AXIS D2210-VE Radar

User manual

Table of Contents

Installation 3
- Installation guide 3
- Considerations 3

Radar profiles 5
- Area monitoring profile 5
- Road monitoring profile 7

Get started 12
- Find the device on the network 12
- Open the device's web interface 12
- Set a new password for the root account 12
- Secure passwords 12
- Verify that no one has tampered with the firmware 13
- Web interface overview 13

Configure your device 14
- Calibrate the radar 14
- Set detection zones 15
- Minimize false alarms 17
- Adjust the radar image 17
- View and record video 18
- Add a LED strip pattern 19
- Set up rules for events 19

The web interface 24
- Status 24
- Radar 25
- Recordings 29
- Apps 30
- System 30
- Maintenance 46

Validate your installation 47
- Validate the installation of the radar 47
- Complete the validation 48

Learn more 49
- Streaming and storage 49
- Overlays 51

Specifications 52
- Product overview 52
- LED indicators 52
- SD card slot 53
- Buttons 53
- Connectors 53

Cleaning recommendations 56

Troubleshooting 57
- Reset to factory default settings 57
- Check the current firmware version 57
- Upgrade the firmware 57
- Technical issues, clues, and solutions 57
- Performance considerations 59
- Contact support 59

Installation

Installation guide

The installation guide and other documents for this product can be found on *axis.com/products/axis-d2210-ve-radar/support*

Considerations

Where to install the product

Open areas

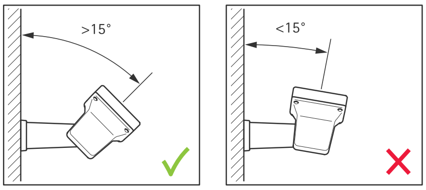
The product is intended for monitoring open areas. Any solid object (such as a wall, a fence, a tree, or a large bush) in the coverage area will create a blind spot (radar shadow) behind it.

Metal objects in the field of view cause reflections that affect the ability of the radar to perform classifications. This can lead to ghost tracks and false alarms in the radar stream. For information about how to handle reflective surfaces, see *Add exclude zones on page 16*.

Positioning

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

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

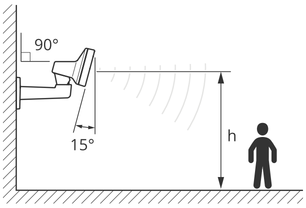


Roll angle

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

Tilt angle

The radar can be tilted 0-30°, but the recommended mounting tilt of the device is 15°. To help you achieve 15° tilt, make sure the back part of the chassis is level, as shown in the illustration.



Coexistence

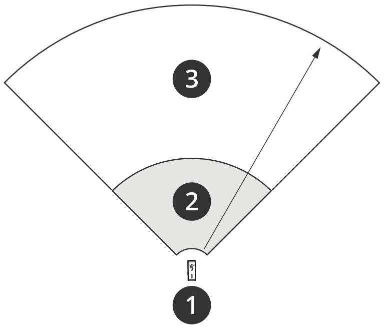
If you mount more than 8 radars operating on the same frequency band close together, they may interfere with each other. To avoid interference, see *Install multiple radars on page 4* .

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

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

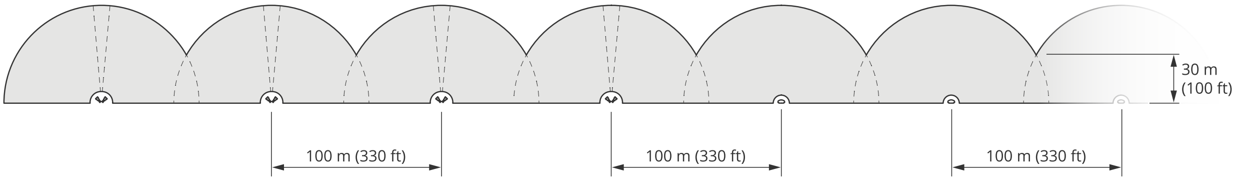


1 *Radar*
2 *Detection area*
3 *Coexistence zone*

This radar operates on the 61 GHz frequency band. You can install up to eight radars operating on the 61 GHz frequency band close to each other, or facing each other, without causing problems. The built-in coexistence algorithm can find a suitable time and frequency slot to operate in to minimize interference.

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

You can combine this radar with Axis radars operating on another frequency band without having to think about coexistence. Axis radars operating on different frequency bands will not interfere with each other.



Four pairs of AXIS D2210-VE Radars and multiple AXIS D2110-VE Security Radars mounted side-by-side.

Environment

There are also other design factors to check when placing multiple radars in a site, like the surrounding environment, swaying objects, flag poles, and swaying vegetation. In some cases you need to filter out swaying objects from the radar stream to avoid false alarms.

Radar profiles

You can use the radar for area monitoring or road monitoring. There are two profiles that are optimized for each one of the scenarios:

- **Area monitoring profile**: track both large and small objects moving at speeds lower than 55 km/h (34 mph)
- **Road monitoring profile**: track mainly vehicles moving at speeds up to 200 km/h (124 mph)

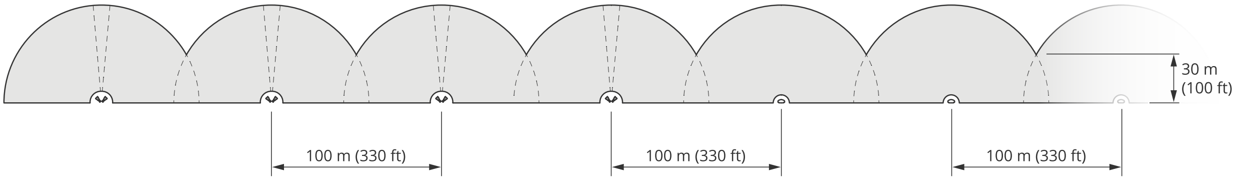
Area monitoring profile

Area monitoring profile is best used 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 event when any of these objects is detected. If you want to track only vehicles, use the *Road monitoring profile on page 7* .

Area installation examples

You can place multiple radars side-by-side to create a virtual fence, for example along or around a building

If you place two AXIS D2210-VE Radars next to each other, you can get 180° coverage. When you install more than one pair of AXIS D2210-VE side-by-side, we recommend placing them with 100 m (330 ft) spacing between each pair, as shown in the example.



Four pairs of AXIS D2210-VE Radars and three AXIS D2110-VE Security Radars mounted side-by-side.

You can combine the radar with other Axis radars operating on another frequency band without interference. In the example, eight AXIS D2210-VE Radars operating on the 61 GHz frequency band are placed next to multiple AXIS D2110-VE Security Radars operating on the 24 GHz frequency band. See *Install multiple radars on page 4* for more information.

Area detection range

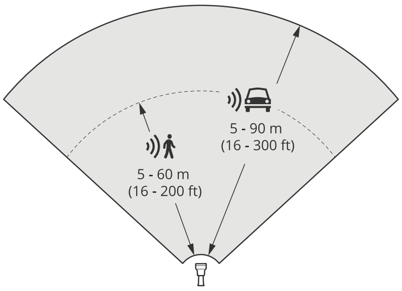
The detection range is the distance within which an object can be tracked and can trigger an alarm. It is measured from a near detection limit (how close to the device a detection can be made) to a far detection limit (how far from the device a detection can be made).

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

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

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

Radar profiles



Note

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

The radar detection range was measured under these conditions:

- The range was measured along the ground.
- The object was a 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	5° tilt	10° tilt	15° tilt	20° tilt	25° tilt	30° tilt
3.5 m (11 ft)	6.0–60+ m (19–196+ ft)	5.0–60+ m (16–196+ ft)	4.0–60+ m (13–196+ ft)	4.0–60 m (13–196 ft)	4.0–55 m (13– 180 ft)	4.0–40 m (13–131 ft)	4.0–30 m (13–98 ft)
4.5 m (14 ft)	6.0–60+ m (19–196+ ft)	6.0–60+ m (19–196+ ft)	5.0–60+ m (16–196+ ft)	4.0–60+ m (13–96+ ft)	4.0–60 m (13–196 ft)	4.0–45 m (13–147 ft)	4.0–40 m (13–131 ft)
6 m (19 ft)	10–60+ m (32–196+ ft)	9.0–60+ m (29–196+ ft)	7.0–60+ m (22–196+ ft)	6.0–60+ m (19–196+ ft)	6.0–60 m (19–196 ft)	5.0–55 m (16–180 ft)	5.0–55 m (16–180 ft)
8 m (26 ft)	16–60 m (52–196 ft)	14–60 m (45–196 ft)	10–60 m (32–196 ft)	8.0–60+ m (26–196+ ft)	8.0–60+ m (26–196+ ft)	7.0–60 m (22–196 ft)	7.0–60 m (22–196 ft)
10 m (32 ft)	21–60 m (68–196 ft)	19–60 m (62–196 ft)	14–60 m (45–196 ft)	12–60+ m (39–196+ ft)	10–60+ m (32–196+ ft)	9.0–60 m (29–196 ft)	9.0–60 m (29–196 ft)
12 m (39 ft)	25–60 m (82–196 ft)	23–60 m (75–196 ft)	19–60 m (62–196 ft)	16–60+ m (52–196+ ft)	13–60+ m (42–196+ ft)	11–60+ m (36–196+ ft)	11–55 m (36–180 ft)

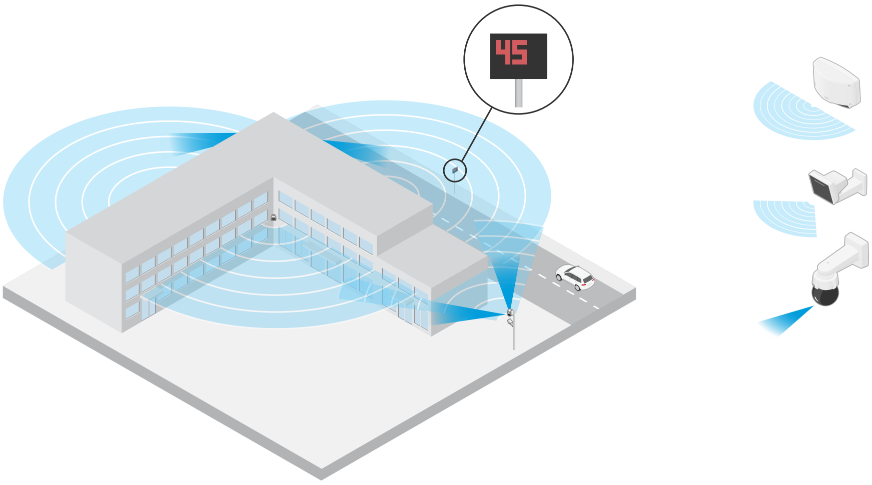
Note

- Setting the radar sensitivity to **Low** will decrease the detection range by 20% while setting it to **High** will increase the detection range by 20%.

Area monitoring use cases

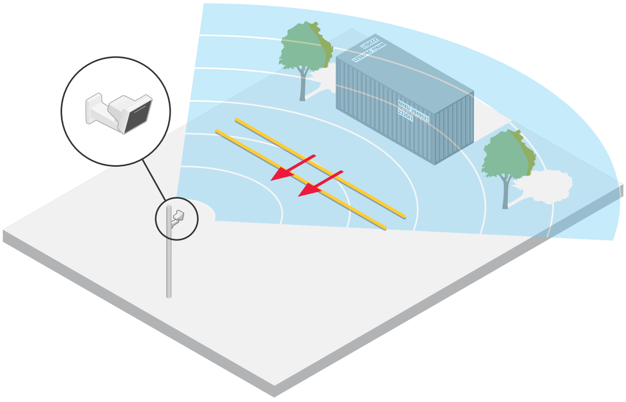
Cover the area around a building

...



Cover an area with swaying objects and reflective surfaces

...



Road monitoring profile

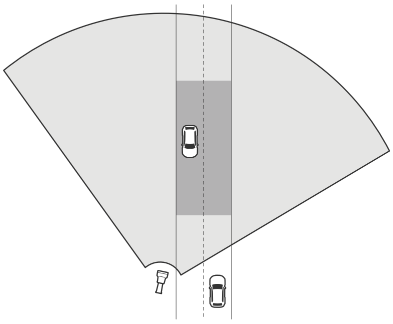
The **Road monitoring profile** is best used to track vehicles moving at up to 200 km/h (124 mph) on sub-urban roads and highways. This mode is mainly used to track vehicles. To track humans and other objects moving at lower speeds, use the *Area monitoring profile on page 5* .

Road installation examples

Side mounted

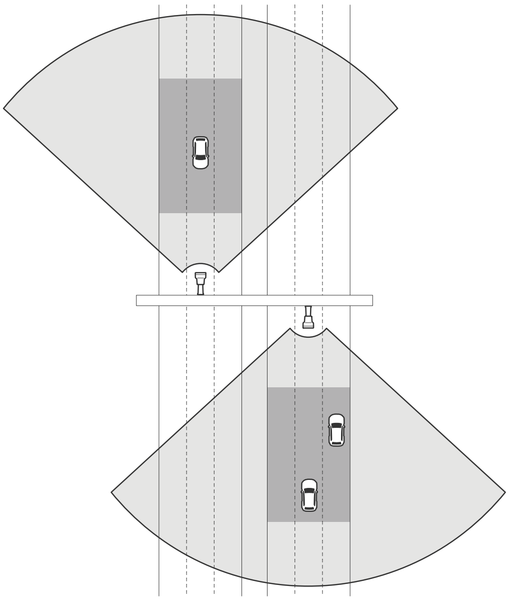
To monitor vehicles travelling along a road you can mount the radar on to the side of the road, for example on a pole.

Radar profiles



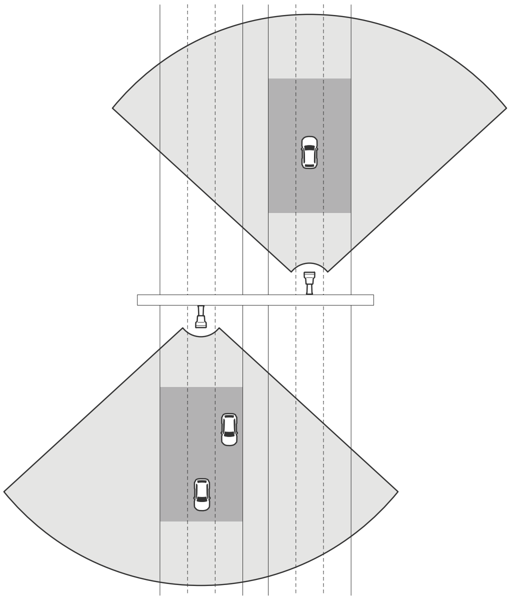
Center mounted

In this example, two radars are used to monitor vehicles on a multi-lane road. The radars are mounted on a gantry above the road.



The same type of installation is possible if you wish to monitor vehicles when driving away from the radar, instead of driving towards it.

Radar profiles



Note

We recommend that the radar is mounted at a height between X m (X ft) and X m (X 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 200 km/h (124 mph).

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

- **X–X m (X–X ft)** for vehicles moving at X km/h (X mph).
- **X–X m (X–X ft)** for vehicles moving at X km/h (X mph).

Note

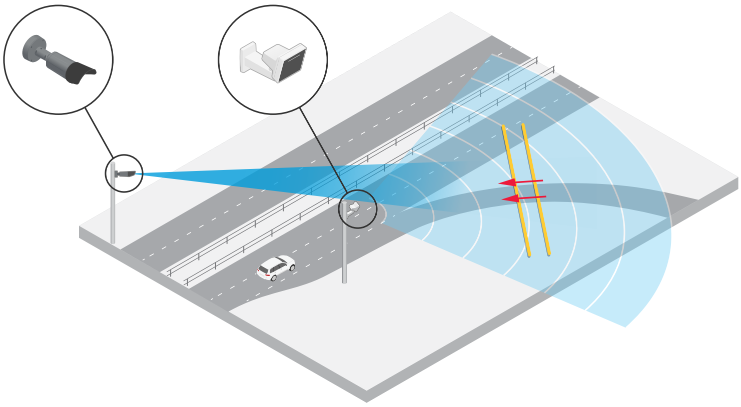
If the maximum number of radars in the same coexistence zone exceeds two then expect a range degradation of approximately 10% (near) and 20% (far).

Road monitoring use cases

Wrong-way detection on a highway ramp

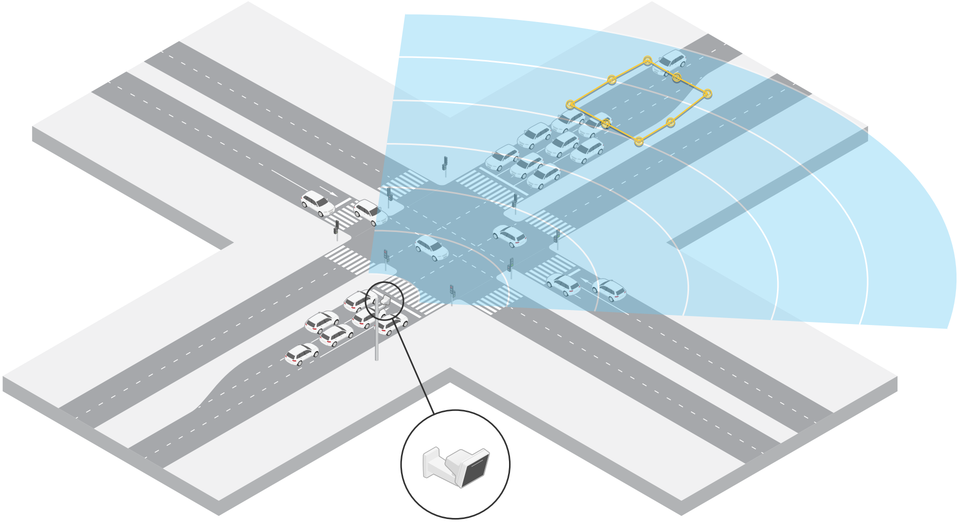
To detect and identify vehicles driving in the wrong direction onto a highway ramp, traffic control uses a radar and a camera. The radar is mounted on a pole facing the highway ramp to detect vehicles driving in the wrong direction. For reliable detections, they set up a scenario in the web interface of the radar with two lines positioned on the ramp. To trigger an alarm, vehicles must pass both lines in the specified direction and within a specified speed range. When the radar triggers an alarm, an Axis bullet camera zooms in on the highway ramp for visual identification of the vehicle.

Radar profiles



Monitor traffic flow at an intersection – queue build-up

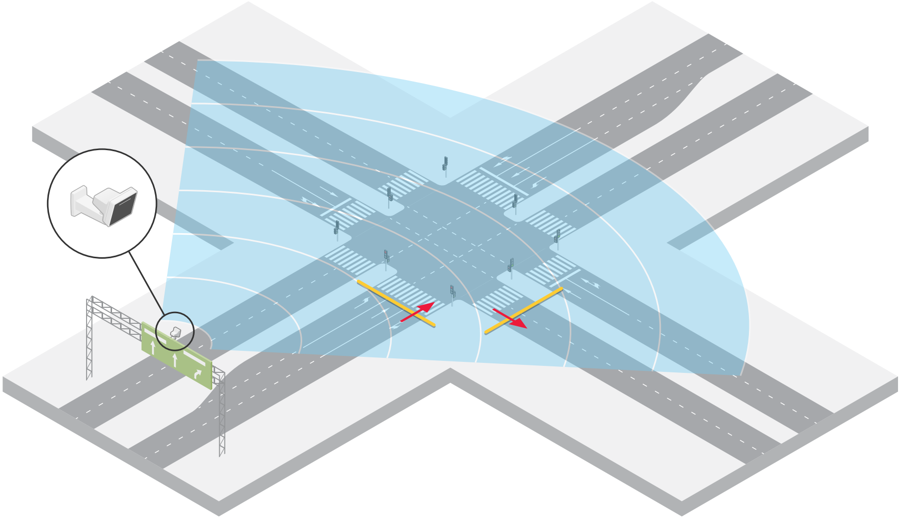
To monitor how and when queues build up in a busy intersection, traffic control installs a radar on a pole on the side of the intersection. They set up a scenario in the web interface of the radar that only covers the part of the road leading up to the intersection. To trigger an alarm, vehicles must drive in slow speeds or come to a stop in the specified area.



Monitor traffic flow at an intersection – direction

To get an overview of the traffic flow and the direction vehicles travel in a busy intersection, traffic control installs a radar on a gantry above the road leading up to the intersection. They set up a scenario in the web interface of the radar where they position two lines in the intersection. The first line covers the lanes leading up to the intersection, and the second line covers the lanes leading to the right. To count the number of vehicles taking a right turn, the vehicles must cross both lines in the specified direction.

To count vehicles travelling in the other directions, a new scenario where the vehicles are required to cross two lines must be set up for each direction.



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

To use AXIS OS web interface with iOS 15 or iPadOS 15, go to **Settings > Safari > Advanced > Experimental Features and disable NSURLSession Websocket.*

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 set the root password. See *Set a new password for the root account on page 12*.

Set a new password for the root account

The default administrator username is `root`. There's no default password for the root account. You set a password the first time you log in to the device.

1. Type a password. Follow the instructions about secure passwords. See *Secure passwords on page 12*.
2. Retype the password to confirm the spelling.
3. Click **Add user**.

Important

If you lose the password for the root account, go to *Reset to factory default settings on page 57* and follow the instructions.

Secure passwords

Important

Axis devices send the initially set password in clear text over the network. To protect your device after the first login, set up a secure and encrypted HTTPS connection and then change the password.

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.

Verify that no one has tampered with the firmware

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

1. Reset to factory default settings. See *Reset to factory default settings on page 57*.

   After the reset, secure boot guarantees the state of the device.

2. Configure and install the device.

Web interface overview

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

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

help.axis.com/?&piaId=92321&section=web-interface-overview

Axis device web interface

Configure your device

Calibrate the radar

The default live view of the radar will show the radar coverage and any detected movement, and you can add detection zones and rules right away. To make it easier to see where objects are moving, upload a reference map, for example a ground plan or an aerial photo, that shows the area covered by the radar.

Image requirements for the reference map:

- Supported file formats are jpeg and png.
- The orientation is not important, since the radar coverage shape will move to adapt to the image during calibration.

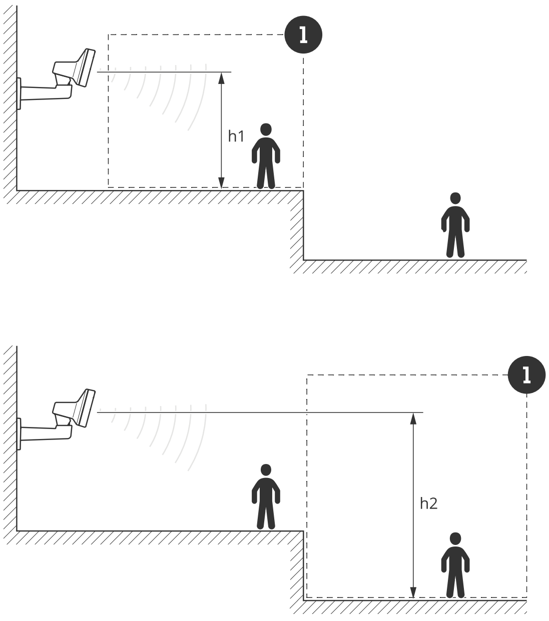
Before you upload a reference map and calibrate the radar, set the correct mounting height in the radar web interface.

Set the mounting height

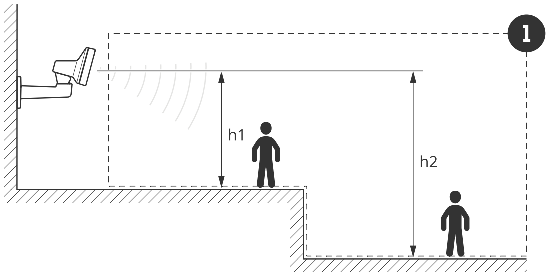
Measure the mounting height from the ground up to the radar in the area of interest.

Example

Examples of mounting height (h1, h2) in different areas of interest (1).



If the surface in the area of interest is uneven, add the average height (in this case *h1 + h2 / 2*) when you configure the radar.



Set the mounting height:

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

Upload a reference map

Upload the reference map and calibrate it so that the actual radar coverage fits the position, direction and scale of the map.

1. Go to **Radar > Map calibration**.
2. Upload your reference map and follow the setup assistant.

Set detection zones

To determine where to detect motion, you can add multiple zones. Different zones can be used 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 (previously called an include zone) is an area in which moving objects will trigger rules. Add scenarios if you want to create different events 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 a line.

Trigger on objects moving in an area:

1. Select **Object moving in area**.
2. Click **Next**.
3. Select the 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.
   - 5.1 Add seconds until trigger.
   - 5.2 Select which object type to trigger on.
   - 5.3 Add a range for the speed limit.
6. Click **Save**.

Trigger on objects crossing a line:

1. Select **Object crossing line**.
2. Click **Next**.
3. Position the line in the scene.

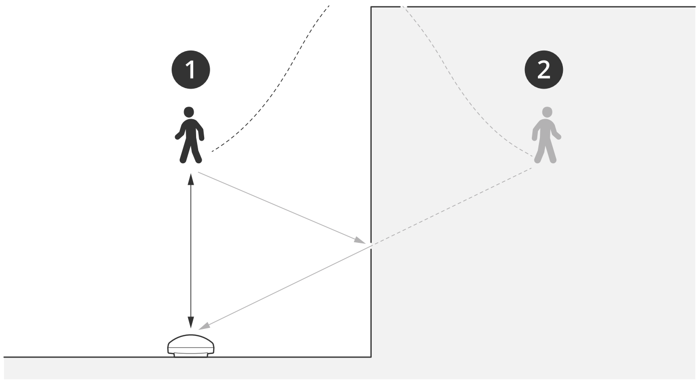
   Use the mouse to move and shape the line.
4. To change the detection direction, turn on **Change direction**.
5. Click **Next**.
6. Add detection settings.
   - 6.1 Add seconds until trigger.
   - 6.2 Select which object type to trigger on.
   - 6.3 Add a range for the speed limit.
7. Click **Save**.

Add exclude zones

Exclude zones are areas in which moving objects will be ignored. Add exclude zones to ignore areas with moving objects that could cause false alarms.

Example

Objects of radar-reflective materials, such as metal roofs, fences, vehicles, and even brick walls may disturb the radar's performance. They may create reflections, or ghost tracks, which cause apparent detections that can be difficult to separate from real detections.



1 Actual detection
2 Reflected detection

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 image or reference map.

Note

From firmware version 11.4, there are no longer any limitations on the number of exclude zones.

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. In this case, modify the scenario, see *Add scenarios on page 15* for more information, or add an exclude zone that ignores everything in the zone, see *Add exclude zones on page 16*.

- Filter on movement:

  Go to **Radar > Settings > Detection** and select **Ignore swaying objects**. This setting will minimize false alarms from trees, bushes, and flagpoles in the coverage zone.

- 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.

Adjust the radar image

This section includes instructions about configuring your device. If you want to learn more about how certain features work, go to *Learn more on page 49*.

Show an image overlay

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

1. Go to **Radar > Overlays**.
2. Select **Image** and click + .
3. Click **Images**.
4. Drag and drop an image.
5. Click **Upload**.
6. Click **Manage overlay**.
7. Select the image and a position. You can also drag the overlay image in the live view to change the position.

Show a text overlay

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

1. Go to **Radar > Overlays**.
2. Select **Text** and click + .
3. Type the text you want to display in the video stream.
4. Select a position. You can also drag the overlay text field in the live view to change the position.

View and record video

This section includes instructions about configuring your device. To learn more about how streaming and storage works, go to *Streaming and storage on page 49*.

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 even if connection fails** 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 *Set up network storage on page 19*
3. To stop recording, click ● again.

Watch video

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

Add a LED strip pattern

The dynamic LED strip on the front of the radar can play different color and light patterns. You can create a rule to trigger a pattern, or use the LED strip as an indication LED.

1. Go to **Radar > Dynamic LED strip**.
2. Select a predefined color and light pattern under **Pattern**.
3. Select if you want to activate the pattern once or continuously under **Type**.

   One-shot activates the pattern once.
4. If you activate the pattern once, set the duration in milliseconds under **Duration**.

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.

Note

If you change the definition of a stream profile that is used in a rule, then you need to restart all the rules that use that stream profile.

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 *Add scenarios on page 15*.

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**.

Record video from a camera when a vehicle drives in the wrong direction

This example explains how to set up the radar and a camera so that the camera starts recording to an SD card when the radar detects a vehicle that drives in the wrong direction.

Before you start

- Create a scenario in the radar's web interface that triggers on line crossing and vehicles crossing two lines.

  See *Add scenarios on page 15* for more information.

- Make sure to position the two lines over the traffic lane where you want to detect vehicles driving in the wrong direction. Use a reference map, such as an aerial photo, to make it easier to see where objects are moving.

  See *Upload a reference map on page 15* for more information.

1. Create two recipients in the radar.

   1.1 In the radar's device interface, go to **System > Events > Recipients** and add the first recipient.

   1.2 Add the following information:

   - **Name**: Activate virtual port
   - **Type**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/virtualinput/activate.cgi

     Replace <IPaddress> with the address of the camera you want to start recording.
   - The username and password of the camera.

   1.5 Click **Test** to make sure all data is valid.

   1.6 Click **Save**.

   1.7 Add a second recipient with the following information:

   - **Name**: Deactivate virtual port
   - **Type**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi

     Replace <IPaddress> with the address of the camera.
   - The username and password of the camera.

   1.5 Click **Test** to make sure all data is valid.

   1.6 Click **Save**.

2. Create two rules in the radar.

   2.1 In the radar's device interface, go to **System > Events > Rules** and add the first rule.

2.2 Add the following information:

- **Name**: Activate virtual IO1
- **Condition**: Select the scenario you created under **Radar motion**.
- **Action**: **Notifications > Send notification through HTTP**
- **Recipient**: **Activate virtual port**
- **Query string suffix**: schemaversion=1&port=1

2.6 Click **Save**.

2.7 Add another rule with the following information:

- **Name**: Deactivate virtual IO1
- **Condition**: Select the scenario you created under **Radar motion**.
- Select **Invert this condition**.
- **Action**: **Notifications > Send notification through HTTP**
- **Recipient**: **Deactivate virtual port**
- **Query string suffix**: schemaversion=1&port=1

2.7 Click **Save**.

3. Create a rule in the camera.

3.1 In the camera's device interface, go to **System > Events > Rules** and add a rule.

3.2 Add the following information:

- **Name**: Trigger on virtual input 1
- **Condition**: **I/O > Virtual input is active**.
- **Port**: **1**
- **Action**: **Recordings > Record video while the rule is active**
- **Storage options**: **SD_DISK**
- Select **Camera** and a **Stream profile**.

3.7 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 *Add scenarios on page 15*.
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**.

Control a PTZ camera with the radar

It is 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:

- Use the built-in **Radar autotracking**. Use this option when you have one PTZ camera and one radar mounted very close together. This option creates an edge-to-edge solution where the radar directly controls the camera. The built-in radar autotracking service supports all Axis PTZ cameras.

  1. Go to **System > Radar autotracking**.
  2. Click on **legacy web client** to open the legacy device interface.
  3. Enter the IP address, username and password for the PTZ camera.
  4. Click **Connect** and follow the instructions.

Note

The camera must be installed directly above or below the radar.

The application does not use scenarios (previously called include zones) that have been set up in the radar. It uses the entire radar coverage, except exclude zones, to detect motion.

- Use the Windows® application **AXIS Radar Autotracking for PTZ**, to use multiple PTZ cameras with multiple radars. Download AXIS Radar Autotracking for PTZ from *axis.com*, and follow the instructions in the application to install it on your VMS server (or another computer with access to both the camera and the radar).

  AXIS Radar Autotracking for PTZ supports specific PTZ cameras, see the compatibility list at *axis.com*.

  This is a server-based solution that can handle different setups:

  - 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.

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.

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 product help.

💬 Change the language.

◐ Set light theme or dark theme.

👤 👤 👤 The user menu contains:

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

⋮ 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 firmware version and serial number.
- **Legacy device interface**: Change the device's web interface to the legacy version.

Status

Device info

Shows the device information, including firmware version and serial number.

Upgrade firmware: Upgrade the firmware on your device. Takes you to the Maintenance page where you can do a firmware upgrade.

Time sync status

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

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

Security

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

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

Connected clients

Shows the number of connections and connected clients.

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

Ongoing recordings

Shows ongoing recordings and their designated storage space.

Recordings: View ongoing and filtered recordings and their source. For more information, see *Recordings on page 29*

💾 ☰ Shows the storage space where the recording is saved.

Radar

Settings

General

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

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

Mounting height: Enter the mounting height for the product.

Note

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

Detection

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

Radar profile ⓘ : Select a profile that suits your needs. Use **Area monitoring** to track both large and small objects moving at lower speeds in open areas, and **Road monitoring** to track vehicles moving at higher speeds in urban zones and on sub-urban roads.

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

View

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

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

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

Color scheme: Select a theme for the radar visualization.

Rotation ⓘ : Select the preferred orientation of the radar image.

Object visualization

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

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

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

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

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.

Select one of the **Zone shape presets** for the exclude zone. **Cover everything** sets the zone to the entire radar coverage area. **Reset to box** creates a rectangle in the middle of the coverage area.

To modify 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 if you want to trigger on objects moving in an area or crossing a line.

Scene: Define the area, or the line, for the trigger.

For area detection, select one of the **Shape presets**, and modify the area.

For cross-line detection, drag and drop the line to where you want it to trigger. To create more points on the line, click and drag anywhere on the line. To remove a point, right-click on it. There are arrows crossing the line showing the detection direction. If you want objects to trigger in the other direction instead, click **Change direction**.

Detection settings: Define trigger criteria for the scenario.

Ignore short-lived objects: Select the delay between when the radar detects the object and when the scenario triggers on the object. This can help to reduce false alarms.

Trigger on object type: Select the type of objects you want the scenario to trigger on.

Speed limit: Trigger on objects moving at speeds within a specific range. **Invert** the range if you want to trigger on speeds above and below the set range.

Map calibration

Use map calibration to upload and calibrate a reference map. This will make it easier to see where objects move in the area covered by the radar.

Upload map: Select the reference map you want to upload.

Set radar position on map: Specify the position of the radar on the map, add a reference point straight in front of the radar and type the distance between the radar and the reference point. Click **Calibrate** to start the calibration.

The result of the calibration is a reference map that displays the radar coverage in the appropriate scale.

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.

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

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

Zipstream

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.

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.

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.
- **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 **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.
- **Streaming indicator** ⓘ : Select to show an animation superimposed over the video stream. The animation indicates that the video stream is live, even if the scene doesn't contain any motion.
  - **Appearance**: Select the animation color and background color, for example, red animation on a transparent background (default).
  - **Size**: Select the desired font size.
  - ◲ : Select the position of the overlay in the image.

Dynamic LED strip

Dynamic LED strip patterns

The dynamic LED strip on the front of the radar can play light- and different color patterns.

Pattern: Select the pattern you want to play when an action is triggered.

Type: Select how you want to play the pattern. **One-shot** activates the pattern once and plays it for a set duration. **Continuos** plays the pattern for the duration of the alarm (or as long as the rule is active).

Duration: Set a duration for the pattern when you activate it once.

Click **Test** to play and verify the pattern you have selected, and click **Stop** to stop it.

Recordings

Ongoing recordings: Show all ongoing recordings on the camera.

● Start a recording on the camera.

Choose which storage device to save to.

● Stop a recording on the camera.

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

Continuous recordings will continue until manually stopped. Even if the camera is shut down, the recording will continue when the camera 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.

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.

Allow root-privileged apps: Turn on to allow apps with root privileges full access to the device.

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 use it in another device. If you deactivate the license, you also remove it from the device. To deactivate the license requires internet access.
- **Settings**: Configure the parameters.
- **Delete**: Delete the app permanently from the device. If you don't deactivate the license first, it remains active.

System

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.
- **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.
- **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.
- **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.

Note

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

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 to 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.

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 hostname is used in the server report and in the system log. Allowed characters are A–Z, a–z, 0–9 and -.

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 used by the device.

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

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

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.

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. Port 80 or any port in the range 1024-65535 are allowed. 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. Port 443 or any port in the range 1024-65535 are allowed. 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.

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**: The default setting. Press and hold the control button on the device to connect to an O3C service over the internet. You need to register the device with the O3C service within 24 hours after you press the control button. Otherwise, the device disconnects from the O3C service. Once you have registered the device, **Always** is enabled and the device stays connected to the O3C service.
- **Always**: The device constantly attempts to connect to an O3C service over the internet. Once you have registered the device, it stays connected to the O3C service. Use this option if the control button on the device is out of reach.
- **No**: Disables 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/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.
  - **Warm start**: Sends a trap message when you change an SNMP setting.
  - **Link up**: Sends a trap message when a link changes from down to up.
  - **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 to access 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.

Filter the certificates in the list.

+ **Add certificate** : Click to add a 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.

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).

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, a signed client certificate must be installed on the device.

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

CA certificate: Select a CA certificate 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.

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.

IP address filter

Use filter: Select to filter which IP addresses that are allowed to access the device.

Policy: Choose whether to **Allow** access or **Deny** access for certain IP addresses.

Addresses: Enter the IP numbers that are either allowed or denied access to the device. You can also use the CIDR format.

Custom-signed firmware certificate

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

Click **Install** to install the certificate. You need to install the certificate before you install the firmware.

Users

+ **Add user**: Click to add a new user. You can add up to 100 users.

Username: Enter a unique username.

New password: Enter a password for the user. 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 users.
- **Operator**: Has access to all settings except:
  - All **System** settings.
  - Adding apps.
- **Viewer**: Doesn't have access to change any settings.

⋮ The context menu contains:

Update user: Edit the user's properties.

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

Anonymous users

Allow anonymous viewers: Turn on to allow anyone to access the device as a viewer without having to log in with a user account.

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

Events

Rules

A rule defines the conditions that must be met for 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**: Click to 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. 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 a 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/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

The manual trigger is used 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 firmware 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 Portal*.

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.

Keep alive interval: The 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 even if connection test fails**: 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 has passed.

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.

Click **Use tool** 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 for administrators.

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 SD card becomes full, old recordings are removed before the selected time period has passed.

Tools

- **Check**: Check for errors on the SD card. This only works for the ext4 file system.
- **Repair**: Repair errors in the ext4 file system. To repair an SD card with the VFAT file system, eject the SD card, insert it in a computer and perform a disk repair.
- **Format**: Format the SD card, for example when you need to change the file system or quickly erase all data. VFAT and ext4 are the two available file system options. The recommended format is ext4, due to its resilience against data loss if the card is ejected or if there is an abrupt power loss. However, 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. **Encrypt** deletes all data stored on the SD card. After using **Encrypt** data that's stored on the SD card is protected using encryption.
- **Decrypt**: Use this tool to format the SD card without encryption. **Decrypt** deletes all data stored on the SD card. After using **Decrypt** data that's stored on the SD card is not protected using encryption.
- **Change password**: Change the password required to encrypt the SD card.

Click **Use tool** 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.

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 *Stream on page 27* for a description of this setting.

Frame rate: See *Stream on page 27* for a description of this setting.

Compression: See *Stream on page 27* for a description of this setting.

Zipstream ⓘ : See *Stream on page 27* for a description of this setting.

Optimize for storage ⓘ : See *Stream on page 27* for a description of this setting.

Dynamic FPS ⓘ : See *Stream on page 27* for a description of this setting.

Dynamic GOP ⓘ : See *Stream on page 27* for a description of this setting.

Mirror ⓘ : See *Stream on page 27* for a description of this setting.

GOP length ⓘ : See *Stream on page 27* for a description of this setting.

Bitrate control: See *Stream on page 27* for a description of this setting.

Include overlays: Select what type of overlays to include. See *Overlays on page 28* for information about how to add overlays.

Include audio ⓘ : See *Stream on page 27* for a description of this setting.

ONVIF

ONVIF users

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 user, you automatically enable ONVIF communication. Use the username and password for all ONVIF communication with the device. For more information see the Axis Developer Community at *axis.com*.

+ **Add user**: Click to add a new ONVIF user.

Username: Enter a unique username.

New password: Enter a password for the user. 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 users.
- **Operator**: Has access to all settings except:
  - All **System** settings.
  - Adding apps.
- **Media user**: Allows access to the video stream only.

⋮ The context menu contains:

Update user: Edit the user's properties.

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

ONVIF media profiles

An ONVIF media profile consists of a set of configurations that you can use to change media stream settings.

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

profile_x: Click a profile to edit.

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 in 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 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 V DC.

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 network speaker or microphone as if it's part of the camera. 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.

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

Username: Enter username.

Password: Enter password for the user.

Speaker pairing: Select to pair a network speaker.

Microphone pairing: Select to pair a microphone.

Clear fields: Click to clear all fields.

Connect: Click to establish connection to the speaker or microphone.

Logs

Reports and logs

Reports

- **View the device server report**: Click to show 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**: Click to download the 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**: Click to 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.

Network trace

Important

A network trace file might contain sensitive information, for example 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**.

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.

- RFC 3164
- RFC 5424

Protocol: Select the protocol and port to use:

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

Severity: Select which messages to send when triggered.

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

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 PTZ 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

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 firmware is digitally signed to ensure that you only install verified firmware on your device. This further increases the overall minimum cybersecurity level of Axis devices. For more information, see the white paper "Signed firmware, secure boot, and security of private keys" at *axis.com*.

Firmware upgrade: Upgrade to a new firmware version. New firmware releases can contain improved functionality, bug fixes, and completely new features. We recommend you to always use the latest 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 firmware 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 firmware 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 firmware version.

Firmware rollback: Revert to the previously installed firmware version.

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.

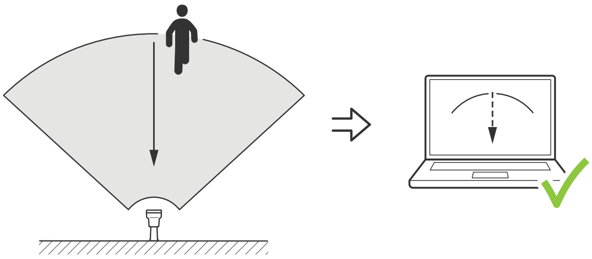
First *Calibrate the radar on page 14* before attempting the validation. Then follow these steps:

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 *Minimize false alarms on page 17*.

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 *Record and watch video on page 19*.
2. Start X m (X 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 *Record and watch video on page 19*.
2. Start X m (X 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 *Record and watch video on page 19* 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.

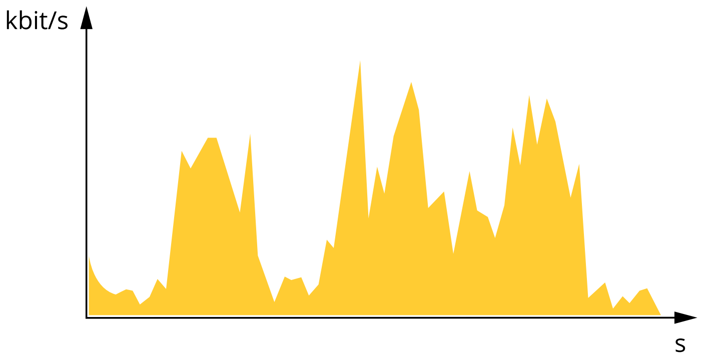
Note

- 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.

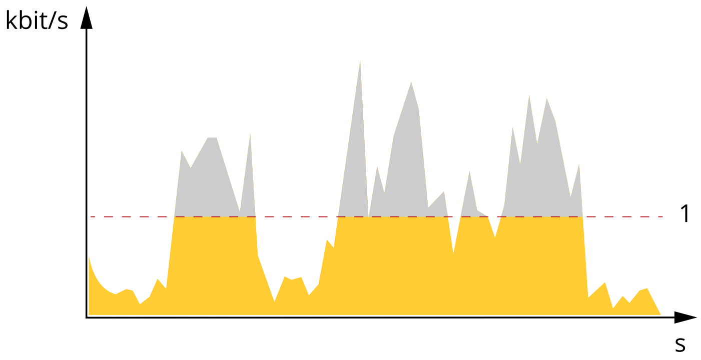
Bitrate control

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.



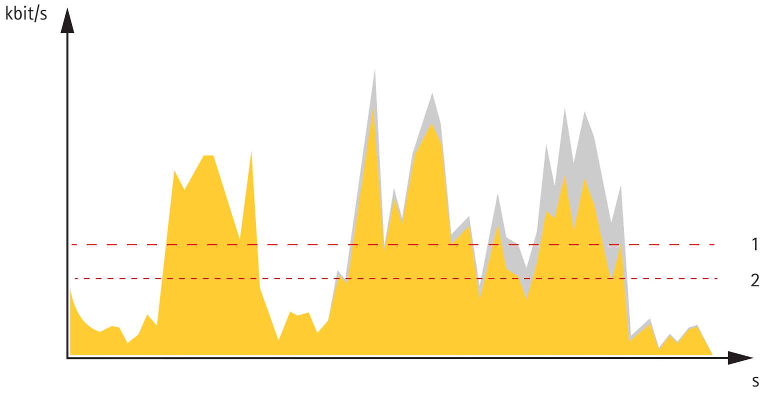
Maximum bitrate (MBR)
Maximum bitrate lets you set a target bitrate to handle bitrate limitations in your system. You might see a decline in image quality or frame rate as the instantaneous bitrate is kept below the specified target bitrate. You can choose to prioritize either image quality or frame 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

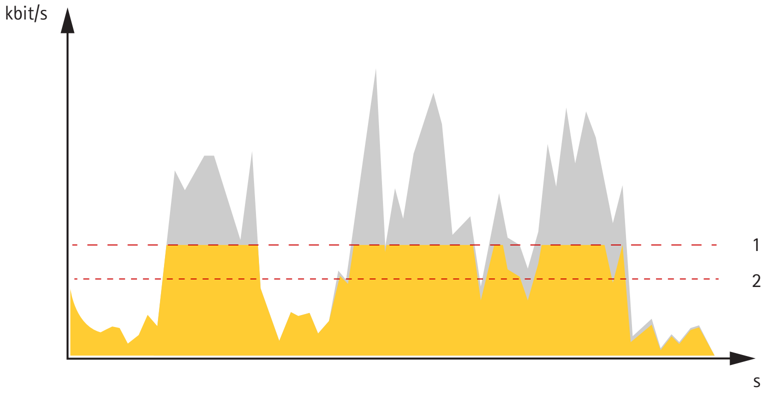
Average bitrate (ABR)
With average bitrate, the bitrate is automatically adjusted over a longer period of time. This is so you can meet the specified target and provide the best video quality based on your available storage. Bitrate is higher in scenes with a lot of activity, compared to static scenes. 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.



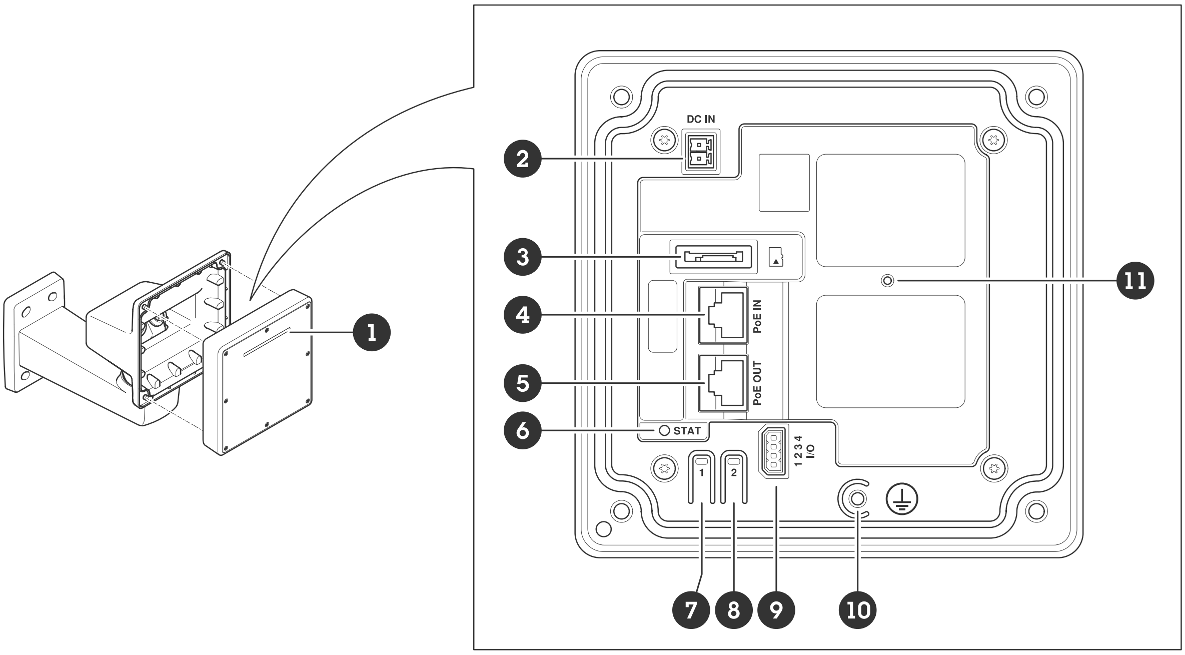
1 Target bitrate
2 Actual average bitrate

Overlays

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

Specifications

Product overview



1 *Dynamic LED strip*
2 *Power connector (DC)*
3 *microSD card slot*
4 *Network connector (PoE in)*
5 *Network connector (PoE out)*
6 *LED status indicator*
7 *Control button*
8 *Action button*
9 *I/O connector*
10 *Grounding screw*
11 *Reset button*

LED indicators

Status LED	Indication
Green	
Red	Firmware upgrade failure.

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

Dynamic LED strip patterns
Red
Blue
Green
Yellow
White
Sweeping red
Sweeping blue
Sweeping green
Strobe

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 *Product overview on page 52*.

The control button is used for:

- Resetting the product to factory default settings. See *page 57*.
- 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

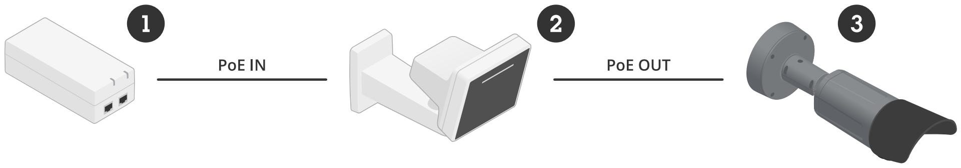
Risk of damage to the device. Do not power the device with both PoE and DC.

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.

Specifications



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 radar will provide the Ethernet connection.

I/O connector

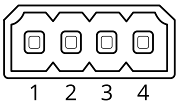
Use the I/O connector with external devices in combination with, for example, event triggering and alarm notifications. In addition to the 0 V DC reference point and power (DC output), the I/O connector provides the interface to:

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.

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

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

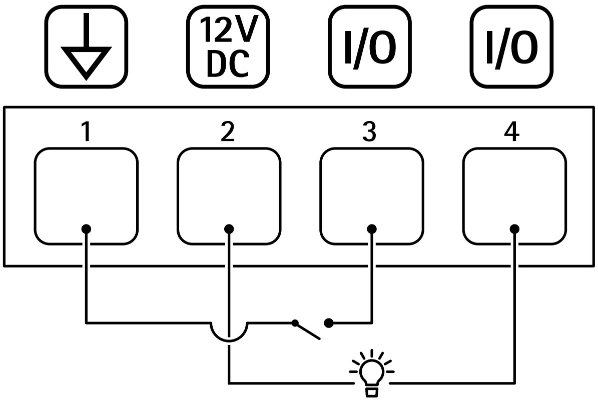
4-pin terminal block



Function	Pin	Notes	Specifications
DC ground	1		0 V DC
DC output	2	Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	12 V DC Max load = 50 mA
Configurable (Input or Output)	3–4	Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC
		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 V DC, open drain, 100 mA

Example

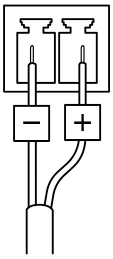
Specifications



1 *DC ground*
2 *DC output 12 V, max 50mA*
3 *I/O configured as input*
4 *I/O configured as output*

Power connector

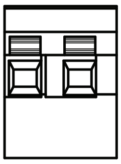
2-pin terminal block for DC power input. Use a Safety Extra Low Voltage (SELV) compliant limited power source (LPS) with either a rated output power limited to ≤100 W or a rated output current limited to ≤5 A.



⚠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

Cleaning recommendations

Cleaning recommendations

NOTICE

Never use harsh detergent, for example gasoline, benzene, or acetone.

1. Use a can of compressed air to remove any dust or loose dirt from the device.
2. If necessary, clean the lens with a soft cloth dampened with lukewarm water.

Note

Avoid cleaning in direct sunlight or at elevated temperatures, as this may cause stains when the water droplets dry.

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:

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 firmware version

Firmware is the software that determines the functionality of network devices. When you troubleshoot a problem, we recommend you to start by checking the current firmware version. The latest firmware version might contain a correction that fixes your particular problem.

To check the current firmware:

1. Go to the device's web interface > **Status**.
2. See the firmware version under **Device info**.

Upgrade the firmware

Important

- Preconfigured and customized settings are saved when you upgrade the firmware (provided that the features are available in the new firmware) 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 firmware 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 the firmware. To find the latest firmware and the release notes, go to *axis.com/support/firmware*.

1. Download the firmware file to your computer, available free of charge at *axis.com/support/firmware*.
2. Log in to the device as an administrator.
3. Go to **Maintenance > Firmware 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*.

Troubleshooting

Problems upgrading the firmware	
Firmware upgrade failure	If the firmware upgrade fails, the device reloads the previous firmware. The most common reason is that the wrong firmware file has been uploaded. Check that the name of the firmware file corresponds to your device and try again.
Problems after firmware upgrade	If you experience problems after a firmware 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 user root is lost, the device must be reset to the factory default settings. See *Reset to factory default settings on page 57*.
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 Companion: free of charge, ideal for small systems with basic surveillance needs.
- AXIS Camera Station: 30-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

The following factors are the most important to consider:

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

Contact support

Contact support at *axis.com/support*.

User manual
AXIS D2210-VE Radar

Ver. M1.24
Date: August 2023
Part no. T10193646