About this Document
This manual is intended for administrators and users of the AXIS M3025-VE Fixed Dome Network Camera, and is applicable to firmware 5.50 and later. It includes instructions for using and managing the product on your network. Previous experience of networking will be of use when using this product. Some knowledge of UNIX or Linux-based systems may also be beneficial, for developing shell scripts and applications. Later versions of this document will be posted to the Axis website, as required. See also the product’s online help, available via the web-based interface.

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

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

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

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

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

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

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

Trademark Acknowledgments
AXIS COMMUNICATIONS, AXIS, ETRAX, ARTEPC 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 WWV 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. UHPSTM is a certification mark of the UHPSTM Implementers Corporation.

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

Regulatory Information


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

Electromagnetic Compatibility (EMC)
This equipment has been designed and tested to fulfill applicable standards for:
- Radio frequency emission when installed according to the instructions and used in its intended environment.
- Immunity to electrical and electromagnetic phenomena when installed according to the instructions and used in its intended environment.

USA
This equipment has been tested using a shielded network cable (STP) and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

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

Cet appareil numérique est conforme à la norme CAN NMB-3 (class B). Le produit doit être connecté à l’aide d’un câble réseau blindé (STP) qui est correctement mis à la terre.

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

This product fulfills the requirements for 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.

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

This product fulfills the requirements for immunity according to EN 61000-2-3 residential, commercial and light-industrial environments.

This product fulfills the requirements for immunity according to EN 61000-2-3 industrial environments.

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� Television 受信機に干渉を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。本製品は、シールドネットワークケーブル（STP）を使用して接続してください。また、適切に接地してください。

Korea
이 기기는 가정용(B급) 전자파적합기로서 주로 가정에서 사용하는 것을 목적으로 하며, 모든 지역에서 사용할 수 있습니다. 적절히 정지된 STP (shielded twisted pair) 케이블을 사용하여 제품을 연결 하십시오.
Safety
This product complies with IEC/EN/UL 60950-1 and IEC/EN/UL 60950-2-22, Safety of Information Technology Equipment. The product shall be grounded either through a shielded network cable (STP) or other appropriate method.

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

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

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

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

Contact Information
Axis Communications AB
Emdalavägen 14
223 69 Lund
Sweden
Tel.: +46 46 272 18 00
Fax: +46 46 13 81 30
www.axis.com

Support
Should you require any technical assistance, please contact your Axis reseller. If your questions cannot be answered immediately, your reseller will forward your queries through the appropriate channels to ensure a rapid response. If you are connected to the Internet, you can:
• download user documentation and software updates
• find answers to resolved problems in the FAQ database. Search by product, category, or phrase
• report problems to Axis support staff by logging in to your private support area
• chat with Axis support staff (selected countries only)
• visit Axis Support at www.axis.com/techsup/

Learn More!
# AXIS M3025-VE Network Camera

## Table of Contents

- **Hardware Overview** ........................................... 6
  - Connectors and Buttons ........................................ 6
  - LED Indicators .................................................. 7

- **Access the Product** ........................................... 8
  - Access from a Browser .......................................... 8
  - Access from the Internet ...................................... 8
  - Set the Root Password ......................................... 8
  - Set Power Line Frequency ..................................... 9
  - The Live View Page ............................................ 9

- **Media Streams** .................................................. 12
  - How to Stream H.264 .......................................... 12
  - MJPEG .......................................................... 12
  - AXIS Media Control (AMC) .................................... 12
  - Alternative Methods of Accessing the Video Stream .... 13

- **Set Up the Product** .......................................... 15
  - Basic Setup .................................................... 15
  - Video .......................................................... 16
  - Video Stream .................................................. 16
  - Stream Profiles ................................................ 17
  - Camera Settings ................................................ 18
  - View Area ....................................................... 19
  - Overlay ........................................................ 19
  - Privacy Mask ................................................... 21

- **Configure the Live View Page** ................................ 22

- **PTZ (Pan Tilt Zoom)** ......................................... 24
  - Preset Positions ............................................... 24
  - Advanced ....................................................... 24

- **Detectors** ...................................................... 26
  - Camera Tampering .............................................. 26
  - Motion Detection ............................................... 26

- **Applications** .................................................. 29
  - Application Licenses ........................................... 29
  - Install Application ............................................ 29
  - Application Considerations ................................... 29

- **Events** .......................................................... 31
  - Convert Event Types to Action Rules ......................... 31
  - Set Up Action Rules ............................................ 31
  - Add Recipients ................................................ 33
  - Create Schedules .............................................. 34
  - Set Up Recurrences ............................................ 35

- **Recordings** .................................................... 36
  - Recording List ................................................ 36
  - Continuous Recording ........................................ 36

- **Languages** ..................................................... 37

- **System Options** ............................................... 38
  - Security ......................................................... 38
  - Date & Time .................................................... 40
  - Network ......................................................... 40
  - Storage ........................................................ 46
  - Ports & Devices ............................................... 47
  - Maintenance .................................................... 47
  - Support ........................................................ 48
  - Advanced ....................................................... 49
  - Reset to Factory Default Settings ........................... 49

- **Troubleshooting** .............................................. 51
  - Check the Firmware ............................................ 51
  - Upgrade the Firmware ......................................... 51
  - Symptoms, Possible Causes, and Remedial Actions ....... 52
  - Problem Retrieving Additional Video Streams ............ 54

- **Technical Specifications** .................................... 55
  - Connectors ...................................................... 57
AXIS M3025–VE Network Camera

Table of Contents

Performance Considerations ........................................... 58
**Connectors and Buttons**

For technical specifications, see page 55.

**Network Connector**

RJ45 Ethernet connector with Power over Ethernet (PoE).

**NOTICE**

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

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

- **Digital output** – For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface, output buttons on the Live View page or by an Action Rule. The output will show as active (shown under System Options > Ports & Devices) if the alarm device is activated.

- **Digital input** – An alarm input for connecting devices that can toggle between an open and closed circuit, for example: PIRs, door/window contacts, glass break detectors, etc. When a signal is received the state changes and the input becomes active (shown under System Options > Ports & Devices).

SD Card Slot

A microSD card (not included) can be used for local recording with removable storage. For more information, see Technical Specifications on page 55.

**NOTICE**

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

**Note**

For SD card recommendations see www.axis.com

Control Button

The control button is used for:

- Resetting the product to factory default settings. See page 49.
- Connecting to an AXIS Video Hosting System service. See page 42. To connect, press and hold the button for about 3 seconds until the Status LED flashes green.
- Connecting to AXIS Internet Dynamic DNS Service. See page 42. To connect, press and hold the button for about 3 seconds.

LED Indicators

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Unlit</td>
<td>Connection and normal operation</td>
</tr>
<tr>
<td></td>
<td>Amber</td>
<td>Steady during startup. Flashes during firmware upgrade.</td>
</tr>
<tr>
<td></td>
<td>Amber/red</td>
<td>Flashes amber/red if network connection is unavailable or lost.</td>
</tr>
<tr>
<td></td>
<td>Red</td>
<td>Flashes red for firmware upgrade failure.</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>Shows steady green for 10 seconds for normal operation after restart.</td>
</tr>
</tbody>
</table>

**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 M3025–VE Network Camera

Access the Product

Access the Product

To install the Axis product, refer to the Installation Guide supplied with the product.

The product can be used with most operating systems and browsers. The recommended browsers are Internet Explorer with Windows, Safari with Macintosh and Firefox with other operating systems. See Technical Specifications on page 55.

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

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 8.

4. The product's Live View page opens in your browser.

Note

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

Access from the Internet

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

For more information, see NAT traversal (port mapping) for IPv4 on page 43. See also AXIS Internet Dynamic DNS Service at www.axis.com.net

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

Set the Root Password

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

To prevent network eavesdropping, the root password can be set via an encrypted HTTPS connection, which requires an HTTPS certificate. HTTPS (Hypertext Transfer Protocol over SSL) is a protocol used to encrypt traffic between web browsers and servers. The HTTPS certificate ensures encrypted exchange of information. See HTTPS on page 38.
AXIS M3025–VE Network Camera

Access the Product

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 49.

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

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

1. Click Use HTTPS.
   A temporary certificate (valid for one year) is created, enabling encryption of all traffic to and from the product, and the password can now be set securely.
2. Enter a password and then re-enter it to confirm the spelling.
3. Click OK. The password has now been configured.

Set Power Line Frequency

Power line frequency is set the first time the Axis product is accessed and can only be changed from Plain Config (see page 49) or by resetting the product to factory default.

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

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

**Note**

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

The Live View Page

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

Controls on the Live View Page

- **Click 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 17.

- **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.
AXIS M3025–VE Network Camera

Access the Product

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 10.

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

Manual Trigger

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

To configure the manual trigger:

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

For more information about action rules, see Events on page 31.

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

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

AXIS Media Control viewer toolbar

The AXIS Media Control viewer toolbar is available in Internet Explorer only. See AXIS Media Control (AMC) on page 12 for more information. The toolbar displays the following buttons:

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

The Stop button stops the media stream.

The Snapshot button takes a snapshot of the video image. 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.
Access the Product

Note

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

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

- Click the Emulate joystick mode button and click in the image to move the camera view in the direction of the mouse pointer.
- Click the Center mode button and click in the image to center the camera view on that position. The center mode button could also be used to zoom in on a specific area. Click in the image and drag to draw a rectangle surrounding the area to be magnified. To zoom out, rotate the mouse wheel.
- 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 24.
- Select a PTZ preset position to steer the camera view to the saved position. See Preset Positions on page 24.

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

The PTZ controls can be disabled under PTZ > Advanced > Controls, see Controls on page 24.
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

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

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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unicast RTP</td>
<td>This unicast method (RTP over UDP) is used for live unicast video, especially when it is important to always have an up-to-date video stream, even if some frames are dropped. Unicasting is used for video-on-demand transmission so that there is no video traffic on the network until a client connects and requests the stream. Note that there are a maximum of 20 simultaneous unicast connections.</td>
</tr>
<tr>
<td>RTP over RTSP</td>
<td>This unicast method (RTP tunneled over RTSP) is useful as it is relatively simple to configure firewalls to allow RTSP traffic.</td>
</tr>
<tr>
<td>RTP over RTSP over HTTP</td>
<td>This unicast method can be used to traverse firewalls. Firewalls are commonly configured to allow the HTTP protocol, thus allowing RTP to be tunneled.</td>
</tr>
<tr>
<td>Multicast RTP</td>
<td>This method (RTP over UDP) should be used for live multicast video. The video stream is always up-to-date, even if some frames are dropped. Multicasting provides the most efficient usage of bandwidth when there are large numbers of clients viewing simultaneously. A multicast cannot however, pass a network router unless the router is configured to allow this. It is not possible to multicast over the Internet, for example. Note also that all multicast viewers count as one unicast viewer in the maximum total of 20 simultaneous connections.</td>
</tr>
</tbody>
</table>

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

**Note**

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

MJPEG

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

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

AXIS Media Control (AMC)

AXIS Media Control (AMC) in Internet Explorer in Windows is the recommended method of accessing live video from the Axis product.
The AMC Control Panel can be used to configure various video settings. Please see the AXIS Media Control User’s Manual for more information.

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

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

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: `axrtpshhttp://<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
Note

- `<ip>` = IP address
- The Axis product supports QuickTime 6.5.1 and later.
- QuickTime may add latency to the video stream.
- It may be possible to use other players to view the H.264 stream using the paths above, although Axis does not guarantee this.
AXIS M3025–VE Network Camera

Set Up the Product

Set Up the Product

The Axis product can be configured by users with administrator or operator rights. To open the product’s Setup pages, click Setup in the top right-hand corner of the Live View page.

- Administrators have unrestricted access to all settings.
- Operators have access to all settings except System Options

See also the online help 📚.

Basic Setup

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

1. Users. See page 38.
2. TCP/IP. See page 40.
3. Date & Time. See page 40.

The Basic Setup menu can be disabled from System Options > Security > Users.
AXIS M3025–VE Network Camera

Set Up the Product

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

• Video stream. See page 16.
• Stream profiles. See page 17.
• Camera settings. See page 18.
• View area. See page 19.
• Overlay image. See page 19.
• Privacy mask. See page 21.

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

• Image. See page 16.
• H.264. See page 17.
• MJPEG. See page 17.

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 with AXIS Media Control (AMC) in Windows. Right-click in the image and select Pixel counter. Use the mouse to move and resize the rectangle.

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

The following settings are available:

• Resolution. Select the default resolution.
• Compression. The compression level affects the image quality, bandwidth and file size of saved images; the lower the compression, the higher the image quality with higher bandwidth requirements and larger file sizes.
• Mirror image. If required, the image can be mirrored.
• Rotate image. If required, the image can be rotated.
• Maximum frame rate. To avoid bandwidth problems, the frame rate allowed to each viewer can be Limited to a fixed amount. Alternatively, the frame rate can be set as Unlimited, which means the Axis product always delivers the highest frame rate possible under the current conditions.

• Overlay settings. See Overlay on page 19.

Click Save to apply the new settings.
AXIS M3025–VE Network Camera

Set Up the Product

H.264

H.264, also known as MPEG-4 Part 10/AVC, is a video compression standard that provides high quality video streams at low bit rates. An H.264 video stream consists of different types of frames such as I-frames and P-frames. An I-frame is a complete image whereas P-frames only contain the differences from previous frames.

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

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

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

- **Main.** The Main profile provides higher compression with maintained video quality compared to the Baseline profile but requires more processing power to decode.

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

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

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

  To apply the settings, click Save.

MJPEG

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

Stream Profiles

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

- When setting up recording using action rules. See Events on page 31.
- When setting up continuous recording. See Continuous Recording on page 36.
- 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 slidebar.

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.

Day/Night

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

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

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

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

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

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

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 40.

Overlay Image

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

For more information about privacy masks, see Privacy Mask on page 21.
To use an overlay image, the image must first be uploaded to the Axis product. The uploaded image should be a Windows 24-bit BMP image with maximum 250 colors. The image width and height, in pixels, must be exactly divisible by 4 and cannot be larger than the maximum image resolution. If combining text and image overlays, take into consideration that the text overlay occupies 16 or 32 pixels in height (depending on the resolution) and has the same width as the video image.

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

To upload an overlay image:

1. Go to Video > Overlay Image.
2. Click Browse and browse to the file.
3. Click Upload.
4. The Transparency Settings page is now displayed:
   - To make a color in the overlay image transparent, select Use transparency and enter the RGB hexadecimal value for the color. Example: To make white transparent, enter #FFFFFF.
   - To scale the image automatically, select Scale with resolution. The image will be scaled down to fit the resolution used by the Axis product.
5. Click Save.

To select the image to use as overlay:

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

To display the overlay image:

1. Go to Video > Video Stream and select the Image tab.
2. Under Overlay Settings, select Include overlay image at the coordinates.
3. To control the image’s position, enter the X and Y coordinates. The X=0 and Y=0 position is the top left corner. If a part of the image is positioned outside the video image, the overlay image will be moved so that the whole image is visible.
4. Click Save.

Use Overlay Text in an Action Rule

Action rules, see page 31, can display an overlay text when the rule is triggered. The text can be used to provide information for forensic video analysis, notify surveillance operators or validate triggers and actions during product installation and configuration.

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

Start by enabling overlay text in the video stream:

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

Create the action rule:

1. Go to Events > Action Rules
2. Click Add to create a new rule.
AXIS M3025–VE Network Camera

Set Up the Product

3. Select a Trigger and, optionally, a Schedule and Additional conditions. See the online help for details.

4. From the Actions list, select Overlay Text

5. Enter the text to display in the Text field. This is the text that #D will be replaced by.

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

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

Privacy Mask

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

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

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

For more information, see the online help.

Important
Adding many privacy masks may affect the product’s performance.
Configure the Live View Page

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

- Stream Profile. See page 17.
- Default Viewer for Browser. See page 22.
- Viewer Settings. See page 22.
- Action Buttons. These are the buttons described in Controls on the Live View Page on page 9.
- User Defined Links. See page 23.
- Output Buttons. See page 23.

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.

<table>
<thead>
<tr>
<th>Browser</th>
<th>Viewer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Internet Explorer</td>
<td>AMC</td>
<td>Recommended viewer in Internet Explorer (H.264/Motion JPEG).</td>
</tr>
<tr>
<td></td>
<td>QuickTime</td>
<td>H.264.</td>
</tr>
</tbody>
</table>
|                        | Java applet | A slower imaging alternative to AMC (Motion JPEG). Requires one of the following installed on the client:  
|                        |        | - JVM (J2SE) 1.4.2 or higher.                                               |
|                        |        | - JRE (J2SE) 5.0 or higher.                                                  |
|                        | Still image | Displays still images only. Click the Refresh button in your browser to view a new image. |
| Other browsers         | Server Push | Recommended viewer for other browsers (Motion JPEG).                       |
|                        | QuickTime | H.264.                                                                      |
|                        | Java applet | A slower imaging alternative to Server Push (Motion JPEG only).             |
|                        | Still image | Displays still images only. Click the Refresh button in your browser to view a new image. |

For more information, please see the online help.

Viewer Settings

To configure options for the viewer, go to Live View Config > Viewer Settings.

- Select Show viewer toolbar to display the AXIS Media Control (AMC) or the QuickTime viewer toolbar under the video image in your browser.

- H.264 decoder installation. The administrator can disable installation of the H.264 decoder included with AXIS Media Control. This is used to prevent installation of unlicensed copies. Further decoder licenses can be purchased from your Axis reseller.

- Select Show crosshair in PTZ joystick mode to enable a cross that will indicate the center of the image in PTZ joystick mode.
Configure the Live View Page

- Select Use PTZ joystick mode as default to enable joystick mode. The mode can be changed temporarily from the PTZ control panel.
- Select Enable recording button to enable recording from the Live View page. This button is available when using the AMC viewer. The recordings are saved to the location specified in the AMC Control Panel. See AXIS Media Control (AMC) on page 12.

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.
For more information about I/O ports, see I/O Ports on page 47.
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 saved view that can be used to quickly steer the camera to a specific position. A preset position consists of the following values:

- Pan and tilt positions

Access the Preset Positions

Preset positions can be accessed in several ways:

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

Add a Preset Position

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

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

Set the Home Position

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

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

Advanced

Controls

Advanced PTZ settings can be configured under PTZ > Advanced > Controls.

The Panel Shortcut Command Buttons list shows the user-defined buttons that can be accessed from the Live View page's Ctrl panel. These buttons can be used to provide direct access to commands issued using the VAPIX® application programming interface. Click Add to add a new shortcut command button.

The following PTZ controls are enabled by default:

- Pan control
- Tilt control
To disable specific controls, deselect the options under Enable/Disable controls.

**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

Camera Tampering

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

To configure tampering:

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

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

1. Go to Events > Action Rules.
2. Click Add to set up a new action rule.
3. Enter a Name for the action rule.
4. Under Condition, select Detectors from the Trigger list.
5. Select Tampering from the list of detectors.
6. 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 27.

To control the number of motion detection alarms, the parameters Object Size, History and Sensitivity can be adjusted. See Motion Detection Parameters on page 27.

Once motion detection windows are configured, the Axis product can be configured to perform actions when motion is detected. Possible actions include uploading images and start recording. For more information, see Set Up Action Rules on page 31.
Detectors

Note

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

Set Up Motion Detection Windows

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

1. Go to 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Object Size</th>
<th>History</th>
<th>Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Object size relative to window size.</td>
<td>Object memory length.</td>
<td>Difference in luminance between background and object.</td>
</tr>
<tr>
<td>High level (100%)</td>
<td>Only very large objects trigger motion detection.</td>
<td>An object that appears in the window triggers motion detection for a long time before it is considered as non-moving.</td>
<td>Ordinary colored objects on ordinary backgrounds trigger motion detection.</td>
</tr>
<tr>
<td>Medium level (50%)</td>
<td></td>
<td></td>
<td>A large difference in luminance is required to trigger motion detection.</td>
</tr>
<tr>
<td>Low level (0%)</td>
<td>Even very small objects trigger motion detection.</td>
<td>An object that appears in the window triggers motion detection only for a very short time before it is considered as non-moving.</td>
<td>Only very bright objects on a dark background trigger motion detection.</td>
</tr>
<tr>
<td>Recommended values</td>
<td>5–15%</td>
<td>60–90%</td>
<td>75–95%</td>
</tr>
<tr>
<td>Default values</td>
<td>15%</td>
<td>90%</td>
<td>90%</td>
</tr>
</tbody>
</table>
AXIS M3025–VE Network Camera

Detectors

Note

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

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

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

Application Licenses

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

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

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

Install Application

To install and start an application:

1. Go to Setup > Applications.
2. Under Upload Application, click Browse. Locate the application file and click Upload Package.
3. Install the license (if applicable). For instructions, see the documentation provided by the application vendor.
4. Start the application. Go to page Applications, select the application in the list of installed applications and click Start.
5. Configure the application. For instructions, see the documentation provided by the application vendor.

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

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

Application Considerations

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

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

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

If the Axis product is restored, installed applications remain unchanged but must be restarted. To start the application, go to Setup > Applications. Select the application in the list of installed applications and click Start. For information about restoring the Axis product, see Maintenance.
If the Axis product is reset to factory default, installed applications and their settings are removed. For information about factory default, see Reset to Factory Default Settings.
Events

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

Convert Event Types to Action Rules

If the Axis product is upgraded to firmware version 5.40 or later, it is recommended to convert Event Types to Action Rules. The legacy user Event Types in the camera will continue to work but will not be visible in the user interface of the camera. The Event Types need to be converted to Action rules to become visible in the user interface.

To convert Event Types to Action Rules go to Events > Action Rules and click Convert.

**NOTICE**

This is not recommended when using a VMS based on the old Event Management System.

Set Up Action Rules

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

For more information about available triggers and actions, see Triggers on page 32 and Actions on page 33.

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 27
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 use more than one trigger for the action rule, select Additional conditions and click Add to add additional triggers. When using additional conditions, all conditions must be met to trigger the action.

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

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

For more information, see the online help.

Triggers

Available action rule triggers and conditions include:

- **Applications** – Use installed applications to trigger the rule. See Applications on page 29.
- **Detectors**
  - **Day/Night Mode** – Trigger the rule when the product switches between day mode (IR cut filter on) and night mode (IR cut filter off). This can for example be used to control an external infrared (IR) light connected to an output port.
  - **Live Stream Accessed** – Trigger the rule when any stream is accessed and during edge storage playback. This can for example be used to send notifications.
  - **Motion Detection** – Trigger the rule when motion is detected. See Motion Detection on page 26.
  - **Tampering** – Trigger the rule when tampering is detected. See Camera Tampering on page 26.
- **Hardware**
  - **Network** – Trigger the rule if network connection is lost or restored. This can for example be used to start recording to the SD card.
- **Input Signal**
  - **Digital Input Port** – Trigger the rule when an I/O port receives a signal from a connected device. See I/O Ports on page 47.
  - **Manual Trigger** – Trigger the rule using the Manual Trigger button in the Live View page. See Controls on the Live View Page on page 9. This can for example be used to validate actions during product installation and configuration.
  - **Virtual Inputs** – can be used by a VMS (Video Management System) to trigger actions. Virtual inputs can, for example, be connected to buttons in the VMS user interface.
- **PTZ**
  - **Error** – Trigger the rule if the PTZ functionality is not working correctly. This can for example be used to send maintenance notifications.
  - **Moving** – Trigger the rule when the camera view moves due to a PTZ operation. This can for example be used as an additional condition to prevent an action rule triggered by motion detection to record video while the camera view moves due to a PTZ operation.
  - **Preset Reached** – Trigger the rule when the camera stops at a preset position. This can be for example be used with the Send Images action to upload images from the preset position.
  - **Ready** – Trigger the rule when the PTZ functionality is ready to be used. This can for example be used to steer the camera to a specific preset position when the product is started.
- **Storage**
  - **Disruption** – Trigger the rule if storage problems are detected, for example if the storage device is unavailable, removed, full, locked or if other read or write problems occur. This can for example be used to send maintenance notifications.
- **System**
  - **System Ready** – Trigger the rule when the product has been started and all services are running. This can for example be used to send a notification when the product restarts.
AXIS M3025–VE Network Camera

Events

- Time
  - Recurrence – Trigger the rule periodically. See Set Up Recurrences on page 35. This can for example be used to upload an image every 5 minutes.
  - Use Schedule – Trigger the rule according to the selected schedule. See Create Schedules on page 34.

Actions

Available actions include:

- Day/Night Vision Mode – Set day mode (IR cut filter on) or night mode (IR cut filter off).
- Output Port – Activate an I/O port to control an external device.
- Overlay Text – Display an overlay text. See Use Overlay Text in an Action Rule on page 20.
- PTZ Control
  - Preset Position – Go to a preset position.
- Record Video – Record video to a selected storage.
- Send Images – Send images to a recipient.
- Send Notifications – Send a notification message to a recipient.
- Send Video Clip – Send a video clip to a recipient.
- Status LED – Flash the LED indicator. This can for example be used to validate triggers such as motion detection during product installation and configuration.

Add Recipients

The product can send media files and messages to notify users about events. Before the product can send media files or notification messages, you must define one ore more recipients. For information about available options, see Recipient Types on page 33.

To add a recipient:

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

Recipient Types

The following recipients are available:

<table>
<thead>
<tr>
<th>Recipient</th>
<th>Use with action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Send Images</td>
<td>An email recipient can contain multiple email addresses. For more information about email recipients, see Set Up Email Recipients on page 34</td>
</tr>
<tr>
<td></td>
<td>Send Notification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Send Video Clip</td>
<td></td>
</tr>
</tbody>
</table>
Events

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>Send Images</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Send Video Clip</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>Send Images</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Send Notification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Send Video Clip</td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>Send Images</td>
<td>Encrypted file transfer using HyperText Transfer Protocol Secure (HTTPS).</td>
</tr>
<tr>
<td></td>
<td>Send Notification</td>
<td>Specify login information for the HTTPS server and validate the server’s certificate. If there is a proxy between the Axis product and the HTTPS server, also specify the proxy settings.</td>
</tr>
<tr>
<td></td>
<td>Send Video Clip</td>
<td></td>
</tr>
<tr>
<td>Network Share</td>
<td>Send Images</td>
<td>A network share can also be used as a storage device for recorded video. Go System Options &gt; Storage to configure a network share before setting up a continuous recording or an action rule to record video. For more information about storage devices, see Storage on page 46.</td>
</tr>
<tr>
<td></td>
<td>Send Video Clip</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>Send Notification</td>
<td></td>
</tr>
</tbody>
</table>

Set Up Email Recipients

Email recipients can be configured by selecting one of the listed email providers, or by specifying the SMTP server, port and authentication used by, for example, a corporate email server.

**Note**

Some email providers have security filters that prevent users from receiving or viewing large amount of attachments, from receiving scheduled emails and similar. Check the email provider’s security policy to avoid delivery problems and locked email accounts.

To set up an email recipient using one of the listed providers:

1. Go to Events > Recipients and click Add.
2. Enter a Name and select Email from the Type list.
3. Enter the email addresses to send emails to in the To field. Use commas to separate multiple addresses.
4. Select the email provider from the Provider list.
5. Enter the user ID and password for the email account.
6. Click Test to send a test email.

To set up an email recipient using for example a corporate email server, follow the instructions above but select User defined as Provider. Enter the email address to appear as sender in the From field. Select Advanced settings and specify the SMTP server address, port and authentication method. Optionally, select Use encryption to send emails over an encrypted connection. The server certificate can be validated using the certificates available in the Axis product. For information on how to upload certificates, see Certificates on page 39.

Create Schedules

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

To create a new schedule:

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

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

**Set Up Recurrences**

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

To set up a recurrence:

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

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 M3025–VE 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 36.
- To set up action rules, see page 31.
- To access recordings, see Recording List on page 36.
- To configure camera controlled storage, see Storage on page 46.

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

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. For information about storage devices, see Storage on page 46. To prevent the disk from becoming full, it is recommended to configure the disk to automatically remove old recordings.

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

To start a continuous recording, follow these steps:

1. Go to Recordings > Continuous.
2. Select Enabled.
3. Select the type of storage device from the Storage list.
4. Select a Stream profile to use for continuous recordings.
5. Click Save to save and start the recording.
Multiple languages can be installed in the Axis product. All web pages including the online help will be displayed in the selected language. To switch languages, go to Setup > Languages and first upload the new language file. Browse and locate the file and click the Upload Language button. Select the new language from the list and click Save.

**Note**

- Resetting the product to factory default settings will erase any uploaded language files and reset the product language to English.
- Clicking the Restore button on the Maintenance page will not affect the language.
- A firmware upgrade will not affect the language used. However if you have uploaded a new language to the product and later upgrade the firmware, it may happen that the translation no longer matches the product's web pages. In this case, upload an updated language file.
- A language already installed in the product will be replaced when a current or a later version of the language file is uploaded.
AXIS M3025–VE Network Camera

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

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

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

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

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

To use HTTPS, an HTTPS certificate must first be installed. Go to System Options > Security > Certificates to install and manage certificates. See Certificates on page 39.

To enable HTTPS on the Axis product:

1. Go to System Options > Security > HTTPS
2. Select an HTTPS certificate from the list of installed certificates.

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

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

5. Click Save to enable the settings.

To access the Axis product via the desired protocol, enter https:// or http:// in the address field in a browser.

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

IEEE 802.1X

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

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

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

You need:

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

To create and install certificates, go to System Options > Security > Certificates. See Certificates on page 39. Many CA certificates are preinstalled.

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

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

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

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

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

**Note**

For authentication to work properly, the date and time settings in the Axis product should be synchronized with an NTP server. See Date & Time on page 40.

Certificates

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

**Server/Client certificates** – To authenticate the Axis product.

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

**Note**

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

A Server/Client certificate can be self-signed or issued by a Certificate Authority (CA). A self-signed certificate offers limited protection and can be used before a CA-issued certificate has been obtained.
To install a self-signed certificate:

1. Go to Setup > System Options > Security > Certificates.
2. Click Create self-signed certificate and provide the requested information.

To create and install a CA-signed certificate:

1. Create a self-signed certificate as described above.
2. Go to Setup > System Options > Security > Certificates.
3. Click Create certificate signing request and provide the requested information.
4. Copy the PEM-formatted request and send to the CA of your choice.
5. When the signed certificate is returned, click Install certificate and upload the certificate.

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

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

1. Go to Setup > System Options > Security > Certificates.
2. Click Install certificate and upload the certificate.

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 43.
  
  If using a host name for the NTP server, a DNS server must be configured. See DNS Configuration on page 42.
- Set manually – Allows you to manually set date and time.

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

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

Network

Basic TCP/IP Settings

The Axis product supports IP version 4 and IP version 6. Both versions can be enabled simultaneously, and at least one version must always be enabled.
IPv4 Address Configuration

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

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

If DHCP is enabled and the product cannot be accessed, run AXIS IP Utility to search the network for connected Axis products, or reset the product to the factory default settings (see page 49) 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 41.

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 408 192.168.0.125

   **Windows syntax (this may require that you run the command prompt as an administrator)**
   
   arp -s <IP address> <serial number>
   ping -l 408 -t <IP address>

   **Windows example (this may require that you run the command prompt as an administrator)**
   
   arp -s 192.168.0.125 00-40-8c-18-10-00
   ping -l 408 -t 192.168.0.125

4. Check that the network cable is connected and then restart the product by disconnecting and reconnecting power.
AXIS M3025–VE Network Camera

System Options

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

Note

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

AXIS Video Hosting System (AVHS)

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

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

One-click enabled – Press and hold the product’s control button (see Hardware Overview on page 6) for about 3 seconds to connect to an AVHS service over the Internet. Once registered, Always will be enabled and the Axis product stays connected to the AVHS service. If the product is not registered within 24 hours from when the button is pressed, the product will disconnect from the AVHS service.

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

AXIS Internet Dynamic DNS Service

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

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

Note

AXIS Internet Dynamic DNS Service requires IPv4.

Advanced TCP/IP Settings

DNS Configuration

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

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

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

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

Primary/Secondary DNS server – Enter the IP addresses of the primary and secondary DNS servers. The secondary DNS server is optional and will be used if the primary is unavailable.
AXIS M3025–VE 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 HTTPS on page 38.

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<sup>TM</sup>.
- In this context, router refers to any network routing device such as a NAT router, Network router, Internet Gateway, Broadband router, Broadband sharing device, or a software such as a firewall.

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

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

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

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

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

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

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

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

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

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

The following traps are available:
- Cold start
- Warm start
- Link up
- Authentication failed

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 38. 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 49.

**UPnP™**

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

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

**RTP/H.264**

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

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

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

**Bonjour**

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

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

SD Card

Notice

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

Note

For SD card recommendations see www.axis.com

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

The following SD card file systems are supported:

- ext4 — recommended due to its resilience against data loss if the card is ejected or if there is abrupt power loss. To access data stored on the card from the Windows operating system, a third-party ext4 driver or application is required.
- vFAT — supported by most operating systems for personal computers.

The SD card is managed on the System Options > Storage page. Click SD Card to open Storage Management.

If the card’s status shows as failed, click Check disk to see if the problem can be found and then try Repair. This option is only available for SD cards with ext4. For SD cards with vFAT, use a card reader or computer to troubleshoot the card.

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

To stop writing to the card and protect recordings from being removed, select Lock under General Settings.

Mount and Unmount SD Card

Notice

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

The SD card is automatically mounted when the card is inserted into the Axis product or when the product is started. A manual mount is only required if the card has been unmounted and not ejected and re-inserted.

To unmount the SD card:

1. Open the Axis product’s webpages and go to Setup > System Options > Storage.
2. Click SD Card.
3. Click Unmount.
4. The card can now be removed.

Format SD Card

Notice

Formatting the SD card will remove all data and recordings stored on the card.

Important

If autoformat is enabled, only use new or empty SD cards. Any data stored on the card will be lost when the card is inserted into the Axis product.

An SD card inserted into the product can be manually formatted to one of the supported file systems. To manually format the SD card, follow these steps:
AXIS M3025–VE Network Camera

System Options

1. Insert the SD card in the SD card slot.
2. Open the Axis product's webpages and go to Setup > System Options > Storage.
3. Click SD Card.
4. Click Format and select the desired file system.
5. Click OK to start formatting the card.

Network Share

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

Note

For NAS recommendations see www.axis.com

To add a network share:

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

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

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

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

Ports & Devices

I/O Ports

The Axis product provides one input port and one output port for connection of external devices. For information about how to connect external devices, see Connectors on page 57.

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.
AXIS M3025–VE Network Camera

System Options

Note

A restart clears all entries in the Server Report.

Click Restore to reset most settings to the factory default values. The following settings are not affected:

- the boot protocol (DHCP or static)
- the static IP address
- the default router
- the subnet mask
- the system time
- the IEEE 802.1X settings
- uploaded applications are kept but must be restarted

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 49.

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

For information about firmware upgrade, see Upgrade the Firmware on page 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.

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).


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

Parameter List – Shows the product’s parameters and their current settings. This may prove useful when troubleshooting or when contacting Axis Support.
Connection List – Lists all clients that are currently accessing media streams.

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

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

Advanced

Scripting

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

**NOTICE**
Imperfect 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 49.

For more information, see www.axis.com/developer

File Upload

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

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

Plain Config

Plain Config is for advanced users with experience of Axis product configuration. Most parameters can be set and modified from this page.

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

Reset to Factory Default Settings

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

**Note**
The installation and management software tools are available on the CD supplied with the product and from the support pages on www.axis.com/techsup

To reset the product to the factory default settings:

1. Disconnect power from the product.
2. Press and hold the control button and reconnect power. See Hardware Overview on page 6.
3. Keep the control button pressed for about 15–30 seconds until the status LED indicator flashes amber.
4. Release the control button. The process is complete when the status LED indicator turns green. The product has been reset to the factory default settings. If no DHCP server is available on the network, the default IP address is 192.168.0.90.

5. Using the installation and management software tools, assign an IP address, set the password, and access the video stream. It is also possible to reset parameters to factory default via the web interface. Go to Setup > System Options > Maintenance.
AXIS M3025–VE Network Camera

Troubleshooting

Check the Firmware

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

Upgrade the Firmware

Important

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

Note

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

To upgrade the product's firmware:

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

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

Emergency Recovery Procedure

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

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

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

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

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

2. If the product does not reply in 30 seconds, restart it and wait for a reply. Press CTRL+C to stop Ping.
3. Open a browser and type in the product's IP address. In the page that opens, use the Browse button to select the upgrade file to use. Then click Load to restart the upgrade process.
4. After the upgrade is complete (1–10 minutes), the product automatically restarts and shows a steady green on the Status indicator.
AXIS M3025–VE Network Camera

Troubleshooting

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

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

**Symptoms, Possible Causes and Remedial Actions**

**Problems setting the IP address**

<table>
<thead>
<tr>
<th>When using ARP/Ping</th>
<th>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 Assign IP Address Using ARP/Ping on page 41.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The product is located on a different subnet</td>
<td>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.</td>
</tr>
</tbody>
</table>
| The IP address is being used by another device | Disconnect the Axis product from the network. Run the Ping command (in a Command/DOS window, type ping and the IP address of the product):
  * If you receive: Reply from <IP address>: bytes=32; time=10...
    this means that the IP address may already be in use by another device on the network. Obtain a new IP address from the network administrator and reinstall the product.
  * If you receive: Request timed out, this means that the IP address is available for use with the Axis product. Check all cabling and reinstall the product. |
| Possible IP address conflict with another device on the same subnet. | The static IP address in the Axis product is used before the DHCP server sets a dynamic address. This means that if the same default static IP address is also used by another device, there may be problems accessing the product. |

**The product cannot be accessed from a browser**

<table>
<thead>
<tr>
<th>Cannot log in</th>
<th>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 http or https in the browser’s address field.</th>
</tr>
</thead>
</table>
| The IP address has been changed by DHCP | IP addresses obtained from a DHCP server are dynamic and may change. If the IP address has been changed, use AXIS IP Utility or AXIS Camera Management to locate the product on the network. Identify the product using its model or serial number, or by the DNS name (if the name has been configured).

If required, a static IP address can be assigned manually. For instructions, see the 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. |
| Certificate error when using IEEE 802.1X | For authentication to work properly, the date and time settings in the Axis product should be synchronized with an NTP server. See Date & Time on page 40. |

**The product is accessible locally but not externally**

<table>
<thead>
<tr>
<th>Router configuration</th>
<th>To configure your router to allow incoming data traffic to the Axis product, enable the NAT-traversal feature which will attempt to automatically configure the router to allow access to the Axis product, see NAT traversal (port mapping) for IPv4 on page 43. The router must support UPnP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall protection</td>
<td>Check the Internet firewall with your network administrator.</td>
</tr>
<tr>
<td>Default routers required</td>
<td>Check if you need to configure the router settings from System Options &gt; Network &gt; TCP/IP &gt; Basic.</td>
</tr>
</tbody>
</table>
## Troubleshooting

### Problems with streaming H.264

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problems with AXIS Media Control (Internet Explorer only)</td>
<td>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.</td>
</tr>
<tr>
<td>No H.264 displayed in the client</td>
<td>Check that the relevant H.264 connection methods and correct interface are enabled in the AMC Control Panel (streaming tab). See AXIS Media Control (AMC) on page 12. In the AMC Control Panel, select the H.264 tab and click Set to default H.264 decoder. Check that RTSP is enabled under System Options &gt; Network &gt; TCP/IP &gt; Advanced.</td>
</tr>
<tr>
<td>Multicast H.264 only accessible by local clients</td>
<td>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.</td>
</tr>
<tr>
<td>No multicast H.264 displayed in the client</td>
<td>Check with your network administrator that the multicast addresses used by the Axis product are valid for your network. Check with your network administrator to see if there is a firewall preventing viewing.</td>
</tr>
<tr>
<td>Installation of additional ActiveX component restricted or prohibited</td>
<td>Configure the Axis product to use a Java applet for updating video images in your browser. Go to Setup &gt; Live View Config and select Java applet under Default viewer.</td>
</tr>
<tr>
<td>Poor rendering of H.264 images</td>
<td>Ensure that your graphics card is using the latest driver. The latest drivers can usually be downloaded from the manufacturer’s website.</td>
</tr>
<tr>
<td>Color saturation is different in H.264 and Motion JPEG Lower frame rate than expected</td>
<td>Modify the settings for your graphics adapter. Refer to the adapter’s documentation for more information. See Performance Considerations on page 58. Reduce the number of applications running on the client computer. Limit the number of simultaneous viewers. Check with the network administrator that there is enough bandwidth available. Check in the AMC Control Panel (H.264 tag) that video processing is NOT set to Decode only key frames. Lower the image resolution. The maximum frames per second is dependent on the utility frequency (60/50 Hz) of the Axis product. See Technical Specifications on page 55.</td>
</tr>
</tbody>
</table>

### Video and image problems, general

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image unsatisfactory</td>
<td>Check the video stream and camera settings under Setup &gt; Video &gt; Video Stream and Setup &gt; Video &gt; Camera Settings.</td>
</tr>
<tr>
<td>Disturbed focus</td>
<td>Set the focus manually by turning the focus ring. See Hardware Overview on page 6</td>
</tr>
</tbody>
</table>

### Motion Detection triggers unexpectedly

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changes in luminance</td>
<td>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.</td>
</tr>
</tbody>
</table>
Storage and disk management problems

<table>
<thead>
<tr>
<th>Problem</th>
<th>Description and Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage disruption</td>
<td>A storage disruption alarm is sent if a storage device is unavailable, removed, full, locked or if other read or write problems occur. To identify the source of the problem, check the System Log under System Options &gt; Support &gt; Logs &amp; Reports. Depending on the problem, it might be necessary to re-mount the storage device. For information on how to set up a storage disruption alarm, see Events on page 31.</td>
</tr>
<tr>
<td>Video cannot be recorded</td>
<td>Check that the SD card is not write protected (that is, read only).</td>
</tr>
<tr>
<td>SD card cannot be mounted</td>
<td>Reformat the SD card and then click Mount. Formatting the card will remove all content, including all recordings, from the SD card.</td>
</tr>
</tbody>
</table>

Problem Retrieving Additional Video Streams

- ‘Video Error’ displayed in AXIS Camera Companion
- ‘503 service unavailable’ error in IE / AMC or Quick Time
- ‘Camera not available’ displayed in AXIS Camera Station
- ‘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

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.

Stream 0: Max resolution – 1920x1080, fixed, cannot be configured for lower resolutions
Stream 1: 1920x1080, 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

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.

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
# AXIS M3025–VE Network Camera

## Technical Specifications

### Function/group | Item | Specifications
--- | --- | ---
**Camera** | Model | AXIS M3025–VE: 2MP/HDTV 1080p
 | Image sensor | 1/2.7" progressive scan RGB CMOS
 | Lens | M12 mount, fixed iris, megapixel resolution, IR corrected 3.6 mm, F2.0
 |  | Horizontal angle of view: 91°
 |  | Vertical angle of view: 49°
 |  | Diagonal angle of view: 108°
 | Day and night | Automatically removable infrared-cut filter
 | Minimum illumination | Color: 0.8 - 100000 lux, F2.0; B/W: 0.16 lux, F2.0
 | Shutter time | 1/8000 to 1/6 s
 | Camera angle adjustment | Pan: +/-175°
 |  | Rotation: +/-175°
 |  | Tilt: 70°

### Video

| Video compression | H.264 Main Profile (MPEG-4 Part 10/AVC)
| Resolutions | 1920x1080 (HDTV 1080p) to 320x240
| Frame rate H.264 | 25/30 fps with power line frequency 50/60 Hz
| Video streaming | Multiple, individually configurable streams in H.264 and Motion JPEG. Controllable frame rate and bandwidth VBR/CBR H.264
| Pan/Tilt/Zoom | Digital PTZ
| Image settings | Compression, color, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, wide dynamic range – dynamic contrast, mirroring of images
|  | Rotation: 0°, 90°, 180°, 270°, including Corridor Format, text and image overlay, privacy mask

### Network

| Security | Password protection, IP address filtering, IEEE 802.1X* network access control, HTTPS* encryption, digest authentication, user access log.
|  | *This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (www.openssl.org/), and cryptographic software written by Eric Young (eay@cryptsoft.com)
| Supported protocols | IPv4/v6, HTTP, HTTPS*, SSL/TLS*, QoS Layer 3 DiffServ, FTP, SMTP, Bonjour, UPnP, SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS. *This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (www.openssl.org/), and cryptographic software written by Eric Young (eay@cryptsoft.com)
## Technical Specifications

<table>
<thead>
<tr>
<th>Function/group</th>
<th>Item</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Integration</strong></td>
<td><strong>Application Programming Interface</strong></td>
<td>Open API for software integration, including the ONVIF specification available at <a href="http://www.onvif.org">www.onvif.org</a>, VAPIX® and AXIS Camera Application Platform from Axis Communications, specifications available at <a href="http://www.axis.com">www.axis.com</a>, AXIS Media Control SDK*, event trigger data in video stream Quality of Service (QoS) layer 3, DiffServ Model Embedded Linux operating system</td>
</tr>
<tr>
<td><strong>Intelligent video</strong></td>
<td></td>
<td>Video motion detection, active tampering alarm Support for AXIS Camera Application Platform enabling installation of additional applications</td>
</tr>
<tr>
<td><strong>Event Triggers</strong></td>
<td></td>
<td>Intelligent video, edge storage events, external input</td>
</tr>
<tr>
<td><strong>Event Actions</strong></td>
<td></td>
<td>File upload via FTP, HTTP, network share and email; notification via email, HTTP and TCP; pre- and post-alarm video buffering; video recording to edge storage; external output activation</td>
</tr>
<tr>
<td><strong>Video access from web browser</strong></td>
<td></td>
<td>Camera live view Video recording to file (ASF) Customizable HTML pages Windows Vista, XP, Windows 7, 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></td>
</tr>
<tr>
<td><strong>Built-in aids in software</strong></td>
<td></td>
<td>Pixel counter</td>
</tr>
<tr>
<td><strong>Data Streaming</strong></td>
<td></td>
<td>Event data</td>
</tr>
</tbody>
</table>
## Technical Specifications

<table>
<thead>
<tr>
<th>Function/group</th>
<th>Item</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Casing</td>
<td>IP66- and NEMA 4X-rated, IK10 impact-resistant aluminum casing with transparent, polycarbonate cover and dehumidifying membrane</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encapsulated electronics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Captive screws (Torx 10)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Color: White NCS S 1002-B</td>
</tr>
<tr>
<td>Memory</td>
<td>Memory</td>
<td>256 MB RAM, 128 MB Flash</td>
</tr>
<tr>
<td>Power</td>
<td>Power</td>
<td>Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 2, max 3.2 W</td>
</tr>
<tr>
<td>Connectors</td>
<td>Connectors</td>
<td>Male RJ45 10BASE-T/100BASE-TX PoE on a 2 m (6.6 ft.) network cable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Terminal block for 1 alarm input and 1 output</td>
</tr>
<tr>
<td>Edge storage</td>
<td>Edge storage</td>
<td>MicroSD/SDHC/SDXC slot supporting memory card up to 64 GB (card not included)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Support for recording to dedicated network-attached storage (NAS)</td>
</tr>
<tr>
<td>Operating conditions</td>
<td>Operating conditions</td>
<td>Humidity 10 – 100% RH (condensing)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-30°C to 50°C (-22°F to 122°F)</td>
</tr>
<tr>
<td>Approvals</td>
<td>Approvals</td>
<td>EN 55022 Class B, EN 55024, EN 61000-6-1 and EN 61000-6-2, FCC Part 15 Subpart B Class B, ICES-003 Class B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VCCI Class B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AS/NZS CISPR 22 Class B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KCC KN22 Class B, KN24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IEC/EN/UL 60950-22</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IEC 60529 IP66, NEMA 250 Type 4X, IEC 62262 IK10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EN 50581</td>
</tr>
<tr>
<td>Dimensions</td>
<td>Dimensions</td>
<td>(Diameter x Height)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>92 mm x 132 mm (3.6 x 5.1 in)</td>
</tr>
<tr>
<td>Weight</td>
<td>Weight</td>
<td>840 g (13.6 lb.)</td>
</tr>
<tr>
<td>Included</td>
<td>Included accessories</td>
<td>Drill hole template, Installation Guide, Installation and Management Software CD, Windows decoder 1-user license, Torx L-key, terminal block connector</td>
</tr>
<tr>
<td>accessories</td>
<td></td>
<td>Video management software</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AXIS Camera Companion (included), AXIS Camera Station and video management software from Axis' Application Development Partners (not included). See <a href="http://www.axis.com/products/video/software">www.axis.com/products/video/software</a></td>
</tr>
</tbody>
</table>

### Connectors

#### I/O connector

4-pin terminal block for:

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

<table>
<thead>
<tr>
<th>Function</th>
<th>Pin</th>
<th>Notes</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 V DC (-)</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DC output</td>
<td>2</td>
<td>Can be used to power auxiliary equipment. Note: This pin can only be used as power out.</td>
<td>12 V DC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max load = 15 mA</td>
<td></td>
</tr>
</tbody>
</table>
AXIS M3025–VE Network Camera

Technical Specifications

<table>
<thead>
<tr>
<th>Digital Input</th>
<th>3</th>
<th>Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.</th>
<th>0 to max 30 V DC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Output</td>
<td>4</td>
<td>Connected to pin 1 when activated, floating (unconnected) when deactivated. If used with an inductive load, e.g. a relay, a diode must be connected in parallel with the load, for protection against voltage transients.</td>
<td>0 to max 30 V DC, open drain, 100 mA</td>
</tr>
</tbody>
</table>

SD Card Slot

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

Performance Considerations

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

The following factors are among the most important to consider:

- High image resolution and/or lower compression levels result in images containing more data. Bandwidth affected.
- Access by large numbers of Motion JPEG and/or unicast H.264 clients. Bandwidth affected.
- Simultaneous viewing of different streams (resolution, compression) by different clients. Effect on frame rate and bandwidth.
- Accessing Motion JPEG and H.264 video streams simultaneously. Frame rate and bandwidth affected.
- Heavy usage of event settings affect the product’s CPU load. Frame rate affected.
- Heavy network utilization due to poor infrastructure. Bandwidth affected.
- Viewing on poorly performing client computers lowers perceived performance. Frame rate affected.
RUNNING MULTIPLE ACAP APPLICATIONS SIMULTANEOUSLY MAY AFFECT PERFORMANCE.