AXIS Q1715 Block Camera

User Manual

AXIS Q1715 Block Camera

Table of Contents

Installation 3
Get started 4
- Find the device on the network 4
- Open the device's webpage 4
- Webpage overview 5

Configure your device 6
- Adjust the image 6
- Adjust the camera view (PTZ) 10
- View and record video 11
- Set up rules for events 12
- Audio 17

Cleaning recommendations 19
Learn more 20
- Capture modes 20
- Privacy masks 20
- Overlays 20
- Pan, tilt, and zoom (PTZ) 20
- Streaming and storage 21
- Applications 23
- Security 24

Troubleshooting 25
- Reset to factory default settings 25
- Firmware options 25
- Check the current firmware version 25
- Upgrade the firmware 25
- Technical issues, clues, and solutions 26
- Performance considerations 27
- Contact support 28

Specifications 29
- Product overview 29
- LED indicators 29
- SD card slot 30
- Buttons 30
- Connectors 30

PTZ drivers 33
- APTP 33
- Pelco 33
- Visca 35

Installation

Installation video for the product.

Get started

Find the device on the network

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

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

Browser support

You can use the device with the following browsers:

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

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

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

Open the device's webpage

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*.

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

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

1. Type a password. Follow the instructions about secure passwords. See *Secure passwords on page 5*.
2. Retype the password to confirm the spelling.
3. Click **Add user**.

Important

If you lose the password for the root account, go to *Reset to factory default settings on page 25* and follow the instructions.

Secure passwords

Important

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

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

To protect your data we strongly recommend that you:

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

Webpage overview

This video gives you an overview of the device interface.

Axis device web interface

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 20*.

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.

Adjust the focus

This product has three focus modes:

- **Auto**: The camera automatically adjusts focus based on the entire image.
- **Area**: The camera automatically adjusts focus based on a selected area of the image.
- **Manual**: The focus is set manually at a fixed distance.

To turn off autofocus and adjust the focus manually:

1. In the live view window, if the **Zoom** slider is visible, click **Zoom** and select **Focus**.
2. Click **M** and use the slider to set the focus.

Select scene profile

A scene profile is a set of predefined image appearance settings including color level, brightness, sharpness, contrast and local contrast. Scene profiles are preconfigured in the product for quick setup to a specific scenario, for example **Forensic** which is optimized for surveillance conditions. For a description of each available setting, see .

You can select a scene profile during the initial setup of the camera. You can also select or change scene profile later.

1. Go to **Video > Image > Appearance**.
2. Go to **Scene profile** and select a profile.

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.

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

Configure your device

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.

Note

When you reduce the max gain, the image can become darker.

- Set the max gain to a lower value.
- If possible, open the aperture.

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.

Configure your device

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. Use the **Tone mapping** slider to adjust the amount of WDR.
5. 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*.

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.

EIS makes the image smoother, steadier and less blurry. It also reduces the file size of the compressed image and lowers the bitrate of the video stream.

Note

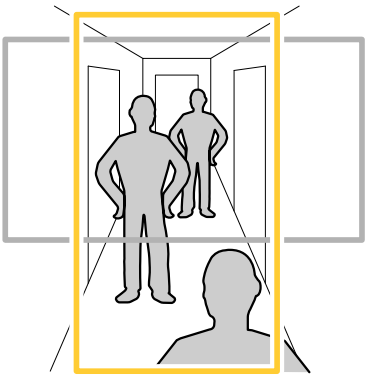
The image is cropped slightly when EIS is enabled, lowering the maximum resolution.

1. Go to **Video > Installation > Image correction**.
2. Turn on **Electronic image stabilization (EIS)**.

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.

Configure your device

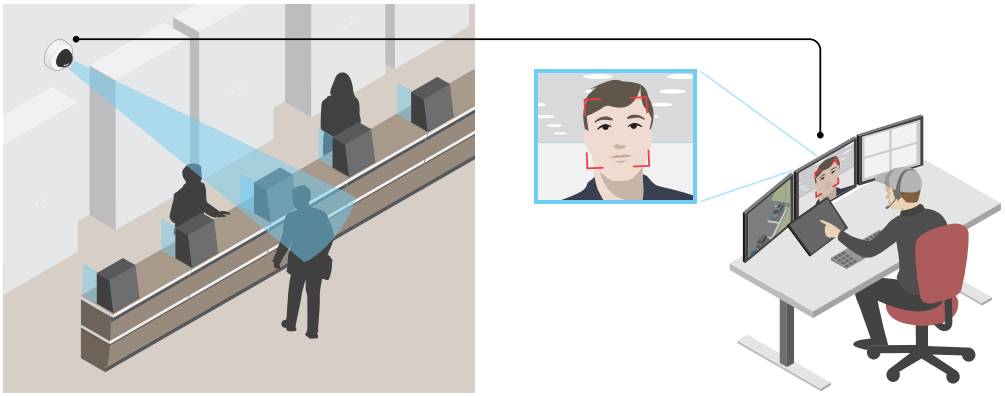


1. Depending on your device, turn the camera or the 3-axis lens in the camera 90° or 270°.
2. If the device doesn't have automatic rotation of the view, go to **Video > Installation**.
3. Rotate the view 90° or 270°.

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

Verify the pixel resolution

To verify that a defined part of the image contains enough pixels to, for example, recognize the face of a person, you can use the pixel counter.



1. Go to **Video > Image** and click .
2. Click for **Pixel counter**.
3. In the camera's live view, adjust the size and position of the rectangle around the area of interest, for example where you expect faces to appear.

   You can see the number of pixels for each of the rectangle's sides, and decide if the values are enough for your needs.

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, expand **Privacy masks** and select a color.

See also *Privacy masks on page 20*

Show an image overlay

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

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

Adjust the camera view (PTZ)

To learn more about different pan, tilt, and zoom settings, see *Pan, tilt, and zoom (PTZ) on page 20*.

Limit the zoom movements

If there are parts of the scene that you don't want the camera to be able to zoom in on, you can limit the maximum zoom level. For example, you want to protect the privacy of residents in an apartment building, which is located close to a parking lot that you intend to monitor.

To limit the maximum zoom level:

1. Click ⋮ and select **Legacy device interface**.
2. Go to **Settings > PTZ > Limits** and set the limits as needed.

Create a guard tour with preset positions

A guard tour displays the video stream from different preset positions either in a predetermined or random order, and for configurable periods of time.

1. Go to **PTZ > legacy device interface**.
2. In the legacy device interface, go to **PTZ > Guard tours**.
3. Click **+**.
4. To edit the guard tour's properties, click ⚙ .

5. Type a name for the guard tour and specify the pause length in minutes between each tour.
6. If you want the guard tour to go to the preset positions in a random order, turn on **Shuffle**.
7. Click **Done**.
8. Click **Add** to add the preset positions that you want in your guard tour.
9. Click **Done** to exit the guard tour settings.
10. To schedule the guard tour, go to **System > Events**.

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 21*.

Reduce bandwidth and storage

Important

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

1. Go to **Video > Stream**.
2. Click  in the live view.
3. Select **Video format H.264**.
4. Go to **Video > Stream > General** and increase **Compression**.
5. Go to **Video > Stream > H.264 and H.265 encoding** and do one or more of the following:
   - Select the **Zipstream** level that you want to use.

   Note

   The **Zipstream** settings are used for both H.264 and H.265.

   - 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 even if connection fails** if you experience temporary connection issues, or if the share is not yet configured.
8. Click **Add**.

Record and watch video

Record video directly from the camera

1. Go to **Video > Image**.
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, check out our guide *Get started with rules for events*.

Trigger an action

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

Note

If you make changes to an active rule, the rule must be turned on again for the changes to take effect.

Record video when the camera detects an object

This example explains how to set up the camera to start recording to the SD card five seconds before it detects an object and to stop one minute after.

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**.

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 17*.

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**.

Zoom in on a specific area automatically with gatekeeper

This example explains how to use the gatekeeper functionality to make the camera zoom in automatically on the license plate of a car that passes through a gate. When the car has passed, the camera zooms out to the home position.

Create the preset positions:

1. Go to **PTZ > Preset positions**.
2. Create the home position that includes the entrance of the gate.
3. Create the zoomed-in preset position so that it covers the area in the image where you assume that the license plate will appear.

Create a rule:

1. Go to **System > Events** and add a rule.
2. Name the rule "Gatekeeper".
3. In the list of actions, under **Preset positions**, select **Go to preset position**.
4. Select a **Video channel**.
5. Select the **Preset position**.
6. To make the camera wait a while before it returns to the home position, select **Home timeout**, and set a time.
7. Click **Save**.

Record video when the camera detects impact

Shock detection allows the camera to detect tampering caused by vibrations or shock. Vibrations due to the environment or to an object can trigger an action depending on the shock sensitivity range, which can be set from 0 to 100. In this scenario, someone is throwing rocks at the camera after hours and you would like to get a video clip of the event.

Turn on shock detection:

1. Go to **System > Detectors > Shock detection**.
2. Turn on shock detection, and set a value for the shock sensitivity.

Create a rule:

3. Go to **System > Events > Rules** and add a rule.
4. Type a name for the rule.
5. In the list of conditions, under **Device status**, select **Shock detected**.
6. Click **+** to add a second condition.
7. In the list of conditions, under **Scheduled and recurring**, select **Scheduled event**.
8. In the list of schedules, select **After hours** .
9. In the list of actions, under **Recordings**, select **Record video while the rule is active**.
10. Select where to save the recordings.
11. Select a **Camera**.
12. Set the prebuffer time to 5 seconds.
13. Set the postbuffer time to 60 seconds.
14. 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 a recipient:

3. Go to **System > Events > Recipients** and click **Add recipient**.
4. Type a name for the recipient.
5. Select **Email**.
6. Type an email address to send the email to.
7. The camera doesn't have it's own email server, so it will need to log into another email server to be able to send mails. Fill in the rest of the information according to your email provider.
8. To send a test email, click **Test**.
9. Click **Save**.

Create a rule

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

Detect tampering with input signal

This example explains how to send an email when the input signal is cut or short-circuited. For more information about the I/O connector, see *page 31*.

1. Go to **System > Accessories** and turn on **Supervised** for the relevant port.

Add an email recipient:

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

Create a rule:

1. Go to **System > Events > Rules** and add a rule.
2. Type a name for the rule.
3. In the list of conditions, under **I/O**, select **Supervised input tampering is active**.
4. Select the relevant port.
5. In the list of actions, under **Notifications**, select **Send notification to email** and then select the recipient from the list.
6. Type a subject and a message for the email.
7. Click **Save**.

Send an email automatically if someone spray paints the lens

Activate the tampering detection:

1. Go to **System > Detectors > Camera tampering**.

2. Set a duration for **Trigger after**. 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**.
7. Type an email address to send the email to.
8. The camera doesn't have it's own email server, so it has to log into another email server to send mails. Fill in the rest of the information according to your email provider.
9. To send a test email, 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 **Video**, select **Tampering**.
14. In the list of actions, under **Notifications**, select **Send notification to email** and then select the recipient from the list.
15. Type a subject and a message for the email.
16. Click **Save**.

Audio

Add audio to your recording

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.
4. If you make any changes to the input source, click **Apply changes**.
5. Edit the stream profile that is used for the recording:
   5.1 Go to **System > Stream profiles** and select the stream profile.
   5.2 Select **Include audio** and turn it on.
   5.3 Click **Save**.

Connect to a network speaker

Network speaker pairing allows you to use a compatible Axis network speaker as if it is connected directly to the camera. Once paired, the speaker acts as an audio out device where you can play audio clips and transmit sound through the camera.

Important

For this feature to work with a video management software (VMS), you must first pair the camera with the network speaker, then add the camera to your VMS.

Configure your device

Pair camera with network speaker

1. Go to **System > Accessories > Network speaker pairing**.
2. Type the network speaker's IP address, username and password.
3. Click **Connect**. A confirmation message appears.

Cleaning recommendations

Cleaning recommendations

NOTICE

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

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

Note

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

Learn more

Capture modes

What capture mode to choose depends on the requirements for the frame rate and resolution of 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. The maximum number of masks depends on the complexity of all the masks combined. The more anchor points in each mask, the fewer masks you can create. Each mask can have 3 to 10 anchor points.

Note

If you view the video stream over HDMI and restart the product, the privacy masks will disappear. To show the privacy masks again, restart the video stream.

Overlays

Note

Image and text overlay will not be displayed on video stream over HDMI.

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.

Pan, tilt, and zoom (PTZ)

Preset positions

A preset position is a saved view that can be used to quickly move the camera view to a specific position.

A preset position can consist of the following values:

- Zoom position
- Focus position (manual or automatic)
- Iris position (manual or automatic)

The preset positions can be reached at any time:

- from the drop-down list in the live view window
- as actions in the event system
- as triggers in the event system
- when setting up a guard tour

Guard tours

A guard tour displays the video stream from different preset positions either in a predetermined or random order, and for configurable periods of time. Once started, a guard tour continues to run until stopped, even when there are no clients (web browsers) viewing the images.

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.

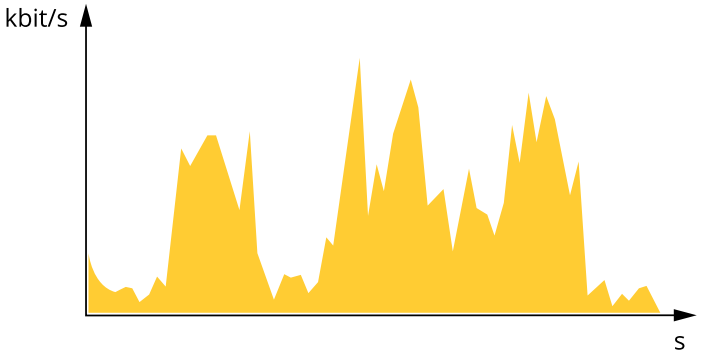
The **Stream profiles** settings override the settings from the **Stream** tab. If you request a stream with a specific stream profile, the stream contains the settings of that profile. If you request a stream without specifying a stream profile, or request a stream profile that doesn't exist in the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

Bitrate control

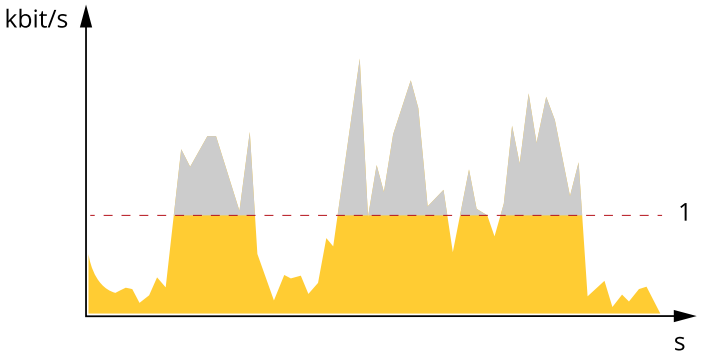
Bitrate control helps you to manage the bandwidth consumption of your video stream.

Learn more

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.



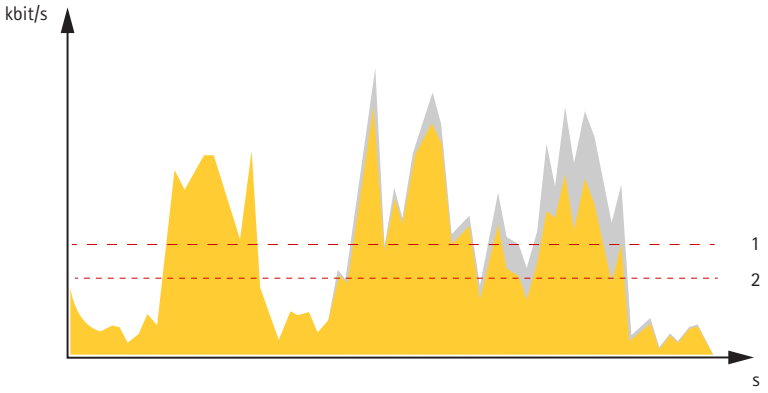
Maximum bitrate (MBR)
Maximum bitrate lets you set a target bitrate to handle bitrate limitations in your system. You might see a decline in image quality or frame rate as the instantaneous bitrate is kept below the specified target bitrate. You can choose to prioritize either image quality or frame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

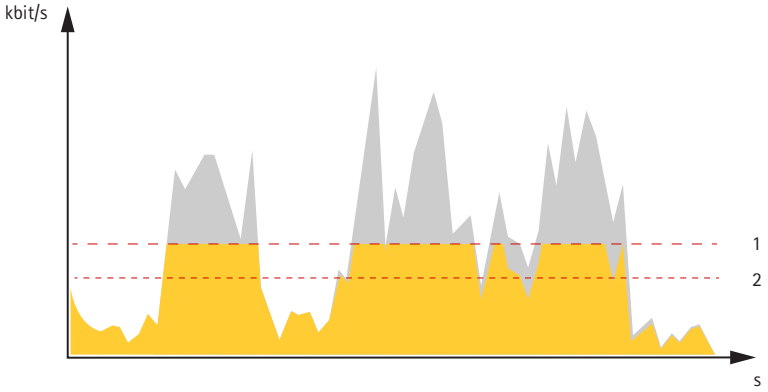
Average bitrate (ABR)
With average bitrate, the bitrate is automatically adjusted over a longer period of time. This is so you can meet the specified target and provide the best video quality based on your available storage. Bitrate is higher in scenes with a lot of activity, compared to static scenes.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

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*.

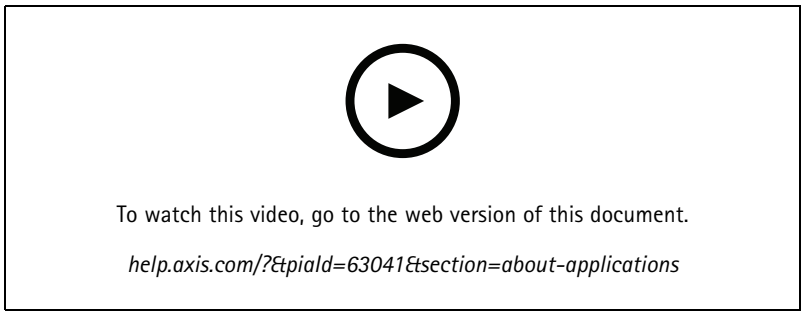
To find the user manuals for Axis applications, go to *help.axis.com*.

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

help.axis.com/?&tpiald=63041&section=about-applications

How to download and install an application

Learn more



How to activate an application licence code on a device

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 the *user manual*.

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.

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. 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 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 webpage. Go to **Maintenance** > **Factory default** 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 version

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

To check the current firmware:

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

Upgrade the firmware

Important

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

Important

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

Troubleshooting

Note

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

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

When the upgrade has finished, the product restarts automatically.

You can use AXIS Device Manager to upgrade multiple devices at the same time. Find out more at *axis.com/products/axis-device-manager*.

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 can't be accessed from a browser	
Can't log in	When HTTPS is enabled, ensure that the correct protocol (HTTP or HTTPS) is used when attempting to log in. You may need to manually type `http` or `https` in the browser's address field. If the password for the user root is lost, the device must be reset to the factory default settings. See *Reset to factory default settings on page 25*.

Troubleshooting

The IP address has been changed by DHCP	IP addresses obtained from a DHCP server are dynamic and may change. If the IP address has been changed, use AXIS IP Utility or AXIS Device Manager to locate the device on the network. Identify the device using its model or serial number, or by the DNS name (if the name has been configured). If required, a static IP address can be assigned manually. For instructions, go to *axis.com/support*.
Certificate error when using IEEE 802.1X	For authentication to work properly, the date and time settings in the Axis device must be synchronized with an NTP server. Go to **System > Date and time**.

The device is accessible locally but not externally

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

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

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

Problems with streaming

Multicast H.264 only accessible by local clients	Check if your router supports multicasting, or if you need to configure the router settings between the client and the device. You might need to increase the TTL (Time To Live) value.
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 that prevents viewing.
Poor rendering of H.264 images	Ensure that your graphics card uses the latest driver. You can usually download the latest drivers from the manufacturer's website.
Color saturation is different in H.264 and Motion JPEG	Modify the settings for your graphics adapter. Go to the adapter's documentation for more information.
Lower frame rate than expected	• See *Performance considerations on page 27*. • 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	Web browsers don't support H.265 decoding. Use a video management system or application that supports 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.
- Access by large numbers of Motion JPEG or unicast H.265 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.

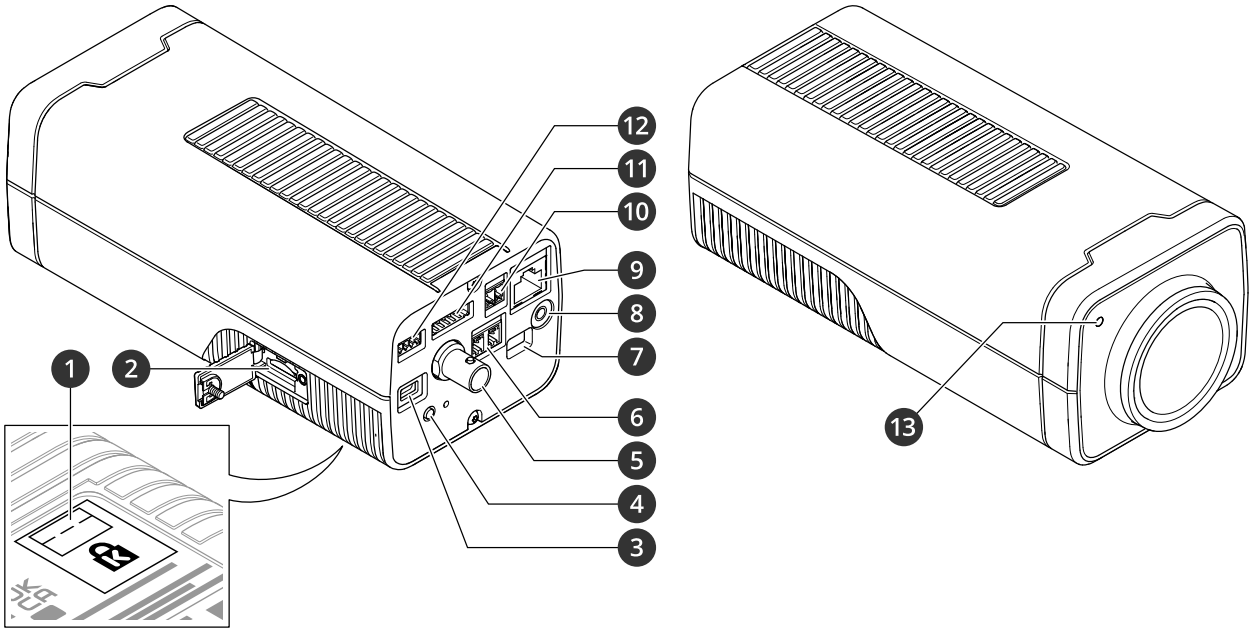
- Accessing Motion JPEG and H.264 video streams simultaneously affects both frame rate and bandwidth.
- Accessing Motion JPEG and H.265 video streams simultaneously affects both frame rate and bandwidth.
- Heavy usage of event settings affects the product's CPU load which in turn affects the frame rate.
- 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.

Contact support

Contact support at *axis.com/support*.

Specifications

Product overview



1 *Security lock slot*
2 *microSD card slot*
3 *HDMI connector*
4 *Control button*
5 *SDI connector*
6 *RS-485/422 connector*
7 *PoE class switch*
8 *Audio in (analogue/digital)*
9 *Network connector (PoE)*
10 *Power connector (DC)*
11 *I/O connector*
12 *I2C connector (camera housing communication connector)*
13 *Status LED*

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 firmware 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. 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 25*.

PoE class switch

Use the switch to select the PoE class you want the device to use. Select PoE class 3 if you're mounting the camera in an outdoor housing that supports it.

Important

When using PoE class 3, HDMI and SDI are turned off.

Connectors

BNC connector

The BNC connector is used for connecting broadcast equipment using SDI. Connect a 75 Ohm coaxial SDI cable.

⚠CAUTION

The connector may be hot during normal operation in elevated ambient temperatures.

HDMI connector

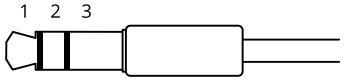
Use the HDMI™ connector to connect a display or public view monitor.

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 input

1 Tip	2 Ring	3 Sleeve

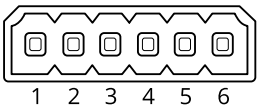
I/O connector

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:

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.

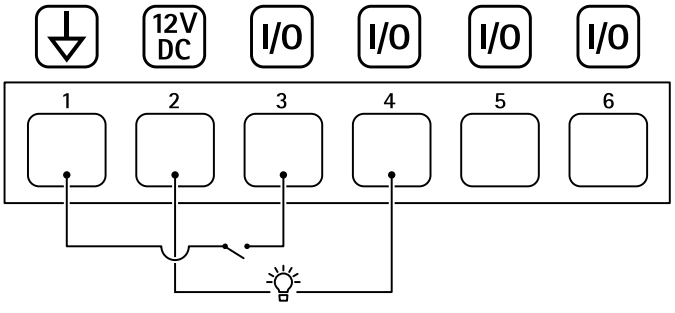
Digital output – For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface, through an event or from the product's webpage.

6-pin terminal block



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

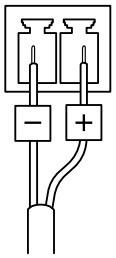
Example



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

Power connector

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

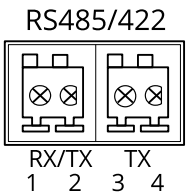


RS485/RS422 connector

Two 2-pin terminal blocks for RS485/RS422 serial interface used to control auxiliary equipment such as pan-tilt devices.

The serial port can be configured to support:

- Two-wire RS485 half duplex
- Four-wire RS485 full duplex
- Two-wire RS422 simplex
- Four-wire RS422 full duplex point to point communication



Function	Pin	Notes
RS485/RS422 RX/TX A	1	(RX) For full duplex RS485/RS422 (RX/TX) For half duplex RS485
RS485/RS422 RX/TX B	2	
RS485/RS422 TX A	3	(TX) For full duplex RS485/RS422
RS485/RS422 TX B	4	

PTZ drivers

APTP

This is a list of models supported by this driver. The physical installation depends on your Axis product and the PTZ unit.

Important

Check what serial communication your Axis product and the PTZ unit will support.

Supported models with RS485 2-wire interface:

- AXIS T99A Positioning Unit Series.

  For information about compatible Axis products, see *axis.com*.

Other models may be supported but this has not been verified by Axis.

Technical information

DEFAULT capabilities for PTZ driver:

Driver	APTP
Version	1.1.0

DEFAULT serial configuration:

PortMode	RS485
BaudRate	115200
DataBits	8
StopBits	1
Parity	None

DEFAULT supported capabilities in this PTZ driver:

Note

Different PTZ units may have other capabilities (both less and more).

Movement	Absolute	Relative	Continuous
Pan	yes	yes	yes
Tilt	yes	yes	yes

Connection

For the RS485/RS422 pin assignment on your device, see *RS485/RS422 connector on page 32*.

To change serial port settings, go to **System > Plain config > Serial** in the device interface.

Pelco

This is a list of models supported by this driver. The physical installation depends on your Axis product and the PTZ unit.

Important

Check what serial communication your Axis product and the PTZ unit will support.

PTZ drivers

Supported models:

- Pelco DD5-C
- Pelco Esprit ES30C/ES31C
- Pelco LRD41C21
- Pelco LRD41C22
- Pelco Spectra III
- Pelco Spectra IV
- Pelco Spectra Mini
- Videotec DTRX3/PTH310P
- Videotec ULISSE
- PTK AMB
- YP3040

Other models may be supported but this has not been verified by Axis.

Technical information

DEFAULT capabilities for PTZ driver:

Driver	Pelco
Version	4.17

DEFAULT serial configuration:

PortMode	RS485
BaudRate	2400
DataBits	8
StopBits	1
Parity	None

DEFAULT supported capabilities in this PTZ driver:

Note

Different PTZ units may have other capabilities (both less and more).

Movement	Absolute	Relative	Continuous
Pan	no	yes	yes
Tilt	no	yes	yes
Zoom	no	yes	yes
Focus	no	yes	yes
Iris	no	yes	yes

AutoIris	yes
AutoFocus	yes
IrCutFilter	no
BackLight	yes
OSDMenu	yes

Connection

For the RS485/RS422 pin assignment on your device, see *RS485/RS422 connector on page 32*.

To change serial port settings, go to **System > Plain config > Serial** in the device interface.

Visca

This is a list of models supported by this driver. The physical installation depends on your Axis product and the PTZ unit.

Important

Check what serial communication your Axis product and the PTZ unit will support.

Supported models with RS422 4-wire interface:

- Sony EVI-D70/D70P
- WISKA DCP-27 (PT-head)

Supported models with RS232 interface (may require external RS422-4-wire/RS232 converter):

- Axis EVI-D30/D31
- Sony EVI-G20/G21
- Sony EVI-D30/D31
- Sony EVI-D100/D100P
- Sony EVI-D70/D70P

Other models may be supported but this has not been verified by Axis.

Technical information

DEFAULT capabilities for PTZ driver:

Driver	Visca/EVI
Version	4.11

DEFAULT serial configuration:

PortMode	RS422
BaudRate	9600
DataBits	8
StopBits	1
Parity	None

DEFAULT supported capabilities in this PTZ driver:

PTZ drivers

Note

Different PTZ units may have other capabilities (both less and more).

Movement	Absolute	Relative	Continuous
Pan	yes	yes	yes
Tilt	yes	yes	yes
Zoom	yes	yes	yes
Focus	yes	yes	yes
Iris	yes	yes	no

AutoIris	yes
AutoFocus	yes
IrCutFilter	yes
BackLight	yes
OSDMenu	no

Connection

For the RS485/RS422 pin assignment on your device, see *RS485/RS422 connector on page 32*.

To change serial port settings, go to **System > Plain config > Serial** in the device interface.

User Manual
AXIS Q1715 Block Camera

Ver. M4.4
Date: November 2022
Part No. T10168073