AXIS D2110-VE Security Radar

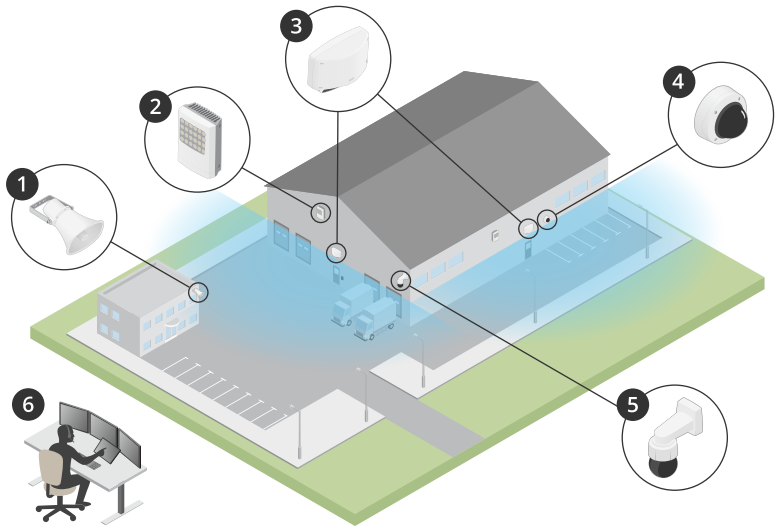
User manual

Table of Contents

Solution overview 4
Radar profiles 4
Where to install the product 4
Area of coverage 5
Area monitoring profile 6
Install multiple radars 6
Install 2-3 radars in the same coexistence zone 6
Install 4-6 radars in the same coexistence zone 6
Area installation examples 7
Area detection range 9
Area monitoring use cases 11
Road monitoring profile 12
Road installation examples 12
Road detection range 12
Road monitoring use cases 12
Get started 14
Find the device on the network 14
Browser support 14
Open the device's web interface 14
Create an administrator account 14
Secure passwords 15
Web interface overview 15
Configure your device 16
Set the mounting height 16
Calibrate a reference map 16
Set detection zones 17
Add scenarios 17
Add exclude zones 18
Minimize false alarms 18
View and record video 19
Reduce bandwidth and storage 19
Set up network storage 19
Record and watch video 20
Control a PTZ camera with the radar 20
Control a PTZ camera with the built-in radar autotracking service 20
Control a PTZ camera with AXIS Radar Autotracking for PTZ 21
Set up rules for events 21
Trigger an action 22
Trigger a notification when the enclosure is opened 22
Record video from a camera when motion is detected 22
Turn on a light when motion is detected 23
Send an email if someone covers the radar with a metallic object 23
The web interface 25
Validate your installation 26
Validate the installation of the radar 26
Validate the radar 26
Complete the validation 27
Learn more 28
Streaming and storage 28
Video compression formats 28
Bitrate control 28
Specifications 31
Product overview 31

.....31
LED Indicators.....31
.....32
SD card slot.....32
Buttons.....32
Control button.....32
Connectors.....32
Network connector.....32
Network connector (PoE out).....32
I/O connector.....33
Power connector.....34
Relay connector.....34
Clean your device.....35
Troubleshooting.....36
Reset to factory default settings.....36
Check the current AXIS OS version.....36
Upgrade AXIS OS.....36
Technical problems and possible solutions.....37
Performance considerations.....38
Cybersecurity.....39
Vulnerability management.....39
Security notifications.....39
Secure product lifecycle.....39

Solution overview



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

Radar profiles

Note

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

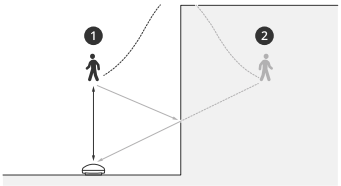
The user manual is set up to help you use your radar depending on what you want it to do. AXIS D2110-VE Security Radar has two profiles:

- **Area monitoring profile** to track both large and small objects moving at speeds lower than 55 km/h (34 mph)
- **Road monitoring profile** to track vehicles moving at speeds up to 105 km/h (65 mph)

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

Where to install the product

- The radar is intended for monitoring open areas. Any solid object (such as a wall, a fence, a tree, or a large bush) in the coverage area will create a blind spot (radar shadow) behind it.
- Install the radar on a stable pole or a spot on a wall where there are no other objects or installations. Objects within 1 m (3 ft) to the left and right of the radar, that reflect radio waves, affect the performance of the radar.
- Metal objects in the field of view causes reflections that affects the ability of the radar to perform classifications.



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

For information about how to handle reflective objects, see *Add exclude zones, on page 18*.

- If you want to install more than two radars in the same coexistence zone, see *Install multiple radars, on page 6*.

Area of coverage

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

Note

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

Area monitoring profile

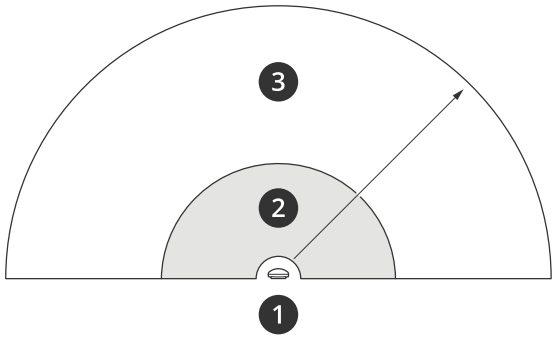
The **area monitoring profile** is optimized for objects moving at up to 55 km/h (34 mph). This profile allows you to detect whether an object is human, vehicle, or unknown. A rule can be set to trigger an action when any of these objects is detected. To track vehicles moving in higher speeds, use the *Road monitoring profile, on page 12*.

Install multiple radars

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

Coexistence

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



1 Radar
2 Detection area
3 Coexistence zone

Note

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

Install 2–3 radars in the same coexistence zone

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

1. Go to **Radar > Settings > Coexistence**.
2. Select the number of neighboring radars.

See *Area installation examples, on page 7* for examples of installations with multiple radars.

Install 4–6 radars in the same coexistence zone

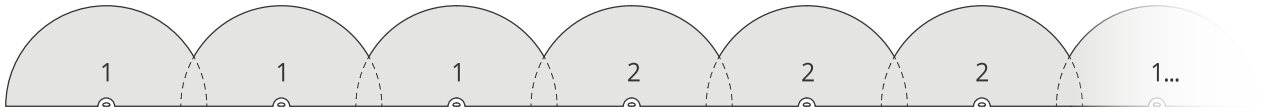
Note

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

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

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

1. Go to **Radar > Settings > Coexistence**.
2. Set the number of neighboring radars to **3–5**.
3. Select a group for your radar.



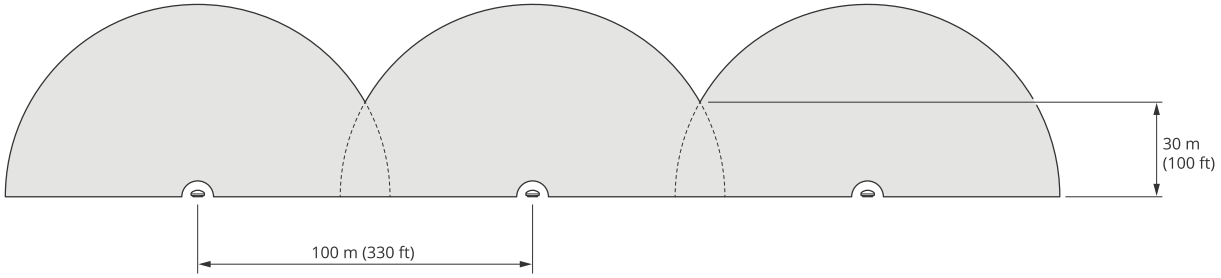
This is an example of how to group multiple radars installed side-by-side in the same coexistence zone.

See *Area installation examples, on page 7* for more examples of installations with multiple radars.

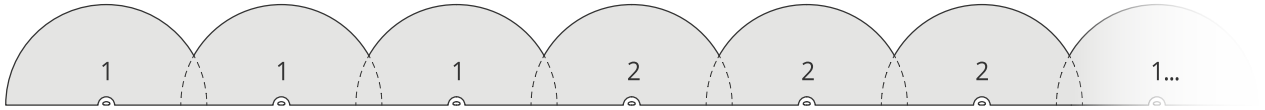
Area installation examples

Create a virtual fence with multiple radars

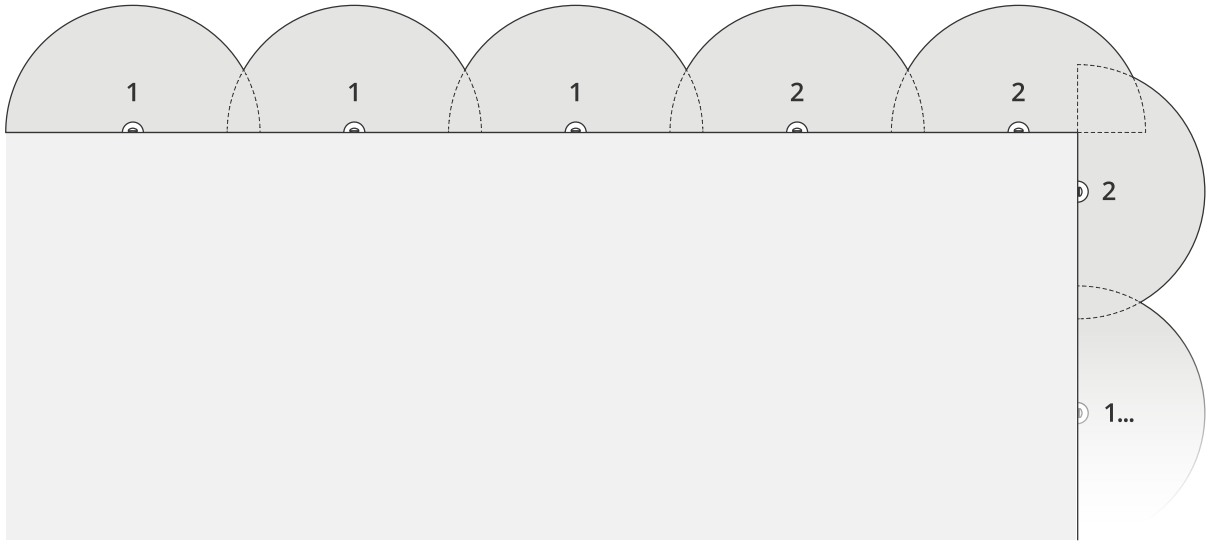
To create a virtual fence, for example along or around a building, you can place multiple radars side-by-side. We recommend placing them with 100 m (330 ft) spacing.



To avoid interference when you mount more than two radars in the same coexistence zone, set the number of neighboring radars in the device interface. Additionally, when you mount more than three radars, add each radar into a group.



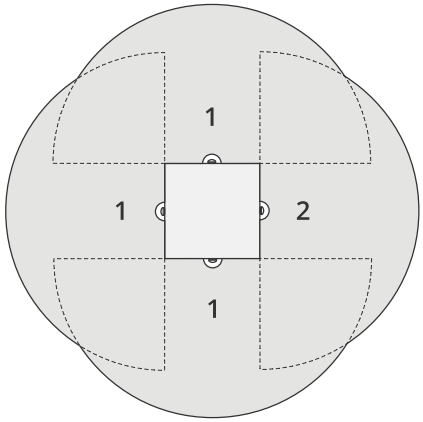
You can adjust the virtual fence to cover corners as well, as illustrated in this example.



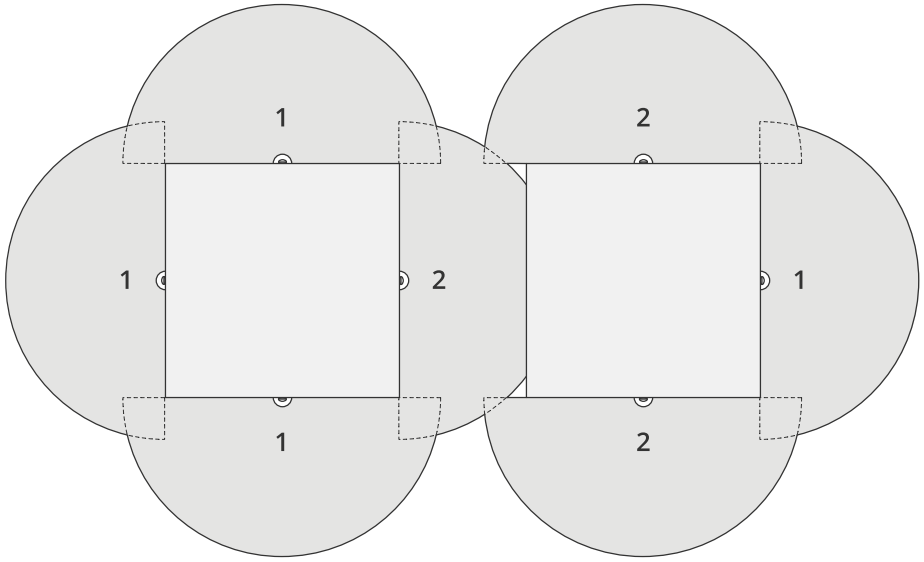
See *Install multiple radars, on page 6* for more information about neighboring radars and groups.

Cover an area around a building

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



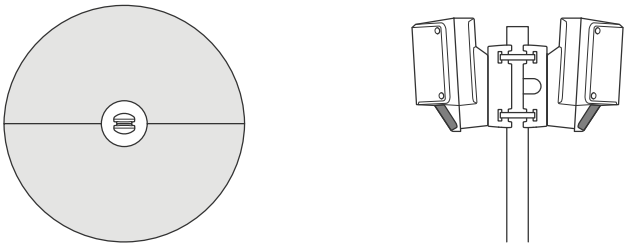
You can also cover the area around multiple buildings.



See *Install multiple radars, on page 6* for more information about neighboring radars and groups.

Cover an open area

To cover a large open area, use two pole mounts to place two radars back-to-back.

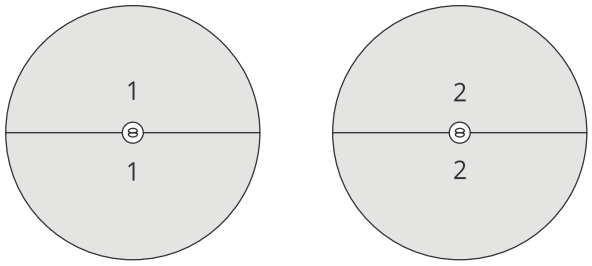


You can use the PoE output from one radar to power the second radar, but it's not possible to connect a third radar this way.

Note

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

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



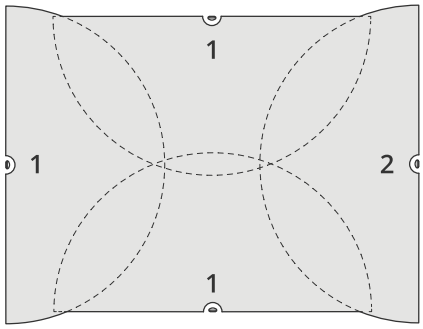
See *Install multiple radars, on page 6* for more information about neighboring radars and groups.

Install multiple radars facing each other

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

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

This is an example of how to group four radars covering a field.



See *Install multiple radars, on page 6* for more information about neighboring radars and groups.

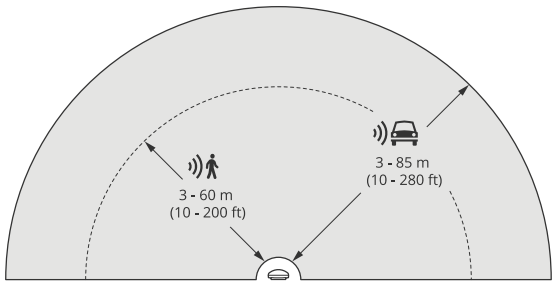
Area detection range

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

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

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

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



Note

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

The detection range was measured under these conditions:

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

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

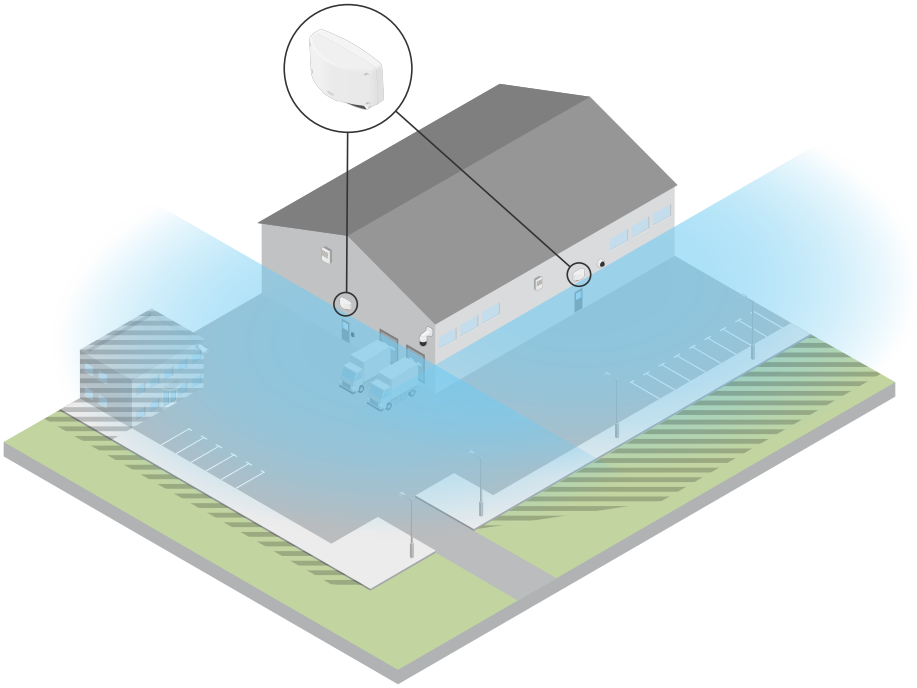
Area monitoring use cases

Swimming pool area coverage

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

Cover the field around a building

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



Cover a large open area

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

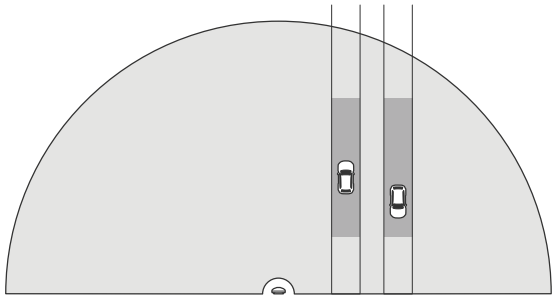
Road monitoring profile

The **Road monitoring profile** is best used to track vehicles moving at up to 105 km/h (65 mph) in urban zones, closed zones, and on sub-urban roads. This mode should not be used for detection of humans or other types of objects. To track objects other than vehicles, use your radar in the *Area monitoring profile, on page 6*.

Road installation examples

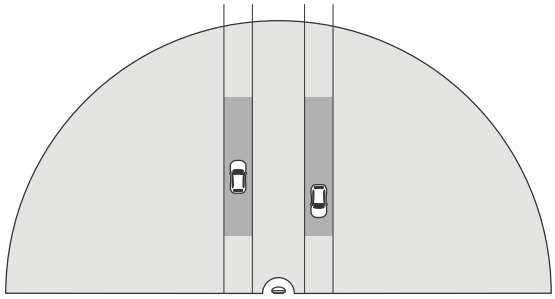
Side mounted

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



Center mounted

This mounting option requires a stable position. The radar can be mounted on a pole in the middle of the road or on a bridge above the road. The radar will then provide a lateral coverage distance of 10 m (32 ft) to both sides of the radar. The radar covers a broader lateral distance when center mounted.



Note

We recommend that the radar is mounted at a height between 3 m (10 ft) and 8 m (26 ft) for the **Road monitoring profile**.

Road detection range

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

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

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

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

Road monitoring use cases

Regulating vehicles in low speed zones

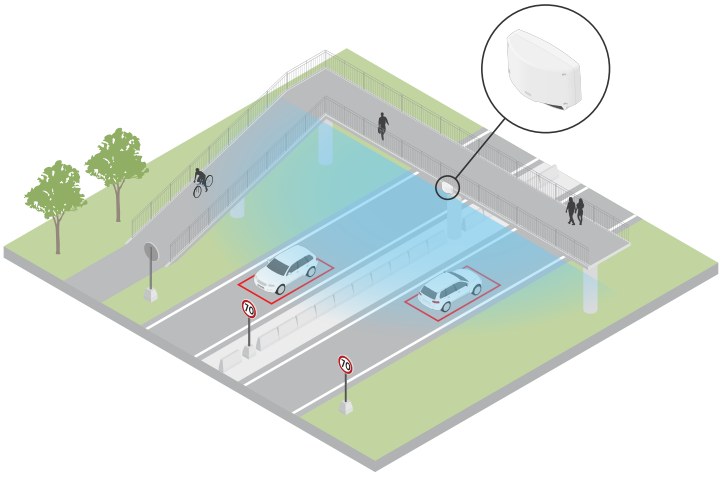
An industrial complex with a long road between two warehouses has installed a radar to help enforce a speed limit of 60 km/h (37 mph). In the **Road monitoring profile**, the radar can detect when a vehicle in its detection zone exceeds that speed. It then triggers an event which sends an email notifications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

Unwanted vehicles on a closed road

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

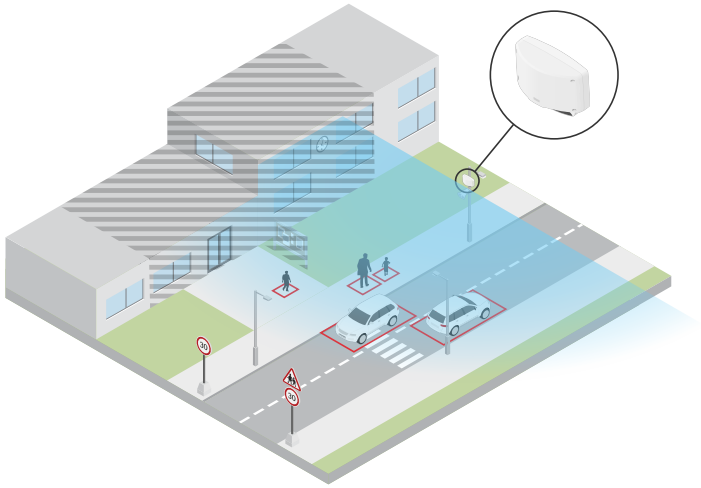
Speed awareness on the road

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



Safety with humans and vehicles

Staff at a school have identified two safety issues that they would like to address. They have experienced unwanted visitors entering the premises during the school day, as well as vehicles violating the low speed zone of 20 km/h (12 mph) outside the school. The radar is mounted on a pole, next to the pedestrian walk path. The *Area monitoring profile, on page 6* was chosen, as it makes the radar capable of tracking both humans and vehicles moving at speeds lower than 55 km/h (34 mph). This helps the staff keep track of people coming and going during school hours while also being able to trigger a speaker to warn pedestrians when a passing vehicle is driving too fast.



Get started

Find the device on the network

To find Axis devices on the network and assign them IP addresses in Windows®, use AXIS IP Utility or AXIS Device Manager. Both applications are free and can be downloaded from *axis.com/support*.

For more information about how to find and assign IP addresses, go to *How to assign an IP address and access your device*.

Browser support

You can use the device with the following browsers:

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

✓: Recommended

*: Supported with limitations

Open the device's web interface

1. Open a browser and type the IP address or host name of the Axis device.
   If you don't know the IP address, use AXIS IP Utility or AXIS Device Manager to find the device on the network.
2. Type the username and password. If you access the device for the first time, you must create an administrator account. See *Create an administrator account, on page 14*.

For descriptions of all features and settings in the web interface of devices with AXIS OS, see *AXIS OS web interface help*.

Create an administrator account

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

1. Enter a username.
2. Enter a password. See *Secure passwords, on page 15*.
3. Re-enter the password.
4. Accept the license agreement.
5. Click **Add account**.

Important

The device has no default account. If you lose the password for your administrator account, you must reset the device. See *Reset to factory default settings, on page 36*.

Secure passwords

Important

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

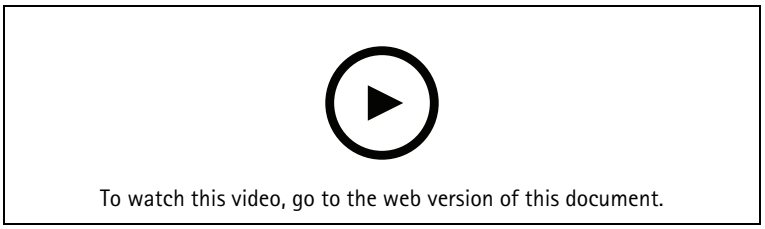
The device password is the primary protection for your data and services. Axis devices do not impose a password policy as they may be used in various types of installations.

To protect your data we strongly recommend that you:

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

Web interface overview

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



Axis device web interface

Configure your device

Set the mounting height

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

Measure the height from the ground up to the radar as accurately as possible. If the ground is uneven, measure from the average ground elevation instead of from a single point.

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

Calibrate a reference map

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

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

Use the setup assistant:

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

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

Edit each setting individually:
The map will calibrate gradually after you adjust each setting.

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

Note

The zoom function doesn't alter the radar's area of coverage. Even if parts of the coverage is out of view after zooming, the radar will still detect moving objects in the entire area of coverage. The only way to exclude detected movement is to add exclude zones. For more information, see *Add exclude zones, on page 18*.

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

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

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

Set detection zones

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

There are two types of zones:

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

Add scenarios

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

Add a scenario:

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

Trigger on objects moving in an area:

1. Select **Movement in area**.
2. Click **Next**.
3. Select the type of zone that should be included in the scenario.
   Use the mouse to move and shape the zone so that it covers the desired part of the radar image or reference map.
4. Click **Next**.
5. Add detection settings.

1. Add seconds until trigger after under **Ignore short-lived objects**.
2. Select which object type to trigger on under **Trigger on object type**.
3. Add a range for the speed limit under **Speed limit**.

6. Click **Next**.
7. Set the minimum duration of the alarm under **Minimum trigger duration**.
8. Click **Save**.

Trigger on objects crossing a line:

1. Select **Line crossing**.
2. Click **Next**.
3. Position the line in the scene.
   Use the mouse to move and shape the line.
4. To change the detection direction, turn on **Change direction**.
5. Click **Next**.
6. Add detection settings.
   6.1. Add seconds until trigger after under **Ignore short-lived objects**.
   6.2. Select which object type to trigger on under **Trigger on object type**.
   6.3. Add a range for the speed limit under **Speed limit**.
7. Click **Next**.
8. Set the minimum duration of the alarm under **Minimum trigger duration**.

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

9. Click **Save**.

Trigger on objects crossing two lines:

1. Select **Line crossing**.
2. Click **Next**.
3. To make the object cross two lines for the alarm to trigger, turn on **Require crossing of two lines**.
4. Position the lines in the scene.
   Use the mouse to move and shape the line.
5. To change the detection direction, turn on **Change direction**.
6. Click **Next**.
7. Add detection settings.
   7.1. Set the time limit between crossing the first and the second line under **Max time between crossings**.
   7.2. Select which object type to trigger on under **Trigger on object type**.
   7.3. Add a range for the speed limit under **Speed limit**.
8. Click **Next**.
9. Set the minimum duration of the alarm under **Minimum trigger duration**.
   The default value is set to 2 seconds. If you want the scenario to trigger every time an object has crossed the two lines, lower the duration to 0 seconds.
10. Click **Save**.

Add exclude zones

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

Add an exclude zone:

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

Minimize false alarms

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

- Adjust the detection sensitivity of the radar:
  Go to **Radar > Settings > Detection** and select a lower **Detection sensitivity**. This decreases the risk of false alarms, but it could also cause the radar to miss some movement.
  The sensitivity setting affects all zones.
  - **Low**: Use this sensitivity when there are a lot of metal objects or large vehicles in the area. It will take longer time for the radar to track and classify objects. This can reduce the detection range, especially for fast moving objects.
  - **Medium**: This is the default setting.
  - **High**: Use this sensitivity when you have an open field without metal objects in front of the radar. This will increase the detection range for humans.
- Modify scenarios and exclude zones:

If a scenario includes hard surfaces, such as a metal wall, there may be reflections that causes multiple detections for a single physical object. You can either modify the shape of the scenario, or add an exclude zone that ignores certain parts of the scenario. For more information, see *Add scenarios, on page 17* and *Add exclude zones, on page 18*.

- Trigger on objects crossing two lines instead of one:
  If a line crossing scenario includes swaying objects or animals moving around, there is a risk that an object will happen to cross the line and trigger a false alarm. In this case, you can configure the scenario to trigger only when an object has crossed two lines. For more information, see *Add scenarios, on page 17*.
- Filter on movement:
  - Go to **Radar > Settings > Detection** and select **Ignore swaying objects**. This setting minimizes false alarms from trees, bushes, and flagpoles in the coverage zone.
  - Go to **Radar > Settings > Detection** and select **Ignore small objects**. This setting is available in the area monitoring profile and minimizes false alarms from small objects in the coverage zone, such as cats and rabbits.
- Filter on time:
  - Go to **Radar > Scenarios**.
  - Select a scenario, and click ⋮ to modify its settings.
  - Select a higher value under **Seconds until trigger**. This is the delay time from when the radar starts tracking an object until it can trigger and alarm. The timer starts when the radar first detects the object, not when the object enters the specified zone in the scenario.
- Filter on object type:
  - Go to **Radar > Scenarios**.
  - Select a scenario, and click ⋮ to modify its settings.
  - To avoid triggering on specific object types, deselect the object types that should not trigger events in the scenario.

View and record video

This section includes instructions about configuring your device. To learn more about how streaming and storage works, go to *Streaming and storage, on page 28*.

Reduce bandwidth and storage

Important

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

1. Go to **Radar > Stream**.
2. Click  in the live view.
3. Select **Video format H.264**.
4. Go to **Radar > Stream > General** and increase **Compression**.

Note

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

Set up network storage

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

1. Go to **System > Storage**.

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

Record and watch video

Record video directly from the radar

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

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

Control a PTZ camera with the radar

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

- *Control a PTZ camera with the built-in radar autotracking service, on page 20*. The built-in option is suitable when you have a PTZ camera and radar mounted very close together.
- *Control a PTZ camera with AXIS Radar Autotracking for PTZ, on page 21*. The Windows application is suitable when you want to use multiple PTZ cameras and radars for tracking objects.

Note

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

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

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

Note

You can use the built-in radar autotracking service to connect one radar with one PTZ camera. For a setup where you want to use more than one radar or PTZ camera, use AXIS Radar Autotracking for PTZ. For more information, see *Control a PTZ camera with AXIS Radar Autotracking for PTZ, on page 21*.

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

Before you start:

- Define the area of interest and avoid unwanted alarms by setting up exclude zones in the radar. Make sure to exclude zones with radar-reflective materials or swaying objects, like foliage, to prevent the PTZ camera from tracking irrelevant objects. For instructions, see *Add exclude zones, on page 18*.

Pair the radar with the PTZ camera:

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

Calibrate the radar and the PTZ camera:

5. Go to **Radar > Radar PTZ autotracking**.
6. To set the mounting height of the camera, go to **Camera mounting height**.
7. To pan the PTZ camera so that it points in the same direction as the radar, go to **Pan alignment**.
8. If you need to adjust the tilt to compensate for a sloping ground, go to **Ground incline offset** and add an offset in degrees.

Set up the PTZ tracking:

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

Control a PTZ camera with AXIS Radar Autotracking for PTZ

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

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

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

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

Set up rules for events

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

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

Trigger an action

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

Trigger a notification when the enclosure is opened

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

Add an email recipient:

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

Create a rule:

9. Go to **System > Events > Rules** and click **Add a rule**.
10. Type a name for the rule.
11. In the list of conditions, select **Casing open**.
12. In the list of actions, select **Send notification to email**.
13. Select a recipient from the list.
14. Type a subject line and message for the email.
15. Click **Save**.

Record video from a camera when motion is detected

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

Connect the devices to each other:

1. Connect a wire 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, for example Record video upon motion.
5. In the list of conditions, select a scenario under **Radar motion**.
6. In 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. In the list of conditions, select **Digital input is active** and then select the port that should trigger the rule.
12. In the list of actions, select **Record video**.
13. In the list of storage options, select **SD card**.
14. Select an existing stream profile or create a new one.
15. Set the prebuffer to 5 seconds.
16. Set the postbuffer to 1 minute.
17. Click **Save**.

Turn on a light when motion is detected

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

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

Connect the devices:

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

Configure the relay port of the radar:

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

Create a rule in the radar:

3. Go to **System > Events** and add a rule.
4. Type a name for the rule.
5. From the list of conditions, select a scenario under **Radar motion**.
   To set up a scenario, see *Add scenarios, on page 17*.
6. From the list of actions, select **Toggle I/O once** and then select the relay port.
7. Select **Active**.
8. Set the **Duration**.
9. Click **Save**.

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

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

Add an email recipient:

1. Go to **System > Events > Recipients** and add a recipient.
2. Type a name for the recipient.
3. Under **Type**, select **Email**.
4. Type an email address to send the email to.
5. Fill in the rest of the information according to your email provider.

The radar device doesn't have its own email server, so it needs to log into an email server to send emails.

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

Create a rule:

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

The web interface

To read about all the features and settings available in the web interface of devices with AXIS OS, go to *AXIS OS web interface help*.

Validate your installation

Validate the installation of the radar

Note

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

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

First before attempting the validation.

It is a good idea to perform the validation whenever:

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

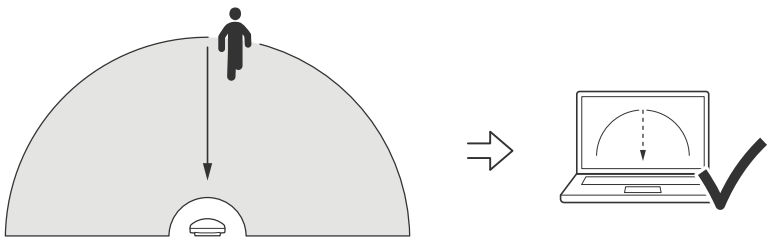
Validate the radar

Check that there are no false detections

1. Check that the detection zone is clear from human activity.
2. Wait for a few minutes to ensure that the radar is not detecting any static objects in the detection zone.
3. If there are no unwanted detections you can skip step 4.
4. If there are unwanted detections, learn how to filter out certain types of movement or objects, change the coverage, or adjust the detection sensitivity in *Minimize false alarms, on page 18*.

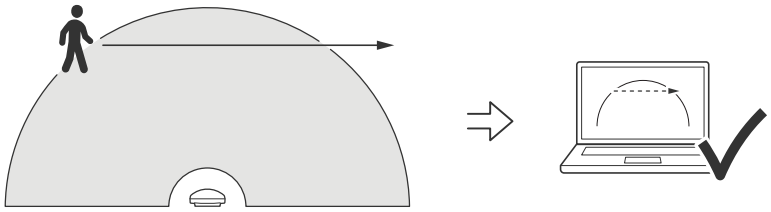
Check for the correct symbol and direction of travel when the radar is approached from the front

1. Go into the radar's web interface and record the session. For help doing this, go to *Record and watch video, on page 20*.
2. Start 60 m (197 ft) in front of the radar and walk directly towards the radar.
3. Check the session in the radar's web interface. The symbol for a human classification should appear when you are detected.
4. Check that the radar's web interface shows the correct direction of travel.



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

1. Go into the radar's web interface and record the session. For help doing this, go to *Record and watch video, on page 20*.
2. Start 60 m (197 ft) out from the radar and walk straight across the radar coverage area.
3. Check that the radar's web interface shows the symbol for a human classification.
4. Check that the radar's web interface shows the correct direction of travel.



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

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

Complete the validation

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

1. Make sure you have configured your radar and followed the instructions.
2. For further validation, add and calibrate a reference map.
3. Set the radar scenario to trigger when an appropriate object is detected. By default, **seconds until trigger** is set to two seconds but you can change this in the web interface if needed.
4. Set the radar to record data when an appropriate object is detected.
   See *Record and watch video, on page 20* 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.

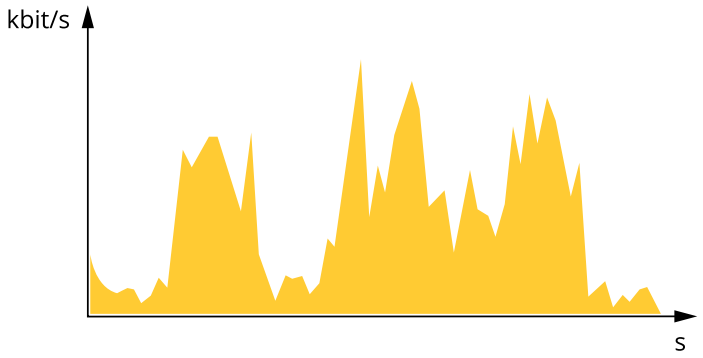
Note

- 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

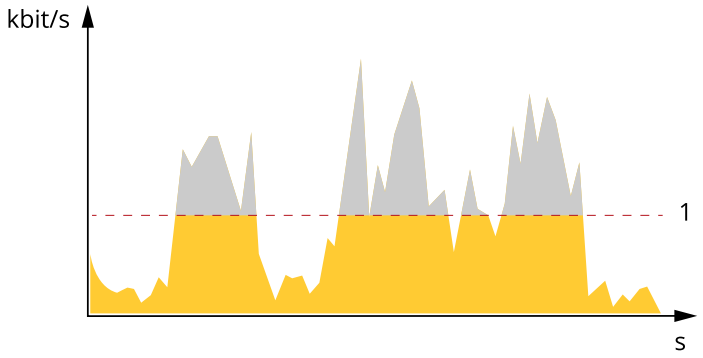
Bitrate control helps you to manage the bandwidth consumption of your video stream.

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.

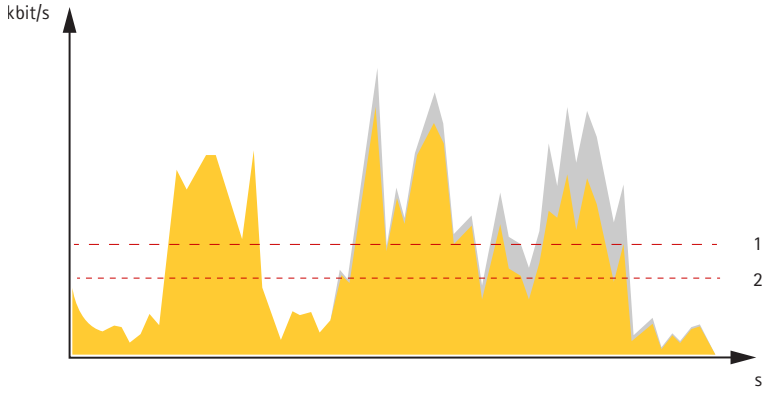


1 Target bitrate

Average bitrate (ABR)

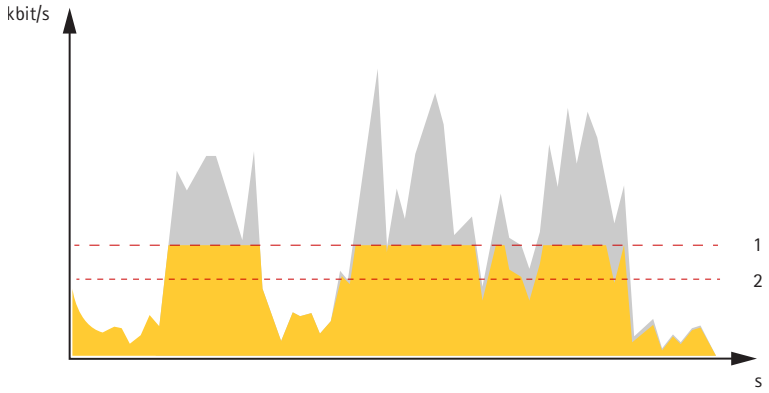
With average bitrate, the bitrate is automatically adjusted over a longer period of time. This is so you can meet the specified target and provide the best video quality based on your available storage. Bitrate is higher in scenes with a lot of activity, compared to static scenes. You are more likely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

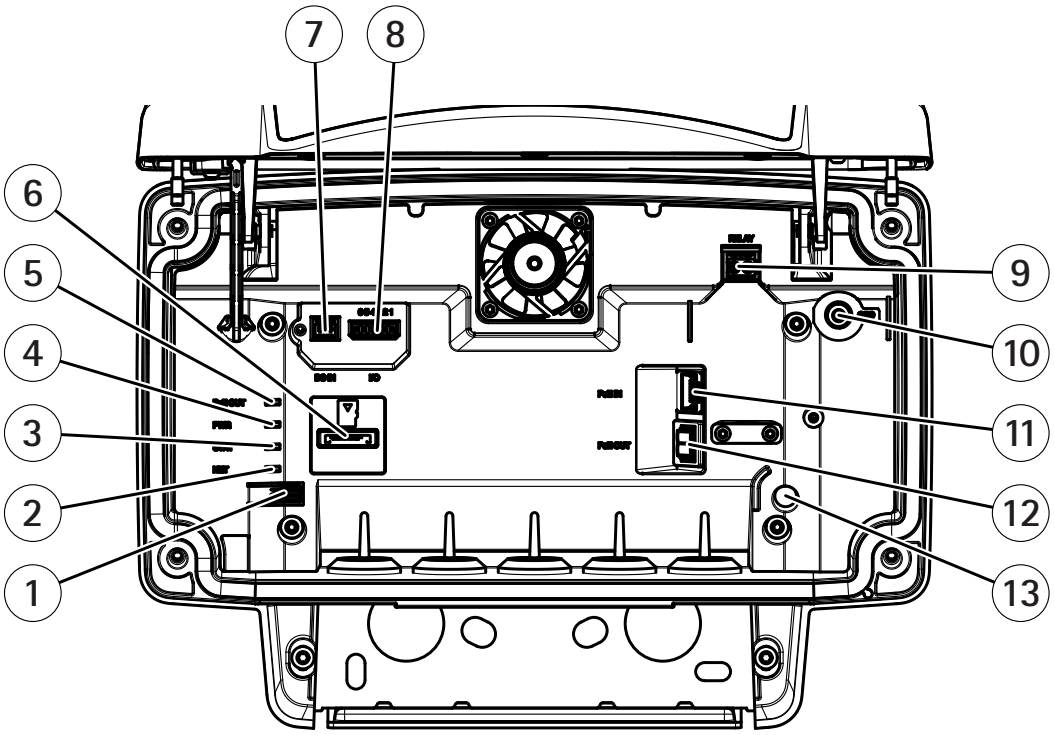
You can also turn on maximum bitrate and specify a target bitrate within the average bitrate option.



1 *Target bitrate*
2 *Actual average bitrate*

Specifications

Product overview



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

For technical specifications, see *Specifications, on page 31*.

LED Indicators

Status LED	Indication
Green	Steady green for normal operation.

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

Power LED	Indication
Green	Normal operation.

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

SD card slot

This device supports microSD/microSDHC/microSDXC cards.

For SD card recommendations, see *axis.com*.

microSD, microSDHC, and microSDXC Logos are trademarks of SD-3C LLC. microSD, microSDHC, microSDXC are trademarks or registered trademarks of SD-3C, LLC in the United States, other countries or both.

Buttons

Control button

For location of the control button, see *Product overview, on page 31*.
The control button is used for:

- Resetting the product to factory default settings. See *page 36*.
- Connecting to an AXIS Video Hosting System service. See . To connect, press and hold the button for about 3 seconds until the Status LED flashes green.

Connectors

Network connector

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

⚠ CAUTION

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

Network connector (PoE out)

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

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

Note

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

Note

If the radar is powered by a 30 W midspan or DC power, the PoE out is disabled.

Note

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

Note

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

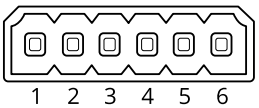
I/O connector

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

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

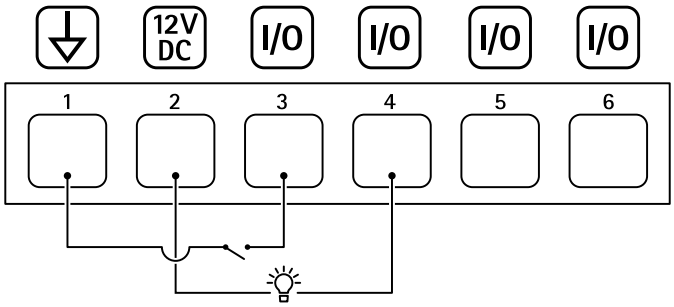
Digital output – For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface, through an event or from the device's web interface.

6-pin terminal block



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

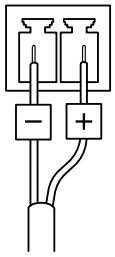
Example:



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

Power connector

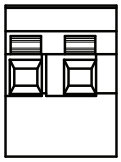
2-pin terminal block for DC power input. Use a Safety Extra Low Voltage (SELV) compliant limited power source (LPS) with either a rated output power limited to ≤100 W or a rated output current limited to ≤5 A.



⚠ CAUTION

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

Relay connector



⚠ CAUTION

Use single core wires for the relay connector.

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

Clean your device

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

NOTICE

- Harsh chemicals can damage the device. Don't use chemicals such as window cleaner or acetone to clean your device.
- Avoid cleaning in direct sunlight or elevated temperatures, since this can cause stains.

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

For more information about cleaning of Axis devices, see the white paper *Chemical resistance to common cleaning agents*.

Troubleshooting

Reset to factory default settings

Important

Reset to factory default should be used with caution. A reset to factory default resets all settings, including the IP address, to the factory default values.

To reset the product to the factory default settings:

1. Disconnect power from the product.
2. Press and hold the control button while reconnecting power. See *Product overview, on page 31*.
3. Keep the control button pressed for 15–30 seconds until the status LED indicator flashes amber.
4. Release the control button. The process is complete when the status LED indicator turns green. If no DHCP server is available on the network, the device IP address will default to one of the following:
   - **Devices with AXIS OS 12.0 and later:** Obtained from the link-local address subnet (169.254.0.0/16)
   - **Devices with AXIS OS 11.11 and earlier:** 192.168.0.90/24
5. Use the installation and management software tools to assign an IP address, set the password, and access the device.
   The installation and management software tools are available from the support pages on *axis.com/support*.

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

Check the current AXIS OS version

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

To check the current AXIS OS version:

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

Upgrade AXIS OS

Important

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

Note

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

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

2. Log in to the device as an administrator.
3. Go to **Maintenance > AXIS OS upgrade** and click **Upgrade**.

When the upgrade has finished, the product restarts automatically.

Technical problems and possible solutions

Problems upgrading AXIS OS

AXIS OS upgrade failed

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

Problems after AXIS OS upgrade

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

Problems setting the IP address

Can't set the IP address

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

Problems accessing the device

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

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

If you've lost the password for the root account, you must reset the device to the factory default settings. For instructions, see *Reset to factory default settings, on page 36*.

The IP address has been changed by DHCP

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

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

Certificate error when using IEEE 802.1X

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

The browser isn't supported

For a list of recommended browsers, see *Browser support, on page 14*.

Can't access the device externally

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

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

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

Problems with MQTT

Can't connect over port 8883 with MQTT over SSL

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

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

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

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

Performance considerations

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

The most important factors to consider:

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

Cybersecurity

Cybersecurity supports a successful product lifecycle with minimized risks. You can find in-depth information and documentation about our cybersecurity approach at *axis.com/about-axis/cybersecurity*. Follow the cybersecurity guidelines below to receive product security notifications from Axis and to configure your product for a secure lifecycle and decommissioning.

At *Axis Trust Center*, you can find information about how Axis implements security compliance, transparency, data protection, and privacy.

Vulnerability management

Axis is a *Common Vulnerability and Exposures (CVE) Numbering Authority (CNA)*. To minimize your risk of exposure, we follow industry standards when identifying and resolving vulnerabilities in our devices, software, and services. Refer to *axis.com/vulnerability-management* for information about our vulnerability management policy or to report a vulnerability.

Security notifications

Subscribe to Axis security notification emails at *axis.com/security-notification-service*. We will send you information about vulnerabilities, corresponding security advisories, and other security-related matters for your Axis product.

Secure product lifecycle

Axis minimizes risks throughout the lifetime of our products through secure lifecycle management. Use our hardening guides at *help.axis.com* to more securely configure and operate your Axis products and to find information about:

Secure first-use – Axis products are pre-configured with high default protection to allow for secure initialization and encrypted communication from the very start.

Intended use and common configuration mistakes – Our guides provide information about the intended usage of Axis products, including common security-relevant misuse and configuration mistakes that should be avoided.

Managing vulnerabilities and supply chain transparency – A Software Bill of Material (SBOM) is published with every software release on *axis.com* to disclose vulnerabilities and improve supply chain transparency.

Decommissioning and the secure erasure of data – To securely decommission a product when it reaches the end of its lifecycle, reset it to factory default settings. This erases your configurations, stored data, and sensitive information.

T10145149

2026-07 (M33.2)