AXIS D2110‑VE Security Radar

User manual

Table of Contents

Solution overview

1 C1310-E horn speaker
2 Door controller
3 D2110–VE Security Radar
4 Fixed dome camera
5 PTZ camera
6 Surveillance center

Radar profiles

> **Note**
> To use radar profiles your device must be running firmware version 10.11 or later. Go to to update your firmware.

The user manual is set up to help you use your radar depending on what you want it to do. AXIS D2110–VE Security Radar has two profiles:

- **Area monitoring profile** to track both large and small objects moving at speeds lower than 55 km/h (34 mph)

- **Road monitoring profile** to track vehicles moving at speeds up to 105 km/h (65 mph)

Any information in this user manual that does not fall under **Area monitoring profile** or **Road monitoring profile** is common to both profiles and can be referenced regardless of which one you use.

Where to install the product

- The radar is intended for monitoring open areas. Any solid object (such as a wall, a fence, a tree, or a large bush) in the coverage area will create a blind spot (radar shadow) behind it.

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

- Metal objects in the field of view causes reflections that affects the ability of the radar to perform classifications.
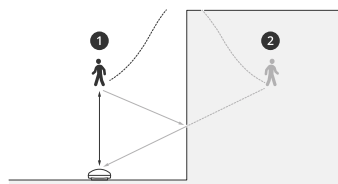
1   *Actual detection*
2   *Reflected detection (ghost track)*

For information about how to handle reflective objects, see .
- If you want to install more than two radars in the same coexistence zone, see .

Area of coverage

The AXIS D2110–VE has a horizontal area coverage of 180°. The detection range corresponds to 5600 m^2 (61000 ft^2) for humans and 11300 m^2 (122000 ft^2) for vehicles.

Note

Optimal area coverage applies when the radar is mounted at 3.5–4 m (11–13 ft). Mounting height will affect the size of the blind spot below the radar.

Area monitoring profile

The **area monitoring profile** is optimized for objects moving at up to 55 km/h (34 mph). This profile allows you to detect whether an object is human, vehicle, or unknown. A rule can be set to trigger an action when any of these objects is detected. To track vehicles moving in higher speeds, use the .

Install multiple radars

You can install multiple radars to cover areas such as the surroundings of a building or the buffer zone outside a fence.

Coexistence

When you place more than two radars within the same coexistence zone, the radio waves from the radars within the zone can cause interference and affect the performance. The coexistence zone radius is 350 m (380 yd).

1   Radar
2   Detection area
3   Coexistence zone
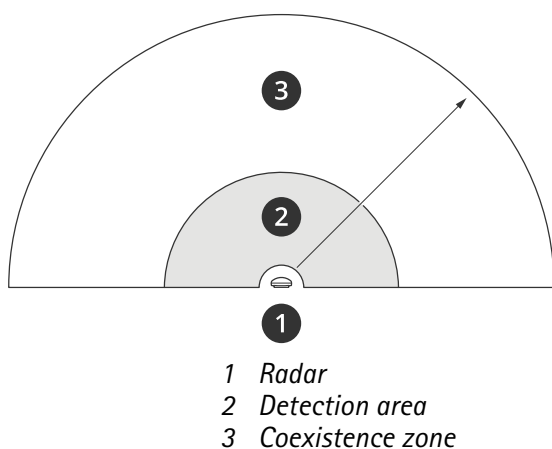
> **Note**
> The performance of the radar in the coexistence zone can also be affected by the environment and/or the radar's direction towards fences, buildings or neighboring radars.

Install 2–3 radars in the same coexistence zone

When you place two or three radars in the same coexistence zone, you need to define the number of neighboring radars in the device interface. This helps to improve the performance of the radars and to avoid interference.

1.   Go to **Radar > Settings > Coexistence**.

2.   Select the number of neighboring radars.

See for examples of installations with multiple radars.

Install 4–6 radars in the same coexistence zone

> **Note**
> The option to install up to six radars in the same coexistence zone is available from firmware version 11.3.

When you mount four to six radars in the same coexistence zone, first set the number of neighboring radars, then add each radar into a group. Start with the radar that is installed farthest away, for example the one farthest to your left. Add the radars in groups of three and add the radars that are closest to each other in the same group.

The radars within the group will sync with each other to optimize the performance and avoid interference between each other.

1.   Go to **Radar > Settings > Coexistence**.

2. Set the number of neighboring radars to **3–5**.

3. Select a group for your radar.
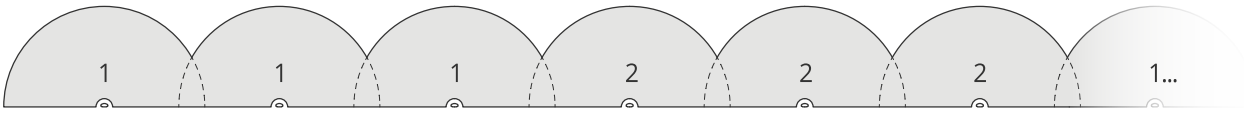
This is an example of how to group multiple radars installed side-by-side in the same coexistence zone.

See for more examples of installations with multiple radars.

Area installation examples

Create a virtual fence with multiple radars

To create a virtual fence, for example along or around a building, you can place multiple radars side-by-side. We recommend placing them with 100 m (330 ft) spacing.
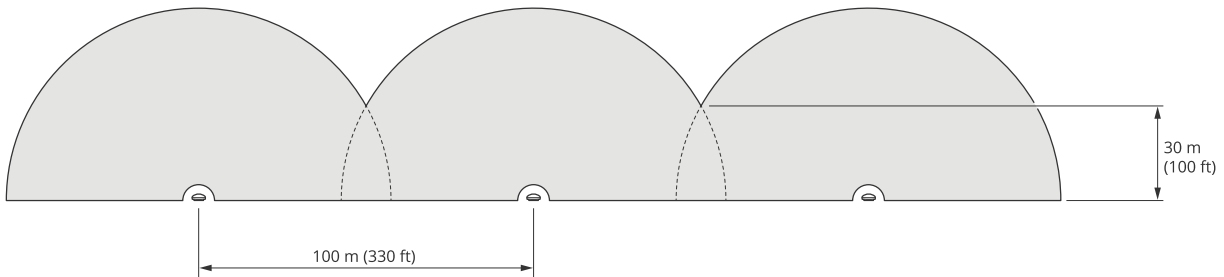
To avoid interference when you mount more than two radars in the same coexistence zone, set the number of neighboring radars in the device interface. Additionally, when you mount more than three radars, add each radar into a group.
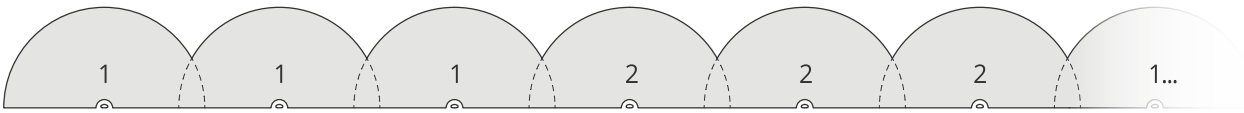
You can adjust the virtual fence to cover corners as well, as illustrated in this example.
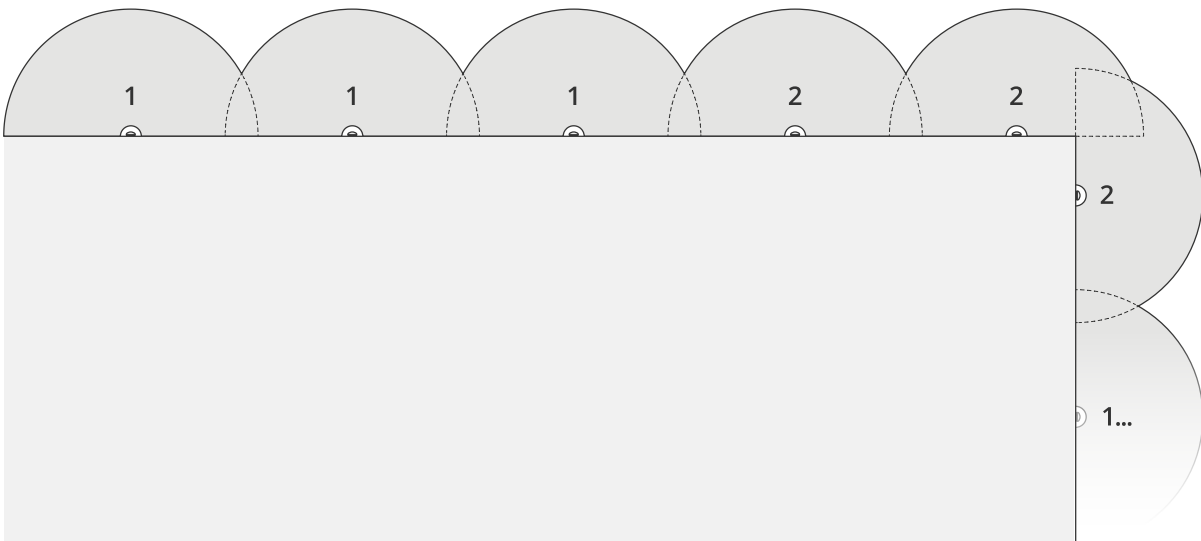
See for more information about neighboring radars and groups.

Cover an area around a building

7

To cover the area around a building, place the radars on the walls of the building facing outwards. If you are placing more than three radars in the same coexistence zone, set the number of neighboring radars in the device interface and add each radar into a group, as illustrated in this example.
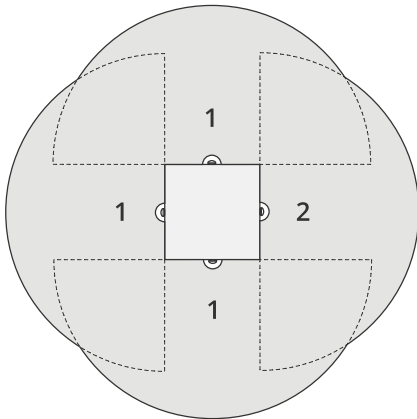
You can also cover the area around multiple buildings.
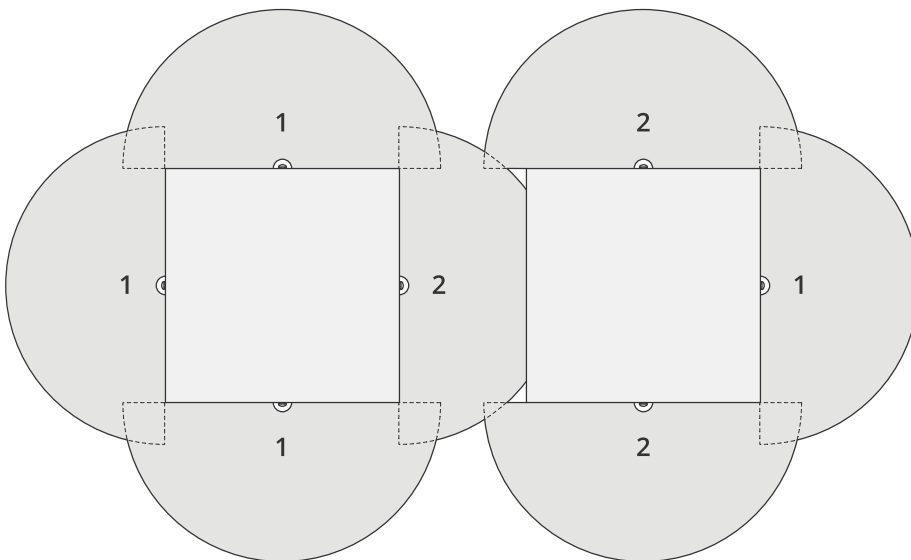
See for more information about neighboring radars and groups.

Cover an open area

To cover a large open area, use two pole mounts to place two radars back-to-back.
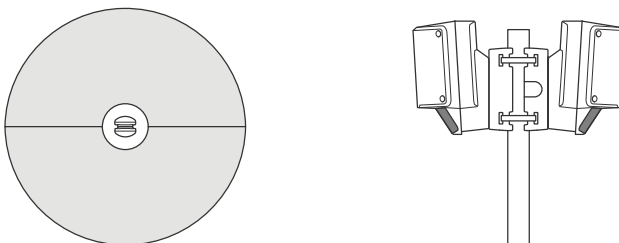
You can use the PoE output from one radar to power the second radar, but it's not possible to connect a third radar this way.

Note

The PoE output on the radar is enabled when the radar is powered by a 60 W midspan.

If you require several back-to-back installations in the same coexistence zone, set the number of neighboring radars in the device interface and add each radar into a group to avoid interference. This is one example of how you can group your radars in a back-to-back installation.
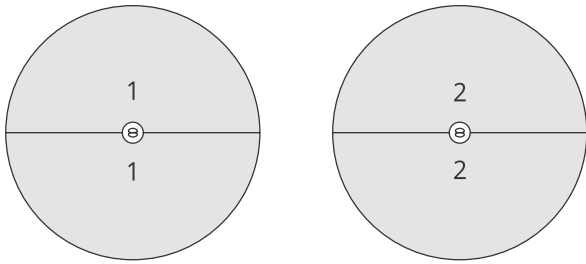
See for more information about neighboring radars and groups.

Install multiple radars facing each other

In general, it is not recommended to install more than three radars facing each other since this increases the risk of interference between the radars. However, in some specific areas it can be necessary. If you want to cover a football field for example, you can't place radars in the middle of the field.

If you install more than three radars facing each other, the minimum distance from one radar to another needs to be 40 meters (130 ft). It is also especially important to set the number of neighboring radars in the device interface and add each radar into a group. This will help to improve the performance of the radars.

This is an example of how to group four radars covering a field.
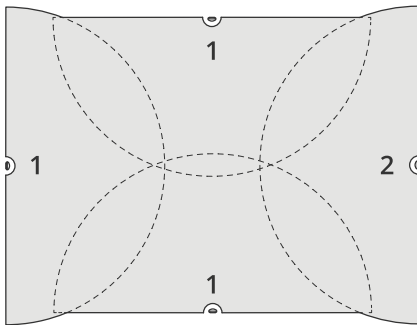
See for more information about neighboring radars and groups.

Area detection range

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

The **Area monitoring profile** is optimized for human detection, however, it will also allow you to track vehicles and other objects moving at up to 55 km/h (34 mph) with a velocity accuracy of +/- 2 km/h (1.24 mph).

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

- **3–60 m (10–200 ft)** when detecting a human
- **3–85 m (10–280 ft)** when detecting a vehicle

9
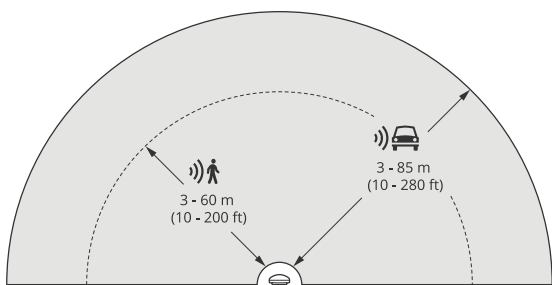
Note
- If you install the radar at a different height, enter the actual mounting height in the product's web pages when you calibrate the radar.
- The detection range is affected by the scene.
- The detection range is affected by neighboring radars.
- The detection range is affected by the object type.

The detection range was measured under these conditions:
- The range was measured along the ground.
- The object was a 170 cm (5 ft 7 in) tall person.
- The person was walking straight in front of the radar.
- The values are measured when the person enters the detection zone.
- The radar sensitivity was set to **Medium**.

Mounting height	0° tilt	10° tilt	20° tilt
2.5 m (8.2 ft)	3.0–60 m (9.8–197 ft)	Not recommended	Not recommended
3.5 m (11 ft)	3.0–60 m (9.8–197 ft)	Not recommended	Not recommended
4.5 m (15 ft)	4.0–60 m (13–197 ft)	Not recommended	Not recommended
5.5 m (18 ft)	7.5–60 m (25–197 ft)	Not recommended	Not recommended
6.5 m (21 ft)	7.5–60 m (25–197 ft)	5.5–60 m (18–197 ft)	Not recommended
8 m (26 ft)	Not recommended	9–60 m (30–197 ft)	7.5–30 m (25–98 ft)
10 m (33 ft)	Not recommended	15–60 m (49–197 ft)	9–35 m (30–115 ft)
12 m (39 ft)	Not recommended	23–60 m (75–197 ft)	13–38 m (43–125 ft)
14 m (36 ft)	Not recommended	27–60 m (89–197 ft)	17–35 m (56–115 ft)
16 m (52 ft)	Not recommended	Not recommended	25–50 m (82–164 ft)

Area monitoring use cases

Swimming pool area coverage

A public swimming pool has had a series of intrusions after hours. Due to the private nature of the business, the owners cannot install video surveillance. They have chosen to install a radar and set it up in the **Area monitoring profile**. The radar is mounted on the building and covers the whole swimming pool and most of the area around it. It triggers a warning from a speaker when a human is detected between closing at 20:00 and opening at 06:00.

Cover the field around a building

A chemical factory adds another layer of security to their system by using radars to cover the area around a sensitive building. The security system already includes cameras, thermal cameras and door controllers. Radars can trigger events that cause cameras to track the intruder, zoom in, and record activity. Flashing beacons, linked to thermal cameras, are triggered to flash so the intruder knows that the area is protected. And door controllers can restrict access. The radars help the defence system move into action long before the intruder has reached the sensitive building.
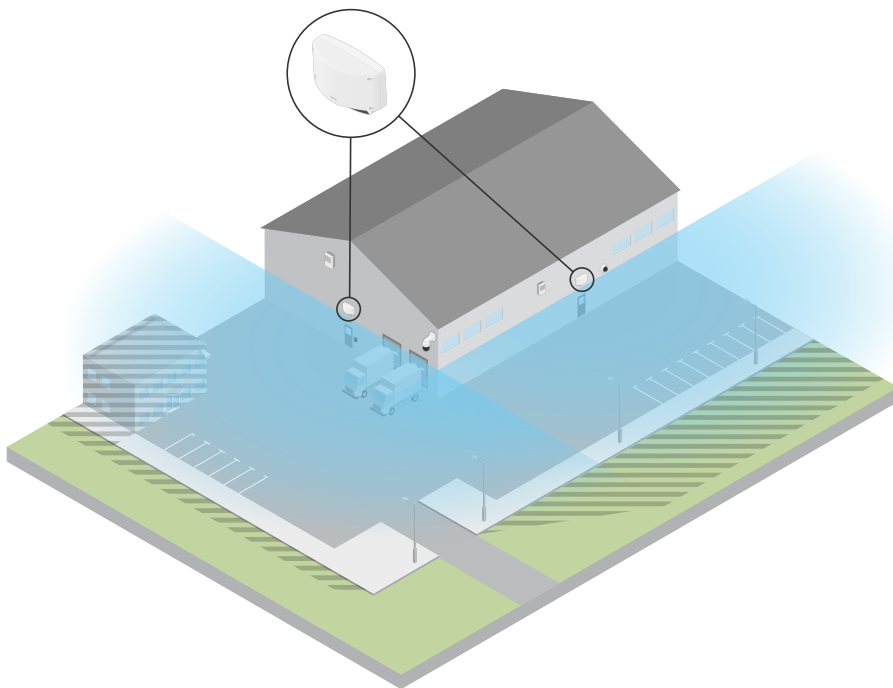
Cover a large open area

A parking lot outside a small shopping center has had increased vehicle break-ins after hours. They have one security guard on duty at a time but feel they need to bolster their security at night without the added cost of hiring more staff. They have decided to install two security radars, in the **Area monitoring profile**, mounted back-to-back so that they cover the entire parking area. The radars are configured to alert the on-duty security guard of suspicious behavior so that they can investigate the scene. They could also install a horn speaker that is triggered by the radars to play an alert that may deter thieves.

11

Road monitoring profile

The **Road monitoring profile** is best used to track vehicles moving at up to 105 km/h (65 mph) in urban zones, closed zones, and on sub-urban roads. This mode should not be used for detection of humans or other types of objects. To track objects other than vehicles, use your radar in the .

Road installation examples

Side mounted

To monitor vehicles travelling along a road you can mount the radar on to the side of the road. The radar will provide a lateral coverage distance of 10 m (32 ft).
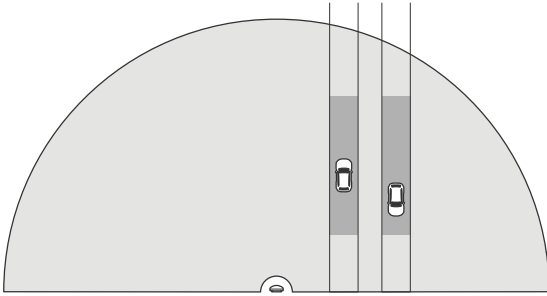
Center mounted

This mounting option requires a stable position. The radar can be mounted on a pole in the middle of the road or on a bridge above the road. The radar will then provide a lateral coverage distance of 10 m (32 ft) to both sides of the radar. The radar covers a broader lateral distance when center mounted.
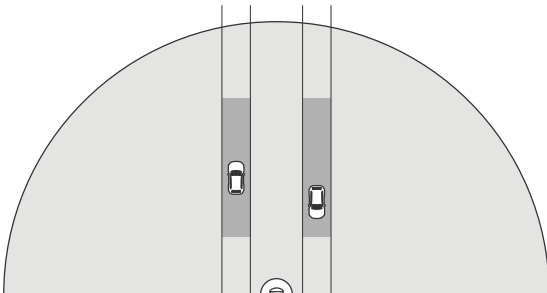
Note
> We recommend that the radar is mounted at a height between 3 m (10 ft) and 8 m (26 ft) for the **Road monitoring profile**.

Road detection range

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

This profile is optimized for detection of vehicles and will produce a velocity accuracy of +/- 2 km/h (1.24 mph) when monitoring vehicles moving at up to 105 km/h (65 mph).

Detection range when the radar is mounted at an optimal installation height:

- **25–70 m (82–229 ft)** for vehicles moving at 60 km/h (37 mph).
- **30–60 m (98–196 ft)** for vehicles moving at 105 km/h (65 mph).

Road monitoring use cases

Regulating vehicles in low speed zones

An industrial complex with a long road between two warehouses has installed a radar to help enforce a speed limit of 60 km/h (37 mph). In the **Road monitoring profile**, the radar can detect when a vehicle in its detection zone exceeds that speed. It then triggers an event which sends an email notifications to drivers and managers. The reminder helps increase compliance with the speed restrictions.

Unwanted vehicles on a closed road

A small road out to an old quarry has been closed, however, reports of vehicles driving on the road have resulted in authorities installing a security radar in the **Road monitoring profile**. The radar is mounted alongside the road and covers the entire width of the road. Whenever a vehicle enters the scenario, it triggers a flashing beacon that warns drivers to leave the road. It also sends a message to the security team so that they can dispatch a unit if needed.

Speed awareness on the road

A road that passes through a small town has had some incidents of speeding. To enforce the speed limit of 70 km/h (43 mph), the traffic control has installed a security radar, in the **Road monitoring profile**, on a bridge that crosses over the road. This has allowed them to detect the speed that vehicles are travelling at and monitor when they should have units stationed long the road to control the traffic.
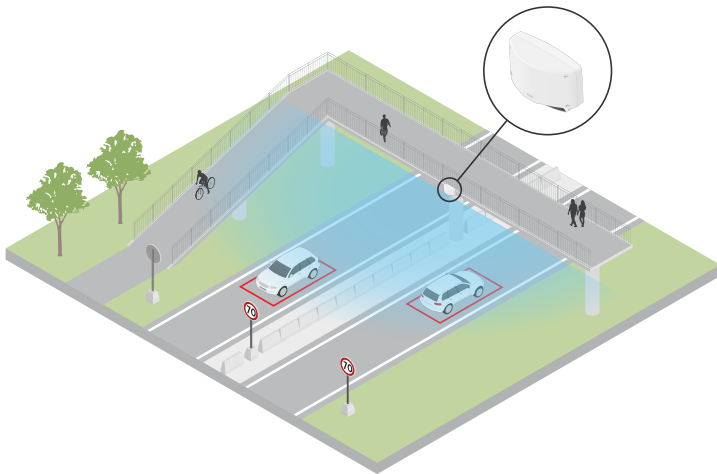
Safety with humans and vehicles

Staff at a school have identified two safety issues that they would like to address. They have experienced unwanted visitors entering the premises during the school day, as well as vehicles violating the low speed zone of 20 km/h (12 mph) outside the school. The radar is mounted on a pole, next to the pedestrian walk path. The was chosen, as it makes the radar capable of tracking both humans and vehicles moving at speeds lower than 55 km/h (34 mph). This helps the staff keep track of people coming and going during school hours while also being able to trigger a speaker to warn pedestrians when a passing vehicle is driving too fast.
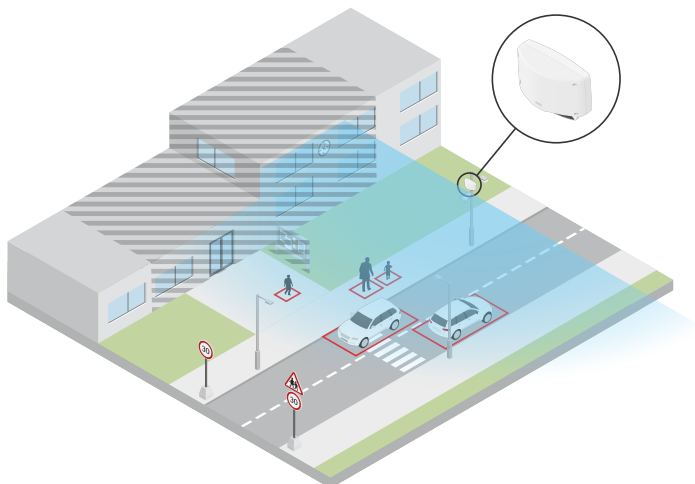
Get started

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^{TM}	Firefox®	Edge^{TM}	Safari®
Windows®	recommended	✓	recommended	
macOS®	recommended	✓	recommended	✓*
Linux®	recommended	✓	recommended	
Other operating systems	✓	✓	✓	✓

*Not fully supported. If you encounter video streaming issues, use a different browser.

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.

Web interface overview

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

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

Axis device web interface

Configure your device

Set the mounting height

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

Measure the height from the ground up to the 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**.

Calibrate a reference map

Upload a reference map to make it easier to see where detected objects are moving. You can use a ground plan or an aerial photo that shows the area covered by the radar. Calibrate the map so the radar coverage fits the position, direction, and scale of the map, and zoom in on the map if you're interested in a specific part of the radar coverage.

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

Use the setup assistant:
1. Go to **Radar > Map calibration**.

2. Click **Setup assistant** and follow the instructions.

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

Edit each setting individually:
The map will calibrate gradually after you adjust each setting.
1. Go to **Radar > Map calibration > Map**.

2. Select the image you want to upload, or drag and drop it in the designated area.
   To reuse a map image with its current pan and zoom settings, click **Download map**.

3. Under **Rotate map**, use the slider to rotate the map into position.

4. Go to **Scale and distance on a map** and click on two pre-determined points on the map.

5. Under **Distance**, add the actual distance between the two points you have added to the map.

6. Go to **Pan and zoom map** and use the buttons to pan the map image, or zoom in and out on the map image.

Note

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

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

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

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

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

Set detection zones

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

There are two types of zones:
- A **scenario** (previously called include zone) is an area in which moving objects will trigger rules. The default scenario matches the entire area covered by the radar.

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

Add scenarios

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

Add a scenario:
1. Go to **Radar > Scenarios**.

2. Click **Add scenario**.

3. Type the name of the scenario.

4. Select if you want to trigger on objects moving in an area or on objects crossing one, or two, lines.

Trigger on objects moving in an area:
1. Select **Movement in area**.

2. Click **Next**.

3. Select the type of zone that should be included in the scenario.
   Use the mouse to move and shape the zone so that it covers the desired part of the radar image or reference map.

4. Click **Next**.

5. Add detection settings.

1. Add seconds until trigger after under **Ignore short-lived objects**.

2. Select which object type to trigger on under **Trigger on object type**.

3. Add a range for the speed limit under **Speed limit**.

6. Click **Next**.

7. Set the minimum duration of the alarm under **Minimum trigger duration**.

8. Click **Save**.

Trigger on objects crossing a line:
1. Select **Line crossing**.

2. Click **Next**.

3. Position the line in the scene.
   Use the mouse to move and shape the line.

4. To change the detection direction, turn on **Change direction**.

5. Click **Next**.

6. Add detection settings.

   6.1. Add seconds until trigger after under **Ignore short-lived objects**.

   6.2. Select which object type to trigger on under **Trigger on object type**.

   6.3. Add a range for the speed limit under **Speed limit**.

7. Click **Next**.

8. Set the minimum duration of the alarm under **Minimum trigger duration**.

The default value is set to 2 seconds. If you want the scenario to trigger every time an object crosses the line, lower the duration to 0 seconds.

9. Click **Save**.

Trigger on objects crossing two lines:

1. Select **Line crossing**.

2. Click **Next**.

3. To make the object cross two lines for the alarm to trigger, turn on **Require crossing of two lines**.

4. Position the lines in the scene.
    Use the mouse to move and shape the line.

5. To change the detection direction, turn on **Change direction**.

6. Click **Next**.

7. Add detection settings.

    7.1. Set the time limit between crossing the first and the second line under **Max time between crossings**.

    7.2. Select which object type to trigger on under **Trigger on object type**.

    7.3. Add a range for the speed limit under **Speed limit**.

8. Click **Next**.

9. Set the minimum duration of the alarm under **Minimum trigger duration**.
    The default value is set to 2 seconds. If you want the scenario to trigger every time an object has crossed the two lines, lower the duration to 0 seconds.

10. Click **Save**.

Add exclude zones

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

Add an exclude zone:

1. Go to **Radar > Exclude zones**.

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

Minimize false alarms

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

- Adjust the detection sensitivity of the radar:
  Go to **Radar > Settings > Detection** and select a lower **Detection sensitivity**. This decreases the risk of false alarms, but it could also cause the radar to miss some movement.
  The sensitivity setting affects all zones.

  - **Low**: Use this sensitivity when there are a lot of metal objects or large vehicles in the area. It will take longer time for the radar to track and classify objects. This can reduce the detection range, especially for fast moving objects.

  - **Medium**: This is the default setting.

  - **High**: Use this sensitivity when you have an open field without metal objects in front of the radar. This will increase the detection range for humans.

- Modify scenarios and exclude zones:

If a scenario includes hard surfaces, such as a metal wall, there may be reflections that causes multiple detections for a single physical object. You can either modify the shape of the scenario, or add an exclude zone that ignores certain parts of the scenario. For more information, see and .

- Trigger on objects crossing two lines instead of one:
  If a line crossing scenario includes swaying objects or animals moving around, there is a risk that an object will happen to cross the line and trigger a false alarm. In this case, you can configure the scenario to trigger only when an object has crossed two lines. For more information, see .

- Filter on movement:
  - Go to **Radar > Settings > Detection** and select **Ignore swaying objects**. This setting minimizes false alarms from trees, bushes, and flagpoles in the coverage zone.

  - Go to **Radar > Settings > Detection** and select **Ignore small objects**. This setting is available in the area monitoring profile and minimizes false alarms from small objects in the coverage zone, such as cats and rabbits.

- Filter on time:
  - Go to **Radar > Scenarios**.

  - Select a scenario, and click ⋮ to modify its settings.

  - Select a higher value under **Seconds until trigger**. This is the delay time from when the radar starts tracking an object until it can trigger and alarm. The timer starts when the radar first detects the object, not when the object enters the specified zone in the scenario.

- Filter on object type:
  - Go to **Radar > Scenarios**.

  - Select a scenario, and click ⋮ to modify its settings.

  - To avoid triggering on specific object types, deselect the object types that should not trigger events in the scenario.

View and record video

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

Reduce bandwidth and storage

Important
Reducing the bandwidth can result in loss of details in the image.

1. Go to **Radar > Stream**.

2. Click ✹ in the live view.

3. Select **Video format H.264**.

4. Go to **Radar > Stream > General** and increase **Compression**.

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

Set up network storage

To store recordings on the network, you need to set up your network storage.
1. Go to **System > Storage**.

2. Click ➕ **Add network storage** under **Network storage**.

3. Type the IP address of the host server.

4. Type the name of the shared location on the host server under **Network share**.

5. Type the username and password.

6. Select the SMB version or leave it on **Auto**.

7. Select **Add share without testing** if you experience temporary connection issues, or if the share is not yet configured.

8. Click **Add**.

Record and watch video

Record video directly from the 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.

Control a PTZ camera with the radar

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

- . The built-in option is suitable when you have a PTZ camera and radar mounted very close together.

- . The Windows application is suitable when you want to use multiple PTZ cameras and radars for tracking objects.

Note

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

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

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

Note

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

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

Before you start:

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

Pair the radar with the PTZ camera:

1. Go to **System > Edge-to-edge > PTZ pairing**.

2. Enter the IP address, username and password for the PTZ camera.

3. Click **Connect**.

4. Click **Configure Radar autotracking** or go to **Radar > Radar PTZ autotracking** to set up radar autotracking.

Calibrate the radar and the PTZ camera:
5. Go to **Radar > Radar PTZ autotracking**.

6. To set the mounting height of the camera, go to **Camera mounting height**.

7. To pan the PTZ camera so that it points in the same direction as the radar, go to **Pan alignment**.

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

Set up the PTZ tracking:
9. Go to **Track** to select if you want to track humans, vehicles and/or unknown objects.

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

11. Turn on **Object switching** if you expect multiple objects that won't fit in the camera view.
    With this setting, the radar gives priority of the objects to track.

12. To determine how many seconds to track each object, set **Object hold time**.

13. To make the PTZ camera return to its home position when the radar no longer tracks any objects, turn on **Return to home**.

14. To determine how long the PTZ camera should stay at the tracked objects last known position before returning to home, set **Return to home timeout**.

15. To fine tune the zoom of the PTZ camera, adjust the zoom on the slider.

Control a PTZ camera with AXIS Radar Autotracking for PTZ

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

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

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

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

Set up rules for events

To learn more, check out our guide *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** the device should 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.

Trigger a notification when the enclosure is opened

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

Add an email recipient:

1. Go to **System > Events > Recipients** and click **Add recipient**.

2. Type a name for the recipient.

3. Select **Email** as the notification type.

4. Type the recipient's email address.

5. Type the email address that you want the camera to send notifications from.

6. Provide the login details for the sending email account, along with the SMTP hostname and port number.

7. To test your email setup, click **Test**.

8. Click **Save**.

Create a rule:

9. Go to **System > Events > Rules** and click **Add a rule**.

10. Type a name for the rule.

11. In the list of conditions, select **Casing open**.

12. In the list of actions, select **Send notification to email**.

13. Select a recipient from the list.

14. Type a subject line and message for the email.

15. Click **Save**.

Record video from a camera when motion is detected

This example explains how to set up the radar and a camera so that the camera starts recording to the SD card five seconds before the radar detects motion and to stop one minute after.

Connect the devices:

1. Connect a cable from an I/O output on the radar to an I/O input on the camera.

Configure the I/O port of the radar:

2. Go to **System > Accessories > I/O ports** and configure the I/O port as an output and select the normal state.

Create a rule in the radar:

3. Go to **System > Events** and add a rule.

4. Type a name for the rule.

5. From the list of conditions, select a scenario under **Radar motion**.
    To set up a scenario, see .

6. From the list of actions, select **Toggle I/O while the rule is active** and then select the port that is connected to the camera.

7. Click **Save**.

Configure the I/O port of the camera:

8. Go to **System > Accessories > I/O ports** and configure the I/O port as an input and select the normal state.

Create a rule in the camera:

9. Go to **System > Events** and add a rule.

10. Type a name for the rule.

11. From the list of conditions, select **Digital input is active** and then select the port that should trigger the rule.

12. From the list of actions, select **Record video**.

13. From the list of storage options, select **SD card**.

14. Select an existing stream profile or create a new one.

15. Set the prebuffer to 5 seconds.

16. Set the postbuffer to 1 minute.

17. Click **Save**.

Turn on a light when motion is detected

Turning on a light when an intruder enters the detection zone can have a deterring effect, and will also improve the image quality of a visual camera recording the intrusion.

This example explains how to set up the radar and an illuminator so that the illuminator turns on when the radar detects motion and turns off after one minute.

Connect the devices:
1. Connect one of the illuminator cables to the power supply via the relay port on the radar. Connect the other cable directly between the power supply and the illuminator.

Configure the relay port of the radar:
2. Go to **System > Accessories > I/O ports** and select **Open circuit** as the normal state of the relay port.

Create a rule in the radar:
3. Go to **System > Events** and add a rule.

4. Type a name for the rule.

5. From the list of conditions, select a scenario under **Radar motion**.
To set up a scenario, see .

6. From the list of actions, select **Toggle I/O once** and then select the relay port.

7. Select **Active**.

8. Set the **Duration**.

9. Click **Save**.

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

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

Note

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

Add an email recipient:
1. Go to **System > Events > Recipients** and click **Add recipient**.

2. Type a name for the recipient.

3. Select **Email**.

4. Type an email address to send the email to.

5. The camera doesn't have it's own email server, so it will need to log into another email server to be able to send mails. Fill in the rest of the information according to your email provider.

6. To send a test email, click **Test**.

7. Click **Save**.

Create a rule:

8. Go to **System > Events** and add a rule.

9. Type a name for the rule.

10. From the list of conditions, under **Device status**, select **Radar data failure**.

11. Under **Reason**, select **Tampering**.

12. From the list of actions, under **Notifications**, select **Send notification to email**.

13. Select the recipient you created.

14. Type a subject and a message for the email.

15. Click **Save**.

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.

A文 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

Time sync status

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

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

Ongoing recordings

Shows ongoing recordings and their designated storage space.

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

🗄 ▭ Shows the storage space where the recording is saved.

Device info

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

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

Connected clients

Shows the number of connections and connected clients.

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

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.
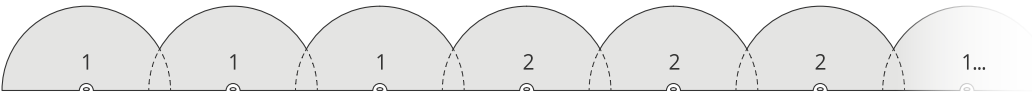
Mounting height: Enter the mounting height for the product.

> 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. The coexistence radius is 350 m (1148 ft).

- **0–1**: Select this option if you mount one to two radars in the same coexistence zone.
- **2**: Select this option if you mount three radars in the same coexistence zone.
- **3–5**: Select this option if you mount four to six radars in the same coexistence zone.
  - **Groups**: Select a group (**Group 1** or **Group 2**) for your radar. This will also help to avoid interference. We recommend that you add three radars in each group, and that you add the radars that are closest to each other in the same group.

For more information, see .

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** (i) : Turn on to minimize false alarms from stationary objects with rotating movements, such as fans or turbines.

  - **Ignore small objects**: Turn on to minimize false alarms from small objects, such as cats or rabbits.

  - **Ignore swaying objects**: Turn on to minimize false alarms from swaying objects, such as trees, bushes, or flagpoles.

- **Road monitoring**: Track vehicles moving at higher speeds in urban zones and on suburban roads

  - **Ignore stationary rotating objects** (i) : Turn on to minimize false alarms from stationary objects with rotating movements, such as fans or turbines.

  - **Ignore swaying objects**: Turn on to minimize false alarms from swaying objects, such as trees, bushes, or flagpoles.

View

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

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

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

Color scheme: Select a theme for the radar visualization.

Rotation (i) : 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.

Exclude zones

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

$+$: Click to create a new exclude zone.

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

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

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

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

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

Scenarios

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

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

Triggering conditions: Select the condition that will trigger alarms.
- **Movement in area**: Select if you want the scenario to trigger on objects moving in an area.
- **Line crossing**: Select if you want 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** ℹ️ : 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** ℹ️ : Select to show an animation superimposed over the video stream. The animation indicates that the video stream is live, even if the scene doesn't contain any motion.

- **Appearance**: Select the animation color and background color, for example, red animation on a transparent background (default).

- **Size**: Select the desired font size.

- ⊞ : Select the position of the overlay in the image or click and drag the overlay to move it around in the live view.

- **Widget: Linegraph** ⓘ : Show a graph chart that displays how a measured value changes over time.
    - **Title**: Enter a title for the widget.

    - **Overlay modifier**: Select an overlay modifier as data source. If you have created MQTT overlays, they will be located at the end of the list.

    - ⊞ : Select the position of the overlay in the image or click and drag the overlay to move it around in the live view.

    - **Size**: Select the size of the overlay.

    - **Visible on all channels**: Turn off to show only on your currently selected channel. Turn on to show on all active channels.

    - **Update interval**: Choose the time between data updates.

    - **Transparency**: Set the transparency of the entire overlay.

    - **Background transparency**: Set the transparency only of the background of the overlay.

    - **Points**: Turn on to add a point to the graph line when data is updated.

    - **X axis**
        - **Label**: Enter the text label for the x axis.

        - **Time window**: Enter how long time the data is visualized.

        - **Time unit**: Enter a time unit for the x axis.

    - **Y axis**
        - **Label**: Enter the text label for the y axis.

        - **Dynamic scale**: Turn on for the scale to automatically adapt to the data values. Turn off to manually enter values for a fixed scale.

        - **Min alarm threshold** and **Max alarm threshold**: These values will add horizontal reference lines to the graph, making it easier to see when the data value becomes too high or too low.

- **Widget: Meter** ⓘ : Show a bar chart that displays the most recently measured data value.
    - **Title**: Enter a title for the widget.

    - **Overlay modifier**: Select an overlay modifier as data source. If you have created MQTT overlays, they will be located at the end of the list.

    - ⊞ : Select the position of the overlay in the image or click and drag the overlay to move it around in the live view.

    - **Size**: Select the size of the overlay.

    - **Visible on all channels**: Turn off to show only on your currently selected channel. Turn on to show on all active channels.

    - **Update interval**: Choose the time between data updates.

    - **Transparency**: Set the transparency of the entire overlay.

    - **Background transparency**: Set the transparency only of the background of the overlay.

    - **Points**: Turn on to add a point to the graph line when data is updated.

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

Radar PTZ autotracking

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

Configure initial settings:

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

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

Save pan offset: Click to save the pan alignment.

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

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

Configure PTZ autotracking:

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

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

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

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

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

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

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

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

Recordings

Ongoing recordings: Show all ongoing recordings on the device.

● Start a recording on the device.

Choose which storage device to save to.

● Stop a recording on the device.

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

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

▷ Play the recording.

□ Stop playing the recording.

∨ ∧ Show or hide information and options about the recording.

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

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

🗑 Click to delete a recording.

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

≡ Click to filter the recordings.

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

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

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

Event: Show recordings based on events.

Storage: Show recordings based on storage type.

Apps

 Add app: Install a new app.

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

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

🔔 View the security updates in AXIS OS and ACAP apps.

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

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

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

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

- **Open-source license**: View information about open-source licenses used in the app.

- **App log**: View a log of the app events. The log is helpful when you contact support.

- **Activate license with a key**: If the app requires a license, you need to activate it. Use this option if your device doesn't have internet access.
  If you don't have a license key, go to *axis.com/products/analytics*. You need a license code and the Axis product serial number to generate a license key.

- **Activate license automatically**: If the app requires a license, you need to activate it. Use this option if your device has internet access. You need a license code to activate the license.

- **Deactivate the license**: Deactivate the license to replace it with another license, for example, when you change from a trial license to a full license. If you deactivate the license, you also remove it from the device.

- **Settings**: Configure the parameters.

- **Delete**: Delete the app permanently from the device. If you don't deactivate the license first, it remains active.

System

Time and location

Date and time

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

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

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

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

Note

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

Device location

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

- **Format**: Select the format to use when you enter your device's latitude and longitude.
- **Latitude**: Positive values are north of the equator.
- **Longitude**: Positive values are east of the prime meridian.
- **Heading**: Enter the compass direction that the device is facing. 0 is due north.
- **Label**: Enter a descriptive name for your device.
- **Save**: Click to save your device location.

Regional settings

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

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

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

Network

IPv4

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

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

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

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

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

Note

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

IPv6

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

Hostname

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

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

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

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

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

DNS servers

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

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

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

HTTP and HTTPS

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

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

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

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

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

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

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

Network discovery protocols

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

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

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

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

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

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

Global proxies

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

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

Allowed formats for http and https proxies:
- http(s)://host:port

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

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

Note

Restart the device to apply the global proxy settings.

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

- Specify an IP address

- Specify an IP address in CIDR format

- Specify a domain name, for example: www.<domain name>.com

- Specify all subdomains in a specific domain, for example .<domain name>.com

One-click cloud connection

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

Allow O3C:

- **One-click**: This is the default option. To connect to O3C, press the control button on the device. Depending on the device model, either press and release or press and hold, until the status LED flashes. Register the device with the O3C service within 24 hours to enable **Always** and stay connected. If you don't register, the device will disconnect from O3C.

- **Always**: The device continuously attempts to connect to an O3C service over the internet. Once you register the device, it stays connected. Use this option if the control button is out of reach.

- **No**: Disconnects the O3C service.

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

Host: Enter the proxy server's address.

Port: Enter the port number used for access.

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

Authentication method:

- **Basic**: This method is the most compatible authentication scheme for HTTP. It's less secure than the **Digest** method because it sends the username and password unencrypted to the server.

- **Digest**: This method is more secure because it always transfers the password encrypted across the network.

- **Auto**: This option lets the device select the authentication method depending on the supported methods. It prioritizes the **Digest** method over the **Basic** method.

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

SNMP

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

SNMP: Select the version of SNMP to use.

- **v1 and v2c:**
    - **Read community**: Enter the community name that has read-only access to all supported SNMP objects. The default value is **public**.

    - **Write community**: Enter the community name that has read or write access to all supported SNMP objects (except read-only objects). The default value is **write**.

    - **Activate traps**: Turn on to activate trap reporting. The device uses traps to send messages for important events or status changes to a management system. In the web interface, you can set up traps for SNMP v1 and v2c. Traps are automatically turned off if you change to SNMP v3 or turn off SNMP. If you use SNMP v3, you can set up traps through the SNMP v3 management application.

    - **Trap address**: Enter the IP address or host name of the management server.

    - **Trap community**: Enter the community to use when the device sends a trap message to the management system.

    - **Traps**:
        - **Cold start**: Sends a trap message when the device starts.

        - **Link up**: Sends a trap message when a link changes from down to up.

        - **Link down**: Sends a trap message when a link changes from up to down.

        - **Authentication failed**: Sends a trap message when an authentication attempt fails.

Note

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

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

Security

Certificates

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

- **Client/server certificates**
  A client/server certificate validates the device's identity, and can be self-signed or issued by a Certificate Authority (CA). A self-signed certificate offers limited protection and can be used before a CA-issued certificate has been obtained.

- **CA certificates**
  You can use a CA certificate to authenticate a peer certificate, for example to validate the identity of an authentication server when the device connects to a network protected by IEEE 802.1X. The device has several pre-installed CA certificates.

These formats are supported:

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

Important

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

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

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

⋮ The context menu contains:

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

Secure keystore ⓘ :

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

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*.

Recipients

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

Note

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

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

Note

You can create up to 20 recipients.

╋ **Add a recipient**: Click to add a recipient.

Name: Enter a name for the recipient.

Type: Select from the list:

- FTP ⓘ
    - **Host**: Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
    - **Port**: Enter the port number used by the FTP server. The default is 21.
    - **Folder**: Enter the path to the directory where you want to store files. If this directory doesn't already exist on the FTP server, you will get an error message when uploading files.
    - **Username**: Enter the username for the login.
    - **Password**: Enter the password for the login.
    - **Use temporary file name**: Select to upload files with temporary, automatically generated filenames. The files get renamed to the desired names when the upload completes. If the upload is aborted/interrupted, you don't get any corrupt files. However, you probably still get the temporary files. This way you know that all files that have the desired name are correct.
    - **Use passive FTP**: Under normal circumstances, the product simply requests the target FTP server to open the data connection. The device actively initiates both the FTP control and data connections to the target server. This is normally needed if there is a firewall between the device and the target FTP server.

- HTTP
    - **URL**: Enter the network address to the HTTP server and the script that will handle the request. For example, http://192.168.254.10/cgi-bin/notify.cgi.
    - **Username**: Enter the username for the login.
    - **Password**: Enter the password for the login.
    - **Proxy**: Turn on and enter the required information if a proxy server must be passed to connect to the HTTP server.

- HTTPS
    - **URL**: Enter the network address to the HTTPS server and the script that will handle the request. For example, https://192.168.254.10/cgi-bin/notify.cgi.
    - **Validate server certificate**: Select to validate the certificate that was created by HTTPS server.
    - **Username**: Enter the username for the login.
    - **Password**: Enter the password for the login.
    - **Proxy**: Turn on and enter the required information if a proxy server must be passed to connect to the HTTPS server.

- Network storage ⓘ
  You can add network storage such as NAS (network-attached storage) and use it as a recipient to store files. The files are stored in the Matroska (MKV) file format.
    - **Host**: Enter the IP address or hostname for the network storage.
    - **Share**: Enter the name of the share on the host.
    - **Folder**: Enter the path to the directory where you want to store files.
    - **Username**: Enter the username for the login.
    - **Password**: Enter the password for the login.

- SFTP ⓘ
  - **Host**: Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
  - **Port**: Enter the port number used by the SFTP server. The default is 22.
  - **Folder**: Enter the path to the directory where you want to store files. If this directory doesn't already exist on the SFTP server, you will get an error message when uploading files.
  - **Username**: Enter the username for the login.
  - **Password**: Enter the password for the login.
  - **SSH host public key type (MD5)**: Enter the fingerprint of the remote host's public key (a 32-digit hexadecimal string). The SFTP client supports SFTP servers using SSH-2 with RSA, DSA, ECDSA, and ED25519 host key types. RSA is the preferred method during negotiation, followed by ECDSA, ED25519, and DSA. Make sure to enter the right MD5 host key that is used by your SFTP server. While the Axis device supports both MD5 and SHA-256 hash keys, we recommend using SHA-256 due to stronger security over MD5. For more information on how to configure an SFTP server with an Axis device, go to the *AXIS OS Portal*.
  - **SSH host public key type (SHA256)**: Enter the fingerprint of the remote host's public key (a 43-digit Base64 encoded string). The SFTP client supports SFTP servers using SSH-2 with RSA, DSA, ECDSA, and ED25519 host key types. RSA is the preferred method during negotiation, followed by ECDSA, ED25519, and DSA. Make sure to enter the right MD5 host key that is used by your SFTP server. While the Axis device supports both MD5 and SHA-256 hash keys, we recommend using SHA-256 due to stronger security over MD5. For more information on how to configure an SFTP server with an Axis device, go to the *AXIS OS Portal*.
  - **Use temporary file name**: Select to upload files with temporary, automatically generated filenames. The files get renamed to the desired names when the upload completes. If the upload is aborted or interrupted, you don't get any corrupt files. However, you probably still get the temporary files. This way, you know that all files that have the desired name are correct.

- SIP or VMS ⓘ :
  SIP: Select to make a SIP call.
  VMS: Select to make a VMS call.
  - **From SIP account**: Select from the list.
  - **To SIP address**: Enter the SIP address.
  - **Test**: Click to test that your call settings works.

- Email
  - **Send email to**: Enter the email address to send emails to. To enter multiple addresses, use commas to separate them.
  - **Send email from**: Enter the email address of the sending server.
  - **Username**: Enter the username for the mail server. Leave this field empty if the mail server does not require authentication.
  - **Password**: Enter the password for the mail server. Leave this field empty if the mail server does not require authentication.
  - **Email server (SMTP)**: Enter the name of the SMTP server, for example, smtp.gmail.com, smtp.mail.yahoo.com.
  - **Port**: Enter the port number for the SMTP server, using values in the range 0-65535. The default value is 587.
  - **Encryption**: To use encryption, select either SSL or TLS.
  - **Validate server certificate**: If you use encryption, select to validate the identity of the device. The certificate can be self-signed or issued by a Certificate Authority (CA).

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

Note

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

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

  - **Port**: Enter the port number used to access the server.

Test: Click to test the setup.

⋮ The context menu contains:

View recipient: Click to view all the recipient details.

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

Delete recipient: Click to delete the recipient permanently.

Schedules

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

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

Manual triggers

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

MQTT

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

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

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

ALPN

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

MQTT client

Connect: Turn on or off the MQTT client.

Status: Shows the current status of the MQTT client.

Broker

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

Protocol: Select which protocol to use.

Port: Enter the port number.

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

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

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

Password: Enter a password for the username.

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

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

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

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

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

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

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

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

Connect message

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

Send message: Turn on to send messages.

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

Topic: Enter the topic for the default message.

Payload: Enter the content for the default message.

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

QoS: Change the QoS layer for the packet flow.

Last Will and Testament message

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

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

Send message: Turn on to send messages.

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

Topic: Enter the topic for the default message.

Payload: Enter the content for the default message.

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

QoS: Change the QoS layer for the packet flow.

MQTT publication

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

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

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

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

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

Retain: Defines which MQTT messages are sent as retained.

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

QoS: Select the desired level for the MQTT publication.

MQTT subscriptions

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

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

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

Subscription type:

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

QoS: Select the desired level for the MQTT subscription.

MQTT overlays

> **Note**
>
> Connect to an MQTT broker before you add MQTT overlay modifiers.

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

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

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

Modifier: Use the resulting modifier when you create the overlay.
- Modifiers that start with **#XMP** show all of the data received from the topic.

- Modifiers that start with **#XMD** show the data specified in the data field.

Storage

Network storage

Ignore: Turn on to ignore network storage.

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

- **Address**: Enter the IP address or host name of the host server, typically a NAS (network-attached storage). We recommend you to configure the host to use a fixed IP address (not DHCP since a dynamic IP address can change) or that you use DNS. Windows SMB/CIFS names are not supported.

- **Network share**: Enter the name of the shared location on the host server. Several Axis devices can use the same network share since each device gets its own folder.

- **User**: If the server requires a login, enter the username. To log in to a specific domain server, type `DOMAIN\username`.

- **Password**: If the server requires a login, enter the password.

- **SMB version**: Select the SMB storage protocol version to connect to the NAS. If you select **Auto**, the device tries to negotiate one of the secure versions SMB: 3.02, 3.0, or 2.1. Select 1.0 or 2.0 to connect to older NAS that don't support higher versions. You can read more about SMB support in Axis devices *here*.

- **Add share without testing**: Select to add the network share even if an error is discovered during the connection test. The error can be, for example, that you didn't enter a password even though the server requires one.

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

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

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

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

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

Tools

- **Test connection**: Test the connection to the network share.

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

Use tool: Click to activate the selected tool.

Onboard storage

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

Unmount: Click to safely remove the SD card.

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

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

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

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

Tools

- **Check**: Check for errors on the SD card.

- **Repair**: Repair errors in the file system.

- **Format**: Format the SD card to change the file system and erase all data. You can only format the SD card to the ext4 file system. You need a third-party ext4 driver or application to access the file system from Windows®.

- **Encrypt**: Use this tool to format the SD card and enable encryption. This erases all data stored on the SD card. Any new data you store on the SD card will be encrypted.

- **Decrypt**: Use this tool to format the SD card without encryption. This erases all data stored on the SD card. Any new data you store on the SD card will not be encrypted.

- **Change password**: Change the password required to encrypt the SD card.

Use tool: Click to activate the selected tool.

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

Stream profiles

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

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

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

Name: Add a name for your profile.

Description: Add a description of your profile.

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

Resolution: See for a description of this setting.

Frame rate: See for a description of this setting.

Compression: See for a description of this setting.

Zipstream ⓘ : See for a description of this setting.

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

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

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

Mirror ⓘ : See for a description of this setting.

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

Bitrate control: See for a description of this setting.

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

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

ONVIF

ONVIF accounts

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

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

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

Account: Enter a unique account name.

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

Repeat password: Enter the same password again.

Role:

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

- **Operator**: Has access to all settings except:
  - All **System** settings.
  - Adding apps.

- **Media account**: Allows access to the video stream only.

⋮ The context menu contains:

Update account: Edit the account properties.

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

ONVIF media profiles

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

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

Profile name: Add a name for the media profile.

Video source: Select the video source for your configuration.

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

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

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

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

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

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

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

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

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

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

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

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

Metadata: Select the metadata to include in your configuration.

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

PTZ ⓘ : Select the PTZ settings for your configuration.

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

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

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

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

Detectors

Shock detection

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

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

Accessories

I/O ports

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

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

Port

Name: Edit the text to rename the port.

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

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

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

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

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

Edge-to-edge

Pairing

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

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

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

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

+ Add: Add a device to pair with.

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

> **Note**
>
> The list will show all Axis devices that are found, not only devices that can be paired.
>
> Only devices with **Bonjour** enabled can be found. To enable **Bonjour** for a device, open the device's web interface and go to **System > Network > Network discovery protocols**.

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

To pair a device from the list, click **+** .

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

Speaker pairing: Select to pair a network speaker.

Microphone pairing : Select to pair a microphone.

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

Username: Enter username.

Password: Enter password for the user.

Close: Click to clear all fields.

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

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

┼ **Add**: Add a device to pair with.

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

> Note
>
> The list will show all Axis devices that are found, not only devices that can be paired.
>
> Only devices with **Bonjour** enabled can be found. To enable **Bonjour** for a device, open the device's web interface and go to **System > Network > Network discovery protocols**.

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

To pair a device from the list, click ┼ .

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

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

Username: Enter the username of the PTZ camera.

Password: Enter the password for the PTZ camera.

Close: Click to clear all fields.

Connect: Click to establish connection to the PTZ camera.

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

Logs

Reports and logs

Reports

- **View the device server report**: View information about the product status in a pop-up window. The Access Log is automatically included in the Server Report.

- **Download the device server report**: It creates a .zip file that contains a complete server report text file in UTF–8 format, as well as a snapshot of the current live view image. Always include the server report .zip file when you contact support.

- **Download the crash report**: Download an archive with detailed information about the server's status. The crash report contains information that is in the server report as well as detailed debug information. This report might contain sensitive information such as network traces. It can take several minutes to generate the report.

Logs

- **View the system log**: Click to show information about system events such as device startup, warnings, and critical messages.

- **View the access log**: Click to show all failed attempts to access the device, for example, when a wrong login password is used.

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.

- **Autorollback**: 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**.

Validate your installation

Validate the installation of the radar

Note

This test helps you to validate your installation under current conditions. The everyday performance of your installation can be affected by changes in the scene.

The radar is ready to use as soon as it is installed, however, we recommend that you perform a validation before you start to use it. This can increase the accuracy of the radar by helping you to identify any problems with the installation or manage objects (such as trees and reflective surfaces) in the scene.

First before attempting the validation.

It is a good idea to perform the validation whenever:
- There are objects in the scene that you want to exclude so that the zones can contain certain objects such as vegetations or metal surfaces.
- You pair the radar with a PTZ camera and want to configure **Radar autotracking**.
- The radar mounting height has changed.

Validate the radar

Check that there are no false detections

1. Check that the detection zone is clear from human activity.
2. Wait for a few minutes to ensure that the radar is not detecting any static objects in the detection zone.
3. If there are no unwanted detections you can skip step 4.
4. If there are unwanted detections, learn how to filter out certain types of movement or objects, change the coverage, or adjust the detection sensitivity in .

Check for the correct symbol and direction of travel when the radar is approached from the front

1. Go into the radar's web interface and record the session. For help doing this, go to .
2. Start 60 m (197 ft) in front of the radar and walk directly towards the radar.
3. Check the session in the radar's web interface. The symbol for a human classification should appear when you are detected.
4. Check that the radar's web interface shows the correct direction of travel.
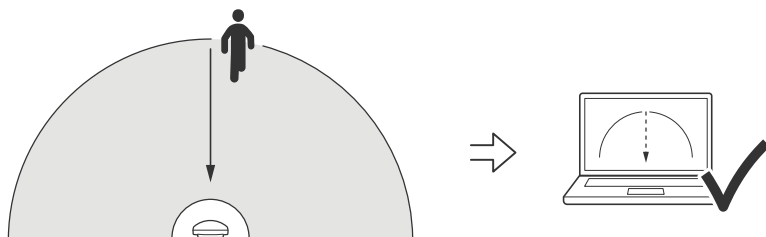
Check for the correct symbol and direction of travel when the radar is approached from the side

1. Go into the radar's web interface and record the session. For help doing this, go to .
2. Start 60 m (197 ft) out from the radar and walk straight across the radar coverage area.
3. Check that the radar's web interface shows the symbol for a human classification.
4. Check that the radar's web interface shows the correct direction of travel.
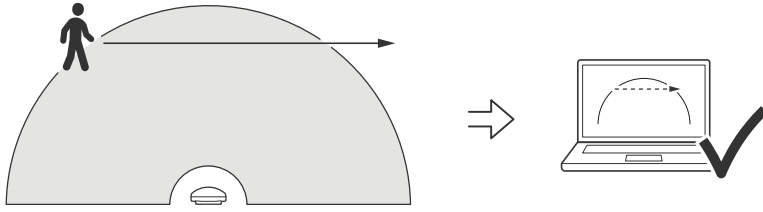
Create a table similar to the one below to help you record the data from your validation.

Test	Pass/Fail	Comment
1. Check that there are no unwanted detections when the area is clear		
2a. Check that the object is detected with the correct symbol for 'Human' when the radar is approached from the front		
2b. Check that the direction of travel is correct when the radar is approached from the front		
3a. Check that the object is detected with the correct symbol for 'Human' when the radar is approached from the side		
3b. Check that the direction of travel is correct when the radar is approached from the side		

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 and followed the instructions.

2. For further validation, add and calibrate a reference map.

3. Set the radar scenario to trigger when an appropriate object is detected. By default, **seconds until trigger** is set to two seconds but you can change this in the web interface if needed.

4. Set the radar to record data when an appropriate object is detected.
   See for instructions.

5. 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, it can be disabled.

6. Walk along the border of the radar coverage area and make sure that the trailing on the system matches the route that you walked.

7. If you are unsatisfied with the results of your validation, re-calibrate the reference map and repeat the validation.

Learn more

Streaming and storage

Video compression formats

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

Motion JPEG

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

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

H.264 or MPEG-4 Part 10/AVC

Note

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

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

H.265 or MPEG-H Part 2/HEVC

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

Note

- H.265 is licensed technology. The Axis product includes one H.265 viewing client license. Installing additional unlicensed copies of the client is prohibited. To purchase additional licenses, contact your Axis reseller.

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

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.
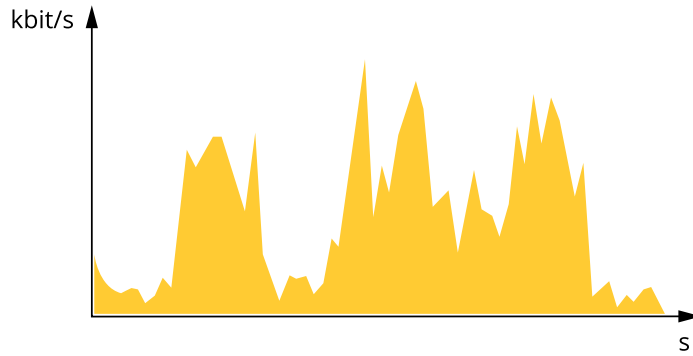
Maximum bitrate (MBR)

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.
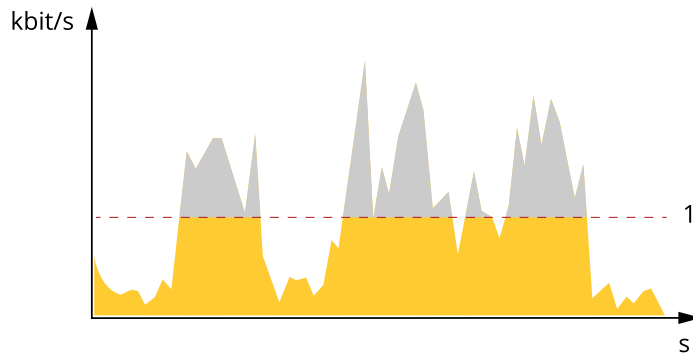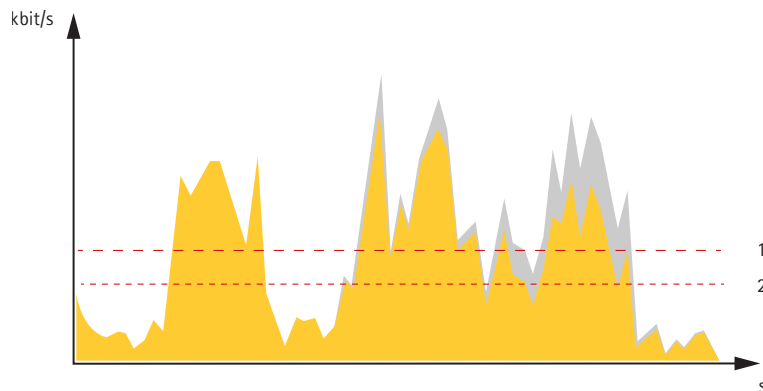

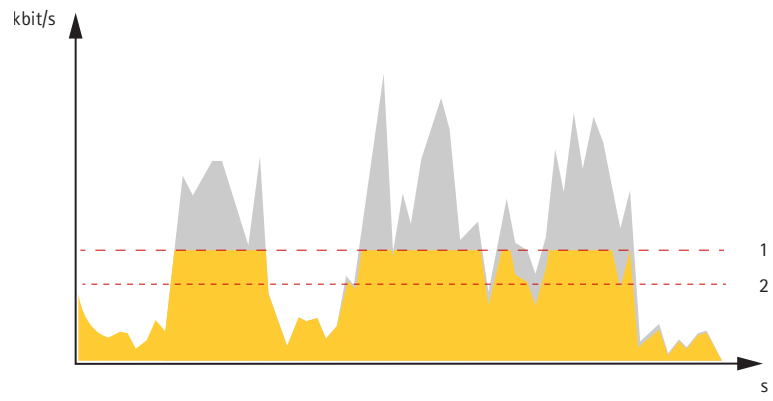*1   Target bitrate*

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
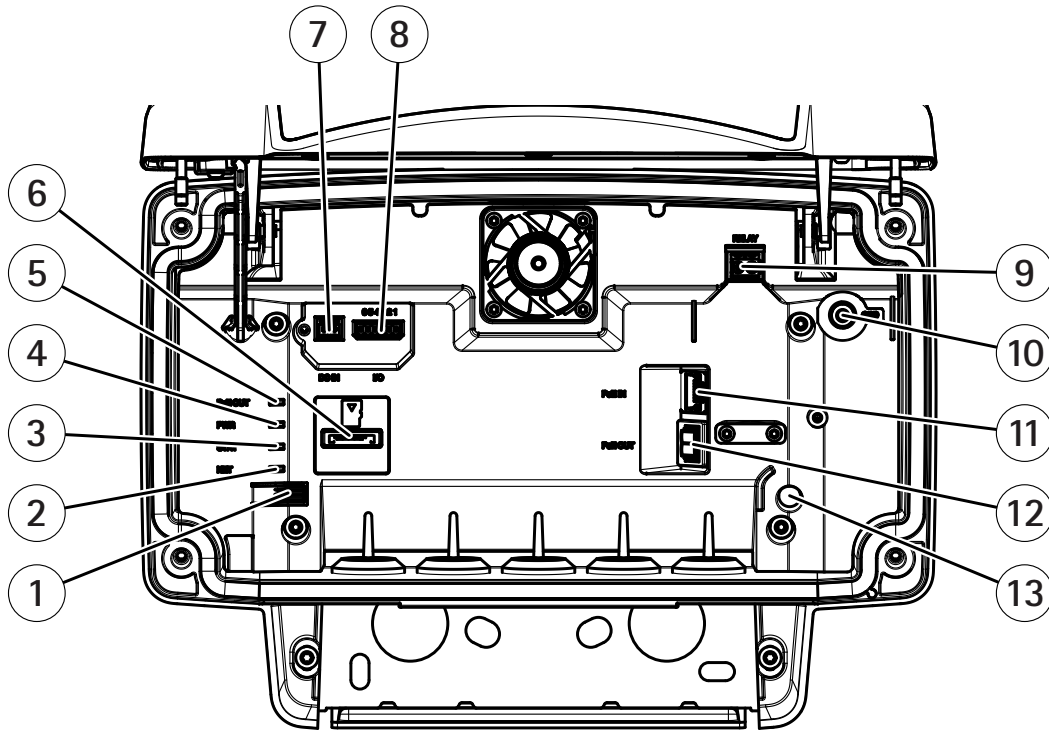*2   Actual average bitrate*

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

70

1　Target bitrate
2　Actual average bitrate

Specifications

Product overview

1   Control button
2   Network LED
3   Status LED
4   Power LED
5   PoE out LED
6   microSD card slot
7   Power connector (DC)
8   I/O connector
9   Relay connector
10 Grounding screw
11 Network connector (PoE in)
12 Network connector (PoE out)
13 Intrusion alarm sensor

For technical specifications, see .

LED Indicators

Status LED	Indication
Green	Steady green for normal operation.

Network LED	Indication
Green	Steady for connection to a 100 Mbit/s network. Flashes for network activity.
Amber	Steady for connection to a 10 Mbit/s network. Flashes for network activity.
Unlit	No network connection.

Power LED	Indication
Green	Normal operation.

PoE out LED	Indication
Unlit	PoE out turned off
Green	PoE out turned on

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

For location of the control button, see .
The control button is used for:
- Resetting the product to factory default settings. See .

- Connecting to an AXIS Video Hosting System service. See . To connect, press and hold the button for about 3 seconds until the Status LED flashes green.

Connectors

Network connector

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

⚠ CAUTION
Risk of damage to the device. Do not power the device with both PoE and DC.

Network connector (PoE out)

Power over Ethernet IEEE 802.3at type 2, max 30W

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

Note
The PoE output is enabled when the radar is powered by a 60 W midspan (Power over Ethernet IEEE 802.3bt, type 3).

Note
If the radar is powered by a 30 W midspan or DC power, 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.

Note

If the connected PoE device requires more than 30 W, you can add a 60 W midspan between the PoE out port on the radar and the device. The midspan will power the device while the security radar will provide the Ethernet connection.
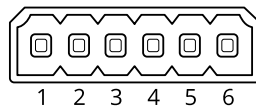
I/O connector

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

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

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

6-pin terminal block

| Function	Pin	Notes	Specifications
DC ground	1		0 VDC
DC output	2	⚠️ Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	12 VDC Max load = 50 mA
Configurable (Input or Output)	3–6	Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 VDC
		Digital output – Internally connected to pin 1 (DC ground) when active, and floating (unconnected) when inactive. If used with an inductive load, e.g., a relay, connect a diode in parallel with the load, to protect against voltage transients.	0 to max 30 VDC, open drain, 100 mA

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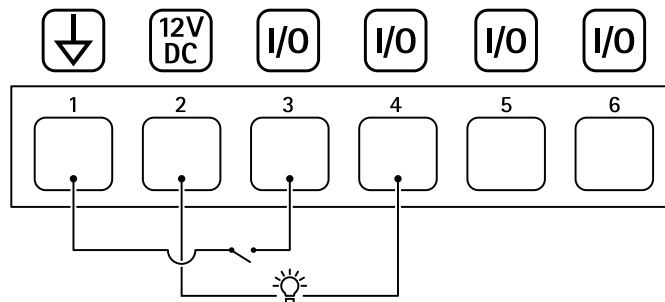
1   DC ground
2   DC output 12 V, max 50 mA
3   I/O configured as input
4   I/O configured as output
5   Configurable I/O
6   Configurable I/O

Power connector

2-pin terminal block for DC power input. Use a Safety Extra Low Voltage (SELV) compliant limited power source (LPS) with either a rated output power limited to ≤100 W or a rated output current limited to ≤5 A.
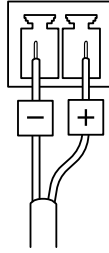
⚠ **CAUTION**
Risk of damage to the device. Do not power the device with both PoE and DC.

Relay connector
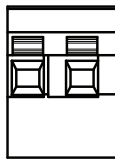
⚠ **CAUTION**
Use single core wires for the relay connector.

Function	Specifications
Type	Normally open
Rating	24 V DC/5 A
Isolation from other circuitry	2.5 kV

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**.

Check the current AXIS OS version

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

To check the current AXIS OS version:

1. Go to the device's web interface > **Status**.

2. Under **Device info**, see the AXIS OS version.

Upgrade AXIS OS

Important

- Preconfigured and customized settings are saved when you upgrade the device software (provided that the features are available in the new AXIS OS) although this is not guaranteed by Axis Communications AB.

- Make sure the device remains connected to the power source throughout the upgrade process.

Note

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

1. Download the AXIS OS file to your computer, available free of charge at *axis.com/support/device-software*.

2. Log in to the device as an administrator.

3. Go to **Maintenance > AXIS OS upgrade** and click **Upgrade**.

When the upgrade has finished, the product restarts automatically.

Technical issues, clues, and solutions

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

Problems upgrading AXIS OS

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

Problems setting the IP address

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

The device can't be accessed from a browser

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

The device is accessible locally but not externally

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

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

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

Can't connect over port 8883 with MQTT over SSL

The firewall blocks traffic using port 8883 as it's deemed insecure.	In some cases the server/broker might not provide a specific port for MQTT communication. It may still be possible to use MQTT over a port normally used for HTTP/HTTPS traffic.

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

Performance considerations

When setting up your system, it is important to consider how various settings and situations affect the amount of needed bandwidth (the bitrate) required.

The following factors are the most important to consider:

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