

AXIS Q1656-DLE Radar-Video Fusion Camera

Table of Contents

Solution overview	5
.....	5
Why fusion?	5
Radar-video fusion explained	5
Installation	7
Preview mode	7
Installation guide	7
Considerations.....	7
Where to install the product.....	7
Radar coverage	9
Radar-video fusion coverage.....	11
Area installation	13
Area installation examples.....	13
Area monitoring use cases.....	13
Road installation.....	16
Road installation examples.....	16
Road monitoring use cases	18
Get started.....	20
Find the device on the network.....	20
Browser support	20
Open the device's web interface.....	20
Create an administrator account.....	20
Secure passwords.....	21
Make sure that no one has tampered with the device software	21
Web interface overview	21
Configure your device.....	22
Basic settings	22
Adjust the image.....	22
Select exposure mode	22
Optimize IR illumination.....	22
Benefit from IR light in low-light conditions by using night mode	22
Reduce noise in low-light conditions.....	23
Reduce motion blur in low-light conditions.....	23
Maximize the details in an image.....	23
Handle scenes with strong backlight.....	23
Stabilize a shaky image with image stabilization.....	24
Hide parts of the image with privacy masks.....	24
Show an image overlay	25
Show the radar live view in the image	25
Add street names and compass direction to the image.....	25
Record and watch video	25
View and record video	26
Reduce bandwidth and storage	26
Set up network storage	26
Configure the radar	26
Select a radar profile.....	27
Set the mounting height	27
Validate the mounting height	27
Calibrate a reference map.....	27
Set detection zones	28
Autocalibrate the device.....	30
Show a text overlay with the tilt angle of the radar.....	30
Configure AXIS Object Analytics	31

Create a scenario.....	31
Use speed to trigger.....	32
Select detection sensitivity.....	32
Minimize false alarms.....	32
Set up rules for events.....	33
Save power when no motion is detected	33
Trigger a notification when the enclosure is opened.....	34
Send an email if someone covers the radar with a metallic object.....	34
Control a PTZ camera with the radar.....	35
Use MQTT to send radar data	36
Record video when the camera detects an object.....	37
Provide visual indication of an ongoing event.....	37
Show a text overlay in the video stream when the device detects an object.....	38
Record video when a PIR detector senses motion	39
Record video when the camera detects loud noises	39
Detect tampering with input signal	40
Audio.....	41
Add audio to your recording	41
The web interface	42
Status.....	42
Video	44
Installation	45
Image.....	48
Stream	54
Overlays	57
Privacy masks.....	59
Radar.....	59
Settings.....	59
Stream	60
Map calibration.....	62
Exclude zones	63
Scenarios.....	64
Overlays	65
Radar PTZ autotracking	67
Autocalibration	67
Analytics.....	68
AXIS Object Analytics.....	68
AXIS Image Health Analytics.....	68
Metadata visualization.....	69
Metadata configuration	69
Audio.....	70
Device settings.....	70
Stream	70
Audio clips.....	70
Audio enhancement.....	71
Recordings	71
Apps	72
System	72
Time and location	72
Network	74
Security.....	78
Accounts	83
Events	85
MQTT	89
Storage	93
Stream profiles.....	95

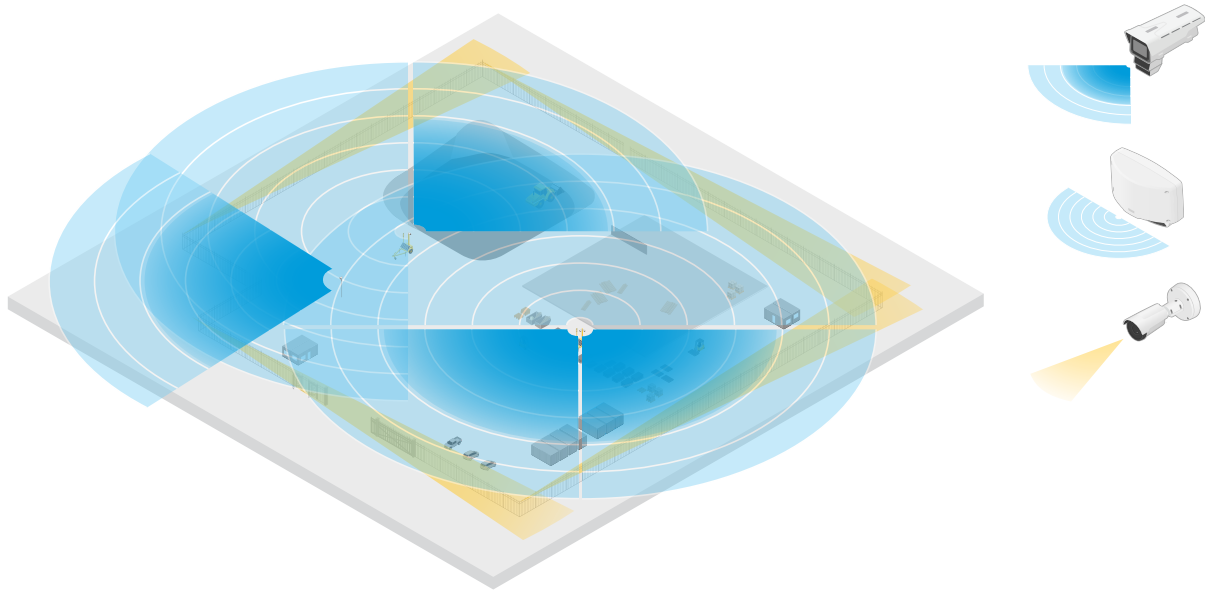
ONVIF.....	96
Detectors.....	99
Accessories.....	99
Edge-to-edge.....	100
Logs.....	102
Plain config.....	103
Maintenance	104
Maintenance.....	104
Troubleshoot.....	105
Learn more.....	106
Long-distance connections.....	106
Capture modes.....	106
Remote focus and zoom.....	107
Privacy masks	107
Overlays.....	107
Streaming and storage.....	108
Video compression formats.....	108
How do Image, Stream, and Stream profile settings relate to each other?.....	108
Bitrate control.....	108
Applications	110
AXIS Object Analytics.....	110
AXIS Image Health Analytics.....	110
Metadata visualization.....	111
Cybersecurity.....	111
Signed OS.....	111
Secure boot	111
Axis Edge Vault	111
TPM module.....	111
Axis device ID.....	111
Signed video	111
Specifications.....	112
Product overview	112
LED indicators.....	113
Buzzer.....	113
Buzzer signal for focus assistant	113
SD card slot.....	113
Buttons.....	113
Control button	113
Intrusion alarm switch	114
Connectors.....	114
Network connector	114
Audio connector.....	114
I/O connector	114
Power connector	115
RS485/RS422 connector.....	116
Troubleshooting.....	117
Reset to factory default settings	117
AXIS OS options.....	117
Check the current AXIS OS version	117
Upgrade AXIS OS.....	118
Technical issues, clues, and solutions.....	118
Performance considerations	120
Contact support.....	120

Solution overview

A radar-video fusion camera is a visual camera with a fully integrated radar module. As such it can use radar and video – separately or combined – to detect and classify objects.

The benefits of radar-video fusion are more accurate detections and classifications, and less false and missed alarms. The fusion of the two technologies comes together in AXIS Object Analytics, which is the main interface used to access and configure the radar-video fusion.

AXIS Q1656-DLE detects and classifies objects in wide areas with depth, and you can use it for area monitoring or road monitoring. Additionally, AXIS Q1656-DLE works well in a site design combined with other devices. Since the detection range of the radar is larger than the field of view of the camera in AXIS Q1656-DLE, combine it with PTZ cameras with IR illumination to achieve visual confirmation in the entire detection range of the radar. Or combine it with thermal cameras, which can detect and classify objects in long and narrow areas.



An example of a construction site with two stand-alone radars that cover the open areas of the site and four radar-video fusion cameras that cover the more complex open areas. Additionally, four thermal cameras cover the narrow corridors along the fence.

Why fusion?

Used on their own, video and radar both have their own strengths and limitations:

- The video typically provides more accurate classifications when there is sufficient contrast and when the object is moving close to the camera. It will also provide more granular classifications than the radar. However, a camera needs good lighting conditions to see.
- The radar on the other hand can detect objects even in challenging lighting conditions, and its detection and classification range is longer. Regardless of the weather conditions, the radar can measure the speed of a moving object, as well as its direction and the distance to it. However, the lack of visual confirmation can make the radar classifications more fragile. Swaying objects and reflective surfaces can trigger false alarms and must be taken into consideration when designing the site and configuring the radar.

The two technologies in the radar-video fusion camera can of course be used on their own but are more powerful when the analytics from both technologies interact to provide more reliable detections and classifications.

Radar-video fusion explained

This product fuses the radar data with the video data in two ways:

- **Visual fusion:** The radar detections and classifications are fused into the video image. This is a way to visualize the radar data in the video stream when the video analytics isn't available.

For example, if an object appears at a distance of 50 m (164 ft), it may be too small for the video analytics to detect, but the radar can identify it. In that case, the radar detection is fused into the image plane and can be used to trigger alarms inside AXIS Object Analytics.

- **Analytics fusion:** The radar detections and classifications are fused with the detections and classifications from the video analytics. This gives the device a combined analytics output where the respective strengths of both technologies are merged. It uses the distance and speed from the radar, and the position and class from the video.

When the object in the example above comes closer, the video analytics also detects it. The radar detection is then fused with the video analytics output to produce an output of higher quality, and with more information, than what the technologies can provide separately.

Installation



Installation video for the device.

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.



This video demonstrates how to use preview mode.

Installation guide

The installation guide and other documents for this product can be found on axis.com/products/axis-q1656-dle/support#support-resources

Considerations

Where to install the product

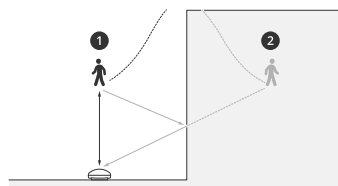
To get the best video and radar coverage, the product must be appropriately mounted. Consider the following when you mount a radar-video fusion camera:

Area or road monitoring

This product is intended for monitoring open areas and you can use it either for area monitoring or road monitoring. For installation examples and use cases, see and .

Avoid solid and reflective objects

Solid and metal objects can affect the performance of the radar in AXIS Q1656-DLE. Most solid objects (such as walls, fences, trees, or large bushes) in the coverage area will create a blind spot (radar shadow) behind them. Metal objects in the field of view cause reflections that affect the ability of the radar to perform classifications. This can lead to ghost tracks and false alarms in the radar stream.



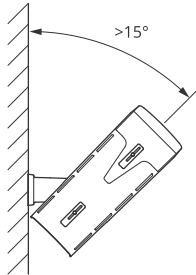
- 1 Actual detection
- 2 Reflected detection (ghost track)

For information about how to handle solid and reflective objects in the coverage area of the radar, see .

Mounting position

Install the product on a stable pole or a spot on a wall where there are no other objects or installations. Objects within 1 m (3 ft) to the left and right of the product, that reflect radio waves, affect the performance of the radar in AXIS Q1656-DLE.

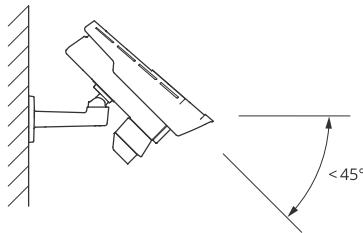
If you install the product on a wall, it needs to point away from the wall at least 15°.



Additionally, the mounting height affects the detection distance and range of both the video and the radar.

Tilt angle

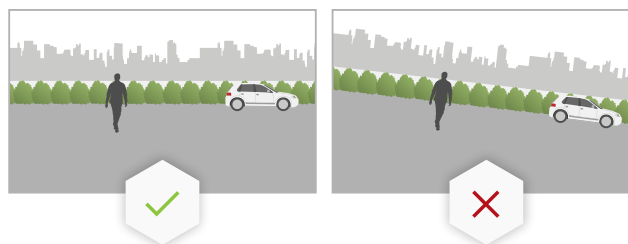
The product must be sufficiently oriented towards the ground so that the center of the image is below the horizon. The recommended mounting tilt is 15–45°.



You can add an overlay in the radar's live view that shows the tilt angle of the product. For instructions, see .

Roll angle

The product's roll angle must be nearly equal to zero, which means that the image should be level with the horizon.



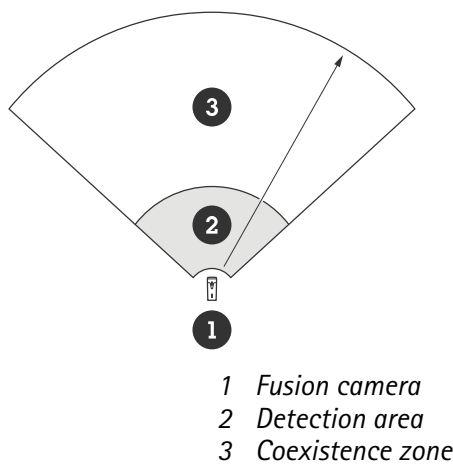
Coexistence

If you mount more than eight radars or radar-video fusion cameras operating on the 60 GHz frequency band close together, they may interfere with each other. To avoid interference, see .

Install multiple Axis radar devices

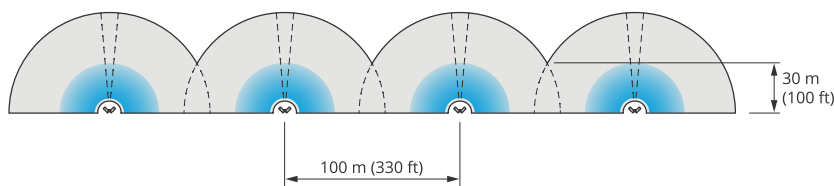
Coexistence

The radio waves of the radar in AXIS Q1656-DLE continue beyond the detection area, and can interfere with other radars up to 350 m (380 yd) away. This is called a coexistence zone.



AXIS Q1656-DLE operates on the 60 GHz frequency band. You can install up to eight Axis radars or radar-video fusion cameras operating on the 60 GHz frequency band close to each other, or facing each other, without causing problems. The built-in coexistence algorithm can find a suitable time slot and frequency channel that will minimize interference.

If an installation contains more than eight radar devices operating on the same frequency band, and many of the devices are pointing away from each other, there is less risk of interference. In general, radar interference will not cause the radar to stop functioning. There is a built-in interference mitigation algorithm that tries to repair the radar signal even when interference is present. A warning about interference is expected to happen in an environment with many radars operating on the same frequency band in the same coexistence zone. The main impact of interference is deterioration of the detection performance, and occasional ghost tracks.



Four pairs of AXIS Q1656-DLE mounted side-by-side.

You can combine the radar-video fusion camera with Axis radars operating on another frequency band without having to think about coexistence. Axis radar devices that are operating on different frequency bands will not interfere with each other.

Radar coverage

The radar in AXIS Q1656-DLE has a horizontal field of detection of 95°. The detection range of the radar depends on factors like the scene, the mounting height and tilt angle of the product, and the size and speed of the moving objects.

The detection range also depends on the **monitoring profile** you select. You can use AXIS Q1656-DLE for area or road monitoring and there are two profiles in the radar that are optimized for each one of the scenarios:

- **Area monitoring profile:** the radar tracks and classifies humans, vehicles and unknown objects moving at speeds lower than 55 km/h (34 mph). For information about detection range, see .
- **Road monitoring profile:** the radar mainly tracks and classifies vehicles moving at speeds up to 200 km/h (125 mph). For information about detection range, see .

Note

When the radar and video is combined in AXIS Object Analytics, AXIS Q1656-DLE can classify vehicle subclasses (buses, cars, bikes, trucks, and other).

Select the area or monitoring profile in the product's web interface. For instructions, see .

Area of coverage

The radar in this device has a horizontal field of detection of 95°. The area of coverage corresponds to 2700 m² (29000 ft²) for humans and 6100 m² (65600 ft²) for vehicles.

Note

Optimal area coverage applies when the product is mounted at 3.5–7 m (11–23 ft). The mounting height will affect the size of the blind spot below the radar.

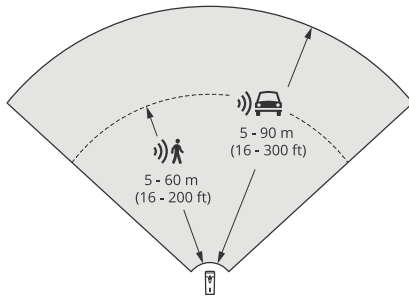
Area detection range

The detection range is the distance within which an object can be tracked and can trigger an alarm. It's measured from a near detection limit (how close to the device a detection can be made) to a far detection limit (how far from the device a detection can be made).

The **area monitoring profile** is optimized for human detection, however, it will also allow you to track vehicles and other objects moving at up to 55 km/h (34 mph) with a speed accuracy of +/- 2 km/h (1.25 mph).

When mounted at the optimal installation height, the detection ranges are:

- 5 – 60 m (16–200 ft) when detecting a human
- 5 – 90 m (16–300 ft) when detecting a vehicle



Note

- Enter the mounting height in the web interface when you calibrate the radar.
- The detection range is affected by the scene and the product's tilt angle.
- The detection range is affected by the moving object type and size.

The radar detection range was measured under these conditions:

- The range was measured along the ground.
- The object was a person with a height of 170 cm (5 ft 7 in).
- The person was walking straight in front of the radar.
- The values were measured when the person entered the detection zone.
- The radar sensitivity was set to **Medium**.

Mounting height	15° tilt	20° tilt	25° tilt	30° tilt	35° tilt	40° tilt	45° tilt
3.5 m (11 ft)	6.0–60+ m (19–196+ ft)	5.0–60+ m (16–196+ ft)	4.0–60+ m (13–196+ ft)	4.0–60 m (13–196 ft)	4.0–55 m (13– 180 ft)	4.0–40 m (13–131 ft)	4.0–30 m (13–98 ft)
4.5 m (14 ft)	6.0–60+ m (19–196+ ft)	6.0–60+ m (19–196+ ft)	5.0–60+ m (16–196+ ft)	4.0–60+ m (13–96+ ft)	4.0–60 m (13–196 ft)	4.0–45 m (13–147 ft)	4.0–40 m (13–131 ft)
6 m (19 ft)	10–60+ m	9.0–60+ m	7.0–60+ m	6.0–60+ m	6.0–60 m (19–196 ft)	5.0–55 m (16–180 ft)	5.0–55 m (16–180 ft)

Mounting height	15° tilt	20° tilt	25° tilt	30° tilt	35° tilt	40° tilt	45° tilt
	(32–196+ ft)	(29–196+ ft)	(22–196+ ft)	(19–196+ ft)			
8 m (26 ft)	16–60 m (52–196 ft)	14–60 m (45–196 ft)	10–60 m (32–196 ft)	8.0–60+ m (26–196+ ft)	8.0–60+ m (26–196+ ft)	7.0–60 m (22–196 ft)	7.0–60 m (22–196 ft)
10 m (32 ft)	21–60 m (68–196 ft)	19–60 m (62–196 ft)	14–60 m (45–196 ft)	12–60+ m (39–196+ ft)	10–60+ m (32–196+ ft)	9.0–60 m (29–196 ft)	9.0–60 m (29–196 ft)
12 m (39 ft)	25–60 m (82–196 ft)	23–60 m (75–196 ft)	19–60 m (62–196 ft)	16–60+ m (52–196+ ft)	13–60+ m (42–196+ ft)	11–60 m (36–196 ft)	11–55 m (36–180 ft)

Note

- Setting the radar sensitivity to **Low** will decrease the detection range by 20% while setting it to **High** will increase the detection range by 20%.
- In installations where you expect small animals to appear outside the fusion zone, but still in the detection zone of the radar, you can minimize the false alarms by setting the radar sensitivity to **Low**. This will however reduce the detection range.

Road detection range

The **road monitoring profile** is optimized for detection of vehicles and provides a speed accuracy of +/- 2 km/h (1.24 mph) when monitoring vehicles moving at up to 200 km/h (125 mph).

The mounting height of the radar-video fusion camera and the vehicle speed will impact the detection range of the radar. When mounted at an optimal installation height, the radar detects approaching and departing vehicles with a speed accuracy of +/- 2 km/h (1.24 mph) within the following ranges:

- 25–100 m (82–328 ft) for vehicles moving at 50 km/h (31 mph).
- 40–80 m (131–262 ft) for vehicles moving at 100 km/h (62 mph).
- 50–70 m (164–230 ft) for vehicles moving at 200 km/h (125 mph).

Note

To minimize the risk of missed detections of vehicles travelling in high speeds, set up a scenario in the radar that triggers on the object types **Vehicle** and **Unknown**. For more information about how to set up a scenario, see .

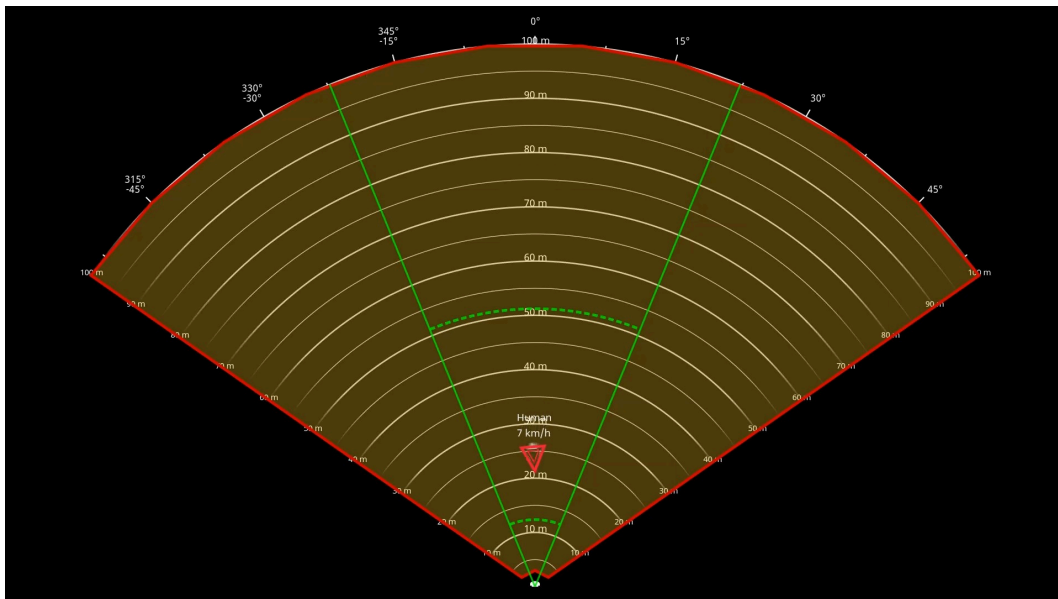
Radar-video fusion coverage

The analytics fusion zone, which is the zone in where an object can be detected and classified by both technologies, depends on factors like:

- The installation height of the camera.
- The tilt angle of the camera.
- The zoom level of the camera lens.
- The lighting conditions of the surrounding environment, and of the light provided by the camera itself and other devices in the site.
- The distance to the moving object.

Once the radar-video fusion camera has been installed, the radar coverage is fixed. The field of view of the camera, however, depends on the zoom level of the lens.

To visualize the camera's field of view in relation to the radar coverage, there are two green lines in the radar stream that represent the approximate field of view of the camera. The lines will adjust when the camera zooms in or out. Additionally, there are two dotted lines that represent the approximate area in which the camera can see. The dotted line closer to the device represent the near detection limit, while the one farther away represents the far detection limit.



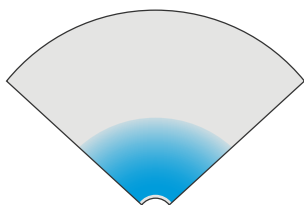
The solid green lines represent the approximate field of view of the camera, while the dotted green lines represent the approximate near and far detection limits.

Zoom level examples

The size of the analytics fusion zone is affected by the zoom level of the lens in AXIS Q1656-DLE. The two extremes of the zoom level are described below.

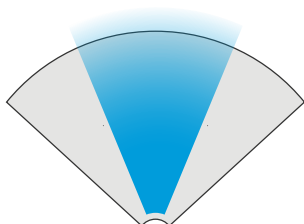
Lens zoomed out (max wide)

When the lens in AXIS Q1656-DLE is zoomed out maximally, objects can get too small to detect for the video analytics. In this scenario, it's likely that objects will be detected by the radar with its wide coverage, but not by the video analytics. If you want to establish visual confirmation in the entire detection range of the radar, you can pair AXIS Q1656-DLE with one or more PTZ cameras.



Lens zoomed in (max tele)

When the lens is zoomed in maximally, it will limit the camera's field of view significantly. However, since objects far away are magnified compared to when the lens is zoomed out maximally, it means the objects can be detected by the video analytics at a much larger distance from the device. In this scenario, it's possible that objects will be detected by the video analytics but not by the radar analytics.



To maximize the chance of accurately classifying an object by both the radar and the video analytics, adjust the zoom – if possible – so that objects in the area of interest are large enough for the video analytics to detect them.

Radar-video detections and classifications

Since AXIS Q1656-DLE can detect and classify objects using radar and video – or just one of the technologies – there are several things to be aware of.

- If two people are walking close together and are detected by the radar, but not the video analytics, they will be classified as one person and only one bounding box will surround them. When they enter the analytics fusion zone and visual confirmation is achieved, they will be accurately classified. The spatial differentiation of the radar in AXIS Q1656-DLE is 3 m (9 ft).
- If an object is outside the camera's field of view, AXIS Q1656-DLE can't fuse any detections or classifications into the image plane. This means that AXIS Object Analytics can't trigger an alarm. To trigger an alarm when an object is detected by the radar only, configure a scenario in the radar's web interface and use conditions to trigger on motion within the radar scenario.
- The exclude zones you add in the radar's web interface are global, which means that any motion detected in these zones will always be ignored – even if the exclude zone overlaps with the analytics fusion zone in AXIS Object Analytics. The exclude zones you add in AXIS Object Analytics, however, will only ignore motion in AXIS Object Analytics scenarios.

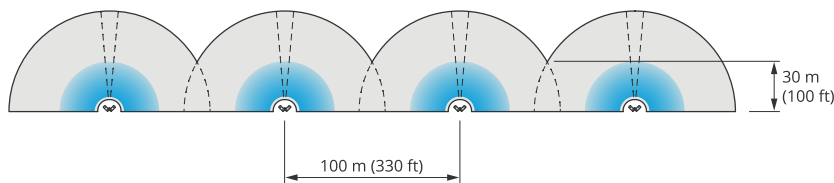
Area installation

To get the best radar performance in area installations, select the **area monitoring profile** in AXIS Q1656-DLE. For more information, see .

Area installation examples

You can place multiple radar-video fusion cameras side-by-side to create a virtual fence, for example along or around a building.

For 180° radar coverage, place two AXIS Q1656-DLE next to each other. When you install more than one pair of radar-video fusion cameras side-by-side, we recommend placing them with 100 m (330 ft) spacing between each pair, as shown in the example.



Four pairs of AXIS Q1656-DLE mounted side-by-side.

You can install up to eight radar-video fusion cameras close together without interference between the radars. For more information about placing Axis radar devices close together, see .

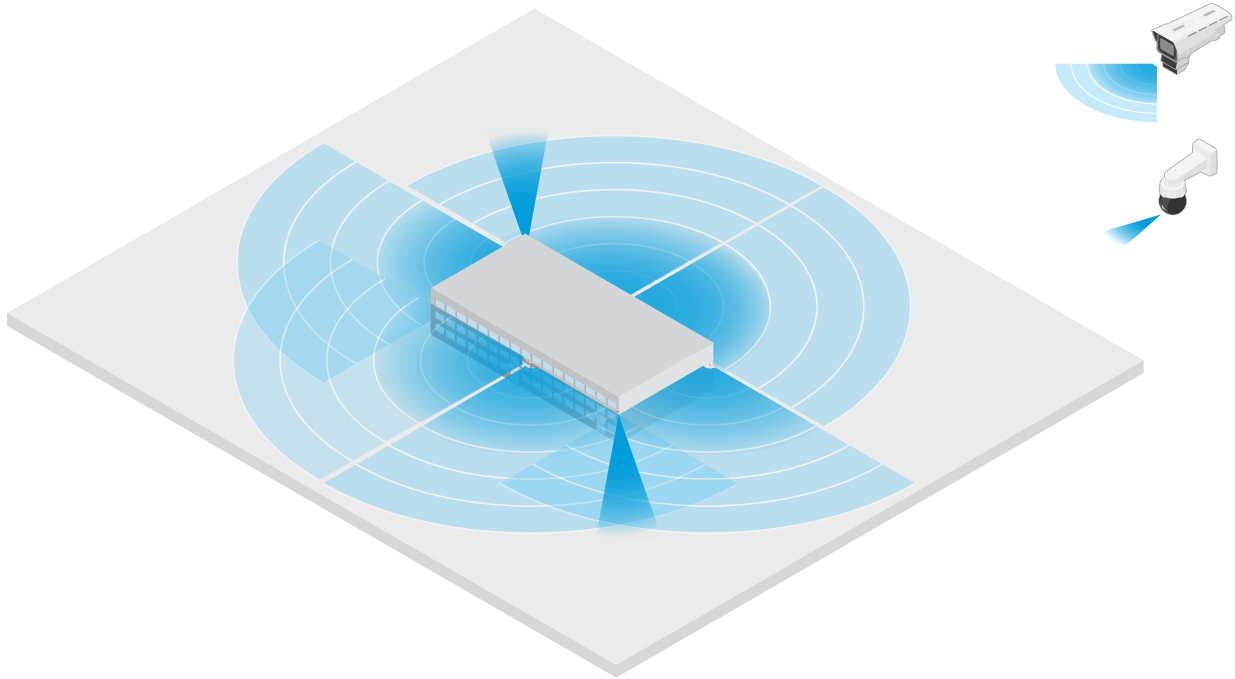
Area monitoring use cases

Cover an open field around a building

A company in an office building needs to secure the premises from intrusion and vandalism, particularly after working hours, on weekends and on public holidays. To cover the area around the building, they install a combination of radar-video fusion cameras and PTZ cameras. They configure the radar-video fusion cameras to trigger an alarm when humans and vehicles approach the building. To get as reliable detections and classifications as possible, they select a detection sensitivity in AXIS Object Analytics suitable for the area. For more information about detection sensitivity, see .

To make sure they get visual confirmation of potential intruders in the entire detection range of the radar, they add two PTZ cameras with built-in IR on the opposite corners of the building. The radars steer the PTZ cameras

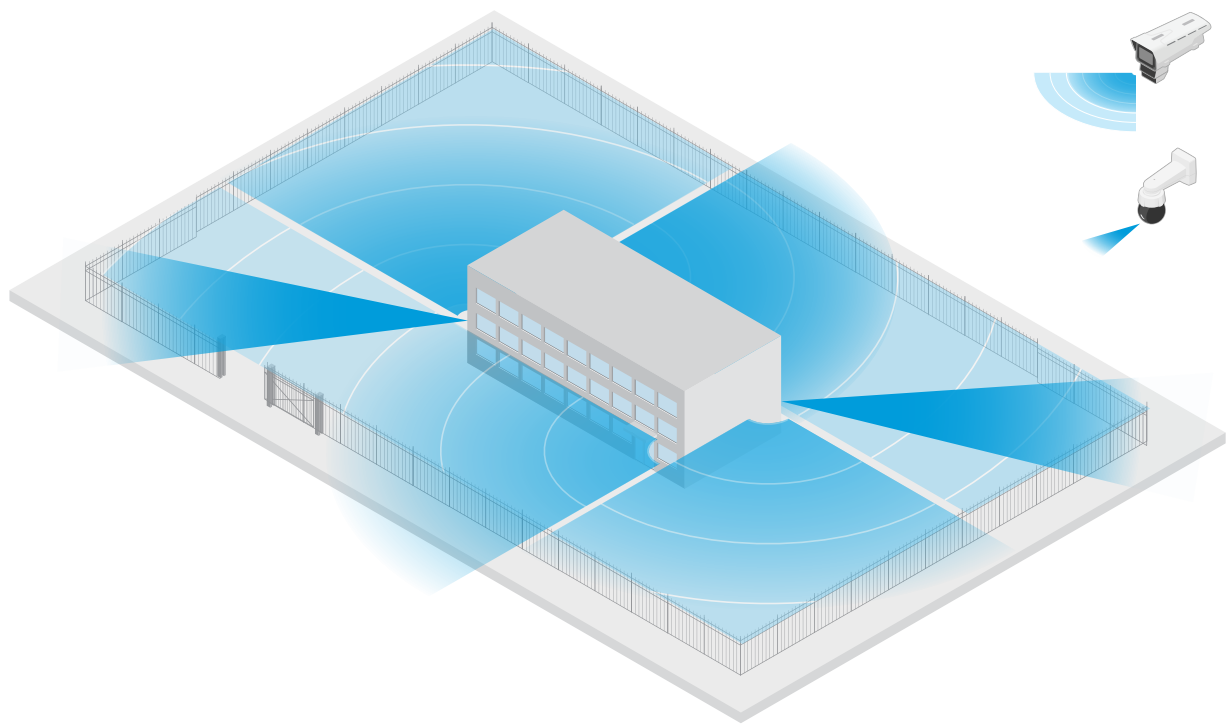
through *AXIS Radar Autotracking for PTZ*, and the built-in IR also provides more light for the radar-video fusion cameras, which makes it possible to detect and identify intruders on a greater distance.



Cover a fenced building

A warehouse that normally keeps goods on the premises is surrounded by a fence to keep intruders away. To detect potential trespassers, they install a combination of radar-video fusion cameras and PTZ cameras with built-in IR to secure the premises. The radar-video fusion cameras provide reliable detections and trigger alarms, while the PTZ cameras extend the visual coverage. The PTZ cameras' built-in IR also provides more light for the radar-video fusion cameras, which makes it possible to detect and identify intruders on a greater distance.

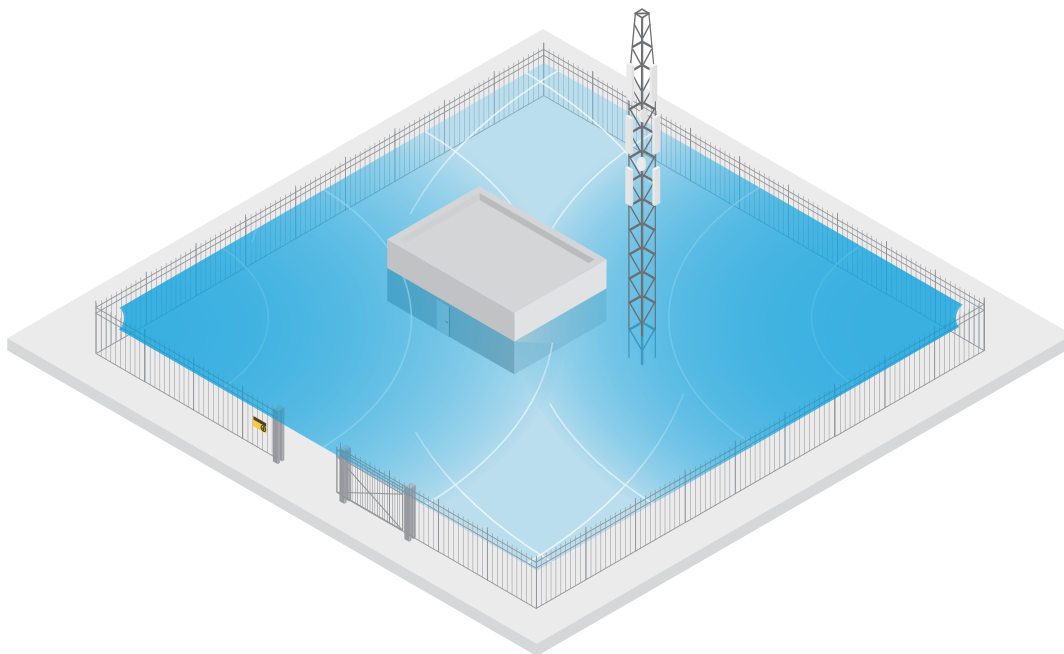
In this scene, the area outside the fence is not covered since it's a busy area that can trigger false alarms. In scenes with less activity, the area outside the fence could be covered as well. In such a scene, it would be possible to configure the cameras to trigger external lights when movement is detected outside the fence to deter potential intruders. They could also trigger an alarm when intruders are actually detected inside the fence. To be able to detect movement outside the fence, the cameras need to be mounted high enough.



Cover a critical asset

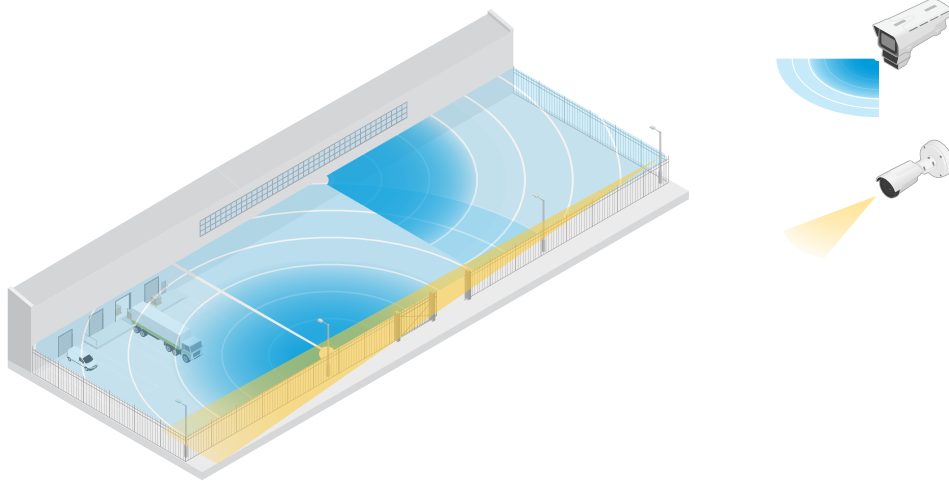
A telecom shelter that contains critical equipment and cabling is surrounded by a fence to keep intruders away. To avoid tampering and sabotage, they need additional protection. Since it's important to keep false alarms to a minimum, they install two radar-video fusion cameras in the opposite corners of the site. The cameras can together cover the shelter, the antennas and the grounds. With the use of both the radar and video technology in the radar-video fusion cameras, the cameras can provide reliable detections and classifications of potential trespassers.

It's possible to place radar-video fusion cameras facing each other in this way without interference between the radars. However, to make sure the video technology can provide accurate detections and classifications, good lighting conditions are required.



Cover the area around a loading bay

The loading bay of a commercial building is surrounded by a fence to protect the premises. For additional security, the company installs a thermal camera and three radar-video fusion cameras on the site. To detect potential trespassers, they install a thermal camera along the fence. To detect intruders that have managed to pass the fence, they install two of the radar-video fusion cameras on a pole facing the loading docks. These cameras will be able to detect and classify humans and vehicles moving around the docks and can trigger an alarm after working hours. To detect any intruders coming through the area with the turning point on the right side, they install an additional radar-video fusion camera facing the area. Finally, the thermal camera can also help to detect tampering attempts of the two cameras installed close to the fence.



Road installation

To get the best radar performance in road installations, select the **road monitoring profile** in AXIS Q1656-DLE. For more information, see .

Road installation examples

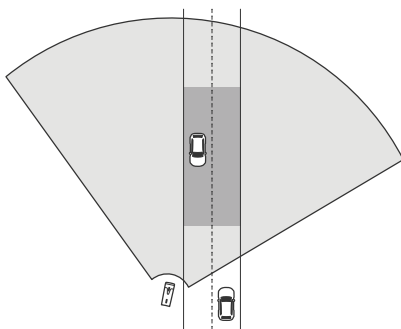
When monitoring roads and highways, make sure to mount the radar-video fusion camera at a sufficient height to avoid blind spots (radar shadow) behind the vehicles.

Note

The size of the radar shadow depends on the radar-video fusion camera's mounting height and the vehicles' height and distance from the radar. For example, when a vehicle with a height of 4.5 m (15 ft) is 50 m (164 ft) away from a radar-video fusion camera that is mounted at a height of 8 m (26 ft), the radar shadow behind the vehicle will be 50 m (164 ft). However, if the radar-video fusion camera is mounted at a height of 12 m (39 ft), the shadow behind the same vehicle will only be 23 m (74 ft).

Side mounted

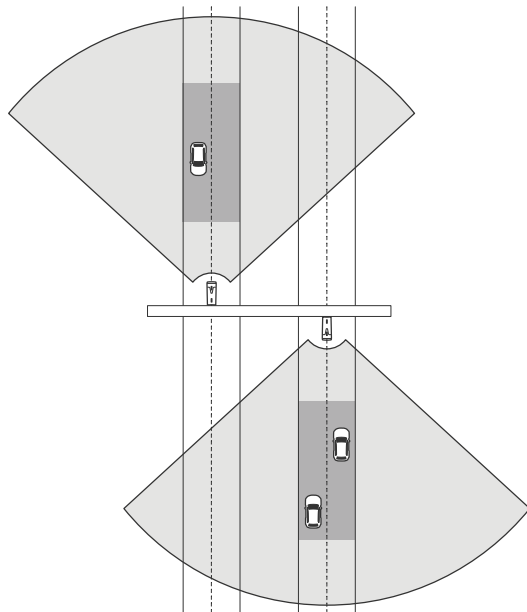
To monitor vehicles travelling along a road you can mount the radar-video fusion camera on the side of the road, for example on a pole. In this type of installation, we recommend a pan angle of max 25°.



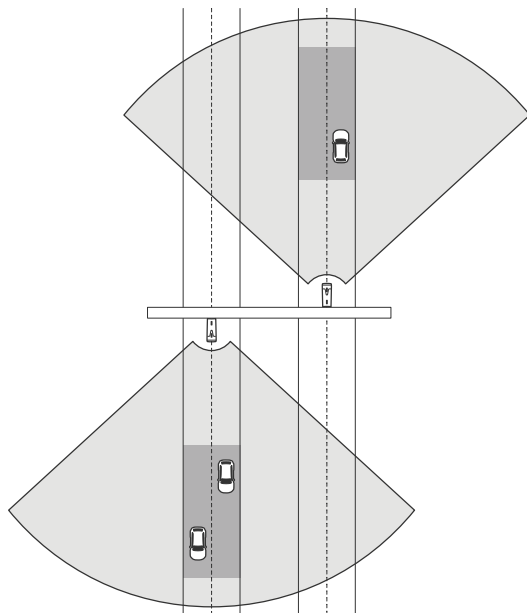
To make it possible for the radar in AXIS Q1656-DLE to measure high speeds accurately, position the radar-video fusion camera within a lateral distance of 10 m (32 ft) from the vehicles. For more information about detection range and velocity accuracy, see .

Center mounted

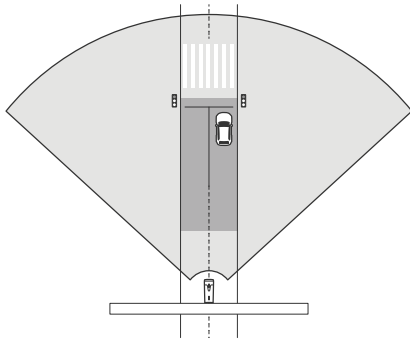
To monitor vehicles on a multi-lane road, you can mount one or more radar-video fusion cameras on a gantry above the road.



The same type of installation is possible if you want to monitor vehicles that drive away from the radar-video fusion camera, instead of driving towards it.



You can also place the radar-video fusion camera on a gantry overlooking a pedestrian crossing with traffic lights, for example to log the speeds of departing vehicles, or detect speed violations.

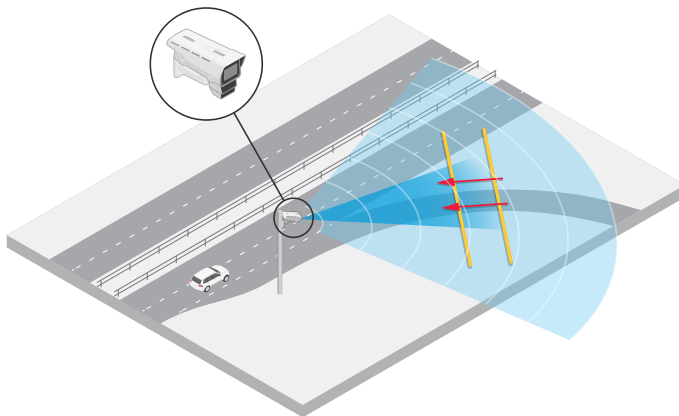


To make it possible for the radar in AXIS Q1656-DLE to measure high speeds accurately, position the radar-video fusion camera within a lateral distance of 10 m (32 ft) from the vehicles. For more information about detection range and velocity accuracy, see .

Road monitoring use cases

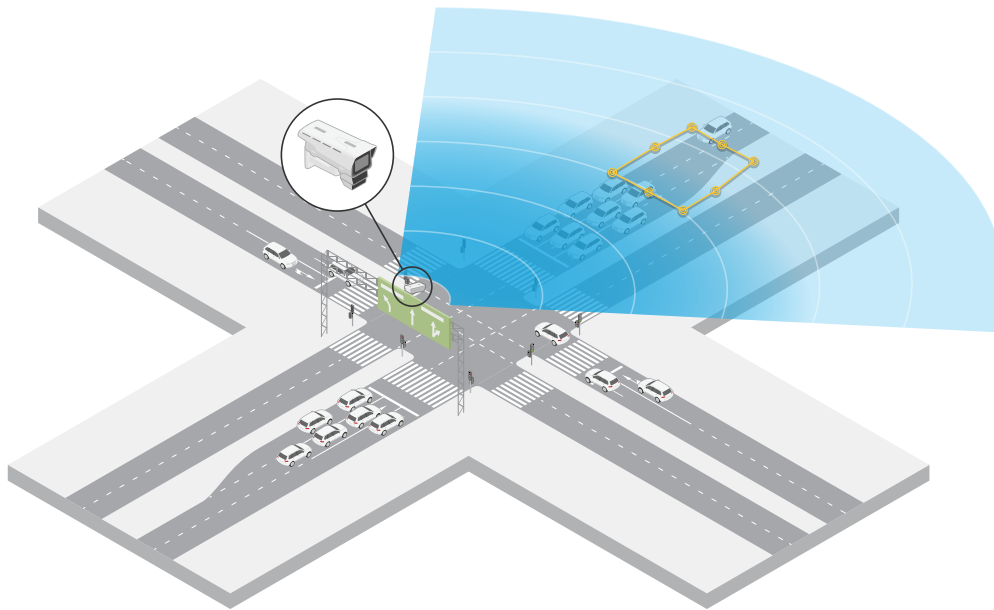
Wrong-way detection on a highway ramp

To detect and identify vehicles driving in the wrong direction on a highway ramp, traffic control mounts AXIS Q1656-DLE on a pole facing the ramp. For reliable detections, they set up a line crossing scenario in the radar pages of the device's web interface and configure it so that vehicles must cross two lines to trigger an alarm. In the radar scenario, they position the two lines on the ramp as seen in the illustration and specify the driving direction and speeds to trigger on. With this configuration, the radar will trigger the alarm, and the camera can provide visual identification of the vehicle on the ramp. For information about how to set up a radar scenario, see .



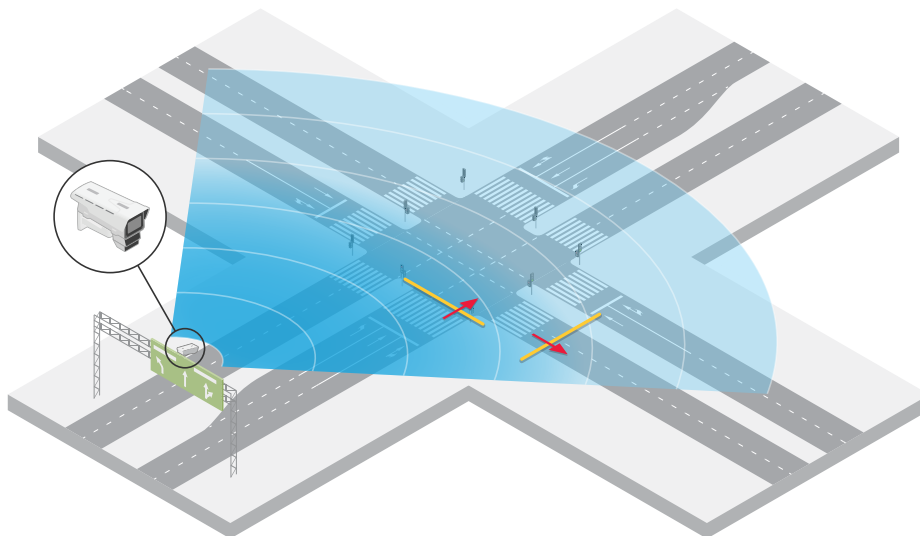
Monitor traffic flow at an intersection – queue build-up

To monitor how and when queues build up in a busy intersection, traffic control installs AXIS Q1656-DLE on a gantry above the intersection. They set up an object in area scenario in AXIS Object Analytics that will trigger on vehicles moving in an area. They shape the scenario to only cover the part of the road leading up to the intersection and select a detection sensitivity that suits the scene. To trigger an alarm when queues start to build up, they configure the scenario to trigger on vehicles moving at speeds below 5 km/h (3 mph). For information about how to configure an AXIS Object Analytics scenario and select a suitable detection sensitivity, see .



Monitor traffic flow at an intersection – direction

To get an overview of the traffic flow and the direction vehicles travel in a busy intersection, traffic control installs AXIS Q1656-DLE on a gantry above the road leading up to the intersection. They set up a line crossing scenario in the radar pages of the device's web interface where vehicles must cross two lines to trigger an alarm. When they configure the radar scenario, they place the first of the two lines over the lanes leading up to the intersection, just after the pedestrian crossing to avoid vehicles stopping at the line. They place the second line over the lanes leading to the right. The vehicles must cross both lines in the specified direction to trigger an alarm. To avoid triggering on more than one vehicle per crossing, they lower the minimum trigger duration in the radar scenario from 2 to 0 seconds.



To monitor the traffic flow in all directions, they create one radar scenario for each direction. For information about how to set up a radar scenario, see .

Note

The radar scenario doesn't count the vehicles crossing the lines, instead you can use the event system in the device's web interface to keep count. One way to count vehicles is to send an MQTT message each time the radar scenario triggers, and count the triggers on the MQTT receiver side.

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

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

Create an administrator account

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

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

Important

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

Secure passwords

Important

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

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

To protect your data we strongly recommend that you:

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

Make sure that no one has tampered with the device software

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

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

Web interface overview

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



Axis device web interface

Configure your device

Basic settings

Set the power line frequency

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

Set the capture mode

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

Adjust the image

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

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**.

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  in the live view and select **Manual**.
4. Adjust the intensity.

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 use the built-in IR light when the camera is in night mode, turn on **Allow illumination** and **Synchronize illumination**.

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.

If you still have problems with motion blur:

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

Maximize the details in an image

Important

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

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

Handle scenes with strong backlight

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



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. 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**.

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

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 the radar live view in the image

Use onscreen controls to see both the live view of the video and the radar in the same stream.

1. Go to **Video > Image**.
2. Click  in the live view to access the product's onscreen controls.
3. Select **Predefined controls**.
4. Turn on **Radar picture-in-picture**.
5. Click **Enable picture-in-picture**.
6. To change the size of the radar projection, click **Resize picture-in-picture**.
7. To change the position of the radar projection, click **Move picture-in-picture**.

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.

Record and watch video

Record video directly from the camera

1. Go to **Video > Stream**.
2. To start a recording, click .

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

3. To stop recording, click  again.

Watch video

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

View and record video

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

Reduce bandwidth and storage

Important

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

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

Note

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

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

Note

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

Set up network storage

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

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

Configure the radar

Note

The radar-video fusion camera is factory-calibrated so that the camera and radar module are perfectly aligned. Do not move or remove the lens, optical unit or radar module since this will undo the calibration and alignment.

Select a radar profile

The radar in this radar-video fusion camera has two profiles; one that is optimized for area monitoring, and one that is optimized for road monitoring. Select the profile that suits your type of installation.

In the web interface:

1. Go to **Radar > Settings > Detection**.
2. Select a profile under **Radar profiles**.

Set the mounting height

Set the mounting height of the device in the radar's web interface. This helps the radar to detect and measure the speed of passing objects correctly.

Measure the height from the ground up to the device as accurately as possible. For scenes with uneven surfaces, set the value that represents the average height in the scene.

Note

If the height is set incorrectly, the bounding boxes that appear in AXIS Object Analytics when an object is detected will not appear in the accurate position.

1. Go to **Radar > Settings > General**.
2. Set the height under **Mounting height**.

You can also set the mounting height in AXIS Object Analytics. Setting the height in one place will automatically populate the mounting height in the other.

1. Go to **Apps > AXIS Object Analytics**.
2. Turn on the application and click **Open**.
3. Click **Settings**.
4. Set the height under **Mounting height**.

Validate the mounting height

To validate that you have measured and set the correct mounting height of the device, add an augmented overlay in the camera's live view. The overlay consists of white bounding boxes projected around moving objects.

1. Go to **Video > Image**.
2. Click  in the live view to access the device's onscreen controls.
3. Expand **Predefined controls**.
4. Turn on **Augmented overlay (radar)**.
5. Click **Toggle augmented bounding boxes**.
6. Ask someone to move in the scene you're monitoring and check in the camera's live view that the bounding boxes are projected around the moving objects, and not above, below, or next to them.
7. If necessary, re-measure the mounting height, adjust the settings, and check again.

Turn off the augmented overlay when you're done with the validation.

Note

If the scene contains variations in elevation, use the autocalibration feature to improve the accuracy of the bounding boxes based on radar detections. For more information, see .

Calibrate a reference map

Upload a reference map to make it easier to see where detected objects are moving. You can use a ground plan or an aerial photo that shows the area covered by the radar. Calibrate the map so the radar coverage fits the

position, direction, and scale of the map, and zoom in on the map if you're interested in a specific part of the radar coverage.

You can either use a setup assistant that takes you through the map calibration step by step, or edit each setting individually.

Use the setup assistant:

1. Go to **Radar > Map calibration**.
2. Click **Setup assistant** and follow the instructions.

To remove the uploaded map and the settings you have added, click **Reset calibration**.

Edit each setting individually:

The map will calibrate gradually after you adjust each setting.

1. Go to **Radar > Map calibration > Map**.
2. Select the image you want to upload, or drag and drop it in the designated area.
To reuse a map image with its current pan and zoom settings, click **Download map**.
3. Under **Rotate map**, use the slider to rotate the map into position.
4. Go to **Scale and distance on a map** and click on two pre-determined points on the map.
5. Under **Distance**, add the actual distance between the two points you have added to the map.
6. Go to **Pan and zoom map** and use the buttons to pan the map image, or zoom in and out on the map image.

Note

The zoom function does not alter the radar's area of coverage. Even if parts of the coverage is out of view after zooming, the radar will still detect moving objects in the entire area of coverage. The only way to exclude detected movement is to add exclude zones. For more information, see .

7. Go to **Radar position** and use the buttons to move or rotate the position of the radar on the map.

To remove the uploaded map and the settings you have added, click **Reset calibration**.



The video shows an example of how to calibrate a reference map in an Axis radar or radar-video fusion camera.

Set detection zones

To determine where to detect motion, you can add one or more detection zones. Use different zones to trigger different actions.

There are two types of zones:

- A **scenario** (previously called include zone) is an area in which moving objects will trigger rules. The default scenario matches the entire area covered by the radar.
- An **exclude zone** is an area in which moving objects will be ignored. Use exclude zones if there are areas inside a scenario that trigger a lot of unwanted alarms.

Add scenarios

A scenario is a combination of triggering conditions and detection settings, which you can use to create rules in the event system. Add scenarios if you want to create different rules for different parts of the scene.

Add a scenario:

1. Go to **Radar > Scenarios**.

2. Click **Add scenario**.
3. Type the name of the scenario.
4. Select if you want to trigger on objects moving in an area or on objects crossing one, or two, lines.

Trigger on objects moving in an area:

1. Select **Movement in area**.
2. Click **Next**.
3. Select the type of zone that should be included in the scenario.
Use the mouse to move and shape the zone so that it covers the desired part of the radar image or reference map.
4. Click **Next**.
5. Add detection settings.
 1. Add seconds until trigger after under **Ignore short-lived objects**.
 2. Select which object type to trigger on under **Trigger on object type**.
 3. Add a range for the speed limit under **Speed limit**.
 6. Click **Next**.
 7. Set the minimum duration of the alarm under **Minimum trigger duration**.
 8. Click **Save**.

Trigger on objects crossing a line:

1. Select **Line crossing**.
2. Click **Next**.
3. Position the line in the scene.
Use the mouse to move and shape the line.
4. To change the detection direction, turn on **Change direction**.
5. Click **Next**.
6. Add detection settings.
 - 6.1. Add seconds until trigger after under **Ignore short-lived objects**.
 - 6.2. Select which object type to trigger on under **Trigger on object type**.
 - 6.3. Add a range for the speed limit under **Speed limit**.
7. Click **Next**.
8. Set the minimum duration of the alarm under **Minimum trigger duration**.
The default value is set to 2 seconds. If you want the scenario to trigger every time an object crosses the line, lower the duration to 0 seconds.
9. Click **Save**.

Trigger on objects crossing two lines:

1. Select **Line crossing**.
2. Click **Next**.
3. To make the object cross two lines for the alarm to trigger, turn on **Require crossing of two lines**.
4. Position the lines in the scene.
Use the mouse to move and shape the line.
5. To change the detection direction, turn on **Change direction**.
6. Click **Next**.
7. Add detection settings.
 - 7.1. Set the time limit between crossing the first and the second line under **Max time between crossings**.

- 7.2. Select which object type to trigger on under **Trigger on object type**.
- 7.3. Add a range for the speed limit under **Speed limit**.
8. Click **Next**.
9. Set the minimum duration of the alarm under **Minimum trigger duration**.
The default value is set to 2 seconds. If you want the scenario to trigger every time an object has crossed the two lines, lower the duration to 0 seconds.
10. Click **Save**.

Add exclude zones

Exclude zones are areas in which moving objects will be ignored. Add exclude zones to ignore, for example, swaying foliage on the side of a road. You could also add exclude zones to ignore ghost tracks caused by radar-reflective materials, for example a metal fence.

Add an exclude zone:

1. Go to **Radar > Exclude zones**.
2. Click **Add exclude zone**.
Use the mouse to move and shape the zone so that it covers the desired part of the radar view or reference map.

Autocalibrate the device

Autocalibration of the radar-video fusion camera improves the accuracy of the bounding boxes that appear around detected objects in AXIS Object Analytics. With autocalibration, the device uses information from the video, like height and angular accuracy, to improve the positioning of the bounding boxes based on the radar detections.

Note

The autocalibration doesn't affect the detections, only the visualization of the bounding boxes.

For elevation calibration:

1. Go to **Radar > Autocalibration > Elevation**.
2. Turn on **Autocalibration**.
The autocalibration occurs as soon as calibration data is available.
3. Select a **Smoothing** option.
 - If your scene contains little variation in elevation, leave **Smoothing** set to **High**.
 - If your scene is hilly or sloped, or if it contains stairs or high buildings, set **Smoothing** to **Low** to keep the differences in elevation.
4. Visualize the result of the calibration in the web interface with the following options:
 - **Show elevation pattern** shows the vertical distance from the ground up to the camera in a pattern of colored dots.
 - **Show color legend** shows a legend containing the colors of the elevation pattern and the vertical distance that each color represent.
 - **Show reference area** shows the area which the calibration is based on.

For azimuth calibration:

1. Go to **Radar > Autocalibration > Azimuth**.
2. Turn on **Autocalibration**.
The autocalibration occurs as soon as calibration data is available.

Show a text overlay with the tilt angle of the radar

You can add an overlay in the radar's live view that shows the tilt angle of the radar. This is helpful during installation, or whenever you need to know the tilt angle of the device.

Note

The tilt angle overlay shows "90" when the device is horizontal. If the overlay shows "75", the tilt angle of the radar is 15° below the horizon.

1. Go to **Radar > Overlays**.
2. Select **Text** and click .
3. Type **#op**.
You can also click **Modifier** and select **#op** from the list.
4. Select a position. You can also drag the overlay field in the live view to change the position.

Configure AXIS Object Analytics

AXIS Object Analytics is an AI-based application that detects and classifies moving objects. It's also the main interface for configuring the radar-video fusion in AXIS Q1656-DLE. The real-time output of the fusion can only be seen in the video stream inside a scenario configured in the application.

Create a scenario

Use scenarios in AXIS Object Analytics to define the detection settings and triggering conditions for your radar-video fusion camera.

1. In the device's web interface, go to **Apps > AXIS Object Analytics**.
2. Start the application and click **Open**.
3. In the welcome screen, click **Step-by-step** and follow the recommended setup procedure.
4. In **Considerations**, read through the information and click **Finish**.
5. Click **+ New scenario**.

Note

By default, the scenarios **Object in area** and **Line crossing** use both video and radar input. The other scenarios in AXIS Object Analytics use video input only.

6. Select a scenario based on your requirements.
7. Select the type of object you want the application to detect.
8. Configure your scenario.
9. Verify your settings and click **Finish**.

Note

To get bounding boxes around the moving objects, go to **Settings** and turn on **Metadata overlay**. When you create two scenarios, where one scenario uses both video and radar input and the other only uses video input, there will be double bounding boxes around the moving object. This behavior is expected.

You have now created a scenario in AXIS Object Analytics. To modify the scenario and apply additional settings, click **Open**. For scenarios that use both radar and video input, you can use speed to trigger and select a detection sensitivity. For instructions, see:

-
-

To learn more about AXIS Object Analytics and its general settings, see *AXIS Object Analytics user manual*.

Note

Some of the considerations and features described in AXIS Object Analytics user manual don't apply to radar-video fusion cameras.

Use speed to trigger

If you have created an **Object in area** or **Line crossing** scenario in AXIS Object Analytics, you can trigger on objects moving within a set speed range, or above and below it.

1. Go to **Apps > AXIS Object Analytics**.
2. Start the application and click **Open**.
3. Select the scenario you want to modify and click **Open**.
4. Go to **Object speed** and turn on **Use speed to trigger**.
5. Set the speed range to trigger on.
6. If you want to trigger on speeds above and below your set range, click **Invert**.

Select detection sensitivity

With the option to select detection sensitivity, you can decide if you want to trigger on detections made by either the video or the radar, or detections made by both. You can also let the device itself, based on the fusion algorithms, decide if it should rely on one of the technologies, or both.

This option is available in **Object in area** and **Line crossing** scenarios.

1. Go to **Apps > AXIS Object Analytics**.
2. Start the application and click **Open**.
3. Select the scenario you want to modify and click **Open**.
4. Go to **Detection sensitivity** and select one of the following options:
 - **Low sensitivity:** Requires both the radar and the camera to detect the object. This reduces the risk of false alarms, but increases the risk of missed detections.
To make sure that objects can be detected by both technologies, the scene can't be too complex. The light conditions need to be good, the detection area needs to be within the detection range of both technologies, and there should preferably not be any disturbing elements, such as trees or bushes.
 - **Automatic:** Lets the application decide if both the radar and the camera, or only one of them, is required to detect the object. This is the default option.
 - **High sensitivity:** Requires either the radar or the camera to detect the object. This increases the risk of false alarms, but reduces the risk of missed detections.
The lighting conditions and the size of the detection area are less important when you select high sensitivity since you only need one of the technologies to detect the object.

Note

You can improve the accuracy of the bounding boxes that appear around detected objects in AXIS Object Analytics with the autocalibration feature. Autocalibration doesn't affect the detections, only the visualization of the bounding boxes.

For more information, see .

Minimize false alarms

If you notice that you get too many false alarms, you can filter out certain types of movement or objects, change the coverage, or adjust the detection sensitivity. See which settings work best for your environment.

- Adjust the detection sensitivity of AXIS Object Analytics:
Go to **Apps > AXIS Object Analytics**, open a scenario, and select a lower **Detection sensitivity**.
 - **Low sensitivity:** Requires both the radar and the camera to detect the object. Reduced risk of false alarms, but increased risk of missed detections.
 - **Automatic:** Lets the application decide if both radar and camera or only one of them is required to detect the object.

- **High sensitivity:** Requires either the radar or the camera to detect the object. Increased risk of false alarms but reduced risk of missed detections.
- Adjust the detection sensitivity of the radar:
Go to **Radar > Settings > Detection** and select a lower **Detection sensitivity**. This decreases the risk of false alarms, but it could also cause the radar to miss some movement.
 - **Low:** Use this sensitivity when there are a lot of metal objects or large vehicles in the area. It will take longer time for the radar to track and classify objects. This can reduce the detection range, especially for fast moving objects.
 - **Medium:** This is the default setting.
 - **High:** Use this sensitivity when you have an open field without metal objects in front of the radar. This will increase the detection range for humans.
- Modify scenarios and exclude zones:
If a scenario includes hard surfaces, such as a metal wall, there may be reflections that causes multiple detections for a single physical object. You can either modify the shape of the scenario, or add an exclude zone that ignores certain parts of the scenario. For more information, see [and](#) .
- Trigger on objects crossing two lines instead of one:
If a line crossing scenario includes swaying objects or animals moving around, there is a risk that an object will happen to cross the line and trigger a false alarm. In this case, you can configure the scenario to trigger only when an object has crossed two lines. For more information, see [.](#)
- Filter on movement:
 - Go to **Radar > Settings > Detection** and select **Ignore swaying objects**. This setting minimizes false alarms from trees, bushes, and flagpoles in the coverage zone.
 - Go to **Radar > Settings > Detection** and select **Ignore small objects**. This setting minimizes false alarms from small objects in the coverage zone, such as cats and rabbits.
- Filter on time:
 - Go to **Radar > Scenarios**.
 - Select a scenario, and click  to modify its settings.
 - Select a higher value under **Seconds until trigger**. This is the delay time from when the radar starts tracking an object until it can trigger and alarm. The timer starts when the radar first detects the object, not when the object enters the specified zone in the scenario.
- Filter on object type:
 - Go to **Radar > Scenarios**.
 - Select a scenario, and click  to modify its settings.
 - To avoid triggering on specific object types, deselect the object types that should not trigger events in the scenario.

Note

The object type setting only affects the radar. It will be ignored by AXIS Object Analytics.

Set up rules for events

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

Save power when no motion is detected

This example explains how to turn on power saving mode when no motion is detected in the scene.

Note

When you turn on power saving mode, the IR illumination range is reduced.

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. Select **Invert this condition**.
5. In the list of actions, under **Power saving mode**, select **Use power saving mode while the rule is active**.
6. Click **Save**.

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**.

Send an email if someone covers the radar with a metallic object

This example explains how to create a rule that sends an email notification when someone tampers with the radar by covering it with a metallic object, such as metallic foil or a metallic sheet.

Note

The option to create rules for radar tampering events is available from AXIS OS 11.11.

Add an email recipient:

1. Go to **System > Events > Recipients** and click **Add recipient**.
2. Type a name for the recipient.
3. Select **Email**.
4. Type an email address to send the email to.
5. The camera doesn't have its own email server, so it will need to log into another email server to be able to send mails. Fill in the rest of the information according to your email provider.

6. To send a test email, click **Test**.
7. Click **Save**.

Create a rule:

8. Go to **System > Events** and add a rule.
9. Type a name for the rule.
10. From the list of conditions, under **Device status**, select **Radar data failure**.
11. Under **Reason**, select **Tampering**.
12. From the list of actions, under **Notifications**, select **Send notification to email**.
13. Select the recipient you created.
14. Type a subject and a message for the email.
15. Click **Save**.

Control a PTZ camera with the radar

It's possible to use the information about objects' positions from the radar to make a PTZ camera track objects. There are two ways to do this:

- . The built-in option is suitable when you have a PTZ camera and radar mounted very close together.
- . The Windows application is suitable when you want to use multiple PTZ cameras and radars for tracking objects.

Note

Use an NTP server to synchronize the time on the cameras and the Windows computer. If the clocks are out of sync, you may experience delays in the tracking, or ghost tracking.

Control a PTZ camera with the built-in radar autotracking service

The built-in radar autotracking creates an edge-to-edge solution where the radar directly controls the PTZ camera. It supports all Axis PTZ cameras.

Note

You can use the built-in radar autotracking service to connect one radar with one PTZ camera. For a setup where you want to use more than one radar or PTZ camera, use **AXIS Radar Autotracking for PTZ**. For more information, see .

This instruction explains how to pair the radar with a PTZ camera, how to calibrate the devices, and how to set up the tracking of objects.

Before you start:

- Define the area of interest and avoid unwanted alarms by setting up exclude zones in the radar. Make sure to exclude zones with radar-reflective materials or swaying objects, like foliage, to prevent the PTZ camera from tracking irrelevant objects. For instructions, see .

Pair the radar with the PTZ camera:

1. Go to **System > Edge-to-edge > PTZ pairing**.
2. Enter the IP address, username and password for the PTZ camera.
3. Click **Connect**.
4. Click **Configure Radar autotracking** or go to **Radar > Radar PTZ autotracking** to set up radar autotracking.

Calibrate the radar and the PTZ camera:

5. Go to **Radar > Radar PTZ autotracking**.
6. To set the mounting height of the camera, go to **Camera mounting height**.
7. To pan the PTZ camera so that it points in the same direction as the radar, go to **Pan alignment**.

8. If you need to adjust the tilt to compensate for a sloping ground, go to **Ground incline offset** and add an offset in degrees.

Set up the PTZ tracking:

9. Go to **Track** to select if you want to track humans, vehicles and/or unknown objects.
10. To start tracking objects with the PTZ camera, turn on **Tracking**.
The tracking automatically zooms in on an object, or a group of objects, to keep them in the view of the camera.
11. Turn on **Object switching** if you expect multiple objects that won't fit in the camera view.
With this setting, the radar gives priority of the objects to track.
12. To determine how many seconds to track each object, set **Object hold time**.
13. To make the PTZ camera return to its home position when the radar no longer tracks any objects, turn on **Return to home**.
14. To determine how long the PTZ camera should stay at the tracked objects last known position before returning to home, set **Return to home timeout**.
15. To fine tune the zoom of the PTZ camera, adjust the zoom on the slider.

Control a PTZ camera with AXIS Radar Autotracking for PTZ

AXIS Radar Autotracking for PTZ is a server-based solution that can handle different setups when tracking objects:

- Control several PTZ cameras with one radar.
- Control one PTZ camera with several radars.
- Control several PTZ cameras with several radars.
- Control one PTZ camera with one radar when they are mounted in different positions covering the same area.

The application is compatible with a specific set of PTZ cameras. For more information, see axis.com/products/axis-radar-autotracking-for-ptz#compatible-products.

Download the application and see the user manual for information about how to set up the application. For more information, see axis.com/products/axis-radar-autotracking-for-ptz/support.

Use MQTT to send radar data

Use the radar-video fusion camera with the application AXIS Speed Monitor to collect radar data for detected objects and send it over MQTT.

This example explains how to set up an MQTT client in the device where you have installed AXIS Speed Monitor, and how to create a condition that will publish the radar data collected in AXIS Speed Monitor as a payload to an MQTT broker.

Before you start:

- Install AXIS Speed Monitor in your radar-video fusion camera, or install it in a camera that you connect to the radar in the radar-video fusion camera.
For more information, see *AXIS Speed Monitor user manual*.
- Set up an MQTT broker and get the broker's IP address, username and password.
Learn more about MQTT and MQTT brokers in *AXIS OS Knowledge Base*.

Set up the MQTT client in the web interface of the device where you have installed AXIS Speed Monitor:

1. Go to **System > MQTT > MQTT client > Broker** and enter the following information:
 - **Host:** The broker IP address
 - **Client ID:** The ID of the device
 - **Protocol:** The protocol the broker is set to
 - **Port:** The port number used by the broker

- The broker Username and Password
2. Click **Save** and **Connect**.

Create a condition that publishes the radar data as a payload to the MQTT broker:

3. Go to **System > MQTT > MQTT publication** and click **+ Add condition**.
4. In the list of conditions, under **Application**, select **Speed Monitor: Track exited zone**.

The device will now be able to send information about the radar tracks for every moving object that exits a scenario. Every object will have its own radar track parameters, for example `rmd_zone_name`, `tracking_id`, and `trigger_count`. You can find the full list of parameters in *AXIS Speed Monitor user manual*.

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**.

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.

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.

Record video when a PIR detector senses motion

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

Required hardware

- 3-wire cable (ground, power, I/O)
- PIR detector, normally closed

NOTICE

Disconnect the device from power before connecting the wires. Reconnect to power after all connections are done.

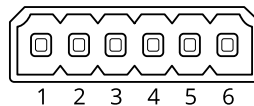
Connect the wires to the device's I/O connector

Note

For information on the I/O connector, see .

1. Connect the ground wire to pin 1 (GND/-).
2. Connect the power wire to pin 2 (12V DC output).
3. Connect the I/O wire to pin 3 (I/O input).

Connect the wires to the PIR detector's I/O connector



1. Connect the other end of the ground wire to pin 1 (GND/-).
2. Connect the other end of the power wire to pin 2 (DC input/+).
3. Connect the other end of the I/O wire to pin 3 (I/O output).

Configure the I/O port in the device web interface

1. Go to **System > Accessories > I/O ports**.
2. Click  to set the direction to input for port 1.
3. Give the input module a descriptive name, for example "PIR detector".
4. If you want to trigger an event whenever the PIR detector senses motion, click  to set the normal state to circuit closed.

Create a rule

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

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 .

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**.

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 .

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**.

Audio

Add audio to your recording

Turn on audio:

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

Edit the stream profile that is used for the recording:

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

The web interface

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

Note

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



Show or hide the main menu.



Access the release notes.



Access the product help.



Change the language.



Set light theme or dark theme.



The user menu contains:

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



The context menu contains:

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

Status

Security

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

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

Time sync status

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

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

Ongoing recordings

Shows ongoing recordings and their designated storage space.

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



Shows the storage space where the recording is saved.

Device info

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

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

Connected clients

Shows the number of connections and connected clients.

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

AXIS Image Health Analytics

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

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

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

Video



Click to play the live video stream.



Click to freeze the live video stream.



Click to take a snapshot of the live video stream. The file is saved in the 'Downloads' folder on your computer. The image file name is [snapshot_YYYY_MM_DD_HH_MM_SS.jpg]. The size of the snapshot depends on the compression that the specific web-browser engine where the snapshot is received applies, therefore, the snapshot size may vary from the actual compression setting that is configured in the device.



Click to show I/O output ports. Use the switch to open or close the circuit of a port, for example, to test external devices.



Click to manually turn on or turn off the IR illumination.



Click to manually turn on or turn off the white light.



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

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



Starts the washer. When the sequence starts, the camera moves to the configured position to receive the wash spray. When the whole wash sequence is completed, the camera returns to its previous position. This icon is only visible when the washer is connected and configured.



Starts the wiper.



Click and select a preset position to go to that preset position in the live view. Or, click **Setup** to go to the preset position page.



Adds or removes a focus recall area. When you add a focus recall area, the camera saves the focus settings at that specific pan/tilt range. When you have set a focus recall area and the camera enters that area in the live view, the camera recalls the previously saved focus. It's enough to cover half of the area for the camera to recall the focus.



Click to select a guard tour, then click **Start** to play the guard tour. Or, click **Setup** to go to the guard tours page.



Click to manually turn on the heater for a selected period of time.



Click to start a continuous recording of the live video stream. Click again to stop the recording. If a recording is ongoing, it will resume automatically after a reboot.



Click to show the storage that is configured for the device. To configure the storage, you need to be logged in as an administrator.



Click to access more settings:

- **Video format:** Select the encoding format to use in the live view.
-  **Autoplay:** Turn on to autoplay a muted video stream whenever you open the device in a new session.
- **Client stream information:** Turn on to show dynamic information about the video stream used by the browser that shows the live video stream. The bitrate information differs from the information shown in a text overlay, because of different information sources. The bitrate in the client stream information is the bitrate of the last second, and it comes from the encoding driver of the device. The bitrate in the overlay is the average bitrate of the last 5 seconds, and it comes from the browser. Both values cover only the raw video stream and not the additional bandwidth generated when it's transported over the network through UDP/TCP/HTTP.
- **Adaptive stream:** Turn on to adapt the image resolution to the viewing client's actual display resolution, to improve the user experience and help prevent a possible overload of the client's hardware. The adaptive stream is only applied when you view the live video stream in the web interface in a browser. When adaptive stream is turned on, the maximum frame rate is 30 fps. If you take a snapshot while adaptive stream is turned on, it will use the image resolution selected by the adaptive stream.
- **Level grid:** Click  to show the level grid. The grid helps you decide if the image is horizontally aligned. Click  to hide it.
- **Pixel counter:** Click  to show the pixel counter. Drag and resize the box to contain your area of interest. You can also define the pixel size of the box in the **Width** and **Height** fields.
- **Refresh:** Click  to refresh the still image in the live view.
- **PTZ controls**  : Turn on to display PTZ controls in the live view.



Click to show the live view at full resolution. If the full resolution is larger than your screen size, use the smaller image to navigate in the image.



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

Installation

Capture mode 

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

Mounting position 

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

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

Zoom  : Use the slider to adjust the zoom level.

Autofocus after zooming  : Turn on to enable autofocus after zooming.

Focus: Use the slider to manually set the focus.

Autofocus: Click to make the camera focus on the selected area. If you don't select an autofocus area, the camera focuses on the entire scene.

Autofocus area: Click  to show the autofocus area. This area should include the area of interest.

Reset focus: Click to make the focus return to its original position.

Note

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

Image correction

Important

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

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

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

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

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

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

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

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

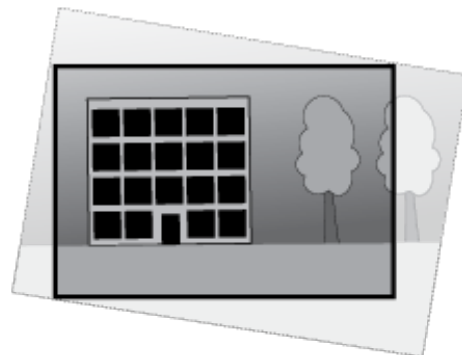
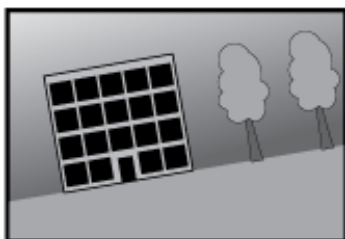
Straighten image ⓘ : Turn on and use the slider to straighten the image horizontally by rotating and cropping it digitally. The functionality is useful when it's not possible to mount the camera exactly level. Ideally, straighten the image during installation.



: Click to show a supporting grid in the image.



: Click to hide the grid.



The image before and after it has been straightened.

Image

Appearance

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

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

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



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



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



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



Wide dynamic range

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

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

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

White balance

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

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

Light environment:

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

Day-night mode

IR-cut filter:

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

Note

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

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

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

IR light

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

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

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

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

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

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

White light 

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

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

Exposure

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

Exposure mode:

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

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

Note

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

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

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

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

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

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

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

Note

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

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

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

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

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

Note

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

Optics

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

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

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

Stream

General

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

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

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

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

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

Zipstream

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

Select the bitrate reduction **Strength**:

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

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

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

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

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

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

Bitrate control

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

Audio

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

Source  : Select what audio source to use.

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

Overlays



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

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

- **Appearance:** Select the animation color and background color, for example, red animation on a transparent background (default).
- **Size:** Select the desired font size.
-  : Select the position of the overlay in the image or click and drag the overlay to move it around in the live view.
- **Widget: Linegraph**  : Show a graph chart that displays how a measured value changes over time.
 - **Title:** Enter a title for the widget.
 - **Overlay modifier:** Select an overlay modifier as data source. If you have created MQTT overlays, they will be located at the end of the list.
 -  : Select the position of the overlay in the image or click and drag the overlay to move it around in the live view.
 - **Size:** Select the size of the overlay.
 - **Visible on all channels:** Turn off to show only on your currently selected channel. Turn on to show on all active channels.
 - **Update interval:** Choose the time between data updates.
 - **Transparency:** Set the transparency of the entire overlay.
 - **Background transparency:** Set the transparency only of the background of the overlay.
 - **Points:** Turn on to add a point to the graph line when data is updated.
 - **X axis**
 - **Label:** Enter the text label for the x axis.
 - **Time window:** Enter how long time the data is visualized.
 - **Time unit:** Enter a time unit for the x axis.
 - **Y axis**
 - **Label:** Enter the text label for the y axis.
 - **Dynamic scale:** Turn on for the scale to automatically adapt to the data values. Turn off to manually enter values for a fixed scale.
 - **Min alarm threshold and Max alarm threshold:** These values will add horizontal reference lines to the graph, making it easier to see when the data value becomes too high or too low.
- **Widget: Meter**  : Show a bar chart that displays the most recently measured data value.
 - **Title:** Enter a title for the widget.
 - **Overlay modifier:** Select an overlay modifier as data source. If you have created MQTT overlays, they will be located at the end of the list.
 -  : Select the position of the overlay in the image or click and drag the overlay to move it around in the live view.
 - **Size:** Select the size of the overlay.
 - **Visible on all channels:** Turn off to show only on your currently selected channel. Turn on to show on all active channels.
 - **Update interval:** Choose the time between data updates.
 - **Transparency:** Set the transparency of the entire overlay.
 - **Background transparency:** Set the transparency only of the background of the overlay.
 - **Points:** Turn on to add a point to the graph line when data is updated.

- **Y axis**
 - **Label:** Enter the text label for the y axis.
 - **Dynamic scale:** Turn on for the scale to automatically adapt to the data values. Turn off to manually enter values for a fixed scale.
 - **Min alarm threshold and Max alarm threshold:** These values will add horizontal reference lines to the bar chart, making it easier to see when the data value becomes too high or too low.

Privacy masks



: Click to create a new privacy mask.

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

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



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

Radar

Settings

General

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

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

Mounting height: Enter the mounting height for the product.

Note

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

Detection

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

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

- **Area monitoring:** Track both large and small objects moving at lower speeds in open areas.
 - **Ignore stationary rotating objects**  : Turn on to minimize false alarms from stationary objects with rotating movements, such as fans or turbines.
 - **Ignore small objects:** Turn on to minimize false alarms from small objects, such as cats or rabbits.
 - **Ignore swaying objects:** Turn on to minimize false alarms from swaying objects, such as trees, bushes, or flagpoles.
- **Road monitoring:** Track vehicles moving at higher speeds in urban zones and on suburban roads
 - **Ignore stationary rotating objects**  : Turn on to minimize false alarms from stationary objects with rotating movements, such as fans or turbines.
 - **Ignore swaying objects:** Turn on to minimize false alarms from swaying objects, such as trees, bushes, or flagpoles.

View

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

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

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

Color scheme: Select a theme for the radar visualization.

Rotation  : Select the preferred orientation of the radar image.

Object visualization

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

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

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

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

Stream

General

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

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

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

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

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

Zipstream

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

Select the bitrate reduction **Strength**:

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

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

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

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

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

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

Bitrate control

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

Audio

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

Source  : Select what audio source to use.

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

Map calibration

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

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

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

Map

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

Download map: Click to download the map.

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

Scale and distance on map

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

Pan and zoom map

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

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

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

Radar position

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

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

Exclude zones

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



: Click to create a new exclude zone.

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

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

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

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

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

Scenarios

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



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

Triggering conditions: Select the condition that will trigger alarms.

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

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

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

Detection settings: Define the trigger criteria for the scenario.

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

Alarm settings: Define the criteria for the alarm.

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

Overlays



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

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

- **Appearance:** Select the animation color and background color, for example, red animation on a transparent background (default).
- **Size:** Select the desired font size.
-  : Select the position of the overlay in the image or click and drag the overlay to move it around in the live view.
- **Widget: Linegraph**  : Show a graph chart that displays how a measured value changes over time.
 - **Title:** Enter a title for the widget.
 - **Overlay modifier:** Select an overlay modifier as data source. If you have created MQTT overlays, they will be located at the end of the list.
 -  : Select the position of the overlay in the image or click and drag the overlay to move it around in the live view.
 - **Size:** Select the size of the overlay.
 - **Visible on all channels:** Turn off to show only on your currently selected channel. Turn on to show on all active channels.
 - **Update interval:** Choose the time between data updates.
 - **Transparency:** Set the transparency of the entire overlay.
 - **Background transparency:** Set the transparency only of the background of the overlay.
 - **Points:** Turn on to add a point to the graph line when data is updated.
 - **X axis**
 - **Label:** Enter the text label for the x axis.
 - **Time window:** Enter how long time the data is visualized.
 - **Time unit:** Enter a time unit for the x axis.
 - **Y axis**
 - **Label:** Enter the text label for the y axis.
 - **Dynamic scale:** Turn on for the scale to automatically adapt to the data values. Turn off to manually enter values for a fixed scale.
 - **Min alarm threshold and Max alarm threshold:** These values will add horizontal reference lines to the graph, making it easier to see when the data value becomes too high or too low.
- **Widget: Meter**  : Show a bar chart that displays the most recently measured data value.
 - **Title:** Enter a title for the widget.
 - **Overlay modifier:** Select an overlay modifier as data source. If you have created MQTT overlays, they will be located at the end of the list.
 -  : Select the position of the overlay in the image or click and drag the overlay to move it around in the live view.
 - **Size:** Select the size of the overlay.
 - **Visible on all channels:** Turn off to show only on your currently selected channel. Turn on to show on all active channels.
 - **Update interval:** Choose the time between data updates.
 - **Transparency:** Set the transparency of the entire overlay.
 - **Background transparency:** Set the transparency only of the background of the overlay.
 - **Points:** Turn on to add a point to the graph line when data is updated.

- **Y axis**
 - **Label:** Enter the text label for the y axis.
 - **Dynamic scale:** Turn on for the scale to automatically adapt to the data values. Turn off to manually enter values for a fixed scale.
 - **Min alarm threshold and Max alarm threshold:** These values will add horizontal reference lines to the bar chart, making it easier to see when the data value becomes too high or too low.

Radar PTZ autotracking

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

Configure initial settings:

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

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

Save pan offset: Click to save the pan alignment.

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

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

Configure PTZ autotracking:

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

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

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

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

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

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

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

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

Autocalibration

Elevation

Status: Shows if calibration data is available or not. The camera and radar collects calibration data continuously.

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

Smoothing: Smooths out differences in elevation.

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

Reset: Resets the autocalibration and the gathered calibration data.

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

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

Color: Select the colors for the elevation pattern.

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

Azimuth

Status: Shows if calibration data is available or not. The camera and radar collects calibration data continuously.

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

Reset: Resets the autocalibration and the gathered calibration data.

Analytics

AXIS Object Analytics

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

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

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

AXIS Image Health Analytics

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

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

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

Metadata visualization

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

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

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

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

Metadata configuration

RTSP metadata producers

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

Note

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

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

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

MQTT

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

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

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

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



The context menu contains:

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

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

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

Audio

Device settings

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

- Input type** ⓘ : Select the type of input, for instance, if it's internal microphone or line.
- Power type** ⓘ : Select power type for your input.
- Apply changes** ⓘ : Apply your selection.
- Echo cancellation** ⓘ : Turn on to remove echoes during two-way communication.
- Separate gain controls** ⓘ : Turn on to adjust the gain separately for the different input types.
- Automatic gain control** ⓘ : Turn on to dynamically adapt the gain to changes in the sound.
- Gain:** Use the slider to change the gain. Click the microphone icon to mute or unmute.

Output: Shows the type of output.

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

Stream

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

Audio clips

-  **Add clip:** Add a new audio clip. You can use .au, .mp3, .opus, .vorbis, .wav files.
-  **Play the audio clip.**
-  **Stop playing the audio clip.**
-  **The context menu contains:**
 - **Rename:** Change the name of the audio clip.
 - **Create link:** Create a URL that, when used, plays the audio clip on the device. Specify the volume and number of times to play the clip.
 - **Download:** Download the audio clip to your computer.
 - **Delete:** Delete the audio clip from the device.

Audio enhancement

Input

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

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

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

Recordings

Ongoing recordings: Show all ongoing recordings on the device.

- Start a recording on the device.



Choose which storage device to save to.

- Stop a recording on the device.

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

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



Play the recording.



Stop playing the recording.



Show or hide information and options about the recording.

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

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



Click to delete a recording.

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



Click to filter the recordings.

From: Show recordings done after a certain point in time.

To: Show recordings up until a certain point in time.

Source ⓘ: Show recordings based on source. The source refers to the sensor.

Event: Show recordings based on events.

Storage: Show recordings based on storage type.

Apps



Add app: Install a new app.

Find more apps: Find more apps to install. You will be taken to an overview page of Axis apps.



Allow unsigned apps ⓘ: Turn on to allow installation of unsigned apps.



View the security updates in AXIS OS and ACAP apps.

Note

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

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

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



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

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

System

Time and location

Date and time

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

Note

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

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

- **Automatic date and time (manual NTS KE servers):** Synchronize with the secure NTP key establishment servers connected to the DHCP server.
 - **Manual NTS KE servers:** Enter the IP address of one or two NTP servers. When you use two NTP servers, the device synchronizes and adapts its time based on input from both.
 - **Trusted NTS KE CA certificates:** Select the trusted CA certificates to use for secure NTS KE time synchronization, or leave at none.
 - **Max NTP poll time:** Select the maximum amount of time the device should wait before it polls the NTP server to get an updated time.
 - **Min NTP poll time:** Select the minimum amount of time the device should wait before it polls the NTP server to get an updated time.
- **Automatic date and time (NTP servers using DHCP):** Synchronize with the NTP servers connected to the DHCP server.
 - **Fallback NTP servers:** Enter the IP address of one or two fallback servers.
 - **Max NTP poll time:** Select the maximum amount of time the device should wait before it polls the NTP server to get an updated time.
 - **Min NTP poll time:** Select the minimum amount of time the device should wait before it polls the NTP server to get an updated time.
- **Automatic date and time (manual NTP servers):** Synchronize with NTP servers of your choice.
 - **Manual NTP servers:** Enter the IP address of one or two NTP servers. When you use two NTP servers, the device synchronizes and adapts its time based on input from both.
 - **Max NTP poll time:** Select the maximum amount of time the device should wait before it polls the NTP server to get an updated time.
 - **Min NTP poll time:** Select the minimum amount of time the device should wait before it polls the NTP server to get an updated time.
- **Custom date and time:** Manually set the date and time. Click **Get from system** to fetch the date and time settings once from your computer or mobile device.

Time zone: Select which time zone to use. Time will automatically adjust to daylight saving time and standard time.

- **DHCP:** Adopts the time zone of the DHCP server. The device must be connected to a DHCP server before you can select this option.
- **Manual:** Select a time zone from the drop-down list.

Note

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

Device location

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

- **Latitude:** Positive values are north of the equator.
- **Longitude:** Positive values are east of the prime meridian.
- **Heading:** Enter the compass direction that the device is facing. 0 is due north.
- **Label:** Enter a descriptive name for your device.
- **Save:** Click to save your device location.

Regional settings

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

Metric (m, km/h): Select for distance measurement to be in meters and speed measurement to be in kilometers per hour.

U.S. customary (ft, mph): Select for distance measurement to be in feet and speed measurement to be in miles per hour.

Network

IPv4

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

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

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

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

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

Note

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

IPv6

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

Hostname

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

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

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

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

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

DNS servers

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

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

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

HTTP and HTTPS

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

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

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

Note

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

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

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

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

Global proxies

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

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

Allowed formats for http and https proxies:

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

Note

Restart the device to apply the global proxy settings.

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

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

Network discovery protocols

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

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

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

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

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

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

One-click cloud connection

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

Allow O3C:

- **One-click:** This is the default option. To connect to O3C, press the control button on the device. Depending on the device model, either press and release or press and hold, until the status LED flashes. Register the device with the O3C service within 24 hours to enable **Always** and stay connected. If you don't register, the device will disconnect from O3C.
- **Always:** The device continuously attempts to connect to an O3C service over the internet. Once you register the device, it stays connected. Use this option if the control button is out of reach.
- **No:** Disconnects the O3C service.

Proxy settings: If needed, enter the proxy settings to connect to the proxy server.

Host: Enter the proxy server's address.

Port: Enter the port number used for access.

Login and Password: If needed, enter username and password for the proxy server.

Authentication method:

- **Basic:** This method is the most compatible authentication scheme for HTTP. It's less secure than the **Digest** method because it sends the username and password unencrypted to the server.
- **Digest:** This method is more secure because it always transfers the password encrypted across the network.
- **Auto:** This option lets the device select the authentication method depending on the supported methods. It prioritizes the **Digest** method over the **Basic** method.

Owner authentication key (OAK): Click **Get key** to fetch the owner authentication key. This is only possible if the device is connected to the internet without a firewall or proxy.

SNMP

The Simple Network Management Protocol (SNMP) allows remote management of network devices.

SNMP: Select the version of SNMP to use.

- **v1 and v2c:**
 - **Read community:** Enter the community name that has read-only access to all supported SNMP objects. The default value is **public**.
 - **Write community:** Enter the community name that has read or write access to all supported SNMP objects (except read-only objects). The default value is **write**.
 - **Activate traps:** Turn on to activate trap reporting. The device uses traps to send messages for important events or status changes to a management system. In the web interface, you can set up traps for SNMP v1 and v2c. Traps are automatically turned off if you change to SNMP v3 or turn off SNMP. If you use SNMP v3, you can set up traps through the SNMP v3 management application.
 - **Trap address:** Enter the IP address or host name of the management server.
 - **Trap community:** Enter the community to use when the device sends a trap message to the management system.
 - **Traps:**
 - **Cold start:** Sends a trap message when the device starts.
 - **Link up:** Sends a trap message when a link changes from down to up.
 - **Link down:** Sends a trap message when a link changes from up to down.
 - **Authentication failed:** Sends a trap message when an authentication attempt fails.

Note

All Axis Video MIB traps are enabled when you turn on SNMP v1 and v2c traps. For more information, see *AXIS OS Portal > SNMP*.

- **v3:** SNMP v3 is a more secure version, which provides encryption and secure passwords. To use SNMP v3, we recommend you to activate HTTPS, as the password is then sent through HTTPS. This also prevents unauthorized parties' access to unencrypted SNMP v1 and v2c traps. If you use SNMP v3, you can set up traps through the SNMP v3 management application.
 - **Password for the account "initial":** Enter the SNMP password for the account named "initial". Although the password can be sent without activating HTTPS, we don't recommend it. The SNMP v3 password can only be set once, and preferably only when HTTPS is enabled. Once the password is set, the password field is no longer displayed. To set the password again, you must reset the device to factory default settings.

Security

Certificates

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

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

These formats are supported:

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

Important

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



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

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



The context menu contains:

- **Certificate information**: View an installed certificate's properties.
- **Delete certificate**: Delete the certificate.
- **Create certificate signing request**: Create a certificate signing request to send to a registration authority to apply for a digital identity certificate.

Secure keystore  :

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

Cryptographic policy

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

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

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

Network access control and encryption

IEEE 802.1x

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

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

IEEE 802.1AE MACsec

IEEE 802.1AE MACsec is an IEEE standard for media access control (MAC) security that defines connectionless data confidentiality and integrity for media access independent protocols.

Certificates

When configured without a CA certificate, server certificate validation is disabled and the device tries to authenticate itself regardless of what network it is connected to.

When using a certificate, in Axis' implementation, the device and the authentication server authenticate themselves with digital certificates using EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).

To allow the device to access a network protected through certificates, you must install a signed client certificate on the device.

Authentication method: Select an EAP type used for authentication.

Client certificate: Select a client certificate to use IEEE 802.1x. The authentication server uses the certificate to validate the client's identity.

CA certificates: Select CA certificates to validate the authentication server's identity. When no certificate is selected, the device tries to authenticate itself regardless of what network it is connected to.

EAP identity: Enter the user identity associated with the client certificate.

EAPOL version: Select the EAPOL version that is used in the network switch.

Use IEEE 802.1x: Select to use the IEEE 802.1x protocol.

These settings are only available if you use **IEEE 802.1x PEAP-MSCHAPv2** as the authentication method:

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

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

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

Prevent brute-force attacks

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

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

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

Firewall

Firewall: Turn on to activate the firewall.

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

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

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

+ **New rule:** Click to create a rule.

Rule type:

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

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

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

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

Custom signed AXIS OS certificate

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

Install: Click to install the certificate. You need to install the certificate before you install the software.



The context menu contains:

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

Accounts

Accounts



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

Account: Enter a unique account name.

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

Repeat password: Enter the same password again.

Privileges:

- **Administrator:** Has full access to all settings. Administrators can also add, update, and remove other accounts.
- **Operator:** Has access to all settings except:
 - All System settings.



The context menu contains:

Update account: Edit the account properties.

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

Anonymous access

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

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

SSH accounts

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

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

Account: Enter a unique account name.

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

Repeat password: Enter the same password again.

Comment: Enter a comment (optional).

 The context menu contains:

Update SSH account: Edit the account properties.

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

Virtual host

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

Enabled: Select to use this virtual host.

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

Port: Enter the port the server is connected to.

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

 The context menu contains:

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

Disabled: The server is disabled.

Client Credentials Grant Configuration

Admin claim: Enter a value for the admin role.

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

Operator claim: Enter a value for the operator role.

Require claim: Enter the data that should be in the token.

Viewer claim: Enter the value for the viewer role.

Save: Click to save the values.

OpenID Configuration

Important

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

Client ID: Enter the OpenID username.

Outgoing Proxy: Enter the proxy address for the OpenID connection to use a proxy server.

Admin claim: Enter a value for the admin role.

Provider URL: Enter the web link for the API endpoint authentication. Format should be https://[insert URL]/well-known/openid-configuration

Operator claim: Enter a value for the operator role.

Require claim: Enter the data that should be in the token.

Viewer claim: Enter the value for the viewer role.

Remote user: Enter a value to identify remote users. This assists to display the current user in the device's web interface.

Scopes: Optional scopes that could be part of the token.

Client secret: Enter the OpenID password

Save: Click to save the OpenID values.

Enable OpenID: Turn on to close current connection and allow device authentication from the provider URL.

Events

Rules

A rule defines the conditions that triggers the product to perform an action. The list shows all the currently configured rules in the product.

Note

You can create up to 256 action rules.



Add a rule: Create a rule.

Name: Enter a name for the rule.

Wait between actions: Enter the minimum time (hh:mm:ss) that must pass between rule activations. It is useful if the rule is activated by, for example, day-night mode conditions, to avoid that small light changes during sunrise and sunset activate the rule repeatedly.

Condition: Select a condition from the list. A condition must be met for the device to perform an action. If multiple conditions are defined, all of them must be met to trigger the action. For information about specific conditions, see *Get started with rules for events*.

Use this condition as a trigger: Select to make this first condition function only as a starting trigger. It means that once the rule is activated, it remains active for as long as all the other conditions are met, no matter the state of the first condition. If you don't select this option, the rule will simply be active whenever all the conditions are met.

Invert this condition: Select if you want the condition to be the opposite of your selection.



Add a condition: Click to add an additional condition.

Action: Select an action from the list and enter its required information. For information about specific actions, see *Get started with rules for events*.

Recipients

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

Note

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

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

Note

You can create up to 20 recipients.



Add a recipient: Click to add a recipient.

Name: Enter a name for the recipient.

Type: Select from the list:

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

You can add network storage such as NAS (network-attached storage) and use it as a recipient to store files. The files are stored in the Matroska (MKV) file format.

 - **Host:** Enter the IP address or hostname for the network storage.
 - **Share:** Enter the name of the share on the host.
 - **Folder:** Enter the path to the directory where you want to store files.
 - **Username:** Enter the username for the login.
 - **Password:** Enter the password for the login.

- **SFTP** 
 - **Host:** Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
 - **Port:** Enter the port number used by the SFTP server. The default is 22.
 - **Folder:** Enter the path to the directory where you want to store files. If this directory doesn't already exist on the SFTP server, you will get an error message when uploading files.
 - **Username:** Enter the username for the login.
 - **Password:** Enter the password for the login.
 - **SSH host public key type (MD5):** Enter the fingerprint of the remote host's public key (a 32-digit hexadecimal string). The SFTP client supports SFTP servers using SSH-2 with RSA, DSA, ECDSA, and ED25519 host key types. RSA is the preferred method during negotiation, followed by ECDSA, ED25519, and DSA. Make sure to enter the right MD5 host key that is used by your SFTP server. While the Axis device supports both MD5 and SHA-256 hash keys, we recommend using SHA-256 due to stronger security over MD5. For more information on how to configure an SFTP server with an Axis device, go to the *AXIS OS Portal*.
 - **SSH host public key type (SHA256):** Enter the fingerprint of the remote host's public key (a 43-digit Base64 encoded string). The SFTP client supports SFTP servers using SSH-2 with RSA, DSA, ECDSA, and ED25519 host key types. RSA is the preferred method during negotiation, followed by ECDSA, ED25519, and DSA. Make sure to enter the right MD5 host key that is used by your SFTP server. While the Axis device supports both MD5 and SHA-256 hash keys, we recommend using SHA-256 due to stronger security over MD5. For more information on how to configure an SFTP server with an Axis device, go to the *AXIS OS Portal*.
 - **Use temporary file name:** Select to upload files with temporary, automatically generated filenames. The files get renamed to the desired names when the upload completes. If the upload is aborted or interrupted, you don't get any corrupt files. However, you probably still get the temporary files. This way, you know that all files that have the desired name are correct.
- **SIP or VMS**  :
 - SIP:** Select to make a SIP call.
 - VMS:** Select to make a VMS call.
 - **From SIP account:** Select from the list.
 - **To SIP address:** Enter the SIP address.
 - **Test:** Click to test that your call settings works.
- **Email**
 - **Send email to:** Enter the email address to send emails to. To enter multiple addresses, use commas to separate them.
 - **Send email from:** Enter the email address of the sending server.
 - **Username:** Enter the username for the mail server. Leave this field empty if the mail server does not require authentication.
 - **Password:** Enter the password for the mail server. Leave this field empty if the mail server does not require authentication.
 - **Email server (SMTP):** Enter the name of the SMTP server, for example, smtp.gmail.com, smtp.mail.yahoo.com.
 - **Port:** Enter the port number for the SMTP server, using values in the range 0-65535. The default value is 587.
 - **Encryption:** To use encryption, select either SSL or TLS.
 - **Validate server certificate:** If you use encryption, select to validate the identity of the device. The certificate can be self-signed or issued by a Certificate Authority (CA).

- **POP authentication:** Turn on to enter the name of the POP server, for example, pop.gmail.com.

Note

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

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

Test: Click to test the setup.



The context menu contains:

View recipient: Click to view all the recipient details.

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

Delete recipient: Click to delete the recipient permanently.

Schedules

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



Add schedule: Click to create a schedule or pulse.

Manual triggers

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

MQTT

MQTT (Message Queuing Telemetry Transport) is a standard messaging protocol for the Internet of Things (IoT). It was designed for simplified IoT integration and is used in a wide variety of industries to connect remote devices with a small code footprint and minimal network bandwidth. The MQTT client in Axis device software can simplify integration of data and events produced in the device to systems which are not video management software (VMS).

Set up the device as an MQTT client. MQTT communication is based on two entities, the clients and the broker. The clients can send and receive messages. The broker is responsible for routing messages between clients.

You can learn more about MQTT in *AXIS OS Knowledge base*.

ALPN

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

MQTT client

Connect: Turn on or off the MQTT client.

Status: Shows the current status of the MQTT client.

Broker

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

Protocol: Select which protocol to use.

Port: Enter the port number.

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

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

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

Password: Enter a password for the username.

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

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

HTTP proxy: A URL with a maximum length of 255 bytes. You can leave the field empty if you don't want to use an HTTP proxy.

HTTPS proxy: A URL with a maximum length of 255 bytes. You can leave the field empty if you don't want to use an HTTPS proxy.

Keep alive interval: Enables the client to detect when the server is no longer available without having to wait for the long TCP/IP timeout.

Timeout: The time interval in seconds to allow a connect to complete. Default value: 60

Device topic prefix: Used in the default values for the topic in the connect message and LWT message on the MQTT client tab, and in the publication conditions on the **MQTT publication** tab.

Reconnect automatically: Specifies whether the client should reconnect automatically after a disconnect.

Connect message

Specifies if a message should be sent out when a connection is established.

Send message: Turn on to send messages.

Use default: Turn off to enter your own default message.

Topic: Enter the topic for the default message.

Payload: Enter the content for the default message.

Retain: Select to keep the state of client on this Topic

QoS: Change the QoS layer for the packet flow.

Last Will and Testament message

The Last Will Testament (LWT) lets a client provide a testament along with its credentials when connecting to the broker. If the client disconnects ungracefully at some point later (maybe because his power source died), it

can let the broker deliver a message to other clients. This LWT message has the same form as an ordinary message and gets routed via the same mechanics.

Send message: Turn on to send messages.

Use default: Turn off to enter your own default message.

Topic: Enter the topic for the default message.

Payload: Enter the content for the default message.

Retain: Select to keep the state of client on this Topic

QoS: Change the QoS layer for the packet flow.

MQTT publication

Use default topic prefix: Select to use the default topic prefix, that is defined in the device topic prefix in the MQTT client tab.

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

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

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



Add condition: Click to add a condition.

Retain: Defines which MQTT messages are sent as retained.

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

QoS: Select the desired level for the MQTT publication.

MQTT subscriptions



Add subscription: Click to add a new MQTT subscription.

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

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

Subscription type:

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

QoS: Select the desired level for the MQTT subscription.

MQTT overlays

Note

Connect to an MQTT broker before you add MQTT overlay modifiers.



Add overlay modifier: Click to add a new overlay modifier.

Topic filter: Add the MQTT topic that contains the data you want to show in the overlay.

Data field: Specify the key for the message payload that you want to show in the overlay, assuming the message is in JSON format.

Modifier: Use the resulting modifier when you create the overlay.

- Modifiers that start with **#XMP** show all of the data received from the topic.
- Modifiers that start with **#XMD** show the data specified in the data field.

Storage

Network storage

Ignore: Turn on to ignore network storage.

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

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

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

Unbind: Click to unbind and disconnect the network share.

Bind: Click to bind and connect the network share.

Unmount: Click to unmount the network share.

Mount: Click to mount the network share.

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

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

Tools

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

Use tool: Click to activate the selected tool.

Onboard storage

Important

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

Unmount: Click to safely remove the SD card.

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

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

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

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

Tools

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

Use tool: Click to activate the selected tool.

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

Stream profiles

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



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

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

Name: Add a name for your profile.

Description: Add a description of your profile.

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

Resolution: See for a description of this setting.

Frame rate: See for a description of this setting.

Compression: See for a description of this setting.

Zipstream  : See for a description of this setting.

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

Dynamic FPS  : See for a description of this setting.

Dynamic GOP  : See for a description of this setting.

Mirror  : See for a description of this setting.

GOP length  : See for a description of this setting.

Bitrate control: See for a description of this setting.

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

Include audio  : See for a description of this setting.

ONVIF

ONVIF accounts

ONVIF (Open Network Video Interface Forum) is a global interface standard that makes it easier for end-users, integrators, consultants, and manufacturers to take advantage of the possibilities offered by network video technology. ONVIF enables interoperability between different vendor products, increased flexibility, reduced cost and future-proof systems.

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



Add accounts: Click to add a new ONVIF account.

Account: Enter a unique account name.

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

Repeat password: Enter the same password again.

Role:

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



The context menu contains:

Update account: Edit the account properties.

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

ONVIF media profiles

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



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

Profile name: Add a name for the media profile.

Video source: Select the video source for your configuration.

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

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

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

Note

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

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

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

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

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

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

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

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

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

Metadata: Select the metadata to include in your configuration.

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

PTZ  : Select the PTZ settings for your configuration.

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

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

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

profile_x: Click on the profile name to open and edit the preconfigured profile.

Detectors

Camera tampering

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

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

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

Note

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

Audio detection

These settings are available for each audio input.

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

Shock detection

Shock detector: Turn on to generate an alarm if the device is hit by an object or if it is tampered with.

Sensitivity level: Move the slider to adjust the sensitivity level at which the device should generate an alarm. A low value means that the device only generates an alarm if the hit is powerful. A high value means that the device generates an alarm even with mild tampering.

Accessories

I/O ports

Use digital input to connect external devices that can toggle between an open and closed circuit, for example, PIR sensors, door or window contacts, and glass break detectors.

Use digital output to connect external devices such as relays and LEDs. You can activate connected devices through the VAPIX® Application Programming Interface or the web interface.

Port

Name: Edit the text to rename the port.

Direction:  indicates that the port is an input port.  indicates that it's an output port. If the port is configurable, you can click the icons to change between input and output.

Normal state: Click  for open circuit, and  for closed circuit.

Current state: Shows the current state of the port. The input or output is activated when the current state is different from the normal state. An input on the device has an open circuit when it's disconnected or when there is a voltage above 1 VDC.

Note

During restart, the output circuit is open. When the restart is complete, the circuit goes back to the normal position. If you change any settings on this page, the output circuits go back to their normal positions regardless of any active triggers.

Supervised  : Turn on to make it possible to detect and trigger actions if someone tampers with the connection to digital I/O devices. In addition to detecting if an input is open or closed, you can also detect if someone has tampered with it (that is, cut or shorted). To supervise the connection requires additional hardware (end-of-line resistors) in the external I/O loop.

Edge-to-edge

Pairing

Pairing allows you to use a compatible Axis device as if it were part of the main device.

Audio pairing allows you to pair with network speaker or microphone. Once paired, the network speaker acts as an audio out device where you can play audio clips and transmit sound through the camera. The network microphone will take up sounds from the surrounding area and make it available as an audio input device, usable in media streams and recordings.

Important

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

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



Add: Add a device to pair with.

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

Note

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

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

Note

An info icon is shown for devices that have already been paired. Hover over the icon to get information about pairings that are already active.



To pair a device from the list, click .

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

Speaker pairing: Select to pair a network speaker.

Microphone pairing  : Select to pair a microphone.

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

Username: Enter username.

Password: Enter password for the user.

Close: Click to clear all fields.

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

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



Add: Add a device to pair with.

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

Note

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

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

Note

An info icon is shown for devices that have already been paired. Hover over the icon to get information about pairings that are already active.



To pair a device from the list, click .

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

Address: Enter host name or IP address of the PTZ camera.

Username: Enter the username of the PTZ camera.

Password: Enter the password for the PTZ camera.

Close: Click to clear all fields.

Connect: Click to establish connection to the PTZ camera.

Configure radar autotracking: Click to open and configure autotracking. You can also go to **Radar > Radar PTZ autotracking** to configure.

Logs

Reports and logs

Reports

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

Logs

- **View the system log:** Click to show information about system events such as device startup, warnings, and critical messages.
- **View the access log:** Click to show all failed attempts to access the device, for example, when a wrong login password is used.
- **View the audit log:** Click to show information about user and system activities, for example, successful or failed authentications and configurations.

Remote system log

Syslog is a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, which indicates the software type generating the message, and assigned a severity level.



Server: Click to add a new server.

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

Format: Select which syslog message format to use.

- Axis
- RFC 3164
- RFC 5424

Protocol: Select the protocol to use:

- UDP (Default port is 514)
- TCP (Default port is 601)
- TLS (Default port is 6514)

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

Severity: Select which messages to send when triggered.

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

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

CA certificate set: See the current settings or add a certificate.

Plain config

Plain config is for advanced users with experience of Axis device configuration. Most parameters can be set and edited from this page.

Maintenance

Maintenance

Restart: Restart the device. This does not affect any of the current settings. Running applications restart automatically.

Restore: Return most settings to the factory default values. Afterwards you must reconfigure the device and apps, reinstall any apps that didn't come preinstalled, and recreate any events and presets.

Important

The only settings saved after restore are:

- Boot protocol (DHCP or static)
- Static IP address
- Default router
- Subnet mask
- 802.1X settings
- O3C settings
- DNS server IP address

Factory default: Return all settings to the factory default values. Afterwards you must reset the IP address to make the device accessible.

Note

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

AXIS OS upgrade: Upgrade to a new AXIS OS version. New releases can contain improved functionality, bug fixes, and completely new features. We recommend you to always use the latest AXIS OS release. To download the latest release, go to axis.com/support.

When you upgrade, you can choose between three options:

- **Standard upgrade:** Upgrade to the new AXIS OS version.
- **Factory default:** Upgrade and return all settings to the factory default values. When you choose this option, you can't revert to the previous AXIS OS version after the upgrade.
- **Automatic rollback:** Upgrade and confirm the upgrade within the set time. If you don't confirm, the device reverts to the previous AXIS OS version.

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

Troubleshoot

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

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

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

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

Network trace

Important

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

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

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

Learn more

Long-distance connections

This product supports fiber-optic cable installations through a media converter. Fiber-optic cable installations offer a number of benefits such as:

- Long-distance connection
- High speed
- Long lifetime
- Large capacity of data transmission
- Electromagnetic interference immunity

Find out more about fiber-optic cable installations in the white paper "Long distance surveillance - Fiber-optic communication in network video" at axis.com/learning/white-papers.

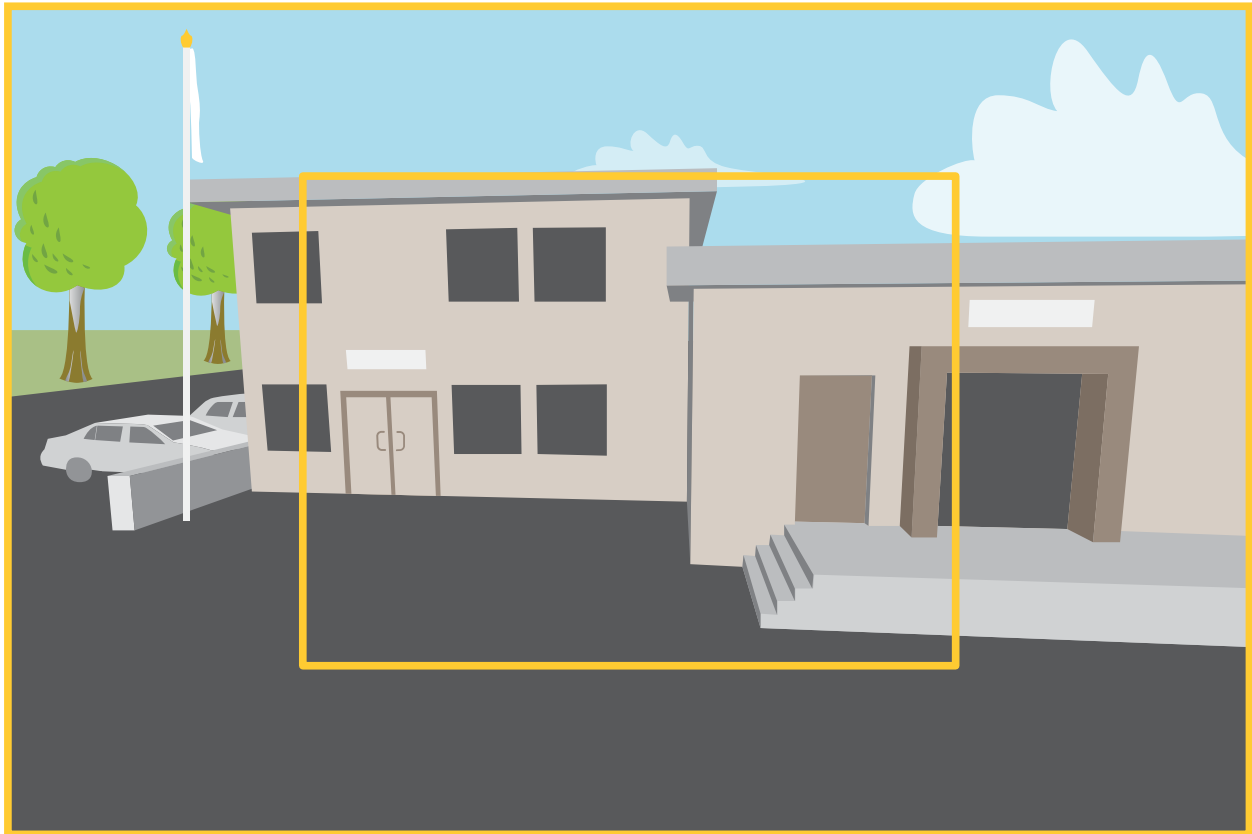
For information about how to install the media converter see the Installation Guide for this product.

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.

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.

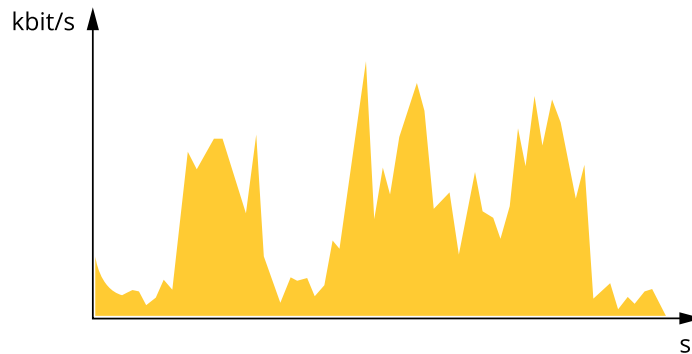
The **Stream profiles** settings override the settings from the **Stream** tab. If you request a stream with a specific stream profile, the stream contains the settings of that profile. If you request a stream without specifying a stream profile, or request a stream profile that doesn't exist in the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

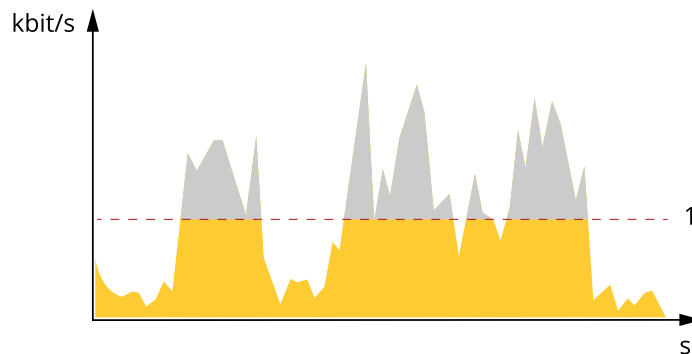
Variable bitrate (VBR)

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.

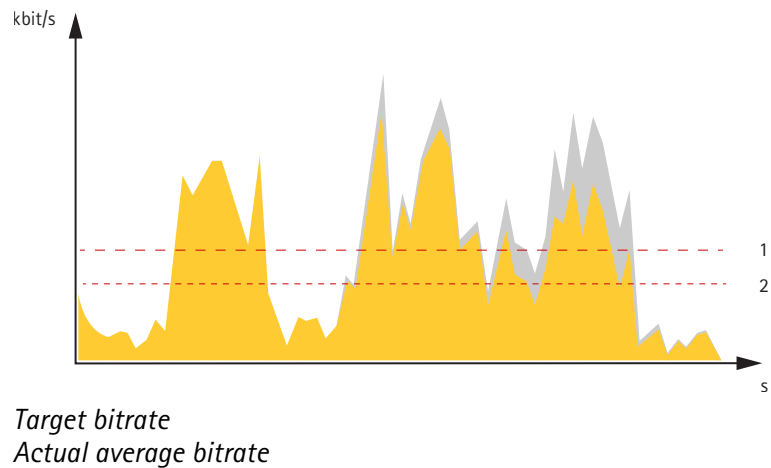


1 Target bitrate

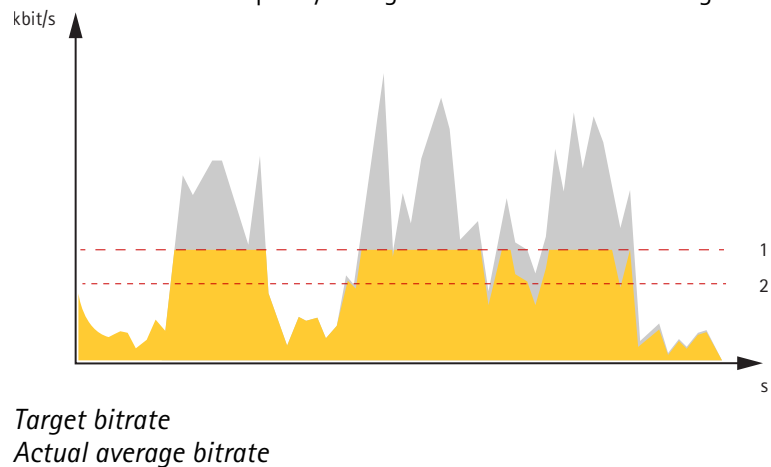
Average bitrate (ABR)

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.



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



Applications

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

To find the user manuals for Axis applications, go to help.axis.com.

Note

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

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*.

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*.

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.

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.

TPM module

The TPM (Trusted Platform Module) is a component that provides cryptographic features to protect information from unauthorized access. It is always activated and there are no settings you can change.

Axis device ID

Being able to verify the origin of the device is key to establishing trust in the device identity. During production, devices with Axis Edge Vault are assigned a unique, factory-provisioned, and IEEE 802.1AR-compliant Axis device ID certificate. This works like a passport to prove the origin of the device. The device ID is securely and permanently stored in the secure keystore as a certificate signed by Axis root certificate. The device ID can be leveraged by the customer's IT infrastructure for automated secure device onboarding and secure device identification.

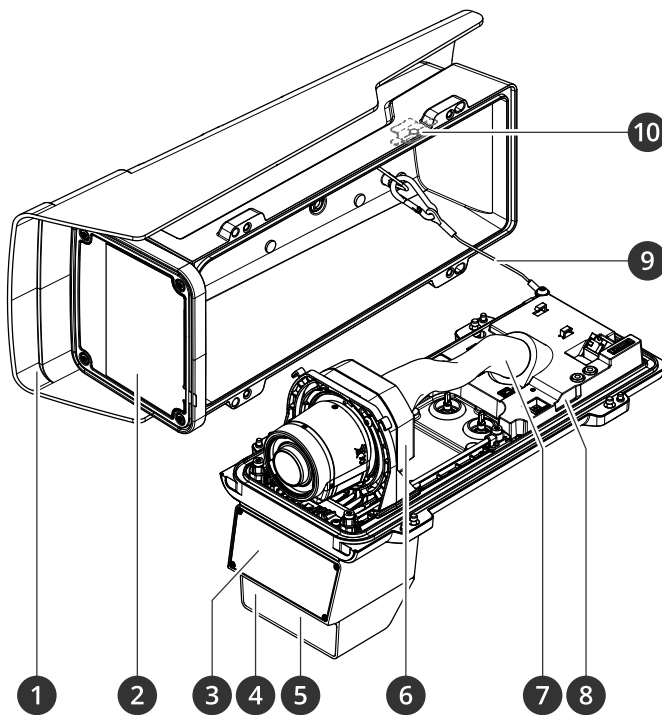
Signed video

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.

Specifications

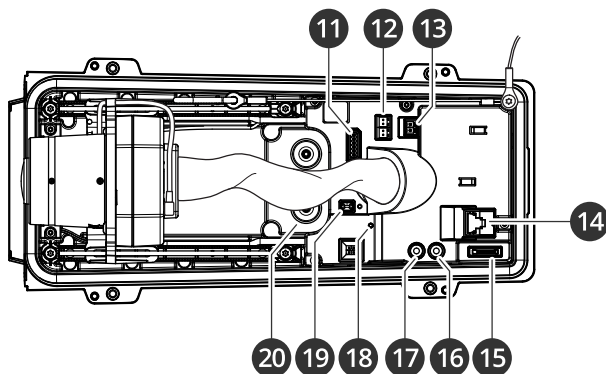
Product overview



- 1 Weather shield
- 2 Window
- 3 Radar
- 4 Light sensor
- 5 IR illumination LED
- 6 Optical unit
- 7 Cable cover
- 8 Intrusion alarm sensor
- 9 Safety wire
- 10 Intrusion alarm magnet

NOTICE

Do not lift the product in the cable cover.



- 1 I/O connector
- 2 RS485/422 connector
- 3 Power connector
- 4 Network connector (PoE)
- 5 microSD card slot
- 6 Audio out

- 7 Audio in
- 8 Status LED
- 9 Control button
- 10 Cable gasket M20 (2x)

LED indicators

Note

- The Status LED can be configured to flash while an event is active.
- The LEDs turn off when you close the casing.

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

Buzzer

Buzzer signal for focus assistant

Note

Only valid for optional P-iris, DC-iris or manual iris lenses.

Buzzer	Lens
Fast interval	Optimally adjusted
Medium interval	Less optimally adjusted
Slow interval	Poorly adjusted

SD card slot

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 .
- Connecting to a one-click cloud connection (O3C) service over the internet. To connect, press and release the button, then wait for the status LED to flash green three times.

Intrusion alarm switch

Use the intrusion alarm switch to get a notification when someone opens the device's housing. Create a rule to make the device perform an action when the switch is activated. See .

Connectors

Network connector

RJ45 Ethernet connector with Power over Ethernet Plus (PoE+).

Audio connector

- **Audio in** – 3.5 mm input for a mono microphone, or a line-in mono signal (left channel is used from a stereo signal).
- **Audio in** – 3.5 mm input for a digital microphone, an analog mono microphone, or a line-in mono signal (left channel is used from a stereo signal).
- **Audio out** – 3.5 mm output for audio (line level) that can be connected to a public address (PA) system or an active speaker with a built-in amplifier. A stereo connector must be used for audio out.



Audio input

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

Audio output

1 Tip	2 Ring	3 Sleeve
Channel 1, unbalanced line, mono	Channel 1, unbalanced line, mono	Ground

I/O connector

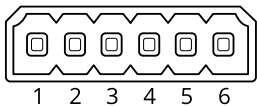
Use the I/O connector with external devices in combination with, for example, motion detection, event triggering, and alarm notifications. In addition to the 0 VDC reference point and power (12 V DC output), the I/O connector provides the interface to:

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

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

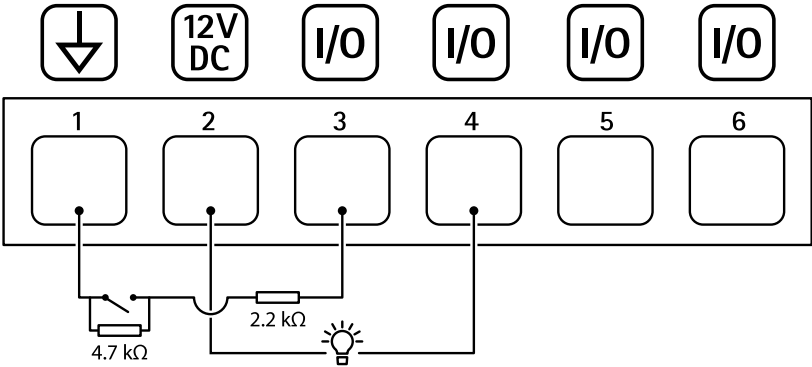
Digital output – For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface, through an event or from the device's web interface.

6-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 = 50 mA
Configurable (Input or Output)	3–6	Digital input or Supervised input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. To use supervised input, install end-of-line resistors. See connection diagram for information about how to connect the resistors.	0 to max 30 VDC
		Digital output – 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

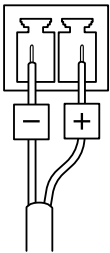
Example:



- 1 DC ground
- 2 DC output 12 V, max 50 mA
- 3 I/O configured as supervised input
- 4 I/O configured as output
- 5 Configurable I/O
- 6 Configurable I/O

Power connector

2-pin terminal block for DC power input. Use a Safety Extra Low Voltage (SELV) compliant limited power source (LPS) with either a rated output power limited to ≤100 W or a rated output current limited to ≤5 A.

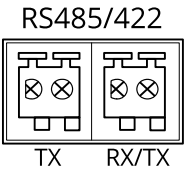


RS485/RS422 connector

Two 2-pin terminal blocks for RS485/RS422 serial interface.

The serial port can be configured to support:

- Two-wire RS485 half duplex
- Four-wire RS485 full duplex
- Two-wire RS422 simplex
- Four-wire RS422 full duplex point to point communication



Function	Notes
RS485/RS422 TX(A)	TX pair for RS422 and 4-wire RS485
RS485/RS422 TX(B)	
RS485A alt RS485/422 RX (A)	RX pair for all modes (combined RX/TX for 2-wire RS485)
RS485B alt RS485/422 RX (B)	

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.

To reset the product to the factory default settings:

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

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

AXIS OS options

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

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

Check the current AXIS OS version

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

To check the current AXIS OS version:

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

Upgrade AXIS OS

Important

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

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.

Technical issues, clues, and solutions

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

Problems upgrading AXIS OS

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

Problems setting the IP address

The device is located on a different subnet	If the IP address intended for the device and the IP address of the computer used to access the device are located on different subnets, you cannot set the IP address. Contact your network administrator to obtain an IP address.
The IP address is being used by another device	Disconnect the Axis device from the network. Run the ping command (in a Command/DOS window, type <code>ping</code> and the IP address of the device): • If you receive: <code>Reply from <IP address>: bytes=32; time=10...</code> this means that the IP address may already be in use by another device on the network. Obtain a new IP address from the network administrator and reinstall the device. • If you receive: <code>Request timed out</code>, this means that the IP address is available for use with the Axis device. Check all cabling and reinstall the device.
Possible IP address conflict with another device on the same subnet	The static IP address in the Axis device is used before the DHCP server sets a dynamic address. This means that if the same default static IP address is also used by another device, there may be problems accessing the device.

The device can't be accessed from a browser

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

The device is accessible locally but not externally

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

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

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

Can't connect over port 8883 with MQTT over SSL

The firewall blocks traffic using port 8883 as it's deemed insecure.	In some cases the server/broker might not provide a specific port for MQTT communication. It may still be possible to use MQTT over a port normally used for HTTP/HTTPS traffic. • If the server/broker supports WebSocket/WebSocket Secure (WS/WSS), typically on port 443, use this protocol instead. Check with the server/broker provider to see if WS/WSS is supported and which port and basepath to use. • If the server/broker supports ALPN, the use of MQTT can be negotiated over an open port, such as 443. Check with your server/broker provider to see if ALPN is supported and which ALPN protocol and port to use.
--	---

Problems with the radar-video fusion

The bounding box is not covering the object precisely	If there is no video analytics detection, the camera will show the projection of the radar detection in the image, which is not as accurate as a video analytics bounding box. It could also be due to elevation differences in the scene, like a sloping road, a hill, or a depression. If the box is too high or low, make sure that the installation height is set correctly. You can also improve the accuracy of the bounding boxes with the autocalibration feature. To use autocalibration, go to Radar > Autocalibration.
The bounding box shows 1 person when in reality there are 2 people	If two people are walking close together and are only detected by the radar, they will be classified as one person and only one bounding box will appear. When they enter the analytics fusion zone, they will be accurately classified.

The bounding box shift its position when tracking an object	When both radar and camera analytics detect the same object, or if only the camera analytics detects the object, the bounding box will be tightly drawn around the object using the camera information. If the video detection is lost, the bounding box will be drawn at the position of the radar projection, which is less accurate. Once the video detection is picked up again, the bounding box will be drawn in the correct position again. You can also improve the accuracy of the bounding boxes with the autocalibration feature. To use autocalibration, go to Radar > Autocalibration.
I don't get the same detection distance as the manual says	There are several factors that affect the detection distance: • Check that the correct height is entered in the settings. • Depending on the approaching angle of the object towards the installation point, the detection distance can vary. At the outer parts of the field of view, the detection sensitivity is lower from a radar perspective. Consider aiming AXIS Q1656-DLE towards the direction where the intruder is expected to get the furthest distance.
How can I minimize false alarms?	Some tips to minimize false alarms: • Make sure that the scene is well lit to maximize the detection probability of the video analytics • Set the sensitivity to Low in AXIS Object Analytics. This requires that video and radar analytics agree before triggering an alarm. • Use exclude areas in the radar to ignore known sources of false detections, such as swaying vegetation, and buildings. • Configure the radar to use low sensitivity. • Use exclude areas in AXIS Object Analytics • Keep the grass in the site short.
Radar interference	The device uses one of two radar channels. Within each channel, up to four radars can negotiate how to best use that frequency. Sometimes you may see a warning message about interference from the camera, despite this functionality. You can then manually select a channel for each device. Devices that are physically close to each other should be set to the same channel. This makes it easier for the devices to avoid interference.

Performance considerations

The following factors are the most important to consider:

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

Contact support

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

T10180975

2025-09 (M24.2)

© 2022 – 2025 Axis Communications AB