

AXIS P1385-E Box Camera

Table of Contents

Get started.....	4
Find the device on the network.....	4
Browser support.....	4
Open the device's web interface.....	4
Create an administrator account.....	4
Secure passwords.....	5
Make sure that no one has tampered with the device software	5
Web interface overview	5
Configure your device.....	6
Basic settings	6
Replace the lens.....	6
Adjust the image.....	6
Level the camera	6
Select scene profile.....	7
Reduce image processing time with low latency mode.....	7
Select exposure mode	7
Benefit from IR light in low-light conditions by using night mode	7
Reduce noise in low-light conditions.....	7
Reduce motion blur in low-light conditions.....	8
Maximize the details in an image.....	8
Handle scenes with strong backlight.....	8
Stabilize a shaky image with image stabilization.....	9
Compensate for barrel distortion.....	9
Monitor long and narrow areas.....	9
Verify the pixel resolution.....	10
Hide parts of the image with privacy masks.....	10
Show an image overlay	11
Show a text overlay.....	11
Add street names and compass direction to the image.....	11
View and record video	11
Reduce bandwidth and storage	11
Set up network storage	12
Record and watch video	12
Verify that no one has tampered with the video.....	12
Set up rules for events.....	13
Trigger an action	13
Record video when the camera detects an object.....	13
Show a text overlay in the video stream when the device detects an object	14
Provide visual indication of an ongoing event.....	14
Record video when the camera detects loud noises	15
Record video when the camera detects impact	15
Detect tampering with input signal	16
Trigger a notification when the camera lens is tampered	16
Set up the intrusion alarm	17
Audio.....	18
Add audio to your recording	18
Connect to a network speaker.....	18
The web interface	19
Learn more.....	20
View area	20
Capture modes.....	20
Remote focus and zoom.....	21
Privacy masks	21

Overlays	21
Streaming and storage.....	21
Video compression formats.....	21
How do Image, Stream, and Stream profile settings relate to each other?.....	22
Bitrate control.....	22
Analytics and apps	24
AXIS People Counter	24
AXIS Scream Detection.....	24
AXIS Blocked View Detection	25
AXIS Object Analytics.....	25
AXIS Image Health Analytics.....	25
Metadata visualization.....	26
AXIS Face Detector	26
Cybersecurity.....	26
Axis Edge Vault	26
Signed OS.....	26
Secure boot	26
Signed video	27
Axis security notification service	27
Vulnerability management.....	27
Secure operation of Axis devices	27
Specifications.....	28
Product overview	28
LED indicators.....	
SD card slot.....	
Buttons.....	
Control button	
Intrusion alarm switch	
Connectors.....	
Network connector	
Audio connector.....	
I/O connector.....	
Power connector	
RS485/RS422 connector.....	
T92G20 connector	
PTZ drivers	
ATP.....	
Pelco	
Visca.....	
Clean your device.....	
Troubleshooting.....	
Reset to factory default settings	
AXIS OS options.....	
Check the current AXIS OS version	
Upgrade AXIS OS.....	
Technical problems and possible solutions	
Performance considerations	
Contact support.....	

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 5*.

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* .
After the reset, secure boot guarantees the state of the device.
2. Configure and install the device.

Web interface overview

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



Axis device web interface

Configure your device

Basic settings

Set the capture mode

1. Go to **Video > Installation > Capture mode**.
2. Click **Change**.
3. Select a capture mode and click **Save and restart**.
See also *Capture modes, on page 20*.

Set the power line frequency

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

Set the orientation

1. Go to **Video > Installation > Rotate**.
2. Select **0**, **90**, **180** or **270** degrees.
See also *Monitor long and narrow areas, on page 9*.

Replace the lens

1. Stop all recordings and disconnect power from the device.
2. Disconnect the lens cable and remove the standard lens.
3. Attach the new lens and connect the lens cable.
4. Reconnect the power.
5. Log in to the device's web interface and go to **Video > Image > Exposure**.
6. Select the **P-Iris** lens you have installed.

Note

If you use a DC iris, manual iris or optional i-CS lens there is no need to select a lens driver.

7. For the changes to take effect, you need to restart the device. Go to **Maintenance** and click **Restart**.
8. Adjust the zoom and focus.

Note

For a lens with P-Iris, DC-iris, or manual iris, manually adjust the focus on the lens before you fine-tune the focus through the web interface.

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 20*.

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.

Select scene profile

A scene profile is a set of predefined image appearance settings including color level, brightness, sharpness, contrast and local contrast. Scene profiles are preconfigured in the product for quick setup to a specific scenario, for example **Forensic** which is optimized for surveillance conditions. For a description of each available setting, see *The web interface, on page 19*.

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

1. Go to **Video > Image > Appearance**.
2. Go to **Scene profile** and select a profile.

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**.

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.

Note

If you use a lens with a larger aperture, the depth of field gets shallower.

- Change to a lens with a larger aperture.

Maximize the details in an image

Important

If you maximize the details in an image, the bitrate will probably increase and you might get a reduced frame rate.

- Make sure to select the capture mode that has the highest resolution.
- Go to **Video > Stream > General** and set the compression as low as possible.
- Below the live view image, click  and in **Video format**, select **MJPEG**.
- Go to **Video > Stream > Zipstream** and select **Off**.

Handle scenes with strong backlight

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



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/web-articles/wdr.

Stabilize a shaky image with image stabilization

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

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

Note

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

1. Go to **Video > Installation > Image correction**.
2. Turn on **Image stabilization**.

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.

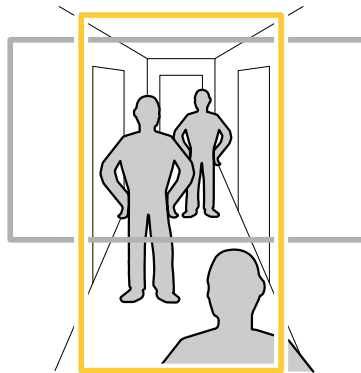
Note

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

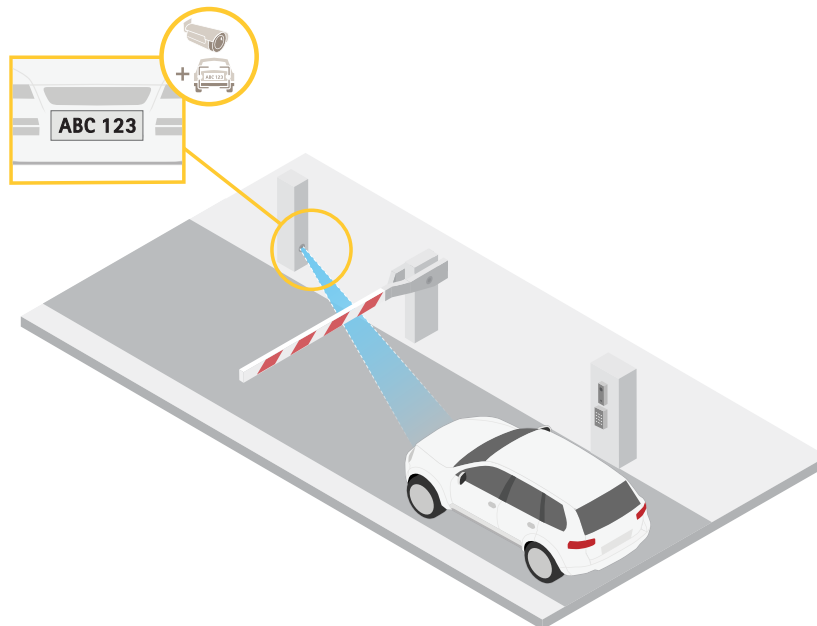
Use corridor format to better utilize the full field of view in a long and narrow area, for example a staircase, hallway, road, or tunnel.



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 21*

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.

Add street names and compass direction to the image

Note

The street name and compass direction will be visible on all video streams and recordings.

1. Go to **Apps**.
2. Select **axis-orientationaid**.
3. Click **Open**.
4. To add a street name, click **Add text** and modify the text to fit the street.
5. To add a compass, click **Add compass** and modify the compass to fit 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 21*.

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 12*

3. To stop recording, click  again.

Watch video

1. Go to **Recordings**.
2. Click  for your recording in the list.

Verify that no one has tampered with the video

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

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

2. Use AXIS Camera Station (5.46 or later) or another compatible video management software to record video. For instructions, see the *AXIS Camera Station user manual*.
3. Export the recorded video.
4. Use AXIS File Player to play the video. *Download AXIS File Player*.



indicates that no one has tampered with the video.

Note

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

Set up rules for events

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

To learn more, 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.

Note

- If you make changes to an active rule, the rule must be turned on again for the changes to take effect.
- If you change the definition of a stream profile that is used in a rule, you need to restart all the rules that use that stream profile.

Record video when the camera detects an object

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

Before you start:

- Make sure you have an SD card installed.

Make sure that AXIS Object Analytics is running:

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

Create a rule:

1. Go to **System > Events** and add a rule.
2. Type a name for the rule.
3. In the list of conditions, under **Application**, select **Object Analytics**.
4. In the list of actions, under **Recordings**, select **Record video while the rule is active**.
5. In the list of storage options, select **SD_DISK**.
6. Select a camera and a stream profile.
7. Set the prebuffer time to 5 seconds.
8. Set the postbuffer time to 1 minute.

9. Click **Save**.

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

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

Make sure that AXIS Object Analytics is running:

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

Add the overlay text:

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

Create a rule:

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

Note

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

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

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. For the port that you connected the AXIS I/O Indication LED to, click  to set the direction to **Output**, and click  to 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.

Record video when the camera detects loud noises

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

Note

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

Turn on audio:

1. Set up the stream profile to include audio, see *Add audio to your recording, on page 18*.

Turn on audio detection:

1. Go to **System > Detectors > Audio detection**.
2. Adjust the sound level according to your needs.

Create a rule:

1. Go to **System > Events** and add a rule.
2. Type a name for the rule.
3. In the list of conditions, under **Audio**, select **Audio Detection**.
4. In the list of actions, under **Recordings**, select **Record video**.
5. In the list of storage options, select **SD_DISK**.
6. Select the stream profile where audio has been turned on.
7. Set the prebuffer time to 5 seconds.
8. Set the postbuffer time to 2 minutes.
9. Click **Save**.

Record video when the camera detects impact

Shock detection allows the camera to detect tampering caused by vibrations or shock. Vibrations due to the environment or to an object can trigger an action depending on the shock sensitivity range, which can be set from 0 to 100. In this scenario, someone is throwing rocks at the camera after hours and you would like to get a video clip of the event.

Turn on shock detection:

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

2. Turn on shock detection, and adjust the shock sensitivity.

Create a rule:

3. Go to **System > Events > Rules** and add a rule.
4. Type a name for the rule.
5. In the list of conditions, under **Device status**, select **Shock detected**.
6. Click **+** to add a second condition.
7. In the list of conditions, under **Scheduled and recurring**, select **Schedule**.
8. In the list of schedules, select **After hours**.
9. In the list of actions, under **Recordings**, select **Record video while the rule is active**.
10. Select where to save the recordings.
11. Select a **Camera**.
12. Set the prebuffer time to 5 seconds.
13. Set the postbuffer time to 50 seconds.
14. Click **Save**.

Detect tampering with input signal

This example explains how to send an email when the input signal is cut or short-circuited. For more information about the I/O connector, see *page* .

1. Go to **System > Accessories > I/O ports** and turn on **Supervised** for the relevant port.

Add an email recipient:

1. Go to **System > Events > Recipients** and add a recipient.
2. Type a name for the recipient.
3. Select **Email** 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:

1. Go to **System > Events > Rules** and add a rule.
2. Type a name for the rule.
3. In the list of conditions, under **I/O**, select **Supervised input tampering is active**.
4. Select the relevant port.
5. In the list of actions, under **Notifications**, select **Send notification to email** and then select the recipient from the list.
6. Type a subject line and message for the email.
7. 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**.

Set up the intrusion alarm

Use the intrusion alarm switch to, for example, send a notification if someone opens the camera housing.

Before you start

- Connect the intrusion alarm switch to pin 1 (ground) and pin 3 (digital I/O) of the camera's I/O connector.

Configure the input port:

1. Go to **System > Accessories > I/O ports**.
2. For **Port 1**:
 - 2.1. Select **Input**.
 - 2.2. Select **Circuit closed**.

Add an email recipient:

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

Create a rule:

11. Go to **System > Events > Rules** and add a rule.
12. Type a name for the rule.
13. In the list of conditions, under **I/O**, select **Digital input**.
14. In the list of ports, select **Port 1**.
15. In the list of actions, under **Notifications**, select **Send notification to email**.
16. Select a recipient from the list or go to **Recipients** to create a new recipient.
To create a new recipient, click . To copy an existing recipient, click .
17. Type a subject line and message for the email.
18. Click **Save**.

Audio

Add audio to your recording

Turn on audio:

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

Edit the stream profile that is used for the recording:

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

Connect to a network speaker

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

Important

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

Pair camera with network speaker

1. Go to **System > Edge-to-edge > Pairing**.
2. Click  **Add** and select the pairing type **Audio** from the drop-down list.
3. Select **Speaker pairing**.
4. Type the network speaker's IP address, username and password.
5. Click **Connect**. A confirmation message appears.

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

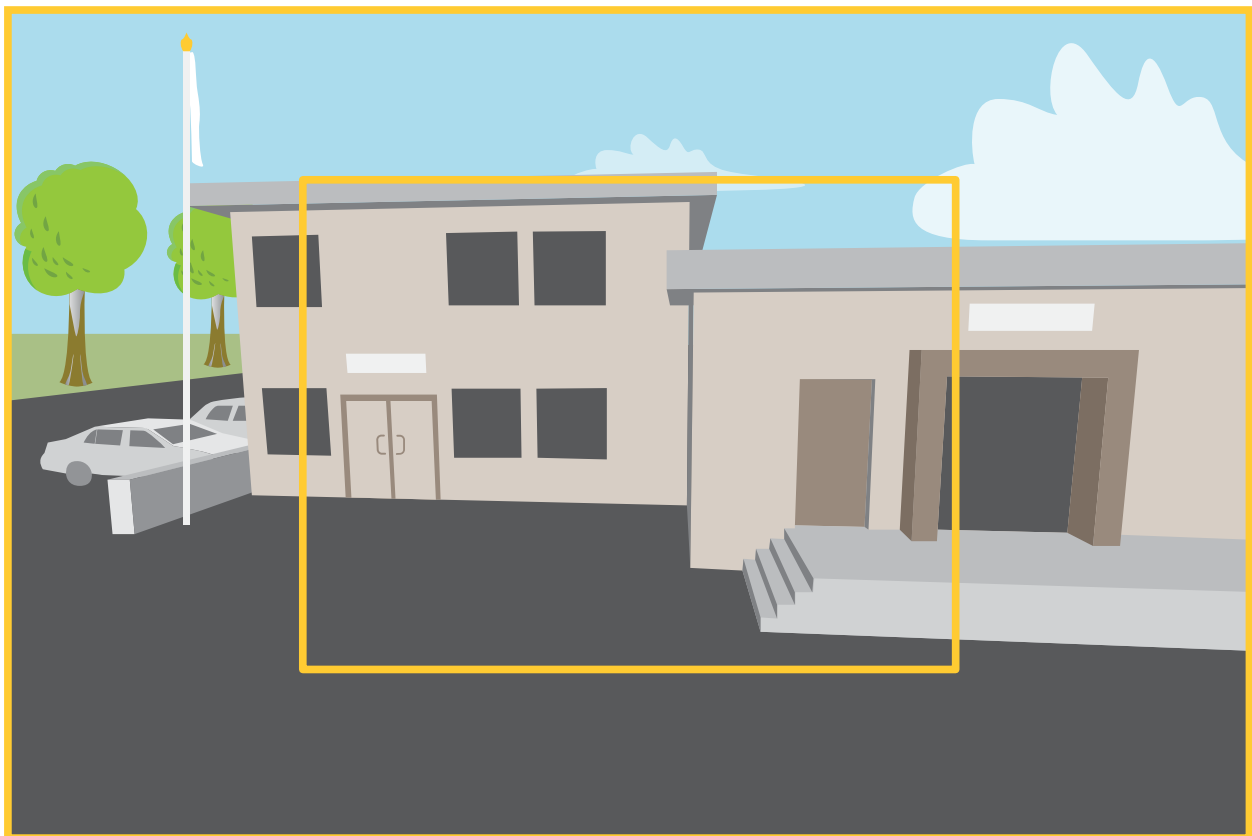
When you set up a view area, we recommend you to set the video stream resolution to the same size as or smaller than the view area size. If you set the video stream resolution larger than the view area size it implies digitally scaled up video after sensor capture, which requires more bandwidth without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

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

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

Streaming and storage

Video compression formats

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

Motion JPEG

Note

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

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

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

H.264 or MPEG-4 Part 10/AVC

Note

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

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

H.265 or MPEG-H Part 2/HEVC

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

Note

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

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

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

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

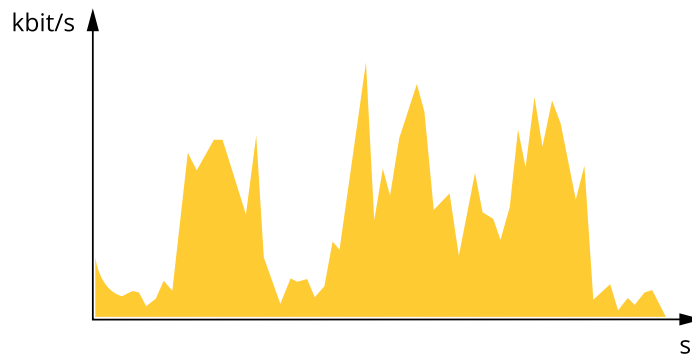
The **Stream profiles** settings override the settings from the **Stream** tab. If you request a stream with a specific stream profile, the stream contains the settings of that profile. If you request a stream without specifying a stream profile, or request a stream profile that doesn't exist in the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

Bitrate control

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

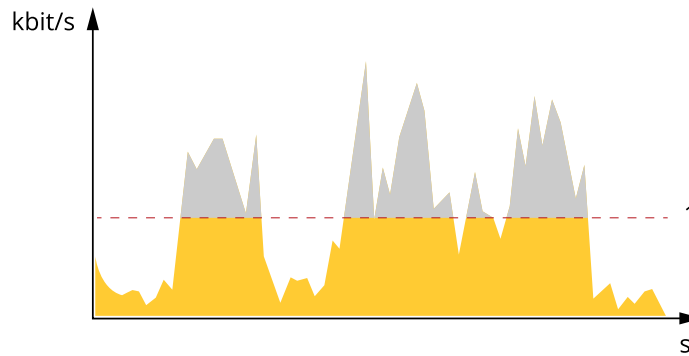
Variable bitrate (VBR)

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



Maximum bitrate (MBR)

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

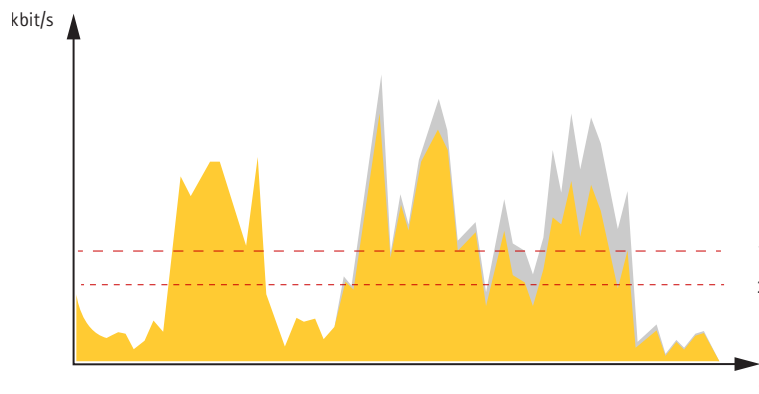


1 Target bitrate

Average bitrate (ABR)

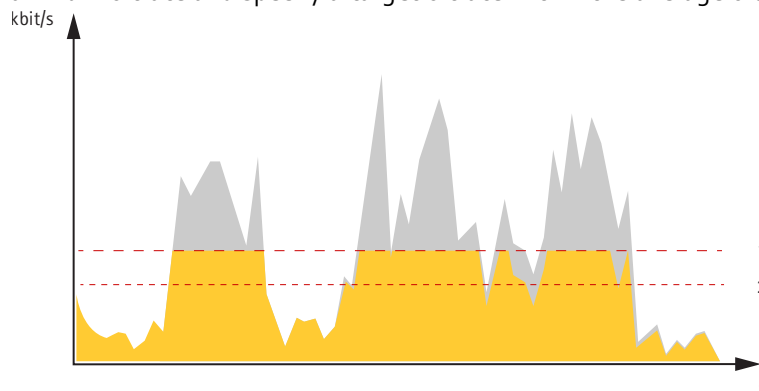
With average bitrate, the bitrate is automatically adjusted over a longer period of time. This is so you can meet the specified target and provide the best video quality based on your available storage. Bitrate is higher in scenes with a lot of activity, compared to static scenes. You are more likely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

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



1 Target bitrate
2 Actual average bitrate

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



1 Target bitrate
2 Actual average bitrate

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.

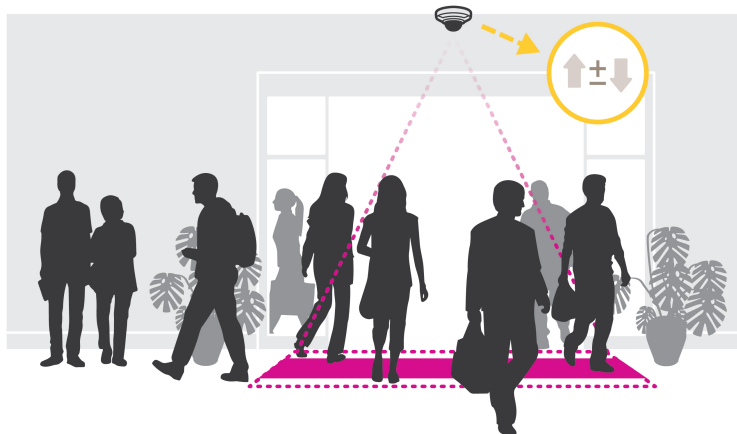
Note

- 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 People Counter

AXIS People Counter is an analytic application that you can install on a network camera. You can use the application to count how many people pass through an entrance, in what direction they pass, and if more than one person passes during a predefined interval. You can also use it to estimate how many people are currently occupying an area, and the average visiting time.

The application runs embedded in the camera which means you don't need a dedicated computer to run the application. AXIS People Counter is suitable for any indoor environment, like stores, libraries, or gyms.



How does estimating occupancy work?

You can use the application to estimate occupancy in areas with one or several entrances and exits. Each entrance and exit needs to be equipped with a network camera with AXIS People Counter installed. If there are several cameras, they communicate with each other over the network in a primary and secondary concept. The primary camera continuously fetches data from the secondary cameras and presents the data in the live view. Every fifteen minutes, the primary camera sends the statistical data to AXIS Store Data Manager. Consequently, the reports generated from AXIS Store Data Manager can present the data in a minimum of 15 minutes time interval.

AXIS Scream Detection

AXIS Scream Detection is an application that triggers an event if a scream is detected. The generated event can be used, for example, to record a video or alert security staff.

Before using the application, consider the following:

- The application is mainly intended for detecting screams in a generally quiet environment. The difference between the background sound level and the scream must be at least 15-20 dB for the application to function effectively. Consider the proximity to the expected sound source, the background noise level and the audio input gain level when installing the product.
- Adjust the audio input gain to a level where the background noise covers approximately 30-50% of the application's audio level graph. To access the **Input gain** setting, click the **Audio Settings** link on the application page.

- If the interval between screams is less than 3 seconds, the application regards it as one scream.

AXIS Blocked View Detection

AXIS Blocked View Detection is an application that triggers an alarm if tampering of the camera is detected, for example, if the lens is covered or sprayed.

For optimal performance, we recommend that the camera view contains objects, patterns or lines that can be detected.



Ideal scene

Avoid large areas of floor, walls and ceiling with few objects.



Not ideal scene

You can set the trigger level by adjusting the sensitivity and change ratio of the tampering detection.

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*.

AXIS Face Detector

AXIS Face Detector is an application that detects faces in a predefined area of the live video. The detected faces are marked within boxes.



To find out more about the application, see axis.com/products/axis-face-detector

Cybersecurity

For product-specific information about cybersecurity, see the product's datasheet at axis.com.

For in-depth information about cybersecurity in AXIS OS, read the *AXIS OS Hardening guide*.

Axis Edge Vault

Axis Edge Vault provides a hardware-based cybersecurity platform that safeguards the Axis device. It offers features to guarantee the device's identity and integrity and to protect your sensitive information from unauthorized access. It builds on a strong foundation of cryptographic computing modules (secure element and TPM) and SoC security (TEE and secure boot), combined with expertise in edge device security.

Signed OS

Signed OS is implemented by the software vendor signing the AXIS OS image with a private key. When the signature is attached to the operating system, the device will validate the software before installing it. If the device detects that the integrity of the software is compromised, the AXIS OS upgrade will be rejected.

Secure boot

Secure boot is a boot process that consists of an unbroken chain of cryptographically validated software, starting in immutable memory (boot ROM). Being based on the use of signed OS, secure boot ensures that a device can boot only with authorized software.

Signed video

Signed video ensures that video evidence can be verified as untampered without proving the chain of custody of the video file. Each camera uses its unique video signing key, which is securely stored in the secure keystore, to add a signature into the video stream. When the video is played, the file player shows whether the video is intact. Signed video makes it possible to trace the video back to the camera origin and verifies that the video has not been tampered with after it left the camera.

To learn more about the cybersecurity features in Axis devices, go to axis.com/learning/white-papers and search for cybersecurity.

Axis security notification service

Axis provides a notification service with information about vulnerability and other security related matters for Axis devices. To receive notifications, you can subscribe at axis.com/security-notification-service.

Vulnerability management

To minimize customers' risk of exposure, Axis, as a **Common Vulnerability and Exposures (CVE) numbering authority (CNA)**, follows industry standards to manage and respond to discovered vulnerabilities in our devices, software, and services. For more information about Axis vulnerability management policy, how to report vulnerabilities, already disclosed vulnerabilities, and corresponding security advisories, see axis.com/vulnerability-management.

Secure operation of Axis devices

Axis devices with factory default settings are pre-configured with secure default protection mechanisms. We recommend using more security configuration when installing the device. To learn more about Axis' approach to cybersecurity, including best practices, resources, and guidelines for securing your devices, go to axis.com/about-axis/cybersecurity.

