AXIS P5415-E PTZ Dome Network Camera

User Manual

About this Document

This manual is intended for administrators and users of AXIS P5415-E PTZ Dome Network Camera, and is applicable to firmware 6.50 and later. It includes instructions for using and managing the product on your network. Previous experience of networking will be of use when using this product. Some knowledge of UNIX or Linux-based systems may also be useful when developing shell scripts and applications. Later versions of this document will be posted at *www.axis.com* See also the product's online help, available through the web-based interface.

Legal considerations

Video and audio surveillance can be regulated by laws that vary from country to country. Check the laws in your local region before using this product for surveillance purposes.

This product includes the following licences:

- one (1) AAC decoder license
- one (1) H.264 decoder license

To purchase further licenses, contact your reseller.

Liability

Every care has been taken in the preparation of this document. Please inform your local Axis office of any inaccuracies or omissions. Axis Communications AB cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. Axis Communications AB makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Axis Communications AB shall not be liable nor responsible for incidental or consequential damages in connection with the furnishing, performance or use of this material. This product is only to be used for its intended purpose.

Intellectual property rights

Axis AB has intellectual property rights relating to technology embodied in the product described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the patents listed at *www.axis.com/patent.htm* and one or more additional patents or pending patent applications in the US and other countries.

This product contains licensed third-party software. See the menu item "About" in the product's user interface for more information.

This product contains source code copyright Apple Computer, Inc., under the terms of Apple Public Source License 2.0 (see *www.opensource.apple.com/apsl*). The source code is available from *https://developer.apple.com/bonjour/*

Equipment modifications

This equipment must be installed and used in strict accordance with the instructions given in the user documentation. This equipment contains no user-serviceable components. Unauthorized equipment changes or modifications will invalidate all applicable regulatory certifications and approvals.

Trademark acknowledgments

AXIS COMMUNICATIONS, AXIS and VAPIX are registered trademarks or trademark applications of Axis AB in various jurisdictions. All other company names and products are trademarks or registered trademarks of their respective companies.

Apple, Boa, Apache, Bonjour, Ethernet, Internet Explorer, Linux, Microsoft, Mozilla, Real, SMPTE, QuickTime, UNIX, Windows, Windows Vista and WWW are registered trademarks of the respective holders. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates. UPnP™ is a certification mark of the UPnP™ Implementers Corporation.

SD, SDHC and SDXC are trademarks or registered trademarks of SD-3C, LLC in the United States, other countries or both. Also, miniSD, microSD, miniSDHC, microSDHC, microSDXC are all trademarks or registered trademarks of SD-3C, LLC in the United States, other countries or both.

Regulatory information

Europe

ϵ This product complies with the applicable CE marking directives and harmonized standards:

- Electromagnetic Compatibility (EMC) Directive 2014/30/EU. See *Electromagnetic compatibility (EMC) on page 2* .
- Low Voltage (LVD) Directive 2014/35/EU. See *Safety on page 3* .
- Restrictions of Hazardous Substances (RoHS) Directive 2011/65/EU. See *Disposal and recycling on page 3* .

A copy of the original declaration of conformity may be obtained from Axis Communications AB. See *Contact information on page 3* .

Electromagnetic compatibility (EMC)

This equipment has been designed and tested to fulfill applicable standards for:

- Radio frequency emission when installed according to the instructions and used in its intended environment.
- Immunity to electrical and electromagnetic phenomena when installed according to the instructions and used in its intended environment.

USA

This equipment has been tested using a shielded network cable (STP) and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The product shall be connected using a shielded network cable (STP) that is properly grounded.

Canada

This digital apparatus complies with CAN ICES-3 (Class B). The product shall be connected using a shielded network cable (STP) that is properly grounded. Cet appareil numérique est conforme à la norme CAN NMB-3 (classe B). Le produit doit être connecté à l'aide d'un câble réseau blindé (STP) qui est correctement mis à la terre.

Europe

This digital equipment fulfills the requirements for RF emission according to the Class B limit of EN 55022. The product shall be connected using a shielded network cable (STP) that is properly grounded.

This product fulfills the requirements for immunity according to EN 61000-6-1 residential, commercial and light-industrial environments.

This product fulfills the requirements for immunity according to EN 61000-6-2 industrial environments.

This product fulfills the requirements for immunity according to EN 55024 office and commercial environments.

Australia/New Zealand

This digital equipment fulfills the requirements for RF emission according to the Class B limit of AS/NZS CISPR 22. The product shall be connected using a shielded network cable (STP) that is properly grounded.

Japan

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。本製品は、シールドネットワークケーブル(STP)を使用して接続してください。また適切に接地してください。

Safety

This product complies with IEC/EN/UL 60950-1 and IEC/EN/UL 60950-22, Safety of Information Technology Equipment. The product shall be grounded either through a shielded network cable (STP) or other appropriate method.

The power supply used with this product shall fulfill the requirements for Safety Extra Low Voltage (SELV) according to clause 2.2 of IEC/UL 60950-1 and Limited Power Source (LPS) according to clause 2.5 of IEC/UL 60950-1 or CEC/NEC Class 2 source of supply as defined in the Canadian Electrical Code, CSA C22.1 and National Electrical Code, ANSI/NFPA 70.

Battery

The Axis product uses a 3.0 V BR2032 lithium battery as the power supply for its internal real-time clock (RTC). Under normal conditions this battery will last for a minimum of five years.

Low battery power affects the operation of the RTC, causing it to reset at every power-up. When the battery needs replacing, a log message will appear in the product's server report. For more information about the server report, see the product´s setup pages or contact Axis support.

The battery should not be replaced unless required, but if the battery does need replacing, contact Axis support at *www.axis.com/support* for assistance.

Lithium coin cell 3.0 V batteries contain 1,2-dimethoxyethane; ethylene glycol dimethyl ether (EGDME), CAS no. 110-71-4.

⚠WARNING

- Risk of explosion if the battery is incorrectly replaced.
- Replace only with an identical battery or a battery which is recommended by Axis.
- Dispose of used batteries according to local regulations or the battery manufacturer's instructions.

Disposal and recycling

When this product has reached the end of its useful life, dispose of it according to local laws and regulations. For information about your nearest designated collection point, contact your local authority responsible for waste disposal. In accordance with local legislation, penalties may be applicable for incorrect disposal of this waste.

Europe

This symbol means that the product shall not be disposed of together with household or commercial waste. Directive 2012/19/EU on waste electrical and electronic equipment (WEEE) is applicable in the European Union member states. To prevent potential harm to human health and the environment, the product must be disposed of in an approved and environmentally safe recycling process. For information about your nearest designated collection point, contact your local authority responsible for waste disposal. Businesses should contact the product supplier for information about how to dispose of this product correctly.

This product complies with the requirements of Directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS).

China

This product complies with the requirements of SJ/T 11364-2014, Marking for the restriction of hazardous substances in electrical and electronic products.

有毒有害物质或元素						
部件名称	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr(VI))	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
电气实装部分	X	O	O	O	O	O

O: 表示该有毒有害物质在该部件所有均质材料中的含量均在GB/T 26572标准规定的限量要求以下。

X: 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出GB/T 26572标准规定的限量要求。

Support

Should you require any technical assistance, please contact your Axis reseller. If your questions cannot be answered immediately, your reseller will forward your queries through the appropriate channels to ensure a rapid response. If you are connected to the Internet, you can:

- download user documentation and software updates
- find answers to resolved problems in the FAQ database. Search by product, category, or phrase
- report problems to Axis support staff by logging in to your private support area
- chat with Axis support staff
- visit Axis Support at *www.axis.com/support*

Warranty information

For information about Axis' product warranty and thereto related information, go to *www.axis.com/warranty/*

Learn more!

Visit Axis learning center *www.axis.com/academy/* for useful trainings, webinars, tutorials and guides.

AXIS P5415-E PTZ Dome Network Camera

Table of Contents

Table of Contents

Safety information

Hazard levels

⚠DANGER

Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

⚠WARNING

Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

⚠CAUTION

Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE

Indicates a situation which, if not avoided, could result in damage to property.

Other message levels

Important

Indicates significant information which is essential for the product to function correctly.

Note

Indicates useful information which helps in getting the most out of the product.

Hardware overview

Hardware overview

For specifications of the hardware components, see *Technical specifications on page 62.*
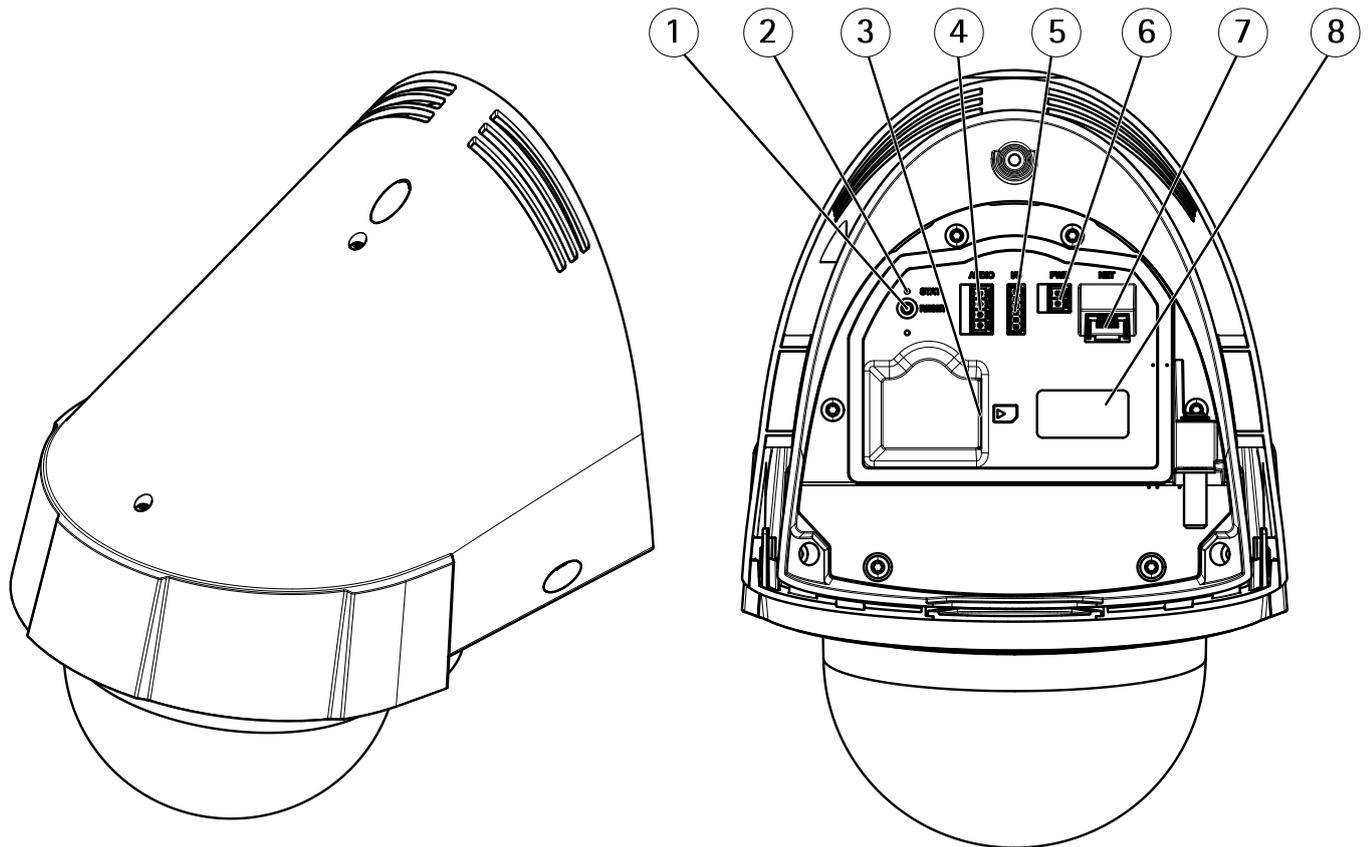
1   *Control button*
2   *Status LED indicator*
3   *SD memory card slot*
4   *Audio connector*
5   *I/O connector*
6   *Power connector*
7   *Network connector (PoE+)*
8   *Part number (P/N) & Serial number (S/N)*

To install the Axis product, see the Installation Guide supplied with the product.

The product can be used with most operating systems and browsers. We recommend the following browsers:

- Internet Explorer® with Windows®

- Safari® with OS X®

- Chrome™ or Firefox® with other operating systems.

To view streaming video in Internet Explorer, allow installation of AXIS Media Control (AMC) when prompted.

The Axis product includes one (1) H.264 decoder license for viewing video streams and one (1) AAC audio license. The licenses are automatically installed with AMC. The administrator can disable the installation of the decoders to prevent installation of unlicensed copies.

Note

- QuickTime™ is also supported for viewing H.264 streams and for audio.

How to access the product from a browser

1. Start a web browser.

2. Enter the IP address or host name of the Axis product in the browser's address field.

    To access the product from a Mac computer (OS X), go to Safari, click on Bonjour and select the product from the drop-down list.

    If you do not know the IP address, use AXIS IP Utility to locate the product on the network. For information about how to discover and assign an IP address, see the document *Assign an IP Address and Access the Video Stream* on Axis Support web at *www.axis.com/support*

Note

To show Bonjour as a browser bookmark, go to **Safari > Preferences**.

3. Enter your username and password. If this is the first time the product is accessed, the root password must first be configured.

4. The product's live view page opens in your browser.

Note

The controls and layout of the live view page may have been customized to meet specific installation requirements and user preferences. Consequently, some of the examples and functions featured here may differ from those displayed in your own live view page.

How to access the product from the Internet

Once connected, the Axis product is accessible on your local network (LAN). To access the product from the Internet you must configure your network router to allow incoming data traffic to the product. To do this, enable the NAT-traversal feature, which will attempt to automatically configure the router to allow access to the product. This is enabled from **Setup > System Options > Network > TCP/IP Advanced**.

For more information, see *NAT traversal (port mapping) for IPv4 on page 49.* See also AXIS Internet Dynamic DNS Service at *www.axiscam.net*

For Technical notes on this and other topics, visit the Axis Support web at *www.axis.com/support*

How to set the root password

To access the Axis product, you must set the password for the default administrator user **root**. This is done in the **Configure Root Password** dialog, which opens when the product is accessed for the first time.

To prevent network eavesdropping, the root password can be set via an encrypted HTTPS connection, which requires an HTTPS certificate. HTTPS (Hypertext Transfer Protocol over SSL) is a protocol used to encrypt traffic between web browsers and servers. The HTTPS certificate ensures encrypted exchange of information. See *HTTPS on page 44.*

The default administrator user name **root** is permanent and cannot be deleted. If the password for root is lost, the product must be reset to the factory default settings. See *How to reset to factory default settings on page 55.*

To set the password via a standard HTTP connection, enter it directly in the dialog.

To set the password via an encrypted HTTPS connection, follow these steps:

1. Click **Use HTTPS**.

   A temporary certificate (valid for one year) is created, enabling encryption of all traffic to and from the product, and the password can now be set securely.

2. Enter a password and then re-enter it to confirm the spelling.

3. Click **OK**. The password has now been configured.

About the live view window

The controls and layout of the live view window may have been customized to meet specific installation requirements and user preferences. Consequently, some of the examples and functions featured here may differ from those displayed in your own live view window. The following provides an overview of each available control.

About the controls in the live view window

Click the **View size** buttons to show the image in full size (right button) or to scale down the image to fit the browser window (left button).
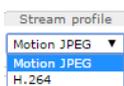
Select a stream profile for the live view window from the **Stream Profile** drop-down list. For information about how to configure stream profiles, see *page 18*.

Click **Pulse** to activate the product's output port for a defined period of time. For information about how to enable and configure output buttons, see *page 26*. The output button name may differ depending on the name entered in the I/O Ports configuration.

Click the **Active/Inactive** buttons to manually activate and inactive the product's output port. For information about how to enable and configure output buttons, see *page 26*.

Use the **Manual Trigger** button to trigger an action rule from the live view window. For information about how to configure and enable the button, see *About the manual trigger on page 10*.

Click **Snapshot** to save a snapshot of the video image. This button is primarily intended for use when the AXIS Media Control viewer toolbar is not available. Enable this button from **Live View Config > Action Buttons**.

How to access the product

The **Audio clip** drop-down list allows you to play an audio clip from the live view window. Select the audio clip and click the **Play** button.

Enable or disable the **Gatekeeper** by selecting On or Off from the drop-down list. For more information about the Gatekeeper, see *page 28*.

About the manual trigger

The **Manual Trigger** is used to trigger an action rule from the Live View page. The manual trigger can for example be used to validate actions during product installation and configuration.

To configure the manual trigger:

1. Go to **Setup > Events**.

2. Click **Add** to add a new action rule.

3. From the **Trigger** drop-down list, select **Input Signal**.

4. From the second drop-down list, select **Manual Trigger**.

5. Select the desired action and configure the other settings as required.

For more information about action rules, see *About events on page 35*.

To show the manual trigger buttons in the Live View page:

1. Go to **Setup > Live View Config**.

2. Under **Action Buttons**, select **Show manual trigger button**.

About the AXIS Media Control viewer toolbar

The AXIS Media Control viewer toolbar is available in Internet Explorer only. See *About AXIS Media Control (AMC) on page 12* for more information. The toolbar displays the following buttons:

The **Play** button connects to the Axis product and starts playing a media stream.

The **Stop** button stops the media stream.

The **Snapshot** button takes a snapshot of the video image.

Click the **View Full Screen** button and the video image will fill the entire screen. Press ESC (Escape) on the computer keyboard to cancel full screen view.

The **Record** button is used to record the current video stream on your computer. The location where the recording is saved can be specified in the AMC Control Panel. Enable this button from **Live View Config** > **Viewer Settings.**

AMC Audio Controls

AMC audio buttons control the speakers and microphone connected to the client computer. The buttons are only visible when audio is enabled.

For information about how to configure audio, see *How to change audio settings on page 22*.

Speaker button — Click to turn the speakers on or off.

Microphone button – Click to mute or unmute the microphone. In *Simplex - speaker only mode*, the **Microphone** and **Talk** buttons must both be active to send audio to the Axis product. Click either button to stop audio transmission.

Use the slider to control the volume of the speakers and the microphone.

Half-duplex mode
The **Talk/Listen button** is used to switch between sending and receiving audio. The button can be configured from the Audio tab in the AMC Control panel:
* Push-To-Talk mode: Click and hold the button to talk/send. Release the button to listen.
* Toggle mode: Click once to switch between talking and listening.

Simplex – speaker only mode
To send audio, the **Talk** and **Microphone** buttons must both be active. Click either button to stop audio transmission.

PTZ Controls

The live view window also displays Pan/Tilt/Zoom (PTZ) controls. The administrator can enable/disable controls for specified users under **System Options > Security > Users**.

With the **PTZ Control Queue** enabled the time each user is in control of the PTZ settings is limited. Click the buttons to request or release control of the PTZ controls. The PTZ Control Queue is set up under **PTZ > Control Queue**.

Select **Focus window** to define an area of the camera's image that focus should be applied on. If the focus window is set from the live view window, any change in the camera position will return the autofocus to the entire window. To set a permanent focus window, see *About preset positions on page 27*

Click the **Emulate joystick mode** button and click in the image to move the camera view in the direction of the mouse pointer.

Click the **Center mode** button and click in the image to center the camera view on that position.

The center mode button could also be used to zoom in on a specific area. Click in the image and drag to draw a rectangle surrounding the area to be magnified. To zoom out, rotate the mouse wheel.
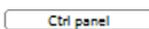
Click the **Ctrl panel** button to open the PTZ control panel which provides additional PTZ controls. User-defined buttons can also appear in the Control panel. See *About advanced PTZ settings on page 30*.
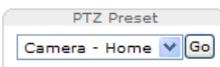
Select a PTZ preset position to steer the camera view to the saved position. See *About preset positions on page 27*.

Pan and Tilt bars – Use the arrows to pan and tilt the camera view, or click on a position on the bar to steer the camera view to that position.

Zoom bar – Use the arrows to zoom in and out, or click on a position on the bar to zoom to that position.

Focus bar – Use the arrows to focus the camera, or click on a position on the bar to set the focus position. Using the focus bar will disable the product's autofocus. To re-enable, use the PTZ control panel which is opened by clicking the **Ctrl panel** button (see above).

The PTZ controls can be disabled under **PTZ > Advanced > Controls**, see *About advanced PTZ settings on page 30*.

About media streams

The Axis product provides several audio and video stream formats. Your requirements and the properties of your network will determine the type you use.

The live view window in the product provides access to H.264 and Motion JPEG video streams, audio streams and to the list of available stream profiles. Other applications and clients can access video and audio streams directly, without going via the live view window.

About H.264 format

H.264 can, without compromising image quality, reduce the size of a digital video file by more than 80% compared with the Motion JPEG format and as much as 50% more than the MPEG-4 standard. This means that much less network bandwidth and storage space are required for a video file. Or seen another way, much higher video quality can be achieved for a given bit rate.

Deciding which combination of protocols and methods to use depends on your viewing requirements, and on the properties of your network. The available options in AXIS Media Control are:

Unicast RTP	This unicast method (RTP over UDP) is used for live unicast video, especially when it is important to have an up-to-date video stream, even if some frames are dropped.	Unicasting is used for video-on-demand transmission so that there is no video traffic on the network until a client connects and requests the stream. Note that there are a maximum of 20 simultaneous unicast connections.
RTP over RTSP	This unicast method (RTP tunneled over RTSP) is useful as it is relatively simple to configure firewalls to allow RTSP traffic.	
RTP over RTSP over HTTP	This unicast method can be used to traverse firewalls. Firewalls are commonly configured to allow the HTTP protocol, thus allowing RTP to be tunneled.	
Multicast RTP	This method (RTP over UDP) should be used for live multicast video. The video stream is always up-to-date, even if some frames are dropped. Multicasting provides the most efficient usage of bandwidth when there are large numbers of clients viewing simultaneously. A multicast cannot however, pass a network router unless the router is configured to allow this. It is not possible to multicast over the Internet, for example. Note also that all multicast viewers count as one unicast viewer in the maximum total of 20 simultaneous connections.	

AXIS Media Control negotiates with the Axis product to determine the transport protocol to use. The order of priority, listed in the AMC Control Panel, can be changed and the options disabled, to suit specific requirements.

Note

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

About MJPEG format

This format uses standard JPEG still images for the video stream. These images are then displayed and updated at a rate sufficient to create a stream that shows constantly updated motion.

The Motion JPEG stream uses considerable amounts of bandwidth, but provides excellent image quality and access to every image contained in the stream. The recommended method of accessing Motion JPEG live video from the Axis product is to use the AXIS Media Control in Internet Explorer in Windows.

About AXIS Media Control (AMC)

AXIS Media Control (AMC) in Internet Explorer in Windows is the recommended method of accessing live video from the Axis product.

About media streams

The AMC Control Panel can be used to configure various video and audio settings. Please see the AXIS Media Control User's Manual for more information.

The AMC Control Panel is automatically installed on first use, after which it can be configured. Open the AMC Control Panel from:

- Windows Control Panel (from the Start screen or Start menu)

- Alternatively, right-click the video image in Internet Explorer and click **Settings**.
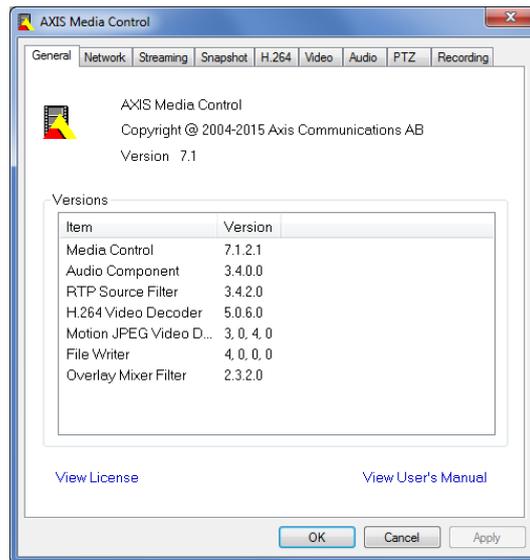
Alternative methods of accessing the video stream

You can also access video and images from the Axis product in the following ways:

- **Motion JPEG server push** (if supported by the client, Chrome or Firefox, for example). This option maintains an open HTTP connection to the browser and sends data as and when required, for as long as required.

- **Still JPEG images in a browser**. Enter the path `http://<ip>/axis-cgi/jpg/image.cgi`

- **Windows Media Player**. This requires AXIS Media Control and the H.264 decoder to be installed. The following paths can be used:

    - Unicast via RTP: `axrtpu://<ip>/axis-media/media.amp`

    - Unicast via RTSP: `axrtsp://<ip>/axis-media/media.amp`

    - Unicast via RTSP, tunneled via HTTP: `axrtsphttp://<ip>/axis-media/media.amp`

    - Multicast: `axrtpm://<ip>/axis-media/media.amp`

- **QuickTime**^{TM}. The following paths can be used:

    - `rtsp://<ip>/axis-media/media.amp`

    - `rtsp://<ip>/axis-media/media.3gp`

About media streams

Note
- `<ip>`= IP address
- The Axis product supports QuickTime 6.5.1 and later.
- QuickTime may add latency to the video stream.
- It may be possible to use other players to view the H.264 stream using the paths above, although Axis does not guarantee this.

Access Audio Streams

The Live View page provides access to audio through AXIS Media Control; in addition audio can be accessed in the following ways:

- **VAPIX® Application Programming Interface (API)** For more information, visit www.axis.com/developer

- **Windows Media Player** supports simplex audio. The following paths can be used:

    - Unicast via RTP: `axrtpu://<ip>/axis-media/media.amp`

    - Unicast via RTSP: `axrtsp://<ip>/axis-media/media.amp`

    - Unicast via RTSP, tunneled via HTTP: `axrtsphttp://<ip>/axis-media/media.amp`

    - Multicast: `axrtpm://<ip>/axis-media/media.amp`

- **QuickTime**^{TM} supports G.711 and AAC audio encoding. The following paths can be used:

    - `rtsp://<ip>/axis-media/media.amp`

    - `rtsp://<ip>/axis-media/media.3gp`

How to set up the product

The Axis product can be configured by users with administrator or operator rights. To open the product's setup pages, click **Setup** in the top right-hand corner of the live view window.

- **Administrators** have unrestricted access to all settings.

- **Operators** have restricted access to settings, see *Users on page 43*

See also the online help .

How to perform a basic setup

Basic Setup provides shortcuts to the settings that should be made before using the Axis product:

1. Users. See *page 43*.

2. TCP/IP. See *page 46*.

3. Date & Time. See *page 45*.

4. Video Stream. See *page 16*.

5. Audio Settings. See *page 22*.

The Basic Setup menu can be disabled from **System Options > Security > Users**.

Video and Audio

The video and audio settings can be used to optimize video and audio quality. You can configure the following:

- Video stream settings. See *page 16*.
- Stream profiles. See *page 18*.
- ONVIF Media Profiles. See *page 18*.
- Camera settings. See *page 18*.
- Overlay image. See *page 20*.
- Privacy mask. See *page 22*.
- Audio settings. See *page 22*.
- Audio clips. See *page 24*.

How to set up video streams

To set up the product's video streams, go to **Video & Audio** > **Video Stream**.

The video stream settings are divided into the following tabs:

- Image. See *page 16*.
- Audio. See *page 22*.
- H.264. See *page 17*.
- MJPEG. See *page 18*.

About the pixel counter

The pixel counter shows the number of pixels in an area of the image. The pixel counter is useful in situations where there is a specific size requirement, for example in face recognition.

The pixel counter can be used:

- When setting up a video stream, see *How to set up video streams on page 16*. Under **Preview**, click **Open** and select the **Show pixel counter** option to enable the rectangle in the image. Use the mouse to move and resize the rectangle, or enter the number of pixels in the **Width** and **Height** fields and click **Apply**.
- When accessing the Live View page in Internet Explorer with AXIS Media Control (AMC) in Windows. Right-click in the image and select **Pixel counter**. Use the mouse to move and resize the rectangle.

Image

The default image settings can be configured under **Video & Audio > Video Stream**. Select the **Image** tab.

The following settings are available:

- **Resolution**. Select the default resolution.
- **Compression**. The compression level affects the image quality, bandwidth and file size of saved images; the lower the compression, the higher the image quality with higher bandwidth requirements and larger file sizes.
- **Rotate image**. If required, the image can be rotated.

- **Maximum frame rate**. To avoid bandwidth problems, the frame rate allowed to each viewer can be **Limited to** a fixed amount. Alternatively, the frame rate can be set as **Unlimited**, which means the Axis product always delivers the highest frame rate possible under the current conditions.

- **Overlay settings**. See *About overlay text on page 20*.

Click **Save** to apply the new settings.

About H.264

H.264, also known as MPEG-4 Part 10/AVC, is a video compression standard that provides high quality video streams at low bitrates. An H.264 video stream consists of different types of frames such as I-frames and P-frames. An I-frame is a complete image, whereas P-frames only contain the differences from previous frames.

About GOP length

A Group of Pictures (GOP) contains one I-frame followed by a number of P-frames. The GOP length is the number of frames between two I-frames.

Equal values for GOP length and frame rate result in one GOP per second. A higher GOP length value results in more small-sized P-frames and fewer large-sized I-frames while keeping the same frame rate. In other words, a high GOP-length value saves bandwidth, but the video quality may decrease. A low GOP-length value increases the video quality but requires more bandwidth.

About H.264 profiles

The Axis product supports the following **H.264 profile(s)**:

- **Baseline**: Use the Baseline profile if the client does not support CABAC entropy coding.

- **Main**: The Main profile uses CABAC and provides a better compression with maintained video quality. It requires a larger amount of processing power to decode than the Baseline profile.

About bitrate control

Bitrate control is useful to make sure the video streaming does not take up too much bandwidth.

About variable bitrate

Variable bitrate (VBR) adjusts the bitrate according to the image complexity. When the activity in the scene increases, VBR adjusts the bitrate according to the complexity, using up more bandwidth for increased activity in the scene, and less for lower scene activity. Variable bitrate is suitable if there is a surplus in bandwidth, where the increased bitrate may not be an issue.

About maximum bitrate

If you have limited bandwidth, we recommend Maximum bit rate (MBR). MBR allows you to set a target bitrate to control the bandwidth consumption. The target value limits the bitrate, but it maintains a flexibility to be able to prioritize a continuous video stream. Consequently, the frame rate might need to go down and the image quality might decrease. To partly compensate for this, you can select which variable shall be prioritized. Not setting a priority means that frame rate and image quality are equally affected.

How to set an H.264 profile

1. To change the settings for all H.264 streams that do not use a stream profile, go to **Video & Audio > Video Stream > H.264**.

2. To increase or decrease the number of frames per GOP, set the **GOP length**.

3. Select one of the H.264 profiles.

4. Select one of the following:

   - **Variable bit rate**

- Maximum bit rate

5. If you select **Maximum bit rate**, select which variable to prioritize in the **Priority** drop-down list.

6. Click **Save**.

How to include current bitrate in a text overlay

1. Go to **Video & Audio > Video Stream > Overlay Settings**.

2. In the **Include text** field enter #b.

3. Click **Save**.

About MJPEG settings

Sometimes the image size is large due to low light or complex scenery. Adjusting the maximum frame size helps to control the bandwidth and storage used by the Motion JPEG video stream in these situations. Setting the frame size to the **Default** setting provides consistently good image quality at the expense of increased bandwidth and storage usage in low light. Limiting the frame size optimizes bandwidth and storage usage, but may result in poor image quality.

About stream profiles

A stream profile is a set of predefined stream settings including resolution, compression, frame rate and overlay settings. Stream profiles can be used:

- When setting up recording using action rules. See *About events on page 35*.

- When setting up continuous recording. See *About continuous recording on page 41*.

- In the Live View page – select the stream profile from the **Stream profile** drop-down list.

To create a new profile or modify an existing profile, go to **Setup > Video & Audio > Stream Profiles**.

To select a default stream profile for the Live View page, go to **Setup > Live View Config**.

About ONVIF media profiles

An ONVIF media profile consists of a set of configurations that can be used to change media stream settings. ONVIF media profiles can be used by a client to configure media stream properties.

The **ONVIF Media Profiles** page lists all preconfigured profiles. These profiles are included in the product for quick setup. You can add, modify or remove ONVIF media profiles from this page.

About camera settings

The **Video & Audio > Camera Settings** page provides access to advanced image settings for the Axis product.

About image appearance

To change Image Appearance go to the menus under **Setup > Video & Audio > Camera Settings**.

Increasing the **Color level** increases the color saturation. The value 100 produces maximum color saturation and the value 0 results in a black and white image.

The image **Brightness** can be adjusted in the range 0–100, where a higher value produces a brighter image.

Increasing the **Sharpness** can increase bandwidth usage. A sharper image might increase image noise especially in low light conditions. A lower setting reduces image noise, but the whole image will appear less sharp.

The **Contrast** changes the relative difference between light and dark. It can be adjusted using the slidebar.

About white balance

To change this setting go to **Setup > Video & Audio > Camera Settings**

White balance is used to make colors in the image appear the same regardless of the color temperature of the light source. The Axis product can be set to automatically identify the light source and compensate for its color. Alternatively, select the type of light source from the drop-down list. For a description of each available setting, see the online help .

The **white balance window** is enabled for the Automatic and Automatic outdoor options that appear in the **White balance** drop-down list. Select one of the options from the drop-down list to set the white balance window properties. Select **Automatic** to use the default settings for the Automatic and Automatic outdoor options (in the White balance drop-down list). Select **Custom** to manually set a reference window for white balance in the view area.

Wide Dynamic Range

Wide dynamic range (**Dynamic Contrast**) can improve the exposure when there is a considerable contrast between light and dark areas in the image. Enable WDR in intense backlight conditions. Disable WDR in low light conditions for optimal exposure.

> **Note**
>
> This setting is only possible when using automatic exposure control.

Exposure Settings

Exposure is the amount of light the camera's sensor captures for a scene. Too much light results in a washed out image and too little light results in a dark image.

Exposure value – Use the **Exposure value** slider to adjust the overall brightness of the image.

Max exposure time – Shutter speed, also called 'exposure time', stands for the length of time the camera shutter is open, thereby exposing the camera sensor to light. If shutter speed is fast it can freeze action effectively. If shutter speed is slow, it can cause moving objects to appear blurred. Decreasing the exposure time will reduce motion blur.

Enable Backlight compensation – Enable this option if a bright spot of light, such as a light bulb, causes other areas in the image to appear too dark.

Exposure zones – This setting determines which part of the image is used to calculate the exposure. For most situations, the **Auto** setting can be used.
You can select a predefined area by defining Include and Exclude windows within the image. Exclude windows exclude areas that are too bright or dark, and Include windows include areas in the scene that have better lighting which will contribute to the exposure data. There must be at least one Include window. There can be a total of ten Include and Exclude windows to tailor the exposure zone. Note that an Exclude window is effective only when placed inside an include window.
Tip: If an area is extremely bright, draw an Include window to cover the whole area and define Exclude windows within it to block out the bright areas.

Shutter & Gain

The shutter and gain settings affect the amount of motion blur and noise in the image. To adapt to different lighting conditions, available storage space and bandwidth, it is often necessary to prioritize either low motion blur or low noise. The Axis product allows different prioritizations in normal and low light.

Shutter speed is related to the amount of time the shutter is opened and is measured in seconds (s). A slow shutter speed allows more light to reach the sensor and can help produce a brighter image in low light. On the other hand, a slow shutter speed can cause moving objects to appear blurry.

Set **Shutter** to:

- **Auto** to set the shutter speed automatically. If required, use **Max shutter** to limit the shutter speed to prevent the frame rate from being reduced.

For example, to get 30 fps, set **Max shutter** to 1/30.

- **Fixed** to use a fixed shutter speed.

Gain, measured in decibel (dB), is the amount of amplification applied to the image. A high gain may provide a better image in low light but will increase the amount of image noise.

Set **Gain** to:

- **Auto** to set the gain automatically. If required, use **Max gain** to limit the applied gain.

- **Fixed** to use a fixed gain.

Example

If storage space or bandwidth is limited, try using a lower gain. This will reduce image noise and produce smaller image files.

Day/Night

The IR cut filter prevents infrared (IR) light from reaching the image sensor. In poor lighting conditions, for example at night, or when using an external IR lamp, set the IR cut filter to **Off**. This increases light sensitivity and allows the product to "see" infrared light. The image is shown in black and white when the IR cut filter is off.

If using automatic **Exposure control**, set the IR cut filter to **Auto** to automatically switch between **On** and **Off** according to the lighting conditions.

About 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.

About overlay text

An overlay text can include the current date and time, or a text string. When using a text string, so-called modifiers can be used to display, for example, the current bit rate or the current frame rate.

You can choose between the following text overlay sizes:

Size	Text height	Background height
Small	10 pixels	20 pixels
Medium	16 pixels	28 pixels
Large	21 pixels	36 pixels

It is also possible to display text when an action rule is triggered, see *How to include overlay text in an action rule on page 21*.

How to include overlay text

1. Go to **Video & Audio > Video Stream** and select the **Image** tab.

2. To include date and time, select **Include date** and **Include time**.

3. To include a text string, select **Include text** and enter the text in the field. Modifiers can be used, see *File Naming & Date/Time Formats* in the online help 🔵.

4. Select size, color, and placement of the text string.

5. Click **Save**.

To modify the date and time format, go to **System Options > Date & Time**. See *Date & Time on page 45*.

How to include overlay text in an action rule

Example

To display the text "Motion detected" when motion is detected, enter #D in the **Include text** field and enter "Motion detected" in the **Text** field when setting up the action rule.

1. Go to **Video & Audio > Video Stream** and select the **Image** tab.

2. Under **Overlay Settings**, select **Include text**.

3. Enter the modifier #D. When the rule is triggered, #D is replaced by the text specified in the action rule.

   Additional text in this field will be displayed also when the action rule is not active.

4. Go to **Events** > **Action Rules** and create your action rule.

5. From the **Actions** list, select **Overlay Text**.

6. Enter the text to display in the **Text** field.

7. Specify the **Duration**. The text can be displayed while the rule is active or for a fixed number of seconds.

How to display the pan or tilt position as a text overlay

It may be useful to retrieve, for instance from a recorded video, the pan or tilt position (in degrees) in which an event has taken place. This can be obtained by including the position in the image as a text overlay, using a modifier. To display the pan position as a text overlay:

1. Go to **Setup** > **Video** > **Video Stream**.

2. Under **Overlay settings**, select **Include text**.

   Enter #x to show the pan position.

   Enter #y to show the tilt position.

3. Configure the optional size, color and position of the text overlay.

4. Click **Save**.

5. Go to the Live View page to confirm the setting.

About overlay images

An overlay image is a static image superimposed over the video stream. The image, for example a company logo, is first uploaded to the Axis product and then used to provide extra information or to mask a part of the image.

Image specifications:

- The uploaded image should be a Windows 24–bit BMP image with maximum 250 colors.

- The image width and height, in pixels, must be exactly divisible by four.

- The image cannot be larger than the maximum image resolution.

- If you combine a text overlay with and image overlay, the text overlay always takes presidence over the overlay image in height. A text overlay always stretches across the whole video image which means you cannot shrink the overlay strip to make room for an image. For information about the different text overlay heights, see *About overlay text*.

Since it is static, the position and size of an overlay image remains the same regardless of resolution and pan, tilt or zoom movements.

To cover a part of the monitored area, use privacy masks. See *About privacy masks on page 22.*

How to upload an overlay image

1. Go to **Video & Audio > Overlay Image**.

2. Click **Browse** and browse to the file.

3. Click **Upload**.

4. The **Transparency Settings** page is now displayed:

    - To make a color in the overlay image transparent, select **Use transparency** and enter the RGB hexadecimal value for the color. Example: To make white transparent, enter FFFFFF.

      For more examples of hexadecimal values, see the online help 🔵.

    - To scale the image automatically, select **Scale with resolution**. The image will be scaled down to fit the resolution used by the Axis product.

5. Click **Save**.

How to include an overlay image

1. Go to **Video & Audio > Overlay Image**.

2. Select the image to use from the **Use overlay image** list and click **Save**.

3. Go to **Video & Audio > Video Stream** and select the **Image** tab.

4. Under **Overlay Settings**, select **Include overlay image at the coordinates**.

5. To control the image's position, enter the X (horizontal) and Y (vertical) coordinates. The X=0 and Y=0 position is the top left corner. If a part of the image is positioned outside the video image, the overlay image will be moved so that the whole image is visible.

6. Click **Save**.

About privacy masks

A privacy mask is an area of solid color that prohibits users from viewing parts of the monitored area. Privacy masks cannot be bypassed via the VAPIX® Application Programming Interface (API).

The Privacy Mask List, **Video & Audio > Privacy Mask**, shows all the masks that are currently configured in the Axis product and indicates if they are enabled.

Since the Pan/Tilt/Zoom coordinates define its size and position, a privacy mask is dynamic in relation to the monitored area. This means that regardless of the angle and zoom of the lens, the same place or object will be hidden. To define at what magnification the mask should be displayed, zoom to the desired level and click **Set level**.

You can add a new mask, re-size the mask with the mouse, choose a color for the mask, and give the mask a name.

For more information, see the online help 🔵.

Important

Adding many privacy masks may affect the product's performance.

How to change audio settings

To change the product's audio settings, go to **Video & Audio > Audio Settings**.

To include the audio stream in a video stream, go to **Video & Audio > Video Stream**. Under the **Audio** tab, select **Enable audio**.

Video and Audio

Each stream profile is a separate video stream. To include the audio stream in all stream profiles, go to the audio tab in each stream profile settings page and enable audio. For more information, see *About stream profiles on page 18*.

Audio Modes

The Axis product supports the following audio modes:

- **Full duplex –** Simultaneous two-way audio allowing the Axis product to transmit and receive audio at the same time.

  There is no echo cancellation; if feedback loops appear, try moving the microphone or the speaker.

- **Half-duplex –** Audio can be transmitted to and from the Axis product but only in one direction at a time. To transmit audio using the Live View page, use the **Talk** and **Listen** buttons, see *AMC Audio Controls on page 10*.

- **Simplex – Network Camera speaker only –** Audio is transmitted from a client to the Axis product and can be played by a speaker connected to the product. To transmit audio using the Live View page, the **Talk** and **Microphone on** buttons must both be active, see *AMC Audio Controls on page 10*.

- **Simplex – Network Camera microphone only –** Audio captured by the product microphone is transmitted from the Axis product to one or more clients.

To set the audio mode, go to **Video & Audio > Audio Settings** and select the desired mode from the **Audio mode** drop-down list.

Audio Input

Note

    If using unbalanced Line in a mono contact must be used. Signal on tip and ground on sleeve.

Select **Microphone** to use an external microphone or **Line** to use a Line in device, e.g. an audio mixer for multiple microphones or a microphone with a built-in amplifier, as audio source.

Select the microphone sensitivity level (**High/Low**) depending on the sound level in the monitored area. For example, if the Axis product is installed in a noisy environment, try setting the input sensitivity to **Low**.

The **Microphone power** option provides DC power for an external microphone.

To use a professional microphone requiring 48V phantom power, you need an external power supply and a balanced-unbalanced converter (audio transformer) in between.

Use the **Input gain** to control the volume of the audio input. If the sound is too low, choose a higher dB value, to amplify the sound. If the sound is too high, choose a lower dB value. The **Level** bar gives a visual representation of the audio signal level in dB relative to the full-scale input level.

- Green — the signal is at a good level.

- Yellow — the signal is becoming distorted.

- Red — the signal is distorted.

Use the **Encoding** option to select digital audio encoding format.

- **AAC** requires a license for both encoding and decoding. AAC is the least complicated and most widely used codec. If achieving the best possible audio quality is a priority, AAC is the recommended codec to use. An AAC license is included in the Axis product.

- **G711** is an unlicensed standard codec that is useful when integrating audio into a VoIP system

- **G726** is an unlicensed speech codec that is most commonly used within the security industry.

Note

The **Sample rate** defines the number of times per second the sound is sampled. A higher sample rate will provide better audio quality, but also requires a greater bandwidth.

Set the required **Bit rate** depending on the selected encoding. A higher bit rate will give better audio quality. A lower bit rate may have latency or delay, but will require less bandwidth.

For more information about these settings, please see the online help 🔵 .

Audio Output

Configure the audio output settings under **Video & Audio** > **Audio Settings**.

Output gain – Control the volume of the line audio output. If the sound is too low, choose a higher dB value. If the sound is too high, choose a lower dB value.

Audio Clips

An audio clip is a sound file that can be played when events occur or directly from the **Live View** page. The audio clip must first be uploaded to the Axis product or recorded by a microphone connected to the product.

To add, download, modify or remove audio clips, go to **Video & Audio > Audio Clips**. For more information see the online help 🔵.

To configure the Axis product to play audio clips when an event occurs, an action rule must be set up. For more information, see *About events on page 35*.

Note

> Audio clips cannot be used if the product's audio functionality is enabled. The audio functionality is enabled on the **Audio** tab under **Video & Audio > Video Stream**.

How to configure the live view window

You can customize the live view window and alter it to suit your requirements. It is possible to define the following features of the live view window.

- Stream Profile. See *page 18*.

- Default Viewer for Browser. See *page 25*.

- Viewer Settings. See *page 25*.

- Action Buttons. These are the buttons described in *About the controls in the live view window on page 9* .

- User Defined Links. See *page 26*.

- Output Buttons. See *page 26*.

How to set default viewer for browsers

From **Live View Config** > **Default Viewer** select the default method for viewing video images in your browser. The product attempts to show the video images in the selected video format and viewer. If this is not possible, the product overrides the settings and selects the best available combination.

Browser	Viewer	Description
Windows Internet Explorer	AMC	Recommended viewer in Internet Explorer (H.264/Motion JPEG).
	QuickTime	H.264.
	Still image	Displays still images only. Click the Refresh button in your browser to view a new image.
Other browsers	Server Push	Recommended viewer for other browsers (Motion JPEG).
	QuickTime	H.264.
	Still image	Displays still images only. Click the Refresh button in your browser to view a new image.

For more information, please see the online help 🔵 .

About viewer settings

To configure options for the viewer, go to **Live View Config > Viewer Settings**.

- Select **Show viewer toolbar** to display the AXIS Media Control (AMC) or the QuickTime viewer toolbar under the video image in your browser.

- **H.264 decoder installation**. The administrator can disable installation of the H.264 decoder included with AXIS Media Control. This is used to prevent installation of unlicensed copies. Further decoder licenses can be purchased from your Axis reseller.

- Select **Show crosshair in PTZ joystick mode** to enable a cross that will indicate the center of the image in PTZ joystick mode.

- Select **Use PTZ joystick mode as default** to enable joystick mode. The mode can be changed temporarily from the PTZ control panel.

- Select **Enable recording button** to enable recording from the Live View page. This button is available when using the AMC viewer. The recordings are saved to the location specified in the AMC Control Panel. See *About AXIS Media Control (AMC) on page 12*.

How to configure the live view window

About user-defined links

To display user-defined links in the live view window, select the **Show custom link** option, give the link a name and then enter the URL to link to. When defining a web link do not remove the 'http://' from the URL address. Custom links can be used to run scripts or activate external devices connected to the product, or they can link to a web page. Custom links defined as cgi links will run the script in the background, in a hidden frame. Defining the link as a web link will open the link in a new window.

Output Buttons

External I/O devices connected to the Axis product's output ports can be controlled directly from the Live View page.

To display output buttons in the Live View page:

1. Go to **Setup > Live View Config**.

2. Under **Output Buttons**, select the type of control to use:

   - **Pulse** activates the output for a defined period of time. The pulse time can be set from 1/100 second to 60 seconds.

   - **Active/Inactive** displays two buttons, one or each action.

To configure the active and inactive states, go to **System Options > Ports & Devices > I/O Ports** and set the port's **Normal state**.

For more information about I/O ports, see *I/O Ports on page 53*.

About PTZ (Pan Tilt Zoom)

About preset positions

A preset position is a saved view that can be used to quickly steer the camera to a specific position. A preset position consists of the following values:

- Pan and tilt positions

- Zoom position

- Focus position (manual or automatic)

How to access the preset positions

Preset positions can be accessed in several ways:

- By selecting the preset from the **Preset positions** drop-down list in the Live View Page.

- When setting up action rules. See *page 35*.

- When setting up guard tours. See *page 28*.

- When setting up the Gatekeeper. See *page 28*.

How to add a preset position

Note

> The focus window rectangle will disappear after a while, but the focus window will still be active.

1. Go to **Setup > PTZ > Preset Positions**.

2. Click in the image or use the controls to steer the camera view to the desired position.

3. To add a focus window, select **Focus window**. Place the mouse pointer on the part of the image that you want to focus on, click and drag to create a rectangle around it and release the mouse button.

   The rectangle will turn green when the focus window has been set. The camera will automatically adjust the image focus to this area.

   For more information about focus windows, see *page 28*.

4. Write a name in the **Current position** field.

5. If required, select **Use current position as Home**.

6. Click **Add** to save the preset position.

How to include the preset position name in an overlay text

1. Go to **Video & Audio**.

2. Select **Include text**.

3. Write the modifier #P in the field.

4. Click **Save**.

How to set the home position

The **Home** position is readily accessible by clicking the **Home** button on the live view window and in the Preset Positions setup window.

AXIS P5415-E PTZ Dome Network Camera

About PTZ (Pan Tilt Zoom)

To set a customized home position, select **Use current position as Home** when adding a preset position. The user-defined home position will have (H) added, for example, Entrance (H). The default Home position, called "Home", will still be available.

The product can be configured to return to the **Home** position when the PTZ functionality has been inactive for a specified length of time. Enter the length of time in the **Return to home when inactive** field and click **Save**. Set the time to zero to prevent the product from automatically returning to the **Home** position.

About the focus window

The focus window makes it possible to select an area of the camera's image to which that focus should be applied. This can be useful if there is a part of the image where focus is more critical, or if a part of the image should be ignored by the autofocus.

When the focus window is set from the Live View page, any change in the camera position will return the autofocus to the entire window.

When clicking the **Focus Window** button in the preset position page, the most recently set focus window from the Live View page appears.

If you set the focus window from the preset positions page, it is included in the settings for that preset. The focus window can be redefined for the preset, but it cannot be deleted unless the preset is deleted.

Gatekeeper

The Advanced Gatekeeper monitors an area such as an entrance gate. When motion is detected in the monitored area, the Gatekeeper will steer the camera to a selected preset position. Using a zoomed-in preset position can make it possible to, for example, read a license plate or identify a person. When motion is no longer detected, the camera returns to its Home position after a defined time.

To enable the Gatekeeper, go to **PTZ > Gatekeeper** and follow the online instructions.

It is also possible to, for example, record video or save images (take a snapshot) while the Gatekeeper is active. Go to **Events** and set up an action rule with **PTZ Preset Reached** as trigger.

About 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.

How to create a guard tour

1. Go to **Setup > PTZ > Guard Tour**.

2. Click **Add**.

3. Type a name.

4. Specify the pause length between runs.

5. Select a preset position from the drop-down list and click **Add**.

6. To specify how fast the camera should move to the preset position, enter a value in the **Move Speed** field.

7. For each preset position, enter the **View Time** in seconds or minutes.

8. Specify the **View Order** of the preset positions, or select **Random view order**.

9. Click **Save**.

How to edit a guard tour

1. Go to **Setup > PTZ > Guard Tour**.

2. Select the guard tour in the **Guard Tour List**.

3. Click **Modify**.

How to delete a guard tour

1. Go to **Setup > PTZ > Guard Tour**.

2. Select the guard tour in the **Guard Tour List**.

3. Click **Remove**.

About tour recording

How to create a recorded tour

Note

> Only the name of the recorded tour and pause between runs can be modified. Starting a new recording will overwrite the existing guard tour.

1. Go to **PTZ > Guard Tour** and click **Add**.

2. Select **Create a record tour** and click **OK**.

3. Type a name.

4. Specify the pause length between runs.

5. Click ⬤ to start recording the pan/tilt/zoom movements.

6. When satisfied, click ⬛.

7. Click **OK**.

8. Activate the recorded tour from the live view, the guard tour pages or through events. For more information see the online help ❓.

OSDI Zones

On-Screen Direction Indicator (OSDI) zones can be included in the overlay text (see *About overlay text on page 20*) to aid the user to navigate the Axis product. Each OSDI zone is set up with coordinates and a descriptive name.

OSDI zones are set up under **PTZ > OSDI Zones**. The Axis product uses the coordinates of the center of the view to set the lower left and upper right zone areas. First navigate to where you would like the lowermost left point of the OSDI zone to be located. Click **Get** to set the coordinates. Proceed to where the upper right point of zone should be located and click **Get**. Give the zone a descriptive name and click **OK**.

To include the name of the OSDI zone in the overlay text, go to **Video & Audio** < **Video Stream** < **Overlay Settings**. Check the **Include text** box and enter the modifier #L in the field. For more information about modifiers, see *File Naming & Date/Time Formats* in the online help ❓.

Advanced

Limits

Define the pan, tilt, zoom and focus limits for the Axis product. Movements to the left and right, up and down, can be restricted to narrow the area under surveillance.

About PTZ (Pan Tilt Zoom)

Near focus limit is used to prevent the camera from autofocusing on objects close to the camera. This way, the camera can ignore objects such as overhead wires, streetlights, or other cameras placed close to the camera.

To make the camera focus on the areas of interest, set the near focus limit to a value that is greater than the distance at which the uninteresting objects tend to appear. See illustration below where x is the near focus limit value.
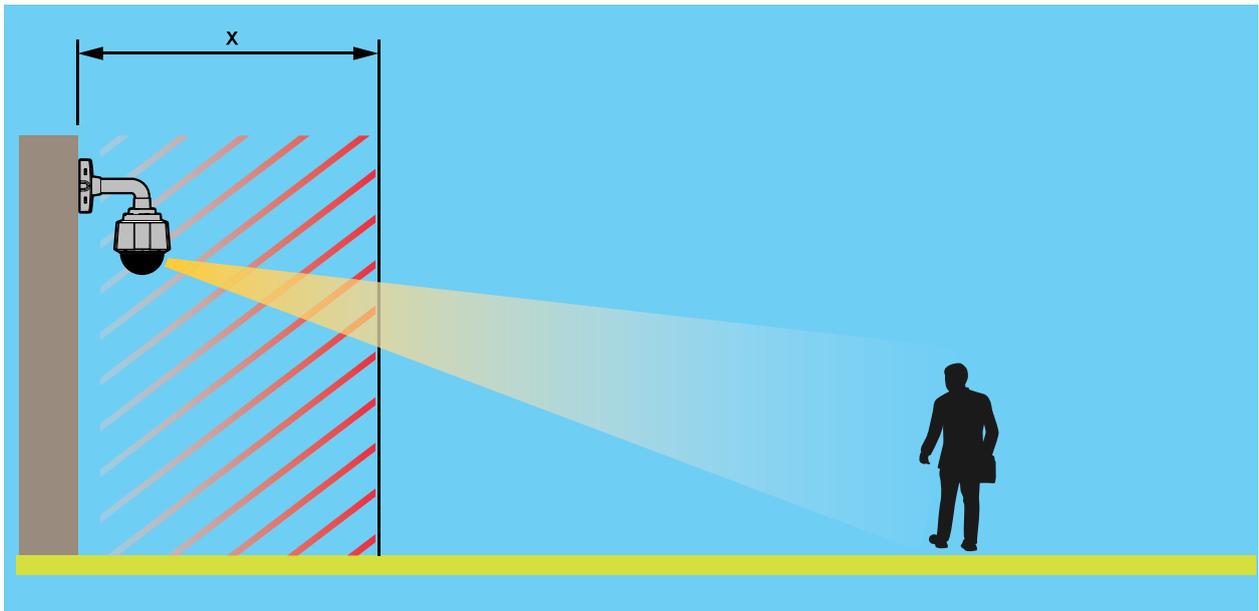
Move speed sets the speed of the camera's pan and tilt movements. The default setting is maximum speed.

When using a joystick (or emulating one with the mouse) the **Enable proportional speed** setting can be used to reduce the maximum pan/tilt movement speed, i.e. the speed the camera view moves at when the joystick is pushed all the way out in any direction. This is useful then the view is zoomed in on an object.

See the online help 🛈 for more information.

About advanced PTZ settings

Advanced PTZ settings can be configured under **PTZ > Advanced > Controls**.

The **Panel Shortcut Command Buttons** list shows the user-defined buttons that can be accessed from the Live View page's **Ctrl panel**. These buttons can be used to provide direct access to commands issued using the VAPIX® application programming interface. Click **Add** to add a new shortcut command button.

The following PTZ controls are enabled by default:

- Pan control

- Tilt control

- Zoom control

- Focus control

To disable specific controls, deselect the options under **Enable/Disable controls**.

Note

> Disabling PTZ controls will not affect preset positions. For example, if the tilt control is disabled, the product can still move to preset positions that require a tilt movement.

About the control queue

Note

- The administrator can enable and disable PTZ controls for selected users.

- To identify different users in the viewer group, cookies must be enabled on the client.

- The **Control queue polltime** is measured in seconds. For more information see the online help .

The administrator can set up a queue for PTZ controllers from **PTZ > Control Queue**. Once set up, the **PTZ Control Queue** buttons appear in the live view window offering one viewer exclusive control for a limited period of time. Other users will be placed in queue.

A user who belongs to a group (see *Users on page 43*) with a higher PTZ priority can go before other users in the queue and take control of the product. The order of priority is as follows:

1. **Administrator** — An administrator takes over PTZ control regardless of who is first in queue. The administrator will be removed from the queue 60 seconds after the last PTZ control command.

2. **Event** — The Axis product can be configured to go to a preset position when triggered by an alarm (see *About events on page 35*). The event will immediately be placed first in the queue except when an administrator is in control.

3. **Operator** — Same as administrator but with lower priority

4. **Guard Tour** — A guard tour (see *page 28*) has PTZ control for an indefinite period of time. It may be overridden by an operator, event or administrator. The guard tour will resume when higher priority groups leave the queue.

5. **Viewer** — Multiple viewers must wait for their turn. The viewer has 60 seconds PTZ control before control is passed on to the next viewer in queue.

About motion detection

Motion detection is used to generate an alarm whenever movement starts or stops in the camera view.

Motion detection is configured by defining up to 10 Include and Exclude windows:

- **Include windows** — define areas where motion should be detected

- **Exclude windows** — define areas within an Include window that should be ignored (areas outside Include windows are automatically ignored).

For instructions, see *How to set up motion detection windows on page 32*.

To control the number of motion detection alarms, the parameters **Object Size**, **History** and **Sensitivity** can be adjusted. See *About motion detection parameters on page 32*.

Once motion detection windows are configured, the Axis product can be configured to perform actions when motion is detected. Possible actions include uploading images and start recording. For more information, see *How to set up action rules on page 35*.

Note
- Using the motion detection feature may decrease the product's overall performance.
- The position of the Motion Detection Window is relative to the orientation of the Camera. Changing the orientation of the camera will also change the position of the Motion Detection Window.

How to set up motion detection windows

To set up a motion detection Include Window, follow these instructions:

1. Go to **Detectors > Motion Detection**.

2. Select the **Configure Included Windows** option and click **New**. Select the new window in the list of windows and enter a descriptive name.

3. Adjust the size (drag the bottom right-hand corner) and the position (click on the text at the top and drag to the desired position) of the window.

4. Adjust the **Object Size**, **History** and **Sensitivity** profile sliders (see *About motion detection parameters* for details). Any detected motion within an active window is indicated by red peaks in the **Activity window**.

5. Click **Save**.

To exclude parts of the include window, select the **Configure Excluded Windows** and position the exclude window within the include window.

To delete an include or exclude window, select the window in the list of windows and click **Del**.

About motion detection parameters

The parameters controlling motion detection are described in the table below:

Parameter	Object Size	History	Sensitivity
Description	Object size relative to window size.	Object memory length.	Difference in luminance between background and object.

High level (100%)	Only very large objects trigger motion detection.	An object that appears in the window triggers motion detection for a long time before it is considered as non-moving.	Ordinary colored objects on ordinary backgrounds trigger motion detection.
Medium level (50%)			A large difference in luminance is required to trigger motion detection.
Low level (0%)	Even very small objects trigger motion detection.	An object that appears in the window triggers motion detection only for a very short time before it is considered as non-moving.	Only very bright objects on a dark background trigger motion detection.
Recommended values	5–15%	60–90%	75–95%
Default values	15%	90%	90%

Note

- To trigger on small objects or movements, use several small motion detection windows rather than one large window, and select a low object size.

- To avoid triggering on small objects, select a high object size.

- While monitoring an area where moving objects are not expected, select a high history level. This will cause motion detection to trigger as long as the object is present in the window.

- To only detect flashing light, select a low sensitivity. In other cases high sensitivity is recommended.

Audio Detection

The Axis product can be configured to generate an alarm when audio rises above or falls below the threshold value. The threshold value can be set in the range 0–100 where 0 is the most sensitive and 100 the least sensitive.

1. Go to **Detectors > Audio Detection**.

2. Set the audio alarm level and click **Save.**

3. Go to **Events > Action Rules** and set up an action rule, see *How to set up action rules on page 35.*

Detected audio is indicated by colored peaks in the **Activity** indicator. An event is triggered when detected audio rises above or falls below the threshold value, which is represented by the bar.

About applications

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

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

Note

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

About application licenses

Some applications need a license to run. Licenses can be installed in two ways:

- Automatic installation — requires access to the Internet
- Manual installation — obtain the license key from the application vendor and upload the key to the Axis product

To request a license, the Axis product serial number (S/N) is required. The serial number can be found on the product label and under **System Options > Support > System Overview**.

How to upload and start an application

To upload and start an application:

1. Go to **Setup > Applications**.

2. Under **Upload Application**, click **Browse**. Locate the application file and click **Upload Package**.

3. Install the license (if applicable). For instructions, see the documentation provided by the application vendor.

4. Start the application. Go to **Applications**, select the application in the list of installed applications and click **Start**.

5. Configure the application. For instructions, see the documentation provided by the application vendor.

Note

- Applications can be uploaded by product administrators.
- Applications and licenses can be installed on multiple products at the same time using AXIS Camera Management, version 3.10 and later.

To generate a log file for the application, go to **Applications**. Select the application and click **Log**.

Application Considerations

If an application is upgraded, application settings, including the license, will be removed. The license must be reinstalled and the application reconfigured.

If the Axis product's firmware is upgraded, uploaded applications and their settings will remain unchanged, although this is not guaranteed by Axis Communications. Note that the application must be supported by the new firmware. For information about firmware upgrades, see *How to upgrade the firmware on page 58*.

If the Axis product is restarted, running applications will restart automatically.

If the Axis product is restored or reset to factory default, uploaded applications and their settings are removed. For information about restoring the Axis product, see *Maintenance on page 54*. For information about factory default, see *How to reset to factory default settings on page 55*.

About events

The event pages allow you to configure your product to perform actions when different events occur. For example, the product can start a recording or send an email notification when motion is detected. The set of conditions that defines how and when the action is triggered is called an action rule.

How to set up action rules

An action rule defines the conditions that must be met for the product to perform an action, for example record video or send an email notification. If multiple conditions are defined, all of them must be met to trigger the action.

For more information about available triggers and actions, see *About triggers on page 35* and *About actions on page 37*.

The following example describes how to set up an action rule to record video to a network share if there is movement in the camera's field of view.

How to set up motion detection and add a network share:

1. Go to **Applications** to start and configure AXIS Video Motion Detection. See the online help.

   It's also possible to go to **Detectors > Motion Detection** and configure a motion detection window. See the online help.

2. Go to **System Options > Storage** and set up the network share. See *page 53*.

How to set up the action rule:

1. Go to **Events > Action Rules** and click **Add**.

2. Select **Enable rule** and enter a descriptive name for the rule.

3. Select **Applications** from the **Trigger** drop-down list and then select **VMD**.

   It's also possible to select **Detectors** from the **Trigger** drop-down list, then select **Motion Detection** and then select the motion detection window.

4. Optionally, select a **Schedule** and **Additional conditions**. See below.

5. Under **Actions**, select **Record Video** from the **Type** drop-down list.

6. Select a **Stream profile** and configure the **Duration** settings as described below.

7. Select Network Share from the **Storage** drop-down list.

To use more than one trigger for the action rule, select **Additional conditions** and click **Add** to add additional triggers. When using additional conditions, all conditions must be met to trigger the action.

To prevent an action from being triggered repeatedly, a **Wait at least** time can be set. Enter the time in hours, minutes and seconds, during which the trigger should be ignored before the action rule can be activated again.

The recording **Duration** of some actions can be set to include time immediately before and after the event. Select **Pre-trigger time** and/or **Post-trigger time** and enter the number of seconds. When **While the rule is active** is enabled and the action is triggered again during the post-trigger time, the recording time will be extended with another post-trigger time period.

For more information, see the online help .

About triggers

Available action rule **triggers** and **conditions** include:

- **Applications** – Use installed applications to trigger the rule. See *About applications on page 34*.

About events

- Detectors

  - **Audio Detection** – Trigger the rule when audio is detected. See *Audio Detection on page 33*.

  - **Day/Night Mode** – Trigger the rule when the product switches between day mode (IR cut filter on) and night mode (IR cut filter off). This can for example be used to control an external infrared (IR) light connected to an output port.

  - **Live Stream Accessed** – Trigger the rule when any stream is accessed and during edge storage playback. This can for example be used to send notifications.

  - **Motion Detection** – Trigger the rule when motion is detected. See *About motion detection on page 32*.

- Hardware

  - **Network** – Trigger the rule if network connection is lost or restored. This can for example be used to start recording to the SD card.

  - **Temperature** – Trigger the rule if the temperature falls outside or inside the operating range of the product. This can for example be used to send maintenance notifications.

- Input Signal

  - **Digital Input Port** – Trigger the rule when an I/O port receives a signal from a connected device. See *I/O Ports on page 53*.

  - **Manual Trigger** – Trigger the rule using the **Manual Trigger** button in the Live View page. See *About the controls in the live view window on page 9* . This can for example be used to validate actions during product installation and configuration.

  - **Virtual Inputs** – can be used by a VMS (Video Management System) to trigger actions. Virtual inputs can, for example, be connected to buttons in the VMS user interface.

- PTZ

  - **Error** – Trigger the rule if the PTZ functionality is not working correctly. This can for example be used to send maintenance notifications.

  - **Ready** – Trigger the rule when the PTZ functionality is ready to be used. This can for example be used to steer the camera to a specific preset position when the product is started.

- Storage

  - **Disruption** – Trigger the rule if storage problems are detected, for example if the storage device is unavailable, removed, full, locked or if other read or write problems occur. This can for example be used to send maintenance notifications.

  - **Recording** – Triggers the rule when the Axis product records to the storage device. The recording status trigger can be used to notify the operator, for example by flashing LED lights, if the product has started or stopped to record to the storage device. Note that, this trigger can be used only for edge storage recording status.

- System

  - **System Ready** – Trigger the rule when the product has been started and all services are running. This can for example be used to send a notification when the product restarts.

- Time

  - **Recurrence** – Trigger the rule periodically. See *How to set up recurrences on page 39*. This can for example be used to upload an image every 5 minutes.

  - **Use Schedule** – Trigger the rule according to the selected schedule. See *How to create schedules on page 39*.

About actions

Available **actions** include:

- **Day/Night Vision Mode** – Set day mode (IR cut filter on) or night mode (IR cut filter off).

- **Output Port** – Activate an I/O port to control an external device.

- **Overlay Text** – Display an overlay text. See *How to include overlay text in an action rule on page 21*.

- **Play Audio Clip** – See *Audio Clips on page 24*.

- **PTZ Control**

    - **Preset Position** – Go to a preset position.

    - **Guard Tour** – Start a guard tour. See *About guard tours on page 28*.

- **Record Video** – Record video and audio to a selected storage. To record audio, use AAC audio encoding and make sure that audio is enabled in the selected stream profile.

- **Send Images** – Send images to a recipient.

- **Send Notification** – Send a notification message to a recipient.

- **Send SNMP Trap** – Send an SNMP trap message to the operator. Make sure that SNMP is enabled and configured under **System Options** > **Network** > **SNMP**.

- **Send Video Clip** – Send a video clip to a recipient.

How to add recipients

The product can send media files and messages to notify users about events. Before the product can send media files or notification messages, you must define one ore more recipients. For information about available options, see *About recipient types on page 37*.

To add a recipient:

1. Go to **Events > Recipients** and click **Add**.

2. Enter a descriptive name.

3. Select a recipient **Type**.

4. Enter the information needed for the recipient type.

5. Click **Test** to test the connection to the recipient.

6. Click **OK**.

About recipient types

The following recipient types are available:

Recipient types	Use with action	Notes
Email	Send Images Send Notification Send Video Clip	An email recipient can contain multiple email addresses.
FTP	Send Images Send Video Clip	

About events

SFTP	Send Images Send Video Clip	Encrypted file transfer using SSH File Transport Protocol (SFTP). SFTP is a more secure method than FTP but file transfer might be slower, especially for large files such as high resolution video. Specify login information for the SFTP server and the server's public key MD5 fingerprint (32 hexadecimal digits). The SFTP recipient supports SFTP servers using SSH–2 with RSA and DSA host key types. RSA is the preferred method. To use DSA, disable the RSA key on the SFTP server.
HTTP	Send Images Send Notification Send Video Clip	
HTTPS	Send Images Send Notification Send Video Clip	Encrypted file transfer using HyperText Transfer Protocol Secure (HTTPS). Specify login information for the HTTPS server and validate the server's certificate. If there is a proxy between the Axis product and the HTTPS server, also specify the proxy settings.
Network Share	Send Images Send Video Clip	A network share can also be used as a storage device for recorded video. Go **System Options > Storage** to configure a network share before setting up a continuous recording or an action rule to record video. For more information about storage devices, see *Storage on page 51*.
TCP	Send Notification	

How to set up email recipients

Email recipients can be configured by selecting one of the listed email providers, or by specifying the SMTP server, port and authentication used by, for example, a corporate email server.

> Note
>
> Some email providers have security filters that prevent users from receiving or viewing large attachments, from receiving scheduled emails and similar. Check the email provider's security policy to avoid delivery problems and locked email accounts.

To set up an email recipient using one of the listed providers:

1. Go to **Events > Recipients** and click **Add**.

2. Enter a **Name** and select **Email** from the **Type** list.

3. Enter the email addresses to send emails to in the **To** field. Use commas to separate multiple addresses.

4. Select the email provider from the **Provider** list.

5. Enter the user ID and password for the email account.

6. Click **Test** to send a test email.

To set up an email recipient using for example a corporate email server, follow the instructions above but select **User defined** as **Provider**. Enter the email address to appear as sender in the **From** field. Select **Advanced settings** and specify the SMTP server address, port and authentication method. Optionally, select **Use encryption** to send emails over an encrypted connection. The server certificate can be validated using the certificates available in the Axis product. For information on how to upload certificates, see *About certificates on page 45*.

How to create schedules

Schedules can be used as action rule triggers or as additional conditions, for example to record video if motion is detected outside office hours. Use one of the predefined schedules or create a new schedule as described below.

To create a new schedule:

1. Go to **Events > Schedules** and click **Add**.

2. Enter a descriptive name and the information needed for a daily, weekly, monthly or yearly schedule.

3. Click **OK**.

To use the schedule in an action rule, select the schedule from the **Schedule** drop-down list in the Action Rule Setup page.

How to set up recurrences

Recurrences are used to trigger action rules repeatedly, for example every 5 minutes or every hour.

To set up a recurrence:

1. Go to **Events > Recurrences** and click **Add**.

2. Enter a descriptive name and recurrence pattern.

3. Click **OK**.

To use the recurrence in an action rule, first select **Time** from the **Trigger** drop-down list in the Action Rule Setup page and then select the recurrence from the second drop-down list.

To modify or remove recurrences, select the recurrence in the **Recurrences List** and click **Modify** or **Remove**.

About recordings

The Axis product can be configured to record video continuously or according to an action rule:

- To start a continuous recording, see *page 41*.

- To set up action rules, see *page 35*.

- To access recordings, see *How to find recordings on page 40*.

- To play recordings, see *How to play recordings on page 40*.

- To export a recording as a video clip, see *How to export a video clip on page 41*.

- To configure camera controlled storage, see *Storage on page 51*.

How to find recordings

Recordings stored on the SD card or network share can be accessed from the **Recordings > List** page. The page lists all recordings on the storage device and shows each recording's start date and time, duration and the event that triggered the recording.

Note

> The recording's start date and time is set according to the Axis product's date and time settings. If the Axis product is configured to use a time zone different from the local time zone, make sure to configure the **Recording time** filters according to the product's time zone. Date and time settings are configured under **System Options > Date & Time**, see *Date & Time on page 45*.

To find a recording, follow these steps:

1. Go to **Recordings > List**.

2. To reduce the number of recordings displayed, select the desired options under **Filter**:

   Recording time – List recordings that started between the **From** and **To** times.

   Event – List recordings that were triggered by a specific event. Select **continuous** to list continuous recordings.

   Storage – List recordings from a specific storage device.

   Sort – Specify how recordings should be sorted in the list.

   Results – Specify the maximum number of recordings to display.

3. To apply the filters, click the **Filter** button. Some filters may take a long time to complete.

4. The recordings are displayed in the **Recording** list.

To play a recording, select the recording and click **Play**. See also *How to play recordings on page 40*.

To view detailed information about a recording, select the recording and click **Properties**.

To export a recording or a part of a recording as a video clip, select the recording and click **Export**. See also *How to export a video clip on page 41*.

To remove a recording from the storage device, select the recording and click **Remove**.

How to play recordings

Recordings on the SD card or network share can be played directly from the Axis product's web pages.

About recordings

To play a recording, follow these steps:

1. Go to **Recordings > List**.

2. To reduce the number of recordings displayed, select the desired options under **Filter** and click the **Filter** button to apply the filters. See also *How to find recordings on page 40*.

3. Select the recording and click **Play**. The recording will be played in a new browser window.

How to export a video clip

Recordings on the SD card or network share can be exported as video clips. You can export a complete recording or a part of a recording.

Note

> The exported recording is a Matroska video file (.mkv). To play the recording in Windows Media Player, AXIS Matroska File Splitter must be installed. AXIS Matroska File Splitter can be downloaded from *www.axis.com/support/downloads*

To export a video clip, follow these steps:

1. Go to **Recordings > List**.

2. To reduce the number of recordings displayed, select the desired options under **Filter** and click the **Filter** button to apply the filters. See also *How to find recordings on page 40*.

3. Select the recording and click **Export**. The **Export Recording** dialog opens.

4. By default, the complete recording is selected. To export a part of the recording, modify the start and stop times.

5. Optionally, enter a file name for the recording.

6. Click **Export**.

Note

> Recordings can also be exported from the playback window.

About continuous recording

The Axis product can be configured to continuously save video to a storage device. For information about storage devices, see *Storage on page 51*. To prevent the disk from becoming full, it is recommended to configure the disk to automatically remove old recordings.

If a new stream profile is selected while a recording is ongoing, the recording will be stopped and saved in the recording list and a new recording with the new stream profile will start. All previous continuous recordings will remain in the recording list until they are removed manually or through automatic removal of old recordings.

To start a continuous recording, follow these steps:

1. Go to **Recordings > Continuous**.

2. Select **Enabled**.

3. Select the type of storage device from the **Storage** list.

4. Select a **Stream profile** to use for continuous recordings. To include audio in the recording, use AAC audio encoding and make sure that audio is enabled in the selected stream profile.

5. Click **Save** to save and start the recording.

About languages

Multiple languages can be installed in the Axis product. All web pages including the online help will be displayed in the selected language. To switch languages, go to **Setup** > **Languages** and first upload the new language file. Browse and locate the file and click the **Upload Language** button. Select the new language from the list and click Save.

Note

- Resetting the product to factory default settings will erase any uploaded language files and reset the product language to English.

- Clicking the **Restore** button on the Maintenance page will not affect the language.

- A firmware upgrade will not affect the language used. However if you have uploaded a new language to the product and later upgrade the firmware, it may happen that the translation no longer matches the product's web pages. In this case, upload an updated language file.

- A language already installed in the product will be replaced when a current or a later version of the language file is uploaded.

About system options

Security

Users

User access control is enabled by default and can be configured under **System Options > Security > Users**. An administrator can set up other users by giving them user names and passwords. It is also possible to allow anonymous viewer login, which means that anybody may access the Live View page.

The user list displays authorized users and user groups (access levels):

- **Viewers** have access to the Live View page

- **Operators** have access to all settings except:

    - creating and modifying PTZ presets

    - creating and modifying PTZ control settings

    - creating and modifying privacy mask settings

    - uploading applications and language files

    - any of the settings included in the **System Options**

- **Administrators** have unrestricted access to all settings. The administrator can add, modify and remove other users.

Note

> Note that when the option **Encrypted & unencrypted** is selected, the webserver will encrypt the password. This is the default option for a new unit or a unit reset to factory default settings.

Under **HTTP/RTSP Password Settings**, select the type of password to allow. You may need to allow unencrypted passwords if there are viewing clients that do not support encryption, or if you upgraded the firmware and existing clients support encryption but need to log in again and be configured to use this functionality.

Under **User Settings**, select the **Enable anonymous viewer login** option to allow anonymous users access to the Live View page.

Select the **Enable anonymous PTZ control login** to allow anonymous users access to the PTZ controls.

Deselect the **Enable Basic Setup** option to hide the Basic Setup menu. Basic Setup provides quick access to settings that should be made before using the Axis product.

ONVIF

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.

By creating a user you automatically enable ONVIF communication. Use the user name and password with all ONVIF communication with the product. For more information see *www.onvif.org*

IP Address Filter

IP address filtering is enabled on the **System Options > Security > IP Address Filter** page. Once enabled, the listed IP address are allowed or denied access to the Axis product. Select **Allow** or **Deny** from the list and click **Apply** to enable IP address filtering.

The administrator can add up to 256 IP address entries to the list (a single entry can contain multiple IP addresses).

About system options

HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol providing encrypted browsing. HTTPS can also be used by users and clients to verify that the correct device is being accessed. The security level provided by HTTPS is considered adequate for most commercial exchanges.

The Axis product can be configured to require HTTPS when users from different user groups (administrator, operator, viewer) log in.

To use HTTPS, an HTTPS certificate must first be installed. Go to **System Options > Security > Certificates** to install and manage certificates. See *About certificates on page 45*.

To enable HTTPS on the Axis product:

1. Go to **System Options > Security > HTTPS**

2. Select an HTTPS certificate from the list of installed certificates.

3. Optionally, click **Ciphers** and select the encryption algorithms to use for SSL.

4. Set the **HTTPS Connection Policy** for the different user groups.

5. Click **Save** to enable the settings.

To access the Axis product via the desired protocol, in the address field in a browser, enter `https://` for the HTTPS protocol and `http://` for the HTTP protocol.

The HTTPS port can be changed on the **System Options > Network > TCP/IP > Advanced** page.

IEEE 802.1X

IEEE 802.1X is a 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, devices must be authenticated. The authentication is performed by an authentication server, typically a **RADIUS server**, examples of which are FreeRADIUS and Microsoft Internet Authentication Service.

In Axis implementation, the Axis product and the authentication server identify themselves with digital certificates using EAP-TLS (Extensible Authentication Protocol - Transport Layer Security). The certificates are provided by a **Certification Authority** (CA). You need:

- • a CA certificate to authenticate the authentication server.

- • a CA-signed client certificate to authenticate the Axis product.

To create and install certificates, go to **System Options > Security > Certificates**. See *About certificates on page 45*.

To allow the product to access a network protected by IEEE 802.1X:

1. Go to **System Options > Security > IEEE 802.1X**.

2. Select a **CA Certificate** and a **Client Certificate** from the lists of installed certificates.

3. Under **Settings**, select the EAPOL version and provide the EAP identity associated with the client certificate.

4. Check the box to enable IEEE 802.1X and click **Save**.

Note

> For authentication to work properly, the date and time settings in the Axis product should be synchronized with an NTP server. See *Date & Time on page 45*.

About system options

About certificates

Certificates are used to authenticate devices on a network. Typical applications include encrypted web browsing (HTTPS), network protection via IEEE 802.1X and secure upload of images and notification messages for example via email. Two types of certificates can be used with the Axis product:

Server/Client certificates – To authenticate the Axis product. A **Server/Client** certificate 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 – To authenticate peer certificates, for example the certificate of an authentication server in case the Axis product is connected to an IEEE 802.1X protected network. The Axis product is shipped with several preinstalled CA certificates.

Note

- If the product is reset to factory default, all certificates, except preinstalled CA certificates, will be deleted.
- If the product is reset to factory default, all preinstalled CA certificates that have been deleted will be reinstalled.

How to create a self-signed certificate

1. Go to **Setup > System Options > Security > Certificates**.

2. Click **Create self-signed certificate** and provide the requested information.

How to create and install a CA-signed certificate

1. Create a self-signed certificate, see *How to create a self-signed certificate on page 45*.

2. Go to **Setup > System Options > Security > Certificates**.

3. Click **Create certificate signing request** and provide the requested information.

4. Copy the PEM-formatted request and send to the CA of your choice.

5. When the signed certificate is returned, click **Install certificate** and upload the certificate.

How to install additional CA certificates

1. Go to **Setup > System Options > Security > Certificates**.

2. Click **Install certificate** and upload the certificate.

Audio Support

Select **Enable audio support** to allow clients to retrieve audio streams from the Axis product. For information on how to configure audio settings, see *How to change audio settings on page 22*.

Note

Deselecting this option will disable audio globally in the Axis product, for configured events and profiles with audio as well.

Date & Time

The Axis product's date and time settings are configured under **System Options > Date & Time**.

Current Server Time displays the current date and time (24h clock). The time can be displayed in 12h clock in the text overlay (see below).

To change the date and time settings, select the preferred **Time mode** under **New Server Time**:

- **Synchronize with computer time** – Sets date and time according to the computer's clock. With this option, date and time are set once and will not be updated automatically.

- **Synchronize with NTP Server** – Obtains date and time from an NTP server. With this option, date and time settings are updated continuously. For information on NTP settings, see *NTP Configuration on page 48*.

    If using a host name for the NTP server, a DNS server must be configured. See *DNS Configuration on page 48*.

- **Set manually** – Allows you to manually set date and time.

If using an NTP server, select your **Time zone** from the drop-down list. If required, check **Automatically adjust for daylight saving time changes**.

The **Date & Time Format Used in Images** is the date and time format displayed as a text overlay in the video stream. Use the predefined formats or see *File Naming & Date/Time Formats* in the online help for information on how to create custom date and time formats. To include date and time in the overlay text, go to **Video & Audio** and select **Include date** and **Include time**.

Network

Basic TCP/IP Settings

The Axis product supports IP version 4 and IP version 6. Both versions can be enabled simultaneously, and at least one version must always be enabled.

IPv4 Address Configuration

By default, the Axis product is set to use IPv4 (IP version 4) and to obtain the IP address automatically via DHCP. The IPv4 settings are configured under **System Options > Network > TCP/IP > Basic**.

DHCP (Dynamic Host Configuration Protocol) allows network administrators to centrally manage and automate the assignment of IP addresses. DHCP should only be enabled if using dynamic IP address notification, or if the DHCP can update a DNS server. It is then possible to access the Axis product by name (host name).

If DHCP is enabled and the product cannot be accessed, run AXIS IP Utility to search the network for connected Axis products, or reset the product to the factory default settings (see *page 55*) and then perform the installation again.

To use a static IP address, check **Use the following IP address** and specify the IP address, subnet mask and default router.

IPv6 Address Configuration

If IPv6 (IP version 6) is enabled, the Axis product will receive an IP address according to the configuration in the network router.

To enable IPv6, go to **System Options > Network > TCP/IP > Basic**. Other settings for IPv6 should be configured in the network router.

ARP/Ping

The product's IP address can be assigned using ARP and Ping. For instructions, see *Assign IP Address Using ARP/Ping on page 46*.

The ARP/Ping service is enabled by default but is automatically disabled two minutes after the product is started, or as soon as an IP address is assigned. To re-assign IP address using ARP/Ping, the product must be restarted to enable ARP/Ping for an additional two minutes.

To disable the service, go to **System Options > Network > TCP/IP > Basic** and clear the option **Enable ARP/Ping setting of IP address**.

Pinging the product is still possible when the service is disabled.

Assign IP Address Using ARP/Ping

The product's IP address can be assigned using ARP/Ping. The command must be issued within 2 minutes of connecting power.

1. Acquire a free static IP address on the same network segment as the computer.

2. Locate the serial number (S/N) on the product label.

3. Open a command prompt and enter the following commands:

   Linux/Unix syntax

   ```
   arp -s <IP address> <serial number> temp
   ping -s 408 <IP address>
   ```

   Linux/Unix example

   ```
   arp -s 192.168.0.125 00:40:8c:18:10:00 temp
   ping -s 408 192.168.0.125
   ```

   Windows syntax (this may require that you run the command prompt as an administrator)

   ```
   arp -s <IP address> <serial number>
   ping -l 408 -t <IP address>
   ```

   Windows example (this may require that you run the command prompt as an administrator)

   ```
   arp -s 192.168.0.125 00-40-8c-18-10-00
   ping -l 408 -t 192.168.0.125
   ```

4. Check that the network cable is connected and then restart the product by disconnecting and reconnecting power.

5. Close the command prompt when the product responds with `Reply from 192.168.0.125:...` or similar.

6. Open a browser and type `http://<IP address>` in the Location/Address field.

For other methods of assigning the IP address, see the document *Assign an IP Address and Access the Video Stream* on Axis Support web at *www.axis.com/support*

Note

- To open a command prompt in Windows, open the **Start menu** and type `cmd` in the **Run/Search** field.
- To use the ARP command in Windows 8/Windows 7/Windows Vista, right-click the command prompt icon and select **Run as administrator**.
- To open a command prompt in Mac OS X, open the **Terminal utility** from **Application > Utilities**.

AXIS Video Hosting System (AVHS)

AVHS used in conjunction with an AVHS service, provides easy and secure Internet access to live and recorded video accessible from any location. For more information and help to find a local AVHS Service Provider go to www.axis.com/hosting

The AVHS settings are configured under **System Options > Network > TCP IP > Basic**. The possibility to connect to an AVHS service is enabled by default. To disable, clear the **Enable AVHS** box.

One-click enabled – Press and hold the product's control button (see *Hardware overview on page 7*) for about 3 seconds to connect to an AVHS service over the Internet. Once registered, **Always** will be enabled and the Axis product stays connected to the AVHS service. If the product is not registered within 24 hours from when the button is pressed, the product will disconnect from the AVHS service.

Always – The Axis product will constantly attempt to connect to the AVHS service over the Internet. Once registered the product will stay connected to the service. This option can be used when the product is already installed and it is not convenient to use the one-click installation.

AXIS Internet Dynamic DNS Service

AXIS Internet Dynamic DNS Service assigns a host name for easy access to the product. For more information, see *www.axiscam.net*

To register the Axis product with AXIS Internet Dynamic DNS Service, go to **System Options > Network > TCP/IP > Basic**. Under **Services**, click the AXIS Internet Dynamic DNS Service **Settings** button (requires access to the Internet). The domain name currently registered at AXIS Internet Dynamic DNS service for the product can at any time be removed.

About system options

Note

AXIS Internet Dynamic DNS Service requires IPv4.

Advanced TCP/IP Settings

DNS Configuration

DNS (Domain Name Service) provides the translation of host names to IP addresses. The DNS settings are configured under **System Options > Network > TCP/IP > Advanced**.

Select **Obtain DNS server address via DHCP** to use the DNS settings provided by the DHCP server.

To make manual settings, select **Use the following DNS server address** and specify the following:

Domain name – Enter the domain(s) to search for the host name used by the Axis product. Multiple domains can be separated by semicolons. The host name is always the first part of a fully qualified domain name, for example, `myserver` is the host name in the fully qualified domain name `myserver.mycompany.com` where `mycompany.com` is the domain name.

Primary/Secondary DNS server – Enter the IP addresses of the primary and secondary DNS servers. The secondary DNS server is optional and will be used if the primary is unavailable.

NTP Configuration

NTP (Network Time Protocol) is used to synchronize the clock times of devices in a network. The NTP settings are configured under **System Options > Network > TCP/IP > Advanced**.

Select **Obtain NTP server address via DHCP** to use the NTP settings provided by the DHCP server.

To make manual settings, select **Use the following NTP server address** and enter the host name or IP address of the NTP server.

Host Name Configuration

The Axis product can be accessed using a host name instead of an IP address. The host name is usually the same as the assigned DNS name. The host name is configured under **System Options > Network > TCP/IP > Advanced**.

Select **Obtain host name via IPv4 DHCP** to use host name provided by the DHCP server running on IPv4.

Select **Use the host name** to set the host name manually.

Select **Enable dynamic DNS updates** to dynamically update local DNS servers whenever the Axis product's IP address changes.

For more information, see the online help 💿.

Link-Local IPv4 Address

Link-Local Address is enabled by default and assigns the Axis product an additional IP address which can be used to access the product from other hosts on the same segment on the local network. The product can have a Link-Local IP and a static or DHCP-supplied IP address at the same time.

This function can be disabled under **System Options > Network > TCP/IP > Advanced**.

HTTP

The HTTP port used by the Axis product can be changed under **System Options > Network > TCP/IP > Advanced**. In addition to the default setting, which is 80, any port in the range 1024–65535 can be used.

HTTPS

The HTTPS port used by the Axis product can be changed under **System Options > Network > TCP/IP > Advanced**. In addition to the default setting, which is 443, any port in the range 1024–65535 can be used.

To enable HTTPS, go to **System Options > Security > HTTPS**. For more information, see *HTTPS on page 44*.

NAT traversal (port mapping) for IPv4

A network router allows devices on a private network (LAN) to share a single connection to the Internet. This is done by forwarding network traffic from the private network to the "outside", that is, the Internet. Security on the private network (LAN) is increased since most routers are pre-configured to stop attempts to access the private network (LAN) from the public network (Internet).

Use **NAT traversal** when the Axis product is located on an intranet (LAN) and you wish to make it available from the other (WAN) side of a NAT router. With NAT traversal properly configured, all HTTP traffic to an external HTTP port in the NAT router is forwarded to the product.

NAT traversal is configured under **System Options > Network > TCP/IP > Advanced**.

Note

- For NAT traversal to work, this must be supported by the router. The router must also support UPnP^{TM}.

- In this context, router refers to any network routing device such as a NAT router, Network router, Internet Gateway, Broadband router, Broadband sharing device, or a software such as a firewall.

Enable/Disable – When enabled, the Axis product attempts to configure port mapping in a NAT router on your network, using UPnP^{TM}. Note that UPnP^{TM} must be enabled in the product (see **System Options > Network > UPnP**).

Use manually selected NAT router – Select this option to manually select a NAT router and enter the IP address for the router in the field. If no router is specified, the product automatically searches for NAT routers on your network. If more than one router is found, the default router is selected.

Alternative HTTP port – Select this option to manually define an external HTTP port. Enter a port in the range 1024–65535. If the port field is empty or contains the default setting, which is 0, a port number is automatically selected when enabling NAT traversal.

Note

- An alternative HTTP port can be used or be active even if NAT traversal is disabled. This is useful if your NAT router does not support UPnP and you need to manually configure port forwarding in the NAT router.

- If you attempt to manually enter a port that is already in use, another available port is automatically selected.

- When the port is selected automatically it is displayed in this field. To change this, enter a new port number and click **Save**.

FTP

The FTP server running in the Axis product enables upload of new firmware, user applications, etc. The FTP server can be disabled under **System Options > Network > TCP/IP > Advanced**.

Note

This FTP server has nothing to do with the product's ability to transfer images via FTP to other locations and servers.

RTSP

The RTSP server running in the Axis product allows a connecting client to start an H.264 stream. The RTSP port number can be changed under **System Options > Network > TCP/IP > Advanced**. The default port is 554.

Note

H.264 video streams will not be available if the RTSP server is disabled.

SOCKS

SOCKS is a networking proxy protocol. The Axis product can be configured to use a SOCKS server to reach networks on the other side of a firewall or proxy server. This functionality is useful if the Axis product is located on a local network behind a firewall, and notifications, uploads, alarms, etc need to be sent to a destination outside the local network (for example the Internet).

SOCKS is configured under **System Options > Network > SOCKS**. For more information, see the online help .

QoS (Quality of Service)

QoS (Quality of Service) guarantees a certain level of a specified resource to selected traffic on a network. A QoS-aware network prioritizes network traffic and provides a greater network reliability by controlling the amount of bandwidth an application may use.

The QoS settings are configured under **System Options > Network > QoS**. Using DSCP (Differentiated Services Codepoint) values, the Axis product can mark different types of traffic.

> Note
>
> Live audio DSCP will be equal to live video DSCP if H.264 over RTSP is used.

SNMP

The Simple Network Management Protocol (SNMP) allows remote management of network devices. An SNMP community is the group of devices and management station running SNMP. Community names are used to identify groups.

AXIS Video MIB (Management Information Base) for video hardware can be used to monitor Axis-specific, hardware-related issues that may need administrative attention. For more information about AXIS Video MIB and to download MIB files, go to *www.axis.com/support*

To enable and configure SNMP in the Axis product, go to the **System Options > Network > SNMP** page.

Depending on the level of security required, select the version on SNMP to use.

Traps are used by the Axis product to send messages to a management system on important events and status changes. Check **Enable traps** and enter the IP address where the trap message should be sent and the **Trap community** that should receive the message.

> Note
>
> If HTTPS is enabled, SNMP v1 and SNMP v2c should be disabled.

Traps for SNMP v1/v2 are used by the Axis product to send messages to a management system on important events and status changes. Check **Enable traps** and enter the IP address where the trap message should be sent and the **Trap community** that should receive the message.

The following traps are available:

- Cold start

- Warm start

- Link up

- Authentication failed

> Note
>
> All AXIS Video MIB traps are enabled when SNMP v1/v2c traps are enabled. It is not possible to turn on or off specific traps.

SNMP v3 provides encryption and secure passwords. To use traps with SNMP v3, an SNMP v3 management application is required.

To use SNMP v3, HTTPS must be enabled, see *HTTPS on page 44.* To enable SNMP v3, check the box and provide the initial user password.

> Note
>
> The initial password can only be set once. If the password is lost, the Axis product must be reset to factory default, see *How to reset to factory default settings on page 55.*

UPnP™

The Axis product includes support for UPnP™. UPnP™ is enabled by default and the product is automatically detected by operating systems and clients that support this protocol.

UPnP™ can be disabled under **System Options > Network > UPnP**.

RTP/H.264

The RTP port range and multicast settings are configured under **System Options > Network > RTP**.

The RTP port range defines the range of ports from which the video/audio ports are automatically selected. For multicast streams, only certain IP addresses and port numbers should be used.

Select **Always Multicast Video** and/or **Always Multicast Audio** to start multicast streaming without opening an RTSP session.

Bonjour

The Axis product includes support for Bonjour. Bonjour is enabled by default and the product is automatically detected by operating systems and clients that support this protocol.

Bonjour can be disabled under **System Options > Network > Bonjour**.

Storage

About SD cards

NOTICE

To prevent data corruption, the SD card should be unmounted before removal.

Note

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

The Axis product supports SD/SDHC/SDXC cards.

The following SD card file systems are supported:

- **ext4** — recommended due to its resilience against data loss if the card is ejected or if there is abrupt power loss. To access data stored on the card from the Windows operating system, a third-party ext4 driver or application is required.

- **vFAT** — supported by most operating systems for personal computers.

The SD card is managed on the **System Options > Storage** page. Click **SD Card** to open **Storage Management**.

If the card's status shows as failed, click **Check disk** to see if the problem can be found and then try **Repair**. This option is only available for SD cards with ext4. For SD cards with vFAT, use a card reader or computer to troubleshoot the card.

To avoid filling the card, it is recommended to remove recordings continuously. Under **General Settings**, select **Remove recordings older than** and select the number of days or weeks.

To stop writing to the card and protect recordings from being removed, select **Lock** under **General Settings**.

How to mount and unmount the SD card

NOTICE

To prevent corruption of recordings, the SD card should always be unmounted before it is ejected.

The SD card is automatically mounted when the card is inserted into the Axis product or when the product is started. A manual mount is only required if the card has been unmounted and not ejected and re-inserted.

To unmount the SD card:

1. Open the Axis product's webpages and go to **Setup > System Options > Storage**.

2. Click **SD Card**.

3. Click **Unmount**.

4. The card can now be removed.

How to format the SD card

NOTICE

Formatting the SD card will remove all data and recordings stored on the card.

The Axis product can be configured to automatically format SD cards that are inserted into the product. If autoformat is enabled and an SD card is inserted, the product will check if the SD card has the ext4 file system. If the card has a different file system, the card will automatically be formatted to ext4.

Important

If autoformat is enabled, only use new or empty SD cards. Any data stored on the card will be lost when the card is inserted into the Axis product.

To enable automatic formatting, follow these steps:

1. Open the Axis product's webpages and go to **Setup > System Options > Storage**.

2. Click **SD Card**.

3. Under **General Settings**, select **Autoformat to**.

4. Click **OK** to save settings.

An SD card inserted into the product can be manually formatted to one of the supported file systems. To manually format the SD card, follow these steps:

1. Insert the SD card in the SD card slot.

2. Open the Axis product's webpages and go to **Setup > System Options > Storage**.

3. Click **SD Card**.

4. Click **Format** and select the desired file system.

5. Click **OK** to start formatting the card.

How to encrypt SD card data

To prevent unauthorized individuals and systems from accessing recorded video, the SD card content can be encrypted. Encryption can only be enabled when the card is unmounted. After enabling encryption, the SD card must be formatted so that no unencrypted data remains on the card. The card must also be mounted before it can be used.

Note

If autoformat is enabled, the card will be formatted and mounted automatically when encryption is enabled. The format and mount steps below should then be skipped.

To encrypt the SD card content:

1. Open the Axis product's webpages and go to **Setup > System Options > Storage**.

2. Click **SD Card** to open **Storage Management**.

3. If the SD card is mounted, click **Unmount** to unmount the card.

4. Click **Encrypt**.

5. Select **Enable SD card encryption** and enter a passphrase.

6. Back in Storage Management, click **Format** to format the SD card.

7. Click **Mount** to mount the SD card.

It is possible to change the passphrase without reformatting the card. Open **Storage Management**, click **Encrypt** and enter the old and new passphrases. The passphrase can only be changed when the card is mounted. Changing the passphrase does not disrupt ongoing recordings.

To disable encryption, unmount the SD card and follow the steps above but clear the **Enable SD card encryption** option. The card must be formatted and mounted when encryption has been disabled.

Network Share

Network share allows you to add network storage such as a NAS (network-attached storage). The NAS shall be dedicated for recordings and data from the Axis products connected to the network. For information about reference NAS devices, go to *www.axis.com/products/axis-companion/support-and-documentation*

Note

> For NAS recommendations see *www.axis.com*

To add a network share:

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

2. Click **Network Share**.

3. Enter the IP address, DNS or Bonjour name to the host server in the **Host** field.

4. Enter the name of the share in the **Share** field. Sub folders cannot be used.

5. If required, select **The share requires login** and enter the user name and password.

6. Click **Connect**.

To clear all recordings and data from the Axis product's folder on the designated share, click **Clear** under **Storage Tools**.

To avoid filling the share, it is recommended to remove recordings continuously. Under **Recording Settings**, select **Remove recordings older than** and select the number of days or weeks.

To stop writing to the share and protect recordings from being removed, select **Lock** under **Recording Settings**.

Ports & Devices

I/O Ports

The Axis product provides four configurable input and output ports for connection of external devices. For information about how to connect external devices, see *Connectors on page 62*.

To configure the I/O ports, go to **System Options** > **Ports & Devices** > **I/O Ports**. Each port can function as input or output:

- Input as Open circuit – The input becomes active when the circuit is grounded by, for example, a REX device. It remains inactive as long as its normal state equals its current status.

- Input as Grounded circuit – The input becomes active when the circuit is opened by for example a monitor.

- Output as Open circuit – The output port is in a non-conductive state when its current status is open circuit. The current status of an output port can be changed by, for example, an action rule.

- Output as Grounded circuit – The output port is in a conductive state when its current status is grounded circuit.

Port Status

The list on the **System Options > Ports & Devices > Port Status** page shows the status of the product's input and output ports.

About system options

Maintenance

The Axis product provides several maintenance functions. These are available under **System Options > Maintenance**.

Click **Restart** to perform a correct restart if the Axis product is not behaving as expected. This will not affect any of the current settings.

> Note
>
> A restart clears all entries in the Server Report.

Click **Restore** to reset most settings to the factory default values. The following settings are not affected:

- the boot protocol (DHCP or static)

- the static IP address

- the default router

- the subnet mask

- the system time

- the IEEE 802.1X settings

> Note
>
> If the Axis product is restored, uploaded applications and their settings are removed.

Click **Default** to reset all settings, including the IP address, to the factory default values. This button should be used with caution. The Axis product can also be reset to factory default using the control button, see *How to reset to factory default settings on page 55*.

To test the product's PTZ mechanics, click **Test** under **PTZ Status**.

For information about firmware upgrade, see *How to upgrade the firmware on page 58*.

Support

Support Overview

The **System Options > Support > Support Overview** page provides information on troubleshooting and contact information, should you require technical assistance.

See also *Troubleshooting on page 58*.

System Overview

To get an overview of the Axis product's status and settings, go to **System Options > Support > System Overview**. Information that can be found here includes firmware version, IP address, network and security settings, event settings, image settings and recent log items.

Logs & Reports

The **System Options > Support > Logs & Reports** page generates logs and reports useful for system analysis and troubleshooting. If contacting Axis Support, please provide a Server Report with your query.

System Log – Provides information about system events.

Access Log – Lists all failed attempts to access the product. The Access Log can also be configured to list all connections to the product (see below).

Server Report – Provides information about the product status in a pop-up window. The Access Log is automatically included in the Server Report.

You can view or download the server report. Downloading the server report creates a .zip file that contains a complete server report text file in UTF–8 format. Select the **Include snapshot with default image settings** option to include a snapshot of the product's Live View. The server report .zip file should always be included when contacting support.

Parameter List – Shows the product's parameters and their current settings. This may prove useful when troubleshooting or when contacting Axis Support.

Connection List – Lists all clients that are currently accessing media streams.

Crash Report – Generates an archive with debugging information. The report takes several minutes to generate.

Advanced

Scripting

Scripting allows experienced users to customize and use their own scripts.

> **NOTICE**
> Improper use may cause unexpected behavior and loss of contact with the Axis product.

Axis strongly recommends that you do not use this function unless you understand the consequences. Axis Support does not provide assistance for problems with customized scripts.

To open the Script Editor, go to **System Options > Advanced > Scripting**. If a script causes problems, reset the product to its factory default settings, see *page 55*.

For more information, see *www.axis.com/developer*

File Upload

Files, for example webpages and images, can be uploaded to the Axis product and used as custom settings. To upload a file, go to **System Options > Advanced > File Upload**.

Uploaded files are accessed through `http://<ip address>/local/<user>/<file name>` where `<user>` is the selected user group (viewer, operator or administrator) for the uploaded file.

Plain Config

Plain Config is for advanced users with experience of Axis product configuration. Most parameters can be set and modified from this page.

To open Plain Config, go to **System Options > Advanced > Plain Config**. Axis Support does not provide assistance with this feature.

How to 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 and reconnect power.

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

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

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

Repainting the Camera

The covers can be repainted to match the installation environment.

The material used in the covers is ASA Geloy XTWM206. Use paint suitable for this material.

1. Remove the two top cover screws.

2. Use a thin palette knife to release the locking tabs while pulling the top cover straight upwards to remove the cover.

3. Remove the two bottom cover screws and remove the bottom cover.

4. Mask the locking tabs in the bottom cover and the three screw covers.

5. Repaint the top cover, the bottom cover, the screw covers, and the conduit cover.

6. Assemble in the reverse order.
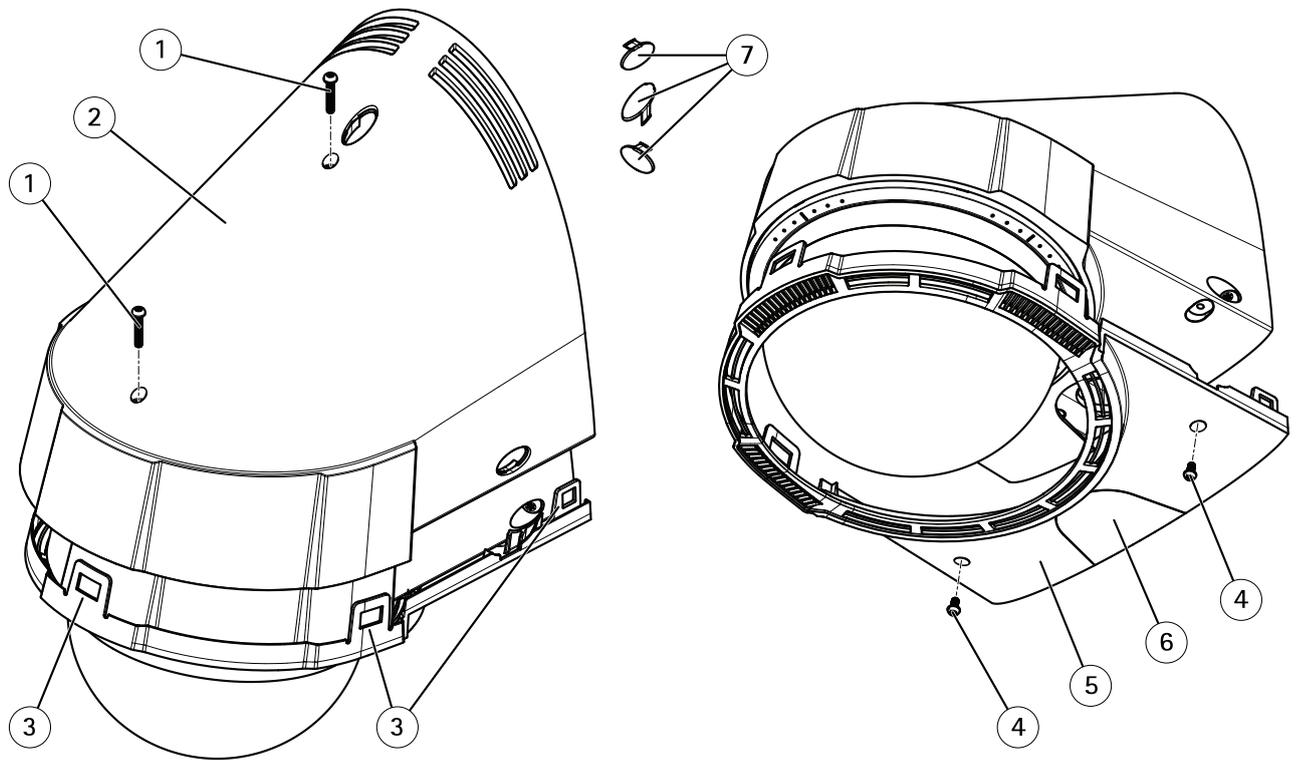
1   Top cover screw
2   Top cover
3   Locking tab
4   Bottom cover screw
5   Bottom cover
6   Conduit cover
7   Screw cover

Troubleshooting

How to check the current firmware

Firmware is software that determines the functionality of network devices. One of your first actions when troubleshooting a problem should be to check the current firmware version. The latest version may contain a correction that fixes your particular problem. The current firmware version in the Axis product is displayed in the page **Setup > Basic Setup** and in **Setup > About**.

How to upgrade the firmware

Important

- Your dealer reserves the right to charge for any repair attributable to faulty upgrade by the user.
- Preconfigured and customized settings are saved when the firmware is upgraded (providing the features are available in the new firmware) although this is not guaranteed by Axis Communications AB.

Note

- After the upgrade process has completed, the product restarts automatically. If you restart the product manually after the upgrade, wait 10 minutes even if you suspect that the upgrade has failed.
- When you upgrade the Axis product with the latest firmware, the product receives the latest functionality available. Always read the upgrade instructions and release notes available with each new release before upgrading the firmware.

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

2. Go to **Setup > System Options > Maintenance** in the product's webpages.

3. Under **Upgrade Server**, click **Browse** and locate the file on your computer.

4. Click **Upgrade**.

5. Wait approximately 10 minutes while the product is being upgraded and restarted. Then access the product.

6. Go to **Setup > Basic Setup** to verify the firmware upgrade.

AXIS Camera Management can be used for multiple upgrades. See *www.axis.com* for more information.

Emergency Recovery Procedure

If power or network connection is lost during the upgrade, the process fails and the product may become unresponsive. Flashing red Status indicator indicates a failed upgrade. To recover the product, follow the steps below. The serial number is found on the product's label.

1. In **UNIX/Linux**, type the following from the command line:

   ```
   arp -s <IP address> <serial number> temp
   ping -l 408 <IP address>
   ```

   In **Windows**, type the following from a command/DOS prompt (this may require that you run the command prompt as an administrator):

   ```
   arp -s <IP address> <serial number>
   ping -l 408 -t <IP address>
   ```

2. If the product does not reply in 30 seconds, restart it and wait for a reply. Press CTRL+C to stop Ping.

3. Open a browser and type in the product's IP address. In the page that opens, use the **Browse** button to select the upgrade file to use. Then click **Load** to restart the upgrade process.

4. After the upgrade is complete (1–10 minutes), the product automatically restarts and shows a steady green on the Status indicator.

5. Reinstall the product, referring to the Installation Guide.

If the emergency recovery procedure does not get the product up and running again, contact Axis support at *www.axis.com/support*

Symptoms, possible causes and remedial actions

Problems upgrading the firmware

Firmware upgrade failure	If the firmware upgrade fails, the product reloads the previous firmware. Check the firmware file and try again.

Problems setting the IP address

When using ARP/Ping	Try the installation again. The IP address must be set within two minutes after power has been applied to the product. Ensure the Ping length is set to 408. For instructions, see *Assign IP Address Using ARP/Ping on page 46*.
The product is located on a different subnet	If the IP address intended for the product and the IP address of the computer used to access the product are located on different subnets, you will not be able to 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 product from the network. Run the Ping command (in a Command/DOS window, type `ping` and the IP address of the product): • 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 product. • If you receive: `Request timed out`, this means that the IP address is available for use with the Axis product. Check all cabling and reinstall the product.
Possible IP address conflict with another device on the same subnet	The static IP address in the Axis product 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 product.

The product cannot be accessed from a browser

Cannot log in	When HTTPS is enabled, ensure that the correct protocol (HTTP or HTTPS) is used when attempting to log in. You may need to manually type `http` or `https` in the browser's address field. If the password for the user root is lost, the product must be reset to the factory default settings. See *How to reset to factory default settings on page 55*.
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 Camera Management to locate the product on the network. Identify the product using its model or serial number, or by the DNS name (if the name has been configured). If required, a static IP address can be assigned manually. For instructions, see the document *Assign an IP Address and Access the Video Stream* on Axis Support web at *www.axis.com/support*.
Certificate error when using IEEE 802.1X	For authentication to work properly, the date and time settings in the Axis product should be synchronized with an NTP server. See *Date & Time on page 45*.

The product is accessible locally but not externally

Router configuration	To configure your router to allow incoming data traffic to the Axis product, enable the NAT-traversal feature which will attempt to automatically configure the router to allow access to the Axis product, see *NAT traversal (port mapping) for IPv4 on page 49*. The router must support UPnP™.

Firewall protection	Check the Internet firewall with your network administrator.
Default routers required	Check if you need to configure the router settings from **System Options > Network > TCP/IP > Basic**.

Problems with streaming H.264

Problems with AXIS Media Control (*Internet Explorer only*)	To enable the updating of video images in Internet Explorer, set the browser to allow ActiveX controls. Also, make sure that AXIS Media Control is installed on your computer.
No H.264 displayed in the client	Check that the relevant H.264 connection methods and correct interface are enabled in the AMC Control Panel (streaming tab). See *About AXIS Media Control (AMC) on page 12*.
	In the AMC Control Panel, select the H.264 tab and click **Set to default H.264 decoder**.
	Check that RTSP is enabled under **System Options > Network > TCP/IP > Advanced**.
Multicast H.264 only accessible by local clients	Check if your router supports multicasting, or if the router settings between the client and the product need to be configured. The TTL (Time To Live) value may need to be increased.
No multicast H.264 displayed in the client	Check with your network administrator that the multicast addresses used by the Axis product are valid for your network.
	Check with your network administrator to see if there is a firewall preventing viewing.
Poor rendering of H.264 images	Ensure that your graphics card is using the latest driver. The latest drivers can usually be downloaded from the manufacturer's website.
Color saturation is different in H.264 and Motion JPEG	Modify the settings for your graphics adapter. Refer to the adapter's documentation for more information.
Lower frame rate than expected	See *Performance considerations on page 64*.
	Reduce the number of applications running on the client computer.
	Limit the number of simultaneous viewers.
	Check with the network administrator that there is enough bandwidth available.
	Check in the AMC Control Panel (H.264 tag) that video processing is not set to **Decode only key frames**.
	Lower the image resolution.
	The maximum frames per second is dependent on the utility frequency (60/50 Hz) of the Axis product.

Video and image problems, general

Image unsatisfactory	Check the video stream and camera settings under **Setup > Video & Audio > Video Stream** and **Setup > Video & Audio > Camera Settings**.

Motion Detection triggers unexpectedly

Changes in luminance	Motion detection is based on changes in luminance in the image. This means that if there are sudden changes in the lighting, motion detection may trigger mistakenly. Lower the sensitivity setting to avoid problems with luminance.

Troubleshooting

No audio

Incorrect setup	Check the sound card in the computer. Ensure that mute is not selected and that the volume settings are correct.
	Check that **Enable audio support** is selected under **Setup > System Options > Security > Audio Support**.
	Check that the correct **Audio Input** source is selected under **Setup > Video & Audio > Audio Settings**.

Poor audio quality

Stuttering	Reduce the number of listeners and viewers. Decrease image resolution and compression.
Unsynchronized audio and video using H.264	Synchronize the product's date and time settings with an NTP server. Go to **Setup > System Options > Date & Time**.
Distorted audio	Check that the correct **Audio Input** source is selected under **Setup > Video & Audio > Audio Settings**.
Feedback loops	Feedback loops might appear in full-duplex mode. Try moving the microphone or the speaker, or use half-duplex mode instead.

Storage and disk management problems

Storage disruption	A storage disruption alarm is sent if a storage device is unavailable, removed, full, locked or if other read or write problems occur. To identify the source of the problem, check the **System Log** under **System Options > Support > Logs & Reports**. Depending on the problem, it might be necessary to re-mount the storage device.
	For information on how to set up a storage disruption alarm, see *About events on page 35*.
Video cannot be recorded	Check that the SD card is not write protected (that is, read only).
SD card cannot be mounted	Reformat the SD card and then click Mount.
	NOTICE
	Formatting the card will remove all content, including all recordings, from the SD card.

To find the latest version of the datasheet, go to www.axis.com > product > Support & Documentation.

LED Indicators

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

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. Disconnect power or unmount the SD card from the product's webpage before removal.

This product supports SD/SDHC/SDXC cards (not included).

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

Buttons

Control Button

For location of the control button, see *Hardware overview on page 7* .

The control button is used for:

- Resetting the product to factory default settings. See *page 55*.

- Connecting to an AXIS Video Hosting System service. See *page 47*. To connect, press and hold the button for about 3 seconds until the Status LED flashes green.

- Connecting to AXIS Internet Dynamic DNS Service. See *page 47*. To connect, press and hold the button for about 3 seconds.

Connectors

Network connector

RJ45 Ethernet connector with Power over Ethernet Plus (PoE+).

NOTICE

The product shall be connected using a shielded network cable (STP). All cables connecting the product to the network shall be intended for their specific use. Make sure that the network devices are installed in accordance with the manufacturer's instructions. For information about regulatory requirements, see the Installation Guide available at *www.axis.com*
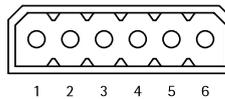
Technical specifications

About I/O connectors

Use the I/O connector with external devices in combination with, for example, tampering alarms, 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 output – For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface or in the product's webpage.

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.

6-pin terminal block

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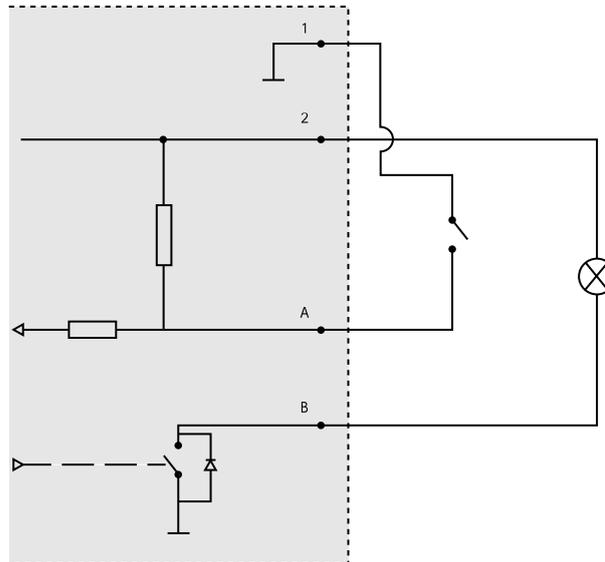
1 0 V DC (–)
2 DC output 12 V, max 50 mA
A I/O configured as input
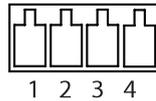B I/O configured as output

Audio connector

4-pin terminal block for audio input and output.

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

4-pin terminal block for:

- Audio input
- Audio output

1 2 3 4

Function	Pin	Notes
Microphone/Line in	1	Microphone or line in (mono)
GND	2	Ground
Line out	3	Line audio out
GND	4	Ground

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.
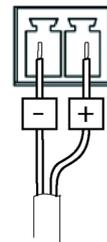
Performance considerations

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

The following factors are the most important to consider:

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

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

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

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

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

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

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

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

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

AXIS P5415-E PTZ Dome Network Camera

Technical specifications

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