

AXIS M1143-L – User Manual

About this Document

This manual is intended for administrators and users of the AXIS M1143-L Network Camera, and is applicable to firmware 5.60 and later. It includes instructions for using and managing the product on your network. Previous experience of networking will be of use when using this product. Some knowledge of UNIX or Linux-based systems may also be beneficial, for developing shell scripts and applications. Later versions of this document will be posted to the Axis website, as required. See also the product's online help, available via the web-based interface.

Legal Considerations

Video 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.

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.

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

This product includes one (1) H.264 decoder license and one (1) AAC decoder license. To purchase further licenses, contact your reseller.

This product includes one (1) H.264 decoder license. To purchase further licenses, contact your reseller.

Liability

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

Intellectual Property Rights

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

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

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

Equipment Modifications

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

Trademark Acknowledgments

AXIS COMMUNICATIONS, AXIS, 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.

The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing LLC in the United States and other countries.

WPA, WPA2 and Wi-Fi Protected Setup are marks of the Wi-Fi Alliance.


Microsoft, Windows, Windows Vista, WWW, Internet Explorer, DirectX, Intel, Intel Core, Pentium and Xeon are registered trademarks of the respective holders.

Acrobat, Adobe, Apache, Debian, Ethernet, Internet Explorer, Iomega, LaCie, Linux, Mac, Macintosh, Microsoft, Mozilla, MySQL, Red Hat, UNIX, Windows, WWW, Wi-Fi 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. WPA is a mark of the Wi-Fi Alliance.

Network Time Protocol Version 4 Distribution is copyright of University of Delaware – © University of Delaware 1992–2011. The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file. Permission to use, copy, modify, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Regulatory Information

Europe

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

- Electromagnetic Compatibility (EMC) Directive 2004/108/EC. See *Electromagnetic Compatibility (EMC)* on page 2.
- Low Voltage (LVD) Directive 2006/95/EC. See *Safety* on page 3.
- Restrictions of Hazardous Substances (RoHS) Directive 2011/65/EU. See *Disposal and Recycling* on page 4.

A copy of the original declaration of conformity may be obtained from Axis Communications AB. See *Contact Information* on page 4.

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

USA

Using an unshielded network cable (UTP) – This equipment has been tested using an unshielded network cable (UTP) and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. 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.

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

- Reorient or relocate the receiving antenna.
 - Increase the separation between the equipment and receiver.
 - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
 - Consult the dealer or an experienced radio/TV technician for help.
- To be used in a residential area or a demanding electrical environment, the product shall be connected using a shielded network cable (STP) that is properly grounded.

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.

USA

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

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

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

Canada

This digital apparatus complies with CAN ICES-3 (Class 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.

Canada

This digital apparatus complies with CAN ICES-3 (Class B). The product shall be connected using a shielded network cable (STP) that is properly grounded.

Cet appareil numérique est conforme à la norme CAN NMB-3 (classe B).

Le produit doit être connecté à l'aide d'un câble réseau blindé (STP) qui est correctement mis à la terre.

Europe

This digital equipment fulfills the requirements for RF emission according to the Class 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.

Europe

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

This product fulfills the requirements for emission and immunity according to EN 50121-4 and IEC 62236-4 railway applications.

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

This product fulfills the requirements for immunity according to EN 55103-2 residential, commercial and light-industrial environments.

This product fulfills the requirements for immunity according to EN 50130-4 residential, commercial, light-industrial and industrial 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.

Australia/New Zealand

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

Japan

この装置は、クラス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。

Japan

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

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.

Korea

이 기기는 가정용(B급) 전자파적합기기로서 주로 가정에서 사용하는 것을 목적으로 하며, 모든 지역에서 사용할 수 있습니다. 적절히 접지된 STP (shielded twisted pair) 케이블을 사용하여 제품을 연결 하십시오.

Safety

Photobiological Safety

This product fulfills the requirements for photobiological safety according to IEC/EN 62471 (risk group 1).

This product fulfills the requirements for photobiological safety according to IEC/EN 62471 (risk group 2).

This product fulfills the requirements for photobiological safety according to IEC/EN 62471 (risk group 3).

Battery

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

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.

The battery shall only be charged when mounted in the installation display. Use the power adapter supplied with the installation display.

⚠ 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 (selected countries only)
- visit Axis Support at www.axis.com/techsup/

Should you require any technical assistance, please contact appropriate channels according to your AVHS license agreement to ensure a rapid response.

Should you require any technical assistance, please contact ADP Helpdesk to ensure a rapid response.

Learn More!

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

AXIS M1143-L - User Manual

Table of Contents

Hardware Overview	7
Connectors and Buttons	7
LED Indicators	9
Access the Product	12
Access from a Browser	12
Access from the Internet	13
Set the Root Password	13
The Live View Page	13
Media Streams	19
How to Stream H.264	19
MJPEG	20
AXIS Media Control (AMC)	20
Alternative Methods of Accessing the Video Stream	21
Set Up the Product	22
Basic Setup	22
Video	23
Video Stream	23
Stream Profiles	25
Camera Settings	26
View Area	28
Overlay	28
Privacy Mask	31
Focus Adjustment	31
Configure the Live View Page	32
PTZ (Pan Tilt Zoom)	34
Preset Positions	34
Guard Tour	34
Advanced	35
Control Queue	35
Detectors	37
Camera Tampering	37
Motion Detection	37
Applications	40
Application Licenses	40
Install Application	40
Application Considerations	40
Events	42
Set Up Action Rules	42
Add Recipients	48
Create Schedules	50
Set Up Recurrences	50
Recordings	51
Find Recordings	51
Play Recording	52
Export Video Clip	52
Continuous Recording	52
Languages	54
System Options	55
Security	55
Date & Time	58
Network	58
Storage	64
Ports & Devices	66
Maintenance	67
Support	68
Advanced	69
Reset to Factory Default Settings	69
Troubleshooting	71
Check the Firmware	71
Upgrade the Firmware	71
Emergency Recovery Procedure	71

AXIS M1143-L - User Manual

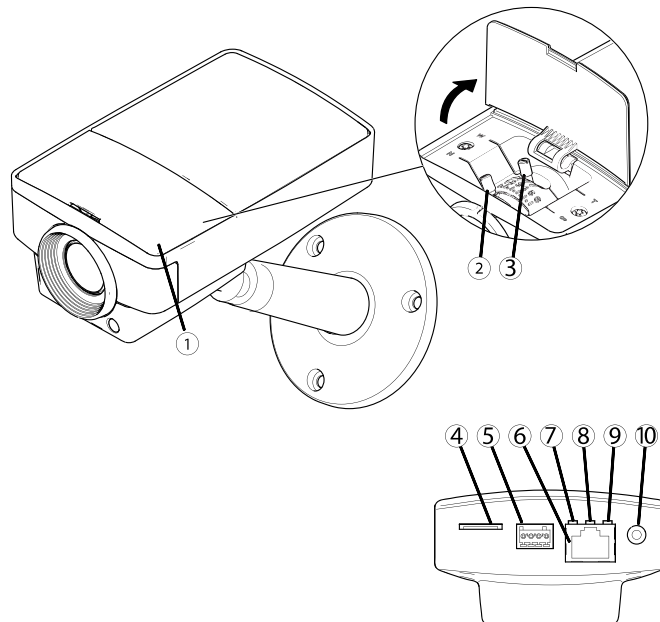
Table of Contents

Symptoms, Possible Causes and Remedial Actions	72
Technical Specifications	77
Connectors	79
Performance Considerations	81

AXIS M1143-L - User Manual

Hardware Overview

Hardware Overview



1. Lid
2. Focus puller
3. Zoom puller
4. microSD card slot
5. I/O connector
6. Network connector (PoE)
7. Network LED
8. Status LED
9. Power LED
10. Control button

Connectors and Buttons

For technical specifications, see [page 77](#).

For specifications and operating conditions, see [page 78](#).

Network Connector

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

RJ45 Ethernet connector.

RJ45 Ethernet connector with Power over Ethernet (PoE).

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

RJ45 with High Power over Ethernet (High PoE).

RJ45 Push-pull Connector (IP66) with High Power over Ethernet (High PoE).

RJ45 Ethernet service port.

D-coded M12 connector with Power over Ethernet (PoE).

AXIS M1143-L - User Manual

Hardware Overview

The unit can only use one Network interface, either an SFP module or RJ45 connector. SFP module has higher priority than the RJ45 connector.

NOTICE

Use the supplied midspan.

NOTICE

Due to local regulations or the environmental and electrical conditions in which the product is to be used, a shielded network cable (STP) may be appropriate or required. All cables connecting the product to the network and that are routed outdoors or in demanding electrical environments 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*.

NOTICE

Due to local regulations or the environmental and electrical conditions in which the product is to be used, a shielded network cable (STP) may be appropriate or required. All cables connecting the product to the network and that are routed outdoors or in demanding electrical environments 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*.

NOTICE

The product shall be connected using a shielded network cable (STP) or an optical fiber cable. 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*.

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*.

NOTICE

To comply with the IP66-rated design of the camera and maintain the IP66 protection, the supplied RJ45 Push-pull Connector (IP66) shall be used. Alternatively, use the RJ45 IP66-rated cable with premounted connector which is available from your Axis reseller. Do not remove the plastic network connector shield from the camera.

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**).

Note

The I/O connector is connected to the housing (fan/heater) on delivery. In the case of a fan or heater error, an input signal will be triggered in the camera. Set up an action rule in the camera to configure which action the signal shall trigger. For information about events and action rules, see *Events on page 42*.

The I/O connector is connected to the housing (fan/heater) on delivery. In the case of a fan or heater error, an input signal will be triggered in the camera. Set up an action rule in the camera to configure which action the signal shall trigger. For information about events and action rules, see the User Manual available on www.axis.com

AXIS M1143-L - User Manual

Hardware Overview

SD Card Slot

An SD card (not included) can be used for local recording with removable storage. For more information, see *Technical Specifications*.

A microSD card (not included) can be used for local recording with removable storage. For more information, see *Technical Specifications on page 77*.

A microSD card (not included) can be used for local recording of data and removable storage. For information about limitations and updates, see the product's release notes.

NOTICE

To prevent corruption of recordings, the SD card should be unmounted before removal. To unmount, go to **Setup > System Options > Storage > SD Card** and click **Unmount**.

NOTICE

To prevent corruption of recordings, the SD card should be unmounted before removal. To unmount, go to **Setup > System Options > Storage > SD Card** and click **Unmount**.

Note

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:

- Enabling the Focus Assistant. Press and very quickly release the Control button.
- Resetting the product to factory default settings. See *page 69*.
- Connecting to an AXIS Video Hosting System service. See *page 60*. 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 60*. To connect, press and hold the button for about 3 seconds.
- Connecting to an AXIS Video Hosting System service or AXIS Internet Dynamic DNS Service. For more information about these services, see the User Manual.

LED Indicators

LED	Color	Indication
Status	Red	Flashes red for firmware upgrade failure.
Status	Unlit	Connection and normal operation
	Amber	Steady during startup. Flashes during firmware upgrade.
	Green	Shows steady green for 10 seconds for normal operation after startup is completed.
	Amber/red	Flashes amber/red if network connection is unavailable or lost.
Tally	Unlit	Camera idle.
	Red	Active transmission or recording.
Microphone power	Unlit	48 V DC phantom power off.
	Blue	48 V DC phantom power on.

AXIS M1143-L - User Manual

Hardware Overview

LED	Color	Indication
Status	Green	Connection and normal operation
	Amber	Steady during startup. Flashes during firmware upgrade.
	Amber/red	Flashes amber/red if network connection is unavailable or lost.
	Red	Flashes red for firmware upgrade failure.

LED	Color	Indication
Network	Green	Steady for connection to a 100 Mbit/s network. Flashes for network activity.
	Amber	Steady for connection to a 10 Mbit/s network. Flashes for network activity.
	Unlit	No network connection.
Network	Green	Steady for connection to a 1 Gbit/s network. Flashes for network activity.
	Amber	Steady for connection to a 10/100 Mbit/s network. Flashes for network activity.
	Unlit	No network connection.
Micro- phone Power	Blue	Steady - 12 V DC phantom power on. Microphone is connected
		Flashes - 12 V DC phantom power on. Microphone is disconnected
	Unlit	12 V DC phantom power off
Status	Green	Steady green for normal operation.
	Amber	Steady during startup and when restoring settings.
	Red	Slow flash for failed upgrade.
Power	Green	Normal operation.
	Amber	Flashes green/amber during firmware upgrade.

LED	Color	Indication
Wireless	Unlit	Wired mode.
	Green	Steady for connection to a wireless network. Flashes for network activity.
	Red	Steady for no wireless network connection. Flashes while scanning for wireless networks.
	Amber	Steady or flashing during wireless network pairing.

LED	Color	Indication
Network	Green	Steady for connection to a 1 Gbit/s network. Flashes for network activity.
	Amber	Steady for connection to a 10/100 Mbit/s network. Flashes for network activity.
	Unlit	No network connection.
Status	Green	Steady green for normal operation.
	Red	Slow flash for failed upgrade.
Power	Green	Normal Operation.
HDD	Amber	Flashing for normal operation.

AXIS M1143-L - User Manual

Hardware Overview

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**.
- The Power 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 Network LED can be disabled so that it does not flash when there is network traffic. To configure, go to **Setup > System Options > Ports & Devices > LED**. See the online help for more information.
- The tally LED can be configured to be lit or unlit during normal operation. To configure, go to **Setup > System Options > Ports & Devices > LED**. See the online help for more information.

LED	Color	Indication
Housing (fan and heater)	Green	Normal operation.
	Flashing green	Single flash: Heater error Double flash: Fan error Triple flash: General error Alarm events will be triggered through the camera's input port. Contact your Axis reseller for information about spare parts and troubleshooting.

Note

This status LED referred to in the table above is located in the housing.

AXIS M1143-L - User Manual

Access the Product

Access the Product

To install the Axis product, refer to 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 Macintosh and Firefox with other operating systems. See *Technical Specifications on page 77*.

The product can be used with most operating systems and browsers. The recommended browsers are Internet Explorer with Windows, Safari with Macintosh and Firefox with other operating systems. See *Technical Specifications on page 77*.

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

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

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.
- QuickTime™ is also supported for viewing H.264 streams.
- If your computer restricts the use of additional software components, the product can be configured to use a Java applet for viewing Motion JPEG.

Access from a Browser

1. Start a browser (Chrome, Internet Explorer, Firefox, Safari).
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 Macintosh computer (Mac OS X), click on the Bonjour tab 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 Installation and Management Software CD or the document *Assign an IP Address and Access the Video Stream* on Axis Support web at www.axis.com/techsup

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 support pages at www.axis.com/techsup or the Installation Guide available at www.axis.com

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 . This information is also available from the support pages at www.axis.com/techsup

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 13*.
4. If this is the first time the product is accessed, the **PTZ Calibration** tool starts automatically. See .
5. The product's Live View page opens in your browser.
6. AXIS Entry Manager opens in your browser. The start page is called the Overview page.

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 the Product

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 AdvancedSetup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**.

For more information, see *NAT traversal (port mapping) for IPv4* on page 61. See also AXIS Internet Dynamic DNS Service at www.axiscam.net

For more information about NAT traversal for IPv4, see the product's User Manual. See also AXIS Internet Dynamic DNS Service at www.axiscam.net

For Technical notes on this and other topics, visit the Axis Support web at www.axis.com/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 55.

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.

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 69.

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. For information about how to reset the product to factory default, see the product's User Manual.

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.

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.

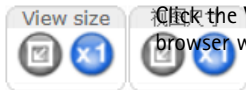
AXIS M1143-L - User Manual

Access the Product

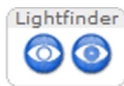
Controls on the Live View Page



Click **View size** to scale the image down to 800 pixels wide or to full scale. Only available in MJPEG.



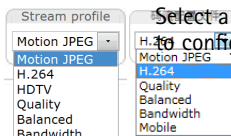
Click the **View size** buttons to show the image in full size (right button) or to scale down the image to fit the browser window (left button).



Click **WDR on** to enable WDR in intense backlight conditions. Read more about wide dynamic range on . Click **Lightfinder Mode** to enable this mode. Read more about Lightfinder on .



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



Select a stream profile for the Live View page from the **Stream Profile** drop-down list. For information about how to configure stream profiles, see [page 25](#).



The **Palette** drop-down list allows you to apply a palette to the image. See [Image on page 24](#)



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 33](#).



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 33](#).



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 15](#).



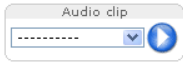
Click **Snapshot** to save a snapshot of the video image. This button is primarily intended for use when the AXIS Media Control viewer toolbar is not available. Enable this button from **Live View Config > Action Buttons**.



Click **Defog** to enable or disable the Defog feature. For more information see .

AXIS M1143-L - User Manual

Access the Product



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.

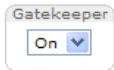


The product's fan is controlled by the ambient temperature and is turned on and off automatically. If required, the fan can be activated manually by clicking the **Fan** button. To show the button, go to **Setup > Live View Config**. Under **Action Buttons**, select **Show fan button** and specify the number of minutes the fan should be activated.

The product's fans are controlled by the ambient temperature and are turned on and off automatically. If required, the fans can be activated manually by clicking the **Fan** button. To show the button, go to **Setup > Live View Config**. Under **Action Buttons**, select **Show fan button** and specify the number of minutes the fans should be activated.



The product's heater is controlled by the ambient temperature and is turned on and off automatically. If required, the heater can be activated manually by clicking the **Heater** button. To show the button, go to **Setup > Live View Config**. Under **Action Buttons**, select **Show heater button** and specify the number of minutes the heater should be activated.



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



Activate or de-activate IR illumination from **Setup > Video & Audio Video > Camera Settings**. Move the slider to increase or decrease the intensity of the LEDs. Enable this button from **Live View Config > Action Buttons**.

Manual Trigger

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

In the Live View page, the manual trigger buttons are available from the **Actions** tab. Click **Trigger on** to start the action. Click **Trigger off** to stop the action.



To configure the manual trigger:

1. Go to **Setup > Events**.
2. Click **Add** to add a new action rule.
3. From the **Trigger** drop-down list, select **Input Signal**.
4. From the second drop-down list, select **Manual Trigger**.
5. Select the desired action and configure the other settings as required.

For more information about action rules, see *Events on page 42*.

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 20* for more information. The toolbar displays the following buttons:

AXIS M1143-L - User Manual

Access the Product



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. The location where the image is saved can be specified in the AMC Control Panel.



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. The location where the recording is saved can be specified in the AMC Control Panel. Enable this button from **Live View Config > Viewer Settings**.

PTZ Controls

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

Note

PTZ controls are only available for view areas, which are visible when the Multiple View Modes option has been selected. See .

Note

PTZ controls are only available for view areas.

Note

These controls are available if digital PTZ is enabled in the selected view area, see *View Area on page 28*.

Note

These controls are available if digital PTZ is enabled in the selected view area or if a PTZ driver has been uploaded. For more information on view areas, see *View Area on page 28*. For more information on how to upload a driver, see . To switch between the two options see .

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

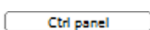
Select **Focus window** to define an area of the camera's image that focus should be applied on. If the focus window is set from the Live View page, any change in the camera position will return the autofocus to the entire window. To set a permanent focus window, see *Preset Positions on page 34*



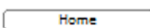
Click the **Emulate joystick mode** button and click in the image to move the camera view in the direction of the mouse pointer.



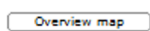
Click the **Center mode** button and click in the image to center the camera view on that position. The center mode button could also be used to zoom in on a specific area. Click in the image and drag to draw a rectangle surrounding the area to be magnified. To zoom out, rotate the mouse wheel.



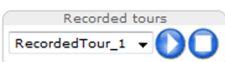
Click the **Ctrl panel** button to open the PTZ control panel which provides additional PTZ controls. User-defined buttons can also appear in the Control panel. See *Controls on page 35*.



Click the **Home** button to go to the Home preset position. See *Preset Positions on page 34*.



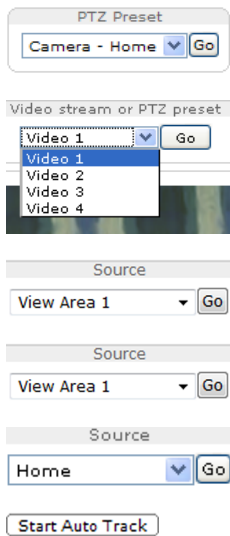
Click the **Overview map** button to hide or view the overview map. See .



Select a recorded tour and click  to play a previously recorded tour and click  to stop. See .

AXIS M1143-L - User Manual

Access the Product



Select a PTZ preset position to steer the camera view to the saved position. See *Preset Positions on page 34*.

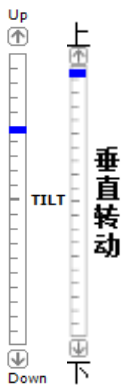
Select the video channel or a PTZ preset position to steer the camera view to the saved position. See *Preset Positions on page 34*.

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

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

Select a PTZ preset position to steer the camera view to the saved position. See *Preset Positions on page 34*.

Click the **Start Auto Track** button to start autotracking directly from the Live View page. See .



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

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

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

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

Focus bar – Click on a position on the focus bar to set the focus position. This will disable the product's autofocus. To re-enable, use the PTZ control panel which is opened by clicking the **Ctrl panel** button (see above). If autofocus is enabled, **Auto** is visible next to the **Focus bar** bar, see below. For more information about the autofocus function, see .

Iris bar – Click on a position on the iris bar to change the degree to which the iris is opened. This will disable the product's auto iris. To re-enable, use the PTZ control panel which is opened by clicking the **Ctrl panel** button (see above). If auto iris is enabled, **Auto** is visible next to the **Iris bar** bar, see below.

Important

Adjusting the iris position will affect the shutter speed and gain. The default setting is recommended.

Brightness bar – Click on a position on the brightness bar to adjust the image brightness. This setting will not be saved. To make a saved change, go to **Setup > Video > Camera Settings > Brightness** and adjust the brightness.



AXIS M1143-L - User Manual

Access the Product

Clicking **Zoom out to overview image** will set the camera to the minimum zoom position. In this position, the camera cannot pan or tilt.

Zoom out to overview image

The PTZ controls can be disabled under **PTZ > Advanced > Controls**, see *Controls on page 35*.

AXIS M1143-L - User Manual

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 Axis product provides several 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.

The Live View page in the product provides access to H.264 and Motion JPEG video streams, and to the list of available stream profiles. Other applications and clients can access video streams directly, without going via the Live View 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 always 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.	

Unicast RTP	This unicast method (RTP over UDP) is used for live unicast video, especially when it is important to always 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 10 simultaneous unicast connections.
RTP over RTSP	This unicast method (RTP tunneled over RTSP) is useful as it is relatively simple to configure firewalls to allow RTSP traffic.	
RTP over RTSP over HTTP	This unicast method can be used to traverse firewalls. Firewalls are commonly configured to allow the HTTP protocol, thus allowing RTP to be tunneled.	
Multicast RTP	This method (RTP over UDP) should be used for live multicast video. The video stream is always up-to-date, even if some frames are dropped.	

AXIS M1143-L - User Manual

Media Streams

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 10 simultaneous connections.
--

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

Note

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

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.

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.

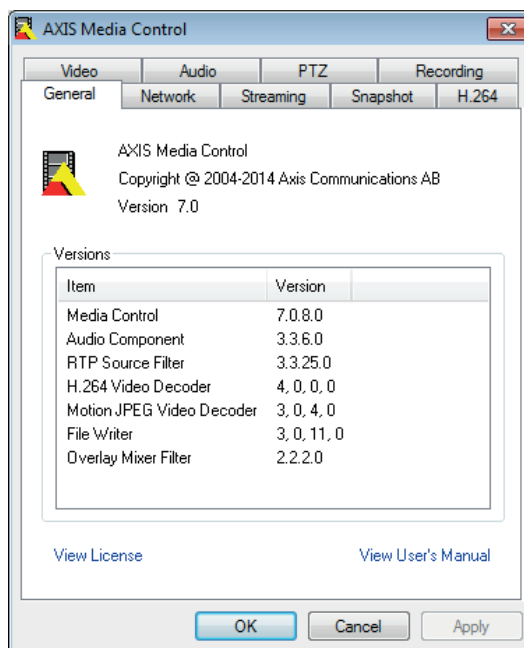
The AMC Control Panel can be used to configure various video settings. Please see the AXIS Media Control User's Manual for more information.

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

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

AXIS M1143-L - User Manual

Media Streams



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, 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`

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.


AXIS M1143-L - User Manual

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 access to all settings except System Options

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 55*.
2. Wireless. See .
3. TCP/IP. See *page 58*.
4. Date & Time. See *page 58*.
5. Video Stream. See *page 23*.
6. Focus & Zoom. See .
7. Focus. See
8. Focus. See *page 31*
9. Audio Settings. See .

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

Set Up the Product

Video

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

- Video stream. See *page 23*.
- Stream profiles. See *page 25*.
- Camera settings. See *page 26*.
- View area. See *page 28*.
- View areas. See *page 28*.
- View areas. See .
- Overlay image. See *page 28*.
- Privacy mask. See *page 31*.
- Privacy mask. See .
- Focus and zoom. See .
- Focus. See .

Video Stream

You can define the following video stream settings from **Video & Audio Video > Video Stream**:

- Image. See *page 24*.
- Audio. See .
- Direction. See .
- H.264. See *page 24*.
- MJPEG. See *page 25*.

Note

Video stream can be configured for each channel including quad stream.

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 requirement that the image is a certain size, for example in face recognition.

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 requirement that the image is a certain size, for example for object identification.

The pixel counter can be accessed from:

- **Video & Audio > Video Stream****Video > Video Stream**. Under **Preview**, click **Open** and select the **Show pixel counter** option to enable the rectangle in the image. Use the mouse to move and resize the rectangle, or enter the number of pixels in the **Width** and **Height** fields and click **Apply**.
- **Video & Audio > Focus**. 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**.
- **Video & Audio > Focus & Zoom**. 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**.

AXIS M1143-L - User Manual

Set Up the Product

- 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 > Video Stream**. Select the **Image** tab.

The following settings are available:

- **Resolution**. Select the default resolution.
- Select **Aspect ratio correction** to improve the appearance of images in the browser when the video stream has a different aspect ratio. Pixels comprising the image are rearranged so as to provide a more accurate representation of the image.
- **Compression**. The compression level affects the image quality, bandwidth and file size of saved images; the lower the compression, the higher the image quality with higher bandwidth requirements and larger file sizes.
- **Mirror image**. If required, the image can be mirrored.
- **Rotate image**. If required, the image can be rotated.
- **Color setting**. Select either **Color** or **Black & White**. **Black & White** uses less bandwidth than **Color**.

Note

Video streams over HDMI can only be rotated 180° or 0°.

- **Palette**. The image can be colored by applying a **palette**. Colors in the image indicate temperature differences and can be used to improve visibility of fine details. The palette selected here is used as the default palette, other palettes can be selected on the Live View page.
- **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 28*.

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

H.264

H.264, also known as MPEG-4 Part 10/AVC, is a video compression standard that provides high quality video streams at low 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 StreamVideo > 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 **GOV length** is the number of frames between two consecutive I-frames. Increasing the GOV 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.
- **High**. The High profile provides reduced bit rate and higher compression with maintained video quality compared to the Main profile but requires more processing power to decode.

The bit rate can be set as **Variable bit rate (VBR)** or **Constant bit rate (CBR)**. 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

AXIS M1143-L - User Manual

Set Up the Product

selecting **Variable bit rate (VBR)** will be sufficient. But if bandwidth is limited, it is recommended to control the bit rate by selecting **Constant bit rate (CBR)**. 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. CBR allows you to set a target bit rate that limits the bandwidth consumption.

The CBR 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 CBR 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 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.

Sometimes the image size is large due to low dynamic 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 dynamic. 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:

- When setting up recording using action rules. See *Events on page 42*.
- When setting up continuous recording. See *Continuous Recording on page 52*.
- In the Live View page – select the stream profile from the **Stream profile** drop-down list.
- In the Live View page – select the stream profile from the **Video** tab.

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 Video > Stream Profiles**.

AXIS M1143-L - User Manual

Set Up the Product

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

Camera Settings

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

Image Appearance

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

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

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

Increasing the **Sharpness** can increase bandwidth usage. A sharper image might increase image noise especially in low dynamic 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 slider.

The **Contrast** changes the relative difference in thermal radiation. It can be adjusted using the slider.

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

Use the **Noise reduction** slider to adjust the noise reduction level. A higher value produces an image with little noise, but at the expense of details in the image. Noise reduction may increase the amount of motion blur.

White Balance

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.

Exposure Settings

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

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

Exposure control – This setting is used to adapt to the amount of light used. **Automatic** is the default setting and can be used in most situations. The shutter speed is automatically set to produce optimum image quality. **Flicker-free 50 or 60 Hz** is used to remove flicker which can be caused by fluorescent and other light sources. The **Hold current** option locks the current exposure settings.

Max exposure time – Decreasing the exposure time will reduce motion blur. For more information, see the online help .

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

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

AXIS M1143-L - User Manual

Set Up the Product

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

Iris adjustment

Select **Enable automatic iris adjustment** to automatically compensate for changing light conditions. This option is not available if a fixed iris is used.

Use the **Iris adjustment** slider to set the preferred F-value. The scale represents the amount the iris is open. If set to 0, the iris is opened as much as possible. If set to 100, the iris is closed as much as possible. The actual F-value is shown below the slider. If automatic iris adjustment is enabled, the iris will stay at this position as long as light conditions are favorable. If light conditions change, the iris will adjust itself to the best iris settings. If automatic iris adjustment is disabled, the iris will lock on the set position regardless of light conditions

Day/Night

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

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

The camera lens is IR corrected, which means that it maintains focus in mixed light, however a small focus adjustment is recommended when IR illumination is used. Select **Enable focus adjustment for IR illumination** to automatically adjust the focus when the IR cut filter switches between on and off.

The **Day/Night shift level** bar helps determine when the camera will shift from day mode to night mode. Normally, the camera automatically changes mode from day to night when very dark (level 100 in the slider). By setting **Day/Night shift level** to a lower value, the camera will change to night mode earlier.

Built-in IR Illuminations LEDs

⚠WARNING

Risk of eye injury. Do not look directly into the IR LED at short distance. Since the light provided from the IR LED is outside of the visible range, it is not possible to see if it is active. Use the camera to check if the IR illumination is active.

The IR illumination can be activated or de-activated, and its intensity can be increased or decreased by moving the slider, from the product's **Live View** page. Other settings can be defined from **Setup > Video & Audio Video > Camera Settings**.

De-select the **Enable IR illumination** option to disable IR illumination altogether. If you disable the **Synchronize IR illumination with day/night** option, IR illumination will not be synchronized with day/night changes.

To configure IR illumination click **Edit**.

The **IR Illumination** window displays the approximate area the IR light will illuminate given the current settings. When **Angle of illumination** is set to **Auto**, the IR illumination is automatically adjusted according to the camera's zoom. When this 'Auto' behavior is disabled, it is possible to manually adjust the angle of the IR light by moving the **Angle of illumination** slider.

The **IR Illumination** window displays the approximate area the IR light will illuminate given the current settings. The default IR illumination zoom is set at 1. If the camera's zoom is adjusted to a different value, move the **Angle of illumination** slider to the same value, for optimal IR illumination in the IR Light window (**Camera Settings > IR Illumination> Edit**) in the camera's GUI.

AXIS M1143-L - User Manual

Set Up the Product

View Area

Note

This feature is available only if digital PTZ was selected when configuring the product for the first time or after resetting to factory default.

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

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

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

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

To configure the view area:

To add a new view area:

1. Go to **Video & Audio > View AreaVideo > 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. Use the mouse to move and resize the view area.
6. A new view area covers the whole image. Use the mouse to move and resize the view area.
7. Select **Enable PTZ** to enable digital PTZ for the view area.
8. 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.

Note

View areas will be disabled if **Optical zoom for monitoring** is selected. See .

Overlay

Overlays are used to provide extra information, for example for 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*.

Image and text overlay will not be displayed on video stream over HDMI.

AXIS M1143-L - User Manual

Set Up the Product

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 58.

Note

Overlay images and transparent text backgrounds are not available in Overview mode.

Note

Overlay is not possible for quad stream.

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.

Since it is static, the position and size of an overlay image will remain the same regardless of resolution and Pan/Tilt 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 31.

For more information about privacy masks, see .

The overlay image is displayed in Normal mode. The image is not available in Overview mode.

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** > **Overlay Image**.
2. Click **Browse** and browse to the file.
3. Click **Upload**.
4. The **Transparency Settings** page is now displayed:
 - To make a color in the overlay image transparent, select **Use transparency** and enter the RGB hexadecimal value for the color. Example: To make white transparent, enter #FFFFFF.

AXIS M1143-L - User Manual

Set Up the Product

- 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 ImageVideo > 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 StreamVideo > 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 42*, 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.

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 & AudioVideo > 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.

Example

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

Note

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

AXIS M1143-L - User Manual

Set Up the Product


Privacy Mask

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

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

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

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

For more information, see the online help 

Important

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

Note

Privacy mask is not available for the quad stream. However, privacy masks configured on each channel will be displayed in the quad.

Note

Privacy masks in view modes other than the Overview mode may appear warped.

Note

To view privacy masks in video over HDMI the video stream must be restarted every time the Axis product is restarted. This can be done for example, by selecting a video stream from the **Stream Profile** drop down list in the top left hand corner in the product's **Live View** page.

Focus Adjustment

The focus can be adjusted under **Basic Setup > Focus**. Follow the on-screen instructions to adjust the focus. For further information about focus, refer to the product's Installation Guide.

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 25*.
- Default Viewer for Browser. See *page 32*.
- Viewer Settings. See *page 32*.
- Action Buttons. These are the buttons described in *Controls on the Live View Page on page 14*.
- Action Buttons. These are the buttons described in .
- User Defined Links. See *page 33*.
- Light Buttons. See .
- Output Buttons. See *page 33*.

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.

Note

The Overview snapshot, see , is only available when using AMC or Server Push.

Browser	Viewer	Description
Windows Internet Explorer	AMC	Recommended viewer in Internet Explorer (H.264/Motion JPEG).
	QuickTime	H.264.
	Java applet	A slower imaging alternative to AMC (Motion JPEG). Requires one of the following installed on the client: <ul style="list-style-type: none">• JVM (J2SE) 1.4.2 or higher.• JRE (J2SE) 5.0 or higher.
	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.
	Java applet	A slower imaging alternative to Server Push (Motion JPEG only).
	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.
- Select **Show viewer toolbar** to display the viewer toolbar under the video image in the Live View page. See .

AXIS M1143-L - User Manual

Configure the Live View Page

- **H.264 decoder installation.** The administrator can disable installation of the H.264 decoder included with AXIS Media Control. This is used to prevent installation of unlicensed copies. Further decoder licenses can be purchased from your Axis reseller.
- Select **Show crosshair in PTZ joystick mode** to enable a cross that will indicate the center of the image in PTZ joystick mode.
- Select **Use PTZ joystick mode as default** to enable joystick mode. The mode can be changed temporarily from the PTZ control panel.
- Select **Enable recording button** to enable recording from the Live View page. This button is available when using the AMC viewer. The recordings are saved to the location specified in the AMC Control Panel. See *AXIS Media Control (AMC) on page 20*.

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.

In the Live View page, user-defined links are available from the **Actions** tab.

Output Buttons

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

Note

To enable this setting at least one I/O port must be configured as an output port. See *I/O Ports on page 66*.

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.

In the Live View page, the buttons are displayed on the **Actions** tab.

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 66*.

Note

A multi-connector cable (available from Axis) is required when connecting external I/O devices to the Axis product. See

AXIS M1143-L - User Manual

PTZ (Pan Tilt Zoom)

PTZ (Pan Tilt Zoom)

The PTZ menu is available if a PTZ driver has been uploaded. See .

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 28*.

This option is only available if you have selected **Optical zoom for installation**. See .

If **Optical zoom for monitoring** has been selected during installation view areas will be disabled. For more information see .

The PTZ menu is available if digital PTZ (pan, tilt and zoom) is enabled.

PTZ controls are only available for view areas.

The PTZ menu is available if digital PTZ (pan, tilt and zoom) is enabled in the selected view area or if a PTZ driver has been uploaded. For more information on view areas, see *View Area on page 28*. For more information on how to upload a driver, see . To switch between the two options see

Preset Positions

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

- Pan and tilt positions
- Zoom position
- Focus position (manual or automatic)
- Iris position (manual or automatic)

Each view area has its own preset positions.

Guard Tour

A guard tour displays the video stream from different preset positions, one-by-one, in a predetermined order or at random and for configurable time periods. The enabled guard tour will keep running after the user has logged off or closed the browser.

The guard tour capability in this Axis product also includes tour recording. Tour recording is described in .


To add a guard tour:

1. Go to **PTZ > Guard Tour** and click **Add**.
2. Select **Create a preset tour** and click **OK**.
3. Enter a descriptive name.
4. Specify the pause length between runs.
5. Select an available preset position and click **Apply**.
6. Specify the **Move Speed**.
7. Specify the **View Time** in seconds or minutes.
8. Specify the **View Order** or select the **Random view order** option.
9. Click **Save**.

AXIS M1143-L - User Manual

PTZ (Pan Tilt Zoom)

To modify or remove guard tours, go to **PTZ > Guard Tour**, select the guard tour in the **Guard Tour List** and click **Modify/Remove**.

For more information see the online help .

Note

This Axis product supports limited guard tours. The pause between successive guard tours must be set to at least 10 minutes.

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:

- Pan control
- Tilt control
- Zoom control
- Focus control
- Iris 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

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 55*) 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 42*). The event will immediately be placed first in the queue except when an administrator is in control.
3. **Operator** – Same as administrator but with lower priority
4. **Guard Tour** – A guard tour (see *page 34*) has PTZ control for an indefinite period of time. It may be overridden by an operator, event or administrator. The guard tour will resume when higher priority groups leave the queue.
5. **Viewer** – Multiple viewers must wait for their turn. The viewer has 60 seconds PTZ control before control is passed on to the next viewer in queue.

AXIS M1143-L - User Manual

PTZ (Pan Tilt Zoom)

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.

Detectors

Detectors

Camera Tampering

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

To configure tampering:

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. Select the video channel.
7. Optionally, select a schedule and set additional conditions.
8. 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 42*.

Motion Detection

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

Motion detection is used to generate an alarm whenever movement starts or stops in the camera's field of view. The alarm is generated when the camera is in Overview Mode, that is, when using the Panopsis lens. See .

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

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

For instructions, see *Set Up Motion Detection Windows on page 38*.

To control the number of motion detection alarms, the parameters **Object Size**, **History** and **Sensitivity** can be adjusted. See *Motion Detection Parameters on page 38*.

Detectors

Once motion detection windows are configured, the Axis product can be configured to perform actions when motion is detected. Possible actions include uploading images and start recording. For more information, see *Set Up Action Rules on page 42*.

Once configured, motion detection windows appear in the list of available triggers for triggered events. See .

Note

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

Set Up Motion Detection Windows

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

1. Go to **Events > Motion Detection**.
2. Go to **Detectors > Motion Detection**.
3. Select a desired resolution for viewing while setting up Motion Detection from the **View in** list.
4. Select the **Configure Included Windows** option and click **New**. Select the new window in the list of windows and enter a descriptive name.
5. Adjust the size (drag the bottom right-hand corner) and the position (click on the text at the top and drag to the desired position) of the window.
6. Adjust the **Object Size**, **History** and **Sensitivity** profile sliders (see *Motion Detection Parameters* for details). Any detected motion within an active window is indicated by red peaks in the **Activity window**.
7. Click **Save**.

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

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

Motion Detection Parameters

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

Parameter	Object Size	History	Sensitivity
Description	Object size relative to window size.	Object memory length.	Difference in luminance between background and object.
High level (100%)	Only very large objects trigger motion detection.	An object that appears in the window triggers motion detection for a long time before it is considered as non-moving.	Ordinary colored objects on ordinary backgrounds trigger motion detection.
Medium level (50%)			A large difference in luminance is required to trigger motion detection.
Low level (0%)	Even very small objects trigger motion detection.	An object that appears in the window triggers motion detection only for a very short time before it is considered as non-moving.	Only very bright objects on a dark background trigger motion detection.

AXIS M1143-L - User Manual

Detectors

Recommended values	5–15%	60–90%	75–95%
Default values	15%	90%	90%

Parameter	Object Size	History	Sensitivity
High level (100%)	Only very large objects trigger motion detection.	An object that appears in the window triggers motion detection for a long time before it is considered as non-moving.	Small variations in thermal radiation between object and background will trigger the motion detection.
Low level (0%)	Even very small objects trigger motion detection.	An object that appears in the window triggers motion detection only for a very short time before it is considered as non-moving.	Large variations in thermal radiation between object and background will trigger motion detection
Default values	Low	High	High

Note

- To trigger on small objects or movements, use several small motion detection windows rather than one large window and select a low object size.
- To avoid triggering on small objects, select a high object size.
- While monitoring an area where moving objects are not expected, select a high history level. This will cause motion detection to trigger as long as the object is present in the window.
- To only detect flashing light, select a low sensitivity. In other cases high sensitivity is recommended.

AXIS M1143-L - User Manual

Applications

Applications

Third party applications can be uploaded to and installed on the Axis product. Applications add functionality to the product, for example video analytics and intelligent video capabilities such as recognition, tracking, detection and counting. For information about available applications, downloads, trials and licenses, go to www.axis.com/applications

Note

- It is recommended to run one application at a time.
- 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.
- Avoid running applications when the built-in motion detection is active.
- Applications are supported on channel 1.
- Applications are not available while using multiple view modes. For more information, see .

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**.

Install Application

To install 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, installed applications and their settings will remain unchanged, although this is not guaranteed by Axis Communications AB. Note that the application must be supported by the new firmware. For information about firmware upgrades, see *Upgrade the Firmware*.

AXIS M1143-L - User Manual

Applications

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

If the Axis product is restored, installed 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*.

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

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.

The Event pages allow you to configure the Axis product to perform actions when different events occur. For example, the product can send an email notification or activate an output port when an alarm is triggered. The set of conditions that defines how and when the action is triggered is called an action rule. 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 43* and *Actions on page 47*.

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.

The following example describes how to set up an action rule to send an email notification when any alarm is triggered.

Set up motion detection and add a network share:

1. Go to **Detectors > Motion Detection** and configure a motion detection window. See *page 38*
2. Go to **System Options > Storage** and set up the network share. See *page 66*.

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 **Detectors** from the **Trigger** drop-down list.
 4. Select **Motion Detection** from the drop-down list. Select the motion detection window to use.
 5. Optionally, select a **Schedule** and **Additional conditions**. See below.
 6. Under **Actions**, select **Record Video** from the **Type** drop-down list.
 7. Select a **Stream profile** and configure the **Duration** settings as described below.
 8. Select **Network Share** from the **Storage** drop-down list.
-
1. Configure the alarms. See .
 2. Go to **Setup > Additional Controller Configuration > Events > Action Rules** and click **Add**.
 3. Select **Enable rule** and enter a descriptive name for the rule.
 4. Select **Event Logger** from the **Trigger** drop-down list.
 5. Optionally, select a **Schedule** and **Additional conditions**. See below.
 6. Under **Actions**, select **Send Notification** from the **Type** drop-down list.
 7. Select an email recipient from the drop-down list. See *Add Recipients on page 48*.

The following example describes how to set up an action rule to activate an output port when the door is forced open.

1. Go to **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports**.


Events

2. Select **Output** from the desired **I/O Port Type** drop-down list and enter a **Name**.
3. Select the I/O port's **Normal state** and click **Save**.
4. Go to **Events > Action Rules** and click **Add**.
5. Select **Door** from the **Trigger** drop-down list.
6. Select **Door Alarm** from the drop-down list.
7. Select the desired door from the drop-down list.
8. Select **DoorForcedOpen** from the drop-down list.
9. Optionally, select a **Schedule** and **Additional conditions**. See below.
10. Under **Actions**, select **Output Port** from the **Type** drop-down list.
11. Select the desired output port from the **Port** drop-down list.
12. Set state **Active**.
13. Select **Duration** and **Go to opposite state after**. Then enter the desired duration of the action.
14. Click **OK**.

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 .

Triggers

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

- **Access Point**
 - **Access Point Enabled** – Triggers the action rule when an access point device such as a reader or REX device is configured, for example when the hardware configuration is completed or an identification type is added.
- **Configuration**
 - **Access Point Changed** – Triggers the action rule when the configuration of an access point device such as a reader or REX device is changed, for example when hardware is configured or an identification type is edited, changing the ways through which a door can be accessed.
 - **Access Point Removed** – Triggers the action rule when the hardware configuration of an access point device such as a reader or REX device is reset.
 - **Area Changed** – Not supported by this version of AXIS Entry Manager. Must be configured by a client such as an access management system, through the VAPIX® application programming interface, that supports this feature and use devices that can provide the required signals. Triggers the action rule when an access area is changed.
 - **Area Removed** – Not supported by this version of AXIS Entry Manager. Must be configured by a client such as an access management system, through the VAPIX® application programming interface, that supports this feature and use devices that can provide the required signals. Triggers the action rule when an access area is removed from the system.

Events

- **Door Changed** – Triggers the action rule when the door configuration settings, for example door name, are changed or when a door is added to the system. This can for example be used to send a notification when a door is installed and configured.
- **Door Removed** – Triggers the action rule when a door is removed from the system. This can for example be used to send a notification when a door is removed from the system.
- **Door**
 - **Door Alarm** – Triggers the action rule when the door monitor indicates that the door has been forced open, the door is open too long, or if the door is faulty in any way. This can for example be used to send a notification when someone is forcing an entry.
 - **Door Double-Lock Monitor** – Triggers the action rule only when the secondary lock changes state to either locked or unlocked.
 - **Door Lock Monitor** – Triggers the action rule when the normal lock changes state to either locked or unlocked. For example, a fault is triggered when the door monitor detects that the door is open although the lock is locked.
 - **Door Mode** – Triggers the action rule when the door changes states, for example, when the door has been accessed or blocked, or the door is in lockdown mode. For more detailed descriptions of these modes, see the online help.
 - **Door Monitor** – Triggers the action rule when the door monitor state changes. This can for example be used to send a notification when a door monitor indicates that the door is opened or closed.
 - **Door Tamper** – Triggers the action rule when the door monitor detects that the connection is interrupted, for example if someone cuts the wires to the door monitor. To use this trigger, make sure that **Enable supervised inputs** is selected and that end of line resistors are installed on the relevant door connector input ports. For more information, see .
 - **Door Warning** – Triggers the action rule before the door open too long alarm goes off. This can be used to, for example, send a warning signal that the door controller will send the real alarm, the door open too long alarm, if the door is not closed within the specified door open too long time. For more information about door open too long time, see .
- **Event Logger** – Keeps track of all events in the door controller, for example when a user swipes a card or opens a door. If **Global events** is enabled, the event logger keeps track of all the events in every controller in the system. To set which alarms and events that can trigger an action rule, go to **Setup > Configure Event and Alarm Logs**. The event logger is shared by the system and can store up to 30 000 events. When the limit is reached, the event logger uses the first in first out (FIFO) rule. This means that the first event is the first to be overwritten.
 - **Alarm** – Triggers the action rule when one of the specified alarms has been triggered. The system administrator can configure which events are more important than others and select whether a particular event should trigger an alarm or not.
 - **Dropped Alarms** – Triggers the action rule when new alarm records cannot be written to the alarm logs. For example if there are so many simultaneous alarms that the event logger cannot keep up. When an alarm is dropped, a notification can be sent to the operator.
 - **Dropped Events** – Triggers the action rule when new event records cannot be written to the event logs. For example, if there are so many simultaneous events that the event logger cannot keep up. When an event is dropped, a notification can be sent to the operator.
- **Applications** – Use installed applications to trigger the rule. See *Applications on page 40*.
- **Detectors**
 - **Audio Detection** – Trigger the rule when audio is detected. See .
 - **Day/Night Mode** – Trigger the rule when the product switches between day mode (IR cut filter on) and night mode (IR cut filter off). This can for example be used to control an external infrared (IR) light connected to an output port.

AXIS M1143-L - User Manual

Events

- **Live Stream Accessed** – Trigger the rule when any stream is accessed and during edge storage playback. This can for example be used to send notifications.
- **Motion Detection** – Trigger the rule when motion is detected. See *Motion Detection on page 37*.
- **Shock Detected** – Trigger the rule when the Axis product detects it has been tilted or hit. See .
- **Enter/Exit** – Trigger the rule when an object has entered or exited the area. See .
- **Fence Detector** – Trigger the rule when an object has crossed a virtual line. See .
- **Object Removed** – Trigger the rule when an object has been removed from a scene. See .
- **PIR** – Trigger the rule when the PIR sensor detects motion. See .
- **Tampering** – Trigger the rule when tampering is detected. See *Camera Tampering on page 37*.
- **Video source connected** – Trigger the rule when a sensor unit is connected to or disconnected from the main unit.
- **Hardware**
 - **Casing Open** – Triggers the action rule if the cover of the door controller is opened or if the door controller is removed from the wall or ceiling. This can for example be used to send a notification if the casing has been opened for maintenance purposes or when someone has tampered with the casing.
 - **Casing Open** – Trigger the rule if the casing of a connected external device, such as a junction box or cabinet (not included), is removed or opened. This can for example be used to send notifications of maintenance or unauthorized tampering.
 - **Fan** – Trigger the rule if the fan is malfunctioning. This can for example be used to send maintenance notifications.
 - **Heater** – Trigger the rule if the heater is malfunctioning. This can for example be used to send maintenance notifications.
 - **Video Signal** – Trigger the rule if video signal is lost.
 - **Network** – Triggers the action rule when the network connection is lost. Select **Yes** to trigger the action rule when the network connection is lost. Select **No** to trigger the action rule when the network connection is restored.
 - **Network** – Trigger the rule if network connection is lost or restored.
 - **Network** – Trigger the rule if network connection is lost or restored. This can for example be used to start recording to the SD card.
 - **Temperature** – Trigger the rule if the temperature falls outside or inside the operating range of the product. This can for example be used to send maintenance notifications.
 - **Peer Connection** – Triggers the action rule when the Axis product has established a connection with another door controller, if the network connection between the devices is lost, or if the pairing of door controllers has failed. This can for example be used to send a notification that a door controller has lost its network connection.
- **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 66*.
 - **Manual Trigger** – Triggers the action rule when the manual trigger is activated. It can be used by a client such as an access management system, through the VAPIX® application programming interface, to manually start or stop the action rule.
 - **Manual Trigger** – Trigger the rule using the **Manual Trigger** button in the Live View page. See *Controls on the Live View Page on page 14*. This can for example be used to validate actions during product installation and configuration.

AXIS M1143-L - User Manual

Events

- **Manual Trigger** – Trigger the rule using the **Manual Trigger** buttons in the Live View page. See *Manual Trigger* on page 15. This can for example be used to validate actions during product installation and configuration.
- **Virtual Inputs** – Triggers the action rule when one of the virtual inputs changes states. It can be used by a client such as an access management system, through the VAPIX® application programming interface, to trigger actions. Virtual inputs can, for example, be connected to buttons in the management system's user interface.
- **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**
 - **Autotracking** – Trigger the rule when autotracking starts or stops. See .
 - **Error** – Trigger the rule if the PTZ functionality is not working correctly. This can for example be used to send maintenance notifications.
 - **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.
 - **Ready** – Trigger the rule when the PTZ functionality is ready to be used. This can for example be used to steer the camera to a specific preset position when the product is started.
- **Storage**
 - **Available** – Trigger the rule when the storage device is unmounted or removed. This can for example be used to send maintenance notifications.
 - **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.
 - **Full** – Trigger the rule when the storage device is full. Under normal operation, the oldest recordings will be overwritten to prevent the storage device from becoming full.
 - **Locked** – Trigger the rule if the storage device is locked (write protected).
- **Schedule**
 - **Interval** – Triggers the action rule at the schedule's start time and remains active until the schedule's end time is reached.
 - **Pulse** – Triggers the action rule when a one-time event occurs. That is, an event that happens at a specific time and has no duration.
- **System**
 - **System Initializing** – Trigger the rule when the product is being started. This can for example be used to send a notification when the product restarts.
 - **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.
 - **System Ready** – Triggers the action rule when the system is in state ready. For example, the Axis product can detect the system state and send a notification when the system has started.

AXIS M1143-L - User Manual

Events

Select Yes to trigger the action rule when the product is in state ready. Note that the rule will only trigger when all necessary services, such as the event system, has started.

- Time
 - **Recurrence** – Triggers the action rule by monitoring the recurrences that you have created. You can use this trigger to initiate recurring actions such as sending notifications every hour. Select a recurrence pattern or create a new one. For more information about setting up a recurrence pattern, see *Set Up Recurrences on page 50*.
 - **Recurrence** – Trigger the rule periodically. See *Set Up Recurrences on page 50*. 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 50*.

Actions

Available actions include:

- **Activate Light** – Turn the built-in light on or off.
- **IR Illumination** – Activate or deactivate IR light.
- **Day/Night Vision Mode** – Set day mode (IR cut filter on) or night mode (IR cut filter off).
- **Defog Mode**– Set Defog Mode to On or Off. This action may be used to change between the modes automatically.
- **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 30*.
- **Play Audio Clip** – See .
- **PTZ Control**
 - **Autotracking** – Start autotracking. See .
 - **Preset Position** – Go to a preset position.
 - **Guard Tour** – Start a guard tour. See *Guard Tour on page 34*.
- **Record Video** – Record video to a selected storage.
- **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 Notifications** – 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.
- **Status LED** – The status LED can be set to flash for the duration of the action rule or for a set number of seconds. The status LED can be used during installation and configuration to visually validate if the trigger settings, for example the door open too long trigger, work correctly. To set the status LED flash color, select an **LED Color** from the drop-down list.
- **WDR Mode** – The WDR Mode or Lightfinder Mode can be turned on when the action rule is triggered. This action may be used to change between these modes automatically.
- **WDR Mode** – The WDR Mode can be turned on or off when the action rule is triggered.

Events

Add Recipients

The product can send messages to notify administrators about events and alarms. But before the product can send notification messages, you must define one or more recipients. For information about available options, see *Recipient Types on page 48*.

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 48*.

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**.
1. Go to **Setup > Additional Controller Configuration > 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:

- HTTP
- HTTPS
- Email
- TCP

The following recipients are available:

Recipient	Use with action	Notes
Email	Send Images Send Notification Send Video Clip	An email recipient can contain multiple email addresses. For more information about email recipients, see <i>Set Up Email Recipients on page 49</i>
FTP	Send Images Send Video Clip	

AXIS M1143-L - User Manual

Events

SFTP	Send Images Send Video Clip	Encrypted file transfer using SSH File Transport Protocol (SFTP). SFTP is a more secure method than FTP but file transfer might be slower, especially for large files such as high resolution video. Specify login information for the SFTP server and the server's public key MD5 fingerprint (32 hexadecimal digits). The SFTP recipient supports SFTP servers using SSH-2 with RSA and DSA host key types. RSA is the preferred method. To use DSA, disable the RSA key on the SFTP server.
HTTP	Send Images Send Notification Send Video Clip	
HTTPS	Send Images Send Notification Send Video Clip	Encrypted file transfer using HyperText Transfer Protocol Secure (HTTPS). Specify login information for the HTTPS server and validate the server's certificate. If there is a proxy between the Axis product and the HTTPS server, also specify the proxy settings.
Network Share	Send Images Send Video Clip	A network share can also be used as a storage device for recorded video. Go System Options > Storage to configure a network share before setting up a continuous recording or an action rule to record video. For more information about storage devices, see <i>Storage on page 64</i> .
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 57*.

Events

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.

Schedules can be used as action rule triggers or as additional conditions. 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**.
1. Go to **Setup > Additional Controller Configuration > 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**.
1. Go to **Setup > Additional Controller Configuration > Events > Recurrences** and click **Add**.
2. Enter a descriptive name and recurrence pattern.
3. Click **OK**.

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

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

Recordings

Recordings

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

The Axis product can be configured to record video continuously or as a result of a triggered or scheduled event:

- To start a continuous recording, see .
- To start a continuous recording, see *page 52*.
- To set up action rules, see *page 42*.
- To access recordings, see .
- To access recordings, see *Find Recordings on page 51*.
- To play recordings, see *Play Recording on page 52*.
- To export a recording as a video clip, see *Export Video Clip on page 52*.
- To set up triggered and scheduled events, see *Events on page 42*.
- To access event recordings, see .
- To configure camera controlled storage, see *Storage on page 64*.

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.

Recordings made to the network share can be accessed from the **Recordings > List** page. The page lists all recordings 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 58*.

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 52*.

AXIS M1143-L - User Manual

Recordings

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 52*.

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.

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

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 51*.
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.

Recordings on the 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 51*.
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 64*. 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.

AXIS M1143-L - User Manual

Recordings

You can start a continuous recording for any of the view modes. See .

To start a continuous recording, follow these steps:

1. Go to **Recordings > Continuous**.
2. Select **Enabled**.
3. Select the type of storage device from the **Storage** list.
4. Select a **Stream profile** to use for continuous recordings.
5. 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.
6. Click **Save** to save and start the recording.

AXIS M1143-L - User Manual

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.

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.

User access control is enabled by default and can be configured under **Setup > Additional Controller Configuration > System Options > Security > Users**. An administrator can set up other users by giving them user names and passwords.

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

Viewer – Access to the Live View page

Operator – Access to the Live View page and to all settings except System Options

Administrator – Unrestricted access to all settings; can add, modify and remove other users.

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

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

HTTPS

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

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

The Axis product can be configured to require HTTPS when administrators log in.

AXIS M1143-L - User Manual

System Options

To use HTTPS, an HTTPS certificate must first be installed. Go to **System Options > Security > CertificatesSetup > Additional Controller Configuration > System Options > Security > Certificates** to install and manage certificates. See *Certificates on page 57*.

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.
-
1. Go to **Setup > Additional Controller Configuration > 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, enter `https://` or `http://` in the address field in a browser.

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 > CertificatesSetup > Additional Controller Configuration > System Options > Security > Certificates**. See *Certificates on page 57*. 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**.
-
1. Go to **Setup > Additional Controller Configuration > 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**.

System Options

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 58.

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.

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

Server/Client certificates – To authenticate the Axis product.

CA certificates – To authenticate peer certificates.

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 > CertificatesSetup > Additional Controller Configuration > 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 > CertificatesSetup > Additional Controller Configuration > 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 > CertificatesSetup > Additional Controller Configuration > System Options > Security > Certificates**.
2. Click **Install certificate** and upload the certificate.

System Options

Date & Time

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


Current Server Time displays the current date and time (24h clock).

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

- **Synchronize with computer time** – Sets date and time according to the computer's clock. With this option, date and time are set once and will not be updated automatically.
- **Synchronize with NTP Server** – Obtains date and time from an NTP server. With this option, date and time settings are updated continuously. For information on NTP settings, see *NTP Configuration on page 60*.

If using a host name for the NTP server, a DNS server must be configured. See *DNS Configuration on page 60*.
- **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 Video** and select **Include date** and **Include time**.

Network

Basic TCP/IP Settings

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

The Axis product supports IP version 4.

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 Setup > Additional Controller Configuration > 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 69*) 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.

AXIS M1143-L - User Manual

System Options

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 59.

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 > BasicSetup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic** and clear the option **Enable ARP/Ping** setting of IP address.

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

Assign IP Address Using ARP/Ping

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

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

Linux/Unix syntax

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

Linux/Unix example

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

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

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

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

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

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

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

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

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 M1143-L - User Manual

System Options

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

AVHS used in conjunction with an AVHS service, provides easy and secure Internet access to controller management and logs 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 > BasicSetup > Additional Controller Configuration > 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.

Note

AVHS support is dependent on the availability of subscriptions from service providers.

AXIS Internet Dynamic DNS Service

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

To register the Axis product with AXIS Internet Dynamic DNS Service, go to **System Options > Network > TCP/IP > BasicSetup > Additional Controller Configuration > 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 > AdvancedSetup > Additional Controller Configuration > 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 > AdvancedSetup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**.

System Options

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 > AdvancedSetup > Additional Controller Configuration > 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 > AdvancedSetup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**.

HTTP

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

HTTPS

The HTTPS port used by the Axis product can be changed under **Setup > Additional Controller Configuration > 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.

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 **Setup > Additional Controller Configuration > System Options > Security > HTTPS**. For more information, see *HTTPS on page 55*.

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

To enable HTTPS, go to **System Options > Security > HTTPS**. For more information, see *HTTPS on page 55*.

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 > AdvancedSetup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**.

AXIS M1143-L - User Manual

System Options

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 > UPnPSetup > Additional Controller Configuration > 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 > AdvancedSetup > Additional Controller Configuration > 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.

The RTSP server running in the Axis product allows a connecting client to start an event stream. The RTSP port number can be changed under **Setup > Additional Controller Configuration > 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.

Note

Event streams will not be available if the RTSP server is disabled.

SOCKS

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

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

System Options

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.

The QoS settings are configured under **Setup > Additional Controller Configuration > System Options > Network > QoS**. Using DSCP (Differentiated Services Codepoint) values, the Axis product can mark event/alarm traffic and management 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 > SNMPSetup > Additional Controller Configuration > System Options > Network > SNMP** page.

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

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

Note

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

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

The following traps are available:

- Cold start
- Warm start
- Link up
- Authentication failed

Note

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

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

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

To use SNMP v3, HTTPS must be enabled, see *HTTPS on page 55*. To enable SNMP v3, check the box and provide the initial user password.

Note

The initial password can only be set once. If the password is lost, the Axis product must be reset to factory default, see *Reset to Factory Default Settings on page 69*.

AXIS M1143-L - User Manual

System Options

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 > UPnPSetup > Additional Controller Configuration > 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.

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

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

Select **Always Multicast Video** to start multicast streaming without opening an RTSP session.

Bonjour

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

Bonjour can be disabled under **System Options > Network > BonjourSetup > Additional Controller Configuration > System Options > Network > Bonjour**.

Storage

SD Card

NOTICE

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

Note

For SD card recommendations see www.axis.com

Important

To access the SD card, the top cover must be removed. After remounting the alignment of the lens may differ slightly and the PTZ mechanics should be recalibrated. Go to **System Options > Maintenance** and click **Calibrate PTZ**. For more information, see .

Note

Do not insert or eject the SD card while the product is running. The product will lose its connection to the wireless network. Reboot the product to reestablish the wireless connection after the card has been inserted or ejected.

The Axis product supports SD cards with up to 64 GB of storage. For best recording performance, use an SDHC or SDXC card with speed class 10.

The Axis product supports SD cards with up to 64 GB of storage. For best recording performance, use ultra-high speed SD cards (SDHC UHS-I or SDXC UHS-I). In temperatures below – 25° C use industrial grade SD card.

Supports microSD cards with up to 64 GB of storage. For best recording performance, use a microSDHC or microSDXC card with speed class 10.

AXIS M1143-L - User Manual

System Options

The Axis product supports microSD cards with up to 64 GB of storage. For best recording performance, use ultra-high speed microSD cards (microSDHC UHS-I or microSDXC UHS-I).

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**.

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.

AXIS M1143-L - User Manual

System Options

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.

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/cam_companion_software/supported.htm

Note

For NAS recommendations see www.axis.com

To add a network share:

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


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

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

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

Ports & Devices

I/O Ports

Configure the input and output ports supported by your Axis product from **System Options > Ports & Devices > I/O Ports**. Ports can be given descriptive names, and their Normal state can be configured. For more information about this see the online help . For information regarding how to connect the input and output on this product see .

The auxiliary connector on the Axis product provides two configurable input and output ports for connection of external devices. For information about how to connect external devices, see the Installation Guide, available on www.axis.com

The Axis product provides one input port and one output port for connection of external devices. For information about how to connect external devices, see *Connectors on page 79*.

The Axis product provides two configurable input and output ports for connection of external devices. For information about how to connect external devices, see *Connectors on page 79*.

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 79*.

AXIS M1143-L - User Manual

System Options

The Axis product provides two configurable input and output ports for connection of external devices. A multi-connector cable (available from Axis) is required when connecting external devices, see .

The Axis product provides four configurable input and output ports for connection of external devices. A multi-connector cable (available from Axis) is required when connecting external devices, see .

The media converter switch provides two configurable input and output ports for connection of external devices. One port is dedicated for the I/O signals between the media converter switch, the supplied multi-connector cable and the camera. For more information about the multi-connector cable, see .

The I/O ports are configured under **System Options > Ports & Devices > I/O Ports**. The ports can be given descriptive names and their **Normal states** can be configured as **Open circuit** or **Grounded circuit**.

The I/O ports are configured under **System Options > Ports & Devices > I/O Ports**. Select the port direction (**Input** or **Output**). The ports can be given descriptive names and their **Normal states** can be configured as **Open circuit** or **Grounded circuit**.

The I/O ports are configured under **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports**. Select the port direction (**Input** or **Output**). The ports can be given descriptive names and their **Normal states** can be configured as **Open circuit** or **Grounded circuit**.

Note

There are four I/O ports for each group of video input connectors.

Port Status

The list on the **Events > Port Status** page shows the status of the product's input and output ports. Inputs and outputs are configured from the **System Options > Ports & Devices** page which requires administrator rights.

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

Note

A multi-connector cable (available from Axis) is required when connecting I/O devices to the Axis product. See .

Maintenance

The Axis product provides several maintenance functions. These are available under **System Options > MaintenanceSetup > Additional Controller Configuration > 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
- the wireless settings
- the focus position

AXIS M1143-L - User Manual

System Options

- uploaded applications are kept but must be restarted

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 69*.

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

To calibrate the PTZ functionality, click **Calibrate PTZ**. See .

To reset the optics, click **Calibrate** under **System Options > Maintenance > Optics**. This may be necessary in situations where the optics has lost its calibration during transport or has been exposed to extreme vibrations. If necessary configure focus and zoom again (see *Basic Setup on page 22*).

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 71*.

Support

Support Overview

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

See also *Troubleshooting on page 71*.

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.

To get an overview of the Axis product's status and settings, go to **Setup > Additional Controller Configuration > System Options > Support > System Overview**. Information that can be found here includes firmware version, IP address, network and security settings, event settings, and recent log items. Many of the captions are links to the proper Setup page.

Logs & Reports

The **System Options > Support > Logs & Reports**Setup > Additional Controller Configuration > 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.

System Options

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

Advanced

Scripting

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

NOTICE

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

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

To open the Script Editor, go to **System Options > Advanced > ScriptingSetup > Additional Controller Configuration > System Options > Advanced > Scripting**. If a script causes problems, reset the product to its factory default settings, see *page 69*.

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 UploadSetup > Additional Controller Configuration > 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 ConfigSetup > Additional Controller Configuration > 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

The installation and management software tools are available on the CD supplied with the product and 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 about 15–30 seconds until the status LED indicator flashes amber.

AXIS M1143-L - User Manual

System Options

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.
6. Refocus the product.
1. Press and hold the control button and the restart button at the same time.
2. Release the restart button but continue to hold down the control button for about 15–30 seconds until the status LED indicator flashes amber.
3. 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
4. Using the installation and management software tools, assign an IP address, set the password and access the video stream
5. Release the restart button and hold the control button.
6. Keep the control button pressed until the power LED indicator turns green and the 6 status LED indicators turn amber (this may take up to 15 seconds).
7. Release the control button. When the status LED indicators display green (which can take up to 1 minute) the process is complete and the unit has been reset.
8. Using the installation and management software tools, assign the IP addresses, set the password and access the video stream.

Note

To reset a single channel to the original factory default settings, use the button provided in that product's webpage.

1. Press and hold the control button and the power button for about 15–30 seconds until the status LED indicator flashes amber. See *Hardware Overview on page 7*.
2. Release the control button but continue to hold down the power button until the status LED indicator turns green.
3. Release the power button and assemble the product.
4. The process is now complete. 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.
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 about 25 seconds until the status LED indicator turns amber for the second time.
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 product.

It is also possible to reset parameters to factory default via the web interface. Go to **Setup > System Options > MaintenanceSetup > Additional Controller Configuration > Setup > System Options > Maintenance**.

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** **Setup > Additional Controller Configuration > Basic Setup** and in **Setup > About** **Setup > Additional Controller Configuration > 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, always wait 10 minutes even if you suspect the upgrade has failed.
- After the upgrade process has completed, the product will restart automatically. If restarting the product manually after the upgrade, always wait 5 minutes even if you suspect the upgrade has failed.
- Because the database of users, groups, credentials, and other data will be updating after a firmware upgrade, the first start-up could take a few minutes to complete. The time required is dependent on the amount of data.
- 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. Save the firmware file to your computer. The latest version of the firmware is available free of charge from Axis website 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. Click **Upgrade**.
4. Wait approximately 10 minutes while the product is being upgraded and restarted. Then access the product.

To upgrade the product's firmware:

1. Save the firmware file to your computer. The latest version of the firmware is available free of charge from Axis website at www.axis.com/techsup
2. Go to **Setup > Additional Controller Configuration > System Options > Maintenance** in the product's webpages.
3. Under **Upgrade Server**, click **Browse** and locate the file on your computer. Click **Upgrade**.
4. Wait approximately 5 minutes while the product is being upgraded and restarted. Then clear the web browser's cache.
5. 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 becomes 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.

AXIS M1143-L - User Manual

Troubleshooting

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

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

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

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

2. If the product does not reply in 30 seconds, restart it and wait for a reply. Press CTRL+C to stop Ping.
3. Open a browser and type in the product's IP address. In the page that opens, use the **Browse** button to select the upgrade file to use. Then click **Load** to restart the upgrade process.
4. After the upgrade is complete (1–10 minutes), the product automatically restarts and shows a steady green on the Status indicator.
5. Reinstall the product, referring to the Installation Guide.

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

Note

The emergency recovery procedure only works on the wired interface.

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 on page 59</i> .
	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 Installation Guide on www.axis.com .
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): <ul style="list-style-type: none">• 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 on page 69</i> .
---------------	--

AXIS M1143-L - User Manual

Troubleshooting

The IP address has been changed by DHCP	<p>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).</p> <p>IP addresses obtained from a DHCP server are dynamic and may change. If the IP address has been changed, use AXIS IP Utility 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).</p> <p>If required, a static IP address can be assigned manually. For instructions, see the Installation and Management Software CD or the document <i>Assign an IP Address and Access the Video Stream</i> on Axis Support web at www.axis.com/techsup.</p> <p>If required, a static IP address can be assigned manually. For instructions, see Installation Guide on www.axis.com/techsup.</p>
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 58.
PTZ Network Camera Connection Failed	<p>Under System Options > PTZ Network Camera > Connection, check the following:</p> <ul style="list-style-type: none">• That the user logged onto the PTZ network camera has PTZ controls enabled• That the IP address and Ports are correct
PTZ Network Camera Authorization Error	Make sure that the password for the user logged onto the PTZ network camera has not been changed.

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 61. The router must support UPnP™.
Firewall protection	Check the Internet firewall with your network administrator.
Default routers required	<p>Check if you need to configure the router settings from System Options > Network > TCP/IP > Basic.</p> <p>Check if you need to configure the router settings from Setup > Network Settings or Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic.</p>

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	<p>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)</i> on page 20.</p> <p>In the AMC Control Panel, select the H.264 tab and click Set to default H.264 decoder.</p> <p>Check that RTSP is enabled under System Options > Network > TCP/IP > Advanced.</p>
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	<p>Check with your network administrator that the multicast addresses used by the Axis product are valid for your network.</p> <p>Check with your network administrator to see if there is a firewall preventing viewing.</p>

AXIS M1143-L - User Manual

Troubleshooting

Installation of additional ActiveX component restricted or prohibited	Configure the Axis product to use a Java applet for updating video images in your browser. Go to Setup > Live View Config and select Java applet under Default viewer .
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	<p>See <i>Performance Considerations on page 81</i>.</p> <p>Reduce the number of applications running on the client computer.</p> <p>Limit the number of simultaneous viewers.</p> <p>Check with the network administrator that there is enough bandwidth available.</p> <p>Check in the AMC Control Panel (H.264 tag) that video processing is NOT set to Decode only key frames.</p> <p>Lower the image resolution.</p> <p>Set a Capture Mode that prioritizes frame rate. Changing the capture mode to prioritize frame rate will lower the maximum resolution. See .</p> <p>The maximum frames per second is dependent on the utility frequency (60/50 Hz) of the Axis product. See <i>Technical Specifications on page 77</i>.</p>

Status and Network indicator LEDs are flashing red rapidly

Hardware failure	Contact your Axis reseller.
------------------	-----------------------------

Video and image problems, general

Image unsatisfactory	Check the video stream and camera settings under Setup > Video > Video StreamSetup > Video & Audio > Video Stream and Setup > Video > Camera SettingsSetup > Video & Audio > Camera Settings .
Disturbed focus	Set the focus manually by turning the focus ring. See <i>Hardware Overview on page 7</i>

PTZ problems

Incorrect mapping between Overview mode and Normal mode	If the camera view does not move to the correct position in Normal mode when clicking an object in Overview mode, the PTZ calibration is inaccurate and should be redone. Go to System Options > Maintenance . See .
---	--

Overlay image is not displayed

No overlay image in Overview mode	The overlay image is only displayed in Normal mode.
-----------------------------------	---

Privacy mask is not displayed

No privacy mask in Overview mode	Privacy masks are only displayed in Normal mode.
----------------------------------	--

Motion Detection triggers unexpectedly

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

AXIS M1143-L - User Manual

Troubleshooting

Motion Detection triggers unexpectedly

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

No audio

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

Poor audio quality

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

Storage and disk management problems

Storage disruption	<p>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.</p> <p>For information on how to set up a storage disruption alarm, see <i>Events on page 42</i>.</p>
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.

PIR Sensor sensitivity

The PIR sensor rarely triggers or not at all	Since IR light is blocked by glass, the PIR sensor will not work if the product is placed behind a window or similar.
--	---

Condensation in dome

Blurred image	Activate fan and heater to remove possible moisture from dome
---------------	---

Focus, zoom, and fan

Remote focus and zoom do not work	During startup in a cold environment, function in these mechanical parts is suspended until they are sufficiently heated.
Fan cannot be activated	During startup in a cold environment, function in this mechanical part is suspended until it is sufficiently heated.

AXIS M1143-L - User Manual

Troubleshooting

Media converter switch

Media converter switch
freezes after hotswapping

The media converter switch does not support hotswapping. Disconnect power from the switch before swapping cameras. Restart the switch after a failed attempt to hotswap.

AXIS M1143-L - User Manual

Technical Specifications

Technical Specifications

Function/group	Item	Specifications
Camera	Models	AXIS M1143-L
	Image sensor	1/4" progressive scan RGB CMOS
	Lens	Varifocal, DC-iris, manual focus and zoom 6mm: 2.5-6 mm, F1.4, Horizontal angle of view*: 72°-34° Vertical angle of view: 54°-24° Diagonal angle of view: 88° -40° *SVGA Resolution
	Minimum illumination	0.6 lux, F1.4 0 lux with IR illumination on
	Shutter time	1/8000 to 1/6 s
	Pan/Tilt/Zoom	Digital PTZ, preset positions
Video	Video compression	H.264 (MPEG-4 Part 10/AVC), Motion JPEG
	Resolutions	800 x 600 to 352 x 240
	Frame rate	H.264: 30 fps in all resolutions Motion JPEG: 30 fps in all resolutions
	Video streaming	Multiple, individually configurable streams in H.264 and Motion JPEG Controllable frame rate and bandwidth VBR/CBR H.264
	Image settings	Compression, color, brightness, sharpness, contrast, white balance, exposure control Rotation: 0°, 90°, 180°, 270° including Corridor Format Text and image overlay, privacy mask and mirroring of images
Network	Security	Password protection, IP address filtering, HTTPS encryption, digest authentication, user access log, centralized certificate management.
	Supported protocols	IPv4/v6, HTTP, HTTPS, SSL/TLS*, QoS Layer 3 DiffServ, FTP, SMTP, Bonjour, UPnP, SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, CIFS/SMB, SSH. *This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.
System Integration	Application Programming Interface	Open API for software integration, including VAPIX® and AXIS Camera Application Platform; specifications at www.axis.com AXIS Video Hosting System (AVHS) with One-Click Camera Connection. ONVIF Profile S; specification available at www.onvif.org AXIS Media Control SDK (available at www.axis.com), event trigger data in video stream Quality of Service (QoS) layer 3, DiffServ Model Embedded Linux operating system
	Intelligent video	Video motion detection, active tampering alarm Support for AXIS Camera Application Platform enabling installation of additional applications
	Event triggers	Detectors: Day/Night Mode, Detection, Live Stream Accessed, Tampering, Motion Detection Hardware: Network, Temperature Input Signal: Digital Input Port, Manual Trigger, Virtual Inputs Storage: Disruption, Recording System: System Ready Time: Recurrence, Use Schedule

AXIS M1143-L - User Manual

Technical Specifications

Function/group	Item	Specifications
	Events actions	File upload via FTP, HTTP and email, Notification via email, HTTP and TCP; pre- and post-alarm video buffering, Activation of IR illumination, External output activation, video recording to local storage
	Video buffer	25 MB pre- and post alarm
	Video access from web browser	Camera live view Video recording to file (ASF) Customizable HTML pages Windows Vista, XP, Windows 7, Server 2003 and Server 2008 DirectX 9c or higher For other operating systems and browsers see www.axis.com/support
	Installation, management and maintenance	AXIS Camera Management tool and web-based configuration Configuration of backup and restore Firmware upgrades over HTTP or FTP, firmware available on www.axis.com
General	Casing	Aluminium and PC/ABS Color: White NCS S 1002-B
	Memory	256 MB RAM, 128 MB Flash Battery backed-up real-time clock
	Power	Power over Ethernet IEEE 802.3af Class 2 (max. 6.49 W)
	IR illumination	Highly efficient IR LEDs with adjustable intensity and angle of illumination. Range of reach up to 15 m (50 ft).
	Connectors	RJ-45 10BASE-T/100BASE-TX 1 alarm input and 1 output
	Edge storage	microSD/microSDHC/microSDXC slot (card not included) Support for recording to dedicated network-attached storage (NAS) For SD card and NAS recommendations see www.axis.com
	Operating conditions	0 °C to 50 °C (32 °F to 122 °F), humidity 20–80% RH (non-condensing)
	Storage temperature	–20 to 60 °C (–4 to 140 °F)
	Approvals	EN 55022: 2006+A1 Class B EN 61000-6-1, EN 61000-6-2, EN 61000-3-2, EN 61000-3-3, EN 55024 EN 60950-1+A11 FCC Part 15, Subpart B, Class B demonstrated by compliance with EN 55022 (CISPR 22) VCCI-2008, Class B, ITE C-tick AS/NZS CISPR 22, demonstrated by compliance with EN 55022 (CISPR 22) ICES-003 Canadian ICES-003, Class B digital, demonstrated by compliance with EN 55022 (CISPR 22) KN22: KN24 UL: cUL, usUL UL-60950-1, IR: SS-EN-62471
	Dimensions	46 x 75 x 115 mm (1.8" x 3.0" x 4.5")
	Weight	250g (0.21 lb.)
	Included accessories	Installation Guide, Windows decoder 1-user license, Stand, Lever tool.
	Video management software (not included)	AXIS Camera Companion (included), AXIS Camera Station and video management software from Axis' Application Development Partners (not included). For more information, see www.axis.com/vms
	Languages	English, German, French, Spanish, Italian, Russian, Simplified Chinese, Japanese, Korean, Portuguese
	Warranty	Axis 1-year warranty and AXIS Extended Warranty option, see www.axis.com/warranty

Technical Specifications

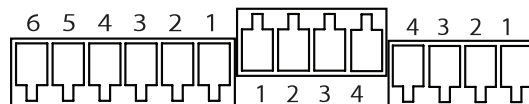
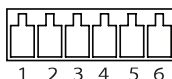
Connectors

I/O Connector

6-pin configurable terminal block for:

4-pin terminal block for:

- Auxiliary power (DC output)
- Digital Input
- Digital Output
- 0 V DC (-)



Note

The I/O connector is connected to the housing (fan/heater) on delivery. In the case of a fan or heater error, an input signal will be triggered in the camera. Set up an action rule in the camera to configure which action the signal shall trigger. For information about events and action rules, see *Events on page 42*.

The I/O connector is connected to the housing (fan/heater) on delivery. In the case of a fan or heater error, an input signal will be triggered in the camera. Set up an action rule in the camera to configure which action the signal shall trigger. For information about events and action rules, see the User Manual available on www.axis.com

Function	Pin	Notes	Specifications
0 V DC (-)	1		0 V DC
DC output	2	Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	3.3 V DC Max load = 250 mA
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

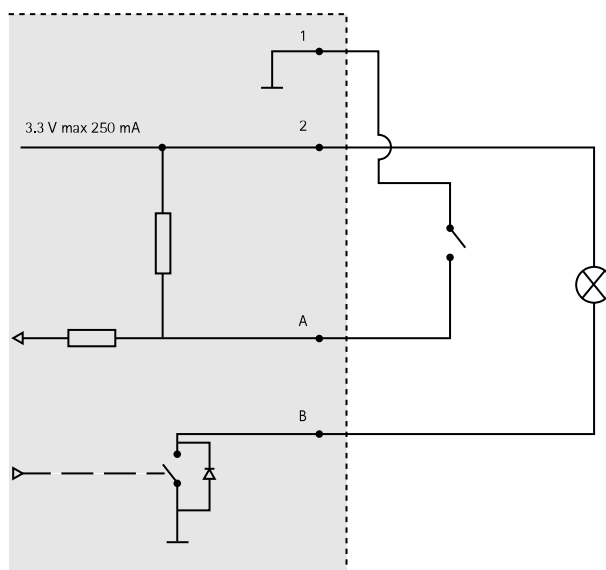
Function	Pin	Notes	Specifications
0 V DC (-)	1		0 V DC
DC output	2	Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	3.3 V DC Max load = 250 mA
Configurable (Input or Output)	3–4	Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	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

Function	Pin	Notes	Specifications
0 V DC (-)	1		0 V DC
DC output	2	Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	3.3 V DC Max load = 50 mA

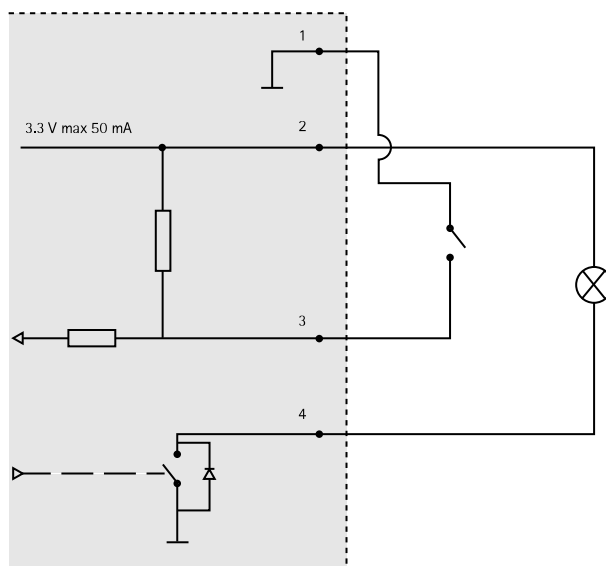
AXIS M1143-L - User Manual

Technical Specifications

Digital Input	3	Connect to pin 1 to activate, or leave floating (unconnected) to deactivate	0 to max 40 V DC
Digital Output	4	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



A I/O configured as input
B I/O configured as output



SD Card Slot

Supports SD cards with up to 64 GB of storage. For best recording performance, use an SDHC or SDXC card with speed class 10.

AXIS M1143-L - User Manual

Technical Specifications

The Axis product supports SD cards with up to 64 GB of storage. For best recording performance, use ultra-high speed SD cards (SDHC UHS-I or SDXC UHS-I).

Supports microSD cards with up to 64 GB of storage. For best recording performance, use a microSDHC or microSDXC card with speed class 10.

The Axis product supports microSD cards with up to 64 GB of storage. For best recording performance, use ultra-high speed microSD cards (microSDHC UHS-I or microSDXC UHS-I).

Supports SD cards with up to 64 GB of storage. For best performance, use an SDHC or SDXC card with speed class 10.

Supports microSD cards with up to 64 GB of storage. For best performance, use a microSDHC or microSDXC card with speed class 10.

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.
- Heavy network utilization due to poor infrastructure. Bandwidth affected.
- Viewing on poorly performing client computers lowers perceived performance. Frame rate affected.
- Running multiple ACAP Applications simultaneously may affect performance.
- If the product includes several camera units, running applications on multiple cameras may affect the frame rate.

