

AXIS A8004-VE Network Video Door Station

User Manual

About this Document

This manual is intended for administrators and users of the AXIS A8004-VE Network Video Door Station, and is applicable to firmware 5.80 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. The latest version of this document can be found on 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 one (1) H.264 decoder license and one (1) AAC decoder license. To purchase further licenses, contact your reseller.

Liability

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

Intellectual Property Rights

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

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

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

Equipment Modifications

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

Trademark Acknowledgments

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

Apple, Boa, Apache, Bonjour, Ethernet, Internet Explorer, Linux, Microsoft, Mozilla, Real, SMPTE, QuickTime, UNIX, Windows, Windows Vista and WWW are registered trademarks of the respective holders.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates. UPnP™ is a certification mark of the UPnP™ Implementers Corporation.

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

Regulatory Information

Europe

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

- Low Voltage (LVD) Directive 2006/95/EC. See *Safety on page 2*.
- Restrictions of Hazardous Substances (RoHS) Directive 2011/65/EU. See *Disposal and Recycling on page 3*.

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

Electromagnetic Compatibility (EMC)

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

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

USA

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

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 NMB ICES-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 55022. 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.

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

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

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

Australia/New Zealand

This digital equipment fulfills the requirements for RF emission according to the Class A limit of AS/NZS CISPR 22. The product shall be connected using a shielded network cable (STP) that is properly grounded. Notice! This is a Class A product. In a domestic environment this product may cause RF interference, in which case the user may be required to take adequate measures.

Japan

この装置は、クラスA 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。本製品は、シールドネットワークケーブル(STP)を使用して接続してください。また適切に接地してください。

Korea

이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다. 적절히 접지된 STP (shielded twisted pair) 케이블을 사용하여 제품을 연결 하십시오.

Safety

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

The power supply used with this product shall fulfill the requirements for Safety Extra Low Voltage (SELV) and Limited Power Source (LPS) according to IEC/EN/UL 60950-1.

Battery

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

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

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

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

⚠ WARNING

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

Disposal and Recycling

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

Europe



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

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

China



This product complies with the requirements of the legislative act Administration on the Control of Pollution Caused by Electronic Information Products (ACPEIP).

Contact Information

Axis Communications AB
Emdalavägen 14
223 69 Lund
Sweden

Tel: +46 46 272 18 00

Fax: +46 46 13 61 30

www.axis.com

Support

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

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

Learn More!

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

AXIS A8004-VE Network Video Door Station

Safety Information

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.

AXIS A8004-VE Network Video Door Station

Table of Contents

Safety Information	4
Hazard Levels	4
Other Message Levels	4
Hardware Overview	7
Back	7
Connectors	8
Connectors and Buttons	8
LED Indicators	9
Access the Product	11
Access from a Browser	11
Access from the Internet	11
Set the Root Password	12
Set Power Line Frequency	12
The Live View Page	12
Media Streams	16
How to Stream H.264	16
MJPEG	16
AXIS Media Control (AMC)	16
Alternative Methods of Accessing the Video Stream	17
Access Audio Streams	18
Set Up the Product	19
Basic Setup	19
Video and Audio	20
Set Up Video Streams	20
Stream Profiles	21
ONVIF Media Profiles	22
Camera Settings	22
View Area	23
Overlay	24
Privacy Mask	26
Set Up Audio	26
Audio Clips	28
Voice over IP (VoIP)	29
VoIP Overview Page	29
Configure the SIP Settings	29
Configure the VMS Settings	31
The Account Settings Page	32
Dual-Tone Multi-Frequency (DTMF)	35
Configure the Live View Page	37
PTZ (Pan Tilt Zoom)	39
Preset Positions	39
Advanced	39
Control Queue	40
Detectors	41
Camera Tampering	41
Audio Detection	41
Applications	43
Application Licenses	43
Upload Application	43
Application Considerations	43
AXIS Video Motion Detection	45
Considerations	45
Start and Stop the Application	45
Configure Application	45
Using the Application in an Action Rule	48
Events	50
Set Up Action Rules	50
Add Recipients	53
Create Schedules	55
Set Up Recurrences	55
Pre-configured Action Rules	56

AXIS A8004-VE Network Video Door Station

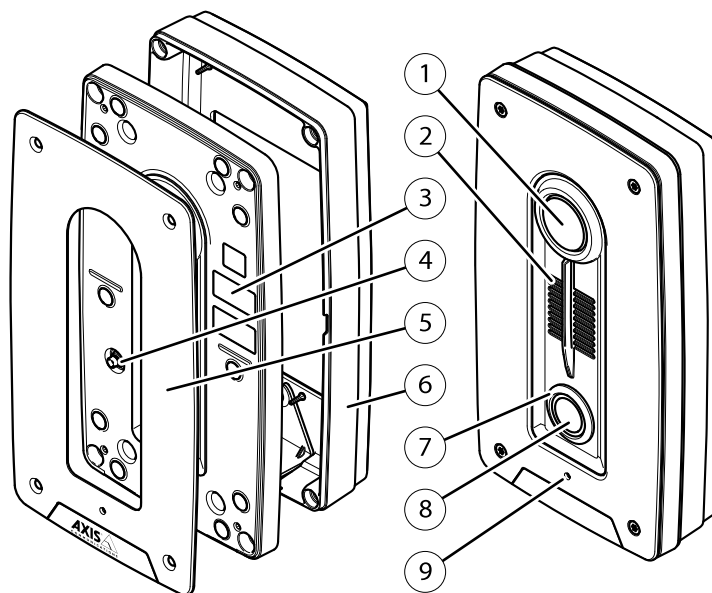
Table of Contents

Recordings	57
Find Recordings	57
Play Recording	57
Export Video Clip	58
Continuous Recording	58
Languages	59
System Options	60
Security	60
Date & Time	62
Network	63
Storage	68
Ports & Devices	71
Maintenance	71
Support	72
Advanced	72
Reset to Factory Default Settings	73
Troubleshooting	74
Check the Firmware	74
Upgrade the Firmware	74
Symptoms, Possible Causes and Remedial Actions	75
Technical Specifications	78
Connectors	78
Connection Diagrams	80
Performance Considerations	81

AXIS A8004-VE Network Video Door Station

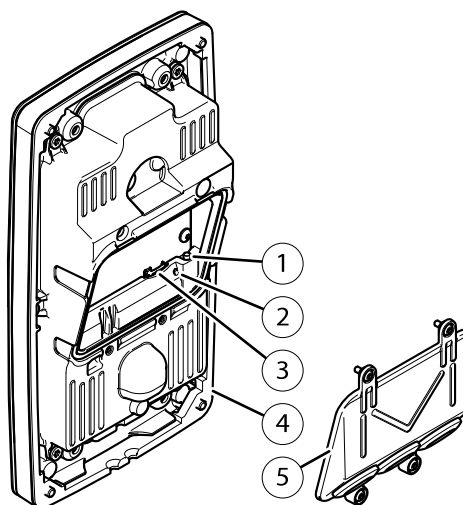
Hardware Overview

Hardware Overview



- 1 Camera
- 2 Speaker
- 3 Part number (P/N) & Serial number (S/N)
- 4 Tampering alarm switch
- 5 Front cover
- 6 Wall mount
- 7 Illuminator
- 8 Call button
- 9 Microphone

Back



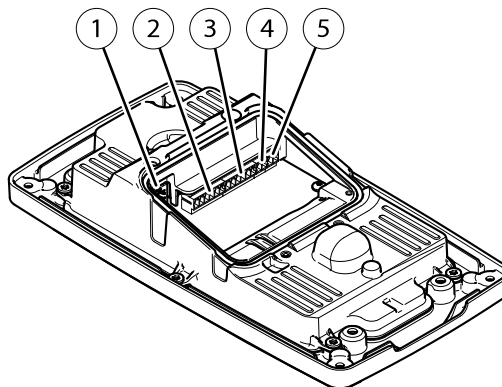
- 1 Control button

AXIS A8004-VE Network Video Door Station

Hardware Overview

- 2 *Status LED*
- 3 *microSD/microSDHC/microSDXC slot supporting memory card up to 64 GB (card not included)*
- 4 *Protective rubber gasket*
- 5 *Back cover*

Connectors



- 1 *Network connector (PoE)*
- 2 *Relay connector*
- 3 *I/O connector*
- 4 *Audio connector*
- 5 *Power connector (DC IN)*

Connectors and Buttons

For technical specifications, see [page 78](#).

Network Connector

RJ45 Ethernet connector with Power over Ethernet (PoE).

NOTICE

The product shall be connected using a shielded network cable (STP). All cables connecting the product to the network shall be intended for their specific use. Make sure that the network devices are installed in accordance with the manufacturer's instructions. For information about regulatory requirements, see *Electromagnetic Compatibility (EMC)* on [page 2](#).

I/O Connector

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

- **Digital output** – For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface, output buttons on the Live View page or by an Action Rule. The output will show as active (shown under **System Options > Ports & Devices**) if the alarm device is activated.
- **Digital input** – An alarm input for connecting devices that can toggle between an open and closed circuit, for example: PIRs, door/window contacts, glass break detectors, etc. When a signal is received the state changes and the input becomes active (shown under **System Options > Ports & Devices**).

AXIS A8004-VE Network Video Door Station

Hardware Overview

Power Connector

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

Audio Connector

2-pin terminal block for line out.

Important

External radio transmitters may interfere with the product's microphone signal. To avoid this, install a snap ferrite (Würth, article number 74271733) on the line out cable. The line out cable shall pass through the snap ferrite twice.

SD Card Slot

NOTICE

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

This product supports microSD/microSDHC/microSDXC cards (not included).

For SD card recommendations, see www.axis.com

Control Button

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

The control button is used for:

- Resetting the product to factory default settings. See *page 73*.
- Connecting to an AXIS Video Hosting System service. See *page 64*. 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 64*. To connect, press and hold the button for about 3 seconds.

Call Button

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

The call button is used by visitors to call users of the Axis product and its connected devices.

The built-in light around the call button can be used to light up the faces of visitors and its intensity can be controlled on the live view page. For more information, see *Light Buttons on page 38* and *Controls on the Live View Page on page 12*.

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.

AXIS A8004-VE Network Video Door Station

Hardware Overview

Green	Steady green for normal operation.
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.

AXIS A8004-VE Network Video Door Station

Access the Product

Access the Product

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

The product can be used with most operating systems and browsers. The recommended browsers are

- Internet Explorer® with Windows®
- Safari® with OS X®
- Chrome™ or Firefox® with other operating systems.

See *Technical Specifications* on page 78.

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 from a Browser

1. Start a web browser.
2. Enter the IP address or host name of the Axis product in the browser's Location/Address field.

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

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

Note

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

3. Enter your user name and password. If this is the first time the product is accessed, the root password must first be configured. For instructions, see *Set the Root Password* on page 12.
4. The product's Live View page opens in your browser.

Note

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

Access from the Internet

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

For more information, see *NAT traversal (port mapping) for IPv4* on page 66. See also AXIS Internet Dynamic DNS Service at www.axiscam.net

AXIS A8004-VE Network Video Door Station

Access the Product

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

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 61.

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 73.

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

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

1. Click **Use HTTPS**.

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

2. Enter a password and then re-enter it to confirm the spelling.
3. Click **OK**. The password has now been configured.

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 73) or by resetting the product to factory default.

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

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

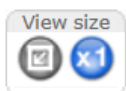
Note

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

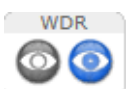
The Live View Page

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

Controls on the Live View Page



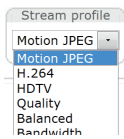
Click the **View size** buttons to show the image in full size (right button) or to scale down the image to fit the browser window (left button).



Click **WDR on** to enable WDR in intense backlight conditions. Click **WDR off** to disable WDR in low light conditions for optimal exposure.

AXIS A8004-VE Network Video Door Station

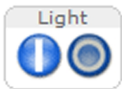
Access the Product



Select a stream profile for the Live View page from the **Stream Profile** drop-down list. For information about how to configure stream profiles, see [page 21](#).



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



Click the **Active/Inactive** buttons to manually turn the built-in light on and off.



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



Click **Pulse** to activate the product's output port for a defined period of time. For information about how to enable and configure output buttons, see [page 38](#). The output button name may differ depending on the name entered in the I/O Ports configuration.



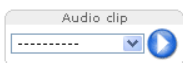
Click the **Active/Inactive** buttons to manually activate and inactive the product's output port. For information about how to enable and configure output buttons, see [page 38](#).



The **Manual Trigger** button is used to trigger an action rule from the Live View page. For information about how to configure and enable the button, see *Manual Trigger on page 13*.



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 page. 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.

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**.

AXIS A8004-VE Network Video Door Station

Access the Product

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 *Events on page 50*.

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

1. Go to **Setup > Live View Config**.
2. Under **Action Buttons**, select **Show manual trigger button**.

AXIS Media Control viewer toolbar

The AXIS Media Control viewer toolbar is available in Internet Explorer only. See *AXIS Media Control (AMC) on page 16* 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 26*.



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.

Note

These controls are available if digital PTZ is enabled in the selected view area, see *View Area on page 23*.

AXIS A8004-VE Network Video Door Station

Access the Product

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.

Source	
View Area 1	Go

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 *Controls on page 39*.

AXIS A8004-VE Network Video Door Station

Media Streams

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 page 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 page.

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 20 simultaneous unicast connections.
RTP over RTSP	This unicast method (RTP tunneled over RTSP) is useful as it is relatively simple to configure firewalls to allow RTSP traffic.	
RTP over RTSP over HTTP	This unicast method can be used to traverse firewalls. Firewalls are commonly configured to allow the HTTP protocol, thus allowing RTP to be tunneled.	
Multicast RTP	This method (RTP over UDP) should be used for live multicast video. The video stream is always up-to-date, even if some frames are dropped. Multicasting provides the most efficient usage of bandwidth when there are large numbers of clients viewing simultaneously. A multicast cannot however, pass a network router unless the router is configured to allow this. It is not possible to multicast over the Internet, for example. Note also that all multicast viewers count as one unicast viewer in the maximum total of 20 simultaneous connections.	

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

Note

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

MJPEG

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.

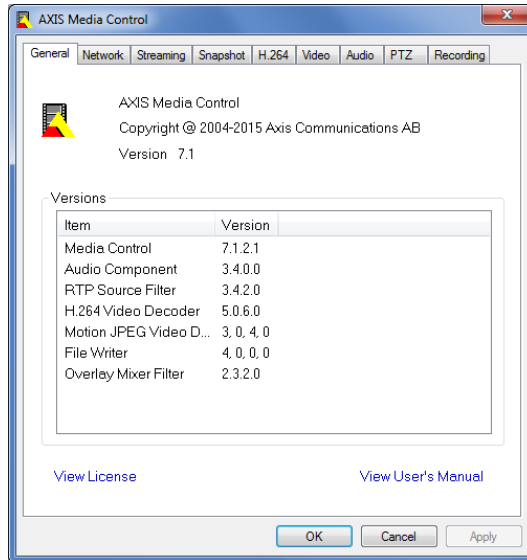
AXIS A8004-VE Network Video Door Station

Media Streams

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

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

- Windows Control Panel (from the Start screen or Start menu)
- Alternatively, right-click the video image in Internet Explorer and click **Settings**.



Alternative Methods of Accessing the Video Stream

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

- **Motion JPEG server push** (if supported by the client, Chrome or Firefox, for example). This option maintains an open HTTP connection to the browser and sends data as and when required, for as long as required.
- **Still JPEG images in a browser**. Enter the path `http://<ip>/axis-cgi/jpg/image.cgi`
- **Windows Media Player**. This requires AXIS Media Control and the H.264 decoder to be installed. The following paths can be used:
 - Unicast via RTP: `axrtpu://<ip>/axis-media/media.amp`
 - Unicast via RTSP: `axrtsp://<ip>/axis-media/media.amp`
 - Unicast via RTSP, tunneled via HTTP: `axrtsphhttp://<ip>/axis-media/media.amp`
 - Multicast: `axrtmp://<ip>/axis-media/media.amp`
- **QuickTime™**. The following paths can be used:
 - `rtsp://<ip>/axis-media/media.amp`
 - `rtsp://<ip>/axis-media/media.3gp`

AXIS A8004-VE Network Video Door Station

Media Streams

Note

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

Access Audio Streams

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

- **VAPIX® Application Programming Interface (API)** For more information, visit www.axis.com/developer
- **Windows Media Player** supports simplex audio. The following paths can be used:
 - Unicast via RTP: `axrtpu://<ip>/axis-media/media.amp`
 - Unicast via RTSP: `axrtsp://<ip>/axis-media/media.amp`
 - Unicast via RTSP, tunneled via HTTP: `axrtsphhttp://<ip>/axis-media/media.amp`
 - Multicast: `axrtsp://<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`

AXIS A8004-VE Network Video Door Station

Set Up the Product

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 page.

- **Administrators** have unrestricted access to all settings.
- **Operators** have restricted access to settings, see *Users on page 60*

See also the online help .

Basic Setup

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

1. **Users.** See *page 60*.
2. **TCP/IP.** See *page 63*.
3. **Date & Time.** See *page 62*.
4. **Video Stream.** See *page 20*.
5. **Audio Settings.** See *page 26*.
6. **VoIP Settings.** See *page 29*.

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

AXIS A8004-VE Network Video Door Station

Video and Audio

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 20*.
- Stream profiles. See *page 21*.
- ONVIF Media Profiles. See *page 22*.
- Camera settings. See *page 22*.
- View areas. See *page 23*.
- Overlay image. See *page 24*.
- Privacy mask. See *page 26*.
- Audio settings. See *page 26*.
- Audio clips. See *page 28*.

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 20*.
- Audio. See *page 26*.
- H.264. See *page 21*.
- MJPEG. See *page 21*.

Pixel Counter

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

The pixel counter can be used:

- When setting up a video stream, see *Set Up Video Streams on page 20*. 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.

AXIS A8004-VE Network Video Door Station

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 *Overlay* on page 24.

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 bit rates. 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.

The H.264 stream settings can be configured from the **Video & Audio > Video Stream** page. Select the **H.264** tab. The settings defined in this page will apply to all H.264 streams that do not use a stream profile.

The **GOP length** is the number of frames between two consecutive I-frames. Increasing the GOP length may save considerably on bandwidth requirements in some cases, but may also have an adverse affect on image quality.

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

- **Baseline.** The Baseline profile is recommended for clients that don't support CABAC entropy coding.
- **Main.** The Main profile provides higher compression with maintained video quality compared to the Baseline profile but requires more processing power to decode.

The bit rate can be set as **Variable bit rate (VBR)** or **Maximum bit rate (MBR)**. VBR adjusts the bit rate according to the image complexity, using up more bandwidth for increased activity in the image, and less for lower image activity. When the activity in the scene increases, the bit rate would usually increase as well. If there is a surplus in bandwidth, this may not be an issue and selecting **Variable bit rate (VBR)** will be sufficient. But if bandwidth is limited, it is recommended to control the bit rate by selecting **Maximum bit rate (MBR)**. When the activity in the scene increases, VBR adjusts the bit rate according to the complexity, using up more bandwidth for increased activity in the scene, and less for lower scene activity. MBR allows you to set a target bit rate that limits the bandwidth consumption.

The MBR target bit rate works like the ceiling of a tent. It limits the bit rate, while maintaining some flexibility. The bit rate may bounce up and down within the set target but when it nears the set target value, the limitation kicks in. However, because MBR will always prioritize a continuous video stream, it allows temporary overshoots from the target bit rate. Because setting a target value prevents the bit rate from increasing, frame rate and image quality are affected negatively. To partly compensate for this, select which variable shall be prioritized, frame rate or image quality. Not setting a priority means that frame rate and image quality are equally affected.

The current bit rate can be set to appear as text overlay. Under **Overlay Settings**, select **Include text** and enter the modifier #b in the field.

To apply the settings, click **Save**.

MJPEG

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 give poor image quality. To prevent increased bandwidth and storage usage, the maximum frame size should be set to an optimal value.

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:

AXIS A8004-VE Network Video Door Station

Video and Audio

- When setting up recording using action rules. See *Events* on page 50.
- When setting up continuous recording. See *Continuous Recording* on page 58.
- In the Live View page – select the stream profile from the **Stream profile** drop-down list.

For quick setup, use one of the predefined stream profiles. Each predefined profile has a descriptive name, indicating its purpose. If required, the predefined stream profiles can be modified and new customized stream profiles can be created.

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**.

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 set through the ONVIF Media Profile Settings page and be used by a client to configure media stream properties.

The **ONVIF Media Profiles** page lists all such pre-configured profiles. These profiles cannot be removed. Pre-configured media profiles have been included in the product for quick setup. It is also possible to configure new ONVIF media profiles as per required specifications. To add a new ONVIF media profile, click **Add** and enter the required information. You can also modify or remove a profile from this page.

Camera Settings

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

Image Appearance

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

Increasing the **Color** level increases the color saturation. The value 100 gives maximum color saturation and the value 0 gives minimum color saturation.

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 sliderbar.

White Balance

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

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

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

Wide Dynamic Range

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

AXIS A8004-VE Network Video Door Station

Video and Audio

Note

This setting is only possible when using automatic exposure control.

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 control – Exposure is the amount of light the camera's sensor captures for a scene. Too much light results in a washed out photo and too little light results in a dark scene. Select a suitable option to control exposure.

The **Flicker-free 50 or 60 Hz** option removes flicker that is caused by fluorescent and other light sources. The **Hold current** option locks the current exposure settings.

Shutter & Gain

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

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

Set Shutter to

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

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

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

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

Set Gain to

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

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 movements during night. To be able to, for example, recognize faces or license plates, move the normal light priority slider toward low motion blur. At nighttime, 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.

Example

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

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.

AXIS A8004-VE Network Video Door Station

Video and Audio

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**.
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.

Overlay

Overlays are used to provide extra information, such as forensic video analysis or during product installation and configuration. Overlays are superimposed over the video stream.

An overlay text can display the current date and time, or a text string.

When using a text string, modifiers can be used to display information such as the current bit rate or the current frame rate.

For information about available modifiers, see *File Naming & Date/Time Formats* in the online help .

It is also possible to display text when an action rule is triggered, see *Use Overlay Text in an Action Rule*.

Note

To enable overlays:

1. Go to **Video & Audio > Video Stream** and select the **Image** tab.
2. To include an overlay image, select **Include overlay image at the coordinates**. The overlay image must first be uploaded to the Axis product, see *Overlay Image*.
3. To include date and time, select **Include date** and **Include time**.
4. 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 .
5. Define text overlay characteristics in the relevant fields.
6. Click **Save**.

To modify the date and time format, go to **System Options > Date & Time**. See *Date & Time* on page 62.

AXIS A8004-VE Network Video Door Station

Video and Audio

Note

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

Overlay Image

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

Since it is static, the position and size of an overlay image will remain the same regardless of resolution and Pan/Tilt/Zoom movements.

Use a privacy mask to set up a dynamic mask which will always mask the specified part of monitored area.

For more information about privacy masks, see *Privacy Mask* on page 26.

To use an overlay image, the image must first be uploaded to the Axis product. 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 4 and cannot be larger than the maximum image resolution. If combining text and image overlays, take into consideration that the text overlay occupies 16 or 32 pixels in height (depending on the resolution) and has the same width as the video image.

To automatically scale the image to the resolution used by the Axis product, select the option **Scale with resolution** from the Transparency Settings page which is displayed when uploading in the image.

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 FFFFFFFF.
 - 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**.

To select the image to use as overlay:

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

To display the overlay image:

1. Go to **Video & Audio > Video Stream** and select the **Image** tab.
2. Under **Overlay Settings**, select **Include overlay image at the coordinates**.
3. To control the image's position, enter the X and Y 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.
4. Click **Save**.

Use Overlay Text in an Action Rule

Action rules, see page 50, can display an overlay text when the rule is triggered. The text can be used to provide information for forensic video analysis, notify surveillance operators or validate triggers and actions during product installation and configuration.

AXIS A8004-VE Network Video Door Station

Video and Audio

To display overlay text when an action rule is triggered, the modifier #D should be used as described below. When the rule is triggered, #D will be replaced by the text specified in the action rule.

Start by enabling overlay text in the video stream:

1. Go to **Video & Audio > Video Stream** and select the **Image** tab.
2. Under **Overlay Settings**, select **Include text**.
3. Enter the modifier #D and, optionally, additional text which will be displayed also when the action rule is not active.

Create the action rule:

1. Go to **Events > Action Rules**
2. Click **Add** to create a new rule.
3. Select a **Trigger** and, optionally, a **Schedule** and **Additional conditions**. See the online help for details.
4. From the **Actions** list, select **Overlay Text**
5. Enter the text to display in the **Text** field. This is the text that #D will be replaced by.
6. Specify the **Duration**. The text can be displayed while the rule is active or for a fixed number of seconds.

Note

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

Privacy Mask

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.

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

For more information, see the online help 

Important

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

Set Up Audio

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

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

Each stream profile is a separate video stream. To include the audio stream in all stream profiles, go to the audio tab in each stream profile settings page and enable audio. For more information, see *Stream Profiles on page 21*.

If you have enabled view areas, remember that each view area is a separate video stream. To include the audio stream in all view areas, go to the audio tab in each video stream page and enable audio. For more information see *View Area on page 23*.

Audio Modes

The Axis product supports the following audio modes:

- **Full duplex** – Simultaneous two-way audio allowing the Axis product to transmit and receive audio at the same time.
- **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 14*.

AXIS A8004-VE Network Video Door Station

Video and Audio

- **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 14*.
- **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

Note

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

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

Microphone power should only be used with microphones that have no battery. This setting should not be enabled when using a dynamic or battery powered microphone.

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

- Green – the signal is at a good level.
- Yellow – the signal is becoming distorted.
- Red – the signal is distorted.

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

- **AAC** requires a license for both encoding and decoding. AAC is the least complicated and most widely used codec. If achieving the best possible audio quality is a priority, AAC is the recommended codec to use. An AAC license is included in the Axis product.
- **G711** is an unlicensed standard codec that is useful when integrating audio into a VoIP system
- **G726** is an unlicensed speech codec that is most commonly used within the security industry.

Note

AXIS A8004-VE Network Video Door Station

Video and Audio

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 *Events on page 50*.

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**.

AXIS A8004-VE Network Video Door Station

Voice over IP (VoIP)

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 29.
- **SIP Settings.** See *Configure the SIP Settings* on page 29.
- **Account Settings.** See *Create or Edit Accounts* on page 32.
- **DTMF Settings.** See *Dual-Tone Multi-Frequency (DTMF)* on page 35.

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 29.

To change the settings, click **Configure**. For more information, see *Configure the SIP Settings* on page 29.
- **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 *Events* on page 50.
- **Account Settings** – Shows an overview of the SIP account settings. See also *The Account Settings Page* on page 32.

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*.

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 34.

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 30.

Or:

1. Go to **Setup > VoIP > SIP Settings**.
2. Select **Enable SIP**.

AXIS A8004-VE Network Video Door Station

Voice over IP (VoIP)

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 30*.
5. Select the protocols you want to enable for NAT traversal. See *Network Address Translation (NAT) Traversal (port forwarding) on page 30*.
6. 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

These settings are SIP specific. For more information about the product's general NAT traversal settings, see *NAT traversal (port mapping) for IPv4 on page 66*.

AXIS A8004-VE Network Video Door Station

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**.

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.

AXIS A8004-VE Network Video Door Station

Voice over IP (VoIP)

The Account Settings Page

The Account Settings page allows you to set up and manage SIP accounts. See *Create or Edit Accounts on page 32*. The SIP accounts can be verified by using **Test SIP Call**. See *Make Test Calls on page 34*.

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 33*.
- SIP address. See also *About SIP Addresses on page 34*.
- Transport mode. See also *Transport Settings on page 33*.
- Default. See also *Account Information on page 33*.
- Registration status. See *Registration Status on page 32*.

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 33*.
- See *Account Credentials on page 33*.
- See *SIP Server Settings on page 33*.

Under the **Network** tab:

- See *Transport Settings on page 33*.
- See *Proxy Settings on page 34*.

Under the **Video** tab:

- See *Video Settings on page 34*
4. Click **OK**.

AXIS A8004-VE Network Video Door Station

Voice over IP (VoIP)

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 30.

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 34.
- **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.

Important

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

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.
- **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.

AXIS A8004-VE Network Video Door Station

Voice over IP (VoIP)

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.

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.

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 34*.
4. Click **Test call**. For more information, see *Transport Settings on page 33*.

The call status is displayed. For more information, see *Call Status on page 35*.

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

AXIS A8004-VE Network Video Door Station

Voice over IP (VoIP)

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 30* and *Transport Settings on page 33*.

For more information about registrar addresses and domains, see *Account Credentials on page 33*.

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.

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.

AXIS A8004-VE Network Video Door Station

Voice over IP (VoIP)

- 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 36*.
5. Enter the sequence. See *DTMF Sequence Properties on page 36*.
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.

AXIS A8004-VE Network Video Door Station

Configure the Live View Page

Configure the Live View Page

You can customize the Live View page and alter it to suit your requirements. It is possible to define the following features of the Live View page.

- Stream Profile. See *page 21*.
- Default Viewer for Browser. See *page 37*.
- Viewer Settings. See *page 37*.
- Action Buttons. These are the buttons described in *Controls on the Live View Page on page 12*.
- User Defined Links. See *page 38*.
- Light Buttons. See *page 38*.
- Output Buttons. See *page 38*.

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.

AXIS A8004-VE Network Video Door Station

Configure the Live View Page

- 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 16.

User Defined Links

To display user-defined links in the Live View page, 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 71.

AXIS A8004-VE Network Video Door Station

PTZ (Pan Tilt Zoom)

PTZ (Pan Tilt Zoom)

The PTZ menu is available if digital PTZ (pan, tilt and zoom) is enabled in the selected view area. For more information on view areas, see *View Area* on page 23.

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.

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 50*.

Add a Preset Position

1. Go to **PTZ > Preset Positions**.
2. Click in the image or use the controls to steer the camera view to the desired position, see *Preset Positions*.
3. Enter a descriptive name in the **Current position** field.
4. Click **Add** to save the preset position.

To include the preset position name in the overlay text, go to **Video & Audio**, select **Include overlay text** and enter the modifier **#P** in the field. For more information about modifiers, see *File Naming & Date/Time Formats* in the online help .

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 page 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.

Advanced

Controls

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:

AXIS A8004-VE Network Video Door Station

PTZ (Pan Tilt Zoom)

- 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 page offering one viewer exclusive control for a limited period of time. Other users will be placed in queue.

A user who belongs to a group (see *Users on page 60*) 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 *Events on page 50*). 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.

AXIS A8004-VE Network Video Door Station

Detectors

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 *Events on page 50*.

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.

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 *Set Up Action Rules on page 50*.

AXIS A8004-VE Network Video Door Station

Detectors

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.

AXIS A8004-VE Network Video Door Station

Applications

Applications

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

Note

- The application AXIS Video Motion Detection is included with this product. See *AXIS Video Motion Detection*.
- 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**.

Upload 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 page **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 *Upgrade the Firmware*.

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

If the Axis product is restored, uploaded applications remain unchanged but must be restarted. To start the application, go to **Setup > Applications**. Select the application in the list of installed applications and click **Start**. For information about restoring the Axis product, see *Maintenance*.

AXIS A8004-VE Network Video Door Station

Applications

If the Axis product is reset to factory default, uploaded applications and their settings are removed. For information about factory default, see *Reset to Factory Default Settings*.

AXIS A8004-VE Network Video Door Station

AXIS Video Motion Detection

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.

Considerations

Before using AXIS Video Motion Detection 3, take the following into consideration:

- Small and distant objects might not be detected.
- Detection accuracy may be affected by weather conditions such as heavy rain or snow.
- Make sure that the lighting conditions are within the Axis product's specification. Add additional lighting if needed.
- Make sure that the camera is not subject to excessive vibrations. Vibrations might cause false detections.

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

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 AXIS Video Motion Detection 3, 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 45*.
2. Optionally, add one or more exclude areas. Objects in an exclude area will be ignored. See *Exclude Area on page 46*.
3. Click **Save** to apply the changes.
4. Use visual confirmation to verify the settings. See *Visual Confirmation on page 46*.
5. If too many unwanted objects are detected, enable and configure one or more of the ignore filters. See *Ignore Filters on page 47*.

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 the area in which moving objects will be detected. Objects moving outside the include area will be ignored. The object will be detected also if only a part of the object is inside the include area.

Note

To modify the include area, Internet Explorer and AXIS Media Control (AMC) must be used.

AXIS A8004-VE Network Video Door Station

AXIS Video Motion Detection

The default include area is a square that covers the whole image. Click on the  icon to highlight the area.

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 square can be changed to a polygon with up to 20 points (corners).

- To add a new point, click on the include area border. Drag the point to the desired position.
- To remove a point, right-click on the point.
- To move a point, drag the point to the new position.
- To move the entire include area, place the mouse pointer inside the area. When the pointer becomes a cross, drag the area to the new position.
- To select the include area, click on the border.

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

Exclude Area

An exclude area is an area in which moving objects will be ignored. Use exclude areas if there are areas inside the include area that trigger a lot of unwanted detected objects. Up to 10 exclude areas can be used.

Note

To add and modify exclude areas, Internet Explorer and AXIS Media Control (AMC) must be used.

To add an exclude area, click **Add**. 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 square can be changed to a polygon with up to 20 points (corners).

- To move the exclude area, place the mouse pointer inside the area. When the pointer becomes a cross, drag the area to the new position.
- To add a new point, click on the exclude area border. Drag the point to the desired position.
- To remove a point, right-click on the point.
- To move a point, drag the point to the new position.
- To select an exclude area, click on the border.

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

To highlight the exclude areas, click on the  icon.

Visual Confirmation

Visual confirmation is used to validate that the settings are correct, that is, that all objects that should be detected are detected.

Note

To use visual confirmation, Internet Explorer and AXIS Media Control (AMC) must be used.

When visual confirmation is enabled, all moving objects found by the application will be encircled and followed by polygons. A red polygon indicates that the object is found and is detected as a moving object. A green polygon indicates that the object is found but is ignored because it is not in the include area or because of one of the ignore filters.

To enable visual confirmation:

1. Select the **Enable visual confirmation** option.
2. Click **Save**.

AXIS A8004-VE Network Video Door Station

AXIS Video Motion Detection

Note

- Visual confirmation is disabled after 15 minutes.
- After modifying a setting, click **Save** to apply the change. The video stream will be restarted and it may take a few seconds before the change is applied.
- Enabling visual confirmation may introduce video latency.

Ignore Filters

If AXIS Video Motion Detection 3 detects too many unwanted objects, start by modifying the include and exclude areas. If still too many objects are detected, use one or more of the ignore filters.

Supported ignore filters:

- Swaying objects — Used to ignore objects that only move a short distance
- Short-lived objects — Used to ignore objects that only appear in the image for a short period of time
- Small objects — Used to ignore small objects

Ignore filters are applied to all moving objects found by the application and should be configured with care to ensure that no important objects are ignored.

Only use ignore filters if needed and use as few filters as possible. Enable and configure one filter at a time and use visual confirmation to verify the settings before enabling another filter. When configuring a filter, start with a small filter size, click **Save** and use visual confirmation to verify the settings. If required, increase the filter size in small steps until the number of unwanted objects is reduced.

Swaying Object Ignore Filter

The swaying object filter is used to avoid detecting 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 detections. 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 and, if set to a value too large, important objects might not be detected.

When the swaying object filter is enabled and the application finds a moving object, the object will not be reported as detected (red polygon in visual confirmation) until it has travelled a distance larger than the set filter size. The alarm sent by the application will be sent when the object is detected. 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 being detected.

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.

AXIS A8004-VE Network Video Door Station

AXIS Video Motion Detection

Short-Lived Object Ignore Filter

The short-lived object filter is used to avoid detecting objects that only appear for a short period of time, such as light beams from a passing car and quickly moving shadows. Use the filter if such objects cause a lot of false detections.

When the short-lived object filter is enabled and the application finds a moving object, the object will not be reported as detected (red polygon in visual confirmation) until the set time has passed. The alarm sent by the application will be sent when the object is detected. 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 being detected.

To enable the filter:

1. Select the **Short-lived objects** option.
2. Enter the number of seconds in the field. The number of seconds is the minimum time that must pass before the object is detected. Start with a small number.
3. Click **Save** to apply the filter.
4. Use visual confirmation to verify the settings.
5. If the result is not satisfactory, increase the filter size in small steps.

Small Object Ignore Filter

The small object filter is used to avoid detecting objects that are too small. For example, if only moving cars should be detected, the small object filter can be used to avoid detecting 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 the camera can still be detected 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. Use the mouse to adjust the filter size. Start with a small size. 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.

AXIS A8004-VE Network Video Door Station

AXIS Video Motion Detection

4. From the **Trigger** drop-down list, select **Applications** and then select **VMD 3**.
5. Configure other settings as required. For example, to only record video during certain time periods, select a **Schedule**.
6. Under **Actions**, select **Record Video** from the **Type** drop-down list.
7. Select the stream profile and storage device to use and configure the pre- and post-trigger times.
8. 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**.

AXIS A8004-VE Network Video Door Station

Events

Events

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

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 52* and *Actions on page 53*.

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 *Set Up Email Recipients on page 55*.
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.

Set up motion detection and add a network share:

1. Go to **Applications** to start and configure AXIS Video Motion Detection 3. See *AXIS Video Motion Detection*.
2. Go to **System Options > Storage** and set up the network share. See *page 70*.

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 **VMD3**
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.

AXIS A8004-VE Network Video Door Station

Events

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

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

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

For more information, see the online help .

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**: 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**.

AXIS A8004-VE Network Video Door Station

Events

Triggers

Available action rule triggers and conditions include:

- **Applications** – Use installed applications to trigger the rule. See *Applications on page 43*.
 - **VMD3** – Trigger the rule when AXIS Video Motion Detection detects a moving object. See *AXIS Video Motion Detection*.
- **Detectors**
 - **Audio Detection** – Trigger the rule when audio is detected. See *Audio Detection on page 41*.
 - **Live Stream Accessed** – Trigger the rule when any stream is accessed and during edge storage playback. This can for example be used to send notifications.
 - **Shock Detection** – Trigger the rule when the Axis product detects it has been tilted or hit. See *Shock Detection on page 41*.
 - **Tampering** – Trigger the rule when tampering is detected. See *Camera Tampering on page 41*.
- **Call**
 - **DTMF** – Triggers the 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 the action rule when a call service state changes to active, calling or idle. This trigger can, for example, be used to play a dial tone when a call is connecting.
 - **State Change** – Triggers the 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**
 - **Casing Open** – Triggers the action rule if the front cover is removed. This can for example be used to send a notification if the front cover has been opened for maintenance purposes or when someone has tampered with the product.
 - **Network** – Trigger the 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** – Trigger the rule when an I/O port receives a signal from a connected device. See *I/O Ports on page 71*.

The input port named **Call Button** is dedicated to the product's Call Button.
 - **Manual Trigger** – Trigger the rule using the **Manual Trigger** button in the Live View page. See *Controls on the Live View Page on page 12*. This can for example be used to validate actions during product installation and configuration.
 - **Virtual Inputs** – can be used by a VMS (Video Management System) to trigger actions. Virtual inputs can, for example, be connected to buttons in the VMS user interface.
- **PTZ**
 - **Moving** – Trigger the 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** – Trigger the 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**

AXIS A8004-VE Network Video Door Station

Events

- **Disruption** – Trigger the rule if storage problems are detected, for example if the storage device is unavailable, removed, full, locked or if other read or write problems occur. This can for example be used to send maintenance notifications.
- **Recording** – Triggers the rule when the Axis product records to the storage device. The recording status trigger can be used to notify the operator, for example by flashing LED lights, if the product has started or stopped to record to the storage device. Note that, this trigger can be used only for edge storage recording status.
- **System**
 - **System Ready** – Trigger the rule when the product has been started and all services are running. This can for example be used to send a notification when the product restarts.
- **Time**
 - **Recurrence** – Trigger the rule periodically. See *Set Up Recurrences on page 55*. This can for example be used to upload an image every 5 minutes.
 - **Use Schedule** – Trigger the rule according to the selected schedule. See *Create Schedules on page 55*.

Actions

Available actions include:

- **Activate Light** – Turn the built-in light on or off.
- **Axis Door Control** – Controls a door that is connected to an AXIS Network Door Controller.
- **Make Call** – Makes a call to the 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 *Use Overlay Text in an Action Rule on page 25*.
- **Play Audio Clip** – See *Audio Clips on page 28*.
- **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.
- **Stop Audio Clip** – Stops playing a recorded audio clip when the Action rule is triggered.
- **WDR Mode** – The WDR Mode can be turned on or off when the action rule is triggered.

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 or more recipients. For information about available options, see *Recipient Types on page 54*.

AXIS A8004-VE Network Video Door Station

Events

To add a recipient:

1. Go to **Events > Recipients** and click **Add**.
2. Enter a descriptive name.
3. Select a recipient **Type**.
4. Enter the information needed for the recipient type.
5. Click **Test** to test the connection to the recipient.
6. Click **OK**.

Recipient Types

The following recipients are available:

Recipient	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 System Options > Storage to configure a network share before setting up a continuous recording or an action rule to record video. For more information about storage devices, see <i>Storage on page 68</i> .

AXIS A8004-VE Network Video Door Station

Events

SIP	Make Call	Typically used as a recipient for SIP calls when using the call button.
TCP	Send Notification	

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 amount of 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 62*.

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.

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**.

AXIS A8004-VE Network Video Door Station

Events

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.

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.

DOOR: REX unlocks – Triggers the Action rule when digital input port is active. A door connected to relay 1 can be accessed (door unlocked for 7 seconds and is then relocked, this time can be changed in the Action Rule Setup) when the output port is activated.

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: Casing open – Triggers the Action rule if the front cover is removed. When the output port is activated, the AXIS 9801 security relay box (not included) connected to Port 4 will lock itself down to prevent any malicious person from short circuiting the lock/device/door connected to it.

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 4 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.

AXIS A8004-VE Network Video Door Station

Recordings

Recordings

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

- To start a continuous recording, see *page 58*.
- To set up action rules, see *page 50*.
- To access recordings, see *Find Recordings on page 57*.
- To play recordings, see *Play Recording on page 57*.
- To export a recording as a video clip, see *Export Video Clip on page 58*.
- To configure camera controlled storage, see *Storage on page 68*.

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 62*.

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 *Play Recording on page 57*.

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 *Export Video Clip on page 58*.

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

Play Recording

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

AXIS A8004-VE Network Video Door Station

Recordings

To play a recording, follow these steps:

1. Go to **Recordings > List**.
2. To reduce the number of recordings displayed, select the desired options under **Filter** and click the **Filter** button to apply the filters. See also *Find Recordings on page 57*.
3. Select the recording and click **Play**. The recording will be played in a new browser window.

Export Video Clip

Recordings on the SD card or network share can be exported as video clips. It is possible to 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/techsup/software

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 *Find Recordings on page 57*.
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 68*. 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.

AXIS A8004-VE Network Video Door Station

Languages

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.

AXIS A8004-VE Network Video Door Station

System Options

System Options

Security

Users

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

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

- **Viewers** have access to the Live View page
- **Operators** have access to all settings except:
 - creating and modifying PTZ presets
 - creating and modifying PTZ control settings
 - creating and modifying privacy mask settings
 - uploading applications and language files
 - any of the settings included in the **System Options**
- **Administrators** have unrestricted access to all settings. The administrator can add, modify and remove other users.

Note

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

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

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

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

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

ONVIF

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

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

IP Address Filter

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

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

AXIS A8004-VE Network Video Door Station

System Options

HTTPS

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

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

To use HTTPS, an HTTPS certificate must first be installed. Go to **System Options > Security > Certificates** to install and manage certificates. See *Certificates on page 62*.

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 62*. Many CA certificates are preinstalled.

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 62*.

AXIS A8004-VE Network Video Door Station

System Options

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 26*.

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**:

AXIS A8004-VE Network Video Door Station

System Options

- **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 65*.
If using a host name for the NTP server, a DNS server must be configured. See *DNS Configuration on page 65*.
- **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 73*) and then perform the installation again.

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

IPv6 Address Configuration

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

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

ARP/Ping

The product's IP address can be assigned using ARP and Ping. For instructions, see *Assign IP Address Using ARP/Ping on page 63*.

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

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

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

Assign IP Address Using ARP/Ping

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

AXIS A8004-VE Network Video Door Station

System Options

1. Acquire a free static IP address on the same network segment as the computer.
2. Locate the serial number (S/N) on the product label.
3. Open a command prompt and enter the following commands:

Linux/Unix syntax

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

Linux/Unix example

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

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

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

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

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

4. Check that the network cable is connected and then restart the product by disconnecting and reconnecting power.
5. Close the command prompt when the product responds with `Reply from 192.168.0.125: . . .` or similar.
6. Open a browser and type `http://<IP address>` in the Location/Address field.

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

Note

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

AXIS Video Hosting System (AVHS)

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

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

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

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

AXIS Internet Dynamic DNS Service

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

AXIS A8004-VE Network Video Door Station

System Options

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

Note

AXIS Internet Dynamic DNS Service requires IPv4.

Advanced TCP/IP Settings

DNS Configuration

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

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

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

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

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

NTP Configuration

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

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

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

Host Name Configuration

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

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

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

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

For more information, see the online help .

Link-Local IPv4 Address

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

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

HTTP

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

AXIS A8004-VE Network Video Door Station

System Options

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 61.

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.

AXIS A8004-VE Network Video Door Station

System Options

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/techsup

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 61*. To enable SNMP v3, check the box and provide the initial user password.

AXIS A8004-VE Network Video Door Station

System Options

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 73.

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 Card

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**.

AXIS A8004-VE Network Video Door Station

System Options

Mount and Unmount 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.

Format 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.

Encrypt SD Card Data

To prevent unauthorized individuals and systems to access 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 remain on the card. The card must also be mounted before it can be used.

AXIS A8004-VE Network Video Door Station

System Options

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. Ongoing recordings will not be affected if the passphrase is changed.

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

Network Share

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

Note

For NAS recommendations see www.axis.com

To add a network share:

1. Go to **System Options > Storage**.
2. Click **Network Share**.
3. Enter the IP address, DNS or Bonjour name to the host server in the **Host** field.
4. Enter the name of the share in the **Share** field. Sub folders cannot be used.
5. If required, select **The share requires login** and enter the user name and password.
6. Click **Connect**.

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

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

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

AXIS A8004-VE Network Video Door Station

System Options

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 78*.

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 is also equipped with two relay connectors. For more information about the relay connectors see *Relay Connector on page 79* and *Relay Connector on page 80*.

To configure the relays, go to **System Options > Ports & Devices > I/O Ports**, and then set the **Normal state**.

- Open circuit – The relay is in a non-conductive state until it becomes active. When the relay becomes active it will change to the opposite of its normal state.
- Closed circuit – The relay is in a conductive state until the relay becomes active.

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
- uploaded applications are kept but must be restarted

AXIS A8004-VE Network Video Door Station

System Options

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 73*.

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 *Upgrade the Firmware on page 74*.

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 74*.

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. Many of the captions are links to the proper Setup page.

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 valid Server Report with your query.

System Log – Provides information about system events.

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

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

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

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

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

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

The log levels for the System Log and the Access Log 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 A8004-VE Network Video Door Station

System Options

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 73*.

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.

Reset to Factory Default Settings

Important

Reset to factory default should be used with caution. A reset to factory default will reset all settings, including the IP address, to the factory default values.

Note

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

To reset the product to the factory default settings:

1. Disconnect power from the product.
2. Press and hold the control button and reconnect power. See *Hardware Overview on page 7*.
3. Keep the control button pressed for 15–30 seconds until the status LED indicator flashes amber.
4. Release the control button. The process is complete when the status LED indicator turns green. The product has been reset to the factory default settings. If no DHCP server is available on the network, the default IP address is 192.168.0.90
5. Using the installation and management software tools, assign an IP address, set the password, and access the video stream.

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

AXIS A8004-VE Network Video Door Station

Troubleshooting

Troubleshooting

Check the 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**.

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

To upgrade the product's firmware:

1. Download the latest firmware file to your computer, available free of charge at www.axis.com/techsup
2. Go to **Setup > System Options > Maintenance** in the product's webpages.
3. Under **Upgrade Server**, click **Browse** and locate the file on your computer.
4. Click **Upgrade**.
5. Wait approximately 10 minutes while the product is being upgraded and restarted. Then access the product.

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

Emergency Recovery Procedure

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

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

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

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

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

2. If the product does not reply in 30 seconds, restart it and wait for a reply. Press CTRL+C to stop Ping.
3. Open a browser and type in the product's IP address. In the page that opens, use the **Browse** button to select the upgrade file to use. Then click **Load** to restart the upgrade process.

AXIS A8004-VE Network Video Door Station

Troubleshooting

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/techsup/

Symptoms, Possible Causes and Remedial Actions

Problems setting the IP address

When using ARP/Ping	Try the installation again. The IP address must be set within two minutes after power has been applied to the product. Ensure the Ping length is set to 408. For instructions, see <i>Assign IP Address Using ARP/Ping</i> on page 63.
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 <code>ping</code> and the IP address of the product): • If you receive: <code>Reply from <IP address>: bytes=32; time=10...</code> 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: <code>Request timed out</code>, this means that the IP address is available for use with the Axis product. Check all cabling and reinstall the product.
Possible IP address conflict with another device on the same subnet.	The static IP address in the Axis product is used before the DHCP server sets a dynamic address. This means that if the same default static IP address is also used by another device, there may be problems accessing the product.

The product cannot be accessed from a browser

Cannot log in	When HTTPS is enabled, ensure that the correct protocol (HTTP or HTTPS) is used when attempting to log in. You may need to manually type <code>http</code> or <code>https</code> in the browser's address field. If the password for the user <code>root</code> is lost, the product must be reset to the factory default settings. See <i>Reset to Factory Default Settings</i> on page 73.
The IP address has been changed by DHCP	IP addresses obtained from a DHCP server are dynamic and may change. If the IP address has been changed, use AXIS IP Utility or AXIS Camera Management to locate the product on the network. Identify the product using its model or serial number, or by the DNS name (if the name has been configured). If required, a static IP address can be assigned manually. For instructions, see the document <i>Assign an IP Address and Access the Video Stream</i> on Axis Support web at www.axis.com/techsup .
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 <i>Date & Time</i> on page 62.

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 <i>NAT traversal (port mapping) for IPv4</i> on page 66. 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 .

AXIS A8004-VE Network Video Door Station

Troubleshooting

Problems with streaming H.264

Problems with AXIS Media Control (<i>Internet Explorer only</i>)	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 <i>AXIS Media Control (AMC) on page 16</i>. In the AMC Control Panel, select the H.264 tab and click Set to default H.264 decoder. Check that RTSP is enabled under System Options > Network > TCP/IP > Advanced.
Multicast H.264 only accessible by local clients	Check if your router supports multicasting, or if the router settings between the client and the product need to be configured. The TTL (Time To Live) value may need to be increased.
No multicast H.264 displayed in the client	Check with your network administrator that the multicast addresses used by the Axis product are valid for your network. Check with your network administrator to see if there is a firewall preventing viewing.
Poor rendering of H.264 images	Ensure that your graphics card is using the latest driver. The latest drivers can usually be downloaded from the manufacturer's website.
Color saturation is different in H.264 and Motion JPEG	Modify the settings for your graphics adapter. Refer to the adapter's documentation for more information.
Lower frame rate than expected	See <i>Performance Considerations on page 81</i>. 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. See <i>Technical Specifications on page 78</i>.

Video and image problems, general

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

No audio

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

Poor audio quality

Stuttering	Reduce the number of listeners and viewers. Decrease image resolution and compression.
------------	--

AXIS A8004-VE Network Video Door Station

Troubleshooting

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 <i>Events on page 50</i>.
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 A8004-VE Network Video Door Station

Technical Specifications

Technical Specifications

You can find the latest version of the technical specifications at www.axis.com

Connectors

I/O connector

6-pin configurable terminal block



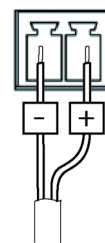
For an example diagram, see *Connection Diagrams* on page 80.

Function	Pin	Notes	Specifications
0 V DC (-)	1		0 V DC
12 V DC	2	Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	Max voltage = +12 V DC Max current = 50 mA ¹ Max current = 200 mA ²
Configurable (Input or Output)	3–6	Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 40 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 40 V DC, open drain, 100 mA

1. When powered through Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 3.
2. When powered through Power over Ethernet Plus (PoE+) IEEE 802.3at Type 2 Class 4 or DC power input.

Power Connector

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



Function	Pin	Notes	Specifications
0 V DC (-)	1		0 V DC
DC input	2	For powering controller when not using Power over Ethernet. Note: This pin can only be used as power in.	10–28 V DC, max 26 W

AXIS A8004-VE Network Video Door Station

Technical Specifications

Audio Connector

2-pin terminal block for:

- Line out (+)
- 0 V DC (-)



Function	Pin	Notes
Line out (+)	1	Line audio out
0 V DC (-)	2	

Relay Connector

6-pin terminal block for solid state relays that can be used in the following ways:

- As a standard relay that opens and closes auxiliary circuits.
- To control a lock directly.
- To control a lock through a safety relay. Using a safety relay on the secure side of the door prevents hotwiring.



For example connection diagrams, see *Connection Diagrams on page 80*.

Function	Pin	Notes	Specifications
0 V DC (-)	1		0 V DC
NO/NC	2, 5	Normally open/normally closed For connecting relay devices. The two relay pins are galvanically separated from the rest of the circuitry.	Max current = 700 mA Max voltage = +30 V DC
CO	3, 6	Common	
12 V DC	4	For powering auxiliary equipment. Note: This pin can only be used as power out.	Max voltage = +12 V DC Max current = 160 mA ¹ Max current = 750 mA ²

1. When powered through Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 3.
2. When powered through Power over Ethernet Plus (PoE+) IEEE 802.3at Type 2 Class 4 or DC power input.

AXIS A8004-VE Network Video Door Station

Technical Specifications

Performance Considerations

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

The following factors are among the most important to consider:

- High image resolution and/or lower compression levels result in images containing more data. Bandwidth affected.
- Access by large numbers of Motion JPEG and/or unicast H.264 clients. Bandwidth affected.
- Simultaneous viewing of different streams (resolution, compression) by different clients. Effect on frame rate and bandwidth.
- Accessing Motion JPEG and H.264 video streams simultaneously. Frame rate and bandwidth affected.
- Heavy usage of event settings affect the product's CPU load. Frame rate affected.
- Using HTTPS may reduce frame rate, in particular if streaming Motion JPEG.
- Heavy network utilization due to poor infrastructure. Bandwidth affected.
- Viewing on poorly performing client computers lowers perceived performance. Frame rate affected.
- Running multiple AXIS Camera Application Platform (ACAP) applications simultaneously may affect the frame rate and the general performance.

