

AXIS F9111 Main Unit

Table of Contents

Get started..... 4

 Connect sensor units 4

 Shorten the sensor unit cable 4

 Find the device on the network..... 4

 Browser support 4

 Access the device 4

 Verify that no one has tampered with the firmware..... 5

 Set a new password for the root account 5

 Secure passwords 5

 Web interface overview 5

Installation 7

 Preview mode 7

Configure your device..... 8

 Adjust the image..... 8

 Level the camera 8

 Reduce image processing time with low latency mode..... 8

 Select exposure mode 8

 Reduce noise in low-light conditions 8

 Reduce motion blur in low-light conditions..... 9

 Handle scenes with strong backlight..... 9

 Monitor long and narrow areas 9

 Hide parts of the image with privacy masks..... 10

 Show an image overlay 10

 View and record video 10

 Reduce bandwidth and storage 10

 Set up network storage 11

 Record and watch video 11

 Set up rules for events 11

 Trigger an action 12

 Record video when the camera detects an object..... 12

 Show a text overlay in the video stream when the device detects an object 12

 Record video when the camera detects loud noises 13

 Set up the intrusion alarm 13

 Trigger a notification when the camera lens is tampered 14

 Audio..... 14

 Add audio to your recording 14

The web interface 16

Learn more..... 17

 Capture modes..... 17

 Privacy masks 17

 Streaming and storage..... 17

 Video compression formats..... 17

 How do Image, Stream, and Stream profile settings relate to each other?..... 18

 Bitrate control..... 18

 Analytics and apps 18

 AXIS Object Analytics..... 19

 Metadata visualization..... 19

 Cybersecurity..... 19

 TPM module..... 19

 Delayed shutdown..... 19

Specifications..... 20

 Product overview 20

 20

LED indicators.....	20
SD card slot.....	20
Buttons.....	21
Control button	21
Connectors.....	21
Network connector.....	21
Audio connector.....	21
I/O connector.....	21
Power connector	22
RS232/RS485 connector.....	24
FAKRA connector.....	24
Troubleshooting.....	25
Reset to factory default settings.....	25
AXIS OS options.....	25
Check the current firmware.....	25
Upgrade the firmware.....	25
Technical issues, clues and solutions	26
Performance considerations	28
Contact support.....	28
Cybersecurity	29
Vulnerability management	29
Security notifications.....	29
Secure product lifecycle.....	29

Get started

Connect sensor units

When you connect a sensor unit to a main unit, we recommend that you make the connection before you power up the main unit. If you disconnect a sensor unit and connect a different one, you must restart the main unit.

Shorten the sensor unit cable

Note

- Incorrect shortening of the cable can lead to image degradation or image loss.
- Check that you have the correct FAKRA connector before cutting the cable.

To shorten the cable follow these steps:

1. Cut the cable to the desired length. Measure from the sensor unit.
2. Strip the plastic outer coating from the end of the cable.
3. Put the small insulator sleeve on the inner conductor of the cable and weld or crimp the center pin on the inner wire of the cable.
4. Put the heat-shrinkable tube and copper tube on the cable.
5. Insert the cable into the connector.
6. Push the copper tube onto the connector and then Hex. Use a crimping tool to fasten the copper tube on the connector.
7. Heat the heat-shrinkable tube.

For more information, see the Connector Kit FAKRA Installation Guide.

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

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 5*.
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 25*. 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 25*



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

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

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

To protect your data we strongly recommend that you:

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

Web interface overview

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



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

Axis device web interface

Installation

Preview mode

Preview mode is ideal for installers when fine tuning the camera view during the installation. No login is required to access the camera view in preview mode. It is available only in factory defaulted state for a limited time from powering up the device.



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

This video demonstrates how to use preview mode.



Configure your device

Adjust the image

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

Level the camera

To adjust the view in relation to a reference area or an object, use the level grid in combination with a mechanical adjustment of the camera.

1. Go to **Video > Image >** and click .
2. Click  to show the level grid.
3. Adjust the camera mechanically until the position of the reference area or the object is aligned with the level grid.

Reduce image processing time with low latency mode

You can optimize the image processing time of your live stream by turning on low latency mode. The latency in your live stream is reduced to a minimum. When you use low latency mode, the image quality is lower than usual.

1. Go to **System > Plain config**.
2. Select **ImageSource** from the drop-down list.
3. Go to **ImageSource/I0/Sensor > Low latency mode** and select **On**.
4. Click **Save**.

Select exposure mode

To improve image quality for specific surveillance scenes, use exposure modes. Exposure modes lets you control aperture, shutter speed, and gain. Go to **Video > Image > Exposure** and select between the following exposure modes:

- For most use cases, select **Automatic** exposure.
- For environments with certain artificial lighting, for example fluorescent lighting, select **Flicker-free**. Select the same frequency as the power line frequency.
- For environments with certain artificial light and bright light, for example outdoors with fluorescent lighting at night and sun during daytime, select **Flicker-reduced**. Select the same frequency as the power line frequency.
- To lock the current exposure settings, select **Hold current**.

Reduce noise in low-light conditions

To reduce noise in low-light conditions, you can adjust one or more of the following settings:

- Adjust the trade-off between noise and motion blur. Go to **Video > Image > Exposure** and move the **Blur-noise trade-off** slider toward **Low noise**.
- Set the exposure mode to automatic.

Note

A high max shutter value can result in motion blur.

- To slow down the shutter speed, set max shutter to the highest possible value.
- If there is an **Aperture** slider, move it towards **Open**.

Reduce motion blur in low-light conditions

To reduce motion blur in low-light conditions, adjust one or more of the following settings in **Video > Image > Exposure**:

Note

When you increase the gain, image noise also increases.

- Set **Max shutter** to a shorter time, and **Max gain** to a higher value.

If you still have problems with motion blur:

- Increase the light level in the scene.
- Mount the camera so that objects move toward it or away from it rather than sideways.

Handle scenes with strong backlight

Dynamic range is the difference in light levels in an image. In some cases the difference between the darkest and the brightest areas can be significant. The result is often an image where either the dark or the bright areas are visible. Wide dynamic range (WDR) makes both dark and bright areas of the image visible.



Image without WDR.



Image with WDR.

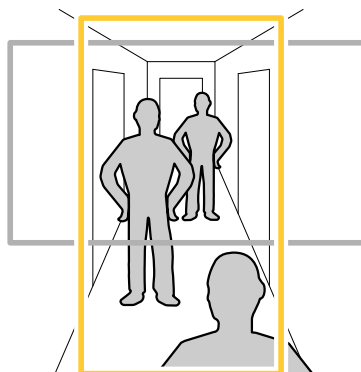
Note

- WDR can cause artifacts in the image.
 - WDR may not be available for all capture modes.
1. Go to **Video > Image > Wide dynamic range**.
 2. Turn on WDR.
 3. Use the **Local contrast** slider to adjust the amount of WDR.
 4. If you still have problems, go to **Exposure** and adjust the **Exposure zone** to cover the area of interest.

Find out more about WDR and how to use it at axis.com/web-articles/wdr.

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, go to **Video > Installation**.
3. Rotate the view 90° or 270°.

Hide parts of the image with privacy masks

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

1. Go to **Video > Privacy masks**.
2. Click **+**.
3. Click the new mask and type a name.
4. Adjust the size and placement of the privacy mask according to your needs.
5. To change the color for all privacy masks, click **Privacy masks** and select a color.

See also *Privacy masks, on page 17*

Show an image overlay

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

1. Go to **Video > 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 17*.

Reduce bandwidth and storage

Important

Reducing the bandwidth can lead to loss of detail in the image.

1. Go to **Video > Stream**.
2. Click  in the live view.

3. Select **Video format AV1** if your device supports it. Otherwise select **H.264**.
4. Go to **Video > Stream > General** and increase **Compression**.
5. Go to **Video > Stream > Zipstream** and do one or more of the following:

Note

The **Zipstream** settings are used for all video encodings except MJPEG.


- Select the Zipstream **Strength** that you want to use.
- Turn on **Optimize for storage**. This can only be used if the video management software supports B-frames.
- Turn on **Dynamic FPS**.
- Turn on **Dynamic GOP** and set a high **Upper limit GOP length** value.

Note

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


Set up network storage

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

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

Record and watch video


Record video directly from the camera

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

If you haven't set up any storage, click  and . For instructions on how to set up network storage, see *Set up network storage, on page 11*

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.

Record video when the camera detects an object

This example explains how to set up the camera to start recording to the SD card when the camera detects an object. The recording will include five seconds before detection and one minute after detection ends.

Before you start:

- Make sure you have an SD card installed.
1. Start the application if it is not already running.
 2. Make sure you have set up the application according to your needs.

Create a rule:



1. Go to **System > Events** and add a rule.
2. Type a name for the rule.
3. In the list of actions, under **Recordings**, select **Record video while the rule is active**.
4. In the list of storage options, select **SD_DISK**.
5. Select a camera and a stream profile.
6. Set the prebuffer time to 5 seconds.
7. Set the postbuffer time to 1 minute.
8. Click **Save**.

Show a text overlay in the video stream when the device detects an object

This example explains how to display the text "Motion detected" when the device detects an object.

1. Start the application if it is not already running.
2. Make sure you have set up the application according to your needs.

Add the overlay text:

1. Go to **Video > Overlays**.
2. Under **Overlays**, select **Text** and click  .
3. Enter #D in the text field.
4. Choose text size and appearance.
5. To position the text overlay, click  and select an option.

Create a rule:

1. Go to **System > Events** and add a rule.
2. Type a name for the rule.
3. In the list of actions, under **Overlay text**, select **Use overlay text**.
4. Select a video channel.
5. In **Text**, type "Motion detected".

6. Set the duration.
7. Click **Save**.

Note

If you update the overlay text it will be automatically updated on all video streams dynamically.

Record video when the camera detects loud noises

This example explains how to set up the camera to start recording to the SD card five seconds before it detects loud noise and to stop two minutes after.

Note

The following instructions require that a microphone is connected to audio-in.

Turn on audio:

1. Set up the stream profile to include audio, see *Add audio to your recording, on page 14*.

Turn on audio detection:

1. Go to **System > Detectors > Audio detection**.
2. Adjust the sound level according to your needs.

Create a rule:

1. Go to **System > Events** and add a rule.
2. Type a name for the rule.
3. In the list of conditions, under **Audio**, select **Audio Detection**.
4. In the list of actions, under **Recordings**, select **Record video**.
5. In the list of storage options, select **SD_DISK**.
6. Select the stream profile where audio has been turned on.
7. Set the prebuffer time to 5 seconds.
8. Set the postbuffer time to 2 minutes.
9. Click **Save**.

Set up the intrusion alarm

Before you start

- Connect the intrusion alarm switch to pin 1 (ground) and pin 3 (digital I/O) of the camera's I/O connector.

Configure the input port:


1. Go to **System > Accessories > I/O ports**.
2. For **Port 1**:
 - 2.1. Select **Input**.
 - 2.2. Select **Circuit closed**.

Add an email recipient:

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

9. To test your email setup, click **Test**.
10. Click **Save**.

Create a rule:

11. Go to **System > Events > Rules** and add a rule.
12. Type a name for the rule.
13. In the list of conditions, under **I/O**, select **Digital input**.
14. In the list of ports, select **Port 1**.
15. In the list of actions, under **Notifications**, select **Send notification to email**.
16. 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 .
17. Type a subject line and message for the email.
18. Click **Save**.

Trigger a notification when the camera lens is tampered

This example explains how to set up an email notification when the camera lens gets either spray painted, covered, or blurred.

Activate the tampering detection:

1. Go to **System > Detectors > Camera tampering**.
2. Set a value for **Trigger delay**. The value indicates the time that must pass before an email is sent.
3. Turn on **Trigger on dark images** to detect if the lens is sprayed, covered, or rendered severely out of focus.

Add an email recipient:

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

Create a rule:

12. Go to **System > Events > Rules** and add a rule.
13. Type a name for the rule.
14. In the list of conditions, under **Video**, select **Tampering**.
15. In the list of actions, under **Notifications**, select **Send notification to email** and then select the recipient from the list.
16. Type a subject line and message for the email.
17. Click **Save**.

Audio

Add audio to your recording

Turn on audio:

1. Go to **Video > Stream > Audio** and include audio.
2. If the device has more than one input source, select the correct one in **Source**.
3. Go to **Audio > Device settings** and turn on the correct input source.

Edit the stream profile that is used for the recording:

4. Go to **System > Stream profiles** and select the stream profile.
5. Select **Include audio** and turn it on.
6. Click **Save**.

The web interface

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

Learn more

Capture modes

Which capture mode to choose depends on the requirements of frame rate and resolution for the specific surveillance setup. For specifications about available capture modes, see the product's datasheet at axis.com.

Privacy masks

A privacy mask is a user-defined area that covers a part of the monitored area. In the video stream, privacy masks appear either as blocks of solid color or with a mosaic pattern.

You'll see the privacy mask on all snapshots, recorded video, and live streams.

You can use the VAPIX® application programming interface (API) to hide the privacy masks.

Important

If you use multiple privacy masks it may affect the product's performance.

You can create several privacy masks. Each mask can have 3 to 10 anchor points.

Streaming and storage

Video compression formats

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

Motion JPEG

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

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

H.264 or MPEG-4 Part 10/AVC

Note

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

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

H.265 or MPEG-H Part 2/HEVC

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

Note

- H.265 is licensed technology. The Axis product includes one H.265 viewing client license. Installing additional unlicensed copies of the client is prohibited. To purchase additional licenses, contact your Axis reseller.
- Most web browsers don't support H.265 decoding and because of this the camera doesn't support it in its web interface. Instead you can use a video management system or application supporting H.265 decoding.

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.

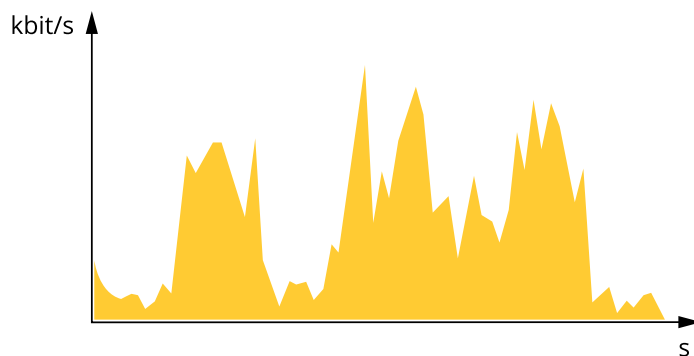
The **Stream profiles** settings override the settings from the **Stream** tab. If you request a stream with a specific stream profile, the stream contains the settings of that profile. If you request a stream without specifying a stream profile, or request a stream profile that doesn't exist in the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

Bitrate control

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

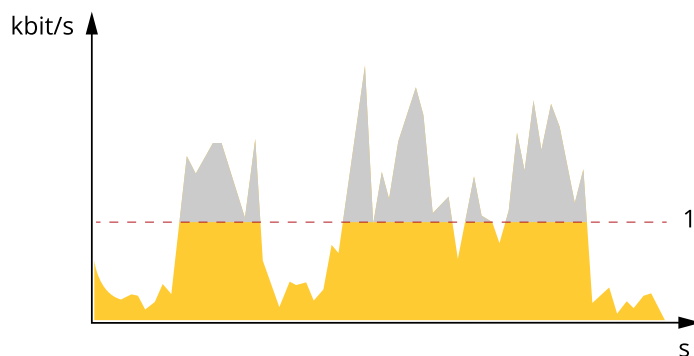
Variable bitrate (VBR)

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

Analytics and apps

With analytics and apps you can get more out of your Axis device. AXIS Camera Application Platform (ACAP) is an open platform that makes it possible for third parties to develop analytics and other apps for Axis devices. Apps can be preinstalled on the device, available for download for free, or for a license fee.

To find the user manuals for Axis analytics and apps, go to *help.axis.com*.

AXIS Object Analytics

AXIS Object Analytics is an analytic application that comes preinstalled on the camera. It detects objects that move in the scene and classifies them as, for example, humans or vehicles. You can set up the application to send alarms for different types of objects. To find out more about how the application works, see *AXIS Object Analytics user manual*.

Metadata visualization

Analytics metadata is available for moving objects in the scene. Supported object classes are visualized in the video stream through a bounding box surrounding the object, along with information about the object type and confidence level of the classification. To learn more about how to configure and consume analytics metadata, see *AXIS Scene Metadata integration guide*.

Cybersecurity

For product-specific information about cybersecurity, see the product's datasheet at axis.com.

For in-depth information about cybersecurity in AXIS OS, read the *AXIS OS Hardening guide*.

TPM module

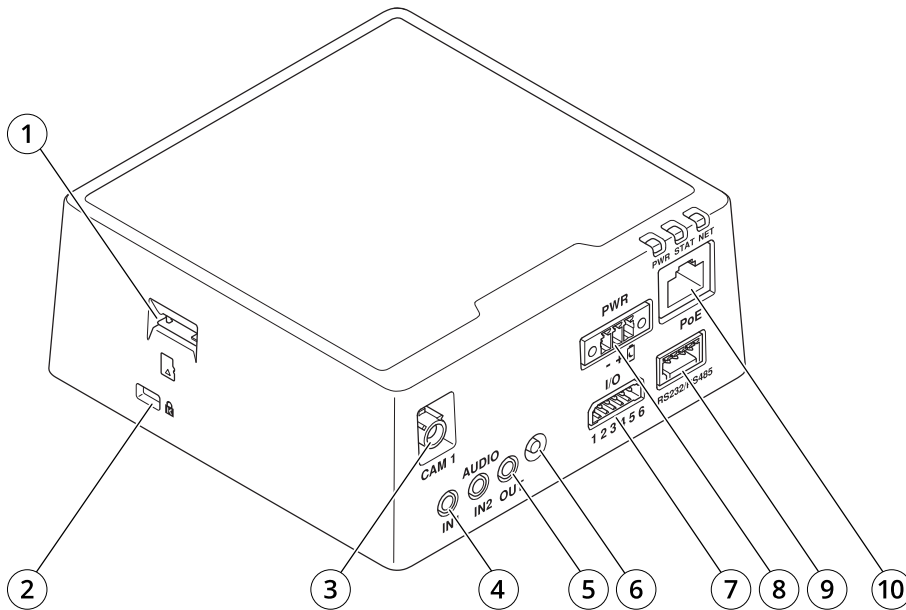
The TPM (Trusted Platform Module) is a component that provides cryptographic features to protect information from unauthorized access. It is always activated and there are no settings you can change.

Delayed shutdown

With **Delayed shutdown** you can turn off the device after a set delay time and reduce the power consumption when not in use. This feature is useful for devices installed in vehicles and connected to the vehicle battery. When the ignition is on, the device starts. When the ignition is off, the device is powered by the battery and turns off after a set delay time.

Specifications

Product overview



- 1 MicroSD card slot
- 2 Kensington lock
- 3 FAKRA connector
- 4 2x Audio in
- 5 Audio out
- 6 Control button
- 7 I/O connector
- 8 Power connector
- 9 RS232/RS485 connector
- 10 Network connector (PoE)

LED indicators

Status LED	Indication
Unlit	Connection and normal operation.
Green	Shows steady green for 10 seconds for normal operation after startup completed.
Amber	Steady during startup. Flashes during device software upgrade or reset to factory default.
Amber/Red	Flashes amber/red if network connection is unavailable or lost.


SD card slot

NOTICE

- Risk of damage to SD card. Don't 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. Unmount the SD card from the device's web interface before removing it. Don't remove the SD card while the product is running.

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 25*.

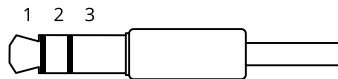
Connectors

Network connector

RJ45 Ethernet connector with Power over Ethernet (PoE).

Audio connector

- Audio in – 3.5 mm input for a mono microphone, or a line-in mono signal (left channel is used from a stereo signal).
- 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-in	Electret power if selected	Ground
Digital signal	Ring power if selected	Ground

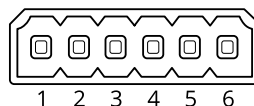
I/O connector


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 VDC reference point and power (12 V DC output), the I/O connector provides the interface to:

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

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

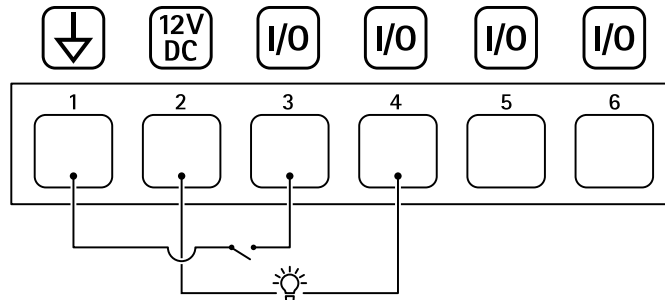
6-pin terminal block



Function	Pin	Notes	Specifications
DC ground	1		0 VDC
DC output	2		12 VDC Max load = 50 mA

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

Example:

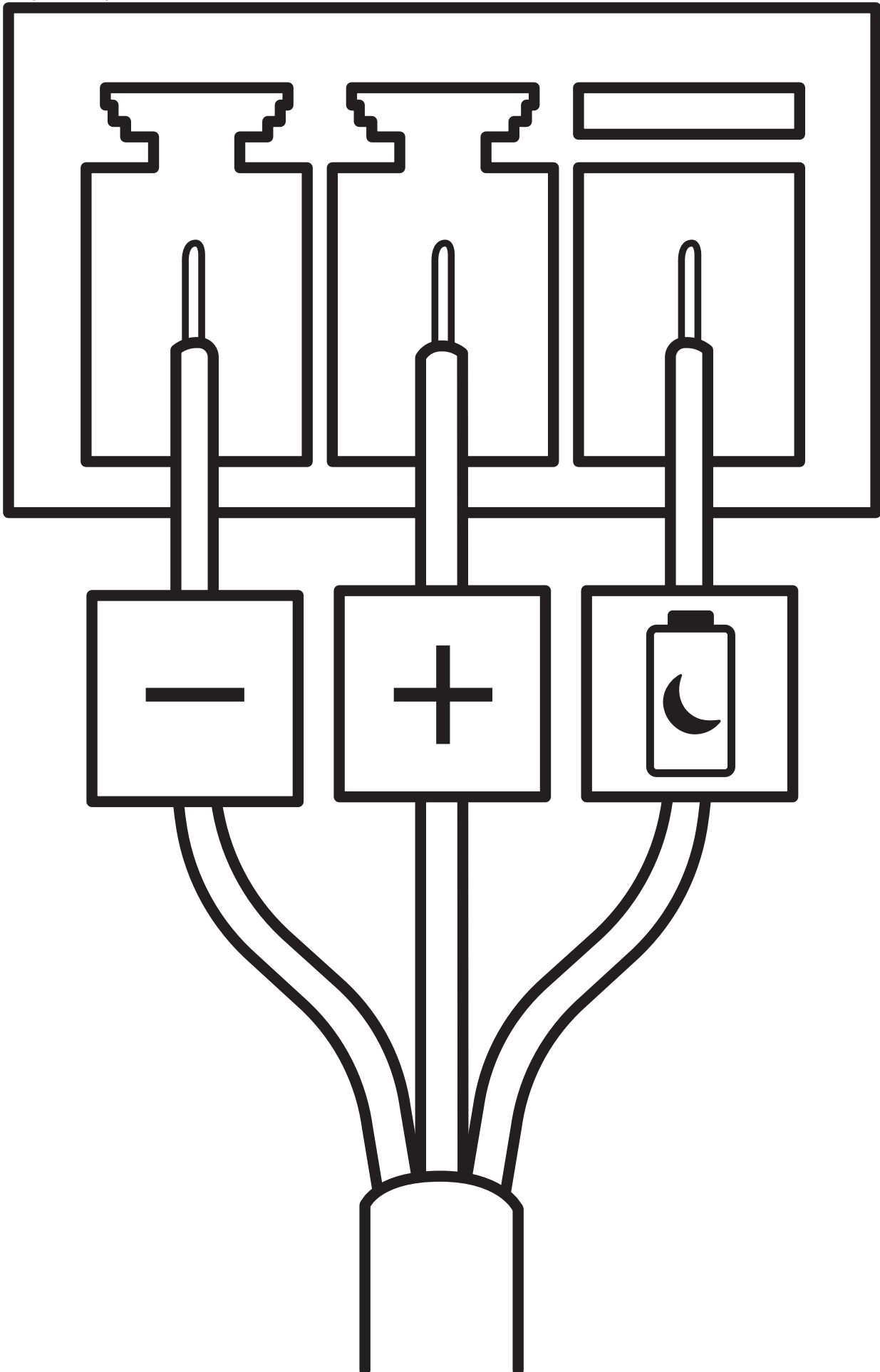


- 1 DC ground
- 2 DC output 12 V, max 50 mA
- 3 I/O configured as input
- 4 I/O configured as output
- 5 Configurable I/O
- 6 Configurable I/O

Power connector

3-pin terminal block for 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.

DC power input:



Delayed shutdown

Important

To avoid unwanted shutdown, only turn on **Delayed shutdown** when the ignition is physically connected to the main unit.

Note

If the device has been without power before it is turned on, a delay occurs before **Delayed shutdown** is activated.

1. Connect to ignition control on the 3-pin terminal block.
2. Go to the device's web interface.
3. Go to **System > Power settings** and turn on **Delayed shutdown**.
4. Set a delay time between 1 and 60 minutes.

RS232/RS485 connector

5-pin terminal block for the RS232/RS485 serial interface used to control auxiliary equipment. In order to use the RS232/RS485 port you need a third-party application for AXIS Camera Application Platform. The port can be used in the following modes:

- 2TX/2RX RS232 interface (TXD, RTS, GND, CTS, RXD)
- Bidirectional RS485 half-duplex port for data transmission using two wires, one combined RX/TX pair.
- Bidirectional RS485 full-duplex port for data transmission using four wires, one RX pair and one TX pair.

Function	Pin	Notes
RS232 TXD alt RS485 TX-	1	RS232 driver output 4-wire RS485 (combined RX/TX pair for 2-wire RS485)
RS232 RTS alt RS485 TX+	2	
RS232 GND alt RS485 GND	3	Ground
RS232 CTS alt RS485 RX-	4	RS232 receiver input 4-wire RS485 (not used for 2-wire RS485)
RS232 RXD alt RS485 RX+	5	

FAKRA connector

The FAKRA connector is used for connecting the sensor unit to the main unit.

For information on how to shorten the sensor unit cable see *Shorten the sensor unit cable, on page 4*.

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 20*.
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**.

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 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.



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 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	<p>Disconnect the Axis device from the network. Run the ping command (in a Command/DOS window, type <code>ping</code> and the IP address of the device):</p> <ul style="list-style-type: none"> • If you receive: <code>Reply from <IP address>: bytes=32; time=10...</code> 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: <code>Request timed out</code>, 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	<p>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 <code>http</code> or <code>https</code> in the browser's address field.</p> <p>If the password for the user root is lost, the device must be reset to the factory default settings. See <i>Reset to factory default settings, on page 25</i>.</p>
The IP address has been changed by DHCP	<p>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).</p> <p>If required, a static IP address can be assigned manually. For instructions, go to axis.com/support.</p>

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	<p>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.</p>
No multicast H.264 displayed in the client	<p>Check with your network administrator that the multicast addresses used by the Axis device are valid for your network.</p> <p>Check with your network administrator to see if there is a firewall preventing viewing.</p>
Poor rendering of H.264 images	<p>Ensure that your graphics card is using the latest driver. The latest drivers can usually be downloaded from the manufacturer's website.</p>
Color saturation is different in H.264 and Motion JPEG	<p>Modify the settings for your graphics adapter. Go to the adapter's documentation for more information.</p>
Lower frame rate than expected	<ul style="list-style-type: none"> • See <i>Performance considerations, on page 28</i>. • 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.
Can't select H.265 encoding in live view	<p>Web browsers do not support H.265 decoding. Use a video management system or application supporting H.265 decoding.</p>

Problems with the image

Image degradation or image loss

- Check the device's 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 performance. Some factors affect bandwidth (bitrate), others affect frame rate, and some affect both.

The most important factors 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 can increase the product's CPU load.
- Access by large numbers of Motion JPEG clients or unicast H.264/H.265/AV1 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 video streams with different codecs simultaneously affects both frame rate and bandwidth. For optimal performance, use streams with the same codec.
- 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.

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.

T10168519

2026-07 (M16.3)

© 2021 – 2026 Axis Communications AB