AXIS P3905-R Mk II Network Camera

User manual

About this Document

This manual is intended for administrators and users of the AXIS P3905–R Mk II 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 beneficial, for developing shell scripts and applications. Later versions of this document will be posted to the Axis website, as required. See also the product's online help, available via the web-based interface.

Legal considerations

Video 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 licenses:
- 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, ARTPEC and VAPIX are registered trademarks of Axis AB in various jurisdictions. All other trademarks are the property of their respective owners.

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.

Regulatory information

Europe

CE

This product complies with the applicable CE marking directives and harmonized standards:
- Electromagnetic Compatibility (EMC) Directive 2014/30/EU. See .
- Low Voltage Directive (LVD) 2014/35/EU. See .
- Restriction of Hazardous Substances (RoHS) Directive 2011/65/EU and 2015/863, including any amendments, updates or replacements. See .

A copy of the original declaration of conformity may be obtained from Axis Communications AB. See .

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機器です。この装置を住宅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。 VCCI – A

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。

本製品は電気通信事業者（移動通信会社、固定通信会社、インターネットプロバイダ等）の通信回線（公衆無線 LAN を含む）に直接接続することができません。本製品をインターネットに接続する場合は、必ずルータ等を経由し接続してください。

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.

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.

The power supply used with this product shall fulfill one of the following requirements:
- Safety Extra Low Voltage (SELV) according to clause 2.2 of IEC/EN/UL 60950-1 and Limited Power Source (LPS) according to clause 2.5 of IEC/EN/UL 60950-1 or CEC/NEC Class 2 source of supply as defined in the Canadian Electrical Code, CSA C22.1 and National Electrical Code, ANSI/NFPA 70
- Class 1 electrical energy source (ES1) and Class 2 power source (PS2) rated output power limited to ≤100 W according to IEC/EN/UL 62368-1

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.

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 and 2015/863 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS).

China

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

	有毒有害物质或元素					
部件名称	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr(VI))	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
电气实装部分	X	0	0	0	0	0

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

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

Contact information
Axis Communications AB
Gränden 1
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/learning* for useful trainings, webinars, tutorials and guides.

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.

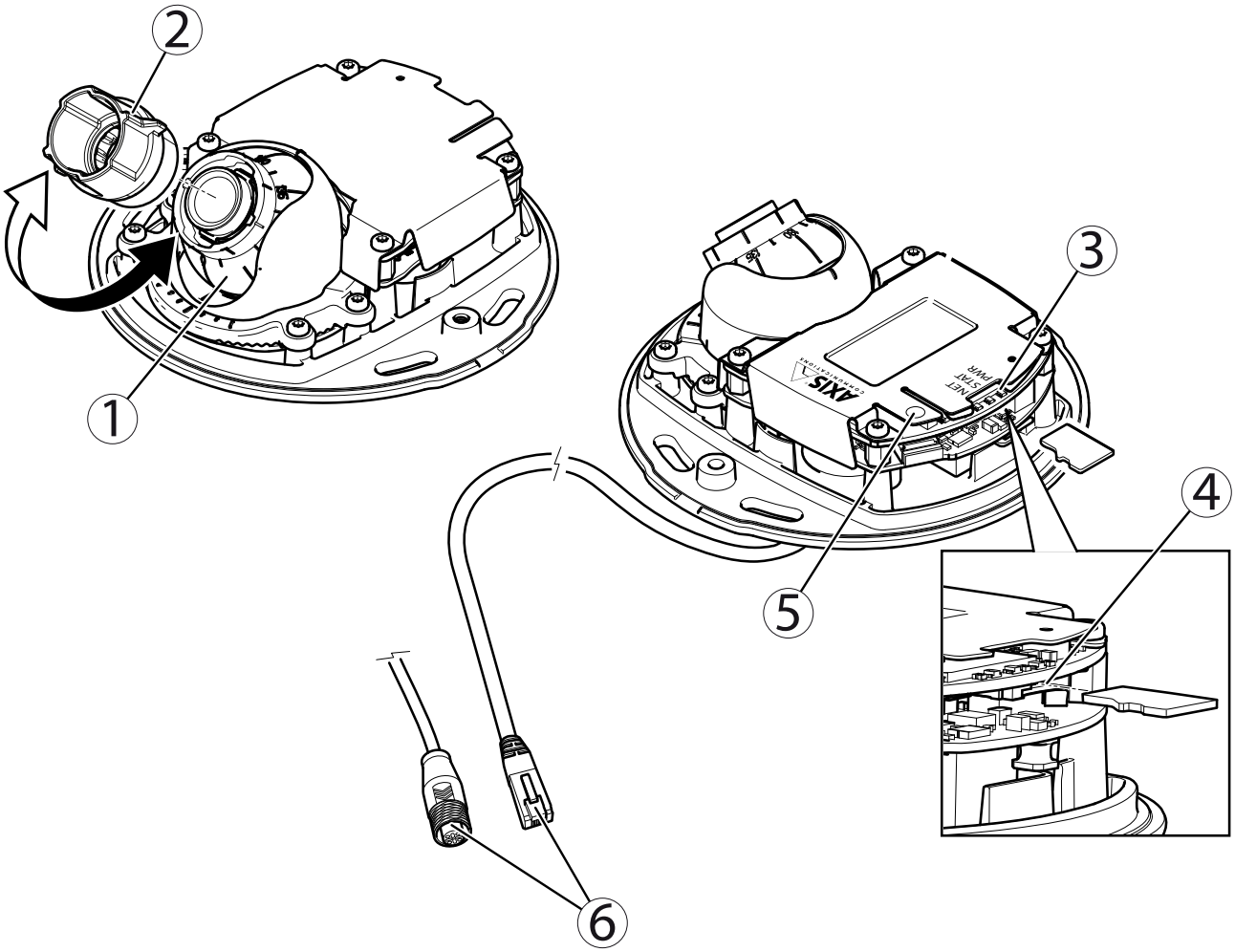
NOTICE
Indicates a situation which, if not avoided, could result in damage to property.

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.

Product overview



1 *Optic assembly*
2 *Lens tool*
3 *LED indicators*
4 *SD card slot (microSD)*
5 *Control button*
6 *Network connector M12/RJ45*

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. The license is 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.

Access the device

1. Open a browser and enter the IP address or host name of the Axis device.
   If you do not know the IP address, use AXIS IP Utility or AXIS Device Manager to find the device on the network.
2. Enter the username and password. If you access the device for the first time, you must set the root password. See .
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 .

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 .

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

Set Power Line Frequency

Power line frequency is set the first time the Axis product is accessed and can only be changed from Plain Config (see) or by resetting the product to factory default.

Select the power line frequency (50 Hz or 60 Hz) used at the location of the Axis product. Selecting the wrong frequency may cause image flicker if the product is used in fluorescent light environments.

When using 50 Hz, the maximum frame rate is limited to 25 fps.

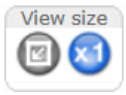
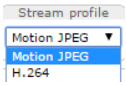
Note

Power line frequency varies depending on geographic region. The Americas usually use 60 Hz, whereas most other parts of the world use 50 Hz. Local variations could apply. Always check with the local authorities.

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.

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 .
	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 .
	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**.

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 .

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**.

AXIS Media Control viewer toolbar

The AXIS Media Control viewer toolbar is available in Internet Explorer only. See 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.**

PTZ Controls

Note

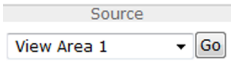
These controls are available if digital PTZ is enabled in the selected view area, see .

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


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


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

The center mode button could also be used to zoom in on a specific area. Click in the image and drag to draw a rectangle surrounding the area to be magnified. To zoom out, rotate the mouse wheel.



To view a specific view area or preset position, select it from the **Source** list.

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

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

The PTZ controls can be disabled under **PTZ > Advanced > Controls**, see .

Media streams

The Axis product provides several 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, and to the list of available stream profiles. Other applications and clients can access video streams directly, without going via the live view window.

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:

<table>
<tr><td>Unicast RTP</td><td>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.</td><td rowspan="3">Unicasting is used for video-on-demand transmission so that there is no video traffic on the network until a client connects and requests the stream.

Note that there are a maximum of 20 simultaneous unicast connections.</td></tr>
<tr><td>RTP over RTSP</td><td>This unicast method (RTP tunneled over RTSP) is useful as it is relatively simple to configure firewalls to allow RTSP traffic.</td></tr>
<tr><td>RTP over RTSP over HTTP</td><td>This unicast method can be used to traverse firewalls. Firewalls are commonly configured to allow the HTTP protocol, thus allowing RTP to be tunneled.</td></tr>
<tr><td>Multicast RTP</td><td colspan="2">This method (RTP over UDP) should be used for live multicast video. The video stream is always up-to-date, even if some frames are dropped.

Multicasting provides the most efficient usage of bandwidth when there are large numbers of clients viewing simultaneously. A multicast cannot however, pass a network router unless the router is configured to allow this. It is not possible to multicast over the Internet, for example. Note also that all multicast viewers count as one unicast viewer in the maximum total of 20 simultaneous connections.</td></tr>
</table>

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.

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.

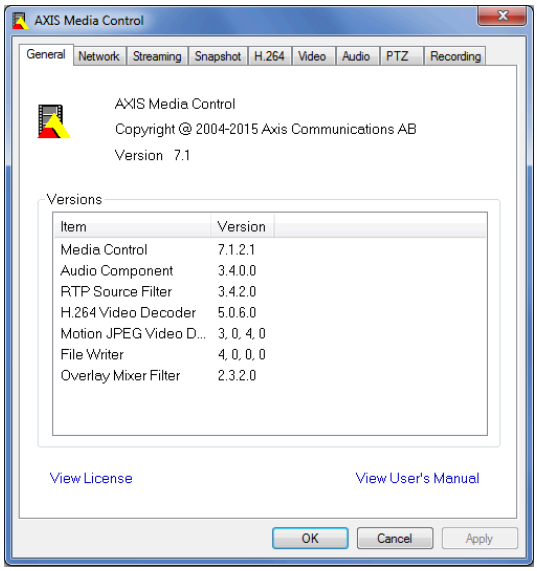
AXIS Media Control (AMC)

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

The AMC Control Panel can be used to configure various video 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**.



Access the video stream

You can access the video stream and still images from the Axis device in different ways.

Important

For these commands to work, the device must have a root account.

- **Still JPEG images in a browser**: enter the path `http://<ip-address>/axis-cgi/jpg/image.cgi`
- **RTSP streaming through most media players (for example VLC)**: enter the path `rtsp://<ip-address>/axis-media/media.amp`
- **ONVIF streaming (for devices with an ONVIF user configured)**: enter the path `rtsp://<ip-address>/onvif-media/media.amp`

You can find more ways to access the video stream in VAPIX® Library.

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

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 .
2. TCP/IP. See .
3. Date & Time. See .
4. Video Stream. See .

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

Video settings

It is possible to configure the following video features in your Axis product:

- Video stream. See .
- Stream profiles. See .
- ONVIF Media Profiles. See .
- Camera settings. See .
- View areas. See .
- Overlay image. See .
- Privacy mask. See .

How to set up video streams

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

The video stream settings are divided into the following tabs:

- Image. See .
- H.264. See .
- Zipstream. See .
- MJPEG. See .

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, **Video & Audio > Video Stream**. 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 > 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.
- **Mirror image**. If required, the image can be mirrored.
- **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 .

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

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.

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.

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.

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 . We recommend using a high bitrate limit to enable the full potential of Zipstream.

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.

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 > 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 > Video Stream > Overlay Settings**.
2. In the **Include text** field enter #b.
3. Click **Save**.

Axis Zipstream technology

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** > **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.

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.

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 .
- When setting up continuous recording. See .
- 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** > **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.

Camera settings

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

Image appearance

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

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

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

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

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

White balance

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

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

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

Wide Dynamic Range

Wide dynamic range (WDR - forensic capture) provides balanced images in scenes where there is a considerable contrast between light and dark areas in the image. The camera automatically handles the transition between such scenes and low-light conditions.

Important

Use WDR in combination with automatic exposure control. Other exposure settings could produce undesirable results.

Traffic Light mode

This mode will decrease the exposure, so that traffic lights and other bright light sources will not saturate when in view at night. In this mode, it is possible to distinguish the color of the traffic lights at any surrounding light level. This mode is also favorable for license plate recognition.

Note

The decrease in exposure will make the whole image darker, during conditions above.

This setting will disable the Exposure Settings for best results.

Exposure settings

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

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

Exposure control – Select a suitable option to control exposure.

For most scenes, the **Automatic** option will provide the best results. The shutter speed is automatically set to produce optimum image quality. Fluorescent lamps or other light sources can sometimes cause flickering in the image. To reduce flicker in the image, select the **Flicker** option that matches the power line frequency.

The **Hold current** option locks the current exposure settings.

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

Exposure zones – This setting determines which part of the image is used to calculate the exposure. For most situations, the **Auto** setting can be used.

You can select a predefined area by defining Include and Exclude windows within the image. Exclude windows exclude areas that are too bright or dark, and Include windows include areas in the scene that have better lighting which will contribute to the exposure data.

There must be at least one Include window. There can be a total of ten Include and Exclude windows to tailor the exposure zone.

Note that an Exclude window is effective only when placed inside an include window.

Tip: If an area is extremely bright, draw an Include window to cover the whole area and define Exclude windows within it to block out the bright areas.

How to set up normal and low light

When **Shutter** and **Gain** are both set to **Auto**, it is possible to set the **Priority** between low motion blur and low noise manually and to use a different **Priority** in **Normal Light** and in **Low Light**.

Example:

Consider an area where people or vehicles move during the day, but where there should be no movement at night. To be able to, for example, recognize faces or license plates, move the normal light priority slider toward low motion blur. At night time, motion detection is more important than identification. Motion blur is acceptable and since low light can cause a lot of noise, move the low light priority slider toward low noise.

Normal light priority

1. Use the slider to set the **Priority** between **Low motion blur** and **Low noise**. When prioritizing low noise (slider all the way to the left), the camera will automatically decrease shutter speed as brightness decreases. When the shutter speed reaches 1/30 s, the camera increases gain until the set maximum gain for normal light is reached.

Low light priority

2. Use the slider to set the **Priority** between **Low motion blur** and **Low noise**. When prioritizing low motion blur (slider all the way to the right), the camera automatically increases gain as brightness decreases. When the gain reaches the set maximum gain for low light, the camera will decrease shutter speed until the set maximum shutter for low light is reached. This is the default priority setting for low light.
3. Select the **Max gain** value from the drop-down list. This defines the upper limit for gain in the context of normal light.
4. **Max fast shutter** sets the shutter speed limit in normal light. Depending on the scenario, the shutter speed limit may need to be defined. This is done through **System Options** > **Advanced** > **Plain Config**.

View Area

A view area is a cropped part of the full view. Each view area is treated as a video source in **Live View** and has its own video stream and PTZ settings.

When setting up a view area, it is recommended that the video stream resolution is the same size as or smaller than the view area size. Setting the video stream resolution larger than the view area size implies digitally scaled up video after sensor capture, requiring more bandwidth without adding image information.

To enable, go to **Video > Camera Settings** and select **Enable View Areas**.

To add a new view area:

1. Go to **Video > View Area**.
2. Click **Add**.
3. The new view area appears under **Selected view area**. Enter a descriptive name in the **Name** field.
4. Select an **Aspect ratio** and a **Video stream resolution**.
5. A new view area covers the whole image. Use the mouse to move and resize the view area.
6. Select **Enable PTZ** to enable digital PTZ for the view area.
7. Click **Save** to save the settings.

To modify a view area, select the view area in the list and modify the settings as required. Click **Save**.

To remove a view area, select the view area and click **Remove**.

Note

The PTZ functionality is useful during installation of the Axis product. Use a view area to crop out a specific part of the full view.

Overlays

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

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

How to include overlay text

1. Go to **Video > 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 .

How to include overlay text in an action rule

Note

To display overlay text in multiple view areas, overlay text must be enabled in each view area.

1. Go to **Video > 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.

About overlay images

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

Image specifications:

- The uploaded image should be a Windows 24-bit BMP image with maximum 250 colors.
- The image width and height, in pixels, must be exactly divisible by four.
- The image cannot be larger than the maximum image resolution.
- If you combine a text overlay with and image overlay, the text overlay always takes presidence over the overlay image in height. A text overlay always stretches across the whole video image which means you cannot shrink the overlay strip to make room for an image. For information about the different text overlay heights, see .

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 .

How to upload an overlay image

1. Go to **Video > 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 > Overlay Image**.
2. Select the image to use from the **Use overlay image** list and click **Save**.
3. Go to **Video > 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**.

Privacy masks

A privacy mask is a user-defined area that covers parts of the monitored area. Privacy masks appear as blocks of solid color and are applied on the video stream. Privacy masks cannot be bypassed using the VAPIX® application programming interface (API).

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

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 configure the live view window

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

- **Stream Profile**. See .
- **Default Viewer** for browsers. See .
- **Viewer Settings**. See .
- **Action Buttons**. See .
- **User Defined Links**. See .

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 .

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 .

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.

PTZ (Pan Tilt Zoom)

PTZ (pan, tilt and zoom) is available if you have enabled digital PTZ in the selected view area. For more information on view areas, see .

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

Each view area has its own preset positions.

How to access the preset positions

Preset positions can be accessed in several ways:

- By selecting the preset from the **Source** drop-down list in the Live View Page.
- When setting up action rules. See .
- When setting up guard tours. See .

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

How to include the preset position name in an overlay text

1. Go to **Video**.
2. Select **Include text**.
3. Write the modifier `#P` in the field.
4. Click **Save**.

How to set the home position

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

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 after** field and click **Save**. Set the time to zero to prevent the product from automatically returning to the **Home** position.

About guard tours

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

Note

For products supporting limited guard tours, the pause between successive guard tours is at least 10 minutes, and the fixed minimum viewing time is 10 seconds.

How to create a guard tour

1. Go to **Setup > PTZ > Guard Tour**.
2. Click **Add**.
3. Type a name.
4. Specify the pause length between runs.
5. Select a preset position from the drop-down list and click **Add**.
6. For each preset position, enter the **View Time** in seconds or minutes.
7. Specify the **View Order** of the preset positions, or select **Random view order**.
8. Click **Save**.

How to edit a guard tour

1. Go to **Setup > PTZ > Guard Tour**.
2. Select the guard tour in the **Guard Tour List**.
3. Click **Modify**.

How to delete a guard tour

1. Go to **Setup > PTZ > Guard Tour**.
2. Select the guard tour in the **Guard Tour List**.
3. Click **Remove**.

Advanced

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

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

If using multiple view areas, deselecting a control will only disable the control in the selected view area.

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.

Control queue

Note

- The administrator can enable and disable PTZ controls for selected users.
- To identify different users in the viewer group, cookies must be enabled on the client.
- The **Control queue polltime** is measured in seconds. For more information see the online help .

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

A user who belongs to a group (see) 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). The event will immediately be placed first in the queue except when an administrator is in control.
3. **Operator** — Same as administrator but with lower priority
4. **Guard Tour** — A guard tour (see) has PTZ control for an indefinite period of time. It may be overridden by an operator, event or administrator. The guard tour will resume when higher priority groups leave the queue.
5. **Viewer** — Multiple viewers must wait for their turn. The viewer has 60 seconds PTZ control before control is passed on to the next viewer in queue.

Detectors

Camera tampering

Camera Tampering can generate an alarm when the camera is repositioned, or when the lens is covered, spray-painted or severely de-focused. To send an alarm, for example via email, an action rule must be set up.

How to configure tampering detection

1. Go to **Detectors > Camera Tampering**.
2. Set the **Minimum duration**, that is the time that must elapse before an alarm is generated. Increase time to prevent false alarms for known conditions that affect the image.
3. Select **Alarm for dark images** if an alarm should be generated when lights are dimmed or turned off, or if the lens is sprayed, covered, or rendered severely out of focus.
4. Click **Save**.

How to configure an action rule for tampering alarm

1. Go to **Events > Action Rules**.
2. Click **Add** to set up a new action rule.
3. Enter a **Name** for the action rule.
4. Under **Condition**, select **Detectors** from the **Trigger** list.
5. Select **Tampering** from the list of detectors.
6. Optionally, select a schedule and set additional conditions.
7. Select the action. **Example:** To send an email, select **Send Notification** and select a **Recipient** from the list of defined recipients.

Note

The **While the rule is active** option under **Duration** cannot be used with camera tampering, since camera tampering does not have a duration and once it has been triggered it will not automatically return to its untriggered state.

For more information on actions rules, see .

Applications

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

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

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.

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 .

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 . For information about factory default, see .

Set up rules for events

You can create rules to make your device perform an action when certain events occur. A rule consists of conditions and actions. The conditions can be used to trigger the actions. For example, the device can start a recording or send an email when it detects motion, or show an overlay text while the device is recording.

To learn more, check out our guide *Get started with rules for events*.

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 and .

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 .

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.

Triggers

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

- **Applications** – Use installed applications to trigger the rule. See .
- **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.

– **Tampering** – Triggers an action rule when tampering is detected. See .

- **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.

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

• **Input Signal**

- **Manual Trigger** – Triggers an action rule using the **Manual Trigger** button in the Live View page. See . 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.

• **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.

• **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 . 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 .

Actions

You can configure several actions:

• **Overlay Text** – Display an overlay text. See .

• **PTZ Control**

- **Preset Position** – Go to a preset position.
- **Guard Tour** – Start a guard tour. See .

• **Record Video** – Record video to a selected storage.

• **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.

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 .

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**.

Recipient types

The following recipient types are available:

	Use with action	Notes
Email	Send Images Send Notification Send Video Clip	An email recipient can contain multiple email addresses.
FTP	Send Images Send Video Clip	
SFTP	Send Images Send Video Clip	Encrypted file transfer using SSH File Transport Protocol (SFTP). SFTP is a more secure method than FTP but file transfer might be slower, especially for large files such as high resolution video. Specify login information for the SFTP server and the server's public key MD5 fingerprint (32 hexadecimal digits).The SFTP recipient supports SFTP servers using SSH-2 with RSA and DSA host key types. RSA is the preferred method. To use DSA, disable the RSA key on the SFTP server.
HTTP	Send Images Send Notification Send Video Clip	
HTTPS	Send Images Send Notification Send Video Clip	Encrypted file transfer using HyperText Transfer Protocol Secure (HTTPS). Specify login information for the HTTPS server and validate the server's certificate. If there is a proxy between the Axis product and the HTTPS server, also specify the proxy settings.

Network Share	Send Images Send Video Clip	A network share can also be used as a storage device for recorded video. Go to **System > 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 .

How to create schedules

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

To create a new schedule:

1. Go to **Events > Schedules** and click **Add**.
2. Enter a descriptive name and the information needed for a daily, weekly, monthly or yearly schedule.
3. Click **OK**.

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

How to set up recurrences

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

To set up a recurrence:

1. Go to **Events > Recurrences** and click **Add**.
2. Enter a descriptive name and recurrence pattern.
3. Click **OK**.

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

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

Recordings

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

- To start a continuous recording, see .
- To set up action rules, see .
- To access recordings, see .
- To play recordings, see .
- To export a recording as a video clip, see .
- To configure camera controlled storage, see .

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 .

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 .

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 .

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 .
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 .
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.

Continuous recording

The Axis product can be configured to continuously save video to a storage device. For information about storage devices, see . 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.
5. Click **Save** to save and start the recording.

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.

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.

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 .

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.

Certificates

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

Server/Client certificates – To authenticate the Axis product. A **Server/Client** certificate can be self-signed or issued by a Certificate Authority (CA). A self-signed certificate offers limited protection and can be used before a CA-issued certificate has been obtained.

CA certificates – To authenticate peer certificates, for example the certificate of an authentication server. 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 .
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.

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 .
  If using a host name for the NTP server, a DNS server must be configured. See .
- **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** 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) 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 .

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 .

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.

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 . 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 .

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 ports are automatically selected. For multicast streams, only certain IP addresses and port numbers should be used.

Select **Always Multicast Video** 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

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.

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.

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**.

Ports & Devices

Port Status

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

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

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 .

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 .

Support

Support Overview

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

See also .

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 .

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.

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

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 .
The product is located on a different subnet	If the IP address intended for the product and the IP address of the computer used to access the product are located on different subnets, you will not be able to set the IP address. Contact your network administrator to obtain an IP address.

The IP address is being used by another device	Disconnect the Axis product from the network. Run the Ping command (in a Command/DOS window, type `ping` and the IP address of the product): • If you receive: `Reply from <IP address>: bytes=32; time=10...` this means that the IP address may already be in use by another device on the network. Obtain a new IP address from the network administrator and reinstall the product. • If you receive: `Request timed out`, this means that the IP address is available for use with the Axis product. Check all cabling and reinstall the product.
Possible IP address conflict with another device on the same subnet	The static IP address in the Axis product is used before the DHCP server sets a dynamic address. This means that if the same default static IP address is also used by another device, there may be problems accessing the product.

The product cannot be accessed from a browser

Cannot log in	When HTTPS is enabled, 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. If the password for the user root is lost, the product must be reset to the factory default settings. See .
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). 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*

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 . 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 . In the AMC Control Panel, select the H.264 tab and click **Set to default H.264 decoder**. Check that RTSP is enabled under **System Options > Network > TCP/IP > Advanced**.

Multicast H.264 only accessible by local clients	Check if your router supports multicasting, or if the router settings between the client and the product need to be configured. The TTL (Time To Live) value may need to be increased.
No multicast H.264 displayed in the client	Check with your network administrator that the multicast addresses used by the Axis product are valid for your network. Check with your network administrator to see if there is a firewall preventing viewing.
Poor rendering of H.264 images	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 . 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.

Status and Network indicator LEDs are flashing red rapidly

Hardware failure	Contact your Axis reseller.

Product does not start up

Product does not start up	If the product does not start up keep the network cable connected and re-insert the power cable to the midspan.

Video and image problems, general

Image unsatisfactory	Check the video stream and camera settings under **Setup > Video > Video Stream** and **Setup > Video > Camera Settings**.
Disturbed focus	Set the focus manually by gently push and turn the focus ring. Set the focus manually by using the black rubber side of the lens tool. Insert the tool carefully and hold pressed while turning to adjust focus.

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 .
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.

Specifications

LED Indicators

Note

- The Status LED can be configured to be unlit during normal operation. To configure, go to **Settings > System > Plain config**.
- 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
Green	Steady green for normal operation.
Amber	Steady during startup. Flashes when restoring settings.
Red	Firmware upgrade failure.

Note

The Network LED can be disabled so that it does not flash when there is network traffic. To configure, go to **Settings > System > Plain config**.

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

Power LED	Indication
Green	Normal operation.
Amber	Flashes green/amber during firmware upgrade.

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 .
The control button is used for:

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

Connectors

Network connector

The Axis product is available in two variants with different network connectors:

RJ45 Ethernet connector with Power over Ethernet (PoE).

D-coded M12 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 image in the GUI will increase the product's CPU load.
- Access by large numbers of Motion JPEG or unicast H.264 clients affects the bandwidth.
- 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.

T10116798

2022-06 (M7.2)