

# USER MANUAL

## AXIS M1004-W Network Camera



## About this Document

This manual is intended for administrators and users of the AXIS M1004-W Fixed Dome Network Camera, and is applicable to firmware 5.4 and later. It includes instructions for using and managing the product on your network. Previous experience of networking will be of use when using this product. Some knowledge of UNIX or Linux-based systems may also be beneficial, for developing shell scripts and applications. Later versions of this document will be posted to the Axis website, as required. See also the product's online help, available via the web-based interface.

## Legal Considerations

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

This product includes 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 <http://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 <http://www.opensource.apple.com/aps/>). The source code is available from <http://developer.apple.com/darwin/projects/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.

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

## Regulatory Information

### Europe

**CE 1177** 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.

- Radio and Telecommunications Terminal Equipment (R & TTE) Directive 1999/5/EC. See *Radio Transmission*, 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 3.

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

## Electromagnetic Compatibility (EMC)

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

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

### USA

This 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.

### Canada

This Class B digital apparatus complies with Canadian ICES-003.

### Europe

This digital equipment fulfills the requirements for RF emission according to the Class B limit of EN 55022.

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

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

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

### Australia/New Zealand

This digital equipment fulfills the requirements for RF emission according to the Class B limit of AS/NZS CISPR 22.

### 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。

### Korea

이 기기는 가정용(B급) 전자파적합기기로서 주로 가정에서 사용하는 것을 목적으로 하며, 모든 지역에서 사용할 수 있습니다.

## Radio Transmission

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

### USA

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesirable operation.

This product complies with FCC radiation exposure limits for an uncontrolled environment. Avoid operating this product at a distance less than 20 cm (7.9 in.) from the user.

## Canada

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

This product complies with IC radiation exposure limits for an uncontrolled environment. Avoid operating this product at a distance less than 20 cm (7.9 in.) from the user.

## Brazil

Este produto está homologado pela ANATEL, de acordo com os procedimentos regulamentados pela Resolução 242/2000 e atende aos requisitos técnicos aplicados.

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

Para maiores informações, consulte o site da ANATEL [www.anatel.gov.br](http://www.anatel.gov.br)

## Europe

Hereby, Axis Communications AB declares that this product is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

A copy of the original declaration of conformity may be obtained from Axis Communications AB, Emdalavägen 14, SE-223 69 Lund.

## FR

Par la présente Axis Communications AB déclare que l'appareil ce produit est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.

## DE

Hiermit erklärt Axis Communications AB, dass sich dieses Produkt in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet.

## IT

Con la presente Axis Communications AB dichiara che questo prodotto è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.

## ES

Por medio de la presente Axis Communications AB declara que el este producto cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.

## FI

Axis Communications AB vakuuttaa täten että tämä tuote tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

## NL

Hierbij verklaart Axis Communications AB dat het toestel in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.

## SV

Härmed intygar Axis Communications AB att denna produkt står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

## DA

Undertegnede Axis Communications AB erklærer herved, at følgende udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.

## PT

Axis Communications AB declara que este produto está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.

## EL

ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Axis Communications AB ΔΗΛΩΝΕΙ ΟΤΙ αυτό το προϊόν ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.

## Australia/New Zealand

This digital equipment fulfills the requirements of the Radio Communications Standard AS/NZS 4771.

## Korea

제품 사양  
주파수: 802.11b/g/n (HT20), 2412~2472 MHz

온도: 0 ~ +40 °C

전원: DC 5 V, 1.5 A

적합성 평가 표시

적합성 평가를 받은 자의 상호: Axis Communications AB.

기자재의 명칭 (모델명): 무선데이터통신시스템용 무선기기 (AXIS M1004-W)

제조연월: 별도 표시

제조사 / 제조국가제조연월: 별도 표시:

Axis Communications AB/Sweden

## A/S정보

Axis Communications AB 한국지사

주소: 서울특별시 금천구 가산동 685번지 가산 Digital Empire 1012호

TEL: 82-2-780-9636

FAX: 82-2-6280-9636

## Japan

This product complies with Technical Regulations Conformity Certification of Specified Radio Equipment.

## Taiwan

【低功率警語】(主要針對BT/WIFI) BT/Wi-Fi Statement第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

## Safety

This product complies with IEC/EN/UL 60950-1, Safety of Information Technology Equipment.

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

## 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).

## 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/](http://www.axis.com/techsup/)

**Learn More!**

Visit Axis learning center [www.axis.com/academy/](http://www.axis.com/academy/) for useful trainings, webinars, tutorials and guides.

# AXIS M1004–W Network Camera

## Table of Contents

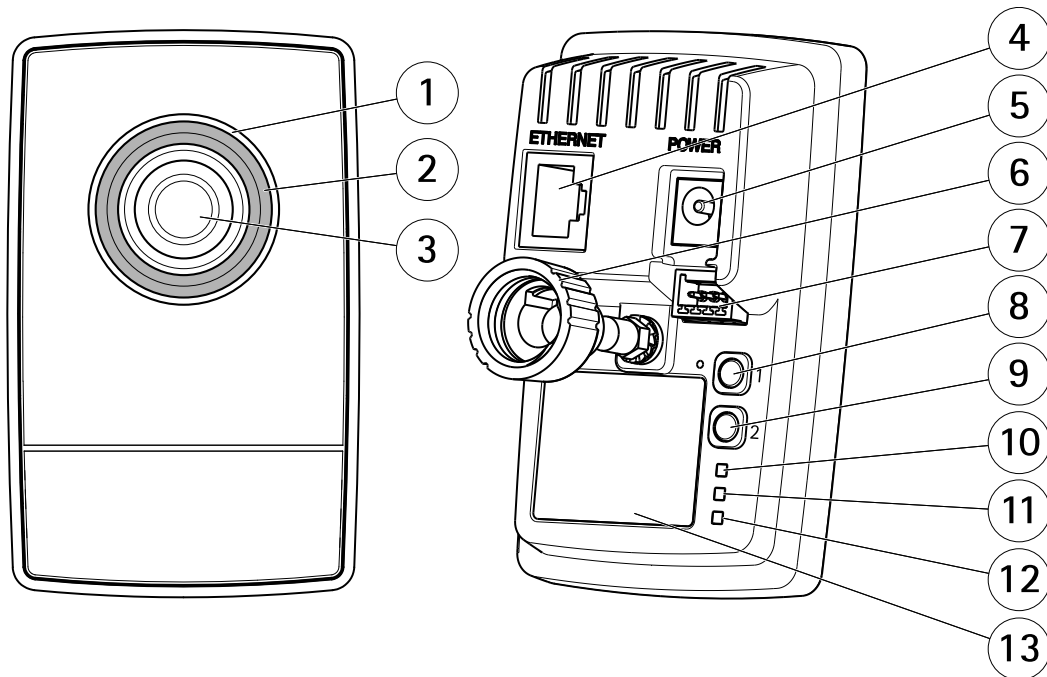
---

<b>Hardware Overview</b>	6
Connectors	6
LED Indicators	7
<b>Accessing the Product</b>	8
Access from a Browser	8
Access from the Internet	9
Set the Root Password	9
The Live View Page	10
<b>Media Streams</b>	13
How to Stream H.264	13
MJPEG	13
AXIS Media Control (AMC)	13
Alternative Methods of Accessing the Video Stream	14
<b>Setting Up the Product</b>	16
Basic Setup	16
Video	17
Video Stream	17
Stream Profiles	18
Camera Settings	19
View Area	19
Overlay	20
Privacy Mask	21
<b>Live View Config</b>	22
<b>PTZ (Pan Tilt Zoom)</b>	25
Preset Positions	25
Guard Tour	25
Advanced	26
<b>Detectors</b>	27
Camera Tampering	27
Motion Detection	27
<b>Applications</b>	30
<b>Events</b>	31
Setting Up an Action Rule	32
Recipients	32
Schedules	33
Recurrences	33
<b>Recordings</b>	35
Recording List	35
Continuous Recording	35
<b>System Options</b>	36
Security	36
Date & Time	38
Network	38
Storage	47
Ports & Devices	48
Maintenance	48
Support	48
Advanced	49
Reset to Factory Default Settings	50
<b>Troubleshooting</b>	51
Checking the Firmware	51
Upgrading the Firmware	51
Symptoms, Possible Causes and Remedial Actions	52
Problem Retrieving Additional Video Streams	55
<b>Technical Specifications</b>	56
Connectors	58
Performance Considerations	59

# AXIS M1004-W Network Camera

## Hardware Overview

### Hardware Overview



- 1 Status LED indicator
- 2 Focus ring
- 3 Lens
- 4 Network connector (RJ45)
- 5 Power connector
- 6 Lock ring
- 7 I/O terminal connector
- 8 Control button
- 9 WLAN pairing button
- 10 Power LED indicator
- 11 Network LED indicator
- 12 Wireless LED indicator
- 13 Part number (P/N) & Serial number (S/N)

The Axis product is equipped with a lens with manual focus. It is delivered with the lens prefocused and manual focusing is usually not required.

#### Note

Only change the focus if required, for example if the image is blurry.

## Connectors

For technical specifications, see [page 56](#).

**Network connector** – RJ-45 Ethernet connector. Supports Power over Ethernet (PoE).

# AXIS M1004–W Network Camera

## Hardware Overview

### NOTICE

The product shall be connected using a shielded network cable (STP). All cables connecting the product to the network switch shall be shielded (STP) and intended for their specific use. Make sure that the network switch is properly grounded. See for regulatory requirements.

**Control button** – The control button is used for:

- Connecting to an AXIS Video Hosting System service. See *page 40*. To connect, press and hold the button for about 1 second until the Status LED flashes green.
- Connecting to AXIS Internet Dynamic DNS Service. See *page 40*. To connect, press and hold the button for about 3 seconds.
- Resetting the product to factory default settings. See *page 50*.

**WLAN pairing button** – For connecting to an access point through push button configuration (PBC).

**I/O terminal connector** – Use in applications for e.g. motion detection, event triggering, time lapse recording and alarm notifications. In addition to an auxiliary power and a GND pin, the I/O terminal 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**).

## LED Indicators

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.
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 during wireless network pairing. Flashes for wireless network activity.

### 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**.

# AXIS M1004–W Network Camera

## Accessing the Product

---

### Accessing 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 56*. To view streaming video in Internet Explorer, allow installation of AXIS Media Control (AMC) when prompted.

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

#### Note

- QuickTime™ is also supported for viewing H.264 streams.
- 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 (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](http://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 9*.
4. The product's Live View page appears in your browser.

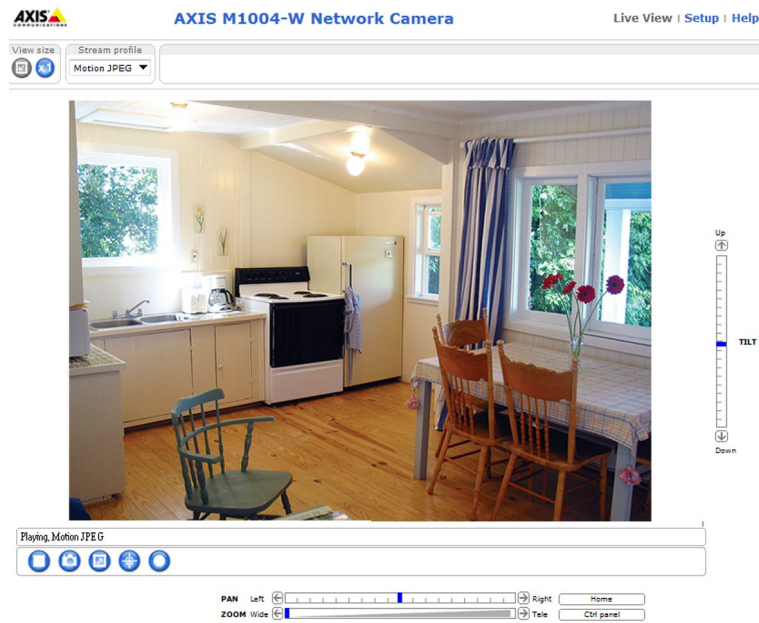
#### Note

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



# AXIS M1004-W Network Camera

## Accessing 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 Advanced**.

For more information, please see *NAT traversal (port mapping) for IPv4, on page 41*. See also **AXIS Internet Dynamic DNS Service** at [www.axiscam.net](http://www.axiscam.net) For Technical notes on this and other topics, visit the Axis Support web at [www.axis.com/techsup](http://www.axis.com/techsup)

### Set the Root Password

To gain access to the Axis product, you must set the password for the default administrator user **root**. This is done in the **Configure Root Password** dialog, which appears 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 41*.

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 50*.

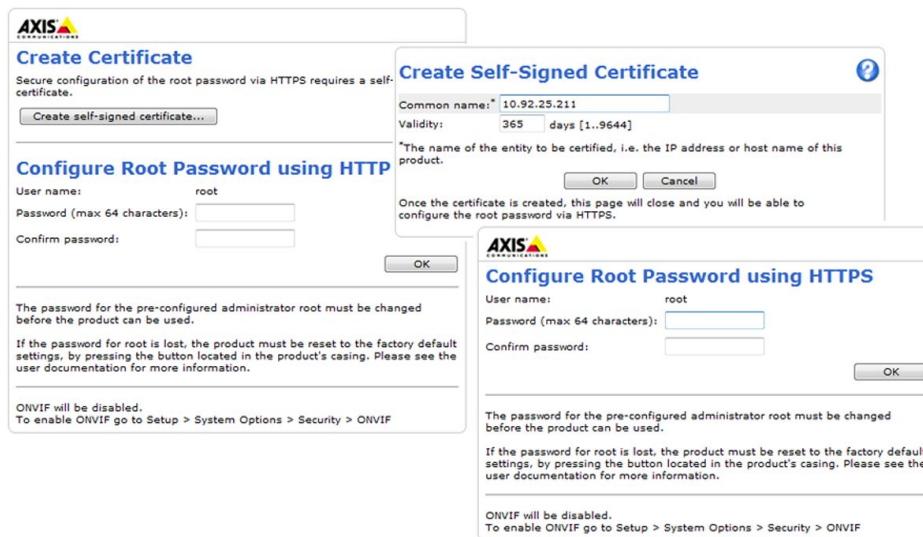
To set the password via a standard HTTP connection, enter it directly in the first dialog.

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

1. Click **Create self-signed certificate**.
2. Provide the requested information and click **OK**. The certificate is created and the password can now be set securely. All traffic to and from the product is encrypted from this point on.
3. Enter a password and then re-enter to confirm the spelling. Click **OK**. The password has now been configured.

# AXIS M1004-W Network Camera

## Accessing the Product



### Set Power Line Frequency

Power line frequency is set the first time the Axis product is accessed and can only be changed from Plain Config (see page 50) or by resetting the product to factory default.

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

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

#### Note

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

### The Live View Page

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

#### Controls on the Live View Page



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



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 18.



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

# AXIS M1004-W Network Camera

## Accessing the Product

---



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 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 23](#).



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 23](#).



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 11](#).



Click **Snapshot** to save a snapshot of the video image. Right-click the video image to save it in JPEG format on your computer. This button is primarily intended for use when the AXIS Media Control viewer toolbar is not available. Enable this button from **Live View Config > Action Buttons**.

### Manual Trigger

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

To configure the manual trigger:

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

For more information about action rules, see [Events, on page 31](#).

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

1. Go to **Setup > Live View Layout**.
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 13](#) for more information. The toolbar displays the following buttons:



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






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

# AXIS M1004–W Network Camera

## Accessing the Product

---

-  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

These controls are available if digital PTZ is enabled in the selected view area, see *View Area, on page 19*.

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 26*.

Select a PTZ preset position to steer the camera view to the saved position. See *Preset Positions, on page 25*.

The PTZ controls can be disabled under **PTZ > Advanced > Controls**, see *Controls, on page 26*.

# AXIS M1004–W Network Camera

## Media Streams

### Media Streams

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

The Live View 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

The video compression standard H.264 makes good use of bandwidth, and can provide high quality video streams at less than 1 Mbit/s.

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

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

#### Note

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

### MJPEG

This format uses standard JPEG still images for the video stream. These images are then displayed and updated at a rate sufficient to create a stream that shows constantly updated motion.

The Motion JPEG stream uses considerable amounts of bandwidth, but provides excellent image quality and access to every image contained in the stream. The recommended method of accessing Motion JPEG live video from the Axis product is to use the AXIS Media Control in Internet Explorer in Windows.

### AXIS Media Control (AMC)

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

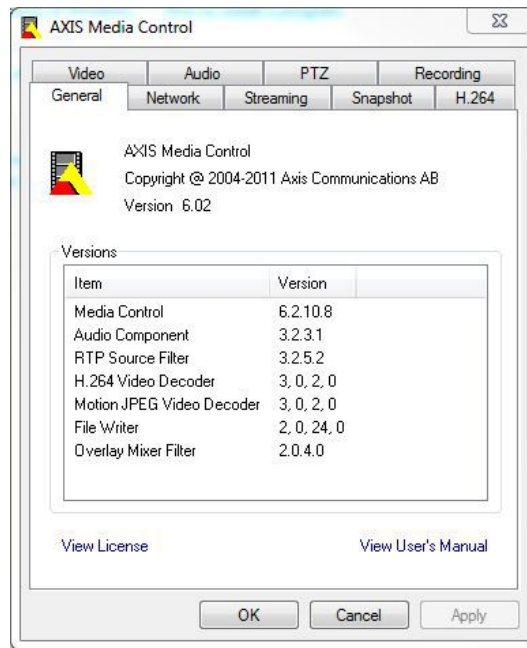
# AXIS M1004–W Network Camera

## Media Streams

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 menu)
- Alternatively, right-click the video image in Internet Explorer and click **Settings**.



## Alternative Methods of Accessing the Video Stream

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

- **Motion JPEG server push** (if supported by the client, 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: `axrtpm://<ip>/axis-media/media.amp`
- **QuickTime™**. The following paths can be used:
  - `rtsp://<ip>/axis-media/media.amp`
  - `rtsp://<ip>/axis-media/media.3gp`

# AXIS M1004–W Network Camera

## Media Streams

---

### Note

- <ip>= IP address
- The Axis product supports QuickTime 6.5.1 and later.
- QuickTime adds 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 M1004–W Network Camera


## Setting Up the Product

---

### Setting 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 36*.
2. **Wireless.** See *page 42*.
3. **TCP/IP.** See *page 38*.
4. **Date & Time.** See *page 38*.
5. **Video Stream.** See *page 17*.

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



# AXIS M1004-W Network Camera

## Setting Up the Product

### Video

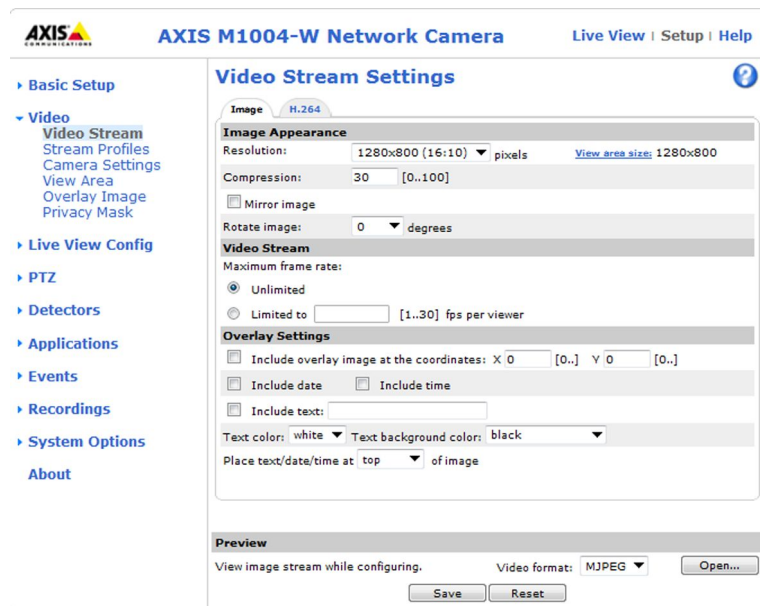
It is possible to configure the following video features in your Axis product:

- Video stream. See *page 17*.
- Stream profiles. See *page 18*.
- Camera settings. See *page 19*.
- View area. See *page 19*.
- Overlay image. See *page 20*.
- Privacy mask. See *page 21*.

### Video Stream

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

- Image. See *page 18*.
- H.264. See *page 18*.



### 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 can be accessed from:

- **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**.
- The Live View page in Internet Explorer in Windows. Right-click in the image and select **Pixel counter**. Use the mouse to move and resize the rectangle.

# AXIS M1004–W Network Camera

## Setting Up the Product

---

### Image

The default image settings can be configured under **Video > Video Stream**. Select the **Image** tab.

The following settings are available:

- **Resolution.** Select the default resolution.
- **Compression.** The compression level affects the image quality, bandwidth and file size of saved images; the lower the compression, the higher the image quality with higher bandwidth requirements and larger file sizes.
- **Rotate image.** If required, the image can be rotated.
- **Mirror.** If required, the image can be mirrored.
- **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 20*.

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 **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 two **H.264 profiles**. The Main profile provides higher compression than the Baseline profile with the same video quality, 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. CBR allows you to set a fixed **Target bit rate** that consumes a predictable amount of bandwidth. As the bit rate would usually need to increase for increased image activity, but in this case cannot, frame rate and image quality are affected negatively. To partly compensate for this, it is possible to prioritize either frame rate or image quality. Not setting a priority means that frame rate and image quality are equally affected. You must save your settings before they can take effect.

The current bit rate can be set to appear as text overlay. To do this, select the **Include text** check box option under **Overlay Settings** and enter the modifier #b in the field.

### MJPEG

Sometimes the image size is large due to low light or complex scenery. Adjusting the maximum frame size helps to control the bandwidth and storage used by the Motion JPEG video stream in these situations. Setting the frame size to the **Default** setting provides consistently good image quality at the expense of increased bandwidth and storage usage in low light. Limiting the frame size optimizes bandwidth and storage usage, but may give poor image quality. To prevent increased bandwidth and storage usage, the maximum frame size should be set to an optimal value.

## Stream Profiles

A stream profile is a set of predefined stream settings including resolution, compression, frame rate and overlay settings. Stream profiles can be used:

- When setting up recording using action rules. See *Events, on page 31*.
- When setting up continuous recording. See *Continuous Recording, on page 35*.

# AXIS M1004–W Network Camera

## Setting Up the Product

---

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

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

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

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

## Camera Settings

The **Video > 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.

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

### 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 .

### Wide Dynamic Range

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

#### Note

This setting is only possible when using automatic exposure control.

### Exposure Settings

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

**Exposure value** – Click in the bar to fine-tune the exposure.

**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 priority** – When **Motion** is prioritized, 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, 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.

### View Area

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.

# AXIS M1004–W Network Camera

## Setting Up the Product

---

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 a view area, go to **Video > Camera Settings** and select **Enable View Area**.

To configure the view area:


1. Go to **Video > View Area**.
2. Select an **Aspect ratio** and a **Video stream resolution**.
3. Use the mouse to move and resize the view area.
4. Select **Enable PTZ** to enable digital PTZ for the view area.
5. Click **Save** to save the settings.

### Note


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

## Overlay

Overlays are used to provide extra information, 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 .

To enable overlays:

1. Go to **Video > 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 38.

## Overlay Image

An overlay image is a static image superimposed over the video stream. The image, for example 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 digital Pan/Tilt movements. To set up a dynamic mask, which will always mask a specified part of the monitored area, see *Privacy Mask*.

To use an overlay image, the image must first be uploaded to the Axis product:

1. Go to **Video > Overlay Image**.
2. Click **Browse** and browse to the file.

# AXIS M1004–W Network Camera

## Setting Up the Product

---

3. Click **Upload**.
4. Select the image to use from the **Use overlay image** list.
5. Click **Save**.

To display the overlay image:

1. Go to **Video > Video Stream** and select the **Image** tab.
2. Under **Overlay Settings**, select **Include overlay image at the coordinates** and enter the X and Y coordinates.
3. Click **Save**.


For information about supported image formats, see the online help .

## Privacy Mask

A privacy mask is an area of solid color that prohibits users from viewing parts of the monitored area. Privacy masks cannot be bypassed via the VAPIX® Application Programming Interface (API).

The Privacy Mask List (**Video > 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.

# AXIS M1004–W Network Camera

## Live View Config

### Live View Config

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 18*.
- Default Viewer for Browser. See *page 22*.
- Viewer Settings. See *page 23*.
- Action Buttons. These are the buttons described in *Controls on the Live View Page, on page 10*.
- User Defined Links. See *page 23*.
- Light Buttons. See .
- Output Buttons. See *page 23*.

The screenshot shows the 'Live View Layout' configuration page. On the left is a navigation menu with options: Basic Setup, Video, Live View Config Layout (selected), PTZ, Detectors, Applications, Events, Recordings, System Options, and About. The main content area is titled 'Live View Layout' and contains several sections:

- Stream Profile:** Stream profile: Motion JPEG (dropdown). A checkbox for 'Show stream profile selection' is checked.
- Default Viewer:** Windows Internet Explorer: AMC (ActiveX) (dropdown). Other Browsers: Server push (dropdown). A note states: 'Note: QuickTime is only used with H.264. Motion JPEG will be shown with AMC in Windows Internet Explorer and with server push in other browsers.'
- Viewer Settings:** Checkboxes for 'Show viewer toolbar', 'Enable H.264 decoder installation', 'Show crosshair in PTZ joystick mode\*', 'Use PTZ joystick mode as default\*', and 'Enable recording button' are all checked. A note below says '\*Not applicable to AMC (ActiveX)'.
- Action Buttons:** Checkboxes for 'Show manual trigger button' and 'Show snapshot button' are checked.
- User Defined Links:** Four entries for 'Custom link 1' through '4'. Each has a 'Show custom link' checkbox (unchecked), a 'Name' field (pre-filled with 'Custom link X'), and a 'URL' field (pre-filled with 'http://'). To the right of each is a 'Use as:' section with radio buttons for 'cgi link' (selected) and 'web link'.
- Output Buttons:** 'Output 1' is set to '-----' (dropdown). 'Save' and 'Reset' buttons are at the bottom.

### 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.

# AXIS M1004–W Network Camera

## Live View Config

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"><li>• JVM (J2SE) 1.4.2 or higher.</li><li>• JRE (J2SE) 5.0 or higher.</li></ul>
	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.
- **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 **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 13.

### 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.

### Output Buttons

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

To display output buttons in the Live View page:

1. Go to **Setup > Live View Config**.
2. Under **Output Buttons**, select the type of control to use:
  - **Pulse** activates the output for a defined period of time. The pulse time can be set from 1/100 second to 60 seconds.
  - **Active/Inactive** displays two buttons, one for each action.

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

## AXIS M1004–W Network Camera

### Live View Config

---

For more information about I/O ports, see *I/O Ports*, on page 48.



# AXIS M1004-W Network Camera

## PTZ (Pan Tilt Zoom)

### PTZ (Pan Tilt Zoom)

The PTZ menu is available if digital PTZ (pan, tilt and zoom) is enabled in the selected view area. For more information on view areas, see *View Area*, on page 19.

### Preset Positions


A preset position is a predefined view that can be used to quickly steer the camera to a specific location. Preset positions can be accessed in several ways:

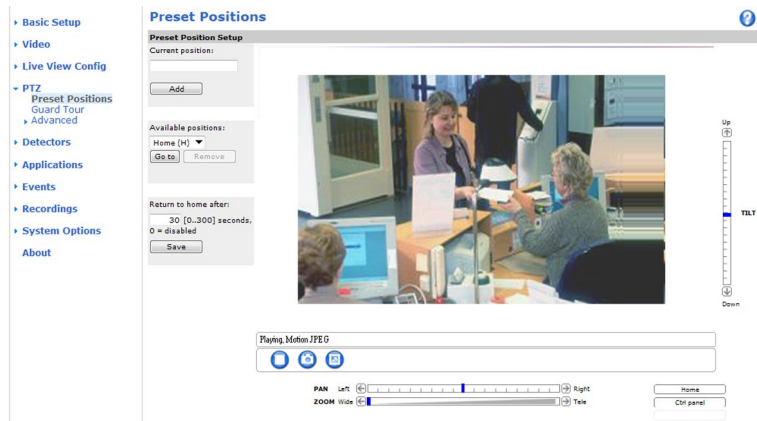
- By selecting the preset from the **Source** drop-down list in the Live View Page.
- When setting up action rules. See page 31.
- When setting up Guard Tour. See page 25.

To add a preset position:

1. Go to **PTZ > Preset Positions**.
2. Use the pan, tilt and zoom controls to steer the camera view to the desired position.
3. Enter a descriptive name in the **Current position** field.

The product can be configured to return to the Home position when the PTZ functionality has been inactive for a specified length of time. Enter the length of time in the field and click **Save**. Set the time to zero to prevent the product from automatically returning to the Home position.

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



### 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.

To add a guard tour:

1. Go to **PTZ > Guard Tour** and click **Add**.
2. Enter a descriptive name.


## AXIS M1004–W Network Camera

### PTZ (Pan Tilt Zoom)

---

3. Specify the pause length between runs.
4. Select an available preset position and click **Apply**.
5. Specify the **View Time** in seconds or minutes.
6. Specify the **View Order** or select the **Random view order** option.
7. Click **Save**.

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 .

### Advanced

#### Controls

**Panel Shortcut Command Buttons** can be configured to provide direct access to commands issued via the VAPIX® Application Programming Interface. The buttons will be displayed in the PTZ control panel, which is available in the Live View page through the **Ctrl panel** button, see *page 12*.

#### 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.

## 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. This can help prevent false alarms for known conditions that affect the image.
3. Select **Alarm for dark images** if an alarm should be generated if lights are dimmed or turned off, or if the lens is sprayed, covered, or rendered severely out of focus.
4. Click **Save**.

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

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

#### Note

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

For more information on actions rules, see *Events, on page 31*.

#### Motion Detection

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

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 28*.

To control the number of motion detection alarms, the parameters **Object Size**, **History** and **Sensitivity** can be adjusted. See *Motion Detection Parameters, on page 28*.

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 *Setting Up an Action Rule, on page 32*.

# AXIS M1004-W Network Camera

## Detectors

**Note**

Using the motion detection feature may decrease the product's overall performance.

### Set Up Motion Detection Windows

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

1. Go to **Detectors > Motion Detection**.
2. Select the **Configure Included Windows** option and click **New**. Select the new window in the list of windows and enter a descriptive name.
3. 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.
4. 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.
5. 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.

## AXIS M1004–W Network Camera

### Detectors

---

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

#### 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.
- If no objects should appear in the Include Window, 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 M1004–W Network Camera

## 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](http://www.axis.com/applications)

#### Note

- It is recommended to run one application at a time.
- Avoid running applications when the built-in motion detection is active.

# AXIS M1004–W Network Camera

## Events

---

### Events

The Axis product can be configured to perform actions when different events occur, for example, start a recording when motion is detected. The set of conditions that defines how and when the action is triggered is called an **Action Rule**.

Available Action Rule triggers and conditions include:

- **Detectors**
  - **Motion Detection** – trigger the rule when motion is detected, see *Motion Detection, on page 27*.
  - **Tampering** – trigger the rule when tampering is detected, see *Camera Tampering, on page 27*.
- **Hardware**
  - **Network** – trigger the rule if network connection is lost or restored.
- **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 48*.
  - **Manual Trigger** – trigger the rule using the **Manual Trigger** button in the Live View page, see *Controls on the Live View Page, on page 10*. This can for example be used to validate actions during product installation and configuration.
- **PTZ**
  - **Moving** – trigger the rule when the camera view moves due to a PTZ operation. This can for example be used as an additional condition to prevent an action rule triggered by motion detection to record video while the camera view moves due to a PTZ operation.
  - **Preset Reached** – trigger the rule when the camera stops at a preset position. This can be for example be used with the Send Images action to upload images from the preset position.
- **Storage**
  - **Available** – trigger the rule when the storage device is unmounted or removed. This can for example be used to send maintenance notifications.
  - **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).
- **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.
- **Time**
  - **Recurrence** – trigger the rule periodically, see *Recurrences, on page 33*. This can for example be used to upload an image every 5 minutes.
  - **Use Schedule** – trigger the rule according to the selected schedule, see *Schedules, on page 33*.

Available actions include:

- **Activate Light** – turn the built-in light on or off.
- **Output Port** – activate an I/O port to control an external device.
- **PTZ Control**

# AXIS M1004–W Network Camera

## Events

---

- **Preset Position** – go to a preset position.
- **Guard Tour** – start a guard tour, see *Guard Tour, on page 25*.
- **Record Video** – record video to a selected storage.
- **Send Images** – send images to a recipient.
- **Send Notifications** – send a notification message 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.

### Setting Up an Action Rule

An action rule defines the conditions that must be met for the product to perform an action, for example record video or send email notifications. If multiple conditions are defined, all must be met to trigger the action.

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

Set up motion detection and add a network share:


1. Go to **Detectors > Motion Detection** and configure a motion detection window, see *page 28*
2. Go to **System Options > Storage** and set up the network share, see *page 47*.

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.

To add additional criteria, select the **Additional conditions** option and add additional triggers. 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 .

### Recipients

Recipients receive media files and notification messages. The following recipients are available:



# AXIS M1004–W Network Camera

## Events

---

Recipient	Use with action
Email	Send Images
	Send Notification
FTP	Send Images
HTTP	Send Images
	Send Notification
Network Share	Send Images
TCP	Send Notification

### Note

A network share can also be used as a storage device for recorded video. Go to **System Options > Storage** to configure a network share before setting up a continuous recording or an action rule to record video. See *Storage, on page 47* for more information about storage devices.

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**.

## Schedules

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

To create a new schedule:

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

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

## Recurrences

Recurrences are used to trigger Action Rules repeatedly, for example every 5 minutes or every hour.

To set up a recurrence:

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

## AXIS M1004–W Network Camera

### Events

---

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

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

# AXIS M1004–W Network Camera

## Recordings

---

### Recordings

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

- To start a continuous recording, see *page 35*.
- To set up action rules, see *page 32*.
- To access recordings, see *Recording List, on page 35*.
- To configure camera controlled storage, see *Storage, on page 47*.

### Recording List

Recorded videos are listed on the **Recordings > List** page. The list shows each recording's start date and time, duration and the event that triggered the recording.

To play or download a recording, follow these steps:

1. Go to **Recordings > List**.
2. Use the filter to narrow the list of recordings. Enter the desired filter criteria and click **Filter**. Some filters may take a long time to complete.
3. Select the recording.
4. Click **Play** to play the recording, or click **Download** to download the recording.

Multiple recordings can be downloaded at the same time. Select the recordings and click **Download**. The downloaded file is a zip file containing a minimum of three files, of which the Matroska (mkv) files are the actual recordings. The recordings are time-stamped with the date and time they were downloaded (that is, not the date the recordings were made).

#### Note

To play recordings in Windows Media Player, AXIS Matroska File Splitter must be installed. AXIS Matroska File Splitter can be downloaded from [www.axis.com/techsup/software](http://www.axis.com/techsup/software)

For detailed recording and video information, select a recording and click **Properties**.

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

### Continuous Recording

The Axis product can be configured to continuously save video to a storage device. See *Storage, on page 47* for more information about storage devices. To prevent the disk from becoming full, it is recommended to configure the disk to automatically remove old recordings. If a new stream profile is selected while a recording is ongoing, the recording will be stopped and saved in the recording list and a new recording with the new stream profile will start. All previous continuous recordings will remain in the recording list until they are removed manually or through automatic removal of old recordings.

To start a continuous recording, follow these steps:

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

## System Options

---

### System Options

#### Security

##### Users

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

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

**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](http://www.onvif.org)

##### IP Address Filter

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

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


##### HTTPS

The Axis product supports encrypted browsing using HTTPS. This is configured on the **System Options > Security > HTTPS** page.

A **self-signed certificate** can be used until a Certificate Authority-issued certificate has been obtained. Click **Create self-signed certificate** to install a self-signed certificate. Although self-signed certificates are free and offer some protection, true security is only implemented after the installation of a signed certificate issued by a Certificate Authority.

To obtain a signed certificate from an issuing Certificate Authority, click **Create Certificate Request**. When the signed certificate is returned, click **Install signed certificate** to import the certificate. The properties of any certificate request currently resident in the product or installed can be viewed by clicking **Properties**.

To enable HTTPS in the Axis product, the **HTTPS Connection Policy** must be set for each user group.

For more information, see the online help .

# AXIS M1004–W Network Camera

## System Options

---

### 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 authenticate themselves. The authentication is performed by a third-party entity called an authentication server, typically a **RADIUS server**, examples of which are FreeRADIUS and Microsoft Internet Authentication Service.

In Axis' implementation, the network device and the authentication server authenticate themselves with the help of digital certificates using EAP-TLS (Extensible Authentication Protocol - Transport Layer Security). The certificates are provided by an **Certification Authority (CA)**. You need:

- a CA certificate to validate the identity of the authentication server
- a CA-signed client certificate and a private key to authenticate the network device.

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

1. Obtain a CA certificate, a client certificate and a client private key (contact your network administrator).
2. Go to **Setup > System Options > Security > IEEE 802.1X** and upload the CA certificate, the client certificate and the client private key.
3. Under **Settings**, select the EAPOL version, provide your EAP identity and private key password.
4. Check the box to enable IEEE 802.1X and click **Save**.

#### Certificates

##### CA Certificate

The CA certificate is used to validate the identity of the authentication server. Enter the path to the certificate directly, or locate the file using the **Browse** button. Then click **Upload**. To remove a certificate, click **Remove**.

##### Client certificate Client private key

The client certificate and private key are used to authenticate the network device. They can be uploaded as separate files or in one combined file (e.g. a PFX file or a PEM file). Use the **Client private key** field if uploading one combined file. For each file, enter the path to the file, or locate the file using the **Browse** button. Then click **Upload**. To remove a file, click **Remove**.

#### Settings

##### EAPOL version

Select the EAPOL version (1 or 2) as used in your network switch.

##### EAP identity

Enter the user identity (maximum 16 characters) associated with your certificate.

##### Private key password

Enter the password (maximum 16 characters) for the private key.

##### Enable IEEE 802.1X

Check the box to enable the IEEE 802.1X protocol.

### Certificates

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

**Server/Client certificates** – to authenticate the Axis product

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

#### Note

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

# AXIS M1004–W Network Camera

## System Options

---

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 **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 **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 **System Options > Security > Certificates**
2. Click **Install certificate** and upload the certificate.

## Date & Time

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

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


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

- **Synchronize with computer time** sets date and time according to the computer's clock. With this option, date and time are set once and will not be updated automatically.
- **Synchronize with NTP Server** obtains date and time from an NTP server. With this option, date and time settings are updated continuously. For information on NTP settings, see *NTP Configuration, on page 41*.

If using a host name for the NTP server, a DNS server must be configured. See *DNS Configuration, on page 40*.

- **Set manually** allows you to manually set date and time.

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

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

## Network

### Basic TCP/IP Settings

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

# AXIS M1004–W Network Camera

## System Options

---

### Network Interface Mode

The network interface to the AXIS product can be wired or wireless. Different settings can be used for each network interface, but only one can be used at a time. In **Auto** mode the product will use a wireless network unless a network cable is connected, in which case it will use the wired network. In **Wired** mode the product will require a network cable to connect to the network.

### IPv4 Address Configuration

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

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

If DHCP is enabled and the product cannot be accessed, run **AXIS IP Utility** to search the network for connected Axis products, or reset the product to the factory default settings (see *page 50*) and then perform the installation again.

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

### IPv6 Address Configuration

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

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

### ARP/Ping

The product's IP address can be assigned using ARP and Ping. For instructions, see *Assign IP Address using ARP/Ping, on page 39*.

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

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

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

### Assign IP Address using ARP/Ping

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

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 408 408 192.168.0.125
```

#### 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>
```

# AXIS M1004–W Network Camera

## System Options

---

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 to the Axis product 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](http://www.axis.com/techsup)

### Note

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

### AXIS Video Hosting System (AVHS)

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

AVHS is enabled by default. The settings are configured under **System Options > Network > TCP/IP > Basic**.

**One-click enabled** – Press the product's control button (see *Hardware Overview, on page 6*) to connect to an AVHS service over the Internet. Once registered, **Always** will be enabled and the Axis product stays connected to the AVHS service. If the product is not registered within 24 hours from when the button is pressed, the product will disconnect from the AVHS service.

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

### AXIS Internet Dynamic DNS Service

AXIS Internet Dynamic DNS Service assigns a host name for easy access to the product. For more information, see [www.axiscam.net](http://www.axiscam.net)

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

## Advanced TCP/IP Settings

### DNS Configuration

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

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

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

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

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



# AXIS M1004–W Network Camera

## System Options

---

### NTP Configuration

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

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

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


### Host Name Configuration

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

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

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

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

For more information, see the online help .

### Link-Local IPv4 Address

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

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

### HTTP

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

### HTTPS

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

To enable HTTPS, go to **System Options > Security > HTTPS**. For more information, see *page 36*.

### NAT traversal (port mapping) for IPv4

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

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

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

#### Note

- For NAT traversal to work, this must be supported by the router. The router must also support UPnP™.
- The router has many different names: "NAT router", "Network router", "Internet Gateway", "Broadband router", "Broadband sharing device" or "Home firewall" but the essential purpose of the device is the same.

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

# AXIS M1004–W Network Camera

## System Options

---

**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 the port number in the field. If no port is entered here, a port number is automatically selected when NAT traversal is enabled.

### Note

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

### FTP

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

### Note

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

### RTSP

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

### Note

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

## Wireless

### Wireless Network Status

To view a list of available wireless networks, go to **System Options > Network > Wireless**. The status of wireless networks list is the result of a network scan and provides the following information:

- **SSID** is the name of a wireless network (or ad-hoc network).
- **Mode** shows the type of network, which can be **Master** (an access point) or **Ad-Hoc**.
- **Security** shows the type of security the network uses.
- **Channel** shows the wireless channel currently in use.
- **Signal strength** shows the quality, the strength, of the signal.
- **Bit rate** shows the current bit rate in Mbit/s. This can only be shown for the access point currently in use.

Click **Refresh** to perform a new scan.

Access points with a disabled SSID Broadcast will not appear unless the Axis product is associated with it. Once the wireless connection is established, the network the Axis product is currently linked to is shown in blue. A network using unsupported security is shown in grey.

# AXIS M1004–W Network Camera

## System Options

---

### Wireless Settings

#### Important

- To establish and maintain communication, all wireless settings must be exactly the same in the Axis product as in the access point or ad-hoc network.
- Always configure or change the wireless settings in the Axis product first, before changing the settings in the wireless access point.
- Keys, passphrases and certificates that are used for security must be entered manually. Contact your Network Administrator for the requirements for the selected access point or ad-hoc network.

The wireless settings control how the Axis product interacts with the wireless network. Apart from identifying the wireless network, it is also possible to enable wireless encryption.

Select **Enable congestion control** to secure the wireless connection between the Axis product and access point in congested environments, for example where there are many available networks and where many devices are using the same access point.

Congestion control uses a Request To Send/Clear To Send (RTS/CTS) handshake to reserve access to the wireless media before transmitting a packet. Using the handshake decreases throughput since it adds an overhead. In some situations, however, the overhead of the RTS/CTS handshake is lower than the overhead caused by collisions on the wireless media. Congestion control is disabled by default.

Select **Enable WLAN pairing button** to allow the wireless Axis product to connect to an access point by pushing a button on both of the devices within a 120 second time window. During this time the devices will automatically discover each other and agree on a configuration.

Make sure the access point also has push button configuration (PBC) enabled and that the Axis product is not connected to the wired network. After a successful pairing any WLAN settings set by the user in the Axis product are overwritten. The WLAN pairing button is enabled by default; deselect this option to prevent unauthorized WLAN pairing.

**SSID** is the name of the selected wireless network, which must be exactly the same as the name in the wireless access point. If the field is left blank the Axis product will not connect to any wireless network.

#### Note

SSID is sometimes written as ESSID.

Select the network **Security** method. All settings must match the settings in the access point. The following security methods are supported, where WPA<sup>TM</sup>-/WPA2<sup>TM</sup>-Enterprise is more secure than WPA-/WPA2-PSK, which in turn is more secure than WEP:

- WPA-/WPA2-PSK. See *page 43*.
- WPA-/WPA-Enterprise. See *page 44*.
- WEP (not recommended). See *page 45*.
- No security (not recommended). See *page 45*.

If applicable, select the **Network type**. Select **Master** to access the network via an access point or **Ad-hoc** to access any other wireless device and create a local network.

Ad-hoc mode allows users to form a wireless LAN without connection through an access point. The Axis product can, for example, connect point-to-point to an existing ad-hoc network, or if there is none, create one itself. Ad-hoc connection may be useful in certain installations and for troubleshooting but is not the recommended method. The ad-hoc option is only available when supported by the selected security method.

### WPA<sup>TM</sup>-/WPA2<sup>TM</sup>-PSK

The security method **WPA-/WPA2-PSK** is designed for small networks and does not require an authentication server. The Axis product uses a PSK (Pre-Shared Key) to authenticate with the access point. The key can be entered either as manual hex — a 64 hexadecimal number (0–9, A–F) — or a passphrase using 8–63 ASCII characters. The longer the passphrase, the more secure is the key.

To configure the wireless settings using the WPA-/WPA2-PSK security method:

# AXIS M1004–W Network Camera

## System Options

---

1. Enter the required **Passphrase** for the access point.
2. Click **Save**.

### WPA™-/WPA-Enterprise

The security method **WPA-/WPA-Enterprise** is designed for large networks and requires an authentication server. The network is protected by EAPOL (Extensible Authentication Protocol Over Lan).

Select the **WPA-Enterprise** type being used by the access point:

- EAP-TLS. See *page 44*.
- EAP-PEAP/MSCHAPv2. See *page 44*.

### EAP-TLS

The authentication protocol **EAP-TLS** (Extensible Authentication Protocol - Transport Layer Security) allows the client and server to authenticate each other using digital certificates provided by a Certification Authority. To gain access to the protected network, the Axis product presents its certificate to the network access point. Access is granted if the certificate is approved.

#### Important

To ensure successful certificate validation, time synchronization should be performed on all clients and servers prior to configuration.

To configure the wireless settings using the WPA™-/WPA-Enterprise security method and EAP-TLS:

1. Enter the user **Identity** associated with your certificate.
2. Enter the **Private key password** for your user identity.
3. Select the **EAPOL version** (1 or 2) as used in the access point.
4. Click **Save**.

For more information on certificates for wireless networks, see *Certificates, on page 45*.

### EAP-PEAP/MSCHAPv2

The authentication protocol **EAP-PEAP/MSCHAPv2** (Extensible Authentication Protocol - Protected Extensible Authentication Protocol/Microsoft Challenge Handshake Authentication Protocol) allows the client to authenticate the network using a digital certificate provided by a Certification Authority. The network authenticates the client using an identity and a password. To gain access to the protected network, the Axis product presents its identity and password to the network access point. If these credentials are approved, the access point allows access on a preconfigured port.

#### Important

To ensure successful certificate validation, time synchronization should be performed on all clients and servers prior to configuration.

To configure the wireless settings using the WPA™-/WPA-Enterprise security method and EAP-PEAP/MSCHAPv2:

1. Enter the user **Identity** associated with your certificate.
2. Enter the **Password** for your user identity.
3. Select the **PEAP Version** (0 or 1) as used in the access point.
4. Select the **PEAP Label** that the access point uses when using PEAP version 1. Select 1 to use client EAP encryption; select 2 to use client PEAP encryption.
5. Select the **EAPOL version** (1 or 2) as used in the access point.

# AXIS M1004–W Network Camera

## System Options

---

6. Click **Save**.

For more information on certificates for wireless networks, see *Certificates*, on page 45.

### WEP

The security method **WEP** (Wired Equivalent Privacy) can be used to help secure a wireless network. However, WEP has some flaws, which makes it more vulnerable to attacks and WPA™-WPA-Enterprise or WPA-/WPA2™-PSK a better choice.

To configure the wireless settings using the WEP security method:

1. Select the network type being used by the access point, **Master** or **Ad-Hoc**.
2. Select the **Authentication** type, **Open** or **Shared Key** depending on the method used by the access point. Not all access points have this option, in which case they probably use open system, also sometimes called SSID Authentication.
3. Select the **Key length**, **64 bit** or **128 bit** used for the wireless encryption.
4. Select the **Key type**, depending on the key type used by the access point and enter the key in the corresponding key fields.

**Manual** allows you to manually enter the hex key. **ASCII** requires the string to be exactly five characters for 64-bit WEP and 13 characters for 128-bit WEP. The **Passphrase** can contain up to 31 characters. In 64-bit WEP the passphrase generates four different keys. For 128-bit WEP, only one key is generated, which then is replicated for all four keys.

The **Active transmit key** selects which of the four keys the Axis product uses when transmitting information.

5. Click **Save**.

### No Security

The **No security** option provides no protection against attacks. It is not a recommended method and should only be used during short periods and exceptional cases.

To configure the wireless settings with no security:

1. Select the network type being used by the access point, **Master** or **Ad-Hoc**.
2. Click **Save**.

### Certificates

Wireless network certificates are used to authenticate devices on a wireless network. Wireless networks using the WPA™-/WPA-Enterprise security method are protected by EAPOL (Extensible Authentication Protocol Over Lan), which is part of the IEEE 802.1X standard. The client and server authenticate each other using digital certificates provided by a Certificate Authority. To gain access to the protected wireless network, the Axis product presents its certificate to the network switch. If the certificate is approved, the switch allows access.

You may need to contact your network administrator for information on certificates, user IDs and passwords

**CA certificate** – Created by the Certification Authority for the purpose of validating itself and is used by the Axis product for checking the server's identity.

**Client certificate/Client private key** – Used for the Axis product to authenticate itself using a client certificate and a private key.

To upload a CA certificate:

1. Enter the path to the certificate directly or click **Browse** to locate the file.
2. Click **Upload**.

To upload a client certificate/client private key:

# AXIS M1004–W Network Camera

## System Options

---

1. Use the **Client private key** field if uploading one combined file. For each file, enter the path to the file or click **Browse** to locate the file.
2. Click **Upload**.

To remove a CA certificate/Client certificate/Client private key, click **Remove**.


### Note

Installed certificates will be deleted if the product is reset to factory default.

For more information about IEEE 802.1X, see *IEEE 802.1X, on page 37*.

## SOCKS

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

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

## QoS (Quality of Service)

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

The QoS settings are configured under **System Options > Network > QoS**. Using DSCP (Differentiated Services Codepoint) values, the Axis product can mark the following types of traffic: live video, event/alarm traffic and management traffic.

## SMTP (email)

To send email messages from the Axis product via SMTP (Simple Mail Transfer Protocol), an SMTP mail server must be set up. This is done under **System Options > Network > SMTP (email)**.

Enter the host names or IP addresses and port numbers for the primary and secondary mail servers in the fields provided. A **From email address** is also required. If the mail server requires authentication, check **Use authentication to log in to this server** and enter the necessary information.

## 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.

The Axis product can be configured to support SNMP on the **System Options > Network > SNMP** page.

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

**SNMP v1/v2** provides the lowest level of security. The community name can be specified as a password for read or read/write access to all supported SNMP devices. The default password for the **Read community** is public and the default password for the **Write community** is write.

### 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

# AXIS M1004–W Network Camera

## System Options

---

- Warm start
- Link up
- Authentication failed

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

To use SNMP v3, HTTPS must be enabled, see *HTTPS*, on page 36. 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 50.

### UPnP™

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

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

### RTP/H.264

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

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

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

### Bonjour

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

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

## Storage

### Network Share

Network share allows you to add network storage such as a NAS (Network Attached Storage) or any server that uses CIFS (Common Internet File System) and use them for storage of recordings.

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**.

# AXIS M1004–W Network Camera

## System Options

---

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

The Axis product provides one input port and one output port for connection of external devices. For information on how to connect external devices, see *Connectors, on page 6*.

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**.

### Port Status

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

## Maintenance

The Axis product provides several maintenance functions. These are available under **System Options > Maintenance**.

Click **Restart** to perform a correct restart if the Axis product is not behaving as expected. This will not affect any of the current settings.

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

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 50*.

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 *Upgrading the Firmware, on page 51*.

## Support

### Support Overview

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

See also *Troubleshooting, on page 51*.



# AXIS M1004–W Network Camera

## System Options

---

### System Overview

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

### Logs & Reports

The **System Options > Support > Logs & Reports** page generates logs and reports useful for system analysis and troubleshooting. If contacting Axis Support, please provide a valid Server Report with your query.

**System Log** – Provides information about system events.

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

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

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

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

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

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

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

## Advanced

### Scripting

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

#### **NOTICE**

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

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

To open the Script Editor, go to **System Options > Advanced > Scripting**. If a script causes problems, reset the product to its factory default settings, see *page 50*.

For more information, see [www.axis.com/developer](http://www.axis.com/developer)

### File Upload

Files, for example web pages and images, can be uploaded to the Axis product and used as custom settings. To upload a file, go to **System Options > Advanced > File Upload**.

Uploaded files are accessed through `http://<ip address>/local/<user>/<file name>` where <user> is the selected user group (viewer, operator or administrator) for the uploaded file.

# AXIS M1004–W Network Camera

## System Options

---

### Plain Config

Plain Config is for advanced users with experience of Axis product configuration. Most parameters can be set and modified from this page. Help is available from the standard help pages.

To open Plain Config, go to **System Options > Advanced > Plain Config**. Axis Support does not provide assistance.

### Reset to Factory Default Settings

#### Important

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

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 6*.
3. Keep the control button pressed for about 15 seconds until the status LED indicator flashes amber.
4. Release the control button. The process is complete when the status LED indicator turns green. The product has been reset to the factory default settings. If no DHCP server is available on the network, the default IP address is 192 . 168 . 0 . 90
5. Use the tools provided on the Installation and Management Software CD to assign an IP address, set the password and access the video stream. This information is also available from the support pages on [www.axis.com/techsup](http://www.axis.com/techsup)

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

# AXIS M1004-W Network Camera

## Troubleshooting

### Troubleshooting

#### Checking the Firmware

Firmware is software that determines the functionality of network devices. One of your first actions when troubleshooting a problem should be to check the current firmware version. The latest version may contain a correction that fixes your particular problem. The current firmware version in the Axis product is displayed in the page **Setup > Basic Setup** and in **Setup > About**.

#### Upgrading the Firmware

When you upgrade the 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, follow these instructions:

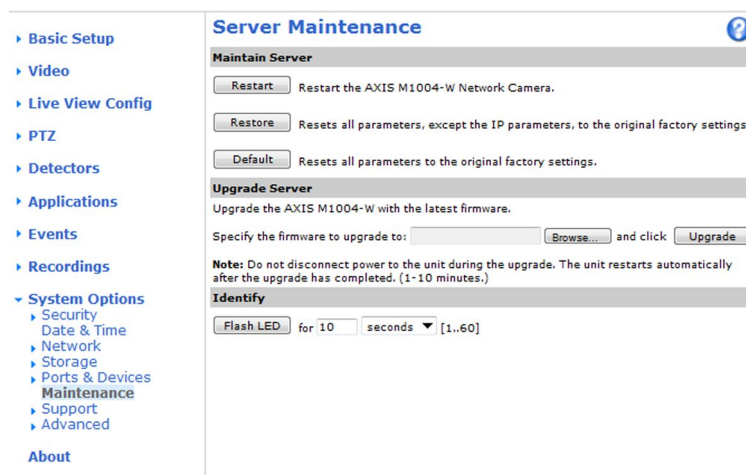
1. Save the firmware file to your computer. The latest version of the firmware is available free of charge from Axis website at [www.axis.com/techsup](http://www.axis.com/techsup)
2. Go to **Setup > System Options > Maintenance** in the products web pages.
3. Under **Upgrade Server**, click **Browse** and locate the file on your computer. Click **Upgrade**.

After starting the upgrade process, always wait at least 5–10 minutes before restarting the product, even if you suspect the upgrade has failed.

AXIS Camera Management can be used for multiple upgrades. See [www.axis.com](http://www.axis.com) for more information.

#### Note

- 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.



#### 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.

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

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

# AXIS M1004–W Network Camera

## Troubleshooting

---

```
ping -s 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 appears, 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/](http://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 39</i> .
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"><li>• If you receive: <code>Reply from &lt;IP address&gt;: 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.</li><li>• 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.</li></ul>
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 root is lost, the product must be reset to the factory default settings. See <i>Reset to Factory Default Settings, on page 50</i> .
---------------	---

# AXIS M1004–W Network Camera

## 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.</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 <a href="http://www.axis.com/techsup">www.axis.com/techsup</a></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 &amp; Time</i> , on page 38.

### 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 41. The router must support UPnP™.
Firewall protection	Check the Internet firewall with your network administrator.
Default routers required	Check if you need to configure the router settings.

### Problems with the H.264 format

---

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 13.</p> <p>In the AMC Control Panel, select the H.264 tab and click <b>Set to default H.264 decoder</b>.</p> <p>Check that RTSP is enabled under <b>System Options &gt; Network &gt; TCP/IP &gt; Advanced</b>.</p>
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>
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.
Poor rendering of H.264 images	<p>Color depth set incorrectly on clients. Set to 16-bit or 32-bit color.</p> <p>If text overlays are blurred, or if there are other rendering problems, you may need to enable Advanced Video Rendering from the Video tab in the AMC Control Panel.</p> <p>Ensure that your graphics card is using the latest driver. The latest drivers can usually be downloaded from the manufacturer's website.</p>
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>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 <b>Decode only key frames</b>.</p> <p>Lower the image resolution.</p>

# AXIS M1004–W Network Camera

## Troubleshooting

---

Why do I not get maximum frames per second?	See <i>Performance Considerations</i> , on page 59.  The maximum frames per second is dependent on the utility frequency (60/50 Hz) of the Axis product. See <i>Technical Specifications</i> , on page 56.
Image degeneration	Decrease the GOV length. Go to <b>Video &gt; Video Stream</b> and select the <b>H.264</b> tab to modify the GOV length.

### Status and Network indicator LEDs are flashing red rapidly

---

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

### No images displayed on web page

---

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.
Installation of additional ActiveX component restricted or prohibited	Configure the Axis product to use a Java applet for updating video images in Internet Explorer. Go to <b>Setup &gt; Live View Config</b> and select Java applet under <b>Default viewer</b> .

### Video and image problems, general

---

Image too dark or too light	Check the video stream and camera settings under <b>Setup &gt; Video &gt; Video Stream</b> and <b>Setup &gt; Video &gt; Camera Settings</b> .
Missing images in uploads	This can occur when trying to use a larger image buffer than is actually available. Try lowering the frame rate or the upload period.
Slow image update	Configuring pre-buffers, motion detection, high-resolution images or high frame rates will affect the performance of the Axis product.
Poor performance	Poor performance may be caused by heavy network traffic, multiple users accessing the product, low performance clients, use of features such as motion detection, event handling or uploaded applications.
Disturbed focus	Set the focus manually by turning the focus ring.

### Poor quality snapshot images

---

Screen incorrectly configured on your computer	Configure your screen to show at least 65000 colors, that is, at least 16 bits. Using only 16 or 256 colors will produce dithering artifacts in the image.
--	--

### Overlay image is not displayed

---

Incorrect size or location of overlay image	The overlay image may have been positioned incorrectly or may be too large. See <i>Overlay Image Settings</i> in the online help for more information.
---	--

### Privacy mask is not displayed

---

Incorrect size or location of privacy mask	The privacy mask may have been positioned incorrectly or may be too large.
--	--

### Browser freezes

---

Firefox can sometimes freeze on a slow computer	Lower the image resolution
---	----------------------------

# AXIS M1004–W Network Camera

## Troubleshooting

---

### Problems uploading files

---

Limited space                      There is only limited space available for the upload of your own files. Delete existing files to free up space.

### 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.

## Problem Retrieving Additional Video Streams

---

'Video Error' displayed in AXIS Camera Companion              This camera is designed to deliver up to four different streams. If a fifth unique stream is requested the camera will not deliver it and an error message is displayed. The error message depends on the way the stream is requested.

'503 service unavailable' error in IE / AMC or Quick Time              Stream 0: Max resolution - 1280 x 800, fixed, cannot be configured for lower resolutions  
Stream 1: 1440 x 900, upscaled, can use lower resolutions  
Stream 2: 1280 x 720, can use lower resolutions  
Stream 3: 720 x 576, used for Axis Camera Application Platform, can use lower resolutions

'Camera not available' displayed in AXIS Camera Station              These streams are used on a first-come-first-served basis. Examples of using a stream are:

- Live viewing in a web browser or other application
- While recording - continuous or motion triggered recording
- An event using images on the camera
- An installed application, such as Axis Video Motion Detection 2.1 will always use a stream, regardless of whether it is used or not.

'If no image is displayed, there might be too many viewers...' in Firefox / Safari

'Error reading video Stream' message in browser when using the Java applet              The camera can deliver more than four simultaneous streams provided the configuration of any additional stream is identical to any of the four first streams. Identical configuration implies exactly the same resolution, frame rate, compression, video format, rotation etc. For more information see [www.axis.com/techsup](http://www.axis.com/techsup)

# AXIS M1004–W Network Camera

## Technical Specifications

### Technical Specifications

Function/group	Item	Specifications
Camera	Model	AXIS M1004–W: Wired and wireless interface, I/O ports
	Image sensor	1/4" progressive scan RGB CMOS
	Lens	2.8 mm: 80° view*, F2.0, fixed iris, adjustable focus *Horizontal angle of view
	Light sensitivity	1.2 - 10000 lux, F2.0
	Shutter time	1/8000 s to 1/6 s
	Pan/Tilt/Zoom	Digital PTZ, Preset positions, Guard tour
Video	Video compression	H.264 (MPEG-4 Part 10/AVC, Main profile) Motion JPEG
	Resolutions	1280 x 800 to 320 x 240
	Frame rate H.264	30 fps in all resolutions
	Frame rate Motion JPEG	30 fps in all resolutions (performance may be reduced in wireless mode)
	Video streaming	Multiple, individually configurable streams in H.264 and Motion JPEG Controllable frame rate and bandwidth VBR/CBR H.264, MJPEG.
	Image settings	Compression, color, brightness, sharpness, contrast, white balance, backlight compensation Rotation: 0°, 90° 180° 270° Mirroring of images Text and image overlay Privacy mask Axis' Corridor Format
Network	Wireless interface	IEEE 802.11g/b/n (802.11n single stream, 20 MHz channel width) Internal antenna
	Security	Password protection, IP address filtering, HTTPS encryption*, IEEE 802.1X network access control*, digest authentication, user access log Wi-Fi pairing button (Wi-Fi Protected Setup* PBC compatible) *This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit ( <a href="http://www.openssl.org">www.openssl.org</a> )
	Supported protocols	IPv4/v6, HTTP, HTTPS*, QoS Layer 3 DiffServ, FTP, CIFS/SMB (not supported in AXIS M1011–W), SMTP, Bonjour, UPnP™, SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS *This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit ( <a href="http://www.openssl.org">www.openssl.org</a> )



## AXIS M1004-W Network Camera

### Technical Specifications

Function/group	Item	Specifications
System Integration	Application Programming Interface	Open API for software integration ONVIF specification available at <a href="http://www.onvif.org">www.onvif.org</a> VAPIX® from Axis Communications, specifications available at <a href="http://www.axis.com">www.axis.com</a> Support for AXIS Video Hosting System (AVHS) with One-Click Camera connection Support for AXIS Camera Application Platform from Axis Communications, specifications available at <a href="http://www.axis.com">www.axis.com</a> AXIS Media Control SDK (Available at <a href="http://www.axis.com">www.axis.com</a> ), 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	Intelligent video, external input
	Event actions	File upload: FTP, HTTP, network share and email Notification: email, HTTP and TCP Pre- and post alarm video buffering External output activation
	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 <a href="http://www.axis.com/techsup">www.axis.com/techsup</a>
	Management and maintenance	AXIS Camera Management tool on CD and web-based configuration Firmware upgrades over HTTP or FTP, firmware available on <a href="http://www.axis.com">www.axis.com</a>
	Built-in aids in software	Pixel counter
General	Casing	Polycarbonate
	Memory	256 MB RAM, 128 MB Flash
	Power	4.9 - 5.1 V DC, max. 6.5 W
	Connectors	DC jack RJ45 10BASE-T/100BASE-TX 1 alarm input and 1 output
	Edge storage	Support for recording to network share (Network Attached Storage or file server)
	Operating conditions	0 °C to 40 °C (32 °F to 104 °F) Humidity 20–80% RH (non-condensing)
	Approvals	CE: EN 55022 Class B, EN 61000-6-3, EN 61000-6-4, EN 61000-3-2, EN 61000-3-3, EN 55024, EN 61000-6-1, EN 61000-6-2, EN 60950-1, EN 62311, EN 300328 V1.8.1, EN 301489-1, EN 301489-17, EN 62471 (risk group 1), EN 50581, EN 50581 FCC: FCC Part 15, Subpart B and C, Class B VCCI: VCCI, Class B, ITE C-Tick: AS/NZS CISPR 22 ICES-003: ICES-003, Class B Safety: IEC/EN/UL 60950-1 Korean KCC: KN22 Class B, KN24, IEC60950-1 Additional radio approvals: Argentina (CNC), Japan (TELEC), Canada (RSS-210), Australia/New-Zeeland (AS/NZS 4771), Brazil (Anatel), Taiwan (NCC), USA (FCC Part 15, Subpart C247), China (SRRC) Power supply: EN 60950-1, cCSAus
	Dimensions (HxWxD)	95 x 59 x 41 mm (3.7 in x 2.3 in x 1.6 in)
	Weight	Camera: 111.4 g(0.24 lb.)

# AXIS M1004–W Network Camera

## Technical Specifications

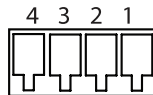
Function/group	Item	Specifications
	Included accessories	Power supply, stand and clamp, Installation Guide, Installation and Management Software CD, Windows decoder 1-user license
	Video management software	AXIS Camera Companion (included) AXIS Camera Station and video management software from Axis' Application Development Partners (not included) For more information, see <a href="http://www.axis.com/products/video/software">www.axis.com/products/video/software</a>
	Optional accessories	PoE Active Splitter Installation Display Network I/O

## Connectors

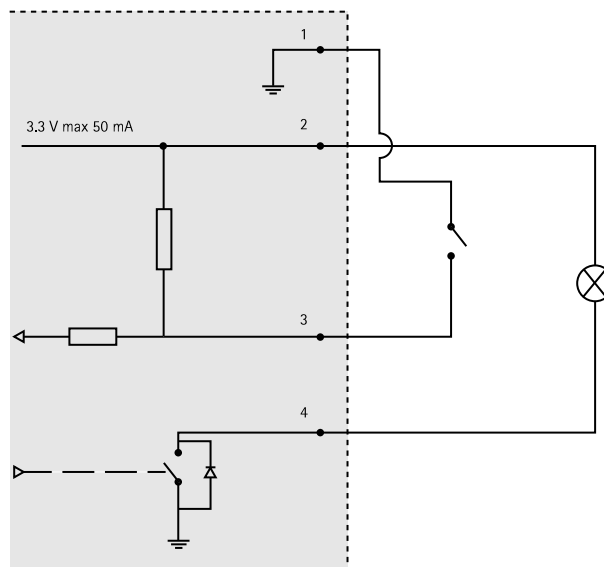
### I/O terminal connector

4-pin terminal block for:

- Digital Input
- Digital Output
- Auxiliary power and ground (GND)



Function	Pin	Notes	Specifications
GND	1	Ground	
3.3 V DC Power	2	Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	Max load = 50 mA
Digital Input	3	Connect to GND to activate, or leave floating (unconnected) to deactivate.	0 to +40 V DC
Digital Output	4	Internal connection to ground 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.	Max load = 100 mA Max voltage = +40 V DC



## Technical Specifications

---

### Performance Considerations

When settings 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.

