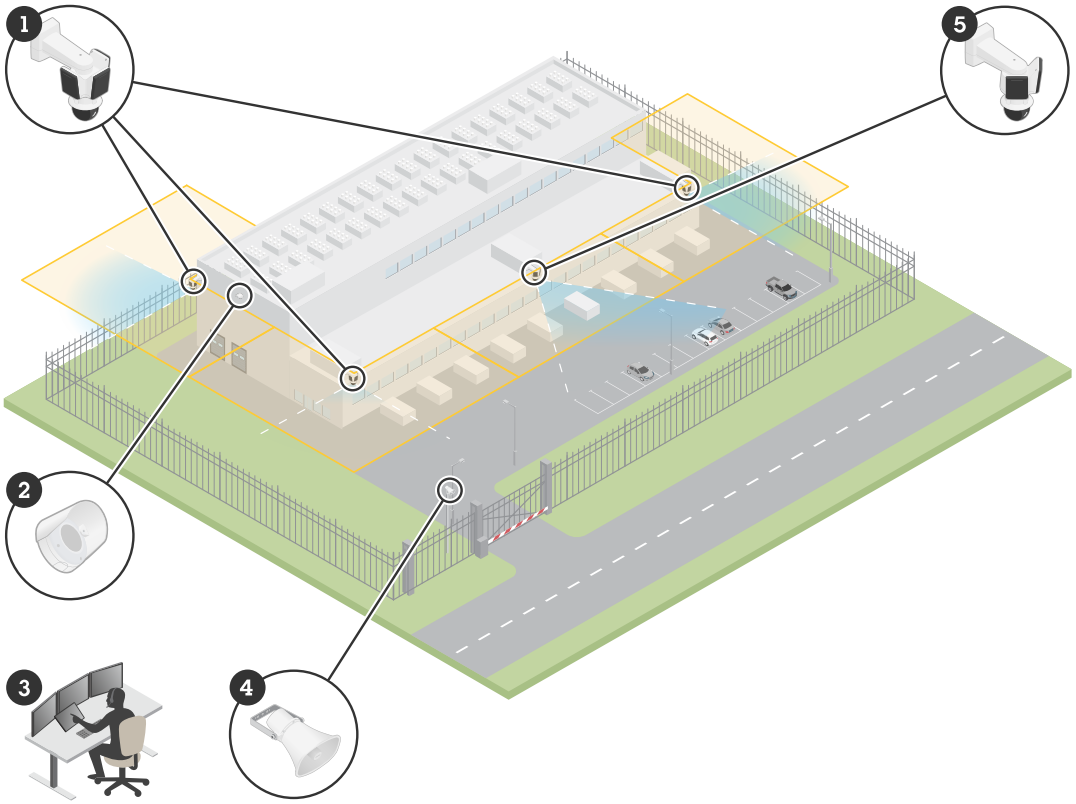
AXIS D21-VE Radar Series

AXIS D2122-VE Radar
AXIS D2123-VE Radar

User manual

Table of Contents

Solution overview



An example of the surveillance solution at a data center.

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

Installation

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

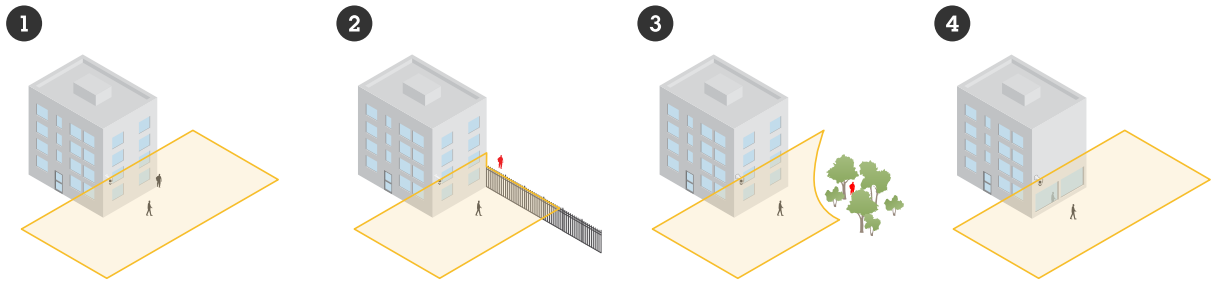
This video is an example on how to install AXIS D2122-VE Radar and AXIS D2123–VE Radar. For instructions on all installation scenarios and safety information, see the installation guide.

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

This animation shows how to mount AXIS D2122-VE Radar and AXIS D2123–VE Radar with AXIS T91D61 Wall Mount, AXIS T91D62 Telescopic Parapet Mount and AXIS TQ6501–E Parapet Mount.

Considerations

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

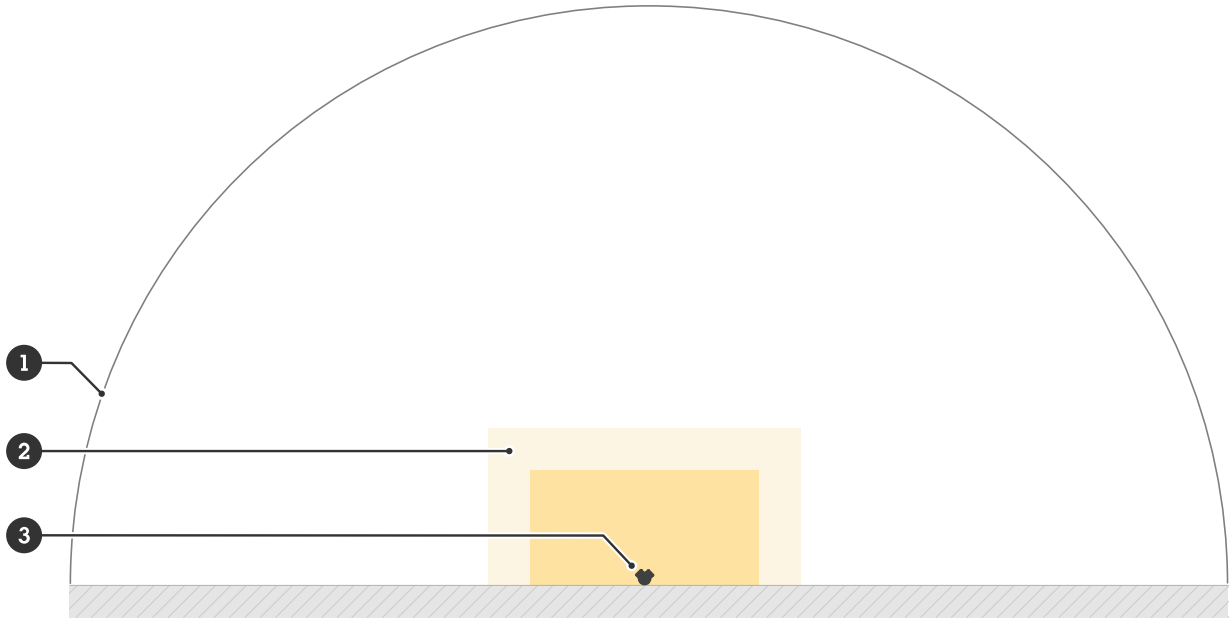


Monitor the scene

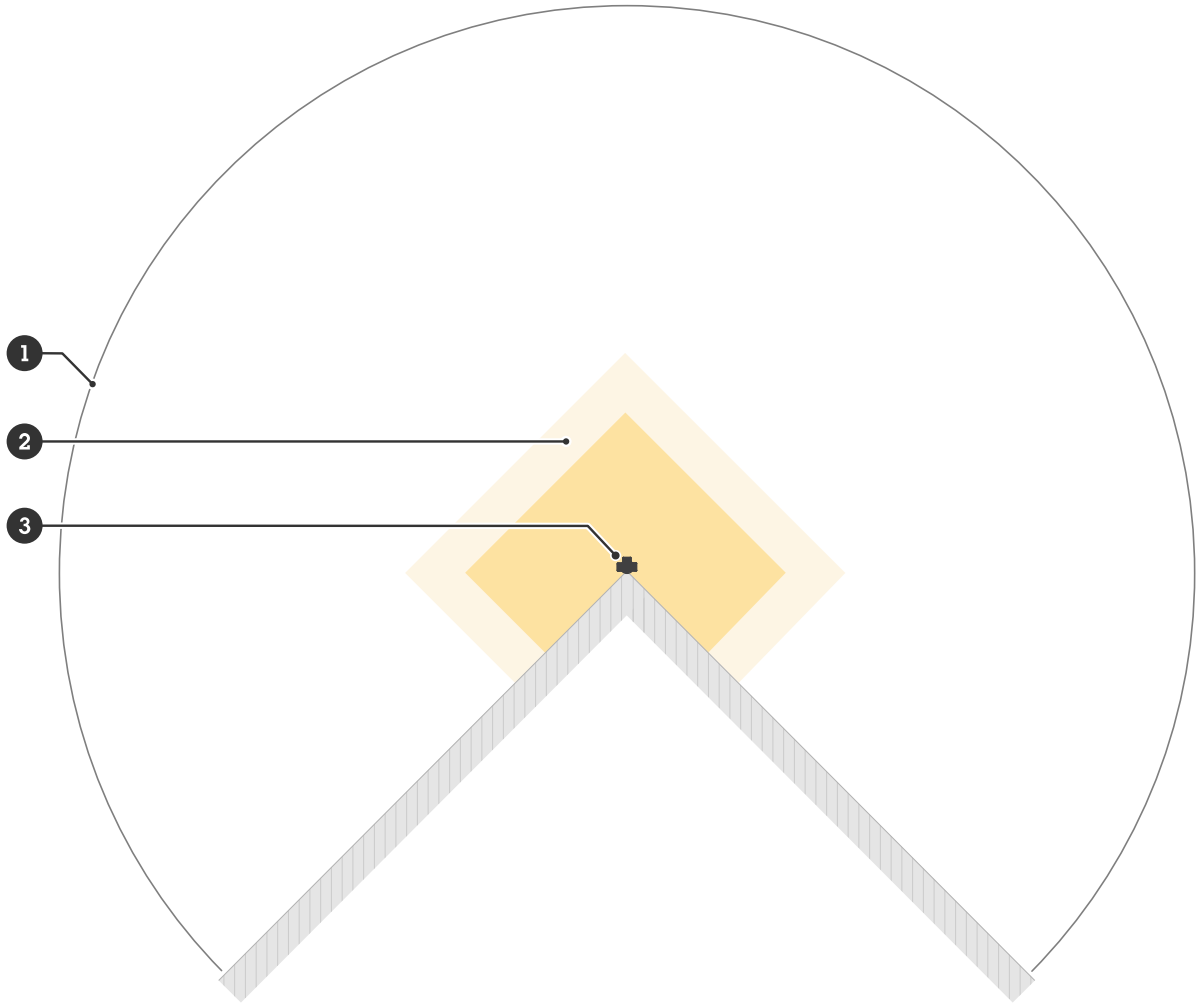
The radar can detect moving objects and classify them as humans, vehicles or unknown. When you monitor an area, use the **Area monitoring** profile.

Install multiple radars

To monitor areas such as the surroundings of a building or the buffer zone outside a fence, you can install multiple radars near each other. Each radar can coexist with up to eleven other AXIS D2122-VE or AXIS D2123-VE radars within a 500-meter (1640 feet) radius, which forms the coexistence zone. You can also install this radar model in the coexistence zone of previous Axis radar models, as they don't interfere with each other. For more information about the coexistence zone, see *Coexistence zone, on page 24*.



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



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

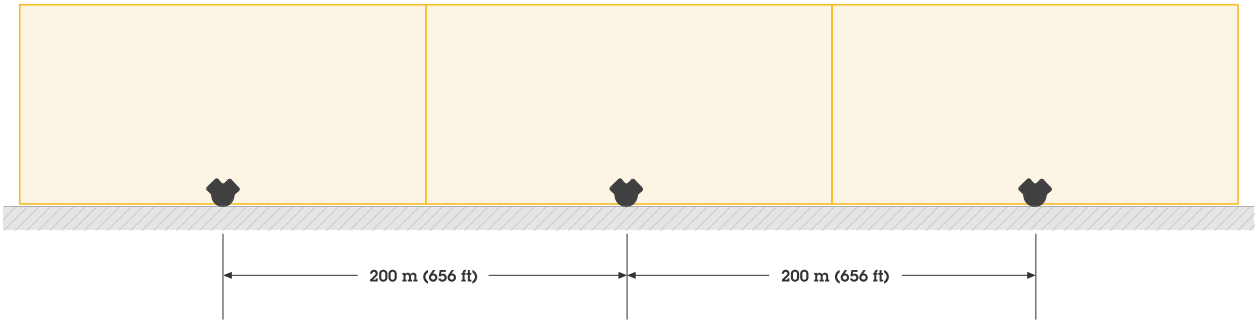
Note

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

Installation examples

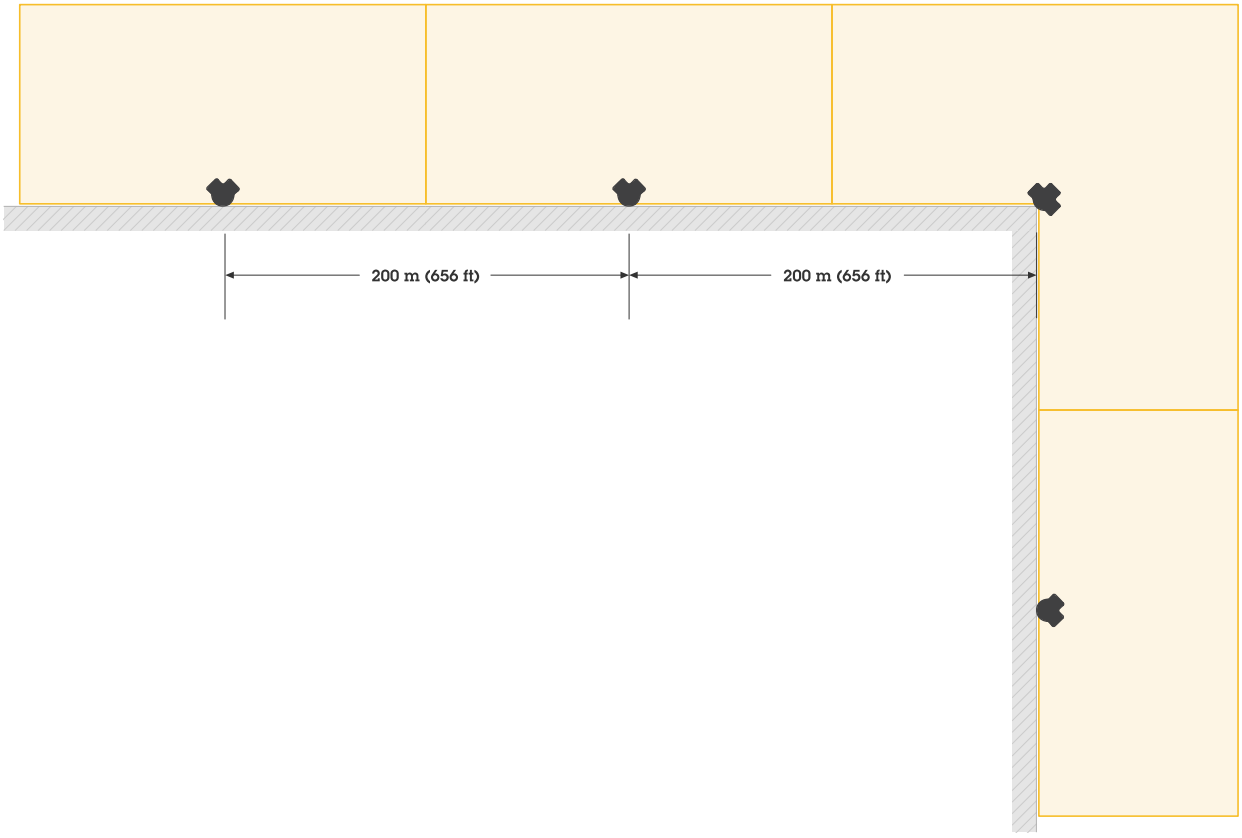
Create a virtual fence with multiple radars

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



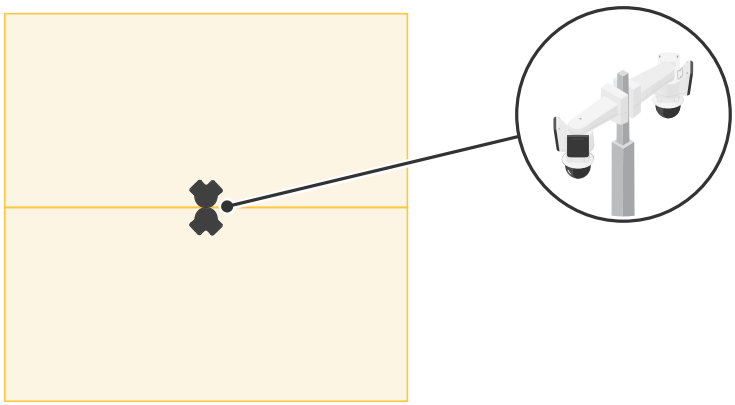
Cover an area around a building

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



Cover an open area

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

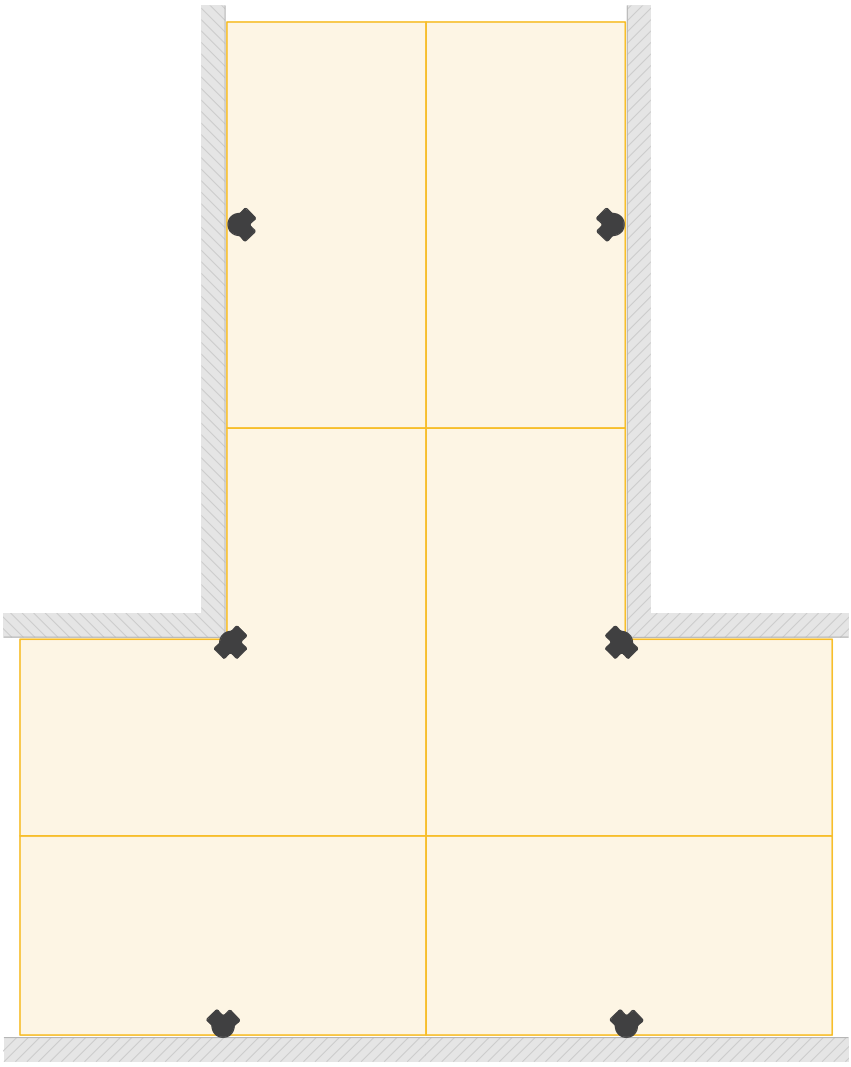


Note

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

Install multiple radars facing each other

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

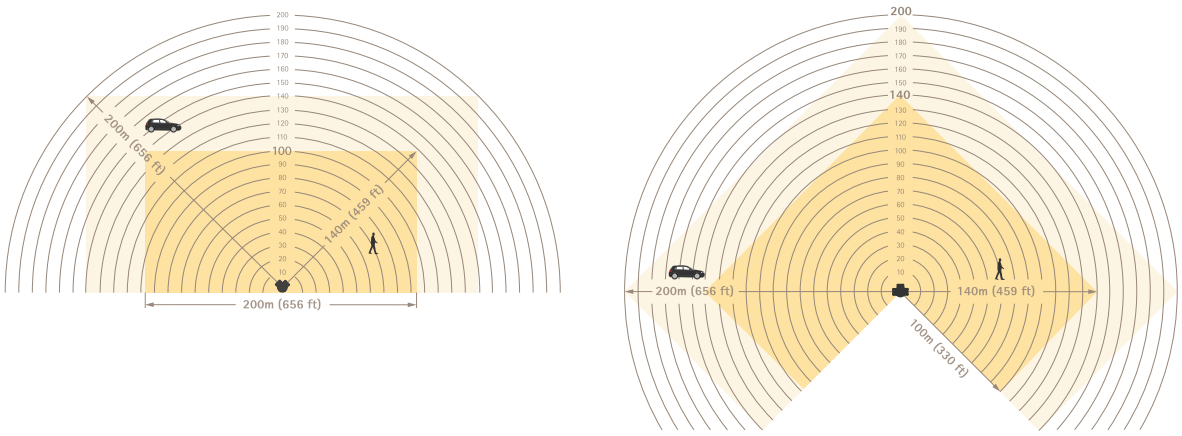


Recognition and detection distances

When the radar is mounted at the optimal installation height:

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

For more information about the zones, see *Recognition and detection zones, on page 24*.



Recognition and detection distances

Note

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

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

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

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

Mounting height	Minimum detection distance
4 m (9.8 ft)	4 m (9.8 ft)
5 m (16.4 ft)	6 m (19.7 ft)
6 m (19.7 ft)	8 m (26 ft)

7 m (23 ft)	11 m (36 ft)
8 m (26 ft)	13 m (42.7 ft)
9 m (29.5 ft)	15 m (49.2 ft)
10 m (32.8.5 ft)	18 m (59 ft)

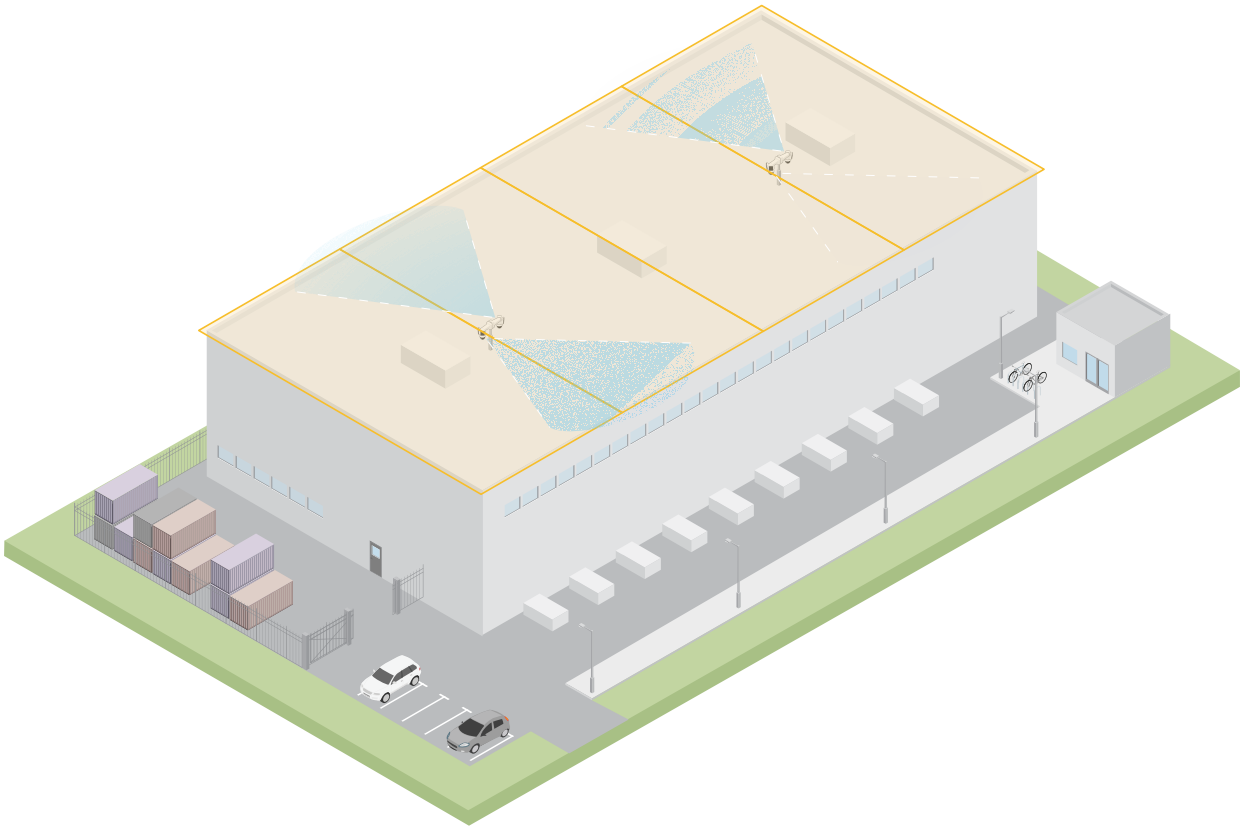
Note

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

Use cases

Rooftop area coverage

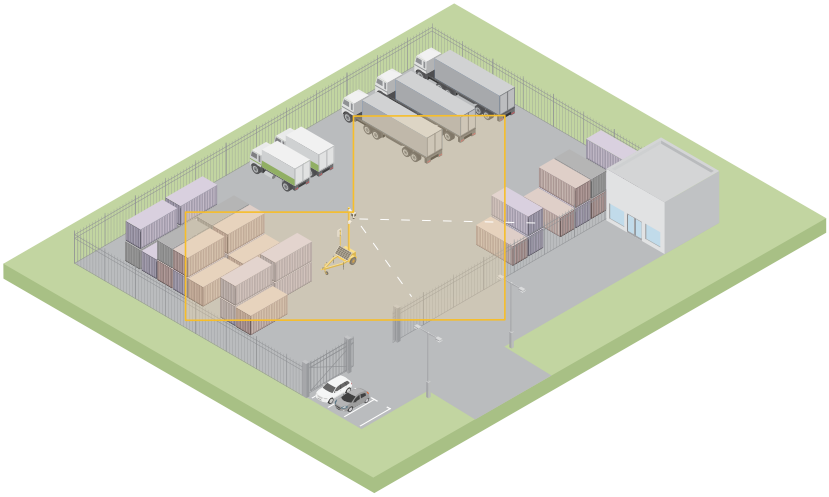
A large distribution center wants to use radars to cover the rooftop area. The radars are paired with ARTPEC-9 PTZ cameras and mounted back-to-back on poles, covering the whole rooftop. The radar discovers and classifies moving objects on the roof, and directs the camera to the object and lets the camera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



Use a mobile surveillance trailer to cover a large open area

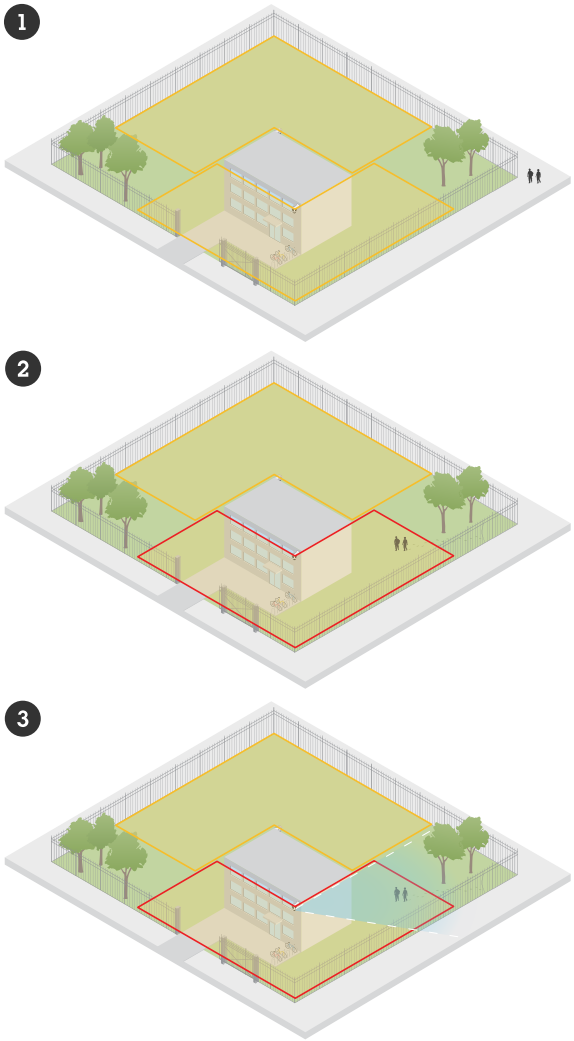
The outdoor yard of a hardware store has had several break-ins after-hours. There is one security guard on duty at a time, but there is a need to bolster the security at night without the added cost of hiring more staff. They have decided to install two radars mounted back-to-back on a mobile surveillance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

investigate the scene. They also consider installing a strobe speaker that is triggered by the radars to deter intruders.



Cover a fenced building

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



1. Intruders are walking outside the fence, not triggering an alarm.
2. Intruders break in through the fence, the radar discovers them and triggers an alarm.

3. The radar directs the PTZ camera towards the intruders, and lets the camera validate the alarm with video analytics.

For more information, see *Autotracking, on page 25*.

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 32*.

Secure passwords

Important

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

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

To protect your data we strongly recommend that you:

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

Configure your device

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

1. *Set the mounting height, on page 16*
2. If you install several radars close to each other: *Set the number of neighboring radars, on page 16*
3. *Add a map for reference, on page 16*
4. *Create a scenario for detecting objects, on page 17*
5. *Minimize false alarms, on page 18*
6. *Validate your installation, on page 19*

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**.

Set the number of neighboring radars

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

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

Add a map for reference

To make it easier to understand where in the scene objects are moving, you can choose to use a map as a background to the radar stream. You can use a ground plan or an aerial photo that shows the area covered by the radar. Adjust and calibrate the map so the radar view fits the position, direction, and scale of the map, and zoom in on the map if you're interested in a specific part of the scene.

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

Note

The maximum supported map image resolution is 1920x1080 px.

Use the setup assistant:

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

Edit each setting individually:

The map calibrates gradually after you adjust each setting.

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

5. Under **Distance**, add the actual distance between the two points you have added to the map.
6. Go to **Pan and zoom map** and use the buttons to pan the map image, or zoom in and out on the map image.

Note

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

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

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

To remove an uploaded map along with your settings, click **Reset calibration**.

Create a scenario for detecting objects

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

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

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

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

Minimize false alarms

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

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

Validate your installation

Validate the installation of the radar

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

Note

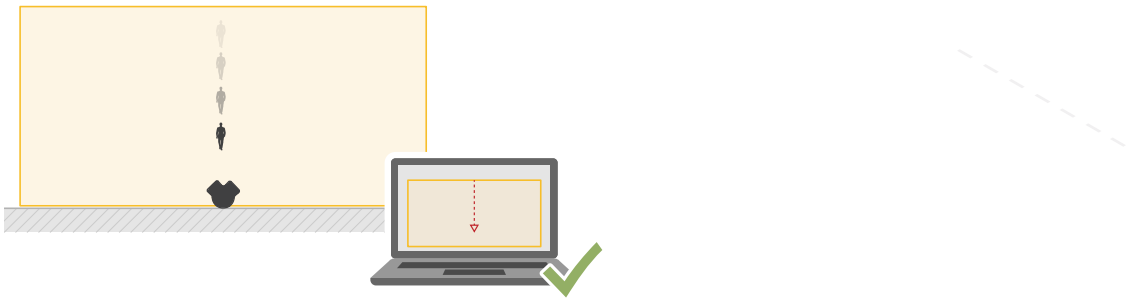
The installation is validated in the conditions that apply at the time of validation. Changed conditions in the scene can affect the everyday performance of your installation.

Check that there are no false detections

1. Check that the recognition zone is clear from human activity.
2. Wait for a few minutes to make sure the radar doesn't detect any static objects in the recognition zone.
3. If there are unwanted detections, you can filter out certain types of movement or objects, adjust the zones where objects trigger alarms, or adjust the detection sensitivity. For instructions, see *Minimize false alarms, on page 18*.

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

1. In the radar's web interface, start a recording. For instructions, see *Record and watch video, on page 20*.
2. Start walking just outside the recognition zone, and walk directly toward the radar.
3. Check that a human classification symbol is shown when the person enters the recognition zone.
4. Check that the radar's web interface shows the correct direction of travel.



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

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

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

Complete the validation

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

1. Make sure you have configured your radar according to the instructions.
2. Make sure you have added and calibrated a reference map.
3. Set the radar scenario to trigger when a human is detected. By default, **Seconds until trigger** is set to two seconds but you can change this if needed.
4. Set the radar to record video when an appropriate object is detected.
   For instructions, see *Record and watch video, on page 20*.
5. Go to **Radar > Settings > Object visualization** and set the **Trail lifetime** to one hour so that it will safely exceed the time it takes for you to leave your seat, walk around the area of surveillance, and return to your seat. The trail lifetime will keep the track in the radar's live view for the set time and, once you have finished the validation, you can disable it.
6. Walk along the border of the recognition zone and make sure that the trailing on the system matches the route that you walked.
7. If you are not satisfied with the results of your validation, re-calibrate the reference map and repeat the validation.

Adjust the radar image

This section includes instructions about configuring the radar image. If you want to learn more about how certain features work, go to *Learn more, on page 24*.

Show an image overlay

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

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

View and record video

This section includes instructions about configuring your device. To learn more about how streaming and storage works, go to *Streaming and storage, on page 25*.

Record and watch video

Record video directly from the radar

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

   If you haven't set up any storage, click and . For instructions on how to set up network storage, see
3. To stop recording, click ● again.

Watch video

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

Set up rules for events

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

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

Trigger an action

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

Note

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

Activate a sweeping red light on the radar

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

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

Create a schedule:

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

Create a rule:

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

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

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

Add an email recipient:

1. Go to **System > Events > Recipients** and add a recipient.
2. Type a name for the recipient.
3. Under **Type**, select **Email**.
4. Type an email address to send the email to.
5. Fill in the rest of the information according to your email provider.
   The radar device doesn't have its own email server, so it needs to log into an email server to send emails.
6. To send a test email, click **Test**.
7. Click **Save**.

Create a rule:

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

Connect to a strobe siren

Network pairing allows you to pair a camera with a compatible Axis device with light and siren functionality. Once paired, the camera can configure and maintain both devices.

Pair the camera with a strobe siren:

1. Go to **System > Edge-to-edge > Pairing**.
2. Click + **Add** and select the pairing type **Network pairing** from the drop-down list.
3. Type the IP address, username and password of the strobe siren.
4. Click **Connect**. A confirmation message appears.

To find devices directly on the network, click **Discover devices**.

Note

- The list shows all Axis devices that are found, not only devices that can be paired.
- An info icon is shown for devices that have already been paired. Hover over the icon to get information about pairings that are already active.
- Make sure the paired devices run the same AXIS OS version.

Important

- It's only possible to discover devices where Bonjour is enabled. To enable Bonjour for a device, open its web interface and go to **System > Network > Network discovery protocols**.

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*.

Learn more

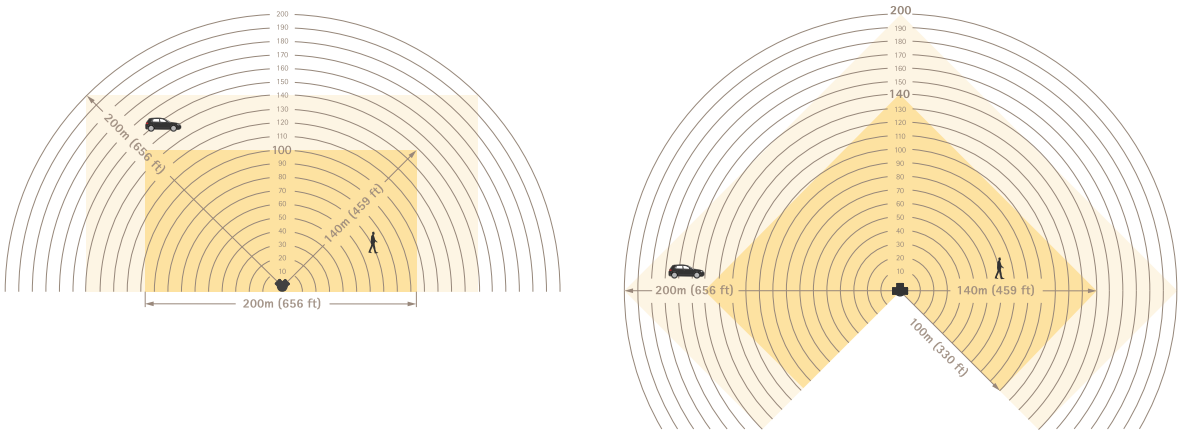
Radar

Recognition and detection zones

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

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

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



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

Scenarios, inclusion zones, and exclusion zones

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

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

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

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

Coexistence zone

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

Radar-video fusion technology

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

Autotracking

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

- If you want to connect one radar and one ARTPEC-9 PTZ camera that are mounted together, use radar pairing to use built-in radar-video fusion autotracking. This option combines AI-powered radar and video analytics to minimize false alarms. For instructions on how to set up radar-video fusion autotracking, see the *Radar-video fusion autotracking user manual*.
- If you want to connect multiple PTZ cameras and radars, use the application AXIS Radar Autotracking for PTZ. For more information, see *Control a PTZ camera with AXIS Radar Autotracking for PTZ, on page 25*.
- If you want to connect one radar and one ARTPEC-7 PTZ camera that are mounted close to each other, use camera pairing to use the built-in radar autotracking.

Control a PTZ camera with AXIS Radar Autotracking for PTZ

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

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

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

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

Overlays

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

Streaming and storage

Video compression formats

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

Motion JPEG

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

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

H.264 or MPEG-4 Part 10/AVC

Note

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

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

AV1

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

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

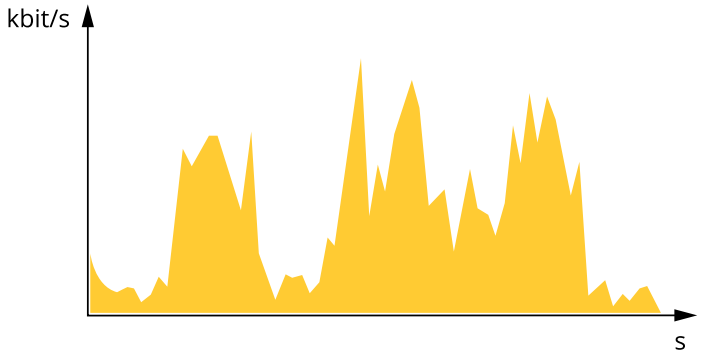
Note

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

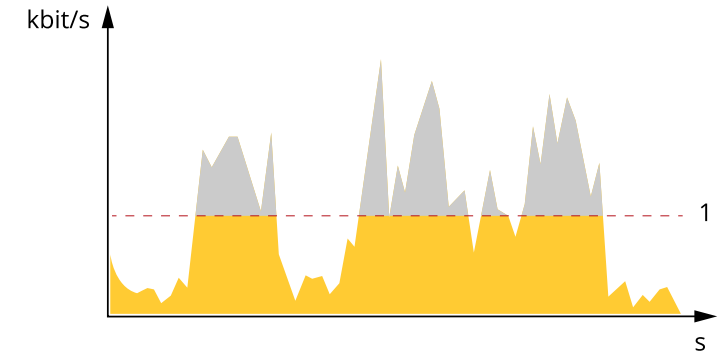
Bitrate control

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

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



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

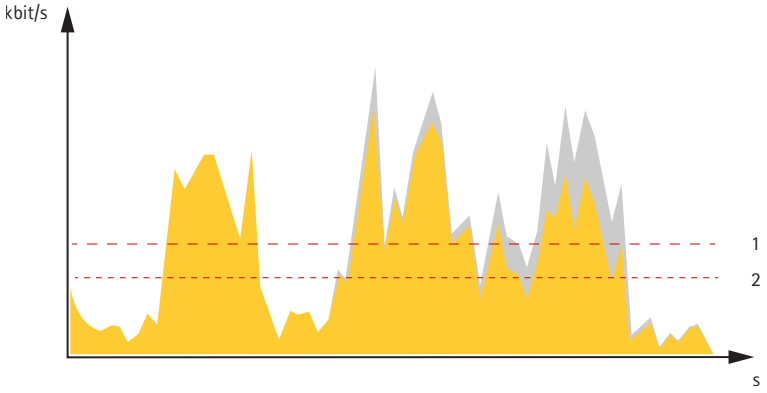


1 Target bitrate

Average bitrate (ABR)

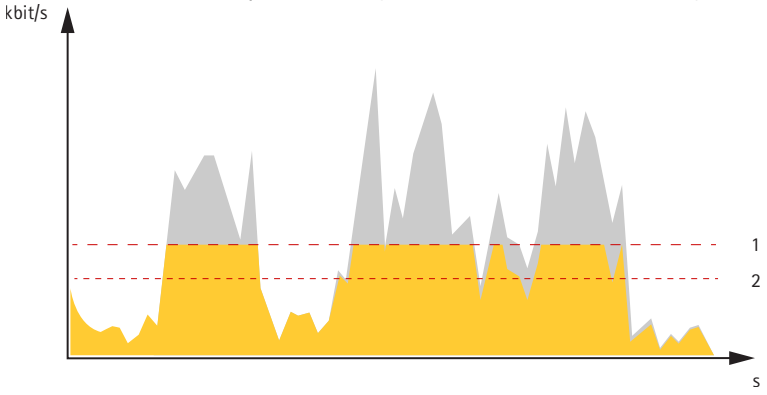
With average bitrate, the bitrate is automatically adjusted over a longer period of time. This is so you can meet the specified target and provide the best video quality based on your available storage. Bitrate is higher in scenes with a lot of activity, compared to static scenes. You are more likely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

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



1 Target bitrate
2 Actual average bitrate

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



1 Target bitrate
2 Actual average bitrate

Edge-to-edge technology

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

Note

Make sure the paired devices run the same AXIS OS version.

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

Speaker pairing

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

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

Microphone pairing

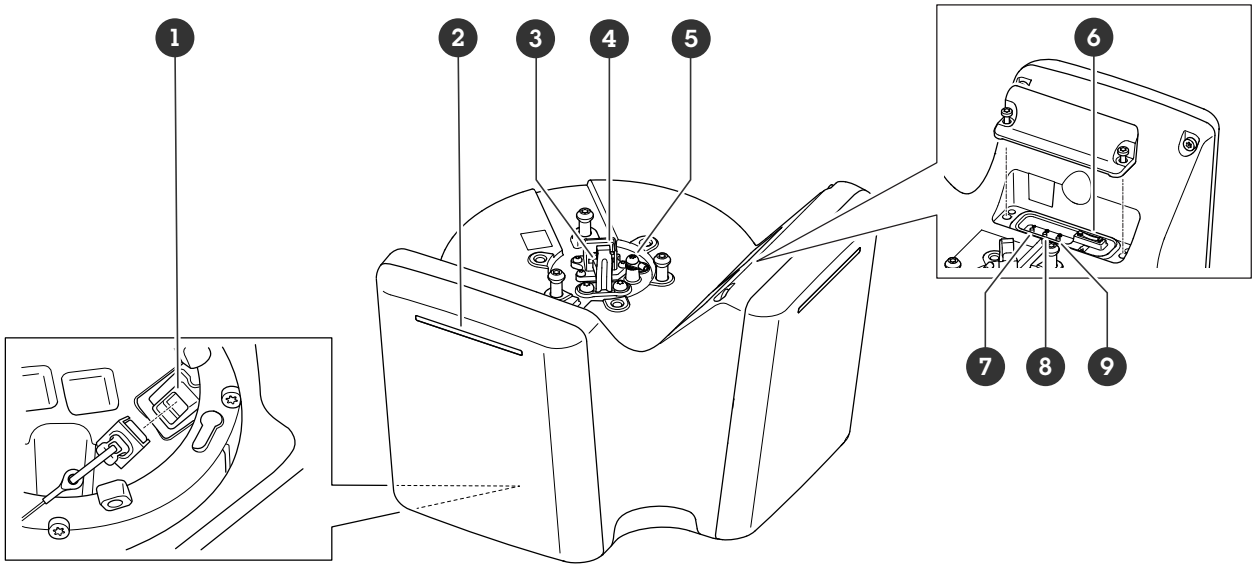
Edge-to-edge microphone pairing allows you to use a compatible Axis microphone as if it's part of your camera. Once paired, the microphone will take up sounds from the surrounding area and make it available as an audio input device, usable in media streams and recordings.

Network pairing

With edge-to-edge network pairing, you can connect your camera to a compatible Axis device with light and siren or illuminator light functionality and benefit from its integrated features.

Specifications

Product overview



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

LED indicators

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

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

SD card slot

This device supports microSD/microSDHC/microSDXC cards.

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

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

Buttons

Control button

The control button is used for:

- Resetting the product to factory default settings. See *Reset to factory default settings, on page 32*.

Connectors

Network connector (PoE in)

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

Note

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

Network connector (PoE out)

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

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

Note

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

Note

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

Clean your device

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

NOTICE

- Harsh chemicals can damage the device. Don't use chemicals such as window cleaner or acetone to clean your device.
- 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 29*.
3. Keep the control button pressed for 15–30 seconds until the status LED indicator flashes amber.
4. Release the control button. The process is complete when the status LED indicator turns green. If no DHCP server is available on the network, the device IP address will default to one of the following:
   - **Devices with AXIS OS 12.0 and later:** Obtained from the link-local address subnet (169.254.0.0/16)
   - **Devices with AXIS OS 11.11 and earlier:** 192.168.0.90/24
5. Use the installation and management software tools to assign an IP address, set the password, and access the device.
   The installation and management software tools are available from the support pages on *axis.com/support*.

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

Make sure that no one has tampered with the device software

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

1. Reset to factory default settings. See *Reset to factory default settings, on page 32*.
   After the reset, secure boot guarantees the state of the device.
2. Configure and install the device.

AXIS OS options

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

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

Check the current AXIS OS version

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

To check the current AXIS OS version:

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

Upgrade AXIS OS

Important

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

Note

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

1. Download the AXIS OS file to your computer, available free of charge at *axis.com/support/device-software*.
2. Log in to the device as an administrator.
3. Go to **Maintenance > AXIS OS upgrade** and click **Upgrade**.

When the upgrade has finished, the product restarts automatically.

Technical problems and possible solutions

Problems upgrading AXIS OS

AXIS OS upgrade failed

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

Problems after AXIS OS upgrade

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

Problems setting the IP address

Can't set the IP address

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

Problems accessing the device

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

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

If you've lost the password for the root account, you must reset the device to the factory default settings. For instructions, see *Reset to factory default settings, on page 32*.

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*.

Problems with the image

Image degradation or image loss

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

Problems with the device turning itself off

The device shuts down

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

Performance considerations

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

The most important factors to consider:

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

Contact support

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

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.

T10223326

2026-07 (M10.3)