# AXIS M5065 PTZ Network Camera

# User Manual

## About this Document

This manual is intended for administrators and users of AXIS M5065 PTZ 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 *axis.com/patent* 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 *opensource.apple.com/apsl*). The source code is available from *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 acknowledgements

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, Apache, Bonjour, Ethernet, Internet Explorer, Linux, Microsoft, Mozilla, Real, SMPTE, QuickTime, UNIX, Windows, 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. The UPnP Word Mark and UPnP Logo are trademarks of Open Connectivity Foundation, Inc. in the United States or other countries.

microSD, microSDHC, and microSDXC Logos are trademarks of SD-3C LLC. microSD, microSDHC, microSDXC are trademarks or registered trademarks of SD-3C, LLC in the United States, other countries or both.

Z-Wave and Z-Wave Plus are registered trademarks of Silicon Laboratories Inc. in the United States and other countries.

**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 device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested using a shielded network cable (STP) and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.The product shall be connected using a shielded network cable (STP) that is properly grounded.

**Contact information**

Axis Communications Inc.
300 Apollo Drive
Chelmsford, MA 01824
United States of America
Tel: +1 978 614 2000

**Canada**

This digital apparatus complies with CAN ICES-3 (Class A). 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 A). 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 A limit of EN 55032. The product shall be connected using a shielded network cable (STP) that is properly grounded. Notice! This is a Class A product. In a domestic environment this product may cause RF interference, in which case the user may be required to take adequate measures.

**Australia/New Zealand**

This digital equipment fulfills the requirements for RF emission according to the Class A limit of AS/NZS CISPR 32. The product shall be connected using a shielded network cable (STP) that is properly grounded. Notice! This is a Class A product. In a domestic environment this product may cause RF interference, in which case the user may be required to take adequate measures.

**Japan**

この装置は、クラスA 情報技術装置です。この装置を家庭環境で使用すると電波妨害 を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求され ることがあります。 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。

**Korea**

이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서 가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다. 적절히 접지된 STP (shielded twisted pair) 케이블을 사용하여 제품을 연결 하십시오.

**Radio transmission**

This equipment may generate or use radio frequency energy. The user could lose the authority to operate this equipment if an unauthorized change or modification is made.

**USA**

This equipment complies with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesirable operation.

This product complies with FCC radiation exposure limits for an uncontrolled environment. This equipment shall be installed and operated with a minimum distance of 20 cm (7.9 in) between the user and the device.

**Canada**
This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
This product complies with IC radiation exposure limits for an uncontrolled environment. This equipment shall be installed and operated with a minimum distance of 20 cm (7.9 in) between the user and the device.
Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
Ce produit est conforme aux limites d'exposition aux radiations IC pour un environnement non contrôlé. L'équipement doit être installé et fonctionné à une distance minimum de 20 cm (7,9 po) entre l'utilisateur et le dispositif.

**Japan**
本製品は、特定無線設備の技術基準適合証明を受けています。

**Safety**
This product complies with IEC/EN/UL 62368-1, safety of audio/video and IT equipment.

If its connecting cables are routed outdoors, the product shall be grounded either through a shielded network cable (STP) or other appropriate method.

When used with Power over Ethernet (PoE), the Power Sourcing Equipment (PSE) shall comply with IEEE 802.3af and Limited Power Source (LPS) according to clause 2.5 of IEC/EN/UL 60950-1 or annex Q of IEC/EN/UL 62368-1.

We recommend the use of Axis midspans or Axis PoE switches.

**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).

**Contact information**
Axis Communications AB
Emdalavägen 14
223 69 Lund
Sweden

Tel: +46 46 272 18 00
Fax: +46 46 13 61 30

*axis.com*

## 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 *axis.com/support*

## Warranty information

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

## Learn more!

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

## Table of Contents


**Safety information** ..... 6
Hazard levels ..... 6
Other message levels ..... 6
**Safety instructions** ..... 7
Transportation ..... 7
Battery ..... 7
**Solution overview** ..... 8
**Hardware overview** ..... 9
**How to access the product** ..... 10
Access the device ..... 10
How to access the product from the internet ..... 10
How to set the root password ..... 11
Configure capture mode ..... 11
About the live view window ..... 11
**About media streams** ..... 13
About H.264 format ..... 13
About MJPEG format ..... 13
About AXIS Media Control (AMC) ..... 13
Alternative methods of accessing the video stream ..... 14
Access Audio Streams ..... 15
**How to set up the product** ..... 16
How to perform a basic setup ..... 16
**Video and Audio** ..... 17
How to set up video streams ..... 17
About stream profiles ..... 20
About ONVIF media profiles ..... 20
About camera settings ..... 20
About overlays ..... 22
About privacy masks ..... 24
How to change audio settings ..... 24
**How to configure the live view window** ..... 25
How to set default viewer for browsers ..... 25
**About PTZ (Pan Tilt Zoom)** ..... 27
About preset positions ..... 27
OSDI Zones ..... 27
Advanced ..... 28
About the control queue ..... 28
**About applications** ..... 30
About application licenses ..... 30
How to upload and start an application ..... 30
Application Considerations ..... 30
About AXIS Audio Volume Detection ..... 31
About AXIS Scream Detection ..... 31
About AXIS Removed Object Detection ..... 31
**About events** ..... 34
How to set up action rules ..... 34
How to add recipients ..... 36
How to create schedules ..... 37
How to set up recurrences ..... 37
**About recordings** ..... 39
How to find recordings ..... 39
How to play recordings ..... 39
How to export a video clip ..... 40
About continuous recording ..... 40
**About wireless I/O (Z-Wave Plus®)** ..... 41
How to add a Z-Wave device ..... 42
How to remove a Z-Wave device ..... 42
How to replace a Z-Wave device ..... 43
How to reset the Z-Wave network ..... 44
How to make the camera's LED flash when the Z-Wave device's battery is low ..... 44

## Table of Contents

How to direct the camera to a preset position when the wireless PIR motion sensor detects motion ... 44
About using Z-Wave as I/O ... 45
**About languages** ... 46
**About system options** ... 47
Security ... 47
Date & Time ... 49
Network ... 50
Storage ... 55
Maintenance ... 57
Support ... 58
Advanced ... 58
How to reset to factory default settings ... 59
**Troubleshooting** ... 60
How to check the current firmware ... 60
How to upgrade the firmware ... 60
Symptoms, possible causes and remedial actions ... 60
**Specifications** ... 64
LED Indicators ... 64
SD card slot ... 64
Buttons ... 64
Connectors ... 65
Performance considerations ... 65

## 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.

## Safety instructions

***NOTICE***

- The Axis product shall be used in compliance with local laws and regulations.
- Axis recommends using a shielded network cable (STP) CAT5 or higher.
- Use only applicable tools when installing the Axis product. Using excessive force with power tools could cause damage to the product.
- Use only accessories that comply with the technical specification of your product. These can be provided by Axis or a third party. Axis recommends using Axis power source equipment compatible with your product.
- Use only spare parts provided by or recommended by Axis.
- Do not attempt to repair the product yourself. Contact Axis support or your Axis reseller for service matters.

### Transportation

***NOTICE***

- When transporting the Axis product, use the original packaging or equivalent to prevent damage to the product.

### Battery

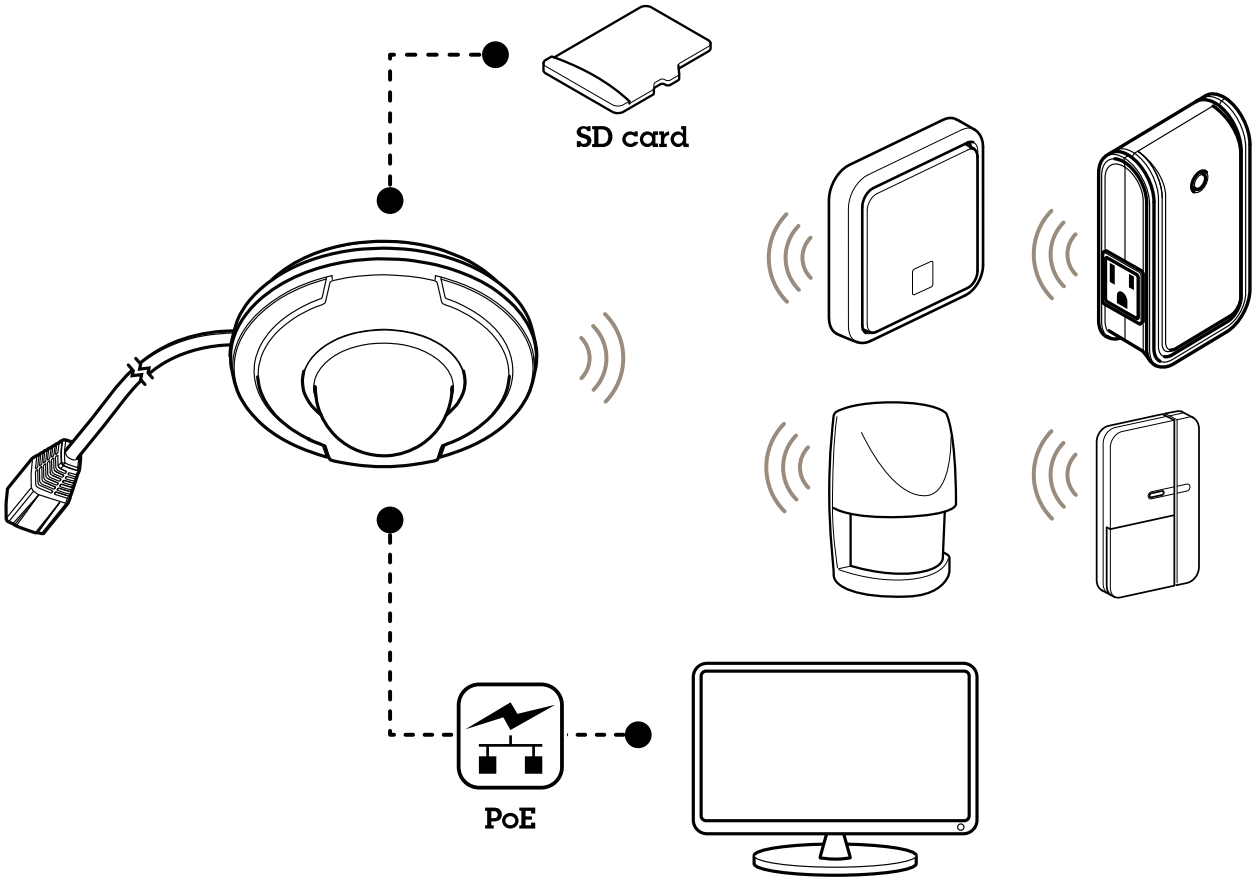
Low battery power affects the operation of the RTC, causing it to reset at every power-up. When the battery needs replacing, a log message will appear in the product's server report. For more information about the server report, see the product´s web page or contact Axis support.

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

**⚠WARNING**

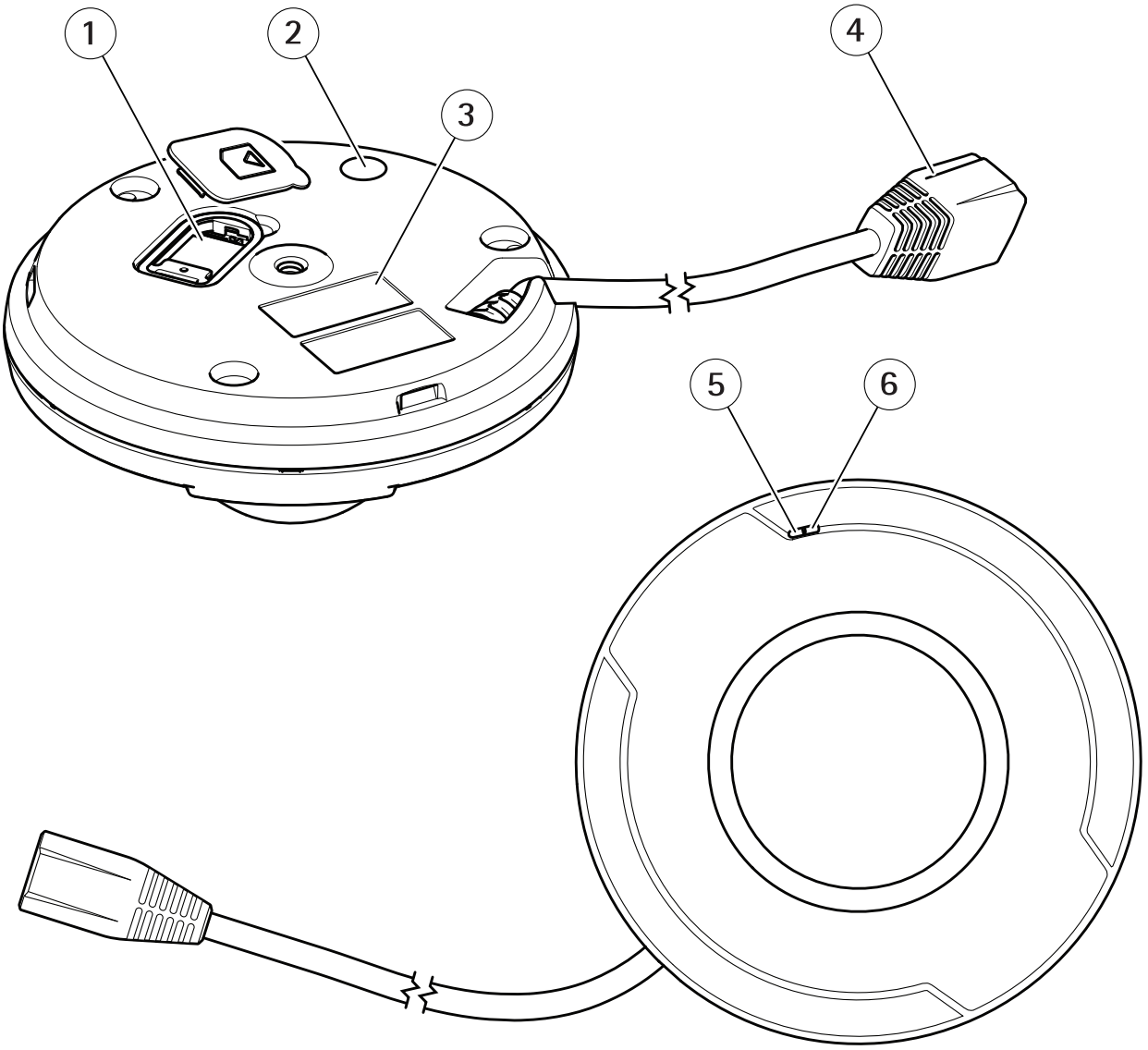
- Risk of explosion if the battery is incorrectly replaced.
- The battery should be replaced with an identical battery only.
- Used batteries should be disposed of according to local regulations or the battery manufacturer's instructions.

## Solution overview



## Hardware overview

For specifications of the hardware components, see *Specifications on page 64*.




1 *microSD card slot*
2 *Control button*
3 *Part number (P/N) and serial number (S/N)*
4 *Network connector (PoE)*
5 *Microphone*
6 *Status LED indicator*

# How to access the product

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

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.

## Access the device

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

   If you have a Mac computer (OS X), go to Safari, click on Bonjour and select the device from the drop-down list. To add Bonjour as a browser bookmark, go to **Safari > Preferences**.

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

2. Enter the username and password. If you access the device for the first time, you must set the root password. See .

3. The live view page opens in your browser.

## How to access the product from the internet

A network router allows products 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 internet.

Most routers are pre-configured to stop attempts to access the private network (LAN) from the public network (internet).

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

**How to turn on the NAT-traversal feature**

- Go to **Settings > System > Plain config > Network**.
- Select **NAT traversal enabled**.
- Enter **External IP address**.
- Enter the IP address of the **NAT traversal router**.
- Manually configure your NAT router to allow access from the internet.

See also AXIS Internet Dynamic DNS Service at *www.axiscam.net*

Note

- In this context, a "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.
- For NAT traversal to work, NAT traversal must be supported by the router. The router must also support UPnP®.

## 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 47*.

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 59*.

To set the password, enter it directly in the dialog.

## Configure capture mode

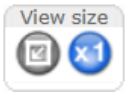
Capture mode defines the maximum frame rate available in the Axis product. The capture mode also affects light sensitivity. A capture mode with a high maximum frame rate has reduced light sensitivity and vice versa.

See also *About capture modes on page 20*.

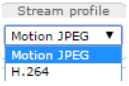
## About the live view window

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 20*.

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 11*.

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**.

#### 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 34*.

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 13* 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 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 24*.

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

Use the slider to control the volume of the speakers.

# 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.<br>Note that there are a maximum of 10 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.<br>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.<br>Note also that all multicast viewers count as one unicast viewer in the maximum total of 10 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)

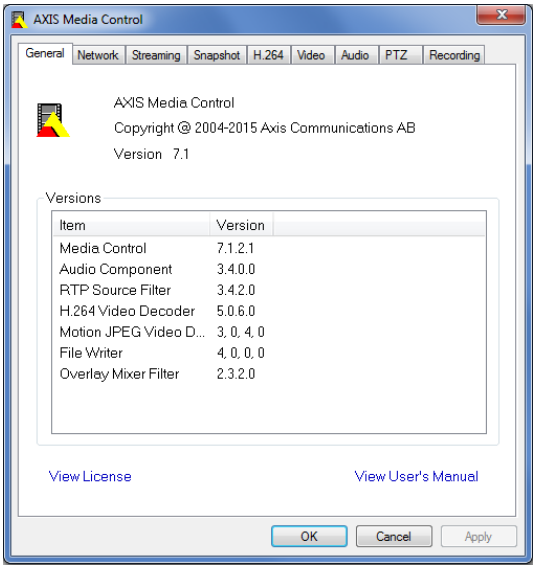
AXIS Media Control (AMC) in Internet Explorer in Windows is the recommended method of accessing live video from the Axis product.

## 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™**. The following paths can be used:
  - `rtsp://<ip>/axis-media/media.amp`
  - `rtsp://<ip>/axis-media/media.3gp`

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™** 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 47*

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 47*.
2. TCP/IP. See *page 50*.
3. Date & Time. See *page 49*.
4. Video Stream. See *page 17*.
5. Audio settings. See *How to change audio settings on page 24*.

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 17*.
- Stream profiles. See *page 20*.
- ONVIF Media Profiles. See *page 20*.
- Camera settings. See *page 20*.
- Privacy mask. See *page 24*.
- Audio settings. 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 17*.
- Audio. See *page 24*.
- H.264. See *page 18*.
- Zipstream. See *page 19*.
- MJPEG. See *page 20*.

### 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 17*. 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 22*.

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.
- **High**: The High profile provides a higher compression than both Main and Baseline profiles, but requires more processing power to decode. High profile supports 8x8 blocks, which reduces the bitrate further compared to the Main profile.

### About bitrate control

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

The built-in bitrate control can be combined with Zipstream, see *About Zipstream on page 19*. We recommend using a high bitrate limit to enable the full potential of Zipstream.

### 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 Zipstream

Axis' Zipstream Technology is a bitrate reduction technology optimized for video surveillance. Zipstream reduces the average bitrate in the H.264 stream by removing unnecessary data, which makes it possible to stream higher resolutions, reduce storage cost or keep recordings for a longer time.

To reduce the average bitrate, Zipstream reduces the bitrate in areas of the image that are less interesting from a video surveillance perspective, for example the background. Image details that are important for forensic video analysis, for example faces and license plates, are encoded with a higher bitrate.

Axis' Zipstream Technology for H.264 conforms to the H.264 standard and is compatible with third-party clients and VMS solutions that decode H.264 video.

**Recommended use of bitrate reduction**

Zipstream offers a number of bitrate reduction presets, from Low to Extreme. **Low** bitrate reduction is enabled by default and is safe to use in all applications while still reducing the bitrate.

We recommend using the **Extreme** bitrate reduction to maximize storage time for cloud-connected cameras or cameras using edge storage. This setting is suitable to combine with motion detection triggering and variable bitrate (VBR) where the bitrate is allowed to adapt to changes in complexity in the scene.

**How to save bandwidth and storage using Zipstream**

The bitrate controller built into the product can be combined with Zipstream to ensure a maximum bitrate (MBR) limit. We recommend using VBR or MBR with a high bitrate limit to enable the full potential of Zipstream.

For instance in railway surveillance where at times there is a lot of movement in the scene and where it is important to capture details, such as facial features, the MBR should be set to 10Mbit/s (for 1080p resolution at 30 fps).

To further save bandwidth go to **Setup** > **Video & Audio** > **Video Stream** and do one or more of the following:

- Go to the **Image** tab and set a low **Maximum frame rate** value.
- Go to the **H.264** tab and set a high **GOP length** value.
- Go to the **Zipstream** tab and select **Extreme** H.264 bitrate reduction.
- Go to the **Zipstream** tab. Enable **Dynamic GOP** and set a high **Max dynamic GOP length** value.
- Go to the **Zipstream** tab and enable **Dynamic FPS**.

Always verify that the video stream meets the quality requirements for your surveillance purposes after changing the video stream settings.

### 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 34*.
- When setting up continuous recording. See *About continuous recording on page 40*.
- 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 capture modes

Capture mode defines the maximum frame rate available in the Axis product and affects light sensitivity. A capture mode with a high maximum frame rate has reduced light sensitivity and vice versa.

Capture mode is set the first time the product is accessed. Select the desired capture mode and click **OK**.

Important

Changing capture mode when the product has been configured is not recommended as most other settings will be either removed or reset.

To change capture mode, follow these steps:

1. Go to **Setup > Video & Audio > Camera Settings**.
2. Select the new capture mode.

Note

When the capture mode is changed, the camera needs to reboot for the changes to take effect.

### 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.

### 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.

### Wide Dynamic Range

**Wide Dynamic Range** 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.

### Exposure Settings

Configure the exposure settings to suit the image quality requirements in relation to lighting, frame rate and bandwidth considerations.

**Exposure control –** This setting is used to adapt to the amount of light available. **Automatic** can be used in most situations. Shutter speed is automatically set to produce optimum image quality.

**Max exposure time –** Available when **Exposure control** is set to **Automatic**. Select the maximum exposure time from the drop-down list. Increasing the time improves image quality, but decreases frame rate. There may also be an increase in motion blur.

**Exposure time –** Available when **Exposure control** is set to **Manual**. Select the exposure time from the drop-down list. Increasing the time improves image quality, but decreases frame rate. There may also be an increase in motion blur.

**Max gain –** Measured in decibels (dB), gain describes the amount of amplification applied to a signal, in this case visual information in the image. A high level of amplification may provide a better image in very low light situations. A high gain will also increase the amount of image noise.

**Exposure zones –** This settings determines which part of the image is used to calculate exposure. The default setting is **Center**.

**Exposure priority –** When **Motion** is prioritized and maximum **Shutter** time is set to a small value, motion blur in the image is minimized. This can be useful for recognizing moving objects such as people and vehicles. However, prioritizing motion may cause an increase in image noise, especially in low light situations.
When **Low noise** is prioritized and **Gain** is set to a small value, image noise is minimized. The file size is also reduced, which can be useful if storage space or bandwidth is limited. However, prioritizing low noise may result in a very dark image, especially in low light situations.

### About image settings

**Image freeze on PTZ –** Select **All movements** to freeze the image while the camera is moving during a pan, tilt or zoom operation. Once the camera reaches its new position, the view from that position is shown. **Presets** freezes the image only when the camera moves between preset positions.

## 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 22*.

### 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 49*.

### How to include overlay text in an 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.
- 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 on page 22*.

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 24*.

### 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**.

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 20*.

### Audio input

Configure the audio input settings under **Audio**> **Audio Settings**.

**Source** lists the built-in microphone.

Use the **Input gain** to control the volume (dB Full Scale) of the audio input. If the sound is too low, choose a higher dB, to amplify the sound. If the sound is too high, choose a lower dB.

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

- **AAC** is used for encoding only in the Axis product. For decoding, no 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.

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 .

## How to configure the live view window

You can configure the following items for your live view window:

- **Stream Profile**. See *page 20*.
- **Default Viewer** for browsers. See *page 25*.
- **Viewer Settings**. See *page 25*.
- **Action Buttons**. See *page 11*.
- **User Defined Links**. 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 13*.

## 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.

# 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 34*.

### How to add a preset position

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. Write a name in the **Current position** field.
4. If required, select **Use current position as Home**.
5. 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.

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.

## OSDI Zones

On-Screen Direction Indicator (OSDI) zones can be included in the overlay text (see *About overlay text on page 22*) 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.

**Move speed** sets the speed of the camera's pan and tilt movements. The default setting is maximum speed.

Select **Enable adjustable zoom speed** to use variable speeds when controlling the zoom with for example a joystick or a mouse wheel. The zoom speed is automatically set through the command `continuouszoommove` in the VAPIX® Application Programming Interface (API). Deselect the feature to use the highest zoom speed which is the same speed for moving to presets.

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.

## About PTZ (Pan Tilt Zoom)

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 47*) 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 34*). 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. **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 applications

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

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

Note

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

## 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 60*.

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 57*. For information about factory default, see *How to reset to factory default settings on page 59*.

## About AXIS Audio Volume Detection

AXIS Audio Volume Detection is an application that triggers an event if the audio volume rises above or falls below the set volume reference level for a specified time period. The generated event can be used, for example, to record a video or alert security staff.

### Considerations

Before using the application, consider the following:

- To avoid false triggers, try different gain and threshold settings to optimize the performance for your environment.
- Adjust the audio input gain to a level where the background noise covers approximately 30-50% of the application's audio level graph. To access the **Input gain** setting, click the **Audio Settings** link on the application page.

### How to set the detection threshold and duration

Note

To disable detection during PTZ operation, select **Detection automatically disabled during PTZ movement**.

1. To set the detection threshold to a level where the gray line is just above the background noise level, enter a value or move the slider for **Threshold**.
2. To set the time required for the audio volume to be above the detection threshold before the trigger is activated, enter a value or move the slider for **Above Threshold (s)**.
3. To set the time required for the audio volume to be below the detection threshold before the trigger is deactivated, enter a value or move the slider for **Below Threshold (s)**.
4. Click **Save**.

An active trigger is indicated by a red color bar in the trigger status area. For more information on how to setup an event for the trigger, see *How to set up action rules on page 34*.

## About AXIS Scream Detection

AXIS Scream Detection is an application that triggers an event if a scream is detected. The generated event can be used, for example, to record a video or alert security staff.

An active trigger is indicated by a red color marker in the trigger status area. For more information on how to setup an event for the trigger, see *How to set up action rules on page 34*.

### Considerations

Before using the application, consider the following:

- The application is mainly intended for detecting screams in a generally quiet environment. The difference between the background sound level and the scream must be at least 15-20 dB for the application to function effectively. Consider the proximity to the expected sound source, the background noise level and the audio input gain level when installing the product.
- Adjust the audio input gain to a level where the background noise covers approximately 30-50% of the application's audio level graph. To access the **Input gain** setting, click the **Audio Settings** link on the application page.
- If the interval between screams is less than 3 seconds, the application regards it as one scream.

## About AXIS Removed Object Detection

AXIS Removed Object Detection is an application that triggers an event if an object in a set area is removed. The generated event can be used, for example, to record a video or alert security staff.

### Considerations

Before using the application, consider the following:

- The camera's home position is used for removed object detection by default. If you want to set a new customized home position for detection, see *How to set the home position on page 27*. We recommend that you name the new position as Home to replace the default home position with the same name. If you name the new home position something else, the name will be displayed with (H) at the end, and the default home position will still be called Home.
- If the camera moves to a new position during removed object detection, the application stops running. When you access the application again, it will request you to go back to the home position or set a new home position for it to run again.

### How to set an include area

Include areas are the areas that the application monitors for removed objects.

To add an include area:

1. Under **Areas**, go to the **Include** tab, and click **Add**.
2. To enable removed object detection in the area, select **Enable**.
3. Enter a descriptive name for the area.
4. To specify the relative size of the object compared to the set area, enter a value or move the slider for **Object size (%)**. Lower values cause the trigger to activate for smaller objects.
5. To enter the desired **Shape** for the area, click **Rectangle** or **Polygon**, and use your mouse to draw the shape to the Live View. If you use a polygon, double click to join the last corner point to the start point of the polygon.
6. If needed, drag the corners or lines to the desired position to adjust the size and shape of the areas.
7. Select a fill color for the added shape.
8. Click **Save**.

To reset the **Include area** settings, click **Reset area**.

To remove the added include area, select it under the **Include** tab, and click **Remove**.

### How to set an exclude area

Exclude areas are the areas that the application excludes from removed object monitoring.

To add an exclude area:

1. Under **Areas**, go to the **Exclude** tab, and click **Add**.
2. To exclude removed object detection in the area, select **Enable**.
3. Enter a descriptive name for the area.
4. To enter the desired **Shape** for the area, click **Rectangle** or **Polygon**, and use your mouse to draw the shape to the Live View. If you use a polygon, double click to join the last corner point to the start point of the polygon.
5. If needed, drag the corners or lines to the desired position to adjust the size and shape of the areas.
6. Click **Save**.

To reset the **Exclude area** settings, click **Reset area**.

To remove the added exclude area, select it under the **Exclude** tab, and click **Remove**.

## About applications

### About trigger evaluation time

You can set a **Trigger evaluation time (s)**, i.e. how long an object is allowed not to be visible before the trigger is activated. For more information on how to setup an event for the trigger, see *How to set up action rules on page 34*.

### How to set the current scene as untampered

The application gradually remembers the current home position scene as the untampered scene. If something changes in that scene, and you want to reset the background, click **Set as untampered scene**.

### About overlays

You can show or hide two overlays in the Live View:

- **Show area overlay** – select to show the set include or exclude areas in the Live View.
- **Show object detection overlay** – select to show detected objects in the Live View.

# 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 34* and *About actions on page 35*.

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.
2. Go to **System Options > Storage** and set up the network share. See *page 57*.

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**.
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 product's built-in help.

### About triggers

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

- **Applications** – Use installed applications to trigger the rule. See *About applications on page 30*.
- **Detectors**
  - **Live Stream Accessed** – Triggers an action rule when any stream is accessed and during edge storage playback. This can for example be used to send notifications.
- **Hardware**

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

- **Input Signal**
  - **Manual Trigger** – Triggers an action rule using the **Manual Trigger** button in the Live View page. See *About the controls in the live view window on page 11*. This can for example be used to validate actions during product installation and configuration.
  - **Virtual Inputs** – Used by VMS (Video Management System) to trigger actions. Virtual inputs can, for example, be connected to buttons in the VMS user interface.
  - **Z-Wave** – Triggers an action rule when the selected Z-Wave device changes state. This can for example be used to turn on a light when a door opens.
- **PTZ**
  - **Moving** – Triggers an action rule when the camera view moves due to a PTZ operation. This can for example be used as an additional condition to prevent an action rule triggered by motion detection to record video while the camera view moves due to a PTZ operation.
  - **Preset Reached** – Triggers an action rule when the camera stops at a preset position. This can be for example be used with the Send Images action to upload images from the preset position.
  - **Ready** – Triggers an action 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** – Triggers an action 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 an action 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** – Triggers an action 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** – Triggers an action rule periodically. See *How to set up recurrences on page 37*. This can for example be used to upload an image every 5 minutes.
  - **Use Schedule** – Triggers an action rule according to the selected schedule. See *How to create schedules on page 37*.

### About actions

You can configure several actions:

- **Overlay Text** – Display an overlay text. See *How to include overlay text in an action rule on page 22*.
- **PTZ Control**
  - **Preset Position** – Go to a preset position.
- **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.
- **Status LED** – Flash the LED indicator. This can for example be used to validate triggers such as motion detection during product installation and configuration.
- **Z-Wave** – Send a command to switch on or off the selected Z-Wave device.

## 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 36*.

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<br>Send Notification<br>Send Video Clip | An email recipient can contain multiple email addresses. |
| FTP | Send Images<br>Send Video Clip | |
| SFTP | Send Images<br>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.<br>Specify login information for the SFTP server and the server's public key MD5 fingerprint (32 hexadecimal digits).<br>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<br>Send Notification<br>Send Video Clip | |

| | | |
|---|---|---|
| HTTPS | Send Images<br>Send Notification<br>Send Video Clip | Encrypted file transfer using HyperText Transfer Protocol Secure (HTTPS).<br>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<br>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. |
| 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 48*.

## 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.

## About events

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 40*.
- To set up action rules, see *page 34*.
- To access recordings, see *How to find recordings on page 39*.
- To play recordings, see *How to play recordings on page 39*.
- To export a recording as a video clip, see *How to export a video clip on page 40*.
- To configure camera controlled storage, see *Storage on page 55*.

### 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 49*.

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 39*.

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 40*.

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.

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 39*.
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 39*.
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 55*. 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 wireless I/O (Z-Wave Plus®)

This is a security enabled Z-Wave Plus® product that can use encrypted Z-Wave Plus messages to communicate with security enabled Z-Wave Plus devices. The product can be operated in any Z-Wave network with compatible Z-Wave certified devices from other manufacturers. To increase the network reliability, all non-battery operated Z-Wave devices in the network act as repeaters regardless of vendor. This product acts as the control device and the Z-Wave devices added to it act as slaves.

## Considerations

Before using wireless I/O with Z-Wave Plus, consider the following:

- You need to be an administrator to do the Z-Wave configurations.
- When performing Z-Wave related actions on the product's web page, such as adding, removing and replacing Z-Wave devices or resetting the Z-Wave network, we recommend that you do not reload the page or move away from it when the action process is ongoing. If done, the action's actual and displayed statuses may differ. To recover, you may need to wait up to several minutes and then reload the page again.
- Replication, i.e. copying network information to another control device, is executed as part of the inclusion process.
- This product ignores all commands in the Basic Command Class.
- Some advanced Z-Wave functions are not accessible from the product's web page. Contact support to get software to access these functions.
- If the network primary controller is missing or otherwise inoperable, you need to reset to factory default settings from the product's web page. To do this, go to **Setup > System Options > Maintenance**, and click **Default**.

## Associations

- This product supports one association group with group identifier = 1 (LifeLine).
- Maximum number of devices that can be added to the association group = 1.
- Group identifier 1 is used to send the Device Reset Locally report.

## Command classes

This product supports the following command classes:

- COMMAND_CLASS_ZWAVEPLUS_INFO
- COMMAND_CLASS_TRANSPORT_SERVICE
- COMMAND_CLASS_CRC_16_ENCAP
- COMMAND_CLASS_APPLICATION_STATUS
- COMMAND_CLASS_SECURITY_2
- COMMAND_CLASS_SECURITY
- COMMAND_CLASS_INCLUSION_CONTROLLER
- COMMAND_CLASS_SUPERVISION

This product supports the following security command classes:

- COMMAND_CLASS_SECURITY
- COMMAND_CLASS_ NETWORK_MANAGEMENT_INCLUSION

- COMMAND_CLASS_NETWORK_MANAGEMENT_BASIC
- COMMAND_CLASS_NETWORK_MANAGEMENT_PROXY
- COMMAND_CLASS_NETWORK_MANAGEMENT_INSTALLATION_MAINTENANCE
- COMMAND_CLASS_MANUFACTURER_SPECIFIC
- COMMAND_CLASS_POWERLEVEL
- COMMAND_CLASS_VERSION
- COMMAND_CLASS_ASSOCIATION
- COMMAND_CLASS_ASSOCIATION_GRP_INFO
- COMMAND_CLASS_DEVICE_RESET_LOCALLY

## How to add a Z-Wave device

Though not limited by the Z-Wave Plus protocol, your product's event system allows you to add a maximum of six Z-Wave devices at any given time. If the maximum number is reached, you need to remove a Z-Wave device before you can add a new one.
See *How to remove a Z-Wave device on page 42*.

1. Go to **Setup > Wireless I/O**.
2. Select **Enable Z-Wave** and click **Save**. You may need to wait for a few minutes for Z-Wave to become active.
3. Click **Add**. The product starts looking for Z-Wave devices in the Z-Wave network.
4. Set the Z-Wave device to be added into inclusion/exclusion mode as described in its User Manual.
5. If requested, enter the PIN delivered with the Z-Wave device, and click **Enter**.
6. Wait until the adding process is finalized as indicated by **Status: Done** on the web page. The device's status information window opens.
7. Click **Refresh** to update the Z-Wave device info, e.g. battery status, and add a name for the device. Click **Save**.

The added Z-Wave device with some status information is now visible on the **Z-Wave Device List**.

Note

If the Z-Wave device is not found, the adding process is terminated automatically.

To check the more detailed status information of the added Z-Wave device, select it from the **Z-Wave Device List**, and click **Modify**.

Note

Status information for an added Z-Wave device varies depending on the device type. Fore more information, see the online help .

You can set the product to trigger action rules with specified Z-Wave trigger conditions. The available Z-Wave triggers and actions vary depending on the added Z-Wave device type. For more information, see *How to set up action rules on page 34*.

## How to remove a Z-Wave device

### How to remove a Z-Wave device through inclusion/exclusion mode

Note

This is the recommended removal procedure.

1. Go to **Setup > Wireless I/O**.
2. Click **Remove**. The product starts looking for Z-Wave devices in the Z-Wave network.
3. Set the Z-Wave device to be added into inclusion/exclusion mode as described in its User Manual.
4. Wait until the removal process is finalized as indicated by **Status: Done** on the web page.

The Z-Wave device is now removed from the **Z-Wave Device List**.

Note

All product-related information in the removed Z-Wave device is erased.

Note

If the Z-Wave device is not found, the adding process is terminated automatically.

### How to remove a Z-Wave device through forced process

There may be a communication fail e.g. due to drained battery so you may not be able to remove the Z-Wave device by setting it to inclusion/exclusion mode. You can perform a forced removal of a Z-Wave device that shows status **Unavailable** or **Sleep** in the **Z-Wave Device List**.

1. Go to **Setup > Wireless I/O**.
2. Select the Z-Wave device to be removed from the **Z-Wave Device List** and click **Modify**. The device's status information window opens.
3. Click **Remove**.
4. Click **OK** to confirm the removal.

The Z-Wave device is now removed from the **Z-Wave Device List**.

Note

All product-related information in the removed Z-Wave device is retained.

## How to replace a Z-Wave device

There may be a communication fail e.g. due to a faulty Z-Wave device, and you want to replace the device with another one. You can perform a forced replacement of a Z-Wave device that shows status **Unavailable** or **Sleep** in the **Z-Wave Device List**.

1. Go to **Setup > Wireless I/O**.
2. Select the Z-Wave device to be replaced from the **Z-Wave Device List** and, click **Modify**. The device's status information window opens.
3. Click **Replace**. The product starts looking for Z-Wave devices in the Z-Wave network.
4. Set the Z-Wave device that is to replace the existing device into inclusion/exclusion mode as described in its User Manual.
5. Wait until the replacement process is finalized as indicated by **Status: Replacing (found node)** on the web page.

The new Z-wave device with some status information is now visible on the **Z-Wave Device List**.

Note

Node ID and event action information is handed over to the new Z-Wave device. All other information is erased.

Note

If the Z-Wave device is not found, the replacement process is terminated automatically.

# About wireless I/O (Z-Wave Plus®)

## How to reset the Z-Wave network

Important

- This procedure removes all Z-Wave devices from the product.
- Use this procedure only when the network primary controller is missing or otherwise inoperable.

1. Go to **Setup > Wireless I/O**.
2. Click **Reset**.
3. Click **OK** to confirm the reset.

All added Z-Wave devices are now removed from the product, and the **Z-Wave Device List** is empty.

## How to make the camera's LED flash when the Z-Wave device's battery is low

1. Go to **Setup > Events > Action Rules** and click **Add**.
2. Select **Enable rule** and enter a descriptive name for the rule.
3. Under **Trigger**, select **Input Signal**.
4. Select **Z-Wave**.
5. Select **<device name> - Battery**.
6. Under **Actions**, select **Status LED**.
7. Select **Flash for 1 seconds** and change the time to 9999 seconds.
8. Select **LED Color**.
9. Click OK.

## How to direct the camera to a preset position when the wireless PIR motion sensor detects motion

Note

There may up to 2 s delay from when the motion is detected to when the camera triggers the action rule. Consider this latency when deciding the best placement of the products.

Add a preset position:

1. Go to **PTZ** and set where you want the camera to be directed by creating a preset position.

Create an action rule for the PIR sensor:

2. Go to **Setup > Events > Action Rules** and click **Add**.
3. Select **Enable rule** and enter a descriptive name for the rule.
4. Under **Trigger**, select **Input Signal**.
5. Select **Z-Wave**.
6. Select **<device name> - Motion Detected**.
7. Under **Actions**, select **PTZ Control**.
8. Select **Preset Position**.

9. Select the preset position you want the camera to go to.
10. If you want the camera to return to it's home position, select **Return to home when the rule is no longer active** and specify how long you want the camera to wait at the current preset position before returning to home.
11. Click **Ok**.

To record video, add an additional action rule:

12. Go to **Events > Action Rules** and click **Add**.
13. Select **Enable rule** and enter a descriptive name for the rule.
14. From the list of triggers, select **PTZ** and then select **Preset Reached**.
15. Select the preset position.
16. From the list of actions, select **Record video**.
17. Select an existing stream profile or create a new one.
18. Enable and set the pre-trigger time to 5 seconds.
19. Enable **While the rule is active**.
20. Enable and set the post-trigger time to 60 seconds.
21. Select **SD card** from the list of storage options.
22. Click **Ok**.

## About using Z-Wave as I/O

This product does not have any physical I/O connectors, but you can use some Z-Wave functions through the I/O interface.

Each connected Z-Wave device is assigned an I/O port number. To see the port numbers, go to **Setup > System Options > Ports & Devices > I/O Ports**. The I/O port number can be changed in the Z-Wave device's information window.

When used as an Digital Input Port event, only one function of the Z-Wave device can be used. The default function depends on what type of device it is. To change which function is used, go to the device's information window.

For more information about using I/O ports see the product's built-in help.

## 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.

### ONVIF

ONVIF is an open industry forum that provides and promotes standardized interfaces for effective interoperability of IP-based physical security products.

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).

### 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.

## About system options

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 48*.

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 48*.

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 49*.

### 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 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 49*.
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 24*.

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 52*.

  If using a host name for the NTP server, a DNS server must be configured. See *DNS Configuration on page 51*.
- **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 59*) 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 an IP address using ARP/Ping on page 50*.

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 an IP address using ARP/Ping

The device'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 device 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. Restart the device by disconnecting and reconnecting the network connector.
5. Close the command prompt when the device responds with `Reply from 192.168.0.125:...` or similar.
6. Open a browser and type `http://<IP address>` in the address field.

For other methods of assigning the IP address, see the document *How to assign an IP address and access your device* at *www.axis.com/support*

Note

- To open a command prompt in Windows, open the **Start** menu and search for `cmd`.
- 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 ) 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 or possible 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.

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 47*.

**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®.
- 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. Note that UPnP 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 47*. 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 59*.

### 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 microSD/microSDHC/microSDXC 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.

## About system options

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 **General 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 **General Settings**.

## 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 59*.

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

To identify the product or test the Status LED, click **Flash LED** under **Identify** and specify the duration in seconds, minutes or hours. This can be useful for identifying the product among other products installed in the same location.

For information about firmware upgrade, see *How to upgrade the firmware on page 60*.

## 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 60*.

### 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).

**View Server Report –** Provides information about the product status in a pop-up window. The access log is automatically included in the server report.

**Download Server Report –** Creates a .zip file that contains a complete server report text file in UTF–8 format. Select the **Include snapshot from Live View** option to include a snapshot of the product's Live View. The .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 59*.

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 *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**.

# Troubleshooting

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

## 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 **Choose file** 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 Device Manager can be used for multiple upgrades. See *www.axis.com* for more information.

## 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. Make sure the Ping length is set to 408. For instructions, see *Assign an IP address using ARP/Ping on page 50*. |
| 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. |

## Troubleshooting

| | |
|---|---|
| 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):<br>• If you receive: `Reply from <IP address>: bytes=32; time=10...` this means that the IP address may already be in use by another device on the network. Obtain a new IP address from the network administrator and reinstall the product.<br>• 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, make sure that the correct protocol (HTTP or HTTPS) is used when attempting to log in. You may need to manually type `http` or `https` in the browser's address field.<br><br>If the password for the user root is lost, the product must be reset to the factory default settings. See *How to reset to factory default settings on page 59*. |
| The IP address has been changed by DHCP | IP addresses obtained from a DHCP server are dynamic and may change. If the IP address has been changed, use AXIS IP Utility or AXIS Device Manager to locate the product on the network. Identify the product using its model or serial number, or by the DNS name (if the name has been configured).<br><br>If required, a static IP address can be assigned manually. For instructions, see the document *How to assign an IP address and access your device* on the product page at *axis.com* |
| 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 49*. |

**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 52*. 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 13*.<br><br>In the AMC Control Panel, select the H.264 tab and click **Set to default H.264 decoder**.<br><br>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.<br><br>Check with your network administrator to see if there is a firewall preventing viewing. |

## Troubleshooting

| | |
|---|---|
| Poor rendering of H.264 images | Make sure 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 | Update 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 65*. |
| | 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**. |

**No audio**

| | |
|---|---|
| Incorrect setup | Check the sound card in the computer. Make sure 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. |

**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 34*. |
| 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. |

## Troubleshooting

| Product does not function | |
|---|---|
| The product does not start and the camera is no longer accessible. | Remove power from the product. Wait for 10 minutes, then reapply power. |

# Specifications

To find the latest version of the product's datasheet, go to the product page at *axis.com* and locate **Support & Documentation**.

## LED Indicators

Note

- The Status LED can be configured to flash while an event is active.
- The Status LED can be configured to flash for identifying the unit. Go to **Settings > System > Plain config**.

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

## SD card slot

***NOTICE***

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

This product supports microSD/microSDHC/microSDXC cards.

For SD card recommendations, see *axis.com*

microSD, microSDHC, and microSDXC Logos are trademarks of SD-3C LLC. microSD, microSDHC, microSDXC are trademarks or registered trademarks of SD-3C, LLC in the United States, other countries or both.

## Buttons

### Control button

For location of the control button, see *Hardware overview on page 9* .

The control button is used for:

- Resetting the product to factory default settings. See *page 59*.
- Connecting to an AXIS Video Hosting System service. See *page 51*. 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 51*. To connect, press and hold the button for about 3 seconds.

## Connectors

### Network connector

RJ45 Ethernet connector with Power over Ethernet (PoE).

## Performance considerations

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

The following factors are the most important to consider:

- High image resolution or lower compression levels result in images containing more data which in turn affects the bandwidth.
- Rotating the lens manually will result in better performance compared to rotating the image from the GUI.
- Access by large numbers of Motion JPEG or unicast H.264 clients affects the bandwidth.
- Simultaneous viewing of different streams (resolution, compression) by different clients affects both frame rate and bandwidth.

  Use identical streams wherever possible to maintain a high frame rate. Stream profiles can be used to ensure that streams are identical.
- Accessing Motion JPEG and H.264 video streams simultaneously affects both frame rate and bandwidth.
- Heavy usage of event settings affects the product's CPU load which in turn affects the frame rate.
- Using HTTPS may reduce frame rate, in particular if streaming Motion JPEG.
- Heavy network utilization due to poor infrastructure affects the bandwidth.
- Viewing on poorly performing client computers lowers perceived performance and affects frame rate.
- Running multiple AXIS Camera Application Platform (ACAP) applications simultaneously may affect the frame rate and the general performance.

User Manual
AXIS M5065 PTZ Network Camera
© Axis Communications AB, 2017 - 2018
Ver. M3.7
Date: November 2018
Part No. T10113315