AXIS D21-VE Radar Series

AXIS D2122-VE Radar
AXIS D2123-VE Radar

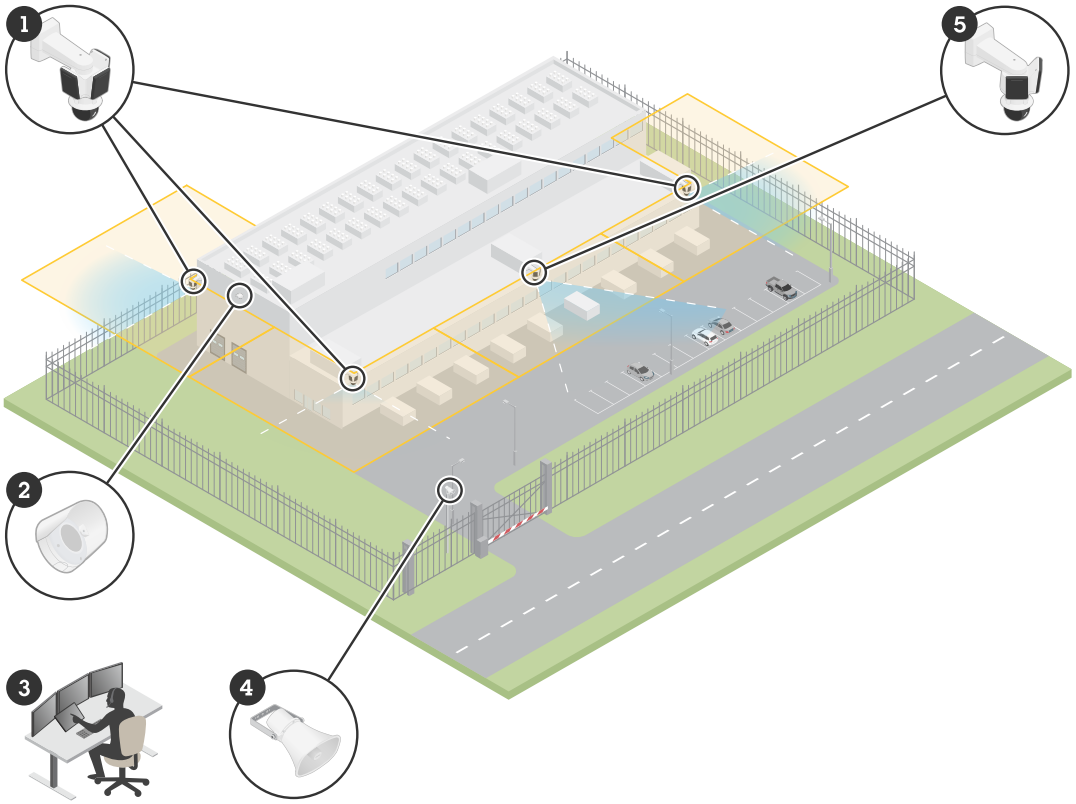
User manual

Table of Contents

Solution overview 4
Installation 5
Considerations 5
Monitor the scene 5
Install multiple radars 5
Recognition and detection distances 9
Use cases 11
Get started 14
Find the device on the network 14
Browser support 14
Open the device's web interface 14
Create an administrator account 14
Secure passwords 15
Configure your device 16
Set the mounting height 16
Set the number of neighboring radars 16
Add a map for reference 16
Create a scenario for detecting objects 17
Minimize false alarms 18
Validate your installation 18
Validate the installation of the radar 18
Complete the validation 19
Adjust the radar image 20
Show an image overlay 20
View and record video 20
Record and watch video 20
Set up rules for events 21
Trigger an action 21
Activate a sweeping red light on the radar 21
Send an email if someone covers the radar with a metallic object 21
The web interface 23
Status 23
Radar 24
Settings 24
Stream 26
Map calibration 26
Exclusion zones 27
Scenarios 28
Overlays 29
Dynamic LED strip 31
Analytics 31
Metadata configuration 31
Recordings 31
Apps 33
System 33
Time and location 33
Network 35
Security 39
Accounts 44
Events 46
MQTT 50
Storage 54
Stream profiles 58

ONVIF....59
Detectors....62
Power settings....62
Power meter....62
Edge-to-edge....63
Logs....64
Plain config....65
Maintenance....66
Maintenance....66
Troubleshoot....67
Learn more....68
Radar....68
Recognition and detection zones....68
Scenarios, inclusion zones, and exclusion zones....68
Coexistence zone....68
Radar-video fusion technology....69
Autotracking....69
Overlays....69
Streaming and storage....69
Video compression formats....69
Bitrate control....70
Edge-to-edge technology....72
Speaker pairing....72
Microphone pairing....72
Cybersecurity....72
Axis security notification service....72
Vulnerability management....72
Secure operation of Axis devices....72
Specifications....73
Product overview....73
LED indicators....73
....73
SD card slot....74
Buttons....74
Control button....74
Connectors....74
Network connector (PoE in)....74
Network connector (PoE out)....74
Clean your device....75
Troubleshooting....76
Reset to factory default settings....76
Make sure that no one has tampered with the device software....76
AXIS OS options....76
Check the current AXIS OS version....76
Upgrade AXIS OS....77
Technical problems and possible solutions....77
Performance considerations....79
Contact support....79

Solution overview



An example of the surveillance solution at a data center.

1 *AXIS D2123–VE Radar paired with AXIS Q6358-LE PTZ camera*
2 *AXIS D4200–VE Strobe speaker*
3 *Surveillance center*
4 *AXIS C1310-E horn speaker*
5 *AXIS D2122–VE Radar paired with AXIS Q6358-LE PTZ camera*

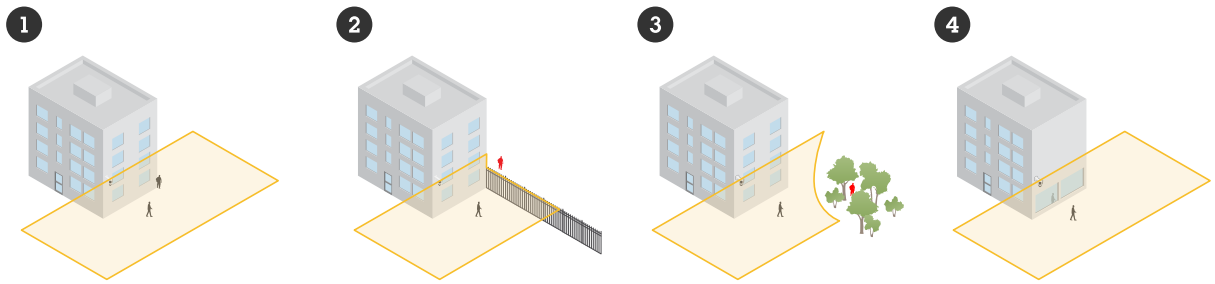
Installation

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

This video is an example on how to install AXIS D21-VE Radar series. For instructions on all installation scenarios and safety information, see the installation guide.

Considerations

- The radar is intended for monitoring open areas (1). Any solid object such as a wall, fence, tree, or large bush in the scene creates a blind spot, a so-called radar shadow, behind it (2, 3). The mounting height affects the size of the radar shadow.
- For more complex scenes, where for example reflective surfaces are present, we recommend radar-video fusion technology with selected PTZ cameras.
- The radar works best if the ground is covered by a paved surface such as asphalt. When the ground is covered by gravel or grass, the detection performance can be affected.
- If you install the radar on a wall, make sure there are no other objects or installations within one meter (three feet) to the left or right of the radar. Such objects can reflect radio waves which can affect the radar's performance.
- If you install the radar on a pole, make sure the pole is stable. The radar has a stabilization mechanism that you can enable, but it can affect the radar sensitivity or the time it takes to detect a moving object.
- A metal object or a reflective surface in the scene can reflect humans or vehicles that move close to it and cause a reflected radar track, or ghost track (4). This can affect the radar's ability to perform accurate classifications and result in false alarms. You can use exclusion zones to filter out such reflections. You can also minimize the impact of reflections if you pair a camera with the radar.
- The recommended mounting height is listed in the device's datasheet at *axis.com*.

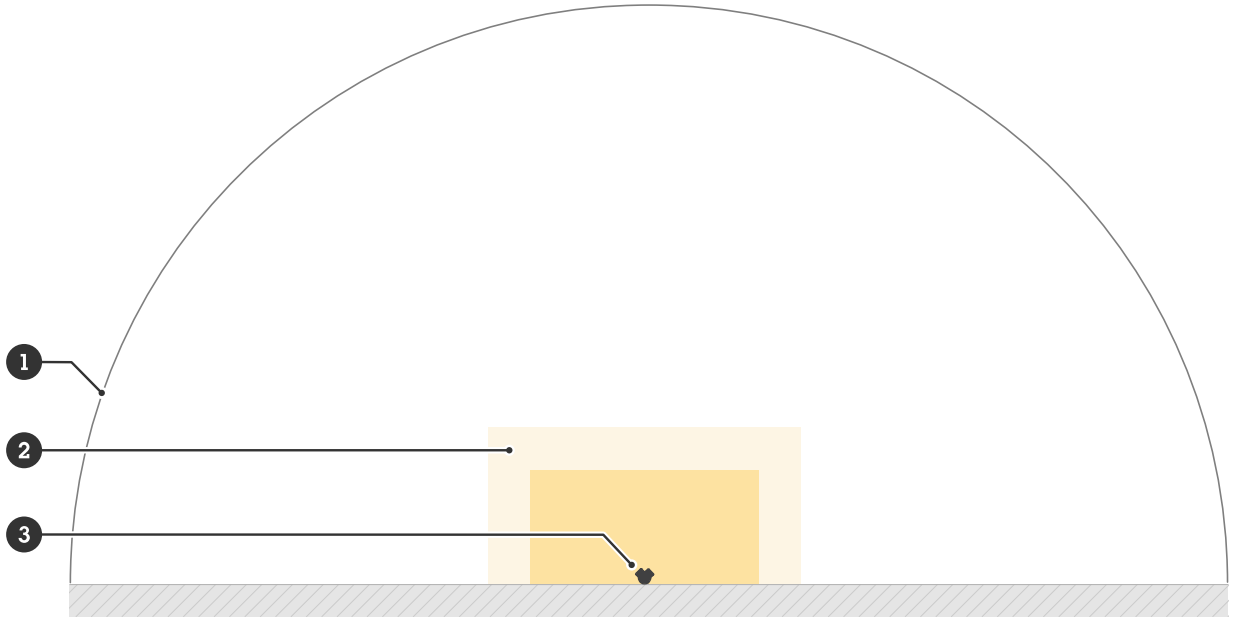


Monitor the scene

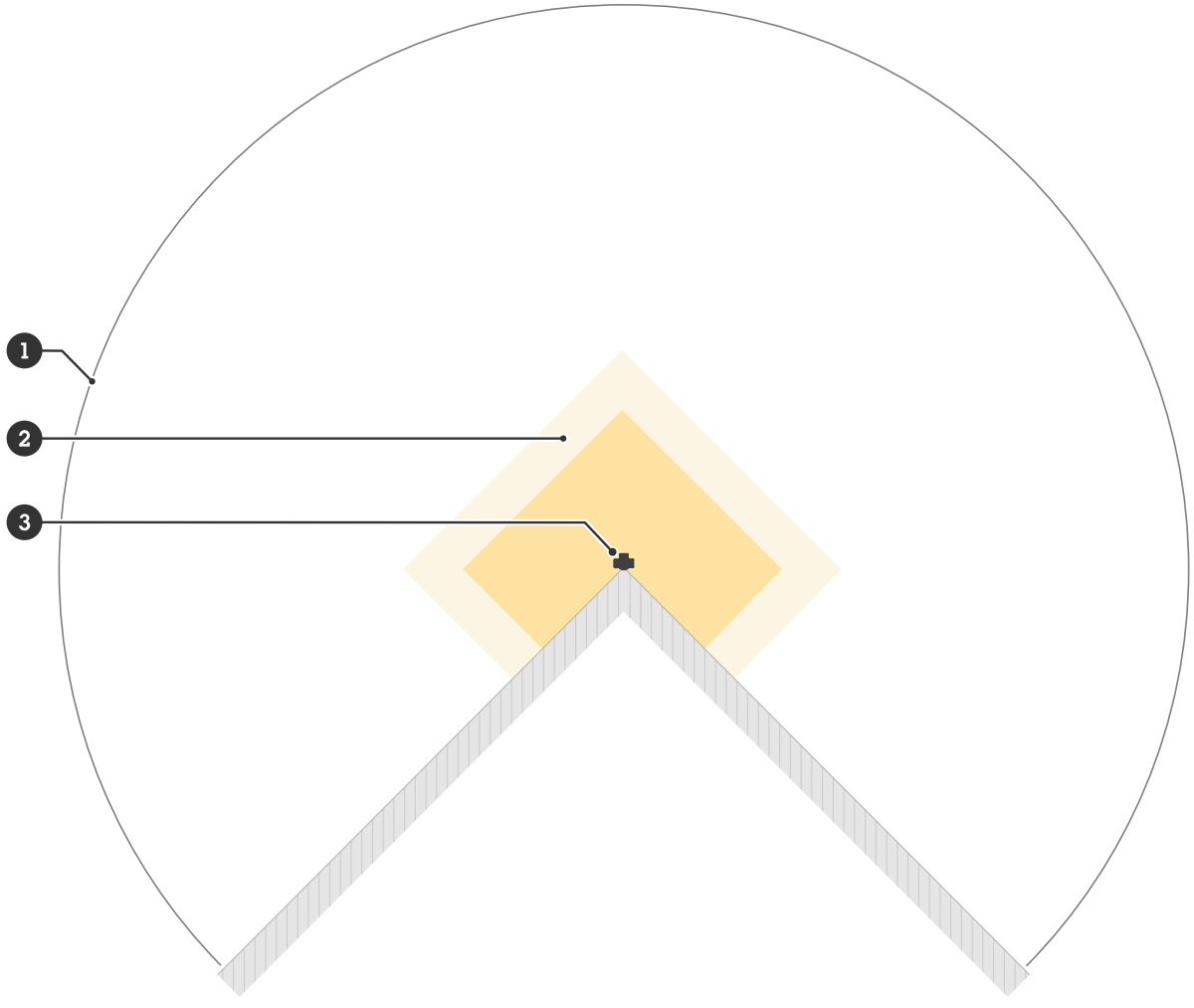
The radar can detect moving objects and classify them as humans, vehicles or unknown. When you monitor an area, use the **Area monitoring** profile.

Install multiple radars

To monitor areas such as the surroundings of a building or the buffer zone outside a fence, you can install multiple radars near each other. Each radar can coexist with up to eleven other AXIS D2122-VE or AXIS D2123-VE radars within a 500-meter (1640 feet) radius, which forms the coexistence zone. You can also install this radar model in the coexistence zone of previous Axis radar models, as they don't interfere with each other. For more information about the coexistence zone, see .



1 *Coexistence zone*
2 *Detection zone*
3 *Axis D2122–VE Radar*



1 *Coexistence zone*

2 *Detection zone*
3 *Axis D2123–VE Radar*

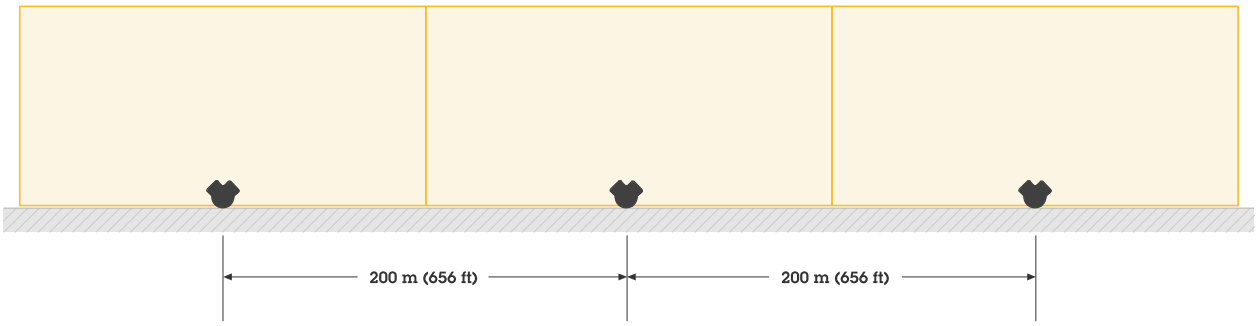
Note

The performance of the radar in the coexistence zone can be affected by the environment and the radar's direction toward fences, buildings, or neighboring radars.

Installation examples

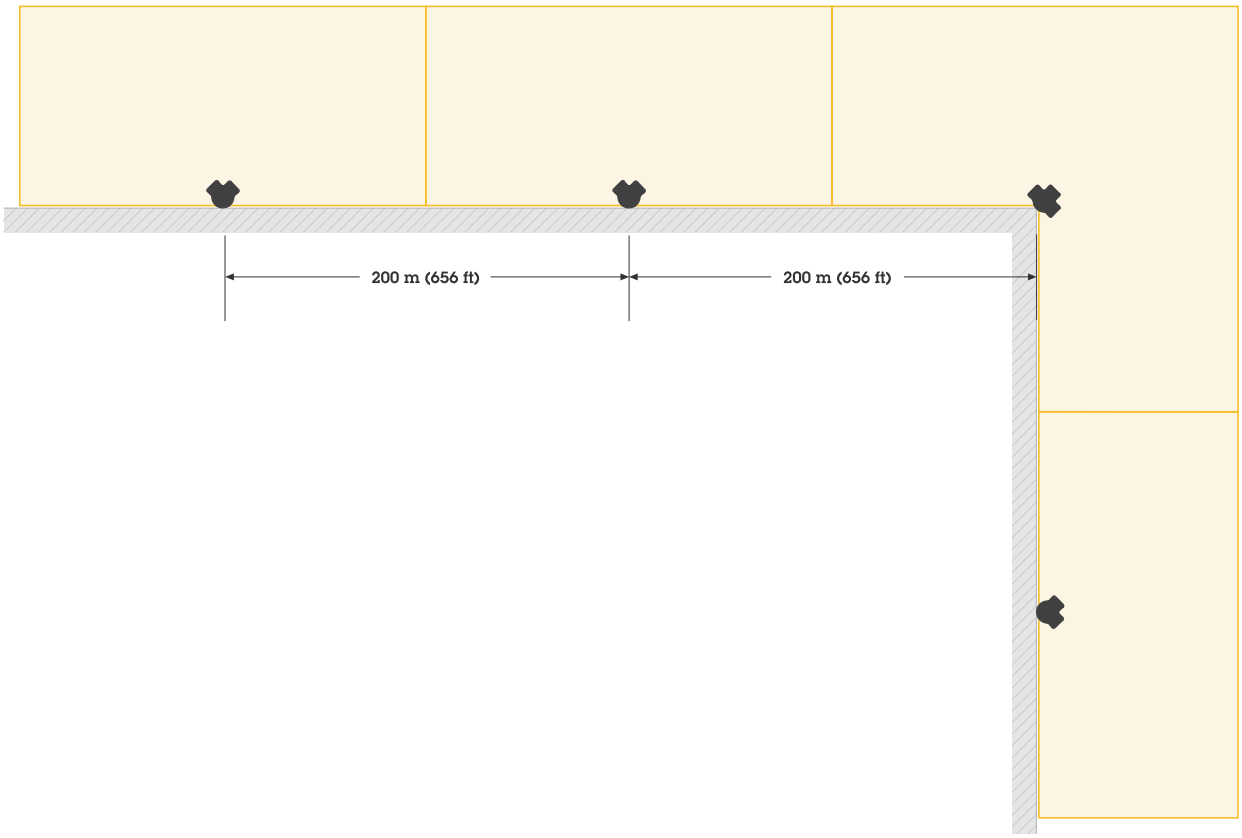
Create a virtual fence with multiple radars

To create a virtual fence, for example along a building, place multiple radars side-by-side. We recommend that you place them with 200 m (656 ft) spacing.



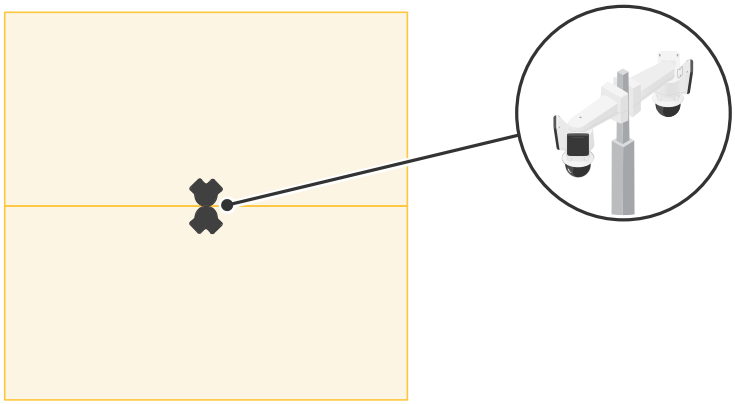
Cover an area around a building

To monitor an area around a building, place radars on the walls of the building facing outwards.



Cover an open area

To monitor a large open area, use two pole mounts to install two AXIS D2122-VE Radars back-to-back.

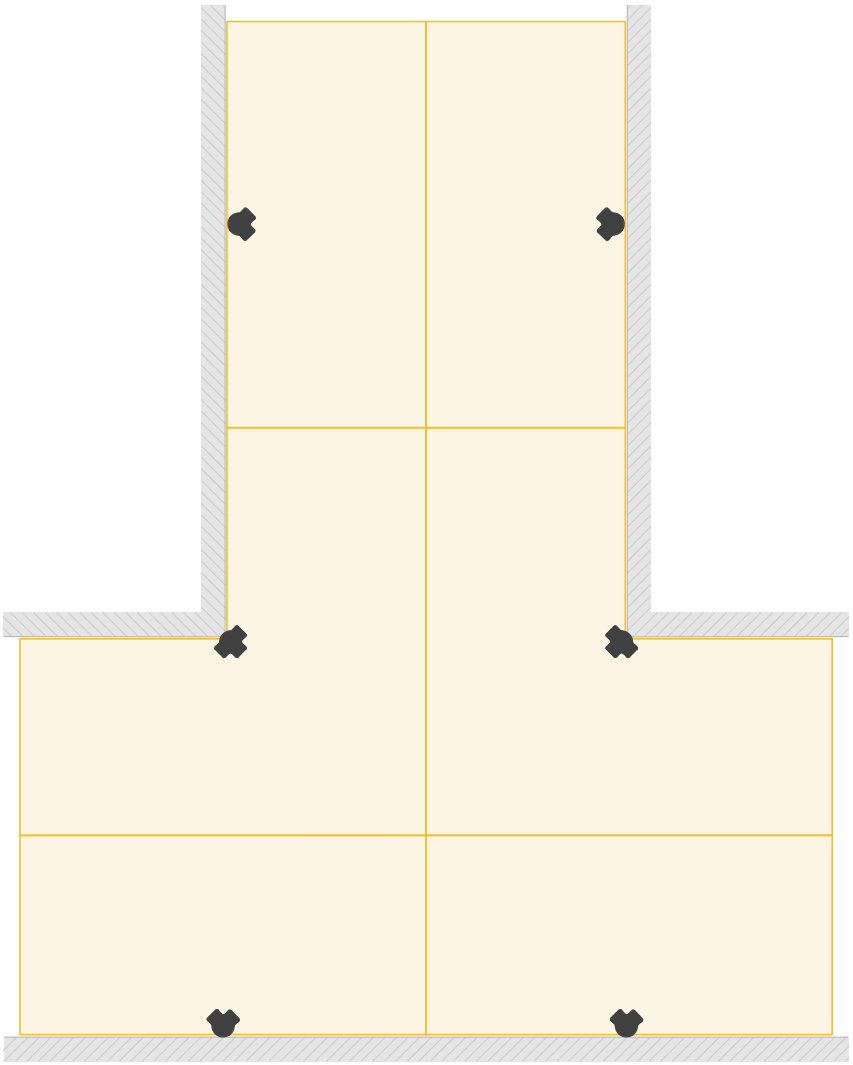


Note

Each radar can provide up to 60 W PoE output when the radar is powered by a 90 W midspan. PoE out requires Power over Ethernet IEEE 802.3bt, Type 4 Class 8.

Install multiple radars facing each other

To monitor an area for example between buildings, place radars facing each other. There can be up to 12 radars facing each other in the same coexistence zone.

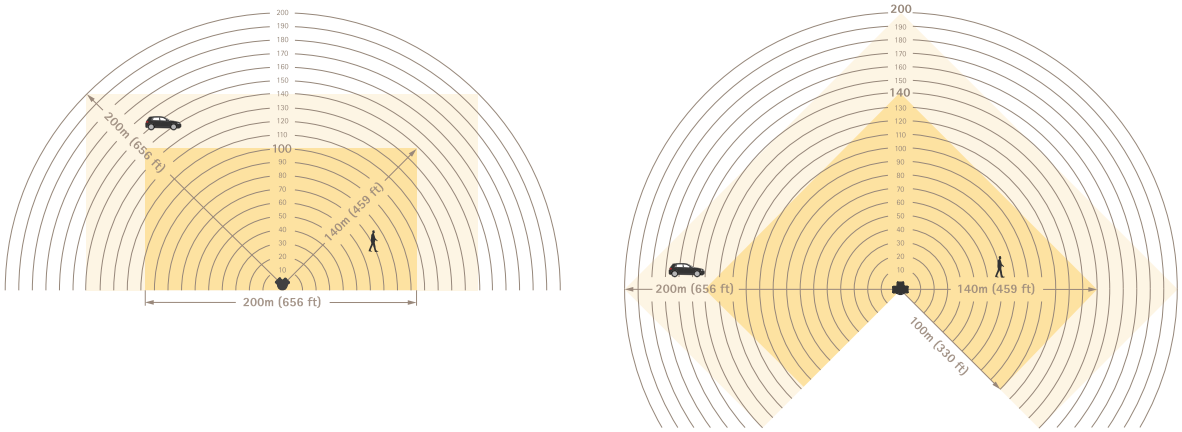


Recognition and detection distances

When the radar is mounted at the optimal installation height:

- In the recognition zone, you can detect and classify humans at a maximum distance of 100–140 meters (330–459 feet) from the radar, depending on the human's position in relation to the radar.
- In the detection zone, you can detect vehicles at a maximum distance of 140–200 meters (459–656 feet) from the radar, depending on:
  - the vehicle's speed
  - the vehicle's direction in relation to the radar
  - the flatness of the ground
  - the ground material

For more information about the zones, see .



Recognition and detection distances

Note

- Enter the actual mounting height in the device's web interface when you calibrate the radar.
- The recognition and detection distances are affected by the scene.
- The recognition and detection distances are different for different object types.

The recognition and detection distances were measured in the following conditions:

- The distance was measured on flat, horizontal ground.
- The radar was mounted with no tilt.
- The object was a 170 cm (5 ft 7 in) tall person.
- There was a clear line of sight from the radar to the person.
- The radar sensitivity was set to **Medium**.

The radar can't detect objects that are closer than the minimum detection distance. The minimum detection distance depends on the radar's mounting height:

Mounting height	Minimum detection distance
4 m (9.8 ft)	4 m (9.8 ft)
5 m (16.4 ft)	6 m (19.7 ft)
6 m (19.7 ft)	8 m (26 ft)
7 m (23 ft)	11 m (36 ft)
8 m (26 ft)	13 m (42.7 ft)
9 m (29.5 ft)	15 m (49.2 ft)
10 m (32.8.5 ft)	18 m (59 ft)

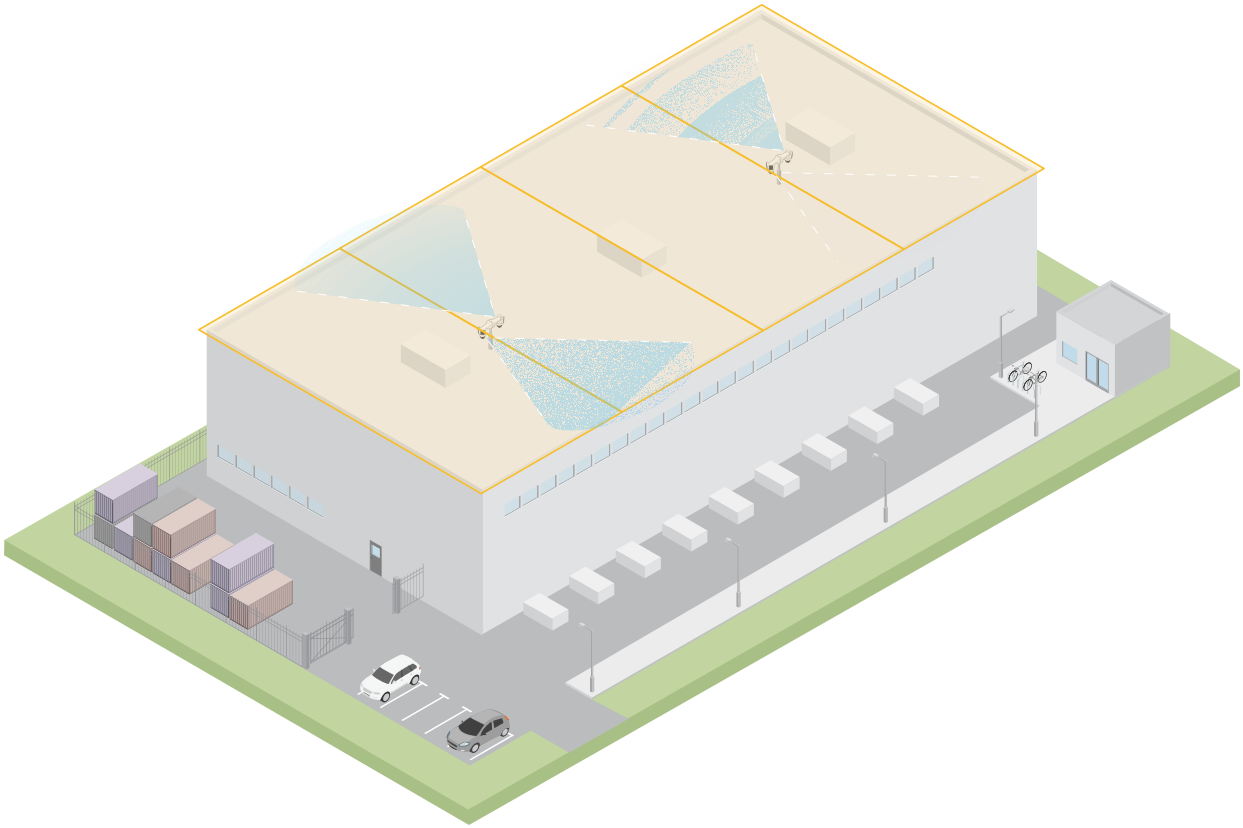
Note

When you pair the radar with a PTZ camera, the camera can continue tracking an object even within the radar's minimum detection distance.

Use cases

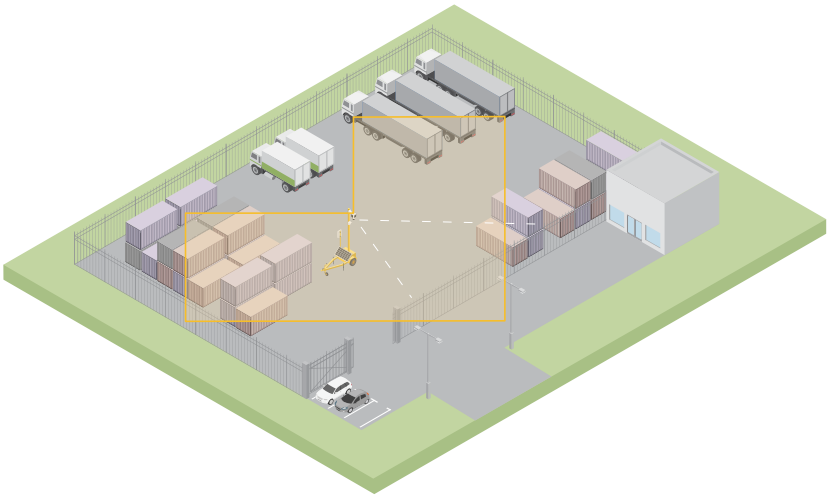
Rooftop area coverage

A large distribution center wants to use radars to cover the rooftop area. The radars are paired with ARTPEC-9 PTZ cameras and mounted back-to-back on poles, covering the whole rooftop. The radar discovers and classifies moving objects on the roof, and directs the camera to the object and lets the camera validate the classification. The camera uses autotracking to continue tracking the object.



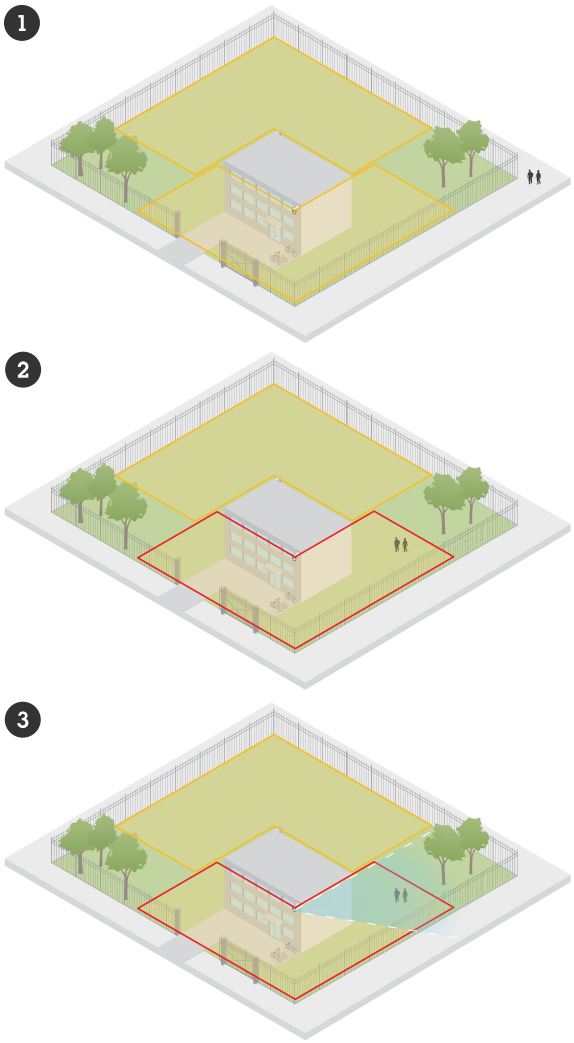
Use a mobile surveillance trailer to cover a large open area

The outdoor yard of a hardware store has had several break-ins after-hours. There is one security guard on duty at a time, but there is a need to bolster the security at night without the added cost of hiring more staff. They have decided to install two radars mounted back-to-back on a mobile surveillance trailer to cover the entire yard. The radars are configured to alert the on-duty security guard of suspicious behavior so that the guard can investigate the scene. They also consider installing a strobe speaker that is triggered by the radars to deter intruders.



Cover a fenced building

In the following scenario, a PTZ camera has been mounted with the radar to validate alarms and provide accurate classification thanks to radar-video-fusion technology.



1. Intruders are walking outside the fence, not triggering an alarm.
2. Intruders break in through the fence, the radar discovers them and triggers an alarm.
3. The radar directs the PTZ camera towards the intruders, and lets the camera validate the alarm with video analytics.

For more information, see .

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.

Configure your device

To get the most out of your device, we recommend that you go through the following steps:

1.
2. If you install several radars close to each other:
3.
4.
5.
6.

Set the mounting height

Set the radar's mounting height in the web interface. The correct mounting height is important for the radar to be able to detect and measure the speed of passing objects correctly. It's also very important for autotracking to work.

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

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

Set the number of neighboring radars

If you install other radars of the same model in this radar's coexistence zone, define the number of neighboring radars in the web interface of each radar. This improves the performance of the radars and minimizes the risk of interference.

1. Go to **Radar > Settings > Coexistence**.
2. Select the number of neighboring radars in this radar's coexistence zone.

Add a map for reference

To make it easier to set up scenarios and to understand where in the scene objects are moving, you can choose to use a map as a background to the radar stream. You can use a ground plan or an aerial photo that shows the area covered by the radar. Adjust and calibrate the map so the radar view 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 scene.

You can use either 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 calibrates 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 at 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 doesn't alter the radar's view. Even if parts of the view aren't visible after zooming, the radar still detects moving objects in the entire view. The only way to exclude detected movement is to add exclusion zones.
- You can adjust the pan and zoom at any time from the **Map calibration**, **Exclusion zones**, or **Scenarios** pages by clicking .

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.

Create a scenario for detecting objects

With a scenario, you can detect or recognize objects that move in the scene. To trigger actions when the conditions in your scenario are fulfilled, create a rule in **Events**. You can create several scenarios to detect different behaviors or cover different parts of the scene.

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 that move inside an area or on objects that cross a line.
5. Click **Next**.
6. For **Movement in area** scenarios:
   6.1. Select the zone shape.
   Use the mouse to move and adjust the zone to cover the desired part of the radar view or reference map.
7. For **Line crossing** scenarios:
   7.1. Position the line in the scene.
   Use the mouse to move and adjust the line.
   7.2. To change the detection direction, turn on **Change direction**.
   7.3. To require the object to cross two lines to trigger actions, turn on **Require crossing of two lines**. Position the second line in the scene.
8. Click **Next**.
9. Add detection settings.
   9.1. For **Movement in area** scenarios and **Line crossing** scenarios with one line, add a delay time to minimize false alarms in **Ignore short-lived objects**.
   9.2. For **Line crossing** scenarios with two lines, set the time limit between crossing the first and the second line under **Max time between crossings**.
   9.3. Select which object type to trigger on under **Trigger on object type**.
   9.4. Add a range for the speed under **Speed limit**.

10. Click **Next**.
11. Set the minimum duration of the alarm under **Minimum trigger duration**.
    For **Line crossing** scenarios, lower the duration to 0 seconds if you want objects to trigger actions as soon as they cross the line.
12. Click **Save**.

Minimize false alarms

If you get many false alarms, you can try to minimize them by changing different settings. For example, you can filter out certain types of movement or objects, adjust the zones where objects trigger alarms, or adjust the detection sensitivity.

- Adjust the detection sensitivity of the radar:
  Go to **Radar > Settings > Detection** and lower the **Detection sensitivity**.
  The sensitivity setting affects all zones.
  - A lower detection sensitivity is suitable when there are many metal objects or large vehicles in the scene. It reduces the risk of false alarms, but also the radar's capability to classify small objects.
  - A higher detection sensitivity is suitable for an open scene, like a field, without metal objects.
- Modify inclusion and exclusion zones:
  Hard surfaces in the scene can cause reflections that result in multiple detections for a single physical object. You can either adjust the shape of the inclusion zone in the scenario, or add a generic exclusion zone to ignore a certain part of the scene.
- Trigger on objects crossing two lines instead of one:
  If the scene in a line-crossing scenario contains swaying objects or animals, there is a risk that such an object crosses the line and triggers a false alarm. In this case, you can adjust the scenario to trigger only when an object has crossed two lines.
- Filter on certain movement:
  - To minimize false alarms caused by trees, bushes, and flags in the scene, go to **Radar > Settings > Detection** and turn on **Ignore swaying objects**.
  - To minimize false alarms caused by small objects, such as cats and rabbits, in the scene, go to **Radar > Settings > Detection** and turn on **Ignore small objects**. This setting is available in the area monitoring profile.
- Filter on time:
  - Go to **Radar > Scenarios**.
  - Select a scenario, and click ⋮ to modify its settings.
  - Increase **Seconds until trigger**. This is the delay time from when the radar starts tracking an object until it can trigger an alarm. The timer starts when the radar detects the object, not when the object enters the inclusion 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, clear the object types that should not trigger alarms in the scenario.

Validate your installation

Validate the installation of the radar

Before you start using the radar, we recommend that you validate the installation. The validation can help you identify problems with the installation or manage static objects such as trees or reflective surfaces in the scene.

Note

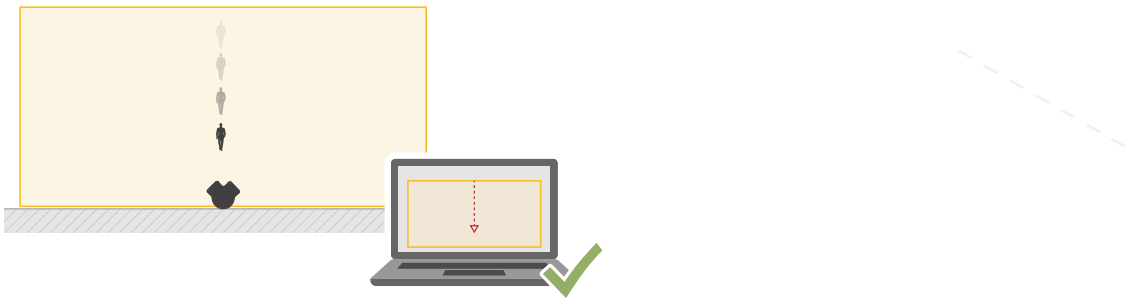
The installation is validated in the conditions that apply at the time of validation. Changed conditions in the scene can affect the everyday performance of your installation.

Check that there are no false detections

1. Check that the recognition zone is clear from human activity.
2. Wait for a few minutes to make sure the radar doesn't detect any static objects in the recognition zone.
3. If there are unwanted detections, you can filter out certain types of movement or objects, adjust the zones where objects trigger alarms, or adjust the detection sensitivity. For instructions, see .

Check for the correct symbol, direction of travel, and position on map

1. In the radar's web interface, start a recording. For instructions, see .
2. Start walking just outside the recognition zone, and walk directly toward the radar.
3. Check that a human classification symbol is shown when the person enters the recognition zone.
4. Check that the radar's web interface shows the correct direction of travel.



5. Check that the person's actual position matches the position on the map.

Create a table similar to the one below to help you record the data from your validation.

Test	Pass/Fail	Comment
1. Check that there are no unwanted detections when the area is clear.		
2. Check that the human classification symbol is shown when the person enters the recognition zone.		
3. Check that the direction of travel is correct.		
4. Make sure that the person's actual position matches the position on the map.		

Complete the validation

Once you have successfully completed the first part of the validation, perform the following tests to complete the validation process.

1. Make sure you have configured your radar according to the instructions.
2. Make sure you have added and calibrated a reference map.

3. Set the radar scenario to trigger when a human is detected. By default, **Seconds until trigger** is set to two seconds but you can change this if needed.
4. Set the radar to record video when an appropriate object is detected.
   For instructions, see .
5. Go to **Radar > Settings > Object visualization** and set the **Trail lifetime** to one hour so that it will safely exceed the time it takes for you to leave your seat, walk around the area of surveillance, and return to your seat. The trail lifetime will keep the track in the radar's live view for the set time and, once you have finished the validation, you can disable it.
6. Walk along the border of the recognition zone and make sure that the trailing on the system matches the route that you walked.
7. If you are not satisfied with the results of your validation, re-calibrate the reference map and repeat the validation.

Adjust the radar image

This section includes instructions about configuring the radar image. If you want to learn more about how certain features work, go to .

Show an image overlay

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

1. Go to **Radar > 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.

View and record video

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

Record and watch video

Record video directly from the radar

1. Go to **Radar > 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.

Set up rules for events

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

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

Trigger an action

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

Note

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

Activate a sweeping red light on the radar

You can use the dynamic LED strip on the front of the radar to indicate that the area is monitored.

This example explains how to activate a red sweeping light after working hours on weekdays.

Create a schedule:

1. Go to **System > Events > Schedules** and add a schedule.
2. Type a name for the schedule, for example `Weekday nights`.
3. Under **Type**, select **Schedule**.
4. Under **Recurrence**, select **Daily**.
5. Set the start time to 06:00 PM.
6. Set the end time to 06:00 AM.
7. Under **Days**, select Monday to Friday.
8. Click **Save**.

Create a rule:

1. Go to **System > Events** and add a rule.
2. Type a name for the rule, for example `Red sweeping light`.
3. In the list of conditions, under **Scheduled and recurring**, select **Schedule**.
4. In the list of schedules, select **Weekday nights**.
5. In the list of actions, under **Radar**, select **Dynamic LED strip**.
6. Select the pattern **Sweeping red**.
7. Set the duration to 12 hours.
8. 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.

Add an email recipient:

1. Go to **System > Events > Recipients** and add a recipient.
2. Type a name for the recipient.
3. Under **Type**, select **Email**.
4. Type an email address to send the email to.
5. Fill in the rest of the information according to your email provider.
   The radar device doesn't have its own email server, so it needs to log into an email server to send emails.
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, for example `Tampering mail`.
10. From the list of conditions, under **Device status**, select **Radar data failure**.
11. Under **Reason**, select **Tampering**.
12. In 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**.

The web interface

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

Note

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

Show or hide the main menu.

Access the release notes.

Access the product help.

Change the language.

Set light theme or dark theme.

The user menu contains:

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

The context menu contains:

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

Status

Device info

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

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

Time sync status

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

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

Security

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

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

Connected clients

Shows the number of connections and connected clients.

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

Ongoing recordings

Shows ongoing recordings and their designated storage space.

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

Shows the storage space where the recording is saved.

Power status

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

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

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.

Coexistence

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

- **0–3**: Select this option if you mount one to four radars in the same coexistence zone.
- **4–5**: Select this option if you mount five to six radars in the same coexistence zone.
- **6–11**: Select this option if you mount seven to twelve radars in the same coexistence zone.

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.
  - **Ignore unknown objects**: Turn on to minimize false alarms caused by objects that the radar can't classify.
- **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.
  - **Ignore unknown objects**: Turn on to minimize false alarms caused by objects that the radar can't classify.

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.

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.

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.

Exclusion zones

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

 : Click to create a new exclusion zone.

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

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

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

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

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

Scenarios

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

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

Triggering conditions: Select the condition that will trigger alarms.

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

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

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

Detection settings: Define the trigger criteria for the scenario.

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

Alarm settings: Define the criteria for the alarm.

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

Overlays

: 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: FFFFFF 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.

Dynamic LED strip

Dynamic LED strip patterns

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

Pattern: Select the pattern you want to test.

Duration: Specify the duration of the test.

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

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

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

Analytics

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.

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

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

- **DHCP**: Adopts the time zone of the DHCP server. The device must be connected to a DHCP server (v4 or v6) before you can select this option. If both versions are available, the device prefers IANA time zones over POSIX, and DHCPv4 over DHCPv6.
  - DHCPv4 uses Option 100 for POSIX time zones and Option 101 for IANA time zones.
  - DHCPv6 uses Option 41 for POSIX and Option 42 for IANA.
- **Manual**: Select a time zone from the drop-down list.

Note

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

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

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

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

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

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

Note

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

IPv6

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

Hostname

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

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

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

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

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

DNS servers

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

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

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

Note

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

HTTP and HTTPS

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

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

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

Note

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

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

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

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

Network discovery protocols

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

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

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

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

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

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

Network ports

Power and ethernet: Select this option to turn on network for the switch port.

Power only: Select this option to turn off network for the switch port. The port still provides power over ethernet.

Global proxies

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

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

Allowed formats for http and https proxies:

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

Note

Restart the device to apply the global proxy settings.

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

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

One-click cloud connection

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

Allow O3C:

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

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

Host: Enter the proxy server's address.

Port: Enter the port number used for access.

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

Authentication method:

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

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

SNMP

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

SNMP: Select the version of SNMP to use.

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

Note

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

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

Security

Certificates

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

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

These formats are supported:

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

Important

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

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

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

The context menu contains:

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

Secure keystore :

- **Trusted Execution Environment (SoC TEE)**: Select to use SoC TEE for secure keystore.
- **Secure element (CC EAL6+, FIPS 140-3 Level 3)** : Select to use secure element for secure keystore.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Level 2)** : Select to use TPM 2.0 for secure keystore.

Cryptographic policy

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

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

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

Network access control and encryption

IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

Certificates

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

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

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

Authentication method: Select an EAP type used for authentication.

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

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

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

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

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

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

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

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

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

Prevent brute-force attacks

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

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

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

Firewall

Firewall: Turn on to activate the firewall.

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

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

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

+ New rule: Click to create a rule.

Rule type:

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

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

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

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

Custom signed AXIS OS certificate

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

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

The context menu contains:

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

Accounts

Accounts

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

Account: Enter a unique account name.

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

Repeat password: Enter the same password again.

Privileges:

- **Administrator**: Has full access to all settings. Administrators can also add, update, and remove other accounts.
- **Operator**: Has access to all settings except:
  - All **System** settings.
- **Viewer**: Doesn't have access to change any 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*.

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

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

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

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

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

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

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

Recipients

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

Note

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

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

Note

You can create up to 20 recipients.

Add a recipient: Click to add a recipient.

Name: Enter a name for the recipient.

Type: Select from the list:

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

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

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

Note

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

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

Test: Click to test the setup.

⋮ The context menu contains:

View recipient: Click to view all the recipient details.

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

Delete recipient: Click to delete the recipient permanently.

Schedules

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

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

Manual triggers

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

MQTT

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

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

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

ALPN

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

MQTT client

Connect: Turn on or off the MQTT client.

Status: Shows the current status of the MQTT client.

Broker

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

Protocol: Select which protocol to use.

Port: Enter the port number.

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

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

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

Password: Enter a password for the username.

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

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

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

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

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

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

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

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

Connect message

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

Send message: Turn on to send messages.

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

Topic: Enter the topic for the default message.

Payload: Enter the content for the default message.

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

QoS: Change the QoS layer for the packet flow.

Last Will and Testament message

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

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

Send message: Turn on to send messages.

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

Topic: Enter the topic for the default message.

Payload: Enter the content for the default message.

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

QoS: Change the QoS layer for the packet flow.

MQTT publication

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

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

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

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

Add condition: Click to add a condition.

Retain: Defines which MQTT messages are sent as retained.

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

QoS: Select the desired level for the MQTT publication.

MQTT subscriptions

Add subscription: Click to add a new MQTT subscription.

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

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

Network storage: Turn on to use network storage.

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

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

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

Unbind: Click to unbind and disconnect the network share.
Bind: Click to bind and connect the network share.

Unmount: Click to unmount the network share.
Mount: Click to mount the network share.

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

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

Tools

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

Use tool: Click to activate the selected tool.

Onboard storage

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.

Onboard storage

Hard drive

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

Tools

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

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

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

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

Onboard storage

RAID

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

Tools

Note

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

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

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

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

Stream profiles

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

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

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

Name: Add a name for your profile.

Description: Add a description of your profile.

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

Resolution: See 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.

Privileges:

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

The context menu contains:

Update account: Edit the account properties.

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

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

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.

Power settings

Power status

Shows power status information. Information varies depending on the product.

Power settings

Delayed shutdown : Turn on if you want to set a delay time before the power turns off.

Delay time : Set a delay time between 1 and 60 minutes.

Power saving mode : Turn on to put the device into power saving mode. When you turn on power saving mode, the IR illumination range reduces.

Set power configuration : Change the power configuration by selecting a different PoE class option. Click **Save and restart** to save the change.

Note

If you set the power configuration to PoE class 3, we recommend you select **Low power profile** if your device has that option.

Dynamic power mode : Turn on to reduce power consumption when the device is inactive.

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

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

Power meter

Energy usage

Shows the current power usage, average power usage, maximum power usage, and power consumption over time.

The context menu contains:

- **Export**: Click to export the chart data.

Edge-to-edge

Pairing

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

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.

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.

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.

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.

Generic pairing allows you to pair with a device with light and siren functionality.

To pair a device from the list, click  .

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

Address: Enter host name or IP address to the device.

Username: Enter username.

Password: Enter password.

Certificate name: Enter certificate name.

Close: Click to clear all fields.

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

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

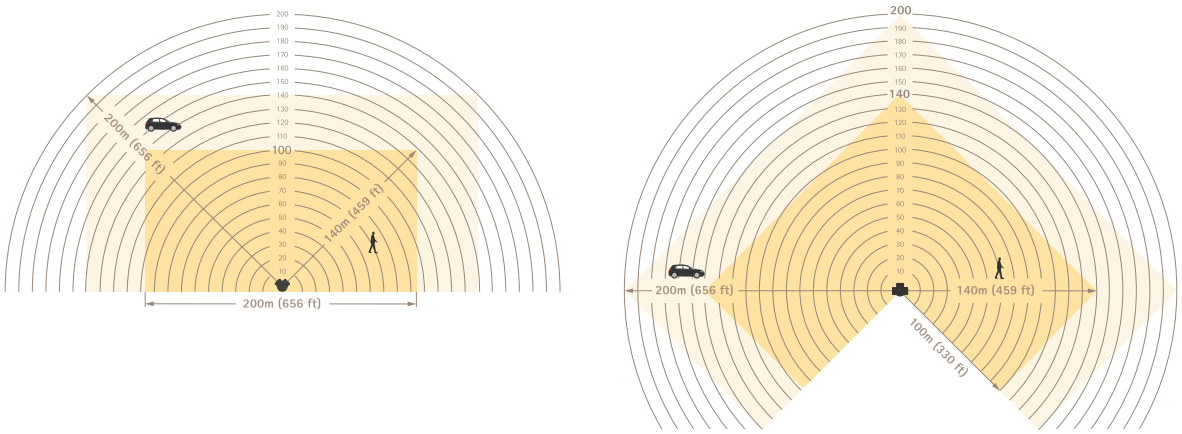
Radar

Recognition and detection zones

The recognition zone is a zone where the radar with certainty can classify objects as humans or vehicles.

The detection zone is a zone where the radar can detect fast-moving vehicles.

The size of each zone depends on installation height and other factors.



The recognition zone is dark yellow, and the detection zone is light yellow.

Scenarios, inclusion zones, and exclusion zones

A **scenario** consists of a set of conditions that moving objects must fulfill to trigger rules in the event system. Some of the conditions are:

- Object type (human, vehicle, unknown)
- Object behavior (movement in area or line crossing)
- Part of the scene (inclusion zone or virtual line)
- Object speed

The **inclusion zone** is the part of the scene where objects in a Movement in area scenario are detected and classified.

If there are areas in the scene where you don't want moving objects to trigger alarms, you can create **exclusion zones**. You can also use exclusion zones if there are areas inside an inclusion zone that cause a lot of unwanted alarms. In an exclusion zone, moving objects are ignored. Use them to filter out, for example, swaying foliage on the side of a road or ghost tracks caused by objects made of radar-reflective materials such as a metal fence.

Coexistence zone

You can install multiple radars to cover areas that are larger than a single radar's specified detection zone. Radars that use the same radio frequency can cause electromagnetic interference, which can affect the performance. Each Axis radar model has a specified coexistence zone. Within this you can install a certain number of radars without causing interference. To find out the radius and the recommended maximum number of radars of the coexistence zone, see the device's datasheet at *axis.com*.

Radar-video fusion technology

Radar-video fusion combines the strengths of an Axis radar with those of an Axis camera. This combination provides great situational awareness and reduces false alarms. When you pair an ARTPEC-9 PTZ camera with an ARTPEC-9 radar from the camera's web interface, the radar can discover and classify a moving object, direct the camera to the object, and let the camera validate the classification. The camera can then continue tracking the object with autotracking, which you can read about in the PTZ camera's user manual.

Autotracking

You can use radar data about different objects' positions to make a PTZ camera track objects. There are three different options:

- If you want to connect multiple PTZ cameras and radars, use the application AXIS Radar Autotracking for PTZ. For more information, see .
- If you want to connect one radar and one ARTPEC-7 PTZ camera that are mounted close to each other, use camera pairing to use the built-in radar autotracking.
- If you want to connect one radar and one ARTPEC-9 PTZ camera that are mounted together, use radar pairing to use built-in radar-video fusion autotracking. This option combines AI-powered radar and video analytics to minimize false alarms. For instructions on how to set up radar-video fusion autotracking, see the PTZ camera's user manual at *help.axis.com/axis-q6325-le*.

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*.

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.

Streaming and storage

Video compression formats

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

Motion JPEG

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

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

H.264 or MPEG-4 Part 10/AVC

Note

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

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

AV1

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

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

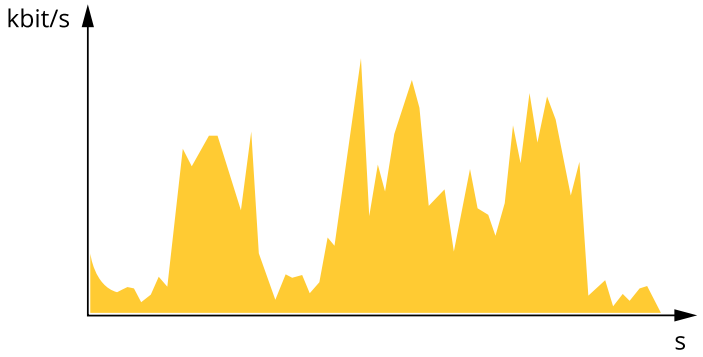
Note

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

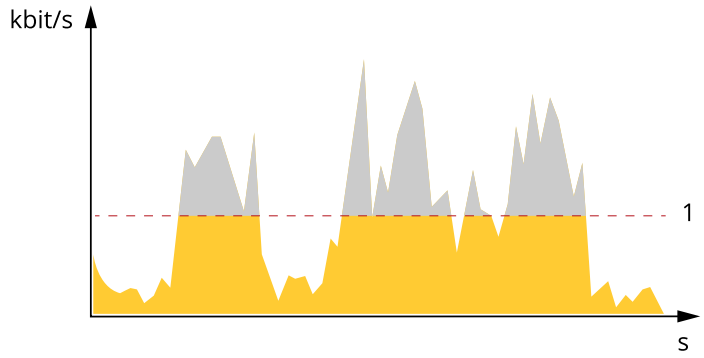
Bitrate control

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

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



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

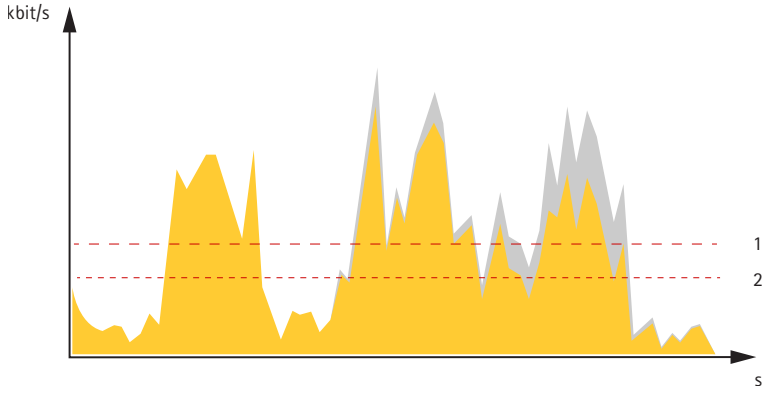


1 Target bitrate

Average bitrate (ABR)

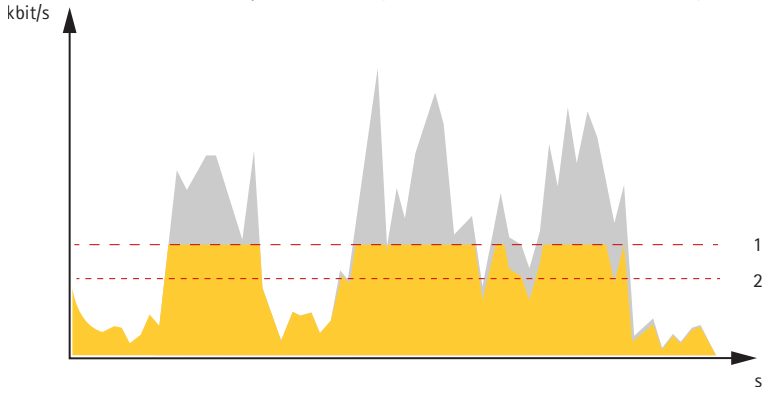
With average bitrate, the bitrate is automatically adjusted over a longer period of time. This is so you can meet the specified target and provide the best video quality based on your available storage. Bitrate is higher in scenes with a lot of activity, compared to static scenes. You are more likely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

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



1 Target bitrate
2 Actual average bitrate

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



1 Target bitrate
2 Actual average bitrate

Edge-to-edge technology

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

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

Speaker pairing

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

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

Microphone pairing

Edge-to-edge microphone pairing allows you to use a compatible Axis microphone as if it's part of your camera. Once paired, the microphone will take up sounds from the surrounding area and make it available as an audio input device, usable in media streams and recordings.

Cybersecurity

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

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

Axis security notification service

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

Vulnerability management

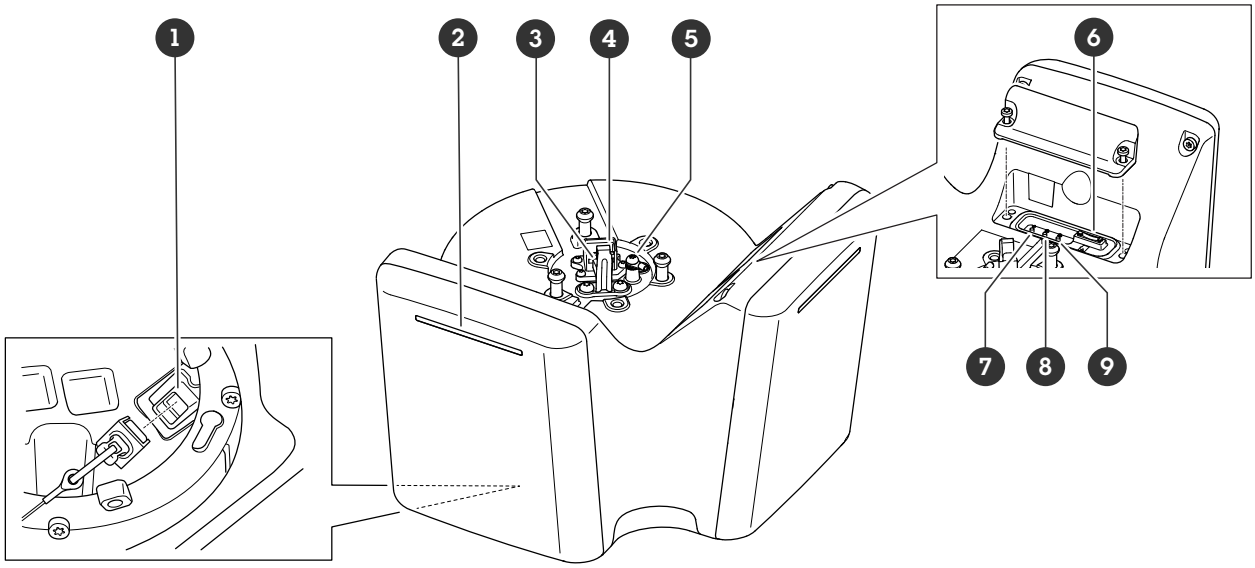
To minimize customers' risk of exposure, Axis, as a **Common Vulnerability and Exposures (CVE) numbering authority (CNA)**, follows industry standards to manage and respond to discovered vulnerabilities in our devices, software, and services. For more information about Axis vulnerability management policy,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

Secure operation of Axis devices

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

Specifications

Product overview



1 *Network connector (PoE out)*
2 *Dynamic LED strip*
3 *Hook for safety wire*
4 *Network connector (PoE in)*
5 *Ground screw*
6 *microSD card slot*
7 *Control button*
8 *Action button*
9 *Function button (not used)*

LED indicators

Status LED	Indication
Green	Steady green for normal operation.
Amber	Steady during startup. Flashes during device software upgrade or reset to factory default.

Dynamic LED strip patterns
Red
Blue
Green
Yellow
White
Sweeping red
Sweeping blue
Sweeping green
Flashing red, blue, white

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 .

Connectors

Network connector (PoE in)

RJ45 Ethernet connector with Power over Ethernet IEEE 802.3bt, Type 4 Class 8.

Note

Power over Ethernet IEEE 802.3bt, Type 4 Class 8, is required for PoE out. When not powering a second device, Power over Ethernet IEEE 802.3at, Type 2 Class 4, is sufficient.

Network connector (PoE out)

Power over Ethernet IEEE 802.3bt, Type 3 Class 6.

Use this connector to supply power to another PoE device, for example a camera, a horn speaker, or a second Axis radar.

Note

- Powering the radar with Power over Ethernet IEEE 802.3bt, Type 4 Class 8 allows for a second device that is using Power over Ethernet IEEE 802.3bt, Type 3 Class 6.
- Powering the radar with Power over Ethernet IEEE 802.3bt, Type 3 Class 6 allows for a second device that is using Power over Ethernet IEEE 802.3bt, Type 2 Class 4.
- If powering the radar with Power over Ethernet IEEE 802.3bt, Type 2 Class 4 the PoE out is disabled.

Note

Maximum Ethernet cable length is 100 m in total for PoE out and PoE in combined. You can increase it with a PoE extender.

Clean your device

You can clean your device with lukewarm water and mild, nonabrasive soap.

NOTICE

- Harsh chemicals can damage the device. Don't use chemicals such as window cleaner or acetone to clean your device.
- Don't spray detergent directly on the device. Instead, spray detergent on a nonabrasive cloth and use that to clean the device.
- Avoid cleaning in direct sunlight or elevated temperatures, since this can cause stains.

1. Use a can of compressed air to remove dust and loose dirt from the device.
2. If necessary, clean the device with a soft microfiber cloth dampened with lukewarm water and mild, nonabrasive soap.
3. To avoid stains, dry the device with a clean, nonabrasive cloth.

Troubleshooting

Reset to factory default settings

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**.

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.

AXIS OS options

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

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

Check the current AXIS OS version

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

To check the current AXIS OS version:

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

Upgrade AXIS OS

Important

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

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 problems and possible solutions

Problems upgrading AXIS OS

AXIS OS upgrade failed

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

Problems after AXIS OS upgrade

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

Problems setting the IP address

Can't set the IP address

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

Problems accessing the device

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

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

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

The IP address has been changed by DHCP

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

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

Certificate error when using IEEE 802.1X

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

The browser isn't supported

For a list of recommended browsers, see .

Can't access the device externally

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

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

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

Problems with MQTT

Can't connect over port 8883 with MQTT over SSL

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

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

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

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

Problems with the image

Image degradation or image loss

- Check the devices server report for the number of times you have lost the link to the sensor unit.
- Check that the connector cable between the sensor unit and the main unit is tight.
- Change to a new sensor unit cable.

Problems with the device turning itself off

The device shuts down

- Disconnect and reconnect power to the device.
- Check if **Delayed shutdown** is turned on. If it's on, the main unit turns off according to the set delay time. You have 300 seconds to turn off **Delayed shutdown** before the device turns itself off again.

Performance considerations

When you set up your system, it's important to consider how different settings and situations affect the required bandwidth (bitrate).

The most important factors to consider:

- Removing or attaching the cover will restart the camera.
- Heavy network utilization due to poor infrastructure affects the bandwidth.

Contact support

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

T10223326

2026-01 (M1.36)