AXIS Q19–E Thermal Camera Series
AXIS Q1951–E Thermal Camera
AXIS Q1952–E Thermal Camera

User Manual

Solution overview
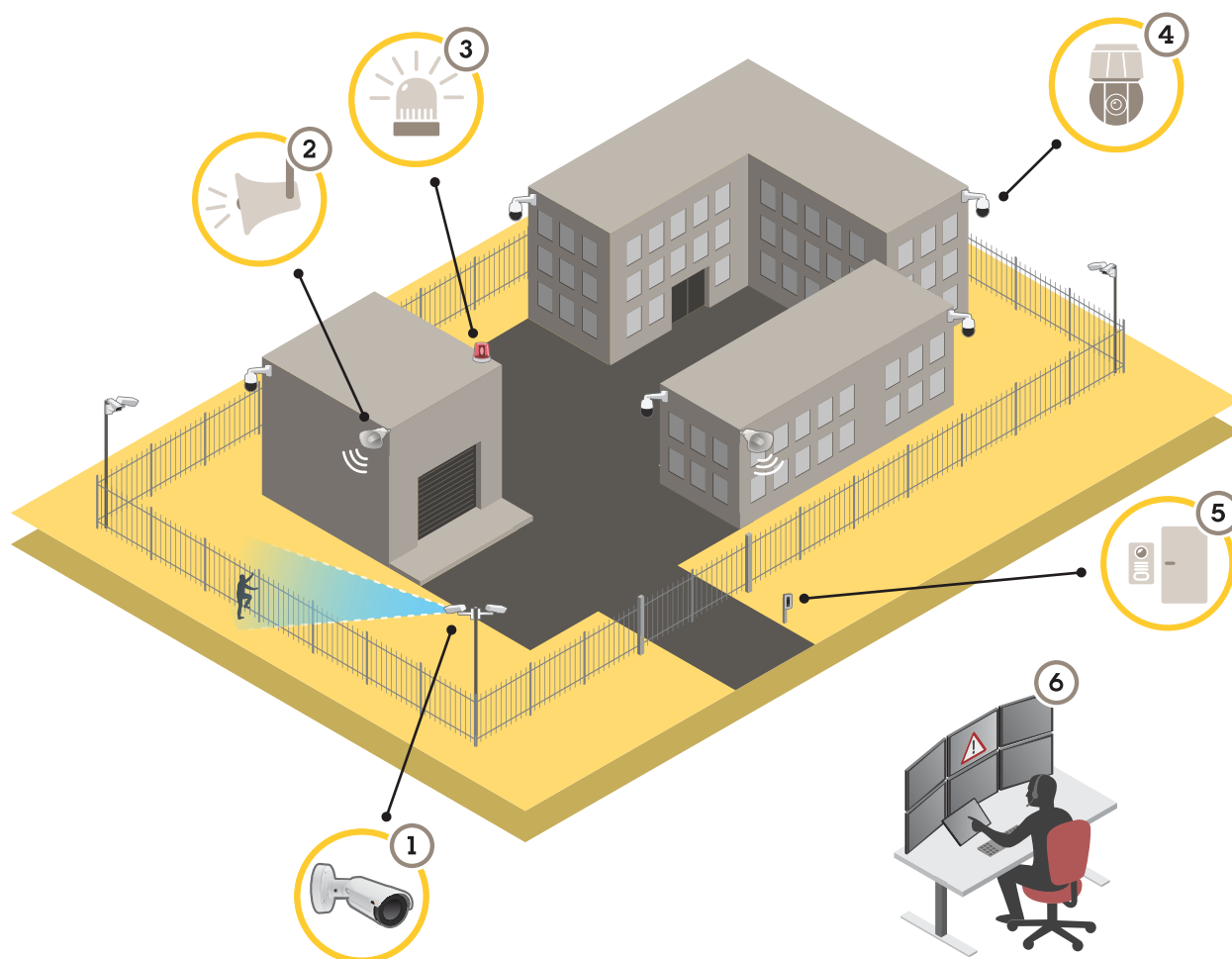
1   Thermal camera with AXIS Perimeter Defender
2   Horn speaker
3   Flashing beacon
4   PTZ network camera
5   Door controller
6   Surveillance center

Perimeter protection

For areas in need of intrusion detection, you can set up perimeter protection using thermal cameras with analytics. The main objective for perimeter protection is to detect a threat or an actual intrusion at the earliest possible stage.

To set up perimeter protection, you need to install an analytics application for perimeter surveillance and protection on your thermal camera. Axis provides the AXIS Perimeter Defender application for this purpose. You can read more about AXIS Perimeter Defender at *axis.com/products/axis-perimeter-defender*

Solution overview

- To let possible intruders know that your perimeter is protected, use a flashing beacon (3). See *Deter intruders with a flashing beacon on page 10.*

- To warn and deter, connect a horn speaker (2) that plays a pre-recorded warning message. See *Deter intruders with audio on page 11.*

Get started

Find the device on the network

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

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

Browser support

You can use the device with the following browsers:

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

Supported in iOS and iPadOS

If you need more information about recommended browsers, go to *AXIS OS Portal*.

Access the device

1. Open a browser and enter the IP address or host name of the Axis device.

   If you do not know the IP address, use AXIS IP Utility or AXIS Device Manager to find the device on the network.

2. Enter the username and password. If you access the device for the first time, you must set the root password. See *Set a new password for the root account on page 4*.

3. The live view page opens in your browser.

Verify that no one has tampered with the firmware

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

1. Reset to factory default settings. See *Reset to factory default settings on page 23*.

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

2. Configure and install the device.

Set a new password for the root account

Important

   The default administrator username is **root**. If the password for root is lost, reset the device to factory default settings. See *Reset to factory default settings on page 23*

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

www.axis.com/products/online-manual/67055#t10098905

Support tip: Password security confirmation check

1. Type a password. Follow the instructions about secure passwords. See *Secure passwords on page 5* .

2. Retype the password to confirm the spelling.

3. Click **Create login**. The password has now been configured.

Secure passwords

Important

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

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

To protect your data we strongly recommend that you:

- Use a password with at least 8 characters, preferably created by a password generator.

- Don't expose the password.

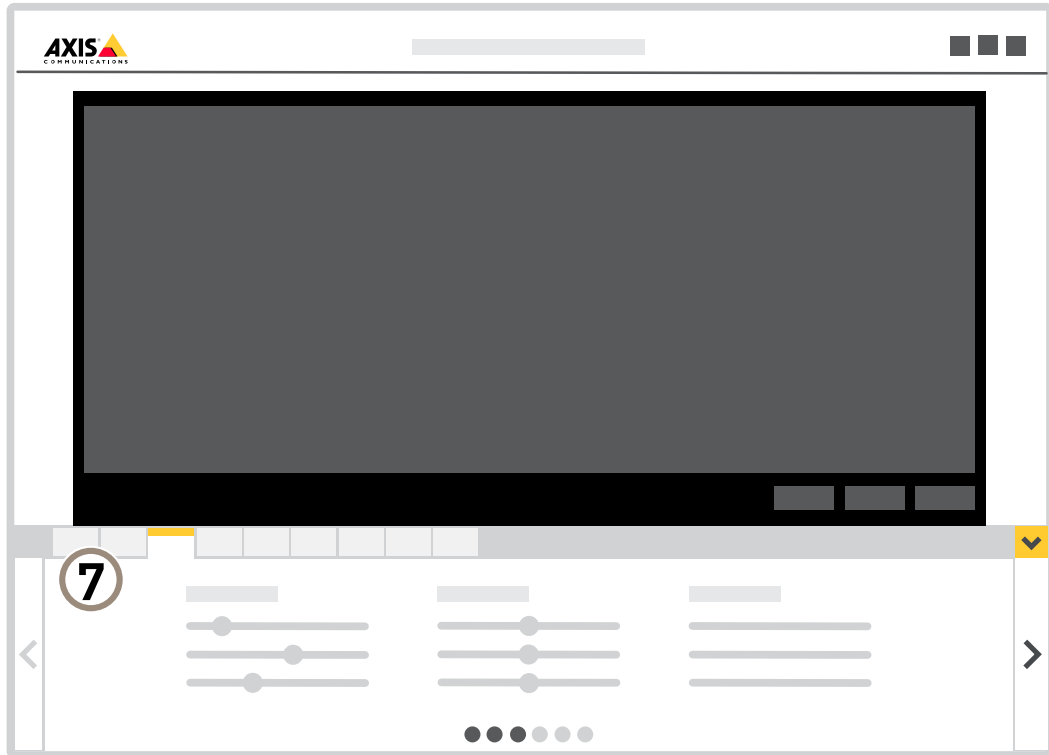- Change the password at a recurring interval, at least once a year.

Webpage overview

1 *Live view control bar*
2 *Live view*
3 *Product name*
4 *User information, color themes, and help*
5 *Video control bar*
6 *Settings toggle*

Get started

7   *Settings tabs*

Configure your device

Adjust the image

This section includes instructions about how to configure your device. If you want to learn more about how certain features function, go to *Learn more on page 17*.

Hide parts of the image with privacy masks

You can create one or several privacy masks to hide parts of the image.

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

www.axis.com/products/online-manual/67055#t10106902

How to create a privacy mask

1. Go to **Settings > Privacy mask**.

2. Click **New**.

3. Adjust the size, color, and name of the privacy mask according to your needs.

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

www.axis.com/products/online-manual/67055#t10106902

How to change the appearance of the mask
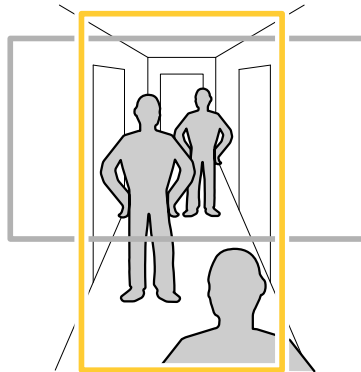
Show an image overlay

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

Monitor long and narrow areas

Use corridor format to better utilize the full field of view in a long and narrow area, for example a staircase, hallway, road, or tunnel.

1. Depending on your device, turn the camera or the 3-axis lens in the camera 90° or 270°.

2. If the device doesn't have automatic rotation of the view, log in to the webpage and go to **Settings** > **System** > **Orientation**.

3. Click ⊡▲ .

4. Rotate the view 90° or 270°.

Find out more at *axis.com/axis-corridor-format*.

Stabilize a shaky image with Electronic Image Stabilization (EIS)

Electronic Image Stabilization (EIS) can be used in environments where the product is mounted in an exposed location and subject to vibrations, for example, wind or passing traffic. Turn on EIS to get a smoother and steadier image without blur.

EIS also reduces the file size of the compressed image and lowers the bitrate of the video stream.

Note

> When EIS is turned on the image is cropped slightly, lowering the maximum resolution.

1. Go to **Settings > Image > Image correction**.

2. Turn on EIS.

View and record video

This section includes instructions about how to configure your device. To learn more about how streaming and storage works, go to *Streaming and storage on page 17*.

Reduce bandwidth and storage

Important

> If you reduce the bandwidth it can result in loss of details in the picture.

1. Go to live view and select **H.264**.

2. Go to **Settings > Stream**.

3. Do one or more of the following:

    -   Turn on the Zipstream functionality and select the desired level.

    Note

    > The zipstream settings are used for both H.264 and H.265.

- – Turn on dynamic GOP and set a high GOP length value.

- – Increase the compression.

- – Turn on dynamic FPS.

Note

Web browsers do not support H.265 decoding. Use a video management system or application supporting H.265 decoding.

Set up network storage

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

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

2. Click **Setup** under **Network storage**.

3. Enter the IP address of the host server.

4. Enter the name of the shared location on the host server.

5. Move the switch if the share requires a login, and enter username and password.

6. Click **Connect**.

Record and watch video

To record video you must first set up network storage, see *Set up network storage on page 10*, or have an SD card installed.

Record video

1. Go to the live view.

2. To start a recording, click **Record**. Click again to stop the recording.

Watch video

1. Click **Storage > Go to recordings**.

2. Select your recording in the list and it will play automatically.

Set up rules and alerts

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.

Deter intruders with a flashing beacon

Use a flashing beacon light to let possible intruders know that your perimeter is protected.

This example explains how to connect a beacon light and set it up to flash whenever the thermal camera detects an intrusion. In this example, the beacon light can only be activated to flash outside office hours, between 18.00 and 08.00 Monday–Friday, and it flashes for 30 seconds each time it is activated.

Required hardware

- Connecting wires (one blue and one red, min area: 0.25 mm^2, max area: 0.5 mm^2)

- Flashing beacon (12 V DC, max 25 mA)

Configure your device

Note

The maximum length of the connecting wires depends on the wire area and the power consumption of the flashing beacon.

Connect the devices physically

1. Connect the red wire to pin 2 (DC output, 12 V DC) of the camera's I/O connector.

2. Connect the other end of the red wire to the connector marked with **+** on the flashing beacon.

3. Connect the blue wire to pin 4 (digital output) of the camera's I/O connector.

4. Connect the other end of the blue wire to the connector marked with **–** on the flashing beacon.

Configure I/O ports

You need to connect the flashing beacon to the camera in the camera's webpage.

1. Go to **System** > **I/O ports**.

2. Under **Port 2**, enter a name for the output module, for example "Flashing beacon".

3. To make the beacon start flashing when an event occurs, select **Open circuit (NO)** as normal state.
    .
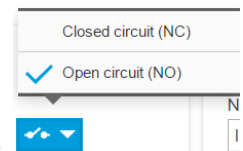
Create a rule

For the camera to send a notification to the beacon to start flashing when something is detected, you need to create a rule in the camera.

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

2. Enter a name, for example "Flashing beacon".

3. In the list of conditions, under **Application**, select the perimeter defender application.

4. Select **Use this condition as a trigger**.

5. Click **+** to add another condition.

6. In the list of conditions, under **Scheduled and recurring**, select **Scheduled event**.

7. In the list of schedules, select **After hours**.

8. In the list of actions, under **I/O**, select **Output port**.

9. In the port list, select **Flashing beacon**.

10. Set the duration to 30 seconds.

11. Click **Save**.

Deter intruders with audio

Use a network horn speaker to warn and deter possible intruders.

This example explains how to connect an Axis network horn speaker and set it up to play an audio clip whenever the thermal camera detects an intrusion. In this example, the horn speaker can only be activated outside office hours, between 18.00 and 08.00 Monday–Friday.
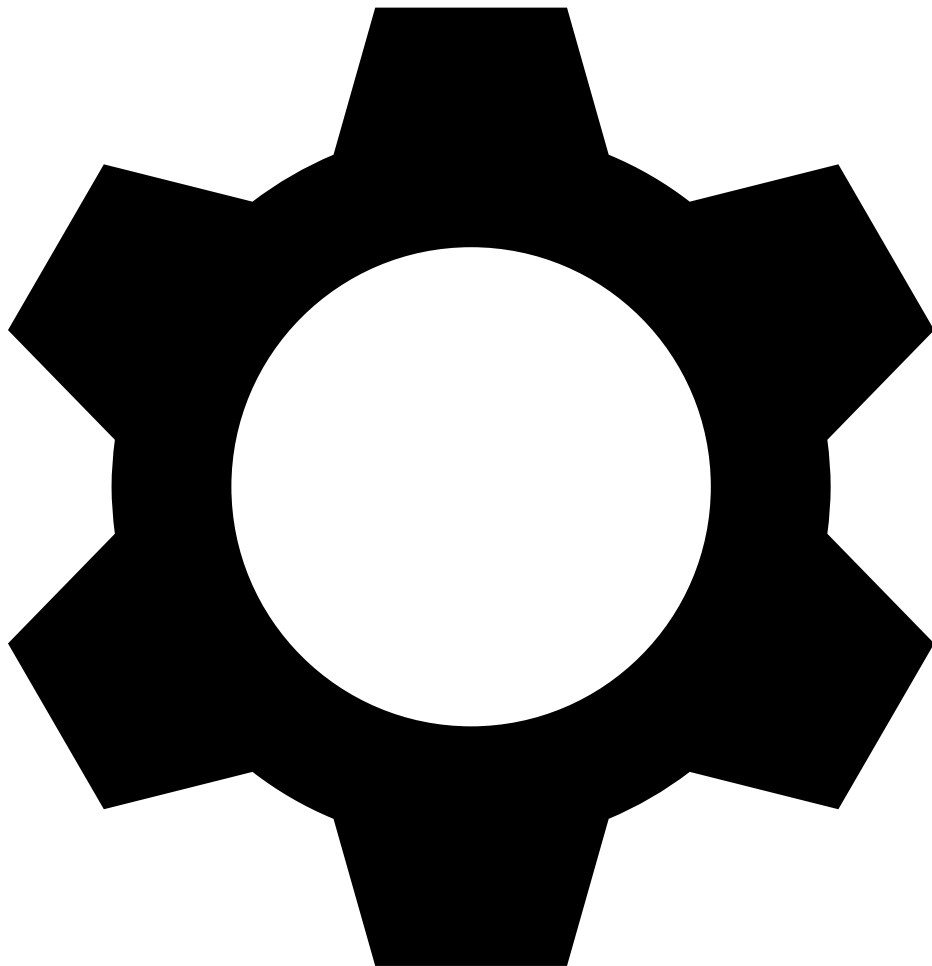
Configure your device

Connect the devices

1. Go to **System > Accessories**.

2. Under **Network speaker pairing**, enter the IP address, username, and password for the speaker. You need to use an administrator or operator account.

3. Click **Connect**.

Upload audio clip to the camera

1. Go to **Audio > Audio clips** and click

.

2. Click **+**.

3. Locate and add the audio clip.

4. Click **Close**.

Create a rule

For the camera to make the speaker play the audio clip when something is detected, you need to create a rule in the camera.

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

2. Enter a name, for example "Deter with audio".

3. In the list of conditions, under **Application**, select the perimeter defender application.

4. Select **Use this condition as a trigger**.

5. Click **+** to add another condition.

6. In the list of conditions, under **Scheduled and recurring**, select **Scheduled event**.

7. In the list of schedules, select **After hours**.

8. In the list of actions, under **Audio clips**, select **Play audio clip**.

9. Under **Clip**, select your uploaded audio clip.

10. Under **Audio output**, select **1** for the paired network speaker.

11. Click **Save**.

Detect tampering with input signal

This example explains how to trigger an alarm when the input signal has been cut or short-circuited. For more information about the I/O connector, see *page 28*.

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

www.axis.com/products/online-manual/67055#t10110432

How to send an email notification when someone tampers with the input signal

1. Go to **Settings > System > I/O Ports** and turn on **Supervised I/O**.

Create a rule:

1. Go to **Settings > System > Events** and add a rule.

2. Type a name for the rule.

3. In the list of conditions, select **Digital input** and then select a port.

4. In the list of actions, select **Send notification to email** and then select a recipient from the list. Go to **Recipients** to create a new recipient.

   To create a new recipient, click ➕ . To copy an existing recipient, click 🗎 .

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

6. Click **Save**.

Send an email automatically if someone spray paints the lens

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

www.axis.com/products/online-manual/67055#t10106687

How to send an email notification if someone spray paint the lens

1. Go to **Settings > System > Detectors**.

2. Turn on **Trigger on dark images**. This will trigger an alarm if the lens is sprayed, covered, or rendered severely out of focus.

3. Set a duration for **Trigger after**. The value indicates the time that must pass before an email is sent.

Create a rule:

1. Go to **Settings > System > Events > Rules** and add a rule.

2. Type a name for the rule.

3. In the list of conditions, select **Tampering**.

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

5. Select a recipient from the list or go to **Recipients** to create a new recipient.

   To create a new recipient, click ➕ . To copy an existing recipient, click ▊ .

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

7. Click **Save**.

Audio

Add audio to your recording

Turn on audio:

1. Go to **Settings > Audio** and turn on **Allow audio**.

2. Go to **Input > Type** and select your audio source.

Edit the stream profile which is used for the recording:

3. Go to **Settings > Stream** and click **Stream profiles**.

4. Select the stream profile and click **Audio**.

5. Select the checkbox and select **Include**.

6. Click **Save**.

7. Click **Close**.

Cleaning recommendations

If the device gets grease stains or becomes heavily soiled, you can clean it with mild, solvent-free soap or detergent.

NOTICE

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

1. Use a can of compressed air to remove any dust or loose dirt from the device.

2. Clean the device with a soft cloth dampened with mild detergent and lukewarm water.

3. Wipe carefully with a dry cloth.

Note

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

Learn more

Color palettes

Color palettes applied to thermal images help the human eye distinguish image details. The colors in the palette are artificially created pseudocolors that emphasize temperature differences.

The product has several color palettes to choose from. If an operator watches the video stream, you can choose any of the palettes. If the video stream is only used by applications, select the white-hot palette.

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.

The video streaming indicator is another type of overlay. It shows you that the live view video stream is live.

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

Note

> To ensure support for the Opus audio codec, the Motion JPEG stream is always sent over RTP.

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 the MPEG-4 standard. 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

Note

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

How do Image, Stream, and Stream profile settings relate to each other?

The **Image** tab contains camera settings that affect all video streams from the product. If you change something in this tab, it immediately affects all video streams and recordings.

The **Stream** tab contains settings for video streams. You get these settings if you request a video stream from the product and don't specify for example resolution, or frame rate. When you change the settings in the **Stream** tab, it doesn't affect ongoing streams, but it will take effect when you start a new stream.

The **Stream profiles** settings override the settings from the **Stream** tab. If you request a stream with a specific stream profile, the stream contains the settings of that profile. If you request a stream without specifying a stream profile, or request a stream profile that doesn't exist in the product, the stream contains the settings from the **Stream** tab.

Bitrate control

With bitrate control, you can manage the bandwidth consumption of your video stream.

Variable bitrate (VBR)
With variable bitrate, the bandwidth consumption varies based on the level of activity in the scene. The more activity in the scene, the more bandwidth you need. You are guaranteed constant image quality but it requires storage margins.
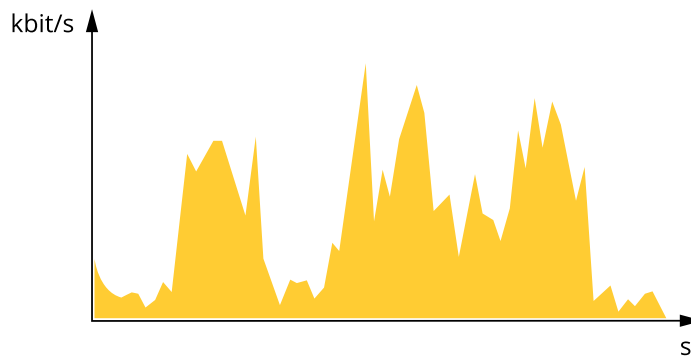
Maximum bitrate (MBR)
With maximum bitrate, you can set a target bitrate to handle bitrate limitations in your system. You may see a decline in image quality or frame rate when the instantaneous bitrate is kept below the specified target bitrate. You can choose to either prioritize image quality or frame rate. We recommend that you configure the target bitrate to a higher value than the expected bitrate. This gives you a margin for additional complexity that needs to be captured.
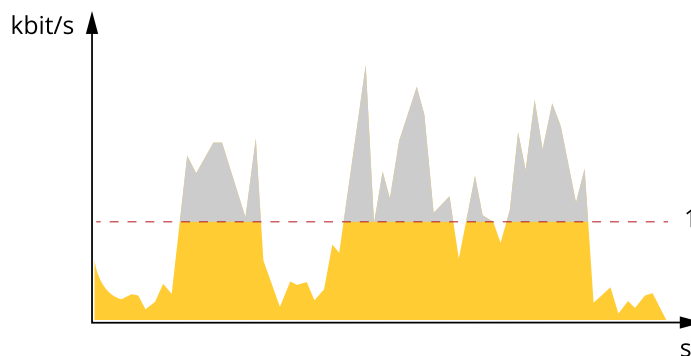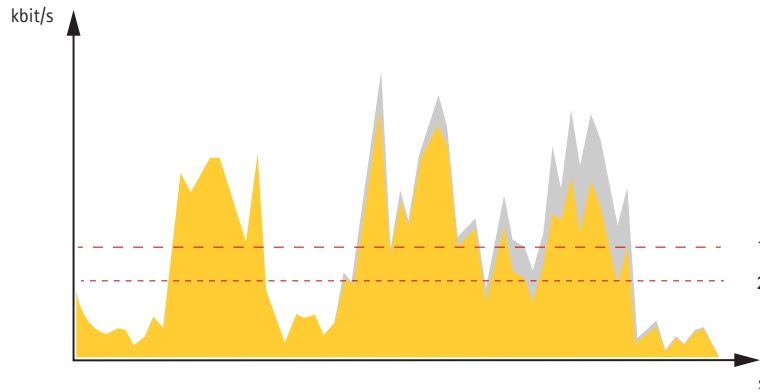

1   Target bitrate

Average bitrate (ABR)
With average bitrate, the bitrate is automatically adjusted over a longer timescale. 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 needed when using 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:
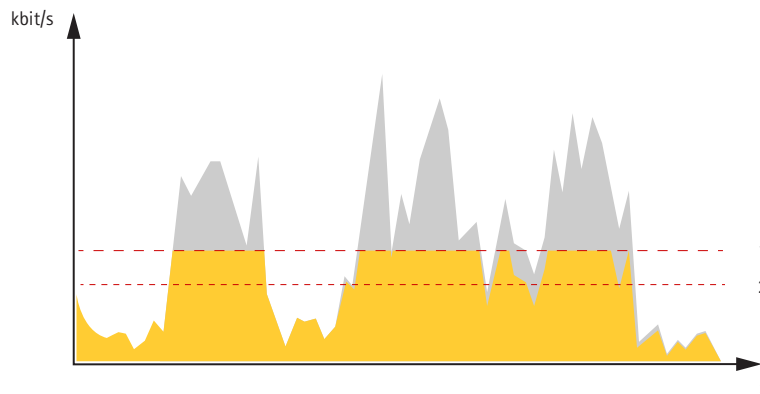
- To calculate the estimated storage need, set the target bitrate and the retention time.

- 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

Applications

AXIS Camera Application Platform (ACAP) is an open platform that enables third parties to develop analytics and other applications for Axis products. To find out more about available applications, downloads, trials and licenses, go to *axis.com/applications*.

To find the user manuals for Axis applications, go to *axis.com*.

Note

- Several applications can run at the same time but some applications might not be compatible with each other. Certain combinations of applications might require too much processing power or memory resources when run in parallel. Verify that the applications work together before deployment.

19

Learn more

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

www.axis.com/products/online-manual/67055#t10001688

How to download and install an application

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

www.axis.com/products/online-manual/67055#t10001688

How to activate an application licence code on a device

AXIS Perimeter Defender

AXIS Perimeter Defender is an application for perimeter surveillance and protection. It is ideal for high-security perimeter protection where there is a need to strengthen the physical access control system with reliable intrusion detection.

AXIS Perimeter Defender is primarily designed for so-called sterile zone protection, for example along a fence marking a boundary. The term sterile zone refers to an area where people are not supposed to be.

Use AXIS Perimeter Defender in an outdoor environment to:

- Detect moving persons.

- Detect moving vehicles, without discriminating between vehicle types.

Learn more
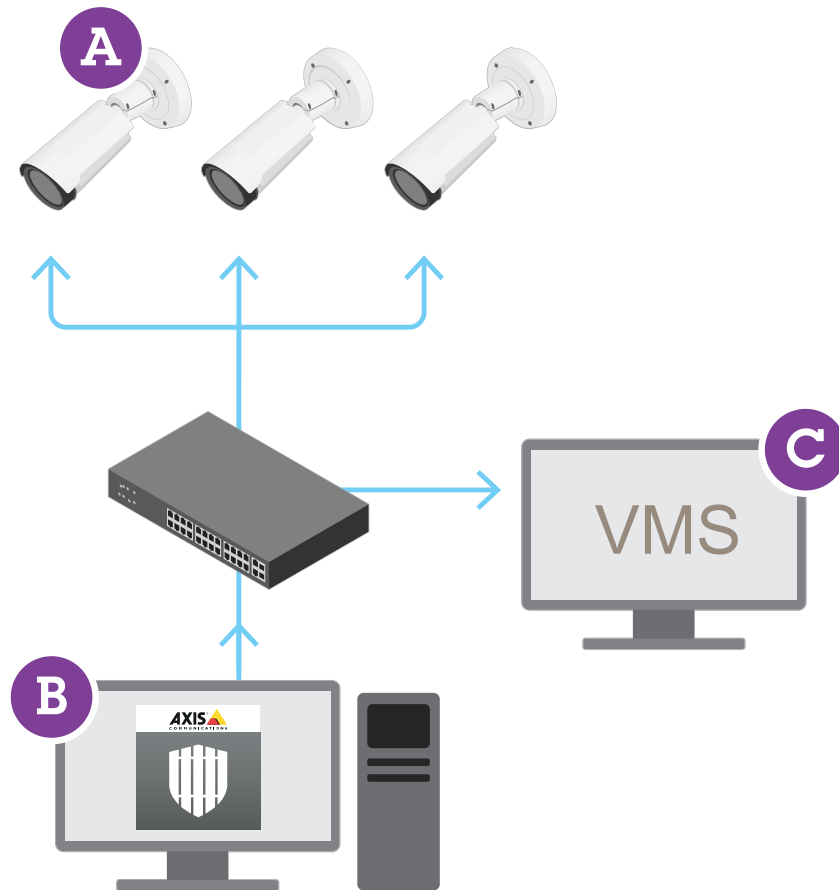
AXIS Q1951-E and AXIS Q1952-E Thermal Cameras can run the application in calibration mode, AI mode, or both modes in combination. If you choose to run it in AI mode only, camera mounting is more flexible and you don't need to calibrate the cameras.

AXIS Perimeter Defender consists of a desktop interface (B), from where you install and set up the application on the cameras (A). You can then configure the system to send alarms to the Video Management Software (C).

AXIS Perimeter Defender PTZ Autotracking is a plugin to the AXIS Perimeter Defender application, using the same desktop interface. With the plugin, you pair a fixed visual or thermal camera with an Axis Q-line PTZ camera. You can then maintain continuous detection coverage of a scene with the fixed camera while the PTZ camera automatically tracks and gives you closer views of detected objects.

Important

      AXIS Perimeter Defender PTZ Autotracking requires calibration of both fixed and PTZ cameras.

AXIS Perimeter Defender offers the following types of detection scenarios:

- **Intrusion**: triggers an alarm when a person or a vehicle enters a zone defined on the ground (from any direction and with any trajectory).

- **Loitering**: triggers an alarm when a person or a vehicle remains in a zone defined on the ground for more than a predefined number of seconds.

- **Zone-crossing**: triggers an alarm when a person or a vehicle passes through two or more zones defined on the ground in a given sequence.

- **Conditional**: triggers an alarm when a person or a vehicle enters a zone defined on the ground without first passing through another zone or zones defined on the ground.

Security

TPM module

The TPM (Trusted Platform Module) is a component that provides cryptographic features to protect information from unauthorized access. It is always activated and there are no settings you can change.

To learn more about TPM, go to *axis.com/press-center/media-resources/white-papers*.

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 27*.

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. The product has been reset to the factory default settings. If no DHCP server is available on the network, the default IP address is 192.168.0.90.

5. Use the installation and management software tools to assign an IP address, set the password, and access the video stream.

    The installation and management software tools are available from the support pages on *axis.com/support*.

It is also possible to reset parameters to factory default through the web interface. Go to **Settings > System > Maintenance** and click **Default**.

Firmware options

Axis offers product firmware 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 firmware 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 product firmware strategy, go to *axis.com/support/firmware*.

Check the current firmware

Firmware is the software that determines the functionality of network devices. One of your first actions when troubleshooting a problem should be to check the current firmware version. The latest version may contain a correction that fixes your particular problem.

To check the current firmware:

1. Go to the product's webpage.

2. Click the help menu ❓ .

3. Click **About**.

Upgrade the firmware

Important

> Preconfigured and customized settings are saved when the firmware is upgraded (provided that the features are available in the new firmware) although this is not guaranteed by Axis Communications AB.

Important

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

Note

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

AXIS Device Manager can be used for multiple upgrades. Find out more at *axis.com/products/axis-device-manager*.

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

www.axis.com/products/online-manual/67055#t10095327

How to upgrade the firmware

1. Download the firmware file to your computer, available free of charge at *axis.com/support/firmware*.

2. Log in to the product as an administrator.

3. Go to **Settings > System > Maintenance**. Follow the instructions on the page. When the upgrade has finished, the product restarts automatically.

Technical issues, clues and solutions

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

Problems upgrading the firmware

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

Problems setting the IP address

The device is located on a different subnet	If the IP address intended for the device and the IP address of the computer used to access the device are located on different subnets, you cannot set the IP address. Contact your network administrator to obtain an IP address.

The IP address is being used by another device	Disconnect the Axis device from the network. Run the ping command (in a Command/DOS window, type `ping` and the IP address of the device):
	• If you receive: `Reply from <IP address>:  bytes=32; time=10...` this means that the IP address may already be in use by another device on the network. Obtain a new IP address from the network administrator and reinstall the device.
	• If you receive: `Request timed out`, this means that the IP address is available for use with the Axis device. Check all cabling and reinstall the device.
Possible IP address conflict with another device on the same subnet	The static IP address in the Axis device is used before the DHCP server sets a dynamic address. This means that if the same default static IP address is also used by another device, there may be problems accessing the device.

The device cannot be accessed from a browser

Cannot log in	When HTTPS is enabled, ensure that the correct protocol (HTTP or HTTPS) is used when attempting to log in. You may need to manually type `http` or `https` in the browser's address field.
	If the password for the user root is lost, the device must be reset to the factory default settings. See *Reset to factory default settings on page 23*.
The IP address has been changed by DHCP	IP addresses obtained from a DHCP server are dynamic and may change. If the IP address has been changed, use AXIS IP Utility or AXIS Device Manager to locate the device on the network. Identify the device using its model or serial number, or by the DNS name (if the name has been configured).
	If required, a static IP address can be assigned manually. For instructions, go to *axis.com/support*.
Certificate error when using IEEE 802.1X	For authentication to work properly, the date and time settings in the Axis device must be synchronized with an NTP server. Go to **Settings > System > Date and time**.

The device is accessible locally but not externally

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

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

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

Problems with streaming

Multicast H.264 only accessible by local clients	Check if your router supports multicasting, or if the router settings between the client and the device need to be configured. The TTL (Time To Live) value may need to be increased.
No multicast H.264 displayed in the client	Check with your network administrator that the multicast addresses used by the Axis device are valid for your network.
	Check with your network administrator to see if there is a firewall preventing viewing.
Poor rendering of H.264 images	Ensure that your graphics card is using the latest driver. The latest drivers can usually be downloaded from the manufacturer's website.
Lower frame rate than expected	• See *Performance considerations on page 26*.
	• Reduce the number of applications running on the client computer.
	• Limit the number of simultaneous viewers.
	• Check with the network administrator that there is enough bandwidth available.
	• Lower the image resolution.
	• The maximum frames per second is dependent on the utility frequency (60/50 Hz) of the Axis device.
Can't select H.265 encoding in live view	Web browsers do not support H.265 decoding. Use a video management system or application supporting H.265 decoding.

Performance considerations

When setting up your system, it is important to consider how various settings and situations affect the performance. Some factors affect the amount of bandwidth (the bitrate) required, others can affect the frame rate, and some affect both. If the load on the CPU reaches its maximum, this also affects the frame rate.

The following factors are the most important to consider:

- High image resolution or lower compression levels result in images containing more data which in turn affects the bandwidth.

- Rotating the image in the GUI will increase the product's CPU load.

- Access by large numbers of Motion JPEG or unicast H.264 clients affects the bandwidth.

- Simultaneous viewing of different streams (resolution, compression) by different clients affects both frame rate and bandwidth.

  Use identical streams wherever possible to maintain a high frame rate. Stream profiles can be used to ensure that streams are identical.

- Accessing Motion JPEG and H.264 video streams simultaneously affects both frame rate and bandwidth.

- Heavy usage of event settings affects the product's CPU load which in turn affects the frame rate.

- Using HTTPS may reduce frame rate, in particular if streaming Motion JPEG.

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

- Viewing on poorly performing client computers lowers perceived performance and affects frame rate.

- Running multiple AXIS Camera Application Platform (ACAP) applications simultaneously may affect the frame rate and the general performance.

- Using palettes affects the product's CPU load which in turn affects the frame rate.
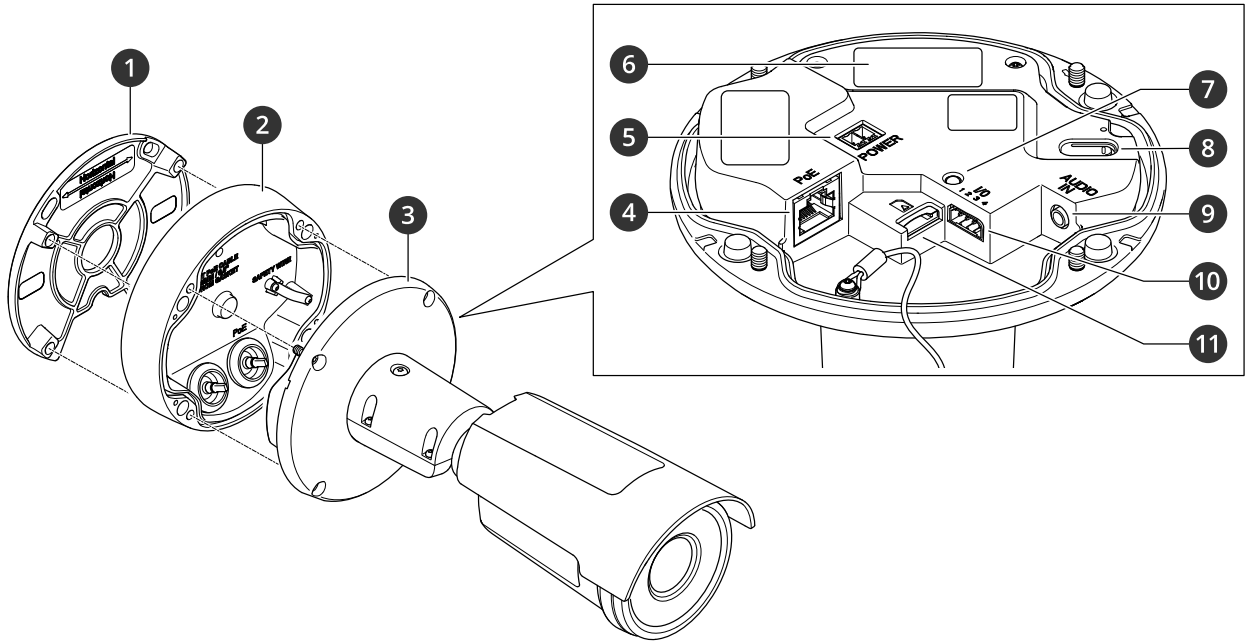
Contact support

Contact support at *axis.com/support*.

Specifications

Specifications

Product overview

1   Mounting bracket
2   Connection lid
3   Camera unit
4   Network connector (PoE)
5   Power connector
6   Part number (P/N) & serial number (S/N)
7   Status LED indicator
8   Control button
9   Audio connector
10   I/O connector
11   SD memory card slot

LED indicators

Status LED	Indication
Unlit	Connection and normal operation.
Green	Connection and normal operation.
Amber	Steady during startup. Flashes during firmware upgrade or reset to factory default.
Amber/Red	Flashes amber/red if network connection is unavailable or lost.
Red	Firmware upgrade failure.

Specifications

SD card slot

NOTICE

- Risk of damage to SD card. Do not use sharp tools, metal objects, or excessive force when inserting or removing the SD card. Use your fingers to insert and remove the card.
- Risk of data loss and corrupted recordings. Do not remove the SD card while the product is running. Unmount the SD card from the product's webpage before removal.

This product 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 23*.
- Connecting to a one-click cloud connection (O3C) service over the internet. To connect, press and hold the button for about 3 seconds until the status LED flashes green.
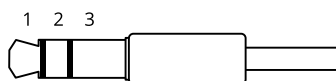
Connectors

Network connector

RJ45 Ethernet connector with Power over Ethernet (PoE).

Audio connector

- **Audio in** – 3.5 mm input for a digital microphone, an analog mono microphone, or a line-in mono signal (left channel is used from a stereo signal).

Audio input

1 Tip	2 Ring	3 Sleeve
Unbalanced microphone (with or without electret power) or line	Electret power if selected	Ground
Digital signal	Ring power if selected	Ground

For audio in, the left channel is used from a stereo signal.

I/O connector

Use the I/O connector with external devices in combination with, for example, motion detection, event triggering, and alarm notifications. In addition to the 0 V DC reference point and power (DC output), the I/O connector provides the interface to:
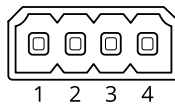
AXIS Q19-E Thermal Camera Series

Specifications

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

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

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

4-pin terminal block

Function	Pin	Notes	Specifications
DC ground	1		0 V DC
DC output	2	Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	12 V DC Max load = 25 mA
Digital Input or Supervised Input	3	Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. To use supervised input, install end-of-line resistors. See connection diagram for information about how to connect the resistors.	0 to max 30 V DC
Digital Output	4	Internally connected to pin 1 (DC ground) when active, and floating (unconnected) when inactive. If used with an inductive load, e.g., a relay, connect a diode in parallel with the load, to protect against voltage transients.	0 to max 30 V DC, open drain, 100 mA

Example
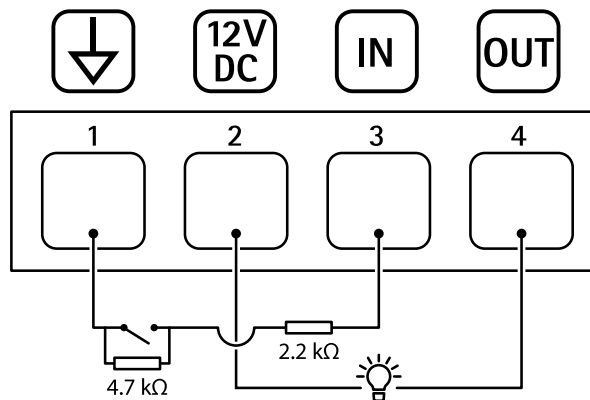
1   DC ground
2   DC output 12 V, max 25 mA
3   Supervised input
4   Digital output

Power connector

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

29

Specifications