AXIS A8105-E Network Video Door Station

User Manual

About this Document

This manual is intended for administrators and users of AXIS A8105–E Network Video Door Station, and is applicable to firmware 1.58.2 and later. It includes instructions for using and managing the product on your network. Previous experience of networking will be of use when using this product. Some knowledge of UNIX or Linux-based systems may also be useful when developing shell scripts and applications. Later versions of this document will be posted at *www.axis.com*. See also the product's online help, available through the web-based interface.

Legal considerations

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

This product includes the following licences:

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

To purchase further licenses, contact your reseller.

Liability

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

Intellectual property rights

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

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

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

Equipment modifications

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

Trademark acknowledgements

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

Apple, Apache, Bonjour, Ethernet, Internet Explorer, Linux, Microsoft, Mozilla, Real, SMPTE, QuickTime, UNIX, Windows, and WWW are registered trademarks of the respective holders. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates. The UPnP Word Mark and UPnP Logo are trademarks of Open Connectivity Foundation, Inc. in the United States or other countries.

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

Regulatory information

Europe

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

- Electromagnetic Compatibility (EMC) Directive 2014/30/EU. See *Electromagnetic compatibility (EMC) on page 2* .
- Low Voltage Directive (LVD) 2014/35/EU. See *Safety on page 3* .
- Restriction of Hazardous Substances (RoHS) Directive 2011/65/EU and 2015/863, including any amendments, updates or replacements. See *Disposal and recycling on page 3* .

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

Electromagnetic compatibility (EMC)
This equipment has been designed and tested to fulfill applicable standards for:

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

USA

This 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 an unshielded network cable (UTP) and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. This equipment has also 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.

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

The power supply used with this product shall fulfill the requirements for Safety Extra Low Voltage (SELV) and Limited Power Source (LPS) according to IEC/EN/UL 62368-1.

Battery

The Axis product uses a 3.0 V CR2032 lithium battery as the power supply for its internal real-time clock (RTC). Under normal conditions this battery will last for a minimum of five years.

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

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
Emdalavägen 14
223 69 Lund
Sweden

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

axis.com

Warranty information

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

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*

Learn more!

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

AXIS A8105-E Network Video Door Station

Table of Contents

AXIS A8105-E Network Video Door Station

Table of Contents

Safety information

Hazard levels

⚠DANGER

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

⚠WARNING

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

⚠CAUTION

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

NOTICE

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

Other message levels

Important

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

Note

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

Requirements for Compliance with UL294 6th Edition

This section contains information and instructions required for UL compliance. To make sure the installation is UL compliant, follow the instructions below in addition to the general information and instructions provided throughout this document. In cases where pieces of information contradict each other, the requirements for UL compliance always replace general information and instructions.

Safety Instructions

- The Axis product shall be installed and serviced by a factory trained professional.

- The Axis product shall be installed within the protected premises (secured area).

- If the Axis product is used together with AXIS A9801 Security Relay, the Axis product can be used in perimeter installations. AXIS A9801 Security Relay improves security for doors controlled by Axis network video door stations. AXIS A9801 is placed on the secure side of the door. At any attempt to tamper with the door station, AXIS A9801 cuts the connection to the door strike and ensures that the door remains securely locked.

- This product must be powered by a UL294 Listed Class 2 power limited PoE injector, providing 44–57 V DC, 15.4 W.

- All wiring methods shall be performed in accordance with NFPA70, local codes and authorities having jurisdiction.

- Recommended test method to verify that the door station can receive calls and unlock doors: Press the call button and verify that the call is received on the operator side. Unlock the door from the operator side, and verify that the door is unlocked.
  Test frequency: once a year.

- When the Axis product has reached the end of its useful life, dispose of it according to local laws and regulations. The product should not be disposed of together with household or commercial waste. See *Disposal and recycling on page 3* .

- **Battery**

  - The 3.0 V lithium battery used by the Axis product is a UL Recognized component: Type CR2032, manufacturers: Fuji, Maxell, Renata, Varta, Panasonic, JHIH, Power Glory Battery Tech

  - Users shall not replace the battery. If the battery needs replacing, a factory trained service professional shall contact Axis support at *www.axis.com/techsup* for assistance.

  - Used batteries shall be disposed of according to local laws and regulations, which may vary from state to state. Waste CR lithium cells are neither listed nor exempted from the USEPA hazardous waste regulations. Waste lithium batteries can be considered reactive hazardous waste if there is a significant amount of unreacted, or unconsumed lithium remaining. For information about how to dispose of used lithium batteries, contact your local authority for waste disposal.

Set Up the Product

- **Wall and Flush Mount**

  - If using a flush mount to mount the Axis product, the flush mount shall be UL Listed.

- **Wiring**

  - Compliance with IEEE 802.3 (at or af) specifications has not been verified as part of UL 294/B.

  - Product is not intended for outside wiring as covered by Article 800 in the National Electrical Code, NFPA 70.

  - The minimum conductor gauge to be used between the PSE or power injector and the PDE, must be 26 AWG. Maximum wire length 30 m (98.4 ft).

  - The conductor gauge to be used for any interconnecting wire shall be no less than 22 AWG. Maximum wire length 30 m (98.4 ft).

  - All interconnecting devices and wiring must be Listed.

- Category 5e cabling is the minimum performance category recommended.

- All wiring shall be performed in accordance with NFPA70, local codes and authorities having jurisdiction.

- **System Considerations**

    - The access control system shall not impair the intended operation of the panic hardware used in conjunction with it.

- **Tampering**

    - To comply with UL 294/38.1.3 (Electrical Supervision), the accelerometer shall trigger an action when the Axis product is subjected to tampering.

- **Firmware Version**

    - UL approved firmware version: AXIS A8105-E Network Door Station – 1.XX.X.X

    - Verify UL approved firmware version: Log in to the product web pages and go to **Setup > Basic Setup** or **Setup > About** to verify that the stated firmware version in the Axis product is the same as the UL approved firmware version.

- **Technical Specifications**

    - Operating conditions: -35 °C to 66 °C (-31 °F to 150.8 °F. Humidity 85%±5% RH (non-condensing).

- **Connectors**

    - I/O connector: Pin 5 and pin 6: The product was evaluated by UL for max current/voltage 350mA at 12 V external sourced. All other ratings were not evaluated by UL.

Performance Levels for Access Control

This section contains performance level information required for UL 294 compliance.

Feature	Level
Destructive Attack Test	I
Line Security	I
Endurance	IV
Standby Power	I

AXIS A8105-E Network Video Door Station

Hardware overview

Hardware overview
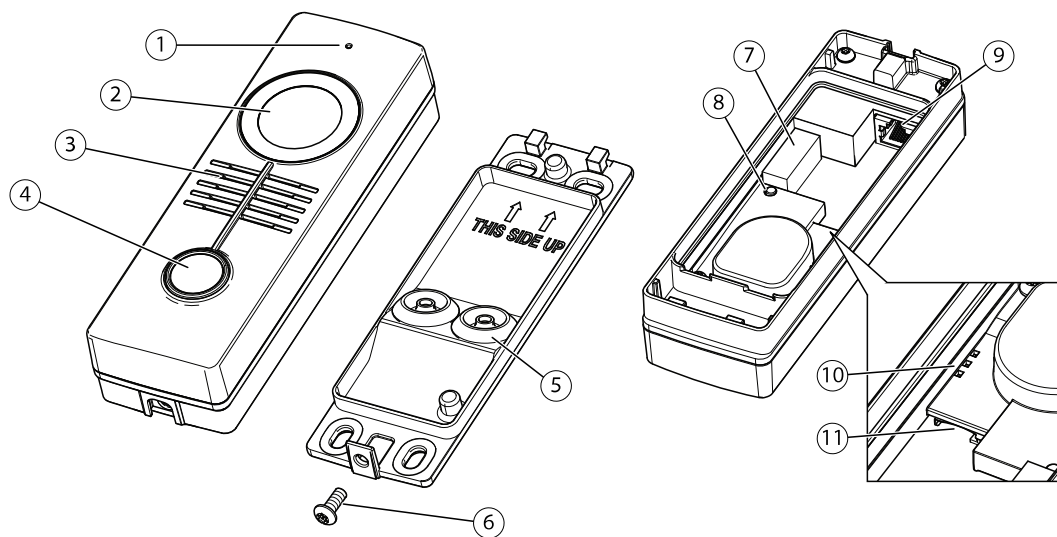
1. Microphone
2. Camera
3. Speaker
4. Call button
5. Gasket
6. Resistorx screw
7. I/O connector
8. Control button
9. Network connector (PoE)
10. Network, Status and Power LEDs
11. microSD/microSDHC/microSDXC slot supporting memory card up to 64 GB (card not included)

AXIS A8105-E Network Video Door Station

Hardware overview

Typical Scenarios

A

AXIS A8105-E

B

AXIS A9801

AXIS A8105-E

C

AXIS A9161

AXIS A8105-E

D

AXIS A1001

AXIS A4011-E
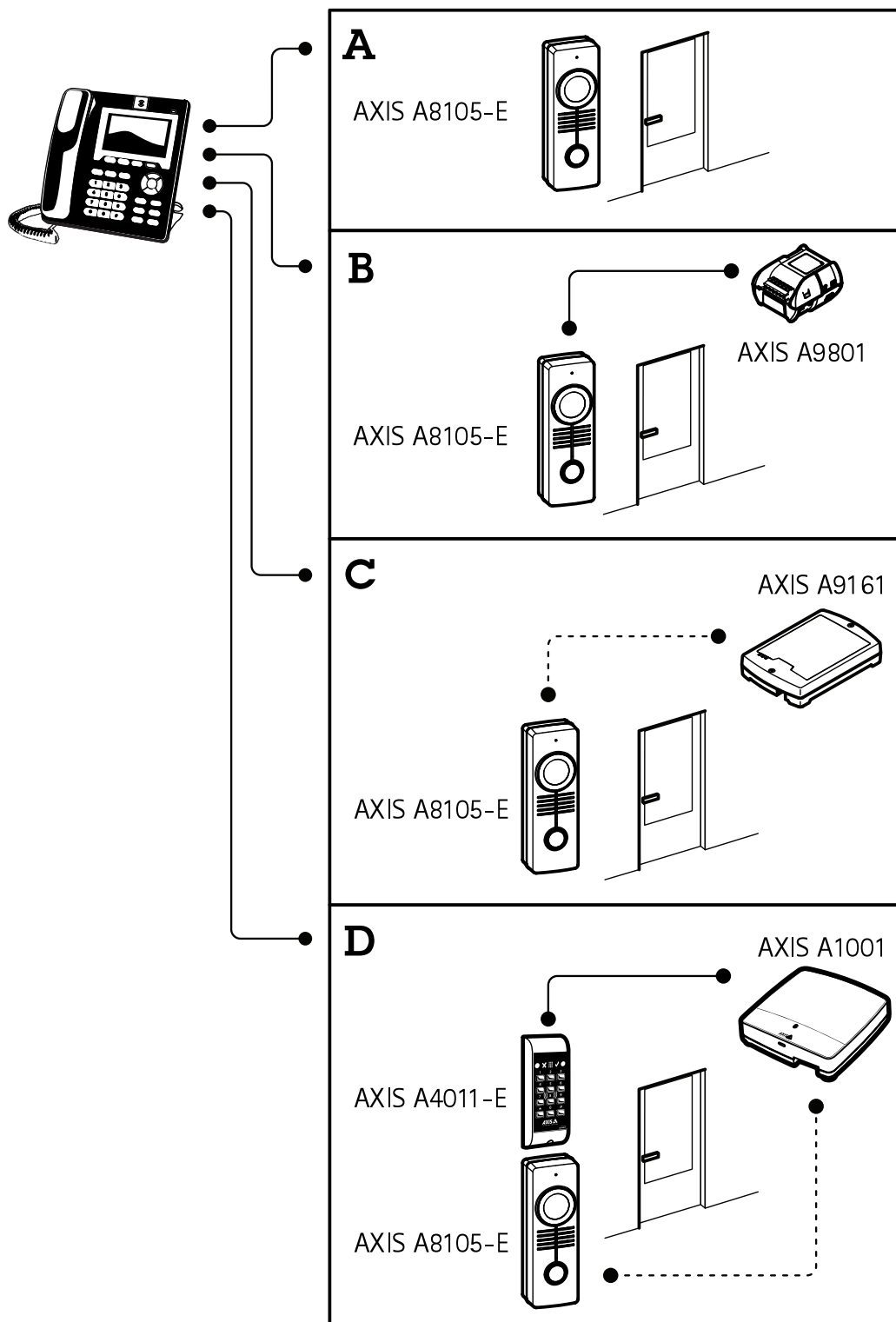
AXIS A8105-E

Connectors and buttons

Network connector

RJ45 Ethernet connector with Power over Ethernet (PoE).

I/O connector

Use the I/O connector with external devices in combination with, for example, motion detection, event triggering, and alarm notifications. In addition to the 0 V DC reference point and power (DC output), the I/O connector provides the interface to:

Digital input – For connecting devices that can toggle between an open and closed circuit, for example PIR sensors, door/window contacts, and glass break detectors.

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

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.

Control button

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

The control button is used for:

- Resetting the product to factory default settings. See *page 76*.
- Connecting to an AXIS Video Hosting System service. See *page 68*. To connect, press and hold the button for about 3 seconds until the Status LED flashes green.
- Connecting to AXIS Internet Dynamic DNS Service. See *page 68*. To connect, press and hold the button for about 3 seconds.

LED Indicators

Note

- The Status LED can be configured to be unlit during normal operation. To configure, go to **Setup > System Options > Ports & Devices > LED**. See the online help for more information.
- 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 **Setup > System Options > Maintenance**.

Status LED	Indication
Unlit	Connection and normal operation.
Green	Steady green for normal operation.

Hardware overview

Amber	Steady during startup. Flashes during firmware upgrade or reset to factory default.
Amber/Red	Flashes amber/red if network connection is unavailable or lost.
Red	Firmware upgrade failure.

How to access the product

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

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

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

Note

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

Access the device

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

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

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

2. Enter the username and password. If you access the device for the first time, you must set the root password. See *How to set the root password on page 14*.

3. The live view page opens in your browser.

How to access the product from the internet

A network router allows products on a private network (LAN) to share a single connection to the internet. This is done by forwarding network traffic from the private network to the internet.

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

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

How to turn on the NAT-traversal feature

- Go to **Settings > System > Plain config > Network**.

- Select **NAT traversal enabled**.

- Enter **External IP address**.

- Enter the IP address of the **NAT traversal router**.

- Manually configure your NAT router to allow access from the internet.

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

Note

- In this context, a "router" refers to any network routing device such as a NAT router, network router, internet gateway, broadband router, broadband sharing device, or a software such as a firewall.

- For NAT traversal to work, NAT traversal must be supported by the router. The router must also support UPnP®.

How to set the root password

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

To prevent network eavesdropping, the root password can be set via an encrypted HTTPS connection, which requires an HTTPS certificate. HTTPS (Hypertext Transfer Protocol over SSL) is a protocol used to encrypt traffic between web browsers and servers. The HTTPS certificate ensures encrypted exchange of information. See *HTTPS on page 64.*

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 *Reset to factory default settings on page 76.*

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 *page 76*) 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 (with WDR) and 50 fps (without WDR).

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
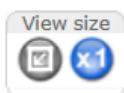
Click the **View size** buttons to show the image in full size (right button) or to scale down the image to fit the browser window (left button).
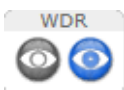
Click **WDR on** to enable WDR in intense backlight conditions. Click **WDR off** to disable WDR in low light conditions for optimal exposure.
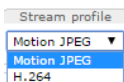
Select a stream profile for the live view window from the **Stream Profile** drop-down list. For information about how to configure stream profiles, see *page 25*.

Click the button activate the built-in light for a defined period of time, for example 20 seconds.

Enable the **WL illumination** button from **Live View Config > Action Buttons**. Click the **On/Off** buttons to manually activate or deactive WL illumination.
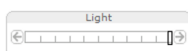
Move the slider to increase or decrease the intensity of WL illumination.

How to access the product

 Click the button activate the product's output port for a defined period of time. For information about how to enable and configure output buttons, see *page 43*. The output button name may differ depending on the name entered in the I/O Ports configuration.

 Click the **On/Off** buttons to manually activate or inactive the product's output port. For information about how to enable and configure output buttons, see *page 43*.

 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 *Manual trigger on page 15*.

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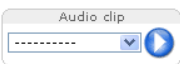
 The **Audio clip** drop-down list allows you to play an audio clip from the live view window. Select the audio clip and click the **Play** button.

 Click **Pulse** to activate the product's door relay for a defined period of time.
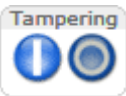
 Click the **ActiveTampering/Inactive Tampering** buttons to manually activate and inactive the product's Tampering output port.
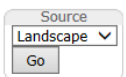
 Select a pre-configured view area or a preset position. View areas and preset positions are configured in **Setup > Video & Audio > View Areas**.

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 *Set up rules and alerts on page 54*.

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 A8105-E Network Video Door Station

How to access the product

AXIS Media Control viewer toolbar

The AXIS Media Control viewer toolbar is available in Internet Explorer only. See *AXIS Media Control (AMC) on page 18* for more information. The toolbar displays the following buttons:

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

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

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

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

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

AMC Audio Controls

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

For information about how to configure audio, see *Set Up Audio on page 30.*

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

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

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

Half-duplex mode
The **Talk/Listen button** is used to switch between sending and receiving audio. The button can be configured from the Audio tab in the AMC Control panel:
- Push-To-Talk mode: Click and hold the button to talk/send. Release the button to listen.
- Toggle mode: Click once to switch between talking and listening.
Simplex – speaker only mode
To send audio, the **Talk** and **Microphone** buttons must both be active. Click either button to stop audio transmission.

PTZ Controls

Note

These controls are available if digital PTZ is enabled in the selected view area, see *View Area on page 27*.

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 *About advanced PTZ settings on page 45.*

Media streams

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

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

How To Stream H.264

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

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

Unicast RTP	This unicast method (RTP over UDP) is used for live unicast video, especially when it is important to have an up-to-date video stream, even if some frames are dropped.	Unicasting is used for video-on-demand transmission so that there is no video traffic on the network until a client connects and requests the stream. Note that there are a maximum of 8 simultaneous unicast connections.
RTP over RTSP	This unicast method (RTP tunneled over RTSP) is useful as it is relatively simple to configure firewalls to allow RTSP traffic.	
RTP over RTSP over HTTP	This unicast method can be used to traverse firewalls. Firewalls are commonly configured to allow the HTTP protocol, thus allowing RTP to be tunneled.	
Multicast RTP	This method (RTP over UDP) should be used for live multicast video. The video stream is always up-to-date, even if some frames are dropped. Multicasting provides the most efficient usage of bandwidth when there are large numbers of clients viewing simultaneously. A multicast cannot however, pass a network router unless the router is configured to allow this. It is not possible to multicast over the Internet, for example. Note also that all multicast viewers count as one unicast viewer in the maximum total of 8 simultaneous connections.	

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

Note

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

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.

Media streams

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

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

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

- Alternatively, right-click the video image in Internet Explorer and click **Settings**.
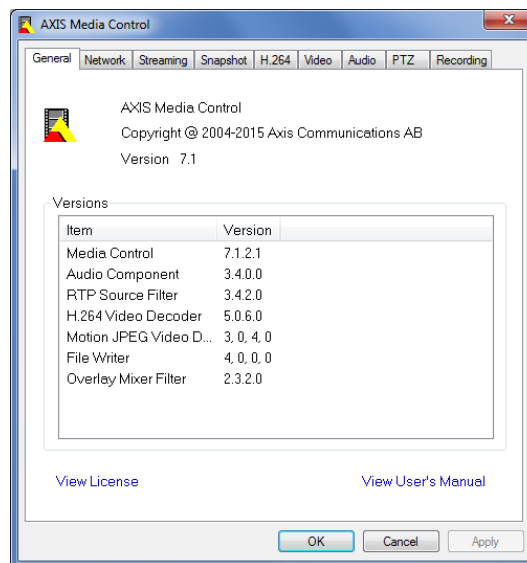
Access the video stream

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

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

- **Windows Media Player**. This requires that you install both AXIS Media Control and the H.264 decoder. The following paths can be used:

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

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

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

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

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

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

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

Media streams

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

Access Audio Streams

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

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

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

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

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

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

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

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

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

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

How to set up the product

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

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

- **Operators** have restricted access to settings, see *Users on page 64*

See also the online help .

How to perform a basic setup

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

1. Users. See *page 64.*

2. TCP/IP. See *page 67.*

3. Date & Time. See *page 66.*

4. Video Stream. See *page 22.*

5. Audio settings. See *page 30.*

6. VoIP Settings. See *page 33.*

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

Video and Audio

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

- Video stream settings. See *page 22.*

- Stream profiles. See *page 25.*

- ONVIF Media Profiles. See *page 25.*

- Camera settings. See *page 25.*

- View areas. See *page 27.*

- Overlay image. See *page 28.*

- Privacy mask. See *page 30.*

- Audio settings. See *page 30.*

- Audio clips. See *page 32.*

How to set up video streams

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

The video stream settings are divided into the following tabs:

- Image. See *page 22.*

- Audio. See *page 30.*

- H.264. See *page 23.*

- MJPEG. See *page 25.*

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 & Audio > Video Stream**. Select the **Image** tab.

The following settings are available:

- **Resolution**. Select the default resolution.

- **Compression**. The compression level affects the image quality, bandwidth and file size of saved images; the lower the compression, the higher the image quality with higher bandwidth requirements and larger file sizes.

- **Mirror image**. If required, the image can be mirrored.

Video and Audio

- **Rotate image**. If required, the image can be rotated.

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

- **Overlay settings**. See *About overlay text on page 28*.

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.

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

Bitrate control

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

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.

About constant bitrate

How to set an H.264 profile

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

Video and Audio

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

3. Select one of the H.264 profiles.

4. Select one of the following:

    - **Variable bit rate**

    - **Maximum bit rate**

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

6. Click **Save**.

How to include current bitrate in a text overlay

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

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

3. Click **Save**.

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 & Audio** > **Video Stream** and do one or more of the following:

- Go to the **Image** tab and set a low **Maximum frame rate** value.

- Go to the **H.264** tab and set a high **GOP length** value.

- Go to the **Zipstream** tab and select **Extreme** H.264 bitrate reduction.

- Go to the **Zipstream** tab. Enable **Dynamic GOP** and set a high **Max dynamic GOP length** value.

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 *Set up rules and alerts on page 54*.

- When setting up continuous recording. See *Continuous recording on page 62*.

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

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

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

About ONVIF media profiles

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

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

Camera settings

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

About capture modes

The capture mode setting reduces image flicker in fluorescent light environments as image data is sampled at a rate that matches the local power line frequency. Capture mode is set the first time the product is accessed. Select the capture mode with the power line frequency (50 Hz or 60 Hz) used at the location of the Axis product and click **OK**. When using 50 Hz, the maximum frame rate is limited to 25 fps (with WDR) and 50 fps (without WDR). When using 60 Hz, the maximum frame rate is limited to 20 fps (with WDR) and 30 fps (without WDR).

Note

> Power line frequency is different in different geographic regions. In the Americas, 60 Hz is usually used; most other parts of the world use 50 Hz. Local variations may apply, always check with the local authorities.

To change capture mode, follow these steps:

1. Go to **Setup > Video & Audio > Camera Settings**.

2. Select the new capture mode.

3. Click **Save**.

Video and Audio

Image appearance

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

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

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

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

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

Local Contrast applies contrast to a specific area of the image. Use the slider to adjust the contrast, where a higher value produces an image with high contrast between the dark and light areas and is suitable for scenes with wide dynamic range.

About image correction

To change these settings go to **Setup > Video & Audio > Camera Settings**.

Barrel Distortion Correction

Barrel distortion is a lens effect that causes an image to look curved. The extent of distortion depends on the zoom level.

To edit barrel distortion settings, click **Edit** from **Video & Audio** > **Camera Settings** > **Image Correction**. In the **Barrel Distortion Correction** window, adjust the slider to correct the distortion, using the grid for assistance.

Note

> Barrel distortion correction also affects image width, height, and resolution. A higher level means that the image width is retained at the expense of image height and resolution. A lower level means that image height and resolution are retained at the expense of image width.

Enable Defog

Enable this feature from **Video & Audio** > **Camera Settings** to counter the effects of foggy weather and for a clear image. Alternatively, click the **Defog** button in the product's **Live View** page. This button can be configured to appear in the **Live View** page from **Live View Config** > **Live View Layout**. Use the **Defog Effect** slider to adjust the degree of correction as required.

Note

> Too much brightness can negatively impact image quality when defog is active.

White balance

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

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

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

Wide Dynamic Range

Wide dynamic range (**WDR – Forensic Capture**) provides balanced images in scenes when 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. In complex light conditions disabling WDR might give a better image.

Video and Audio

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

Use the **Highlights recovery** slider to improve the image appearance by decreasing brightness in the bright parts of the image.

Use the **Shadows recovery** slider to improve the image appearance by increasing brightness in the dark parts of the image.

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 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.

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 & Audio > Camera Settings** and select **Enable View Areas**.

To add a new view area:

1. Go to **Video & Audio > View Area**.

Video and Audio

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.

Pre-Configured View Areas

Note

For the pre-configured view areas, the image is by default automatically rotated. To change the settings, go to the **Video Stream** setting page for that view area.

The product has three pre-configured view areas:

- **Landscape** – Gives you a horizontally oriented view, suitable for scenes that require a wide field of view.

- **Corridor** – AXIS Digital Corridor Format allows you to get a vertically oriented, portrait-shaped view from the camera, suitable for scenes such as staircases, hallways and aisles.

- **Full sensor** – Gives you a wide hemispherical view, suitable for scenes that require a wide field of view in all directions.

Note

Overlays are not included in the video stream when using SIP calls.

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

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

Video and Audio

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

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

5. Click **Save**.

To modify the date and time format, go to **System Options > Date & Time**. See *Date & Time on page 66*.

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

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

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

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

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

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

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

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

About overlay images

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

Image specifications:

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

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

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

- If you combine a text overlay with and image overlay, the text overlay always takes presidence over the overlay image in height. A text overlay always stretches across the whole video image which means you cannot shrink the overlay strip to make room for an image. For information about the different text overlay heights, see *About overlay text on page 28*.

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 *Privacy masks on page 30*.

How to upload an overlay image

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

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

3. Click **Upload**.

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

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

29

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

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

5. Click **Save**.

How to include an overlay image

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

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

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

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

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

6. Click **Save**.

Privacy masks

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

For more information, see the online help 💡

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

Set Up Audio

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

Audio channels

The Axis product supports the following audio modes:

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

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

- **Half-duplex –** Audio can be transmitted to and from the Axis product but only in one direction at a time. To transmit audio using the Live View page, use the **Talk** and **Listen** buttons, see *AMC Audio Controls on page 16*.

- **Simplex – Network Camera speaker only –** Audio is transmitted from a client to the Axis product and can be played by a speaker connected to the product. To transmit audio using the Live View page, the **Talk** and **Microphone on** buttons must both be active, see *AMC Audio Controls on page 16*.

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

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

Dynamic Processing

Dynamic processing is used to improve the perceived sound quality. It consists of a group of technologies that correct and control audio signals. Common dynamic processing methods include reducing the volume of loud unwanted sounds and amplifying quiet sounds.

In the Axis product, the following dynamic processing methods are available:

- **Audio processing** – Select to enable audio processing, which includes equalization that balances the levels of different frequencies and automatic gain control that amplifies weak signals.

  When selected, echo cancellation and noise reduction are automatically enabled.

- **Echo cancellation** – Select to cancel echoes from transmitted signals. Echoes typically occur when sounds travel from the speaker and back to the microphone. These signals will be identified and canceled, saving users from hearing repetitions of their own voices.

- **Noise reduction** – Select to reduce background noise and enhance speech. Unwanted processing noise, for example music playing in the background, will be avoided and speech will sound clearer.

Audio Input

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

Source lists the built-in microphone.

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

- Green – the signal is at a good level.

- Yellow – the signal is becoming distorted.

- Red – the signal is distorted.

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

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

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

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

- **OPUS** free open source audio codec that is commonly used for storage and streaming applications, real-time interaction through, for example, Voice over IP (VoIP) and video conferencing.

- **LPCM**

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

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

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

Audio Output

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

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

Audio Clips

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

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

To configure the Axis product to play audio clips when an event occurs, an action rule must be set up. For more information, see *Set up rules and alerts on page 54.*

Note

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

Voice over IP (VoIP)

Voice over IP (VoIP) is a group of technologies that enables voice communication and multimedia sessions over IP networks. In the Axis product, VoIP is enabled through the Session Initiation Protocol (SIP) and Dual-Tone Multi-Frequency (DTMF) signaling.

To open the product's VoIP pages, go to **Setup > VoIP.**

The VoIP settings include the following pages:

- **VoIP Overview.** See *VoIP Overview Page on page 33.*

- **SIP Settings.** See *Configure the SIP Settings on page 33.*

- **VMS Settings.** See *Configure the VMS Settings on page 35*

- **Account Settings.** See *Create or Edit Accounts on page 36.*

- **DTMF Settings.** See *About Dual-Tone Multi-Frequency (DTMF) on page 40.*

The VoIP settings can be configured by users with administrator rights.

VoIP Overview Page

The VoIP Overview page shows basic information about the SIP, VoIP action rules, and Account Settings.

- **SIP Settings** – Shows the basic Session Initiation Protocol (SIP) settings, and indicates whether SIP is enabled and allows incoming calls or not.

  To change the settings, click **Configure** or go to **VoIP > SIP Settings.** For more information, see *Configure the SIP Settings on page 33.*

- **VoIP Action Rules** – Shows an overview of the VoIP action rules.

  To set up a new action rule or see all action rules, click **Configure** or go to **Events > Action Rules.** For more information about events and action rules in general, see *Set up rules and alerts on page 54.*

- **Account Settings** – Shows an overview of the SIP account settings. See also *The Account Settings Page on page 36.*

  To create a new account, test an account, or change the account settings, click **Configure** or go to **VoIP > Account Settings.** For more information, see *Create or Edit Accounts on page 36.*

Configure the SIP Settings

Session Initiation Protocol (SIP) is a text-based protocol, similar to HTTP and SMTP, for interactive communication sessions between users. The sessions can include voice and video elements. See *About SIP Addresses on page 39.*

Before the Axis product can be used to make and receive calls, you need to configure the SIP settings. This includes enabling SIP, configuring the ports, and setting the rules for Network Address Translation (NAT) traversal.

To configure the SIP settings:

1. Go to **Setup > VoIP > SIP Settings.**

2. Click **Start** to start the SIP Setup Assistant. For more information, see *SIP Setup Assistant on page 34.*

Or:

1. Go to **Setup > VoIP > SIP Settings.**

2. Select **Enable SIP.**

3. To allow the Axis product to receive calls, select **Allow incoming SIP calls**.

4. Enter the **SIP port** number and the **SIP TLS port** number. For more information, see *Port Settings on page 34*.

5. Select the protocols you want to enable for NAT traversal. See *Network Address Translation (NAT) Traversal (port forwarding) on page 34*.

6. Configure the value for **Registration interval** and **Max call duration** if needed.

7. Click **Save**.

> **NOTICE**
>
> Allowing incoming calls enables the AXIS product to accept calls from any device connected to the network. It is recommended to disable incoming calls for products that are accessible from public networks or the Internet.

> Note
>
> Even if you choose to not enable SIP, you can configure the SIP settings. But remember that when SIP is disabled, you cannot make or receive calls.

SIP Setup Assistant

The SIP Setup Assistant helps you with the SIP configuration. After completing all the steps in the setup assistant, the product is ready to perform basic VoIP actions, such as making a call when the call button is pressed. Each time you finish the SIP setup assistant, new action rules and DTMF rules will be created.

Port Settings

- **SIP port** – Enter the port used for SIP sessions. The signalling traffic through this port will be non-encrypted. The default port number is 5060.

- **SIP TLS port** – Enter the port used for SIPS sessions and TLS-secured SIP sessions. The signalling traffic through this port will be encrypted using Transport Layer Security (TLS). The default port number is 5061.

- **RTP start port** – Enter the port used for the first RTP media stream in a SIP call. The default start port for media transport is 4000. Some firewalls might block RTP traffic on certain port numbers. A port number must be between 1024 and 65535.

> Note
>
> If the PBX changes the port used for SIP messages, it is possible to receive a notification regarding this. Enable the **Allow port update messages through MWI** option from the **Add Account** window (**Applications > VoIP Client > VoIP Settings**. Click **Configure** under **Account Settings**. Click **Add**).

Network Address Translation (NAT) Traversal (port forwarding)

Use NAT traversal when the Axis product is connected to the network behind a NAT router or firewall device.

Without SIP-specific port forwarding, users of clients within the same private network would be able to talk to each other but users of clients in different networks would not.

The following NAT traversal settings are available:

- **STUN** – Session Traversal Utilities for NAT (STUN).

- **TURN** – Traversal Using Relays around NAT (TURN).

- **ICE** – Interactive Connectivity Establishment (ICE).

Each NAT traversal protocol can be used separately or in different combinations depending on the network environment.

> Note
>
> For more information about the product's general NAT traversal settings, see *NAT traversal (port mapping) for IPv4 on page 70*.

Voice over IP (VoIP)

Interactive Connectivity Establishment (ICE)

Interactive Connectivity Establishment (ICE) enables the product to send a request that includes multiple addresses to the receiving device. In its response, the receiving device also includes multiple addresses. Through a process of connectivity checks, also called handshakes, the channel for communication is established.

ICE increases the chances of finding the most efficient path to successful communication between peer devices. If you also enable STUN and TURN, you improve the ICE protocol's chances of finding the most efficient path to successful communication.

Session Traversal Utilities for NAT (STUN)

Session Traversal Utilities for NAT (STUN) is a client-server network protocol that enables the product to ask a STUN server on the Internet for a mapped public IP address. The STUN server response includes this IP address and port so that the client can use them in its SIP messages to other hosts and clients.

Like TURN, STUN can be used in full-cone, address-restricted cone, and port-restricted cone NAT setups. STUN is fast because it is lightweight. However, STUN does not allow incoming messages from symmetric NATs, and it cannot communicate with a peer behind the same NAT device.

Traversal Using Relays around NAT (TURN)

Traversal Using Relays around NAT (TURN) is a client-server network protocol that enables the product to ask a TURN server for a relayed IP address. The TURN server responds with its IP address and port so that the client can use them in its SIP messages.

TURN is primarily used in symmetric NAT setups. Like STUN, TURN can also be used in full-cone, address-restricted cone, and port-restricted cone NAT setups. But because the IP address and port provided by the TURN server are those of the TURN server itself, it works like a relay that forwards information to and from the client. This means that while TURN servers are reliable, they sometimes cause a bit of latency.

Audio Codec Settings

1. Find out which audio codecs that your call recipients use.

2. Locate one or several audio codecs under **Available codecs** that match your call recipient codecs.

3. Use the arrows to move your selections, one by one, between **Available codecs** and **Selected codecs**.

4. Click the up and down arrows to adjust the priority between your **Selected codecs**.

5. Click **Save**.

Advanced SIP Settings

SIP can temporarily switch transport protocol from UDP to TCP, if a request is within 200 bytes of the MTU or larger than 1300 bytes, to avoid fragmentation. For systems not listening to SIP traffic over TCP, this setting can be disabled to enhance compatibility.

Configure the VMS Settings

Video Management Software (VMS) settings are used to simulate VoIP calls in a VMS system. A call is active when the number of streams are equal or above the set stream values.

When VMS calls are enabled, outgoing calls can be initiated by pressing the device button. The ring tone and LED state act in the same way as for a SIP call.

Enable VMS call – Select to simulate VoIP calls by tracking media streams.

Set the number of streams to or from the device that classifies the call state as active:

Number of audio streams from device – Set a range between 0 and 8.

Number of audio streams to device – Set a range between 0 and 1.

Number of video streams from device – Set a range between 0 and 8.

Call timeout – The number of seconds to wait before the call times out.

The Account Settings Page

The Account Settings page allows you to set up and manage SIP accounts. See *Create or Edit Accounts on page 36*. The SIP accounts can be verified by using **Test SIP Call**. See *Make Test Calls on page 39*.

The Account Settings page also includes an account list that shows an overview of the SIP account settings, including:

- Name. See also *Account Information on page 37*.

- SIP address. See also *About SIP Addresses on page 39*.

- Transport mode. See also *Transport Settings on page 38*.

- Default. See also *Account Information on page 37*.

- Registration status. See *Registration Status on page 36*.

Registration Status

The account status is indicated with dots in different colors. For more detailed information about an account's status, hover the mouse pointer over the status dot or select the account in the account list and click **Modify**.

SIP disabled – SIP is disabled.
Account not registered – The SIP account is not registered with a PBX, or the SIP account is a peer-to-peer account which does not register itself.

Provisional – The product is trying to register the account.
Redirection – The account or address needs to be redirected.

Successful – The account has successfully registered with the SIP registrar.

Failure – There is a problem with the account, such as the account credentials are wrong.

Create or Edit Accounts

To set up a SIP account:

1. Go to **Setup > VoIP > Account Settings**.

2. Click **Add**.

3. Enter the account details.

Under the **General** tab:

- See *Account Information on page 37*.

- See *Account Credentials on page 37*.

- See *SIP Server Settings on page 37*.

Under the **Network** tab:

- See *Transport Settings on page 38*.

-   See *Proxy Settings on page 38.*

Under the **Video** tab:

-   See *Video Settings on page 38*

4. Click **OK**.

To edit an account, select the account in the account list and click **Modify**.

To remove an account, select the account in the account list and click **Remove**.

Account Information

-   **Name** – Enter a descriptive name. This can for example be a first and last name, a role, or a location. The name is used as an alias and is especially useful when several accounts have the same user ID.

-   **Default account** – Select to make this the default account. Only one account can be the default account.

    At startup, the first time the product is accessed or after a reset, a peer account is created automatically and set to be the default account. This peer account can only be removed if at least one more account has been added to the list.

    The default account will be used when making a VAPIX® Application Programming Interface (API) call without specifying which SIP account to call from. For more information, visit *www.axis.com/developer*.

Account Credentials

-   **User ID** – User ID is typically the extension or phone number assigned to the Axis product at the SIP server. It is also possible to use a SIP URI as a User ID if required by the SIP server.

-   **Authentication ID** – Enter the Authenticaion ID used for authenticating against the SIP server. This is typically the same as the User ID.

-   **Password** – Enter the password associated with the SIP account for authenticating against the SIP server.

-   **Caller ID** – The name that is presented to the recipient of calls from this Axis product.

To create an account that is registered with a PBX or a service provider, enter the user ID, password, and the registrar address or domain name. See SIP Server Settings below. If you only enter a user ID, the account will be used as a peer-to-peer account.

Note

> Unless the devices are connected to NATs with SIP-specific port forwarding such as STUN or TURN, the account will only be able to communicate with devices that are connected to the same private network. For more information, see *Network Address Translation (NAT) Traversal (port forwarding) on page 34.*

SIP Server Settings

-   **Domain name** – If available, enter the public domain name. The domain name will be shown as part of the SIP address when calling other accounts. For more information, see *About SIP Addresses on page 39.*

-   **Registrar address** – Enter the SIP server's registrar address. This is to point out the SIP registrar with which the account should register itself. The SIP registrar is the part of the PBX that keeps track of all the extensions.

-   **Secondary SIP Server** – The Axis product will try to register on the secondary SIP server if registration on the primary SIP server fails.

Important

> The registrar address should be an IPv4 address. The product's VoIP capabilities currently do not include support for IPv6.

Voice over IP (VoIP)

Transport Settings

- **Enable SIPS** – Select to use Secure Session Initiation Protocol (SIPS). SIPS uses the TLS transport mode to encrypt traffic. If you enable SIPS, you cannot select any other transport mode than TLS.

- **Transport mode** – Select the SIP transport mode for the account: UDP, TCP, or TLS. By default, TLS is used when media encryption is activated.

- **Media encryption** – Encrypts media (audio and video) in SIP calls.

    - **SRTP Best Effort** – Supports both encrypted and unencrypted media. Encryption is always used if available. Supported crypto suites are AES_CM_128_HMAC_SHA1_80 and AES_CM_128_HMAC_SHA1_32.

    - **SRTP Mandatory** – Supports only encpted media, that is, SIP calls are only set up if the remote party offers SRTP media encryption. Supported crypto suites are AES_CM_128_HMAC_SHA1_80 and AES_CM_128_HMAC_SHA1_32.

Note

> If more than one TLS peer-to-peer account is created and they are using different media encryption, the strictest value is applied to all of them. Registered accounts are not affected.

- **Allow port update messages through MWI** – Message waiting indicator (MWI) notifies the user of changes in the port settings.

The difference between SIPS (**Enable SIPS**) and SIP over TLS (**Transport mode – TLS**) is that SIPS ensures that each message transfer is encrypted, while TLS only ensures encryption of the SIP traffic to the next node in the network.

SIP over UDP **Transport mode – UDP** is generally faster as the message will be sent without the handshakes that SIPS, SIP over TLS, and SIP over TCP **Transport mode – TCP** offer.

Certificates

Certificates are only available when TLS is used as transport mode.

The product supports Server/Client certificates and CA certificates. Certificates are managed in **System Options > Certificates**.

Certificates – The selected certificate is applied to all the accounts that use transport mode TLS. To stop using the certificate, unselect it or deactivate TLS for all accounts.

Verify server certificate – Select to verify the certificate of the server the product is connecting to against the CA Certificates list on the product.

Proxy Settings

A SIP proxy manages registration and routing requests from calling devices. The SIP proxy communicates with the private branch exchange (PBX) in order to find a route that a call has to take to reach a device that is set in a different location or site.

Address – Enter the SIP proxy server's address.

Username – Enter a user name for the SIP proxy server if required.

Password – Enter a password for the SIP proxy server if required.

Video Settings

Resolution – Select a resolution. This setting is used for all SIP calls for this account. A higher resolution uses more bandwidth and system resources.

Frame rate – Select a frame rate between 1-30 fps. This setting is used for all SIP calls for this account. A higher frame rate uses more bandwidth and system resources.

View area – Select one of the available view areas to be used in a SIP call. Additional view areas can be set up in **Video & Audio > View Areas**.

Make Test Calls

To make sure that calls can be made from the Axis product, you can make a test call:

1. Go to **VoIP > Account Settings**.

2. From the list on the Account Settings page, select the account to make the test call from.

3. In the test call field, enter a valid SIP address to the other device. Use the format `sip:<extension>@<domain>` or `sips:<extension>@<domain>`. For more information and examples, see *About SIP Addresses on page 39*.

4. Click **Test call**. For more information, see *Transport Settings on page 38*.

   The call status is displayed. For more information, see *Call Status on page 39*.

5. To end the call, click **End call**.

About SIP Addresses

SIP addresses are used to identify users within a network just like you would use a phone number or an email address to contact a friend or colleague.

Like email addresses, SIP addresses are a type of uniform resource identifier (URI) that include two user-specific parts, a user ID or extension and a domain or IP address. Together with a prefix and the @ symbol, they make up a unique address. For example, if Caesar of ancient Rome had both an email address and a SIP address, they would be `mailto:caesar@ancientrome.it` and `sip:caesar@ancientrome.it` respectively. For local peer-to-peer calls only the IP address is required. For more examples and descriptions, see below.

SIP addresses are also known as SIP URIs or, in some cases, SIP numbers. For more information, see the PBX's and service provider's instructions.

Example
```
sip:192.168.0.90
sip:3468@172.25.33.142
sip:3468@voipprovider.com
```

Description

`sip:`	Prefix that tells the system that a SIP session is being started.
`sips:`	Prefix that tells the system that a SIPS session is being started.
`<extension>`	The user ID or extension of the recipient of the call. Or, if it is a peer-to-peer call, the IP address of the receiving device.
`@<domain>`	The domain name or registrar address (IPv4 address) of the receiving device.

Important
    The Axis product's VoIP functionality does not include support for IPv6.

For more information about SIP, SIPS, and TLS, see *Port Settings on page 34* and *Transport Settings on page 38*.

For more information about registrar addresses and domains, see *Account Credentials on page 37*.

Call Status

The call status is indicated with dots in different colors. More information about the call status is shown next to the status dot.

Idle – No active calls.
Terminated – The call was denied or ended, there was no answer, or the connection failed.

Calling – Calling and waiting for an answer.

Active – The call has been answered and is ongoing.

About Dual-Tone Multi-Frequency (DTMF)

Dual-Tone Multi-Frequency (DTMF), also known as touch-tone, is a signaling system used by telecommunication devices. DTMF can be used to remotely control other devices. When you press a button on a keypad, a DTMF packet is created and sent to the other device. The receiving device then decodes and performs the requested action.

Edit DTMF Configurations

Note

Once you create a DTMF sequence it appears as a trigger and can have an action associated with it. Go to **Events > Action Rules** and click **Add**. Select the trigger (Call > DTMF) and the corresponding action from the **Action Rule Setup** window.

To modify a DTMF configuration:

1. Go to **Setup > VoIP > DTMF Settings**.

2. Click the symbol **Modify DTMF Configuration for SIP Account** 🖉.

3. Select the desired DTMF protocol(s).

Note

Both SIP INFO and RTP are out-of-band methods, meaning that the DTMF packet is sent in a dedicated channel, separated from the one used for the voice call. Digital out-of-band packets, as opposed to analog in-band tone signals, cannot be heard by the callers and are resistant to falsing.

If you have enabled SIPS with TLS as the transport mode and if you choose DTMF using SIP INFO (RFC2976), the same encrypted transport mode will be used for DTMF as for SIP traffic.

4. Enter a name and a DTMF sequence.

   - Allowed characters: **0–9**, **A–D**, *****, **#**.

   - When having two DTMF sequences that start with the same sequence, for example, **01** and **0123**, only the **01** DTMF event will be triggered. This is because **01** will always be the first match. To trigger on both sequences, add a suffix that will differentiate the sequences. For example, **01#** is not a prefix to **0123#**, hence both sequences will be triggered.

   - Duplicate sequences are not allowed.

DTMF Configuration Properties

- **DTMF using SIP INFO (RFC 2976)** – The DTMF attributes are sent in a Session Initiation Protocol (SIP) message according to the RFC 2976 standard.

- **DTMF using RTP INFO (RFC 2833)** – A DTMF event is sent with the Real-time Transport Protocol (RTP) stream according to the RFC 2833 standard.

Both SIP INFO and RTP are out-of-band methods, meaning that the DTMF packet is sent in a dedicated channel, separated from the one used for the voice call. Digital out-of-band packets, as opposed to analog in-band tone signals, cannot be heard by the callers and are resistant to falsing.

Create and edit DTMF Sequences

The DTMF sequences list shows all the available DTMF sequences.

To create a new DTMF sequence:

1. Go to **Setup > VoIP > DTMF Settings**.

2. Click **Modify DTMF Configuration for SIP Account** 🖉.

3. Click Add.

4. Enter a name. See *DTMF Sequence Properties on page 41*.

5. Enter the sequence. See *DTMF Sequence Properties on page 41*.

6. Click **OK**.

To edit a DTMF sequence, select the item in the sequence list and click **Modify**.

To remove a DTMF sequence, select the item in the sequence list and click **Remove**.

DTMF Sequence Properties

- **Name** (required) – Enter a name. This could be a descriptive name or the characters of the sequence. The DTMF sequence can be used to trigger an action. When creating an action rule, the name of the DTMF sequence will appear in the trigger list.

- **Sequence** (required) – Enter a valid DTMF sequence.

    - Allowed characters: **0–9**, **A–D**, *****, **#**.

    - When having two DTMF sequences that start with the same sequence, for example, **01** and **0123**, only the **01** DTMF event will be triggered. This is because **01** will always be the first match. To trigger on both sequences, add a suffix that will differentiate the sequences. For example, **01#** is not a prefix to **0123#**, hence both sequences will be triggered.

    - Duplicate sequences are not allowed.

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

- **Stream Profile**. See *page 25*.

- **Default Viewer** for browsers. See *page 42*.

- **Viewer Settings**. See *page 42*.

- **Action Buttons**. See *page 14*.

- **User Defined Links**. See *page 43*.

- **Output Buttons**. See *page 43*.

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 *AXIS Media Control (AMC) on page 18*.

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.

Light Buttons

The built-in light on the AXIS product can be controlled directly from the Live View page by enabling the display of light buttons. To display the light buttons in the Live view Page, select the type of control from the drop-down list under **Live View Config > Light Buttons**:

- **Pulse** activates the light for a defined period of time. The pulse time can be set as short as 1/100 second, and as long as 60 seconds

- **Active/Inactive** displays two buttons (on/off).

- **Slider** controls the brightness of the built-in light, slide left to dim and slide right do to brighten.

Output Buttons

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

To display output buttons in the Live View page:

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

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

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

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

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

For more information about I/O ports, see *I/O Ports on page 74*.

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 *View Area on page 27*.

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 *page 54*.

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 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

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**.

About tour recording

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.

PTZ (Pan Tilt Zoom)

A user who belongs to a group (see *Users on page 64*) 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 *Set up rules and alerts on page 54*). The event will immediately be placed first in the queue except when an administrator is in control.

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

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

Detectors

Camera Tampering

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

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 if lights are dimmed or turned off, or if the lens is sprayed, covered, or rendered severely out of focus.

4. Click **Save**.

To configure the product to send an alarm when tampering occurs:

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. 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 *Set up rules and alerts on page 54*.

Shock detection

Enable **Shock Detection** from the **Detectors** menu. Shock detection is used, for example, to generate an alarm if the product is hit by an object or if the product is tampered with.

Use the **Shock sensitivity** slider to adjust the sensitivity level at which the product should send an alarm. Low sensitivity value implies that the product will generate an alarm only if the hit is powerful. A high sensitivity value implies that the product will generate an alarm even with mild tampering.

Tilt Detection

The Axis product can detect if it has been tilted. It is possible to generate an alarm if the product's mounted position changes, for example if the product is manipulated. The default tilt trigger angle is set to 3 degrees.

If an Axis security relay is connected to the product, tilt detection triggers the security relay.

Audio Detection

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

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

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

3. Go to **Events > Action Rules** and set up an action rule, see *How to set up action rules on page 54.*

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

Applications

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

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

Note

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

Application licenses

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

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

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

How to upload and start an application

To upload and start an application:

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

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

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

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

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

Note

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

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

Application Considerations

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

If the Axis product's firmware is upgraded, uploaded applications and their settings will remain unchanged, although this is not guaranteed by Axis Communications. Note that the application must be supported by the new firmware. For information about firmware upgrades, see *How to upgrade the firmware on page 78*.

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

If the Axis product is restored or reset to factory default, uploaded applications and their settings are removed. For information about restoring the Axis product, see *Maintenance on page 75*. For information about factory default, see *Reset to factory default settings on page 76*.

AXIS Video Motion Detection

AXIS Video Motion Detection is an application that detects moving objects in the camera's field of view. When a moving object is detected, AXIS Video Motion Detection sends an alarm that can be used by the Axis product or by third-party software to for example, record video or send a notification.

AXIS Video Motion Detection 3 is included with the Axis product and is available under **Setup > Applications**. To use AXIS Video Motion Detection, the application must first be started. To avoid detecting unwanted objects, the application should be configured. During configuration, visual confirmation can be used to help understand the effect of the different filters. When visual confirmation is enabled, red polygons show which objects the application detects and green polygons show which objects the application ignores.

Camera mounting recommendations

Before you start to use the application, consider the following recommendations:

- Detection accuracy may be affected by weather conditions such as heavy rain or snow.

- Make sure that the lighting conditions are within the product's specification. Use additional lighting if needed.

- Make sure that the camera is not subject to excessive vibrations. Vibrations might trigger false alarms.

- Small and distant objects might not be detected.

Start and Stop the Application

To start the application, select it in the **Installed Applications** list on the **Applications** page and click **Start**.

To stop the application, select it in the list and click **Stop**.

Configure Application

Once installed, the application is available from **Setup > Applications > Motion Detection 3** in the Axis product's webpages. Go to **Settings** and then click **AXIS Video Motion Detection settings** to open the application's webpage.

The application is available from **Setup > Applications > Motion Detection 3**. Go to **Settings** and then click **AXIS Video Motion Detection settings** to open the application's webpage.

To configure the application, follow these steps:

1. Modify the size and position of the include area. This is the area in which moving objects will be detected. See *Include area on page 50*.

2. Optionally, add one or more exclude areas. Objects in an exclude area will be ignored. See *Exclude areas on page 51*.

3. Click **Save** to apply the changes.

4. Use visual confirmation to verify the settings. See *Visual confirmation on page 51*.

5. If too many unwanted alarms are triggered, configure one or more of the ignore filters. See *Ignore filters on page 52*.

After modifying a setting, click **Save** to apply the changes. The video stream will be restarted and it may take a few seconds before the change is applied.

Include area

The include area is an area in which moving objects trigger alarms. Objects can trigger alarms even if only a part of the object is inside the include area. The application ignores any moving objects outside the include area.

AXIS Video Motion Detection

The default include area is a square that covers the whole image. To highlight the area, click

Use the mouse to reshape and resize the area so that it only covers the part of the image in which moving objects should be detected. The default rectangle can be changed to a polygon with up to 20 corners.

- To add a new corner, click the border of the include area. Drag the corner to the desired position.

- To move a corner, click and drag the corner to the new position.

- To remove a corner, right-click the corner.

- To move the entire include area, place the mouse pointer inside the area. When the pointer changes shape, drag the area to the new position.

- To select the include area, click the border.

- To reset the include area to its default size, click **Reset**.

Exclude areas

An exclude area is an area in which moving objects do not trigger alarms. Use exclude areas if there are areas inside the include area that trigger a lot of unwanted alarms. You can use up to 10 exclude areas.

The default exclude area is a rectangle placed in the center of the image. Use the mouse to move, reshape and resize the area so that it covers the desired part of the image. The default rectangle can be changed to a polygon with up to 20 corners.

- To add an exclude area, click **Add**.

- To add a new corner, click the exclude area border. Drag the corner to the desired position.

- To move a corner, click and drag the corner to the new position.

- To remove a corner, right-click the corner.

- To move the exclude area, place the pointer inside the area. Click and drag the area to the new position.

- To select the exclude area, click the border.

- To remove an exclude area, select the area and then click **Remove**.

- To highlight the exclude areas, click

Visual confirmation

Use visual confirmation to make sure that all objects that should be detected are detected.

The visual confirmation shows outlines on all moving objects. A green outline indicates that the application has detected the object. A red outline indicates that the object triggers an alarm.

Note

- After you have changed a setting, click **Save**. The video stream is automatically restarted and it may take a few seconds before the change is applied.
- Visual confirmation can cause video latency and affect performance during configuration.
- To improve performance, visual confirmation automatically turns off after 15 minutes.

To turn on visual confirmation, do the following:

1. Select **Enable visual confirmation**.

2. Click **Save**.

1. Go to...

51

Ignore filters

If the application triggers too many unwanted alarms, start by modifying the include and exclude areas. If too many alarms are still triggered, use one or more of the ignore filters:

Short-lived objects – Use this to ignore objects that only appear in the image for a short period of time.

Small objects – Use this to ignore small objects.

Swaying objects – Use this to ignore objects that only move a short distance.

Filter recommendations

- Ignore filters are applied to all moving objects found by the application and should be set up with care to make sure that no important objects are ignored.

- Use as few ignore filters as possible.

- Set up one ignore filter at a time and use visual confirmation to check the settings before you turn on another filter.

- Change the filter settings carefully until you've reached the desired result.

- When configuring a filter, start with a small filter size, click **Save** and use visual confirmation to verify the settings.

Swaying Object

The swaying object filter is used to avoid triggering alarms for objects that only move a short distance. For example moving trees, flags and their shadows. Use the filter if such objects cause a lot of false alarms. If the swaying objects in the scene are large, for example large ponds or large trees, use exclude areas instead of the filter. The filter will be applied to all moving objects in scene. If a value is set too high, important objects might not trigger an alarm.

When the swaying object filter is enabled and the application finds a moving object, the object will not trigger an alarm until it has travelled a distance larger than the set filter value. If the alarm is used to start a recording, configure the pre-trigger time so that the recording also includes the time the object moved in the scene before triggering an alarm.

To enable the filter:

1. Select the **Swaying objects** option.

2. Click on the ⬬ icon to show the filter size in the image.

3. Use the mouse to adjust the filter size. Start with a small size. Objects moving a distance shorter than the distance from the center of the cross to one of the arrowheads will be ignored. The filter can be moved to the location of a swaying object to make it easier to adjust the size. Note that the filter will be applied to all objects in the image, not only to the ones at the location where the filter is placed.

4. Click **Save** to apply the filter.

5. Use visual confirmation to verify the settings.

6. If the result is not satisfactory, increase the filter size in small steps.

The filter size can also be set by entering a value between 10 and 50 in the field. The value corresponds to the distance from the center of the cross to one of the arrowheads. The value 100 implies that an object must travel from its initial point to one third of the image width or height before being detected. The value 50 implies half that distance, that is, the object must travel a distance of one sixth of the image width or height before being detected.

The short-lived objects filter

Use the short-lived objects filter to avoid alarms for objects that only appear for a short period of time, such as light beams from a passing car or quickly moving shadows.

When you turn on the short-lived objects filter and the application finds a moving object, the object does not trigger an alarm until the set time has passed. If the alarm is used to start a recording, configure the pre-trigger time so that the recording also includes the time the object moved in the scene before triggering the alarm.

Small Object

The small object filter is used to avoid triggering alarms for objects that are too small. For example, if only moving cars should trigger alarms, the small object filter can be used to avoid triggering alarms caused by people and animals.

If using the small object filter, take into consideration that an object far from the camera appears smaller than an object close to the camera. If the filter is set to ignore objects the size of a person, people that are close to be camera can still trigger alarms because they are larger than the filter size.

To enable the filter:

1. Select the **Small objects** option.

2. Click on the ⬭ icon to show the filter size in the image.

3. Adjust the filter size. Start with a small value. Moving objects that fit inside the rectangle will be ignored. The filter displayed in the image can be moved to make it easier to compare the filter size with the size of objects in the image. Note that the filter will be applied to all objects in the image, also to objects that are not located at the position of the displayed filter.

4. Click **Save** to apply the filter.

5. Use visual confirmation to verify the settings.

6. If the result is not satisfactory, increase the filter size in small steps.

The filter size can also be set by entering the width and height in the fields. The width and height are the maximum width and maximum height of the objects to ignore and are measured in percent of the image width and height. Values between 5 and 100 can be used.

Using the Application in an Action Rule

The following example shows how to configure the Axis product to record video when AXIS Video Motion Detection 3 detects motion.

1. Insert an SD card in the Axis product, or go to **Setup > System Options > Storage** in the Axis product's webpages and configure the product to use a network share.

2. Optionally, go to **Setup > Video & Audio > Stream Profiles** and create a stream profile to use for recording.

3. Go to **Setup > Events > Action Rules** and click **Add** to create a new action rule.

4. Configure other settings as required. For example, to only record video during certain time periods, select a **Schedule**.

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

6. Select the stream profile and storage device to use and configure the pre- and post-trigger times.

7. Make sure that the rule is enabled and then click **OK**.

Note

To appear in the **Trigger** list, the application must be started and its status must be Idle or Running.

Set up rules and alerts

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 when it records.

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 *Triggers on page 56* and *Actions on page 57*.

The following example describes how to set up an action rule to send an email notification with an attached jpeg image when the call button is pushed.

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

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

3. Select **Input Signal** from the **Trigger** drop-down list.

4. Select **Digital Input Port** from the second drop-down list.

5. Select **Call Button** from the third drop-down list.

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

7. Select **Send Images** from the **Actions** drop-down list.

8. Select **Send only the first** and enter 1.

9. Select an email recipient from the **Recipient** drop-down list. Or create a new recipient. See *How to set up email recipients on page 58*.

10. Click **OK**.

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

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

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

2. Go to **System Options > Storage** and set up the network share. See *page 74*.

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.

Set up rules and alerts

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.

Set up multiple action rules to call predefined recipients and assign the call to the first recipient

Create a **maximum** of **six** action rules according to the following:

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

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

3. Select **Input Signal** from the **Trigger** drop-down list.

4. Select **Digital Input Port** from the second drop-down list.

5. Select **Call Button (Port 1)** from the third drop-down list.

6. Optionally, select a **Schedule** and **Additional conditions**.

7. Select **Make Call** from the **Actions** drop-down list.

8. Select a recipient from the **Recipient** drop-down list. Or click **New Recipient** to create a new recipient.

9. Click **OK**.

Set up an action rule to call alternative recipients when the first recipient fails to answer

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

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

3. Select **Call** from the **Trigger** drop-down list.

4. Select **StateChange** from the second drop-down list.

5. Select one of the following from the third drop-down list:

    Busy: The recipient is in a call.

    Denied: The recipient receives the call but chooses to reject the call.

    Failed: No contact can be established with the recipient, for example if the number does not exist on the network.

    NoAnswer: The recipient does not answer and the call times out.

6. Optionally, select a **Schedule** and **Additional conditions**.

7. Select **Make Call** from the **Actions** drop-down list.

8. Select a recipient from the **Recipient** drop-down list. Or click **New Recipient** to create a new recipient.

9. Click **OK**.

Set up rules and alerts

Triggers

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

- **Applications** – Use installed applications to trigger the rule. See *Applications on page 49*.

- **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.

  - **Shock Detection** – Triggers an action rule when the Axis product detects it has been tilted or hit. See *Shock detection on page 47*.

  - **Tilt Detection** – Triggers an action rule whenever the product's mounting position changes due to intentional or unintentional tilting or if the product's casing is opened or removed. See *Tilt Detection on page 47*.

  - **Tampering** – Triggers an action rule when tampering is detected. See *Camera Tampering on page 47*.

- **Call**

  - **DTMF** – Triggers an action rule when a configured DTMF Sequence is activated. This trigger can for example, be used to open a door or turn on light.

  - **State** – Triggers an action rule when a call service state changes to active, calling, idle or ringing. This trigger can, for example, be used to play a dial tone when a call is connecting.

  - **State Change** – Triggers an action rule when a call state changes. This trigger can for example, be used to play a busy tone when a call is busy.

- **Hardware**

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

- **Input Signal**

  - **Digital Input Port** – Triggers an action rule when an I/O port receives a signal from a connected device. See *I/O Ports on page 74*.

    The input port named **Call Button** is dedicated to the product's Call Button.

  - **Manual Trigger** – Triggers an action rule using the **Manual Trigger** button in the Live View page. See *Controls in the live view window on page 14*. 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 *How to set up recurrences on page 59*. This can for example be used to upload an image every 5 minutes.

  - **Use Schedule** – Triggers an action rule according to the selected schedule. See *How to create schedules on page 59*.

Actions

You can configure several actions:

- **Axis Door Control** – Control a door that is connected to an AXIS Network Door Controller.

- **Defog Mode**– Set the Defog Mode on or off. You can use this action to automatically switch between the modes.

- **Make Call** – Make a call to a specified SIP or Video Management System (VMS) recipient.

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

- **Overlay Text** – Display an overlay text. See *How to include overlay text in an action rule on page 29*.

- **Play Audio Clip** – Play an audio clip. See *Audio Clips on page 32*.

- **PTZ Control**

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

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

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

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

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

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

- **Status LED** – Flash the LED indicator. This can for example be used to validate triggers such as motion detection during product installation and configuration.

- **WDR Mode** – The WDR Mode can be turned on or off when the action rule is triggered.

- **WL Illumination** – Activate or deactivate the white light.

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 *Recipient types on page 58*.

To add a recipient:

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

Set up rules and alerts

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
Axis Door Controller	Axis Door Control	An Axis Door Controller enables access management of doors that are connected to it. The Axis Door Controller recipient is typically used when sending a DTMF sequence to open a door.
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.
SIP	Make Call	Typically used as a recipient for SIP calls when using the call button.
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 *Certificates on page 65*.

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**.

Pre-configured Action Rules

The Axis product is pre-configured with a set of action rules in order to simplify different setup requirements.

AUDIO: Calling – Triggers the Action rule when a call service state changes to calling. An audio clip is played when a call is connecting.

AUDIO: Stop on Active call – Triggers the Action rule when a call service state changes to active. An active audio clip is stopped when a call is answered.

Set up rules and alerts

AUDIO: Stop on Idle call – Triggers the Action rule when a call service state changes to idle. An active audio clip is stopped when all calls end.

BUTTON: VMS call – Triggers the Action rule when digital input port is active. A call request is made to a Video Management System (VMS) recipient.

LIGHT: Active call – Triggers the Action rule when a call state changes to active. The built-in illuminator fades to 90% intensity when a call is ongoing.

LIGHT: Calling – Triggers the Action rule when a call state changes to calling. The built-in illuminator flashes when a call is connecting.

LIGHT: Idle – Triggers the Action rule when a call state changes to idle. The built-in illuminator fades to 10 % intensity when a call ends.

TAMPERING: Tilt detected – Triggers the Action rule if the product is tilted more than the defined number of degrees.

TAMPERING: Shock detected – Triggers the Action rule if the Axis product detects it has been tilted or hit. When the output port is activated, the AXIS 9801 security relay box (not included) connected to Port 2 will lock itself down to prevent any malicious person from short circuiting the lock/device/door connected to it. It is recommended to tune the shock detection level or turn off this rule if the door station is installed on materials that are prone to movements, for example, plaster walls, posts and metal sheets.

Recordings

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

- To start a continuous recording, see *page 62.*

- To set up action rules, see *page 54.*

- To access recordings, see *How to find recordings on page 61.*

- To play recordings, see *How to play recordings on page 61.*

- To export a recording as a video clip, see *How to export a video clip on page 62.*

- To configure camera controlled storage, see *Storage on page 72.*

How to find recordings

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

Note

> The recording's start date and time is set according to the Axis product's date and time settings. If the Axis product is configured to use a time zone different from the local time zone, make sure to configure the **Recording time** filters according to the product's time zone. Date and time settings are configured under **System Options > Date & Time**, see *Date & Time on page 66.*

To find a recording, follow these steps:

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

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

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

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

   Storage – List recordings from a specific storage device.

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

   Results – Specify the maximum number of recordings to display.

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

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

To play a recording, select the recording and click **Play**. See also *How to play recordings on page 61.*

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

To export a recording or a part of a recording as a video clip, select the recording and click **Export**. See also *How to export a video clip on page 62.*

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

How to play recordings

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

To play a recording, follow these steps:

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

2. To reduce the number of recordings displayed, select the desired options under **Filter** and click the **Filter** button to apply the filters. See also *How to find recordings on page 61*.

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

How to export a video clip

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

Note

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

To export a video clip, follow these steps:

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

2. To reduce the number of recordings displayed, select the desired options under **Filter** and click the **Filter** button to apply the filters. See also *How to find recordings on page 61*.

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 *Storage on page 72*. To prevent the disk from becoming full, it is recommended to configure the disk to automatically remove old recordings.

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

To start a continuous recording, follow these steps:

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

2. Select **Enabled**.

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

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

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

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 *Certificates on page 65*.

To enable HTTPS on the Axis product:

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

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

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

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

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

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

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

IEEE 802.1X

IEEE 802.1X is a standard for port-based Network Admission Control providing secure authentication of wired and wireless network devices. IEEE 802.1X is based on EAP (Extensible Authentication Protocol).

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

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

- a CA certificate to authenticate the authentication server.

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

To create and install certificates, go to **System Options > Security > Certificates**. See *Certificates on page 65*.

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

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

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

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

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

Note

> For authentication to work properly, the date and time settings in the Axis product should be synchronized with an NTP server. See *Date & Time on page 66*.

Certificates

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

Server/Client certificates – To authenticate the Axis product.

CA certificates – To authenticate peer certificates, for example the certificate of an authentication server in case the Axis product is connected to an IEEE 802.1X protected network.

Note

Installed certificates, except preinstalled CA certificates, will be deleted if the product is reset to factory default. Preinstalled CA certificates that have been deleted will be reinstalled.

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.

To install a self-signed certificate:

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

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

To create and install a CA-signed certificate:

1. Create a self-signed certificate as described above.

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.

Server/Client certificates can be installed as **Certificate from signing request** or as **Certificate and private key**. Select **Certificate and private key** if the private key is to be upload as a separate file or if the certificate is in PKCS#12 format.

The Axis product is shipped with several preinstalled **CA certificates**. If required, additional CA certificates can be installed:

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

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

Audio Support

Select **Enable audio support** to allow clients to retrieve audio streams from the Axis product. For information on how to configure audio settings, see *Set Up Audio on page 30*.

Note

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

Date & Time

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

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

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

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

- **Synchronize with NTP Server** – Obtains date and time from an NTP server. With this option, date and time settings are updated continuously. For information on NTP settings, see *NTP Configuration on page 69*.

  If using a host name for the NTP server, a DNS server must be configured. See *DNS Configuration on page 69*.

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

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

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

Network

Basic TCP/IP Settings

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

IPv4 Address Configuration

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

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

If DHCP is enabled and the product cannot be accessed, run AXIS IP Utility to search the network for connected Axis products, or reset the product to the factory default settings (see *page 76*) and then perform the installation again.

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

IPv6 Address Configuration

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

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

ARP/Ping

The product's IP address can be assigned using ARP and Ping. For instructions, see *Assign an IP address using ARP/Ping on page 67*.

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.

System options

Advanced TCP/IP Settings

DNS Configuration

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

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

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

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

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

NTP Configuration

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

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

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

Host Name Configuration

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

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

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

Select **Enable dynamic DNS updates** to dynamically update local DNS servers whenever the Axis product's IP address changes. For more information, see the online help.

Link–Local IPv4 Address

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

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

HTTP

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

HTTPS

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

To enable HTTPS, go to **System Options > Security > HTTPS**. For more information, see *HTTPS on page 64*.

NAT traversal (port mapping) for IPv4

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

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

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

Note

- For NAT traversal to work, this must be supported by the router. The router must also support UPnP®.
- In this context, router refers to any network routing device such as a NAT router, Network router, Internet Gateway, Broadband router, Broadband sharing device, or a software such as a firewall.

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

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

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

Note

- An alternative HTTP port can be used or be active even if NAT traversal is disabled. This is useful if your NAT router does not support UPnP and you need to manually configure port forwarding in the NAT router.
- If you attempt to manually enter a port that is already in use, another available port is automatically selected.
- When the port is selected automatically it is displayed in this field. To change this, enter a new port number and click **Save**.

FTP

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

Note

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

RTSP

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

Note

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

SOCKS

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

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

QoS (Quality of Service)

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

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

Note

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

SNMP

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

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

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

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

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

Note

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

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

The following traps are available:

- Cold start

- Warm start

- Link up

- Authentication failed

Note

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

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

To use SNMP v3, HTTPS must be enabled, see *HTTPS on page 64*. 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 *Reset to factory default settings on page 76*.

UPnP

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

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

RTP/H.264

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

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

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

Bonjour

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

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

Storage

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

I/O Ports

The Axis product provides four configurable input and output ports for connection of external devices. For information about how to connect external devices, see *Connectors on page 84*.

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

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

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

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

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

The product also provides a non-configurable input that is dedicated to the call button.

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

- the IEEE 802.1X settings

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

Click **Default** to reset all settings, including the IP address, to the factory default values. This button should be used with caution. The Axis product can also be reset to factory default using the control button, see *Reset to factory default settings on page 76*.

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

For information about firmware upgrade, see *How to upgrade the firmware on page 78*.

Support

Support Overview

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

See also *Troubleshooting on page 78*.

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).

System options

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.

The log levels for the system and access logs are set under **System Options > Support > Logs & Reports > Configuration** . The access log can be configured to list all connections to the product (select Critical, Warnings & Info).

Advanced

Scripting

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

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

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

To open the Script Editor, go to **System Options > Advanced > Scripting**. If a script causes problems, reset the product to its factory default settings, see *page 76*.

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 while reconnecting power. See *Hardware overview on page 9* .

3. Keep the control button pressed for 15–30 seconds until the status LED indicator flashes amber.

4. Release the control button. The process is complete when the status LED indicator turns green. The product has been reset to the factory default settings. If no DHCP server is available on the network, the default IP address is `192.168.0.90`.

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

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

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

Troubleshooting

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

How to check the current firmware

Firmware is software that determines the functionality of network devices. One of your first actions when troubleshooting a problem should be to check the current firmware version. The latest version may contain a correction that fixes your particular problem.

The current firmware version in the Axis product is displayed in the page **Setup > Basic Setup** and in **Setup > About**.

How to upgrade the firmware

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

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

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

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

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

4. Click **Upgrade**.

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

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

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

Emergency Recovery Procedure

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

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

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

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

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

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

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

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

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

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

Symptoms, possible causes and remedial actions

Problems upgrading the firmware

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

Problems setting the IP address

When using ARP/Ping	Try the installation again. The IP address must be set within two minutes after power has been applied to the product. Make sure the Ping length is set to 408. For instructions, see *Assign an IP address using ARP/Ping on page 67*.
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 *Reset to factory default settings on page 76*.
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*
Certificate error when using IEEE 802.1X	For authentication to work properly, the date and time settings in the Axis product should be synchronized with an NTP server. See *Date & Time on page 66*.

The product is accessible locally but not externally

Router configuration	To configure your router to allow incoming data traffic to the Axis product, enable the NAT-traversal feature which will attempt to automatically configure the router to allow access to the Axis product, see *NAT traversal (port mapping) for IPv4 on page 70*. 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 *AXIS Media Control (AMC) on page 18*.
	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 *Performance considerations on page 85*.
	Reduce the number of applications running on the client computer.
	Limit the number of simultaneous viewers.
	Check with the network administrator that there is enough bandwidth available.
	Check in the AMC Control Panel (H.264 tag) that video processing is not set to **Decode only key frames**.
	Lower the image resolution.
	The maximum frames per second is dependent on the utility frequency (60/50 Hz) of the Axis product.

Video and image problems, general

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

Troubleshooting

No audio

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

Poor audio quality

Stuttering	Reduce the number of listeners and viewers. Decrease image resolution and compression.
Unsynchronized audio and video using H.264	Synchronize the product's date and time settings with an NTP server. Go to **Setup > System Options > Date & Time**.
Distorted audio	Check that the correct **Audio Input** source is selected under **Setup > Video & Audio > Audio Settings**.

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 *Set up rules and alerts on page 54*.
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.

AXIS A8105-E Network Video Door Station

Specifications

Specifications

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

Camera	
Image sensor	1/2.8" progressive scan RGB CMOS
Lens	1.56 mm, F2.8 Horizontal field of view: 180° Vertical field of view: 120° Fixed focus, IR corrected
Minimum illumination	**LED lit:** 0 lux **LED unlit (with WDR):** 2.23 lux **LED unlit (without WDR):** 1.96 lux
Shutter time	1/143000 s to 2 s with 50 Hz 1/143000 s to 2 s with 60 Hz

Video	
Video compression	H.264 (MPEG-4 Part 10/AVC), Baseline, Main, and High profiles Motion JPEG
Resolution	1920x1200 to 160x90
Frame rate	Capture modes: 1920×1200 25/20fps @50/60 Hz (WDR), 1920×1200 50/30 fps @50/60 Hz (no WDR)
Video streaming	Multiple, individually configurable streams in H.264 and Motion JPEG Axis Zipstream technology in H.264 Controllable frame rate and bandwidth
Image settings	Compression, color, brightness, sharpness, contrast, white balance, exposure control, fine-tuning of behavior at low light, WDR - forensic capture, rotation: auto, 0°, 90°, 180°, 270° including Axis Digital Corridor Format, portrait/landscape, text and image overlay, mirroring of images, privacy mask
Pan/Tilt/Zoom	Digital PTZ

Audio	
Audio streaming	Two-way, full duplex Echo cancellation and noise reduction
Audio compression	AAC-LC 8/16 kHz, G.711 PCM 8 kHz, G.726 ADPCM 8 kHz, OPUS (in SIP calls only) Configurable bit rate
Audio input/output	Built-in microphone (can be disabled), built-in speaker 85 dB (at 0.5 m / 20 in)

Lock control	
Lock integration	Integration with AXIS A9801 Safety Relay Box: 300 mA at 12 V DC Integration with AXIS A1001 Network Door Controller: maximum voltage/current: 0.7 A at 30 V

Network	
Security	Password protection, IP address filtering, HTTPS[a] encryption, IEEE 802.1X[a] network access control, Digest authentication, User access log, Centralized Certificate Management
Supported protocols	IPv4/v6, HTTP, HTTPS[a], SSL/TLS[a], QoS Layer 3 DiffServ, FTP, CIFS/SMB, SMTP, Bonjour, UPnP[TM], SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SIP, SIPS, SRTP, SIP TLS

System integration	
Application Programming Interface	Open API for software integration, including VAPIX® and AXIS Camera Application Platform; specifications at *axis.com* AXIS Video Hosting System (AVHS) with One-Click Connection

AXIS A8105-E Network Video Door Station

Specifications

	ONVIF® Profile S, specification at *onvif.org*
Software	Third-party video management software and mobile applications. For compatibility, go to *axis.com*
VoIP	Support for Session Initiation Protocol (SIP) for integration with Voice over IP (VoIP) systems, peer to peer or integrated with SIP/PBX. Tested with various SIP software such as Cisco, Bria and Grandstream Tested with various PBX softwares such as Cisco, Avaya and Asterisk AXIS Parallel Call Forking, AXIS Sequential Call Forking
Analytics	Included AXIS Video Motion Detection, active tampering alarm, audio detection Support for AXIS Camera Application Platform enabling installation of additional applications, see *axis.com/acap*
Event triggers	Analytics, external input, edge storage events Call: DTMF, state, state changes Detectors: audio detection, live stream accessed, shock detection Hardware: temperature, tilt detection, network Input Signal: digital input port, manual trigger, virtual inputs Storage: disruption, recording System: system ready Time: recurrence, use schedule
Event actions	Axis door control, video and audio recording to edge storage, Pre- and post-alarm video buffering, External output activation, Play audio clip, Overlay text, PTZ control, Status LED, WDR mode Make call: SIP, API File upload via FTP, SFTP, HTTP, HTTPS network share and email Notification via email, HTTP, HTTPS and TCP
Data streaming	Event data
Built-in installation aids	Pixel counter

General

Casing	IP65- and NEMA 4X-rated, aluminum casing, stainless steel button, polycarbonate (PC) dome Color: White NCS S 1002-B
Sustainability	PVC free
Memory	256 MB RAM, 128 MB Flash
Power	**Power out:** 1x12 V DC, **Max. out:** 350 mA at 12 V DC **Relay:** See Lock control Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 3[b]
Connectors	RJ45 10BASE-T/100BASE-TX PoE I/O: 6-pin 3.81 mm terminal block. 2 I/O, 12V output (max 350mA) and 1 relay
Storage	Support for microSD/microSDHC/microSDXC card Recording to network-attached storage (NAS) For SD card and NAS recommendations, see *axis.com*
Operating conditions	-25 °C to 55 °C (-13 °F to 131 °F) Humidity 10-100% RH (condensing)
Approvals	EN 55032 Class A, EN 55024, EN 61000-6-1, EN 61000-6-2, FCC Part 15 Subpart B Class A, ICES-003 Class A, RCM AS/NZS CISPR22 Class A, IEC/EN/UL 60950-22, IEC/EN/UL 62368-1, EN 50581, IEC 60529 IP65, NEMA 250 Type 4X, IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27, UL 294
Dimensions	H x D x W: 147.5 mm x 35 mm x 48 mm Flush mount: 217 mm x 40 mm x 105 mm
Weight	280 g (9.88 oz)

AXIS A8105-E Network Video Door Station

Specifications

|	
Included accessories	Installation Guide, Terminal block connector, Cable gasket, AXIS Connector guard A, AVHS Authentication key
Mounting option	Wall mount or recessed with AXIS A8105-E Flush Mount accessory.
Optional accessories	AXIS A8105-E Flush Mount, AXIS A9801 Security Relay Box, AXIS T8120 PoE Injector, AXIS TA8501 Physical Tampering Switch For more accessories, see *www.axis.com*
Video management software	Video management software from Axis and Application Development Partners (not included). For more information, see *axis.com/vms*
Languages	English, German, French, Spanish, Italian, Russian, Simplified Chinese, Japanese, Korean, Portuguese, Traditional Chinese
Warranty	Axis 3-year warranty and AXIS Extended Warranty option, see *axis.com/warranty*

a. *This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (www.openssl.org), and cryptographic software written by Eric Young (eay@cryptsoft.com).*
b. *Support for one lock (max. total 300 mA) . For higher power requirements connect external power (max. 30V DC 0.7A).*

Environmental responsibility:
axis.com/environmental –responsibility

Connectors

I/O connector

6-pin configurable terminal block

1 2 3 4 5 6
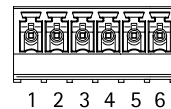
For an example diagram, see *Connection Diagrams on page 85*.

| Function	Pin	Notes	Specifications
0 V DC (-)	1		0 V DC
12 V DC	2		Max current = 350 mA
Configurable (Input or Output)	3-4	Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC
		Digital output – Connected to pin 1 when activated, floating (unconnected) when deactivated. If used with an inductive load, e.g. a relay, a diode must be connected in parallel with the load, for protection against voltage transients.	0 to max 30 V DC
Normally open/normally closed	5	For connecting relay devices. The two relay pins are galvanically separated from the rest of the circuitry.	Max current/voltage = 700mA at 30 V external sourced *
Common	6		Max current/voltage = 700mA at 30 V external sourced *

* The product was evaluated by UL for max current/voltage 350mA at 12 V external sourced. All other ratings were not evaluated by UL.

Specifications

Connection Diagrams

I/O Connector
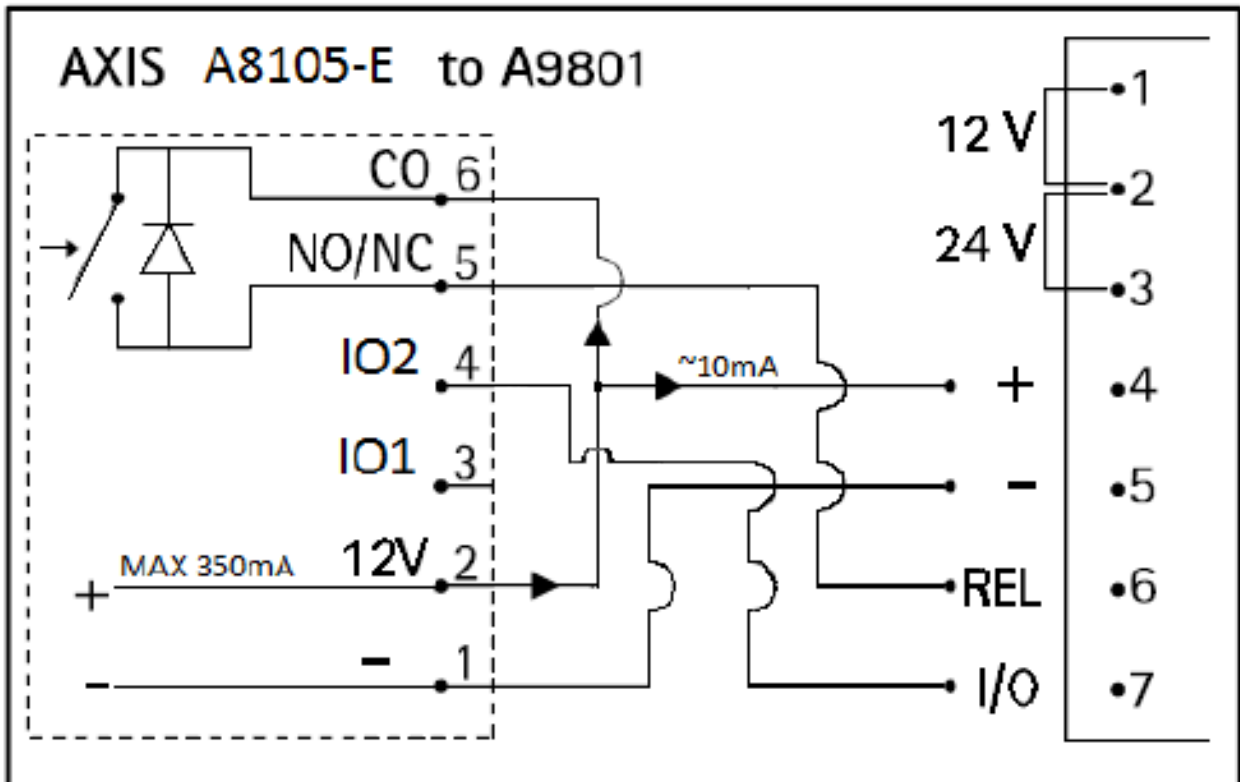
Example setup of the I/O connector: AXIS A8105–E connected to AXIS A9801 Security Relay

1   *0 V DC (-)*
2   *DC output 12 V, max current 350 mA*
3   *I/O 1 configured as input*
4   *I/O 2 configured as output*
5   *Normally open/normally closed. For connecting relay devices. Max current/voltage = 700mA at 30 V external sourced **
6   *Common. Max current/voltage = 700mA at 30 V external sourced **

* The product was evaluated by UL for max current/voltage 350mA at 12 V external sourced. All other ratings were not evaluated by UL.

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.

Specifications

- 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.