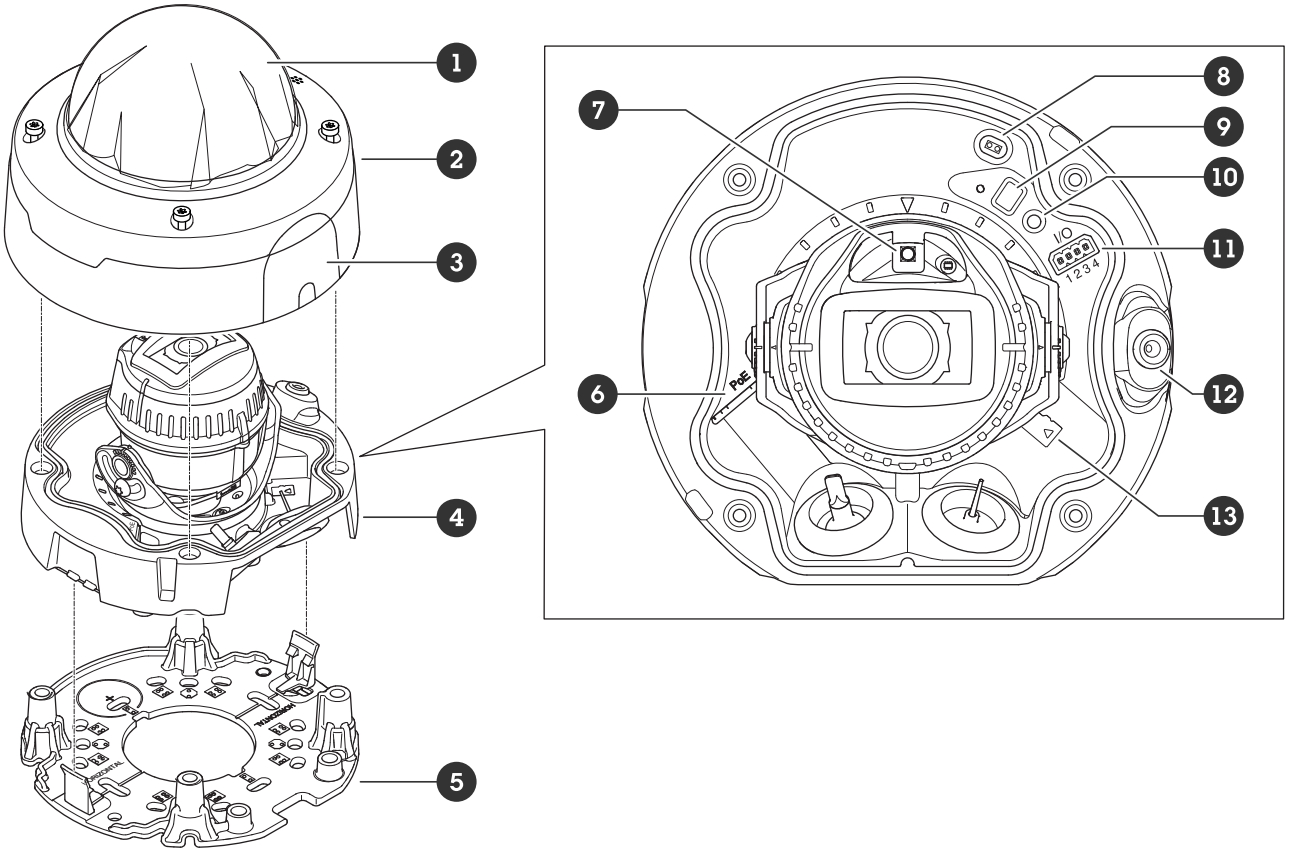
To find out more about how the application works, see *AXIS Image Health Analytics user manual*.

Metadata visualization

Analytics metadata is available for moving objects in the scene. Supported object classes are visualized in the video stream through a bounding box surrounding the object, along with information about the object type and confidence level of the classification. To learn more about how to configure and consume analytics metadata, see *AXIS Scene Metadata integration guide*.

Specifications

Product overview



1 *Dome*
2 *Dome casing*
3 *Lid*
4 *Camera unit*
5 *Mounting bracket*
6 *Network connector (PoE)*
7 *IR LED*
8 *Case open detector*
9 *Control button*
10 *Status LED indicator*
11 *I/O connector*
12 *Acoustic sensor*
13 *SD card memory slot*

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*.

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

Buttons

Control button

The control button is used for:

- Resetting the product to factory default settings. See *Reset to factory default settings, on page 55*.

Connectors

Network connector

RJ45 Ethernet connector with Power over Ethernet (PoE).

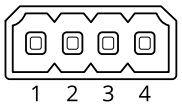
I/O connector

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.

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

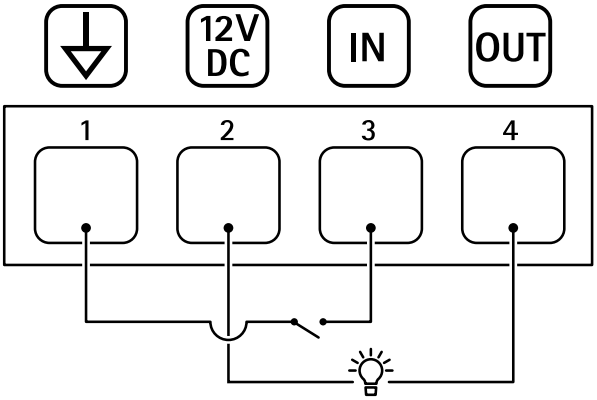
4-pin terminal block



Function	Pin	Notes	Specifications
DC ground	1		0 VDC
DC output	2	Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	12 VDC Max load = 25 mA

Digital Input	3	Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 VDC
Digital Output	4	Internally connected to pin 1 (DC ground) when active, and floating (unconnected) when inactive. If used with an inductive load, e.g., a relay, connect a diode in parallel with the load, to protect against voltage transients.	0 to max 30 VDC, open drain, 100 mA

Example:



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

Clean your device

NOTICE

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

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

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

Troubleshooting

Reset to factory default settings

WARNING

Possibly hazardous optical radiation is emitted from this product. It can be harmful to the eyes. Don't 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 need to reinstall the license key. See .

To reset the product to the factory default settings:

1. Disconnect power from the product.
2. Press and hold the control button while reconnecting power. See *Product overview, on page 51*.
3. Keep the control button pressed for 15–30 seconds until the status LED indicator flashes amber.
4. Release the control button. The process is complete when the status LED indicator turns green. If no DHCP server is available on the network, the device IP address will default to one of the following:
   - **Devices with AXIS OS 12.0 and later:** Obtained from the link-local address subnet (169.254.0.0/16)
   - **Devices with AXIS OS 11.11 and earlier:** 192.168.0.90/24
5. Use the installation and management software tools to assign an IP address, set the password, and access the device.
   The installation and management software tools are available from the support pages on *axis.com/support*.

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

AXIS OS options

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

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

Check the current AXIS OS version

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

To check the current AXIS OS version:

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

Upgrade AXIS OS

Important

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

Note

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

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

When the upgrade has finished, the product restarts automatically.

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

Technical problems and possible solutions

Problems upgrading AXIS OS

AXIS OS upgrade failed

If the upgrade fails, the device reloads the previous version. The most common reason is that the wrong AXIS OS file has been uploaded. Check that the name of the AXIS OS file corresponds to your device and try again.

Problems after AXIS OS upgrade

If you experience problems after the upgrade, roll back to the previously installed version from the **Maintenance** page.

Problems setting the IP address

Can't set the IP address

- If the IP address intended for the device and the IP address of the computer used to access the device are located on different subnets, you can't set the IP address. Contact your network administrator to obtain an IP address.
- The IP address could be in use by another device. To check:
  1. Disconnect the Axis device from the network.
  2. In a Command/DOS window, type `ping` and the IP address of the device.
  3. If you receive: `Reply from <IP address>: bytes=32; time=10...` this means that the IP address might already be in use by another device on the network. Obtain a new IP address from the network administrator and reinstall the device.
  4. If you receive: `Request timed out`, this means that the IP address is available for use with the Axis device. Check all cabling and reinstall the device.
- There could be a possible IP address conflict with another device on the same subnet. The static IP address in the Axis device is used before the DHCP server sets a dynamic address. This means that if the same default static IP address is also used by another device, there could be problems accessing the device.

Problems accessing the device

Can't log in when accessing the device from a browser

When HTTPS is enabled, make sure that you use the correct protocol (HTTP or HTTPS) when you try to log in. You might need to manually type `http` or `https` in the browser's address field.

If you've lost the password for the root account, you must reset the device to the factory default settings. For instructions, see *Reset to factory default settings, on page 55*.

The IP address has been changed by DHCP

IP addresses obtained from a DHCP server are dynamic and could change. If the IP address has been changed, use AXIS IP Utility or AXIS Device Manager to locate the device on the network. Identify the device using its model or serial number, or by the DNS name (if the name has been configured).

If required, you can assign a static IP address manually. For instructions, go to *axis.com/support*.

Certificate error when using IEEE 802.1X

For authentication to work properly, the date and time settings in the Axis device must be synchronized with an NTP server. Go to **System > Date and time**.

The browser isn't supported

For a list of recommended browsers, see *Browser support, on page 4*.

Can't access the device externally

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

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

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

Problems with streaming

Multicast H.264 only accessible by local clients

Check if your router supports multicasting, or if you need to configure the router settings between the client and the device. You might need to increase the TTL (Time To Live) value.

No multicast H.264 displayed in the client

Check with your network administrator that the multicast addresses used by the Axis device are valid for your network.

Check with your network administrator to see if there is a firewall that prevents viewing.

Poor rendering of H.264 images

Ensure that your graphics card uses the latest driver. You can usually download the latest drivers from the manufacturer's website.

Color saturation is different in H.264 and Motion JPEG

Modify the settings for your graphics adapter. Check the adapter's documentation for more information.

Lower frame rate than expected

- See *Performance considerations, on page 59*.
- Reduce the number of applications running on the client computer.
- Limit the number of simultaneous viewers.
- Check with the network administrator that there is enough bandwidth available.
- Lower the image resolution.
- Log in to the device's web interface and set a capture mode that prioritizes frame rate. If you change the capture mode to prioritize frame rate it might lower the maximum resolution, depending on the device used and capture modes available.

Can't select H.265 encoding in live view

Web browsers don't support H.265 decoding. Use a video management system or application that supports H.265 decoding.

Problems with MQTT

Can't connect over port 8883 with MQTT over SSL

The firewall blocks traffic that uses port 8883 since it's regarded insecure.

In some cases the server/broker might not provide a specific port for MQTT communication. It might still be possible to use MQTT over a port normally used for HTTP/HTTPS traffic.

- If the server/broker supports WebSocket/WebSocket Secure (WS/WSS), typically on port 443, use this protocol instead. Check with the server/broker provider to see if WS/WSS is supported and which port and basepath to use.
- If the server/broker supports ALPN, the use of MQTT can be negotiated over an open port, such as 443. Check with your server/broker provider to see if ALPN is supported and which ALPN protocol and port to use.

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

Performance considerations

When you set up your system, it's important to consider how different settings and situations affect performance. Some factors affect bandwidth (bitrate), others affect frame rate, and some affect both.

The most important factors to consider:

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

Contact support

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

Cybersecurity

Cybersecurity supports a successful product lifecycle with minimized risks. You can find in-depth information and documentation about our cybersecurity approach at *axis.com/about-axis/cybersecurity*. Follow the cybersecurity guidelines below to receive product security notifications from Axis and to configure your product for a secure lifecycle and decommissioning.

At *Axis Trust Center*, you can find information about how Axis implements security compliance, transparency, data protection, and privacy.

Vulnerability management

Axis is a *Common Vulnerability and Exposures (CVE) Numbering Authority (CNA)*. To minimize your risk of exposure, we follow industry standards when identifying and resolving vulnerabilities in our devices, software, and services. Refer to *axis.com/vulnerability-management* for information about our vulnerability management policy or to report a vulnerability.

Security notifications

Subscribe to Axis security notification emails at *axis.com/security-notification-service*. We will send you information about vulnerabilities, corresponding security advisories, and other security-related matters for your Axis product.

Secure product lifecycle

Axis minimizes risks throughout the lifetime of our products through secure lifecycle management. Use our hardening guides at *help.axis.com* to more securely configure and operate your Axis products and to find information about:

Secure first-use – Axis products are pre-configured with high default protection to allow for secure initialization and encrypted communication from the very start.

Intended use and common configuration mistakes – Our guides provide information about the intended usage of Axis products, including common security-relevant misuse and configuration mistakes that should be avoided.

Managing vulnerabilities and supply chain transparency – A Software Bill of Material (SBOM) is published with every software release on *axis.com* to disclose vulnerabilities and improve supply chain transparency.

Decommissioning and the secure erasure of data – To securely decommission a product when it reaches the end of its lifecycle, reset it to factory default settings. This erases your configurations, stored data, and sensitive information.

T10243447

2026-07 (M1.6)

© 2026 Axis Communications AB