# AXIS P7316 Video Encoder

# User Manual

# AXIS P7316 Video Encoder

## Table of Contents


**Get started** ..... 4
- Find the device on the network ..... 4
- Open the device's webpage ..... 4
- Set a new password for the root account ..... 4
- Secure passwords ..... 4
- Verify that no one has tampered with the firmware ..... 5
- Webpage overview ..... 5

**Configure your device** ..... 6
- Set video input ..... 6
- Adjust the image ..... 6
- Adjust the camera view (PTZ) ..... 8
- View and record video ..... 8
- Set up rules for events ..... 10
- Audio ..... 13

**The device interface** ..... 14
- Status ..... 14
- Video ..... 15
- Audio ..... 20
- Recordings ..... 21
- Apps ..... 22
- System ..... 22
- Maintenance ..... 37

**Learn more** ..... 38
- Privacy masks ..... 38
- Overlays ..... 38
- Pan, tilt, and zoom (PTZ) ..... 38
- Streaming and storage ..... 38
- Applications ..... 39

**Specifications** ..... 40
- Product overview ..... 40
- LED indicators ..... 40
- SD card slot ..... 41
- Buttons ..... 41
- Connectors ..... 41

**Troubleshooting** ..... 44
- Reset to factory default settings ..... 44
- Firmware options ..... 44
- Check the current firmware version ..... 44
- Upgrade the firmware ..... 44
- Technical issues, clues, and solutions ..... 45
- Performance considerations ..... 46
- Contact support ..... 47

**PTZ drivers** ..... 48
- American Dynamics ..... 48
- Bosch ..... 48
- Canon ..... 48
- Cohu ..... 48
- Daiwa ..... 49
- Dennard ..... 50
- Elmo ..... 51
- Ernitec ..... 51
- Forwardvision ..... 52
- Geutebrück ..... 53
- JVC ..... 53
- Kalatel ..... 54
- Kalatel Digiplex ..... 55
- KDec300 ..... 56
- Lilin ..... 56
- OpenEye ..... 57
- Panasonic ..... 57
- Pelco ..... 58

## Table of Contents

Philips ..... 60
Samsung ..... 61
Sensormatic ..... 63
Siemens ..... 64
Smartscan ..... 64
Teb ..... 64
Ultrak ..... 65
VCC ..... 67
VCL ..... 67
Vicon ..... 69
Videmech ..... 70
Videotec ..... 71
Videotec Macro ..... 71
Visca ..... 71

# 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*.

## 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 4*.
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 44* 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.

## 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:

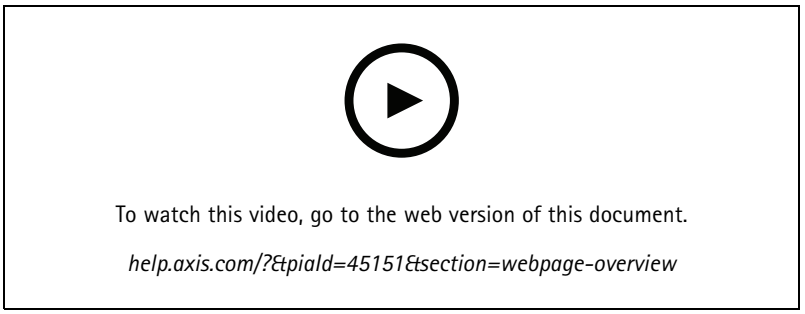
1. Reset to factory default settings. See *Reset to factory default settings on page 44*.

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

2. Configure and install the device.

## Webpage overview

This video gives you an overview of the device interface.




*Axis device web interface*

# Configure your device

## Set video input

To use the video encoder, you must set the video inputs for the connected cameras (channels). When you log in to your device for the first time, the automatically detected video inputs for the cameras are set to **Automatic**.

To change the video inputs:

1. Go to **System > Video input**.
2. Select **Manual** and select the video standard and resolution for each channel you want to change.
3. Click **Save changes & restart**.

### Configure Quad HD or 4K resolution

Quad HD (1440p) or 4K (2160p) resolution is only supported on channel 1. Once it is configured on channel 1, channel 3 is disabled.

You must manually configure Quad HD or 4K resolution:

1. Go to **System > Video input**.
2. Under **Channel 1**, select **Manual**.
3. Select the video standard and Quad HD or 4K resolution.
4. Click **Save changes & restart**.

## 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 38*.

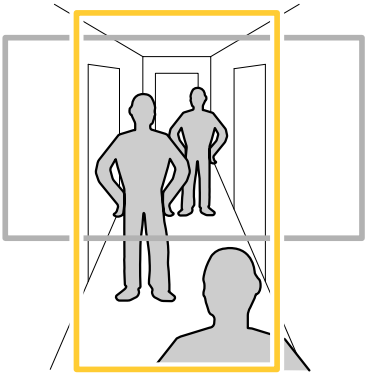
### Level the camera

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.

### 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°.

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

### 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 38*

### 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.

### Show a text overlay

You can add a text field as an overlay in the video stream. This is useful for example when you want to display the date, time or a company name in the video stream.

1. Go to **Video > Overlays**.
2. Select **Text** and click + .
3. Enter the text you want to display in the video stream.
4. Select a position. You can also drag the overlay text field in the live view to change the position.

## Adjust the camera view (PTZ)

### Install the PTZ driver

1. Go to **PTZ > legacy device interface**.
2. In the legacy device interface, go to **Settings > System > Accessories**.
3. Go to **Select driver to use** and select PTZ driver from the drop-down list.
4. Select a video channel.
5. Enter the **Device id** and select **Device type** from the drop down-list. To decide which device type to use, see *PTZ drivers on page 48*.
6. Go to the **PTZ** tab and check that the PTZ settings are available.

### 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 38*.

# Configure your device

## 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 9*

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.

Make sure that AXIS Video Motion Detection is running:

1. Go to **Apps > AXIS Video Motion Detection**.
2. Start the application if it is not already running.
3. 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 conditions, under **Application**, select **VMD4**.
4. In the list of actions, under **Recordings**, select **Record video while the rule is active**.
5. In the list of storage options, select **SD_DISK**.
6. Select a camera and a stream profile.

7. Set the prebuffer time to 5 seconds.
8. Set the postbuffer time to 1 minute.
9. 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 13*.

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**.

### Provide visual indication of an ongoing event

You have the option to connect the AXIS I/O Indication LED to your network camera. This LED can be configured to turn on whenever certain events occur in the camera. For example, to let people know that video recording is in progress.

**Required hardware**

- AXIS I/O Indication LED
- An Axis network video camera

Note

For instructions on how to connect the AXIS I/O Indication LED, see the installation guide provided with the product.

The following example shows how to configure a rule that turns on the AXIS I/O Indication LED to indicate that camera is recording.

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

2. For the port that you connected the AXIS I/O Indication LED to, set the direction to **Output**, and set the normal state to **Circuit open**.
3. Go to **System > Events**.
4. Create a new rule.
5. Select the **Condition** that must be met to trigger the camera to start recording. It can, for example, be a time schedule or motion detection.
6. In the list of actions, select **Record video**. Select a storage space. Select a stream profile or create a new. Also set the **Prebuffer** and **Postbuffer** as required.
7. Save the rule.
8. Create a second rule and select the same **Condition** as in the first rule.
9. In the list of actions, select **Toggle I/O while the rule is active**, and then select the port the AXIS I/O Indication LED is connected to. Set the state to **Active**.
10. Save the rule.

Other scenarios where AXIS I/O Indication LED can be used are for example:

- Configure the LED to turn on when the camera starts, to indicate the presence of the camera. Select **System ready** as a condition.
- Configure the LED to turn on when live stream is active to indicate that a person or a program is accessing a stream from the camera. Select **Live stream accessed** as a condition.

### 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**.

## The device interface

To reach the device interface, enter the device's IP address in a web browser.

Note

Support for the features and settings described in this section varies between devices.

Show or hide the main menu.

Access the product help.

Change the language.

Set light theme or dark theme.

The user menu contains:

- Information about the user who is logged in.
- **Change user** : Log out the current user and log in a new user.
- **Log out** : Log out the current user.

The context menu contains:

- **Analytics data**: Accept to share non-personal browser data.
- **Feedback**: Share any feedback to help us improve your user experience.
- **Legal**: View information about cookies and licenses.
- **About**: View device information, including firmware version and serial number.
- **Legacy device interface**: Change the device interface to the legacy device interface.

### Status

**NTP sync**

Shows NTP synchronization information, including if the device is in sync with an NTP server and the time remaining until the next sync.

**NTP settings**: Click to go to the Date and time page where you can change the NTP settings.

**Video input**

Shows video input information, including if video input is configured and detailed information for each channel.

**Video input settings**: Click to go to the Video input page where you can change the video input settings.

**Device info**

Shows device information, including firmware version and serial number.

**Upgrade firmware**: Click to go to the Maintenance page where you can do a firmware upgrade.

## Video

Click to play the live video stream.

Click to freeze the live video stream.

Click to take a snapshot of the live video stream. The file is saved in the 'Downloads' folder on your computer. The image file name is [snapshot_YYYY_MM_DD_HH_MM_SS.jpg]. The size of the snapshot depends on the compression that is applied from the specific web-browser engine where the snapshot is received, therefore, the snapshot size may vary from the actual compression setting that is configured in the device.

Click to show I/O output ports. Use the switch to open or close the circuit of a port, for example to test external devices.

Click to manually turn on or turn off the IR illumination.

Click to access onscreen controls:

- **Predefined controls**: Turn on to use the available onscreen controls.
- **Custom controls**: Click **Add custom control** to add an onscreen control.

Click to manually turn on the heater for a selected period of time.

Click to start a continuous recording of the live video stream. Click again to stop the recording. If a recording is ongoing, it will resume automatically after a reboot.

Click to show the storage that is configured for the device. To configure the storage you need to be logged in as an administrator.

Click to access more settings:

- **Video format**: Select the encoding format to use in the live view. If you select a format with video compression, it results in a higher CPU and memory usage.
- **Client stream information**: Turn on to show dynamic information about the video stream used by the browser that shows the live video stream. The bitrate information differs from the information shown in a text overlay, because of different information sources. The bitrate in the client stream information is the bitrate of the last second, and it comes from the encoding driver of the device. The bitrate in the overlay is the average bitrate of the last 5 seconds, and it comes from the browser. Both values cover only the raw video stream and not the additional bandwidth generated when it's transported over the network through UDP/TCP/HTTP.
- **Adaptive stream**: Turn on to adapt the image resolution to the viewing client's actual display resolution, to increase the user experience and help prevent a possible overload of the client's hardware. The adaptive stream is only applied when you view the live video stream in the web interface in a browser. When adaptive stream is turned on, the maximum frame rate is 30 fps. If you take a snapshot while adaptive stream is turned on, it will use the image resolution selected by the adaptive stream.
- **Level grid**: Click to show the level grid. The grid helps you decide if the image is horizontally aligned. Click to hide it.
- **Pixel counter**: Click to show the pixel counter. Drag and resize the box to contain your area of interest. You can also define the pixel size of the box in the **Width** and **Height** fields.

- **Refresh**: Click to refresh the still image in the live view.

**1:1** Click to show the live view at full resolution. If the full resolution is larger than your screen size, use the smaller image to navigate in the image.

Click to show the live video stream in full screen. Press ESC to exit full screen mode.

### Installation

**Capture mode** : A capture mode is a preset configuration that defines how the camera captures images. When you change the capture mode, it can affect many other settings, such as view areas and privacy masks.

**Mounting position** : The orientation of the image can change depending on how the camera is mounted.

**Power line frequency**: Select the frequency that is used in your region to minimize image flicker. The American regions usually use 60 Hz. The rest of the world mostly uses 50 Hz. If you're not sure of your region's power line frequency, check with the local authorities.

**Rotate**: Select the preferred image orientation.

### Image

**Appearance**

**Scene profile** : Select a scene profile that suits your surveillance scenario. A scene profile optimizes image settings, including color level, brightness, sharpness, contrast, and local contrast, for a specific environment or purpose.

- **Forensic**: Suitable for surveillance purposes.
- **Indoor** : Suitable for indoor environments.
- **Outdoor** : Suitable for outdoor environments.
- **Vivid**: Useful for demonstration purposes.
- **Traffic overview**: Suitable for vehicle traffic monitoring.

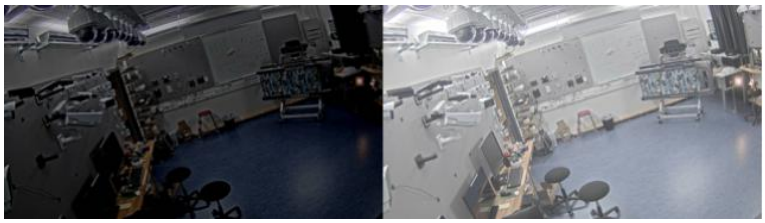
**Saturation**: Use the slider to adjust the color intensity. You can for example get a grayscale image.



**Contrast**: Use the slider to adjust the difference between light and dark.



**Brightness**: Use the slider to adjust the light intensity. This can make objects easier to see. Brightness is applied after image capture, and doesn't affect the information in the image. To get more details from a dark area, it's usually better to increase gain or exposure time.



**Sharpness**: Use the slider to make objects in the image appear sharper by adjusting the edge contrast. If you increase the sharpness, it may increase the bitrate and the amount of storage space needed as well.



**Video input**

**Deinterlacing**: Select a method to improve the video stream image quality from analog devices.

- **None**: No deinterlacing.
- **Blending**: Improves the image quality without putting too much load on the processor.
- **Adaptive interpolation**: Applies different filters to the image. Can in rare cases give better results than motion-adaptive interpolation.
- **Motion-adaptive interpolation**: Applies different filters to different parts of the video stream image, depending on the level of motion in different parts of the scene. This option usually gives the best image quality.

**Video termination**: Turn off when the device is connected alongside other equipment. If you leave video termination on, it can affect the image quality. We recommend you to only keep video termination turned on for the last device in the video signal chain.

**X offset**: Enter a value to horizontally adjust the orientation of the image.

**Y offset**: Enter a value to vertically adjust the orientation of the image.

**General**

**Name**: Enter a name for the selected camera.

### Stream

**General**

**Resolution**: Select the image resolution suitable for the surveillance scene. A higher resolution increases bandwidth and storage.

**Frame rate**: To avoid bandwidth problems on the network or reduce storage size, you can limit the frame rate to a fixed amount. If you leave the frame rate at zero, the frame rate is kept at the highest possible rate under the current conditions. A higher frame rate requires more bandwidth and storage capacity.

**Compression**: Use the slider to adjust the image compression. High compression results in a lower bitrate and lower image quality. Low compression improves the image quality, but uses more bandwidth and storage when you record.

**Signed video** : Turn on to add the signed video feature to the video. Signed video protects the video from tampering by adding cryptographic signatures to the video.

**H.26x encoding**

**Zipstream**: A bitrate reduction technology, optimized for video surveillance, that reduces the average bitrate in an H.264 or H.265 stream in real time. Axis Zipstream applies a high bitrate in scenes where there are multiple regions of interest, for example in scenes with moving objects. When the scene is more static, Zipstream applies a lower bitrate, and thereby reduces the required storage. To learn more, see *Reducing the bit rate with Axis Zipstream*

Select the desired level of bitrate reduction:

- **Off**: No bitrate reduction.
- **Low**: No visible quality degradation in most scenes. This is the default option and it can be used in all types of scenes to reduce the bitrate.
- **Medium**: Visible effects in some scenes through less noise and a slightly lower level of detail in regions of lower interest, for example where there's no movement.
- **High**: Visible effects in some scenes through less noise and a lower level of detail in regions of lower interest, for example where there's no movement. We recommend this level for cloud-connected devices and devices that use local storage.
- **Higher**: Visible effects in some scenes through less noise and a lower level of detail in regions of lower interest, for example where there's no movement.
- **Extreme**: Visible effects in most scenes. The bitrate is optimized for smallest possible storage.

**Dynamic FPS** (frames per second): Turn on to allow the bandwidth to vary based on the level of activity in the scene. More activity requires more bandwidth.

**Lower limit** : Enter a value to adjust the frame rate between minimal fps and the stream default fps based on scene motion. We recommend you to use lower limit in scenes with very little motion, where the fps could drop to 1 or lower.

**Dynamic GOP** (Group of Pictures): Turn on to dynamically adjust the interval between I-frames based on the level of activity in the scene.

**Upper limit** : Enter a maximum GOP length, that is, the maximum number of P-frames between two I-frames.

**P-frames**: Enter the desired number of P-frames. The higher the number, the less bandwidth is required. However, if there are network congestion, there could be a noticeable deterioration in the video quality.

**Bitrate control**:

- **Average**: Select to automatically adjust the bitrate over a longer time period and provide the best possible image quality based on the available storage.
  - Click to calculate the target bitrate based on available storage, retention time, and bitrate limit.
  - **Target bitrate**: Enter desired target bitrate.
  - **Retention time**: Enter the number of days to keep the recordings.
  - **Storage**: Shows the estimated storage that can be used for the stream.

- **Maximum bitrate**: Turn on to set a bitrate limit.
- **Bitrate limit** : Enter a bitrate limit that is higher than the target bitrate.

- **Maximum**: Select to set a maximum instant bitrate of the stream based on your network bandwidth.
  - **Maximum**: Enter the maximum bitrate.
- **Variable**: Select to allow the bitrate to vary based on the level of activity in the scene. More activity requires more bandwidth. We recommend this option for most situations.

**Orientation**

**Rotate** : Rotate the image to match your requirements.

**Mirror**: Turn on to mirror the image.

**Audio**

**Include**: Turn on to use audio in the video stream.

**Source** : Select what audio source to use.

**Stereo** : Turn on to include built-in audio as well as audio from an external microphone.

### Overlays

+ : Click to add an overlay. Select the type of overlay from the dropdown list:

- **Text**: Select to show a text that is integrated in the live view image and visible in all views, recordings and snapshots. You can enter your own text, and you can also include pre-configured modifiers to automatically show for example time, date, frame rate.
  - : Click to add the date modifier `%F` to show yyyy-mm-dd.
  - : Click to add the time modifier `%X` to show hh:mm:ss (24-hour clock).
  - **Modifiers**: Click to select any of the modifiers shown in the list to add them to the text box. For example, `%a` shows the day of the week.
  - **Size**: Select the desired font size.
  - **Appearance**: Select the text color and background color, for example, white text on a black background (default).
  - : Select the position of the overlay in the image.
- **Image**: Select to show a static image superimposed over the video stream. You can use .bmp, .png, .jpeg, or .svg files. To upload an image, click **Images**. Before you upload an image, you can choose to:
  - **Scale with resolution**: Select to automatically scale the overlay image to fit the video resolution.
  - **Use transparency**: Select and enter the RGB hexadecimal value for that color. Use the format RRGGBB. Examples of hexadecimal values: FFFFFF for white, 000000 for black, FF0000 for red, 6633FF for blue, and 669900 for green. Only for .bmp images.
- **Streaming indicator** : Select to show an animation superimposed over the video stream. The animation indicates that the video stream is live, even if the scene doesn't contain any motion.
  - **Appearance**: Select the animation color and background color, for example, red animation on a transparent background (default).
  - **Size**: Select the desired font size.
  - : Select the position of the overlay in the image.

### Privacy masks

: Click to create a new privacy mask. The maximum number of masks depend on the complexity of all masks combined. Each mask can have maximum 10 anchor points.

**Privacy masks**: Click to change the color of all privacy masks, or to delete all privacy masks permanently.

**Cell size**: If you choose mosaic color, the privacy masks appear as pixilated patterns. Use the slider to change the size of the pixels.

 **Mask x**: Click to rename, disable, or permanently delete the mask.

## Audio

### Device settings

**Input**: Turn on or off audio input. Shows the type of input.

**Input type**: Select the type of input, for instance if it's a microphone or line-in.

**Power type**: Select power type for your input.

**Apply changes**: Click to apply your selection.

**Separate gain controls** : Turn on to adjust the gain separately for the different input types.

**Automatic gain control** : Turn on to dynamically adapt the gain to changes in the sound.

**Gain**: Use the slider to change the gain. Click the microphone icon to mute or unmute.

**Output** : Shows the type of output.

**Gain**: Use the slider to change the gain. Click the speaker icon to mute or unmute.

### Stream

**Encoding**: Select the encoding to use for the input source streaming. You can only choose encoding if audio input is turned on. If audio input is tuned off, click **Enable audio input** to turn it on.

### Audio clips

**Add clip**: Click to add a new audio clip.

Click to play the audio clip.

Click to stop playing the audio clip.

The context menu contains:

- **Rename**: Change the name of the audio clip.
- **Create link**: Create a URL which, when used, plays the audio clip on the device. Specify the volume and number of times to play the clip.
- **Download**: Download the audio clip to your computer.
- **Delete**: Delete the audio clip from the device.

### Audio mixer

**Input**

**Ten Band Graphic Audio Equalizer**: Turn on to adjust the level of different frequency bands within an audio signal.

**Voice enhancement** : Turn on to adjust the voice content in relation to other sounds.

## Recordings

Click to filter the recordings.

**From**: Show recordings done after a certain point in time.

**To**: Show recordings up until a certain point in time.

**Source** : Show recordings based on source.

**Event**: Show recordings based on events.

**Storage**: Show recordings based on storage type.

Click to play the recording.

Click to stop the recording.

Click to show more information and options about the recording.

**Set export range**: If you only want to export part of the recording, enter from when to when.

Click to delete the recording.

**Export**: Click to export (part of) the recording.

## Apps

**Add app**: Click to install a new app.

**Find more apps**: Click to go to an overview page of Axis apps.

The context menu contains:

- **App log**: Click to view a log of the app events. The log is helpful when you contact support.
- **Activate license with a key**: If the app requires a license, you need to activate it. Use this option if your device doesn't have internet access.
  If you don't have a license key, go to *axis.com/applications*. You need a license code and the Axis product serial number to generate a license key.
- **Activate license automatically**: If the app requires a license, you need to activate it. Use this option if your device has internet access. You need a license code to activate the license.
- **Deactivate the license**: Deactivate the license to use it in another device. If you deactivate the license, you also remove it from the device. To deactivate the license requires internet access.
- **Settings** : Configure the parameters.
- **Delete**: Delete the app permanently from the device. If you don't deactivate the license first, it remains active.

Note

The device's performance might be affected if you run several apps at the same time.

**Start**: Start or stop the app.

**Open**: Click to access the app's settings. The available settings depend on the application. Some applications don't have any settings.

## System

### Date and time

The time format depends on the web browser's language settings.

Note

We recommend you to synchronize the device's date and time with an NTP server.

**Synchronization**: Select an option for synchronizing the device's date and time.

- **Automatic date and time (manual NTS KE servers)**: Synchronize with the secure NTP key establishment servers connected to the DHCP server.
  - **Manual NTS KE servers**: Enter the IP address of one or two NTP servers. When you use two NTP servers, the device synchronizes and adapts its time based on input from both.
- **Automatic date and time (NTP servers using DHCP)**: Synchronize with the NTP servers connected to the DHCP server.
  - **Fallback NTP servers**: Enter the IP address of one or two fallback servers.
- **Automatic date and time (manual NTP servers)**: Synchronize with NTP servers of your choice.
  - **Manual NTP servers**: Enter the IP address of one or two NTP servers. When you use two NTP servers, the device synchronizes and adapts its time based on input from both.
- **Custom date and time**: Manually set the date and time. Click **Get from system** to fetch the date and time settings once from your computer or mobile device.

**Time zone**: Select which time zone to use. Time will be automatically adjusted for daylight saving time and standard time.

Note

The system uses the date and time settings in all recordings, logs and system settings.

### Network

**IPv4**

**Assign IPv4 automatically**: Select to let the network router assign an IP address to the device automatically. We recommend automatic IP (DHCP) for most networks.

**IP address**: Enter a unique IP address for the device. Static IP addresses can be assigned at random within isolated networks, provided that each address is unique. To avoid conflicts, we recommend you to contact your network administrator before you assign a static IP address.

**Subnet mask**: Enter the subnet mask to define what addresses are inside the local area network. Any address outside the local area network goes through the router.

**Router**: Enter the IP address of the default router (gateway) used to connect devices that are attached to different networks and network segments.

**IPv6**

**Assign IPv6 automatically**: Select to turn on IPv6 and to let the network router assign an IP address to the device automatically.

**Hostname**

**Assign hostname automatically**: Select to let the network router assign a hostname to the device automatically.

**Hostname**: Enter the hostname manually to use as an alternative way of accessing the device. The Hostname is used in the server report and in the system log. Allowed characters are A–Z, a–z, 0–9 and -.

**DNS servers**

**Assign DNS automatically**: Select to let the network router assign search domains and DNS server addresses to the device automatically. We recommend automatic DNS (DHCP) for most networks.

**Search domains**: When you use a hostname that is not fully qualified, click **Add search domain** and enter a domain in which to search for the hostname used by the device.

**DNS servers**: Click **Add DNS server** and enter the IP address of the DNS server. This provides the translation of hostnames to IP addresses on your network.

**HTTP and HTTPS**

**Allow access through**: Select if a user is allowed to connect to the device through the **HTTP**, **HTTPS**, or both **HTTP and HTTPS** protocols.

HTTPS is a protocol that provides encryption for page requests from users and for the pages returned by the web server. The encrypted exchange of information is governed by the use of an HTTPS certificate, which guarantees the authenticity of the server.

To use HTTPS on the device, you must install an HTTPS certificate. Go to **System > Security** to create and install certificates.

Note

If you view encrypted web pages through HTTPS, you might experience a drop in performance, especially when you request a page for the first time.

**HTTP port**: Enter the HTTP port to use. Port 80 or any port in the range 1024-65535 are allowed. If you are logged in as an administrator, you can also enter any port in the range 1-1023. If you use a port in this range, you get a warning.

**HTTPS port**: Enter the HTTPS port to use. Port 443 or any port in the range 1024-65535 are allowed. If you are logged in as an administrator, you can also enter any port in the range 1-1023. If you use a port in this range, you get a warning.

**Certificate**: Select a certificate to enable HTTPS for the device.

**Friendly name**

**Bonjour®**: Turn on to allow automatic discovery on the network.

**Bonjour name**: Enter a friendly name to be visible on the network. The default name is the device name and MAC address.

**Use UPnP®**: Turn on to allow automatic discovery on the network.

**UPnP name**: Enter a friendly name to be visible on the network. The default name is the device name and MAC address.

**One-click cloud connection**

One-click cloud connection (O3C) together with an O3C service provides easy and secure internet access to live and recorded video from any location. For more information, see *axis.com/end-to-end-solutions/hosted-services*.

**Allow O3C**:

- **One-click**: The default setting. Press and hold the control button on the device to connect to an O3C service over the internet. You need to register the device with the O3C service within 24 hours after you press the control button. Otherwise, the device disconnects from the O3C service. Once you have registered the device, **Always** is enabled and the device stays connected to the O3C service.
- **Always**: The device constantly attempts to connect to an O3C service over the internet. Once you have registered the device, it stays connected to the O3C service. Use this option if the control button on the device is out of reach.
- **No**: Disables the O3C service.

**Proxy settings**: If needed, enter the proxy settings to connect to the HTTP server.

**Host**: Enter the proxy server's address.

**Port**: Enter the port number used for access.

**Login** and **Password**: If needed, enter username and password for the proxy server.

**Authentication method**:

- **Basic**: This method is the most compatible authentication scheme for HTTP. It's less secure than the **Digest** method because it sends the username and password unencrypted to the server.
- **Digest**: This method is more secure because it always transfers the password encrypted across the network.
- **Auto**: This option lets the device select the authentication method depending on the supported methods. It prioritizes the **Digest** method over the **Basic** method.

**Owner authentication key (OAK)**: Click **Get key** to fetch the owner authentication key. This is only possible if the device is connected to the internet without a firewall or proxy.

**SNMP**

The Simple Network Management Protocol (SNMP) allows remote management of network devices.

**SNMP**: Select the version of SNMP to use.

- **v1 and v2c**:
  - **Read community**: Enter the community name that has read-only access to all supported SNMP objects. The default value is **public**.
  - **Write community**: Enter the community name that has read/write access to all supported SNMP objects (except read-only objects). The default value is **write**.
  - **Activate traps**: Turn on to activate trap reporting. The device uses traps to send messages for important events or status changes to a management system. In the device interface, you can set up traps for SNMP v1 and v2c. Traps are automatically turned off if you change to SNMP v3 or turn off SNMP. If you use SNMP v3, you can set up traps through the SNMP v3 management application.
  - **Trap address**: Enter the IP address or host name of the management server.
  - **Trap community**: Enter the community to use when the device sends a trap message to the management system.
  - **Traps**:
  - **Cold start**: Sends a trap message when the device starts.

- **Warm start**: Sends a trap message when you change an SNMP setting.
- **Link up**: Sends a trap message when a link changes from down to up.
- **Authentication failed**: Sends a trap message when an authentication attempt fails.

Note

All Axis Video MIB traps are enabled when you turn on SNMP v1 and v2c traps. For more information, see *AXIS OS Portal > SNMP*.

- **v3**: SNMP v3 is a more secure version, which provides encryption and secure passwords. To use SNMP v3, we recommend you to activate HTTPS, as the password is then sent through HTTPS. This also prevents unauthorized parties to access unencrypted SNMP v1 and v2c traps. If you use SNMP v3, you can set up traps through the SNMP v3 management application.
  - **Password for the account "initial"**: Enter the SNMP password for the account named "initial". Although the password can be sent without activating HTTPS, we don't recommend it. The SNMP v3 password can only be set once, and preferably only when HTTPS is enabled. Once the password is set, the password field is no longer displayed. To set the password again, you must reset the device to factory default settings.

**Connected clients**

The list shows all clients that are connected to the device.

**Update**: Click to refresh the list.

## Security

**Certificates**

Certificates are used to authenticate devices on a network. The device supports two types of certificates:

- **Client/server certificates**
  A client/server certificate validates the device's identity, and can be self-signed or issued by a Certificate Authority (CA). A self-signed certificate offers limited protection and can be used before a CA-issued certificate has been obtained.
- **CA certificates**
  You can use a CA certificate to authenticate a peer certificate, for example to validate the identity of an authentication server when the device connects to a network protected by IEEE 802.1X. The device has several pre-installed CA certificates.

These formats are supported:

- Certificate formats: .PEM, .CER, and .PFX
- Private key formats: PKCS#1 and PKCS#12

Important

If you reset the device to factory default, all certificates are deleted. Any pre-installed CA certificates are reinstalled.

Filter the certificates in the list.

**Add certificate** : Click to add a certificate.

The context menu contains:

- **Certificate information**: View an installed certificate's properties.
- **Delete certificate**: Delete the certificate.
- **Create certificate signing request**: Create a certificate signing request to send to a registration authority to apply for a digital identity certificate.

**IEEE 802.1x**

IEEE 802.1x is an IEEE standard for port-based network admission control providing secure authentication of wired and wireless network devices. IEEE 802.1x is based on EAP (Extensible Authentication Protocol).

To access a network protected by IEEE 802.1x, network devices must authenticate themselves. The authentication is performed by an authentication server, typically a RADIUS server (for example FreeRADIUS and Microsoft Internet Authentication Server).

**Certificates**

When configured without a CA certificate, server certificate validation is disabled and the device tries to authenticate itself regardless of what network it is connected to.

When using a certificate, in Axis' implementation, the device and the authentication server authenticate themselves with digital certificates using EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).

To allow the device to access a network protected through certificates, a signed client certificate must be installed on the device.

**Client certificate**: Select a client certificate to use IEEE 802.1x. The authentication server uses the certificate to validate the client's identity.

**CA certificate**: Select a CA certificate to validate the authentication server's identity. When no certificate is selected, the device tries to authenticate itself regardless of what network it is connected to.

**EAP identity**: Enter the user identity associated with the client certificate.

**EAPOL version**: Select the EAPOL version that is used in the network switch.

**Use IEEE 802.1x**: Select to use the IEEE 802.1x protocol.

**Prevent brute-force attacks**

**Blocking**: Turn on to block brute-force attacks. A brute-force attack uses trial-and-error to guess login info or encryption keys.

**Blocking period**: Enter the number of seconds to block a brute-force attack.

**Blocking conditions**: Enter the number of authentication failures allowed per second before the block starts. You can set the number of failures allowed both on page level and device level.

**IP address filter**

**Use filter**: Select to filter which IP addresses that are allowed to access the device.

**Policy**: Choose whether to **Allow** access or **Deny** access for certain IP addresses.

**Addresses**: Enter the IP numbers that are either allowed or denied access to the device. You can also use the CIDR format.

**Custom-signed firmware certificate**

To install test firmware or other custom firmware from Axis on the device, you need a custom-signed firmware certificate. The certificate verifies that the firmware is approved by both the device owner and Axis. The firmware can only run on a specific device which is identified by its unique serial number and chip ID. Custom-signed firmware certificates can only be created by Axis, since Axis holds the key to sign them.

Click **Install** to install the certificate. You need to install the certificate before you install the firmware.

### Users

**Add user**: Click to add a new user. You can add up to 100 users.

**Username**: Enter a unique username.

**New password**: Enter a password for the user. Passwords must be 1 to 64 characters long. Only ASCII printable characters (code 32 to 126) are allowed in the password, for example letters, numbers, punctuation, and some symbols.

**Repeat password**: Enter the same password again.

**Role**:

- **Administrator**: Has full access to all settings. Administrators can also add, update, and remove other users.
- **Operator**: Has access to all settings except:
  - All **System** settings.
  - Adding apps.
- **Viewer**: Has access to:
  - Watch and take snapshots of a video stream.
  - Watch and export recordings.
  - With PTZ user access: pan, tilt, and zoom.

The context menu contains:

**Update user**: Edit the user's properties.

**Delete user**: Delete the user. You can't delete the root user.

**Anonymous users**

**Allow anonymous viewers**: Turn on to allow anyone to access the device as a viewer without having to log in with a user account.

**Allow anonymous PTZ operators**: Turn on to allow anonymous users to pan, tilt, and zoom the image.

### Events

**Rules**

A rule defines the conditions that must be met for the product to perform an action. The list shows all the currently configured rules in the product.

Note

You can create up to 256 action rules.

**Add a rule**: Click to create a rule.

**Name**: Enter a name for the rule.

**Wait between actions**: Enter the minimum time (hh:mm:ss) that must pass between rule activations. It is useful if the rule is activated by for example day-night mode conditions, to avoid that small light changes during sunrise and sunset activate the rule repeatedly.

**Condition**: Select a condition from the list. A condition must be met for the device to perform an action. If multiple conditions are defined, all of them must be met to trigger the action. For information about specific conditions, see *Get started with rules for events*.

**Use this condition as a trigger**: Select to make this first condition function only as a starting trigger. It means that once the rule is activated it remains active for as long as all the other conditions are met, no matter the state of the first condition. If you don't select this option, the rule will simply be active whenever all the conditions are met.

**Invert this condition**: Select if you want the condition to be the opposite of your selection.

+ **Add a condition**: Click to add an additional condition.

**Action**: Select an action from the list and enter its required information. For information about specific actions, see *Get started with rules for events*.

**Recipients**

You can set up your device to notify recipients about events or send files. The list shows all the recipients currently configured in the product, along with information about their configuration.

Note

You can create up to 20 recipients.

+ **Add a recipient**: Click to add a recipient.

**Name**: Enter a name for the recipient.

**Type**: Select from the list:

- **FTP**
  - **Host**: Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
  - **Port**: Enter the port number used by the FTP server. The default is 21.
  - **Folder**: Enter the path to the directory where you want to store files. If this directory doesn't already exist on the FTP server, you will get an error message when uploading files.
  - **Username**: Enter the username for the login.
  - **Password**: Enter the password for the login.
  - **Use temporary file name**: Select to upload files with temporary, automatically generated filenames. The files get renamed to the desired names when the upload completes. If the upload is aborted/interrupted, you don't get any corrupt files. However, you probably still get the temporary files. This way you know that all files that have the desired name, are correct.
  - **Use passive FTP**: Under normal circumstances the product simply requests the target FTP server to open the data connection. The device actively initiates both the FTP control and data connections to the target server. This is normally needed if there is a firewall between the device and the target FTP server.
- **HTTP**
  - **URL**: Enter the network address to the HTTP server and the script that will handle the request. For example: http://192.168.254.10/cgi-bin/notify.cgi.
  - **Username**: Enter the username for the login.
  - **Password**: Enter the password for the login.
  - **Proxy**: Turn on and enter the required information if a proxy server must be passed to connect to the HTTP server.
- **HTTPS**
  - **URL**: Enter the network address to the HTTPS server and the script that will handle the request. For example: https://192.168.254.10/cgi-bin/notify.cgi.
  - **Validate server certificate**: Select to validate the certificate that was created by HTTPS server.
  - **Username**: Enter the username for the login.
  - **Password**: Enter the password for the login.
  - **Proxy**: Turn on and enter the required information if a proxy server must be passed to connect to the HTTPS server.
- **Network storage**

You can add network storage such as a NAS (Network Attached Storage) and use it as a recipient to store files. The files are stored in the Matroska (MKV) file format.
- **Host**: Enter the IP address or hostname for the network storage.
- **Share**: Enter the name of the share on the host.
- **Folder**: Enter the path to the directory where you want to store files.
- **Username**: Enter the username for the login.
- **Password**: Enter the password for the login.

- **SFTP**
  - **Host**: Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
  - **Port**: Enter the port number used by the SFTP server. The default is 22.
  - **Folder**: Enter the path to the directory where you want to store files. If this directory doesn't already exist on the SFTP server, you will get an error message when uploading files.
  - **Username**: Enter the username for the login.
  - **Password**: Enter the password for the login.
  - **SSH host public key type (MD5)**: Enter the fingerprint of the remote host's public key (a 32-digit hexadecimal string). The SFTP client supports SFTP servers using SSH-2 with RSA, DSA, ECDSA, and ED25519 host key types. RSA is the preferred method during negotiation, followed by ECDSA, ED25519, and DSA. Make sure to enter the right MD5 host key that is used by your SFTP server. While the Axis device supports both MD5 and SHA-256 hash keys, we recommend using SHA-256 due to stronger security over MD5. For more information on how to configure an SFTP server with an Axis device, go to the *AXIS OS Portal*.
  - **SSH host public key type (SHA256)**: Enter the fingerprint of the remote host's public key (a 43-digit Base64 encoded string). The SFTP client supports SFTP servers using SSH-2 with RSA, DSA, ECDSA, and ED25519 host key types. RSA is the preferred method during negotiation, followed by ECDSA, ED25519, and DSA. Make sure to enter the right MD5 host key that is used by your SFTP server. While the Axis device supports both MD5 and SHA-256 hash keys, we recommend using SHA-256 due to stronger security over MD5. For more information on how to configure an SFTP server with an Axis device, go to the *AXIS OS Portal*.
  - **Use temporary file name**: Select to upload files with temporary, automatically generated filenames. The files get renamed to the desired names when the upload completes. If the upload is aborted/interrupted, you don't get any corrupt files. However, you probably still get the temporary files. This way you know that all files that have the desired name, are correct.
- **SIP** :
  - **From SIP account**: Select from the list.
  - **To SIP address**: Enter the SIP address.
- **Email**
  - **Send email to**: Enter the email address to send emails to. To enter multiple addresses, use commas to separate them.
  - **Send email from**: Enter the email address of the sending server.
  - **Username**: Enter the username for the mail server. Leave this field empty if the mail server does not require authentication.
  - **Password**: Enter the password for the mail server. Leave this field empty if the mail server does not require authentication.
  - **Email server (SMTP)**: Enter the name of the SMTP server, for example smtp.gmail.com, smtp.mail.yahoo.com.
  - **Port**: Enter the port number for the SMTP server, using values in the range 0-65535. The default value is 587.
  - **Encryption**: To use encryption, select either SSL or TLS.
  - **Validate server certificate**: If you use encryption, select to validate the identity of the device. The certificate can be self-signed or issued by a Certificate Authority (CA).
  - **POP authentication**: Turn on to enter the name of the POP server, for example pop.gmail.com.

Note

Some email providers have security filters that prevent users from receiving or viewing large amount of attachments, from receiving scheduled emails and similar. Check the email provider's security policy to avoid your email account being locked or missing out on your expected emails.

- **TCP**
  - **Host**: Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
  - **Port**: Enter the port number used to access the server.

**Test**: Click to test the setup.

The context menu contains:

**View recipient**: Click to view all the recipient details.

**Copy recipient**: Click to copy a recipient. When you copy, you can make changes to the new recipient.

**Delete recipient**: Click to delete the recipient permanently.

**Schedules**

Schedules and pulses can be used as conditions in rules. The list shows all the schedules and pulses currently configured in the product, along with information about their configuration.

**Add schedule**: Click to create a schedule or pulse.

**Manual trigger**

The manual trigger is used to manually trigger a rule. The manual trigger can for example be used to validate actions during product installation and configuration.

### MQTT

MQTT (Message Queuing Telemetry Transport) is a standard messaging protocol for the Internet of Things (IoT). It was designed for simplified IoT integration and is used in a wide variety of industries to connect remote devices with a small code footprint and minimal network bandwidth. The MQTT client in Axis device firmware can simplify integration of data and events produced in the device to systems which are not video management systems (VMS).

Set up the device as an MQTT client. MQTT communication is based on two entities, the clients and the broker. The clients can send and receive messages. The broker is responsible for routing messages between clients.

You can learn more about MQTT in *AXIS OS Portal*.

**MQTT client**

**Connect**: Turn on or off the MQTT client.

**Status**: Shows the current status of the MQTT client.

**Broker**

**Host**: Enter the hostname or IP address of the MQTT server.

**Protocol**: Select which protocol to use.

**Port**: Enter the port number.

- 1883 is the default value for **MQTT over TCP**
- 8883 is the default value for **MQTT over SSL**
- 80 is the default value for **MQTT over WebSocket**
- 443 is the default value for **MQTT over WebSocket Secure**

**Username**: Enter the username that the client will use to access the server.

**Password**: Enter a password for the username.

**Client ID**: Enter a client ID. The client identifier is sent to the server when the client connects to it.

**Clean session**: Controls the behavior at connection and disconnection time. When selected, the state information is discarded at connect and disconnect.

**Keep alive interval**: The keep alive interval enables the client to detect when the server is no longer available without having to wait for the long TCP/IP timeout.

**Timeout**: The time interval in seconds to allow a connect to complete. Default value: 60

**Device topic prefix**: Used in the default values for the topic in the connect message and LWT message on the **MQTT client** tab, and in the publication conditions on the **MQTT publication** tab.

**Reconnect automatically**: Specifies whether the client should reconnect automatically after a disconnect.

**Connect message**

Specifies if a message should be sent out when a connection is established.

**Send message**: Turn on to send messages.

**Use default**: Turn off to enter your own default message.

**Topic**: Enter the topic for the default message.

**Payload**: Enter the content for the default message.

**Retain**: Select to keep the state of client on this **Topic**

**QoS**: Change the QoS layer for the packet flow.

**Last Will and Testament message**

The Last Will Testament (LWT) lets a client provide a testament along with its credentials when connecting to the broker. If the client disconnects ungracefully at some point later (maybe because his power source died), it can let the broker deliver a message to other clients. This LWT message has the same form as an ordinary message and gets routed via the same mechanics.

**Send message**: Turn on to send messages.

**Use default**: Turn off to enter your own default message.

**Topic**: Enter the topic for the default message.

**Payload**: Enter the content for the default message.

**Retain**: Select to keep the state of client on this **Topic**

**QoS**: Change the QoS layer for the packet flow.

**MQTT publication**

**Use default topic prefix**: Select to use the default topic prefix, that is defined in the device topic prefix in the **MQTT client** tab.

**Include topic name**: Select to include the topic that describes the condition in the MQTT topic.

**Include topic namespaces**: Select to include ONVIF topic namespaces in the MQTT topic.

**Include serial number**: Select to include the device's serial number in the MQTT payload.

+ **Add condition**: Click to add a condition.

**Retain**: Defines which MQTT messages are sent as retained.

- **None**: Send all messages as non-retained.
- **Property**: Send only stateful messages as retained.
- **All**: Send both stateful and stateless messages as retained.

**QoS**: Select the desired level for the MQTT publication.

MQTT subscriptions

**Add subscription**: Click to add a new MQTT subscription.

**Subscription filter**: Enter the MQTT topic that you want to subscribe to.

**Use device topic prefix**: Add the subscription filter as prefix to the MQTT topic.

**Subscription type**:

- **Stateless**: Select to convert MQTT messages into a stateless message.
- **Stateful**: Select to convert MQTT messages into a condition. The payload is used as the state.

**QoS**: Select the desired level for the MQTT subscription.

## Storage

Network storage

**Add network storage**: Click to add a network share where you can save recordings.

- **Address**: Enter the IP address or host name of the host server, typically a NAS (Network Attached Storage). We recommend you to configure the host to use a fixed IP address (not DHCP since a dynamic IP address can change) or that you use DNS. Windows SMB/CIFS names are not supported.
- **Network share**: Enter the name of the shared location on the host server. Several Axis devices can use the same network share, since each device gets its own folder.
- **User**: If the server requires a login, enter the username. To log in to a specific domain server, type `DOMAIN\username`.
- **Password**: If the server requires a login, enter the password.
- **SMB version**: Select the SMB storage protocol version to connect to the NAS. If you select **Auto**, the device tries to negotiate one of the secure versions SMB: 3.02, 3.0, or 2.1. Select 1.0 or 2.0 to connect to older NAS that don't support higher versions. You can read more about SMB support in Axis devices *here*.
- **Add share even if connection test fails**: Select to add the network share even if an error is discovered during the connection test. The error can be, for example, that you didn't enter a password even though the server requires one.

**Remove network storage**: Click to remove the connection to the network share. This removes all settings for the network share.

**Write protect**: Turn on to stop writing to the network share and protect recordings from being removed. You can't format a write-protected network share.

**Ignore**: Turn on to stop storing recordings on the network share.

**Retention time**: Select how long to keep recordings, to limit the amount of old recordings or to comply with regulations regarding data storage. If the network storage becomes full, old recordings are removed before the selected time period has passed.

Tools

- **Test connection**: Test the connection to the network share.
- **Format**: Format the network share, for example when you need to quickly erase all data. cifs is the available file system option.

Click **Use tool** to activate the selected tool.

Onboard storage

Important

Risk of data loss and corrupted recordings. Do not remove the SD card while the device is running. Unmount the SD card before you remove it.

**Unmount**: Click to safely remove the SD card.

**Write protect**: Turn on to stop writing to the SD card and protect recordings from being removed. You can't format a write-protected SD card.

**Autoformat**: Turn on to automatically format a newly inserted SD card. It formats the file system into ext4.

**Ignore**: Turn on to stop storing recordings on the SD card. When you ignore the SD card, the device no longer recognizes that the card exists. The setting is only available for administrators.

**Retention time**: Select how long to keep recordings, to limit the amount of old recordings or to comply with regulations regarding data storage. If the SD card becomes full, old recordings are removed before the selected time period has passed.

**Tools**

- **Check**: Check for errors on the SD card. This only works for the ext4 file system.
- **Repair**: Repair errors in the ext4 file system. To repair an SD card with the VFAT file system, eject the SD card, insert it in a computer and perform a disk repair.
- **Format**: Format the SD card, for example when you need to change the file system or quickly erase all data. VFAT and ext4 are the two available file system options. The recommended format is ext4, due to its resilience against data loss if the card is ejected or if there is an abrupt power loss. However, you need a third-party ext4 driver or application to access the file system from Windows®.
- **Encrypt**: Use this tool to format the SD card and enable encryption. **Encrypt** deletes all data stored on the SD card. After using **Encrypt** data that's stored on the SD card is protected using encryption.
- **Decrypt**: Use this tool to format the SD card without encryption. **Decrypt** deletes all data stored on the SD card. After using **Decrypt** data that's stored on the SD card is not protected using encryption.
- **Change password**: Change the password required to encrypt the SD card.

Click **Use tool** to activate the selected tool.

**Wear trigger**: Set a value for the SD card wear level at which you want to trigger an action. The wear level ranges from 0–200%. A new SD card that has never been used has a wear level of 0%. A wear level of 100% indicates that the SD card is close to its expected lifetime. When the wear-level reaches 200% there is a high risk of the SD card malfunctioning. We recommend setting the wear trigger between 80–90%. This gives you time to download any recordings as well as replace the SD card in time before it potentially wears out. The wear trigger allows you to set up an event and get a notification when the wear level reaches your set value.

### Stream profiles

Click + to create and save groups of video stream settings. You can use the settings in different situations, for example in continuous recording or when you use action rules to record.

### ONVIF

**ONVIF users**

ONVIF (Open Network Video Interface Forum) is a global interface standard that makes it easier for end-users, integrators, consultants, and manufacturers to take advantage of the possibilities offered by network video technology. ONVIF enables interoperability between different vendor products, increased flexibility, reduced cost and future-proof systems.

+ **Add user**: Click to add a new ONVIF user.

**Username**: Enter a unique username.

**New password**: Enter a password for the user. Passwords must be 1 to 64 characters long. Only ASCII printable characters (code 32 to 126) are allowed in the password, for example letters, numbers, punctuation, and some symbols.

**Repeat password**: Enter the same password again

**Role**:

- **Administrator**: Has full access to all settings. Administrators can also add, update, and remove other users.
- **Operator**: Has access to all settings except:
  - All **System** settings.
  - Adding apps.
- **Media user**: Allows access to the video stream only.

⋮ The context menu contains:

**Update user**: Edit the user's properties.

**Delete user**: Delete the user. You can't delete the root user.

By creating an ONVIF user, you automatically enable ONVIF communication. Use the username and password for all ONVIF communication with the device. For more information see the Axis Developer Community at *axis.com*.

**ONVIF media profiles**

An ONVIF media profile consists of a set of configurations that you can use to change media stream settings.

+ **Add media profile**: Click to add a new ONVIF media profile.

**profile_x**: Click a profile to edit.

### Analytics metadata

**Metadata producers**

**Metadata producers** lists the channels used by apps and the metadata they are streaming from the device.

**Producer**: The app producing the metadata.

**Channel**: The channel used by the app. Check to enable the metadata stream. Uncheck to disable the stream for compatibility or resources management reasons.

### Detectors

**Camera tampering**

The camera tampering detector generates an alarm when the scene changes, for example because the lens is covered, sprayed or severely put out of focus, and the time in **Trigger after** has passed. The tampering detector only activates when the camera has not moved for at least 10 seconds. During this period the detector sets up a scene model to use as a comparison to detect tampering in current images. For the scene model to be set up properly, make sure that the camera is in focus, the lighting conditions are correct, and the camera doesn't point at a scene that lacks contours, for example a blank wall. Camera tampering can be used as a condition to trigger actions.

**Trigger after**: Enter the minimum time that the tampering conditions must be active before the alarm triggers. This can help prevent false alarms for known conditions that affect the image.

**Trigger on dark images**: It is very difficult to generate alarms when the camera lens is sprayed, since it is impossible to distinguish that event from other situations where the image turns dark in a similar way, for example when the lighting conditions change. Turn on this parameter to generate alarms for all cases where the image turns dark. When it's turned off, the device doesn't generate any alarm when the image turns dark.

**Audio detection**

These settings are available for each audio input.

**Sound level**: Adjust the sound level to a value from 0–100, where 0 is the most sensitive and 100 the least sensitive. Use the activity indicator as a guide when you set the sound level. When you create events, you can use the sound level as a condition. You can choose to trigger an action if the sound level rises above, falls below or passes the set value.

### Video input

Each video input is terminated using a coax/BNC connector and displayed as a numbered channel.

Connect a 75 Ohm coaxial video cable; the recommended maximum length is 250 m (800 ft).

**Automatic**: The default setting. The encoder detects the video standard and resolution automatically.

**Manual**: Lock the channel to the selected video standard and resolution.

**Reload**: Click to restore to the current encoder settings.

**Mark as configured**: Click to acknowledge the video input settings. The video input is shown as configured in the Status page.

**Save changes & restart**: Click to save the changes and restart the device. If you restart the device, it will affect ongoing recordings.

### Accessories

**I/O ports**

Use digital input to connect external devices that can toggle between an open and closed circuit, for example PIR sensors, door or window contacts, and glass break detectors.

Use digital output to connect external devices such as relays and LEDs. You can activate connected devices through the VAPIX® Application Programming Interface or in the device interface.

**Port**

**Name**: Edit the text to rename the port.

**Direction**:  indicates that the port is an input port.  indicates that it's an output port. If the port is configurable, you can click the icons to change between input and output.

**Normal state**: Click  open circuit, and  for closed circuit.

**Current state**: Shows the current state of the port. The input or output is activated when the current state is different from the normal state. An input on the device has an open circuit when it's disconnected or when there is a voltage above 1 V DC.

Note

During restart the output circuit is open. When the restart is complete, the circuit goes back to the normal position. If you change any settings on this page, the output circuits go back to their normal positions regardless of any active triggers.

**Supervised**  : Turn on to make it possible to detect and trigger actions if someone tampers with the connection to digital I/O devices. In addition to detecting if an input is open or closed, you can also detect if someone has tampered with it (that is, cut or shorted). To supervise the connection requires additional hardware (end-of-line resistors) in the external I/O loop.

## Logs

**Reports and logs**

**Reports**

- **View the device server report**: Click to show information about the product status in a pop-up window. The Access Log is automatically included in the Server Report.
- **Download the device server report**: Click to download the server report. It creates a .zip file that contains a complete server report text file in UTF-8 format, as well as a snapshot of the current live view image. Always include the server report .zip file when you contact support.
- **Download the crash report**: Click to download an archive with detailed information about the server's status. The crash report contains information that is in the server report as well as detailed debug information. This report might contain sensitive information such as network traces. It can take several minutes to generate the report.

**Logs**

- **View the system log**: Click to show information about system events such as device startup, warnings and critical messages.
- **View the access log**: Click to show all failed attempts to access the device, for example when a wrong login password is used.

**Network trace**

Important

A network trace file might contain sensitive information, for example certificates or passwords.

A network trace file can help you troubleshoot problems by recording activity on the network. Select the duration of the trace in seconds or minutes, and click **Download**.

**Remote system log**

Syslog is a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, which indicates the software type generating the message, and assigned a severity level.

+ **Server**: Click to add a new server.

**Host**: Enter the hostname or IP address of the server.

**Format**: Select which syslog message format to use.

- RFC 3164
- RFC 5424

**Protocol**: Select the protocol and port to use:

- UDP (Default port is 514)
- TCP (Default port is 601)
- TLS (Default port is 6514)

**Severity**: Select which messages to send when triggered.

**CA certificate set**: See the current settings or add a certificate.

### Plain config

Plain config is for advanced users with experience of Axis device configuration. Most parameters can be set and edited from this page.

## Maintenance

**Restart**: Restart the device. This does not affect any of the current settings. Running applications restart automatically.

**Restore**: Return *most* settings to the factory default values. Afterwards you must reconfigure the device and apps, reinstall any apps that didn't come preinstalled, and recreate any events and PTZ presets.

Important

The only settings saved after restore are:

- Boot protocol (DHCP or static)
- Static IP address
- Default router
- Subnet mask
- 802.1X settings
- O3C settings

**Factory default**: Return *all* settings to the factory default values. Afterwards you must reset the IP address to make the device accessible.

Note

All Axis device firmware is digitally signed to ensure that you only install verified firmware on your device. This further increases the overall minimum cybersecurity level of Axis devices. For more information, see the white paper "Signed firmware, secure boot, and security of private keys" at *axis.com*.

**Firmware upgrade**: Upgrade to a new firmware version. New firmware releases can contain improved functionality, bug fixes, and completely new features. We recommend you to always use the latest release. To download the latest release, go to *axis.com/support*.

When you upgrade, you can choose between three options:

- **Standard upgrade**: Upgrade to the new firmware version.
- **Factory default**: Upgrade and return all settings to the factory default values. When you choose this option, you can't revert to the previous firmware version after the upgrade.
- **Autorollback**: Upgrade and confirm the upgrade within the set time. If you don't confirm, the device reverts to the previous firmware version.

**Firmware rollback**: Revert to the previously installed firmware version.

## Learn more

### 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.

### Overlays

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

### Pan, tilt, and zoom (PTZ)

#### 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.

Note

The pause between successive guard tours is at least 10 minutes, and the fixed minimum viewing time is 10 seconds.

### 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.

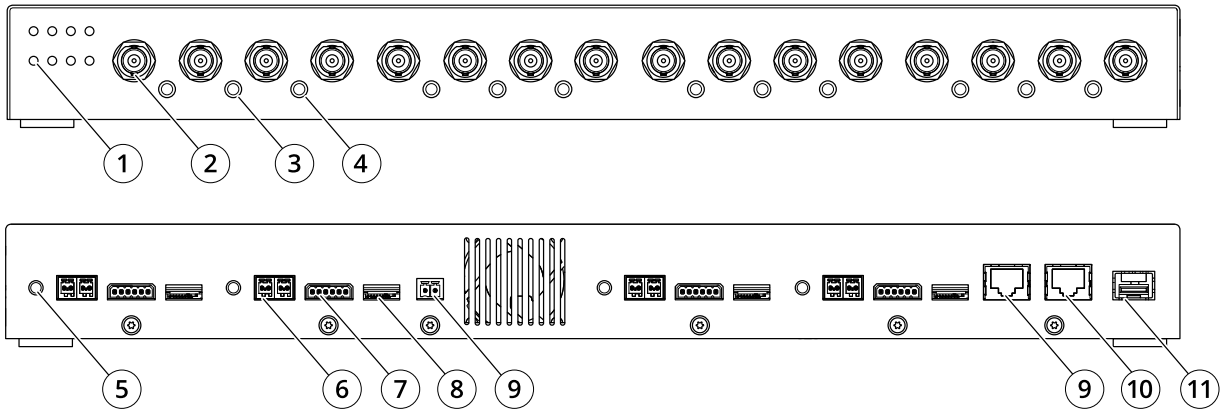
## Applications

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*.

# Specifications

## Product overview




1 *4x Status LED*
2 *16x BNC connectors*
3 *8x Audio input*
4 *4x Audio output*
5 *4x Control button*
6 *4x RS485/RS422 connector*
7 *4x I/O connector*
8 *4x MicroSD card slot*
9 *Power connector*
10 *AUX/Maintenance RJ45*
11 *Ethernet RJ45*
12 *SFP connector*

## LED indicators

| Status LED | Indication |
|---|---|
| Unlit | Connection and normal operation. |
| Green | Steady green for normal operation. |
| Amber | Steady during startup, during reset to factory default or when restoring settings. |

| Network LED | Indication |
|---|---|
| Green | Steady for connection to a 1 Gbit/s network. Flashes for network activity. |
| Amber | Steady for connection to a 10/100 Mbit/s network. Flashes for network activity. |
| Unlit | No network connection. |

## 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 44*.

## Connectors

### Bus connector

The bus connectors are the physical interfaces to the video encoder chassis that provide power, network, RS485, and I/O terminal connections.

### BNC connector

Each video input is terminated using a coax/BNC connector.

Connect a 75 Ohm coaxial video cable; the recommended maximum length is 250 m (800 ft).

Note

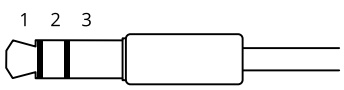
75 Ohm video termination can be enabled/disabled for the video input through the product's webpage at . Video termination is enabled on factory default. If the product is connected in parallel with other equipment, for optimum video quality, we recommended to enable video termination only for the last device in the video signal chain.

### Network connector

RJ45 Ethernet connector.

### 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 |

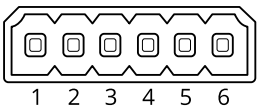
### I/O connector

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.

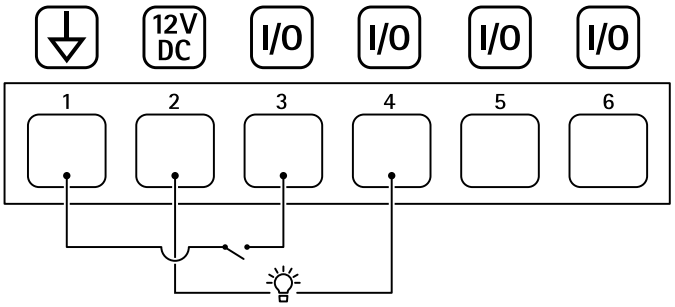
**Digital output –** For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface, through an event or from the product's webpage.

6-pin terminal block




| Function | Pin | Notes | Specifications |
|---|---|---|---|
| DC ground | 1 | | 0 V DC |
| DC output | 2 | Can be used to power auxiliary equipment.<br>Note: This pin can only be used as power out. | 12 V DC<br>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 |

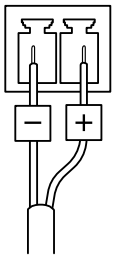
Example




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

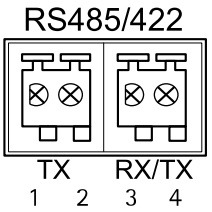
2-pin terminal block for DC power input. Use a Safety Extra Low Voltage (SELV) compliant limited power source (LPS) with either a rated output power limited to ≤100 W or a rated output current limited to ≤5 A.




### RS485/RS422 connector

Two 2-pin terminal blocks for RS485/RS422 serial interface. 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 TX A | 1 | (TX) For full duplex RS485/RS422 |
| RS485/RS422 TX B | 2 | |
| RS485/RS422 RX/TX A | 3 | (RX) For full duplex RS485/RS422<br>(RX/TX) For half duplex RS485 |
| RS485/RS422 RX/TX B | 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 40*.
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.

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):<br>• 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.<br>• 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.<br><br>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 44*. |

| | |
|---|---|
| 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).<br><br>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.<br><br>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 46*.<br>• Reduce the number of applications running on the client computer.<br>• Limit the number of simultaneous viewers.<br>• Check with the network administrator that there is enough bandwidth available.<br>• 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

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.
- 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.

## Contact support

Contact support at *axis.com/support*.

## PTZ drivers

### American Dynamics

For more details, go to *Sensormatic on page 63*.

### Bosch

For more details, go to *Philips on page 60*.

### Canon

For more details, go to *VCC on page 67*.

### Cohu

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Cohu 3950 iVIEW
- Cohu ER8945
- Cohu ER8945A

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

**Technical information**

DEFAULT capabilities for PTZ driver:

| | |
|---|---|
| **Driver** | Cohu |
| **Version** | 4.10 |

DEFAULT serial configuration:

| | |
|---|---|
| **PortMode** | RS422 |
| **BaudRate** | 9600 |
| **DataBits** | 8 |
| **StopBits** | 1 |
| **Parity** | None |

DEFAULT supported capabilities in this PTZ driver:

Note

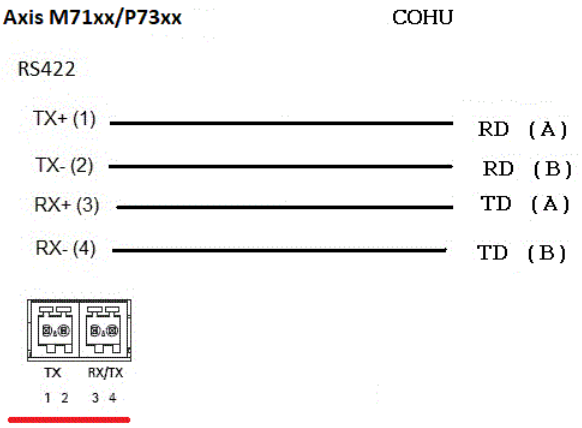
Different PTZ models may have other capabilities (both less and more).

## PTZ drivers

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

| | |
|---|---|
| **AutoIris** | yes |
| **AutoFocus** | yes |
| **IrCutFilter** | yes |
| **BackLight** | no |
| **OSDMenu** | no |

**Connection example**




### Daiwa

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Daiwa DMP15-H1
- Daiwa DMP23-H2

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

**Technical information**

DEFAULT capabilities for PTZ driver:

## PTZ drivers

| | |
|---|---|
| **Driver** | Daiwa |
| **Version** | 4.05 |

DEFAULT serial configuration:

| | |
|---|---|
| **PortMode** | RS485 |
| **BaudRate** | 9600 |
| **DataBits** | 8 |
| **StopBits** | 1 |
| **Parity** | None |

DEFAULT supported capabilities in this PTZ driver:

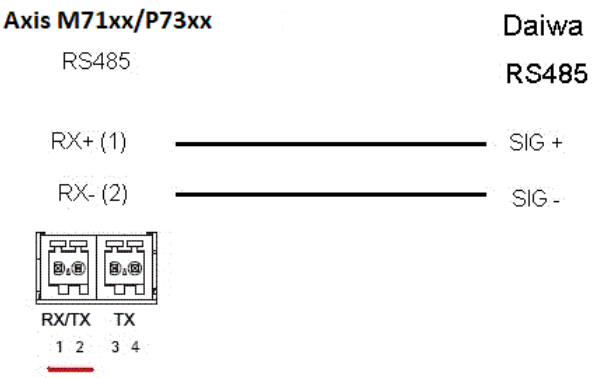
Note

Different PTZ models 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 | no | yes | yes |
| Iris | no | no | no |

| | |
|---|---|
| **AutoIris** | no |
| **AutoFocus** | yes |
| **IrCutFilter** | no |
| **BackLight** | no |
| **OSDMenu** | yes |

**Connection example**



## Dennard

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Dennard 2050
- Dennard 2060

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

## Elmo

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Elmo PTC-400C
- Elmo PTC-1000

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

## Ernitec

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Ernitec ICU-PTZ-S 51PA
- Ernitec Orion 361-23C
- Ernitec Orion/3-DN

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

**Technical information**

DEFAULT capabilities for PTZ driver:

| | |
|---|---|
| **Driver** | Ernitec |
| **Version** | 4.01 |

DEFAULT serial configuration:

| | |
|---|---|
| **PortMode** | RS485 |
| **BaudRate** | 2400 |
| **DataBits** | 8 |
| **StopBits** | 1 |
| **Parity** | None |

DEFAULT supported capabilities in this PTZ driver:

Note

Different PTZ models 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** | no |
| **OSDMenu** | yes |

## Forwardvision

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- MIC1-400

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

**Technical information**

DEFAULT capabilities for PTZ driver:

| | |
|---|---|
| **Driver** | Forwardvision |
| **Version** | 4.04 |

DEFAULT serial configuration:

| | |
|---|---|
| **PortMode** | RS485 |
| **BaudRate** | 9600 |

| | |
|---|---|
| **DataBits** | 8 |
| **StopBits** | 1 |
| **Parity** | Odd |

DEFAULT supported capabilities in this PTZ driver:

Note

Different PTZ models 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 | no | yes | no |
| Iris | no | yes | no |

| | |
|---|---|
| **AutoIris** | yes |
| **AutoFocus** | yes |
| **IrCutFilter** | no |
| **BackLight** | no |
| **OSDMenu** | no |

## Geutebrück

For more details, go to *KDec300 on page 56*.

## JVC

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- JVC TK-C676

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

**Technical information**

DEFAULT capabilities for PTZ driver:

| | |
|---|---|
| **Driver** | JVC |
| **Version** | 4.07 |

DEFAULT serial configuration:

| | |
|---|---|
| **PortMode** | RS485 |
| **BaudRate** | 9600 |
| **DataBits** | 8 |
| **StopBits** | 1 |
| **Parity** | Even |

DEFAULT supported capabilities in this PTZ driver:

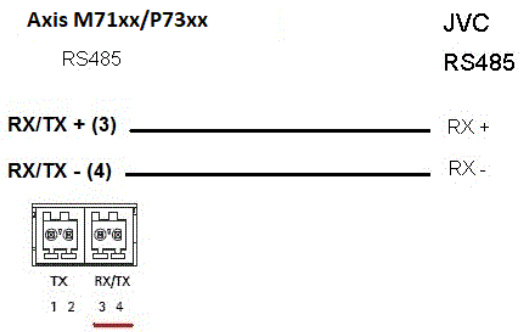
Note

Different PTZ models 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 example**




## Kalatel

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Kalatel KTD-312 (Computer Interface/Data-merger)

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

**Technical information**

DEFAULT capabilities for PTZ driver:

| | |
|---|---|
| **Driver** | Kalatel |
| **Version** | 4.05 |

DEFAULT serial configuration:

| | |
|---|---|
| **PortMode** | RS422 |
| **BaudRate** | 9600 |
| **DataBits** | 8 |
| **StopBits** | 1 |
| **Parity** | None |

DEFAULT supported capabilities in this PTZ driver:

Note

Different PTZ models 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** | no |
| **AutoFocus** | yes |
| **IrCutFilter** | no |
| **BackLight** | no |
| **OSDMenu** | yes |

## Kalatel Digiplex

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Kalatel KTD-312 (Computer Interface/Data-merger)
- Cyberdome ver 1.0

- Cyberdome ver 1.2
- Cyberdome ver 2.0

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

## KDec300

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Geutebruck KDec300 (Argus unit)

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

## Lilin

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Lilin PIH-717
- Lilin PIH-7000

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

**Technical information**

DEFAULT capabilities for PTZ driver:

| | |
|---|---|
| **Driver** | Lilin |
| **Version** | 4.03 |

DEFAULT serial configuration:

| | |
|---|---|
| **PortMode** | RS485 |
| **BaudRate** | 9600 |
| **DataBits** | 8 |
| **StopBits** | 1 |
| **Parity** | None |

DEFAULT supported capabilities in this PTZ driver:

Note

Different PTZ models 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 | no |

| | |
|---|---|
| **AutoIris** | yes |
| **AutoFocus** | yes |
| **IrCutFilter** | no |
| **BackLight** | no |
| **OSDMenu** | no |

## OpenEye

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- OpenEye CM-510
- OpenEye CM-525

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

## Panasonic

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Panasonic WV-CS850/CS854
- Panasonic WV-CS850A/CS854A

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

Panasonic WV-860/860A (Verified by third party).

**Technical information**

DEFAULT capabilities for PTZ driver:

| | |
|---|---|
| **Driver** | Panasonic |
| **Version** | 4.02 |

## PTZ drivers

DEFAULT serial configuration:

| | |
|---|---|
| **PortMode** | RS485 |
| **BaudRate** | 19200 |
| **DataBits** | 8 |
| **StopBits** | 1 |
| **Parity** | None |

DEFAULT supported capabilities in this PTZ driver:

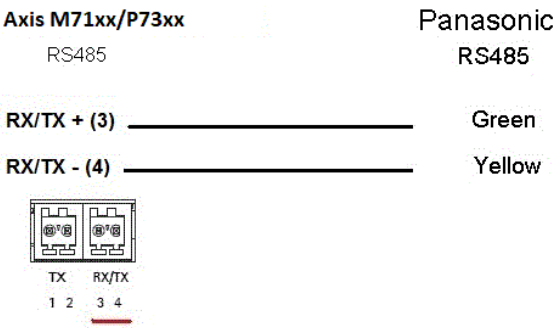
Note

Different PTZ models 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 | no |

| | |
|---|---|
| **AutoIris** | yes |
| **AutoFocus** | yes |
| **IrCutFilter** | yes |
| **BackLight** | no |
| **OSDMenu** | yes |

**Connection example**




## Pelco

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

Important

Check what serial communication the video encoder and 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** | 4.15 |

DEFAULT serial configuration:

| | |
|---|---|
| **PortMode** | RS485 |
| **BaudRate** | 2400 |
| **DataBits** | 8 |
| **StopBits** | 1 |
| **Parity** | None |

DEFAULT supported capabilities in this PTZ driver:

Note

Different PTZ models 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 example**




## Philips

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Bosch/Philips Autodome G3A
- Bosch Autodome VG4
- Bosch MIC 400
- Bosch MIC 500

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

**Technical information**

DEFAULT capabilities for PTZ driver:

| | |
|---|---|
| Driver | Philips |
| Version | 4.06 |

DEFAULT serial configuration:

| | |
|---|---|
| PortMode | RS485 |
| BaudRate | 19200 |
| DataBits | 8 |

| | |
|---|---|
| **StopBits** | 1 |
| **Parity** | None |

DEFAULT supported capabilities in this PTZ driver:

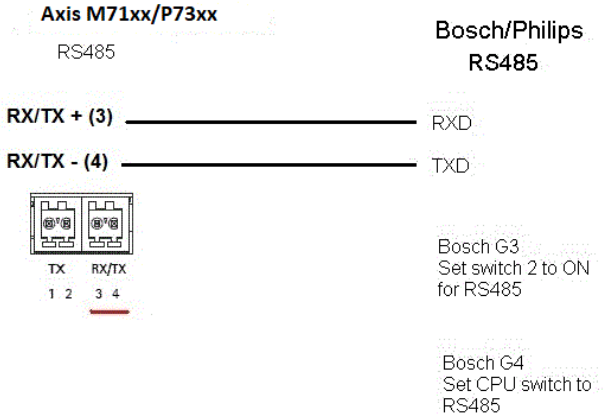
Note

Different PTZ models 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 example**




## Samsung

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Samsung SCC-643

## PTZ drivers

- Samsung SCP-2120

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

**Technical information**

DEFAULT capabilities for PTZ driver:

| | |
|---|---|
| **Driver** | Samsung |
| **Version** | 4.02 |

DEFAULT serial configuration:

| | |
|---|---|
| **PortMode** | RS485 |
| **BaudRate** | 38400 |
| **DataBits** | 8 |
| **StopBits** | 1 |
| **Parity** | None |

DEFAULT supported capabilities in this PTZ driver:

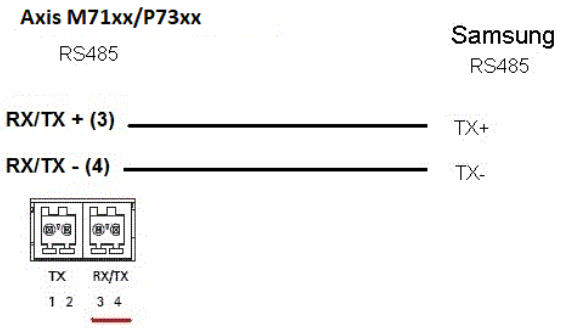
Note

Different PTZ models 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** | no |
| **AutoFocus** | yes |
| **IrCutFilter** | no |
| **BackLight** | no |
| **OSDMenu** | yes |

**Connection example**




## Sensormatic

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Sensormatic Ultra I
- Sensormatic Ultra II
- Sensormatic Ultra III
- Sensormatic Ultra V
- Sensormatic Ultra VII

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

**Technical information**

DEFAULT capabilities for PTZ driver:

| | |
|---|---|
| **Driver** | Sensormatic |
| **Version** | 4.09 |

DEFAULT serial configuration:

| | |
|---|---|
| **PortMode** | RS485 |
| **BaudRate** | 4800 |
| **DataBits** | 8 |
| **StopBits** | 1 |
| **Parity** | None |

DEFAULT supported capabilities in this PTZ driver:

Note

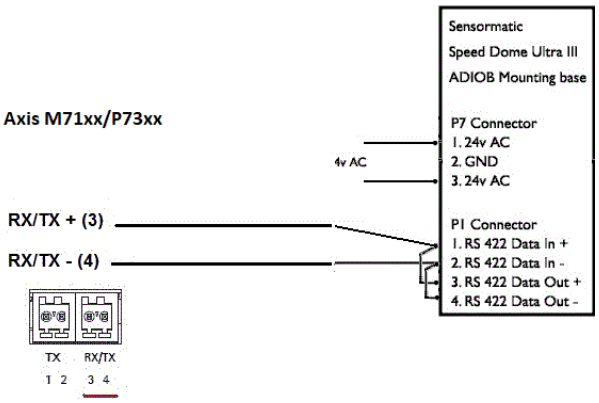
Different PTZ models may have other capabilities (both less and more).

## PTZ drivers

| 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** | no |
| **OSDMenu** | yes |

**Connection example**




## Siemens

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Siemens CCDA1435-DNX

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

## Smartscan

For more details, go to *Ultrak on page 65*.

## PTZ drivers

### Teb

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Teb TUB

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

**Technical information**

DEFAULT capabilities for PTZ driver:

| | |
|---|---|
| **Driver** | Teb |
| **Version** | 4.00 |

DEFAULT serial configuration:

| | |
|---|---|
| **PortMode** | RS422 |
| **BaudRate** | 9600 |
| **DataBits** | 8 |
| **StopBits** | 1 |
| **Parity** | None |

DEFAULT supported capabilities in this PTZ driver:

Note

Different PTZ models 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 | no |

| | |
|---|---|
| **AutoIris** | yes |
| **AutoFocus** | yes |
| **IrCutFilter** | no |
| **BackLight** | no |
| **OSDMenu** | yes |

### Ultrak

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

## PTZ drivers

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Ultrak UltraDome KD6
- Ultrak UltraDome KD6i

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

**Technical information**

DEFAULT capabilities for PTZ driver:

| | |
|---|---|
| **Driver** | Ultrak |
| **Version** | 4.04 |

DEFAULT serial configuration:

| | |
|---|---|
| **PortMode** | RS485 |
| **BaudRate** | 9600 |
| **DataBits** | 8 |
| **StopBits** | 1 |
| **Parity** | Even |

DEFAULT supported capabilities in this PTZ driver:

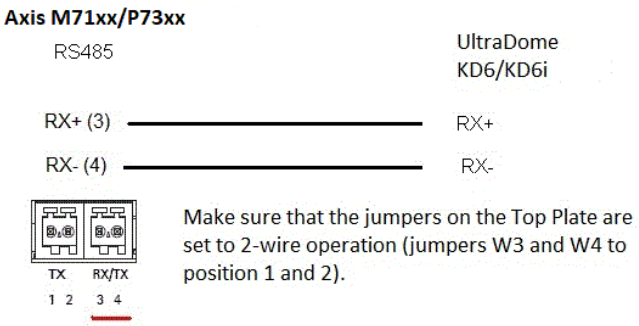
Note

Different PTZ models 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 | no | no | no |
| Iris | no | no | no |

| | |
|---|---|
| **AutoIris** | yes |
| **AutoFocus** | yes |
| **IrCutFilter** | yes |
| **BackLight** | yes |
| **OSDMenu** | no |

Connection example




## VCC

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Canon VC-C4
- Canon VC-C4R
- Canon VC-C50i
- Canon VC-C50iR
- Canon NU-700N
- Canon NU-700P
- Canon NU-701N
- Canon NU-701P
- Canon BU-45H
- Canon BU-50H

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

## VCL

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Vcl Orbiter MicroSphere
- Vcl Orbiter Gold

## PTZ drivers

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

**Technical information**

DEFAULT capabilities for PTZ driver:

| | |
|---|---|
| **Driver** | Vcl_rel |
| **Version** | 4.04 |

DEFAULT serial configuration:

| | |
|---|---|
| **PortMode** | RS485 |
| **BaudRate** | 9600 |
| **DataBits** | 8 |
| **StopBits** | 2 |
| **Parity** | None |

DEFAULT supported capabilities in this PTZ driver:

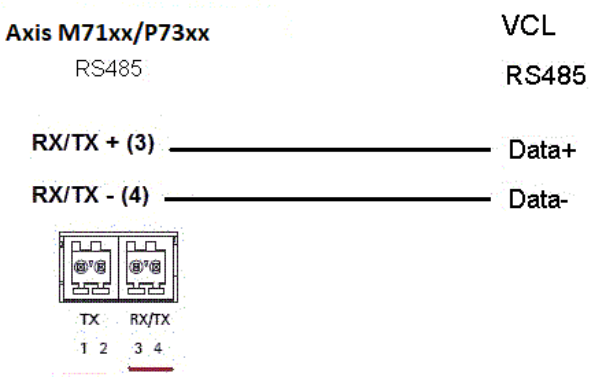
Note

Different PTZ models 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** | no |
| **OSDMenu** | no |

**Connection example**




## Vicon

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Vicon SVFT-W23

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

**Technical information**

DEFAULT capabilities for PTZ driver:

| | |
|---|---|
| **Driver** | Vicon |
| **Version** | 4.05 |

DEFAULT serial configuration:

| | |
|---|---|
| **PortMode** | RS485 |
| **BaudRate** | 19200 |
| **DataBits** | 8 |
| **StopBits** | 1 |
| **Parity** | None |

DEFAULT supported capabilities in this PTZ driver:

Note

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

| Movement | Absolute | Relative | Continuous |
|---|---|---|---|
| Pan | no | yes | yes |
| Tilt | no | yes | yes |

| Movement | Absolute | Relative | Continuous |
|---|---|---|---|
| Zoom | no | yes | yes |
| Focus | no | yes | yes |
| Iris | no | no | no |

| | |
|---|---|
| **AutoIris** | no |
| **AutoFocus** | no |
| **IrCutFilter** | no |
| **BackLight** | no |
| **OSDMenu** | yes |

## Videmech

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Videmech 682
- Videmech 555RX

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

**Technical information**

DEFAULT capabilities for PTZ driver:

| | |
|---|---|
| **Driver** | Videmech |
| **Version** | 4.06 |

DEFAULT serial configuration:

| | |
|---|---|
| **PortMode** | RS485 |
| **BaudRate** | 9600 |
| **DataBits** | 8 |
| **StopBits** | 1 |
| **Parity** | Odd |

DEFAULT supported capabilities in this PTZ driver:

Note

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

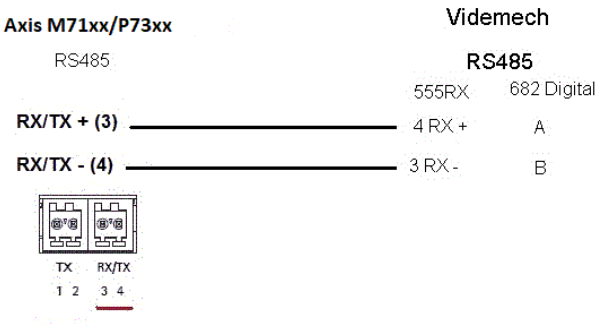
| Movement | Absolute | Relative | Continuous |
|---|---|---|---|
| Pan | yes | yes | yes |
| Tilt | yes | yes | yes |

## PTZ drivers

| Movement | Absolute | Relative | Continuous |
|---|---|---|---|
| Zoom | yes | yes | yes |
| Focus | yes | yes | yes |
| Iris | no | no | no |

| | |
|---|---|
| **AutoIris** | no |
| **AutoFocus** | no |
| **IrCutFilter** | no |
| **BackLight** | no |
| **OSDMenu** | no |

**Connection example**




### Videotec

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Videotec DTMRX2

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

### Videotec Macro

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

Important

Check what serial communication the video encoder and PTZ unit will support.

Supported models:

- Videotec ULISSE

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

## PTZ drivers

### Visca

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

Important

Check what serial communication the video encoder and 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:

Note

Different PTZ models 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 |

## PTZ drivers

| | |
|---|---|
| AutoIris | yes |
| AutoFocus | yes |
| IrCutFilter | yes |
| BackLight | yes |
| OSDMenu | no |

User Manual
AXIS P7316 Video Encoder
© Axis Communications AB, 2021 - 2022
Ver. M4.3
Date: October 2022
Part No. T10156402