About this Document
This manual is intended for administrators and users of AXIS Q3709-PVE
Network Camera, and is applicable to firmware 5.75 and later. It
includes instructions for using and managing the product on your
network. Previous experience of networking will be of use when using
this product. Some knowledge of UNIX or Linux-based systems may
also be useful when developing shell scripts and applications. Later
versions of this document will be posted at www.axis.com. See also the
product’s online help, available through the web-based interface.

Legal Considerations
Video 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/apls). The source code is available from

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, ARTEC 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 WWWW are registered trademarks of the respective holders.
Java and all Java-based trademarks and logos are trademarks or
registered trademarks of Oracle and/or its affiliates. UPnP® is a
certification mark of the UPnP Implementers Corporation.

Regulatory Information
Europe
This product complies with the applicable CE marking directives and
harmonized standards:
  Electromagnetic Compatibility (EMC) on page 2.
• Restrictions of Hazardous Substances (RoHS) Directive 2011/65/EU.
  See Disposal and Recycling on page 3.

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

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

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

Canada
This digital apparatus complies with CAN ICES-3 (Class A). The product
shall be connected using a shielded network cable (STP) that is
properly grounded. Cet appareil numérique est conforme à la norme
NMB ICES-3 (classe A). Le produit doit être connecté à l’aide d’un câble
réseau blindé (STP) qui est correctement mis à la terre.

Europe
This digital equipment fulfills the requirements for RF emission
according to the Class A limit of EN 55022. The product shall be
connected using a shielded network cable (STP) that is properly
grounded. Notice! This is a Class A product. In a domestic environment
this product may cause RF interference, in which case the user may be
required to take adequate measures.
This product fulfills the requirements for emission and immunity
according to EN 50121-4 and IEC 62336-4 railway applications.
This product fulfills the requirements for immunity according to
EN 61000-6-1, EN 61000-6-2 and EN 61000-6-3.

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

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

Korea
이 기기는 업무용(A급) 전자파적합기로서 판매자 또는 사
용자는 이 점을 주의하시기 바랍니다. 가정외의 지역에서 사용
하는 것을 목적으로 합니다. 적절히 접지된 STP (shielded
twisted pair) 케이블을 사용하여 제품을 연결 하십시오.

Safety
This product complies with IEC/EN/UL 60950-1 and
IEC/EN/UL 60895-2, Safety of Information Technology
Equipment. The product shall be grounded either through a shielded
network cable (STP) or other appropriate method.
The power supply used with this product shall fulfill the requirements
for Safety Extra Low Voltage (SELV) and Limited Power Source (LPS)
according to IEC/EN/UL 60895-1.
Battery
Low battery power affects the operation of the RTC, causing it to reset at every power-up. When the battery needs replacing, a log message will appear in the product’s server report. For more information about the server report, see the product’s setup pages or contact Axis support.

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

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

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

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

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

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

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

Contact Information
Axis Communications AB
Emdlåvägen 14
223 69 Lund
Sweden
Tel: +46 46 272 18 00
Fax: +46 46 13 61 30
www.axis.com

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

Learn More!
AXIS Q3709-PVE Network Camera

Safety Information

Safety Information

Hazard Levels

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

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

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

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

Other Message Levels

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

**Note**
Indicates useful information which helps in getting the most out of the product.
# Table of Contents

Safety Information ................................................. 4  
Hazard Levels .................................................. 4  
Other Message Levels ......................................... 4  

Hardware Overview .............................................. 7  
Weather Shield .................................................. 7  
Connectors and Buttons ........................................ 8  
LED Indicators .................................................. 8  

Access the Product ............................................... 9  
Access from a Browser ......................................... 9  
Access from the Internet ....................................... 10  
Set the Root Password ......................................... 10  
Set Power Line Frequency ..................................... 10  
Configure Capture Mode ....................................... 10  
The Live View Page ............................................. 12  
Channel Configuration ......................................... 12  

Media Streams ................................................... 14  
How to Stream H.264 .......................................... 14  
MJPEG .......................................................... 14  
AXIS Media Control (AMC) ................................... 14  
Alternative Methods of Accessing the Video Stream .......... 15  

Set Up the Product ............................................... 16  
Basic Setup .................................................... 16  

Video .......................................................... 17  
Set Up Video Streams ......................................... 17  
Stream Profiles ................................................ 18  
Camera Settings ............................................... 18  
Align the Channel Images .................................... 20  
View Area ..................................................... 20  
Overlay ......................................................... 21  
Privacy Mask .................................................. 23  

Configure the Live View Page ................................. 24  

PTZ (Pan Tilt Zoom) ........................................... 26  
Preset Positions ............................................... 26  
Advanced ....................................................... 26  
Control Queue ................................................ 27  

Detectors ......................................................... 28  
Camera Tampering ............................................. 28  
Motion Detection .............................................. 28  

Applications ...................................................... 31  
Application Licenses ......................................... 31  
Upload Application .......................................... 31  
Application Considerations .................................. 31  

Events .......................................................... 33  
Set Up Action Rules ........................................... 33  
Add Recipients ............................................... 35  
Create Schedules ............................................. 37  
Set Up Recurrences .......................................... 37  

Recordings ....................................................... 38  
Find Recordings ................................................. 38  
Play Recording ................................................ 39  
Export Video Clip ............................................. 39  
Continuous Recording ....................................... 39  

Languages ........................................................ 40  

System Options .................................................. 41  
Security ........................................................ 41  
Date & Time .................................................... 43  
Network ......................................................... 44  
Storage ........................................................ 49  
Maintenance ................................................... 49  
Support ........................................................ 50  
Advanced ....................................................... 51
## Table of Contents

- Reset to Factory Default Settings ........................................... 51
- **Troubleshooting** .......................................................... 52
  - Check the Firmware ....................................................... 52
  - Upgrade the Firmware .................................................... 52
  - Symptoms, Possible Causes and Remedial Actions .................. 53
- **Technical Specifications** ............................................... 56
- Performance Considerations ............................................... 57
AXIS Q3709-PVE Network Camera

Hardware Overview

Hardware Overview

1 Dome cover
2 Ground screw
3 Hook for safety wire
4 Part number (P/N) & Serial number (S/N)
5 Network connector
6 Unit holder (3x)
7 Status LED indicator
8 Control button
9 Restart button

Weather Shield

1 Weather shield (top)
AXIS Q3709-PVE Network Camera

Hardware Overview

2  Slot for removing Weather shield (bottom)
3  Weather shield (bottom)

Connectors and Buttons

For technical specifications, see page 56.

Network Connector

RJ45 with High Power over Ethernet (High 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.

Control Button

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

The control button is used for:

- Resetting the product to factory default settings. See .
- Connecting to an AXIS Video Hosting System service. See page 45. 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 45. To connect, press and hold the button for about 3 seconds.

Restart Button

Press the restart button to restart the product.

LED Indicators

**Note**

- 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.

<table>
<thead>
<tr>
<th>Status LED</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlit</td>
<td>Connection and normal operation.</td>
</tr>
</tbody>
</table>
| Green      | Shows steady green for 10 seconds for normal operation after startup completed.  
            | Flashes before startup if the temperature is below -20 °C and heating is required. The product starts when it reaches operating temperature. |
| Amber      | Steady during startup. Flashes during firmware upgrade. |
| Amber/Red  | Flashes amber/red if network connection is unavailable or lost. |
AXIS Q3709-PVE Network Camera

Access the Product

Access the Product

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

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

- Internet Explorer® 10 or later versions with Windows®
- Safari® with OS X®
- Chrome™ with other operating systems.

See Technical Specifications on page 56.

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

The Axis product includes three (3) 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

Note

- The Axis product can be accessed through any of its three IP addresses.
- Login is required for each of the three channels separately.

1. Start a web browser.

2. Enter the IP address or host name of the Axis product in the browser’s Location/Address field.

   Any of the three IP addresses will provide access to the product

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

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

Note

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

3. Enter your user name and password. If this is the first time the product is accessed, the root password must first be configured. For instructions, see Set the Root Password on page 10.

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 47. 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 42.

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 .

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 51) 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.

Configure Capture Mode

Capture mode defines the maximum resolution and maximum frame rate available in the Axis product. The capture mode setting also affects the camera’s angle of view.

Select the desired capture mode from the drop-down list and click OK.

The 5 MP capture modes offer an image quality with less noise.

See also Capture Mode on page 18.
AXIS Q3709-PVE Network Camera

Access the Product

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

Controls on the Live View Page

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

Select a stream profile for the Live View page from the Stream Profile drop-down list. For information about how to configure stream profiles, see page 18.

The Manual Trigger button is used to trigger an action rule from the Live View page. For information about how to configure and enable the button, see Manual Trigger on page 11.

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

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

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

Click Divider to display partition lines between the images. This can be useful for instance when identifying potential blind spots between the images during installation.

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 33.

To show the manual trigger buttons in the Live View page:
AXIS Q3709-PVE Network Camera

Access the Product

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 14 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.
- Click the View Full Screen button and the video image will fill the entire screen. Press ESC (Escape) on the computer keyboard to cancel full screen view.
- The Record button is used to record the current video stream on your computer. The location where the recording is saved can be specified in the AMC Control Panel. Enable this button from Live View Config > Viewer Settings.

PTZ Controls

Note

These controls are available if digital PTZ is enabled in the selected view area, see View Area on page 20.

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

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

To view a specific view area or preset position, select it from the Source list. When view areas are disabled the source list includes options for the different channels (left, center, right) as well as the full panorama view.

The three buttons represent the different channels, left, center and right.

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

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

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

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

Channel Configuration

Where applicable, the Axis product enables individual setup for the different channels; Left Channel, Center Channel and Right Channel.
AXIS Q3709-PVE Network Camera

Access the Product

On pages, such as View Areas, Privacy Masks and Motion Detection the channels are represented by tabs, on which the individual settings are made.

Settings, such as Overlay settings, Image Appearance and White Balance, can be expanded or collapsed to enable individual or common configuration respectively. To expand the settings for the individual channels select Expand all channels above the current setting.

Manual IPv4 Address or Host Name Configuration and UPnP™ Settings require individual input for each channel. For these settings all channels are presented on the page by default.
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:

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

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

- **Still JPEG images in a browser.** Enter the path http://<ip>/axis-cgi/jpg/image.cgi?camera=<source no>

- **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: axrtptu://<ip>/axis-media/media.amp?camera=<source no>
  - Unicast via RTSP: axrtsp://<ip>/axis-media/media.amp?camera=<source no>
  - Unicast via RTSP, tunneled via HTTP: axrtsphttp://<ip>/axis-media/media.amp?camera=<source no>
  - Multicast: axrtpm://<ip>/axis-media/media.amp?camera=<source no>

- **QuickTime™.** The following paths can be used:
  - rtsp://<ip>/axis-media/media.amp?camera=<source no>
  - rtsp://<ip>/axis-media/media.3gp?camera=<source no>

**Note**
- `<ip>` = IP address
- `<source no>` = video source number
- 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.
Set Up the Product

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

- **Administrators** have unrestricted access to all settings.
- **Operators** have restricted access to settings, see *Users on page 41*

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 41*.
2. TCP/IP. See *page 44*.
3. Date & Time. See *page 43*.
4. Video Stream. See *page 17*.

The Basic Setup menu can be disabled from *System Options > Security > Users*. 
AXIS Q3709-PVE Network Camera

Video

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

- Video stream. See page 17.
- Stream profiles. See page 18.
- Camera settings. See page 18.
- View areas. See page 20.
- Overlay image. See page 21.
- Privacy mask. See page 23.

Set Up Video Streams

To set up the product’s video streams, go to Video > Video Stream.

The video stream settings are divided into the following tabs:

- Image. See page 17.
- MJPEG. See page 18.

Pixel Counter

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

The pixel counter can be used:

- When setting up a video stream, see Set Up Video Streams on page 17. Under Preview, click Open and select the Show pixel counter option to enable the rectangle in the image. Use the mouse to move and resize the rectangle, or enter the number of pixels in the Width and Height fields and click Apply.
- When accessing the Live View page in Internet Explorer with AXIS Media Control (AMC) in Windows. Right-click in the image and select Pixel counter. Use the mouse to move and resize the rectangle.

Image

The default image settings can be configured under Video > 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.
- 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 21.

Click Save to apply the new settings.
AXIS Q3709-PVE Network Camera

Video

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

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

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

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 33.
- When setting up continuous recording. See Continuous Recording on page 39.
- 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.

Capture Mode

Capture mode defines the maximum resolution and maximum frame rate available in the Axis product. A capture mode with a large maximum resolution has a reduced maximum frame rate and vice versa. The capture mode setting also affects the camera’s angle of view as the effective size of the image sensor differs between capture modes.

Capture mode is set the first time the product is accessed. Select the desired capture mode and click OK.
Important
Changing capture mode when the product has been configured is not recommended as most other settings will be either removed or reset.

To change capture mode, follow these steps:

1. Go to Setup > Video > Camera Settings.
2. Select the new capture mode.
3. Click Save.

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

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

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

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

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

White Balance
To change this setting go to Setup > Video > Camera Settings.

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

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

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

Note
This setting is only possible when using automatic exposure control.

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

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

Exposure zones – This setting determines which part of the image is used to calculate the exposure. For most situations, the Auto setting can be used.
You can select a predefined area by defining Include and Exclude windows within the image. Exclude windows exclude areas that are too bright or dark, and Include windows include areas in the scene that have better lighting which will contribute to the exposure data. There must be at least one Include window. There can be a total of ten Include and Exclude windows to tailor the exposure zone. Note that an Exclude window is effective only when placed inside an include window.
Tip: If an area is extremely bright draw an include window to cover the whole area and define Exclude windows within it to block out the bright areas.

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

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

Set **Exposure priority** to

- **Automatic** to set the shutter speed automatically.
- **Low motion blur** to prioritize low motion blur.
- **Low noise** to prioritize low noise.

It is also possible to set the **Min** and **Max** limits for **Shutter** and **Gain**.

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

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

Example

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

**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.

**Align the Channel Images**

The lenses in the Axis product are aligned during production. However fine tuning of the image alignment may be required depending on, for instance, the distances within the scene. Also a larger overlap between the images will guarantee a complete coverage of the whole scene to a larger extent.

To set the individual image alignment for each channel go to **Setup > Video > Capture Alignment** and use the **LEFT/RIGHT** and **UP/DOWN** buttons or enter a value in pixels directly.

**View Area**

A view area is a cropped part of the full view. Each view area is treated as a video source in **Live View** and has its own video stream and P/T/Z 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 Areas.

To add a new view area:
1. Go to Video > View Area.
2. Click Add.
3. The new view area appears under Selected view area. Enter a descriptive name in the Name field.
4. Select an Aspect ratio and a Video stream resolution.
5. A new view area covers the whole image. Use the mouse to move and resize the view area.
6. Select Enable PTZ to enable digital PTZ for the view area.
7. Click Save to save the settings.

To modify a view area, select the view area in the list and modify the settings as required. Click Save.

To remove a view area, select the view area and click Remove.

Note

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

Overlay

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

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

When using a text string, modifiers can be used to display information such as the name of the current week or month.

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

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

Note

To enable overlays:
1. Go to Video > 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 43.
Overlay Image

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

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

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

For more information about privacy masks, see Privacy Mask on page 23.

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.
     
     For more examples of hexadecimal values, see the online help.
   - To scale the image automatically, select Scale with resolution. The image will be scaled down to fit the resolution used by the Axis product.

5. Click Save.

To select the image to use as overlay:

1. Go to Video > 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 33, 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:
AXIS Q3709-PVE Network Camera

Video

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

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

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

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.

The grey bar on the edge of the image represents a privacy mask in an adjacent video stream and it enables you to align a new privacy mask to the existing one.

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:

- Default Live View Video. See page 18.
- Stream Profile. See page 18.
- Default Viewer for Browser. See page 24.
- Viewer Settings. See page 24.
- Action Buttons. These are the buttons described in Controls on the Live View Page on page 11.
- User Defined Links. See page 25.

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>
<tr>
<td></td>
<td>Still image</td>
<td>Displays still images only. Click the Refresh button in your browser to view a new image.</td>
</tr>
<tr>
<td>Other browsers</td>
<td>Server Push</td>
<td>Recommended viewer for other browsers (Motion JPEG).</td>
</tr>
<tr>
<td></td>
<td>QuickTime</td>
<td>H.264.</td>
</tr>
<tr>
<td></td>
<td>Still image</td>
<td>Displays still images only. Click the Refresh button in your browser to view a new image.</td>
</tr>
</tbody>
</table>

For more information, please see the online help 📌.

Viewer Settings

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

- Select Show viewer toolbar to display the AXIS Media Control (AMC) or the QuickTime viewer toolbar under the video image in your browser.
- H.264 decoder installation. The administrator can disable installation of the H.264 decoder included with AXIS Media Control. This is used to prevent installation of unlicensed copies. Further decoder licenses can be purchased from your Axis reseller.
- Select Show crosshair in PTZ joystick mode to enable a cross that will indicate the center of the image in PTZ joystick mode.
- Select Use PTZ joystick mode as default to enable joystick mode. The mode can be changed temporarily from the PTZ control panel.
- Select Enable recording button to enable recording from the Live View page. This button is available when using the AMC viewer. The recordings are saved to the location specified in the AMC Control Panel. See AXIS Media Control (AMC) on page 14.
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.
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 20.

Preset Positions

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

- Pan and tilt positions
- Zoom position

Each view area has its own preset positions.

Access the Preset Positions

Preset positions can be accessed in several ways:

- By selecting the preset from the Source drop-down list in the Live View Page.
- When setting up action rules. See page 33.

Add a Preset Position

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

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

Set the Home Position

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

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

Advanced

Controls

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

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

The following PTZ controls are enabled by default:
**AXIS Q3709-PVE Network Camera**

**PTZ (Pan Tilt Zoom)**

- Pan control
- Tilt control
- Zoom control

To disable specific controls, deselect the options under **Enable/Disable controls**.

If using multiple view areas, deselecting a control will only disable the control in the selected view area.

**Note**

Disabling PTZ controls will not affect preset positions. For example, if the tilt control is disabled, the product can still move to preset positions that require a tilt movement.

**Control Queue**

**Note**

- The administrator can enable and disable PTZ controls for selected users.
- To identify different users in the viewer group, cookies must be enabled on the client.
- The Control queue polltime is measured in seconds. For more information see the online help.

The administrator can set up a queue for PTZ controllers from **PTZ > Control Queue**. Once set up, the PTZ Control Queue buttons appear in the Live View page offering one viewer exclusive control for a limited period of time. Other users will be placed in queue.

A user who belongs to a group (see **Users** on page 41) with a higher PTZ priority can go before other users in the queue and take control of the product. The order of priority is as follows:

1. **Administrator** — An administrator takes over PTZ control regardless of who is first in queue. The administrator will be removed from the queue 60 seconds after the last PTZ control command.

2. **Event** — The Axis product can be configured to go to a preset position when triggered by an alarm (see **Events** on page 33). The event will immediately be placed first in the queue except when an administrator is in control.

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

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

Camera Tampering

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

To configure tampering detection:

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

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

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

Note

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

For more information on actions rules, see Events on page 33.

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 29.

To control the number of motion detection alarms, the parameters Object Size, History and Sensitivity can be adjusted. See Motion Detection Parameters on page 29.

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 33.
AXIS Q3709-PVE Network Camera

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 a desired resolution for viewing while setting up Motion Detection from the View in list.
3. Select the Configure Included Windows option and click New. Select the new window in the list of windows and enter a descriptive name.
4. 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.
5. 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.
6. 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 Q3709-PVE 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

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

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

**Application Licenses**

Some applications need a license to run. Licenses can be installed in two ways:
- Automatic installation — requires access to the Internet
- Manual installation — obtain the license key from the application vendor and upload the key to the Axis product

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

An application license is valid for one channel. Additional licenses must be obtained in order to run an application on multiple channels.

**Upload Application**

To upload and start an application:

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

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

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

**Application Considerations**

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

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

If the Axis product is restarted, running applications will restart automatically.
AXIS Q3709-PVE Network Camera

Applications

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

If the Axis product is reset to factory default, uploaded applications and their settings are removed. For information about factory default, see .
Events

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

Set Up Action Rules

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

For more information about available triggers and actions, see Triggers on page 33 and Actions on page 34.

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 29.
2. Go to System Options > Storage and set up the network share. See page 49.

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.

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 31.
- Detectors
AXIS Q3709-PVE Network Camera

Events

- **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 28*.
- **Tampering** – Trigger the rule when tampering is detected. See *Camera Tampering on page 28*.

- **Hardware**
  - **Fan** – Trigger the rule if the fan is malfunctioning. This can for example be used to send maintenance notifications.
  - **Network** – Trigger the rule if network connection is lost or restored.
  - **Temperature** – Trigger the rule if the temperature falls outside or inside the operating range of the product. This can for example be used to send maintenance notifications.

- **Input Signal**
  - **Manual Trigger** – Trigger the rule using the Manual Trigger button in the Live View page. See *Controls on the Live View Page on page 11*. This can for example be used to validate actions during product installation and configuration.
  - **Virtual Inputs** – can be used by a VMS (Video Management System) to trigger actions. Virtual inputs can, for example, be connected to buttons in the VMS user interface.

- **PTZ**
  - **Moving** – Trigger the rule when the camera view moves due to a PTZ operation. This can for example be used as an additional condition to prevent an action rule triggered by motion detection to record video while the camera view moves due to a PTZ operation.
  - **Preset Reached** – Trigger the rule when the camera stops at a preset position. This can be for example be used with the Send Images action to upload images from the preset position.

- **Storage**
  - **Disruption** – Trigger the rule if storage problems are detected, for example if the storage device is unavailable, removed, full, locked or if other read or write problems occur. This can for example be used to send maintenance notifications.
  - **Recording** – Triggers the rule when the Axis product records to the storage device. The recording status trigger can be used to notify the operator, for example by flashing LED lights, if the product has started or stopped to record to the storage device. Note that, this trigger can be used only for edge storage recording status.

- **System**
  - **System Ready** – Trigger the rule when the product has been started and all services are running. This can for example be used to send a notification when the product restarts.

- **Time**
  - **Recurrence** – Trigger the rule periodically. See *Set Up Recurrences on page 37*. 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 37*.

Actions

Available actions include:
AXIS Q3709-PVE Network Camera

Events

- **Day/Night Vision Mode** – Set day mode (IR cut filter on) or night mode (IR cut filter off).
- **Overlay Text** – Display an overlay text. See *Use Overlay Text in an Action Rule on page 22.*
- **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 Notification** – Send a notification message to a recipient.
- **Send SNMP Trap** – Send an SNMP trap message to the operator. Make sure that SNMP is enabled and configured under System Options > Network > SNMP.
- **Send Video Clip** – Send a video clip to a recipient.
- **Status LED** – Flash the LED indicator. This can for example be used to validate triggers such as motion detection during product installation and configuration.

**Add Recipients**

The product can send media files and messages to notify users about events. Before the product can send media files or notification messages, you must define one or more recipients. For information about available options, see *Recipient Types on page 35.*

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>
</table>
| Email     | Send Images
           | Send Notification
           | Send Video Clip                   | An email recipient can contain multiple email addresses. |
| FTP       | Send Images
           | Send Video Clip                   |                                                |
**AXIS Q3709-PVE Network Camera**

**Events**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Recipient Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFTP</td>
<td>Send Images, Send Video Clip</td>
<td>Encrypted file transfer using SSH File Transport Protocol (SFTP). SFTP is a more secure method than FTP but file transfer might be slower, especially for large files such as high resolution video. Specify login information for the SFTP server and the server’s public key MD5 fingerprint (32 hexadecimal digits). The SFTP recipient supports SFTP servers using SSH-2 with RSA and DSA host key types. RSA is the preferred method. To use DSA, disable the RSA key on the SFTP server.</td>
</tr>
<tr>
<td>HTTP</td>
<td>Send Images, Send Notification, Send Video Clip</td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>Send Images, Send Notification, Send Video Clip</td>
<td>Encrypted file transfer using HyperText Transfer Protocol Secure (HTTPS). Specify login information for the HTTPS server and validate the server’s certificate. If there is a proxy between the Axis product and the HTTPS server, also specify the proxy settings.</td>
</tr>
<tr>
<td>Network Share</td>
<td>Send Images, Send Video Clip</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 <em>Storage on page 49</em>.</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 43*. 

36
Events

Create Schedules

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

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.
Recordings

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

- To start a continuous recording, see page 39.
- To set up action rules, see page 33.
- To access recordings, see Find Recordings on page 38.
- To play recordings, see Play Recording on page 39.
- To export a recording as a video clip, see Export Video Clip on page 39.
- To configure camera controlled storage, see Storage on page 49.

Find Recordings

Recordings made to the network share can be accessed from the Recordings > List page. The page lists all recordings and shows each recording’s start date and time, duration and the event that triggered the recording.

The recording list also displays the name of the channel (left, centre, or right) on which the recording was made.

**Note**

The recording’s start date and time is set according to the Axis product’s date and time settings. If the Axis product is configured to use a time zone different from the local time zone, make sure to configure the Recording time filters according to the product’s time zone. Date and time settings are configured under System Options > Date & Time, see Date & Time on page 43.

To find a recording, follow these steps:

1. Go to Recordings > List.
2. To reduce the number of recordings displayed, select the desired options under Filter:
   - **Recording time** – List recordings that started between the From and To times.
   - **Event** – List recordings that were triggered by a specific event. Select continuous to list continuous recordings.
   - **Storage** – List recordings from a specific storage device.
   - **Sort** – Specify how recordings should be sorted in the list.
   - **Results** – Specify the maximum number of recordings to display.
3. To apply the filters, click the Filter button. Some filters may take a long time to complete.
4. The recordings are displayed in the Recording list.

To play a recording, select the recording and click Play. See also Play Recording on page 39.

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

To export a recording or a part of a recording as a video clip, select the recording and click Export. See also Export Video Clip on page 39.

To remove a recording from the storage device, select the recording and click Remove.
AXIS Q3709-PVE Network Camera

Recordings

Play Recording

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

To play a recording, follow these steps:

1. Go to Recordings > List.
2. To reduce the number of recordings displayed, select the desired options under Filter and click the Filter button to apply the filters. See also Find Recordings on page 38.
3. Select the recording and click Play. The recording will be played in a new browser window.

Export Video Clip

Recordings on the network share can be exported as video clips. It is possible to export a complete recording or a part of a recording.

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

To export a video clip, follow these steps:

1. Go to Recordings > List.
2. To reduce the number of recordings displayed, select the desired options under Filter and click the Filter button to apply the filters. See also Find Recordings on page 38.
3. Select the recording and click Export. The Export Recording dialog opens.
4. By default, the complete recording is selected. To export a part of the recording, modify the start and stop times.
5. Optionally, enter a file name for the recording.
6. Click Export.

Note: Recordings can also be exported from the playback window.

Continuous Recording

The Axis product can be configured to continuously save video to a storage device. For information about storage devices, see Storage on page 49. 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.
**AXIS Q3709-PVE Network Camera**

**Languages**

Multiple languages can be installed in the Axis product. All web pages including the online help will be displayed in the selected language. To switch languages, go to Setup > Languages and first upload the new language file. Browse and locate the file and click the Upload Language button. Select the new language from the list and click Save.

**Note**

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

Security

Users

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

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

- **Viewers** have access to the Live View page
- **Operators** have access to all settings except:
  - creating and modifying PTZ presets
  - creating and modifying PTZ control settings
  - creating and modifying privacy mask settings
  - uploading applications and language files
  - any of the settings included in the System Options

- **Administrators** have unrestricted access to all settings. The administrator can add, modify and remove other users.

*Note*

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

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

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

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

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

ONVIF

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

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

IP Address Filter

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

The administrator can add up to 256 IP address entries to the list (a single entry can contain multiple IP addresses).
AXIS Q3709-PVE Network Camera

System Options

HTTPS

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

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

To use HTTPS, an HTTPS certificate must first be installed. Go to System Options > Security > Certificates to install and manage certificates. See Certificates on page 43.

To enable HTTPS on the Axis product:

1. Go to System Options > Security > HTTPS
2. Select an HTTPS certificate from the list of installed certificates.
3. Optionally, click Ciphers and select the encryption algorithms to use for SSL.
4. Set the HTTPS Connection Policy for the different user groups.
5. Click Save to enable the settings.

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

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

IEEE 802.1X

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

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

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

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

To create and install certificates, go to System Options > Security > Certificates. See Certificates on page 43. Many CA certificates are preinstalled.

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

1. Go to System Options > Security > IEEE 802.1X.
2. Select a CA Certificate and a Client Certificate from the lists of installed certificates.
3. Under Settings, select the EAPOL version and provide the EAP identity associated with the client certificate.
4. Check the box to enable IEEE 802.1X and click Save.

*Note*

For authentication to work properly, the date and time settings in the Axis product should be synchronized with an NTP server. See Date & Time on page 43.

42
**AXIS Q3709-PVE Network Camera**

**System Options**

**Certificates**

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

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

**Note**

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

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

To install a self-signed certificate:

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

To create and install a CA-signed certificate:

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

Server/Client certificates can be installed as Certificate from signing request or as Certificate and private key. Select Certificate and private key if the private key is to be uploaded 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 46**.

  If using a host name for the NTP server, a DNS server must be configured. See **DNS Configuration on page 46**.

- **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.

Note
To avoid conflict resulting in lost access to video streams, always configure all channels when assigning static IP addresses manually using IPv4 address configuration, IPv6 address configuration, ARP/Ping, or IP Utility.

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 ) 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 44.

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:
AXIS Q3709-PVE Network Camera

System Options

Linux/Unix syntax

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

Linux/Unix example

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

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

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

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

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

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

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

Note

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

AXIS Video Hosting System (AVHS)

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

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

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

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

AXIS Internet Dynamic DNS Service

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

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

Note

AXIS Internet Dynamic DNS Service requires IPv4.
Advanced TCP/IP Settings

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

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

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

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

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

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

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

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

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

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

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

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

For more information, see the online help.

Link-Local IPv4 Address
Link-Local Address is enabled by default and assigns the Axis product an additional IP address which can be used to access the product from other hosts on the same segment on the local network. The product can have a Link-Local IP and a static or DHCP-supplied IP address at the same time.

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

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

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

To enable HTTPS, go to System Options > Security > HTTPS. For more information, see HTTPS on page 42.
AXIS Q3709-PVE Network Camera

System Options

NAT traversal (port mapping) for IPv4

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

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

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

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

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

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

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

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

FTP

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

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

RTSP

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

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

SOCKS

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

SOCKS is configured under System Options > Network > SOCKS. For more information, see the online help 📖.
QoS (Quality of Service)

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

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

SNMP

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

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

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

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

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

Note

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

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

The following traps are available:

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

Note

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

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

To use SNMP v3, HTTPS must be enabled, see HTTPS on page 42. 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 .

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
AXIS Q3709-PVE Network Camera

System Options

RTP/H.264
The RTP port range and multicast settings are configured under System Options > Network > RTP.
The RTP port range defines the range of ports from which the video ports are automatically selected. For multicast streams, only certain IP addresses and port numbers should be used.
Select Always Multicast Video to start multicast streaming without opening an RTSP session.

Bonjour
The Axis product includes support for Bonjour. Bonjour is enabled by default and the product is automatically detected by operating systems and clients that support this protocol.
Bonjour can be disabled under System Options > Network > Bonjour.

Storage

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

Note
For NAS recommendations see www.axis.com

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

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

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

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

Maintenance

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

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

Note
A restart clears all entries in the Server Report.

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

49
System Options

- 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 .

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 52.

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 52.

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 Axis 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.
Advanced

Scripting

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

**NOTICE**

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

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

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

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

File Upload

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

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

Plain Config

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

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

Reset to Factory Default Settings

**Important**

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

**Note**

The installation and management software tools are available from the support pages on [www.axis.com/techsup](http://www.axis.com/techsup)

To reset the product to the factory default settings:

1. Press and hold the control button and the restart button at the same time.
2. Release the restart button but continue to hold down the control button for 15–30 seconds while the status LED indicator shows steady amber.
3. Release the control button. The process is complete when the status LED indicator turns green. The product has been reset to the factory default settings. If no DHCP server is available on the network, the default IP address is 192.168.0.90.
4. Using the installation and management software tools, assign an IP address, set the password and access the video stream.

It is also possible to reset parameters to factory default via the web interface. Go to **Setup > System Options > Maintenance** and click **Default**.
**AXIS Q3709-PVE 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, wait 10 minutes even if you suspect the upgrade has failed.
- When you upgrade the Axis product with the latest firmware from Axis website, the product receives the latest functionality available. Always read the upgrade instructions and release notes available with each new release before upgrading the firmware.

To upgrade the product’s firmware:

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

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

**Emergency Recovery Procedure**

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

1. In UNIX/Linux, type the following from the command line:
   ```
   arp -s <IP address> <serial number> temp
   ping -l 408 <IP address>
   ```
   In Windows, type the following from a command/DOS prompt (this may require that you run the command prompt as an administrator):
   ```
   arp -s <IP address> <serial number>
   ping -l 408 -t <IP address>
   ```
2. If the product does not reply in 30 seconds, restart it and wait for a reply. Press CTRL+C to stop Ping.
3. Open a browser and type in the product's IP address. In the page that opens, use the Browse button to select the upgrade file to use. Then click Load to restart the upgrade process.
AXIS Q3709-PVE Network Camera

Troubleshooting

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

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

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

Symptoms, Possible Causes and Remedial Actions

<table>
<thead>
<tr>
<th>Problems setting the IP address</th>
<th>Possible IP address conflict with another device on the same subnet.</th>
</tr>
</thead>
<tbody>
<tr>
<td>When using ARP/Ping</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 product is located on a different subnet | 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 | 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>
<tbody>
<tr>
<td>The IP address has been changed by DHCP</td>
<td>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).</td>
</tr>
<tr>
<td>Certificate error when using IEEE 802.1X</td>
<td>For authentication to work properly, the date and time settings in the Axis product should be synchronized with an NTP server. See Date &amp; Time on page 43.</td>
</tr>
<tr>
<td>The browser is not supported</td>
<td>See Access the Product on page 9 for a list of recommended browsers.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The product is accessible locally but not externally</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router configuration</td>
</tr>
<tr>
<td>Firewall protection</td>
</tr>
</tbody>
</table>
**Troubleshooting**

<table>
<thead>
<tr>
<th>Default routers required</th>
<th>Check if you need to configure the router settings from System Options &gt; Network &gt; TCP/IP &gt; Basic.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera and router settings</td>
<td>On the camera go to System Options &gt; Network &gt; Advanced and:</td>
</tr>
<tr>
<td></td>
<td>• Configure DNS servers.</td>
</tr>
<tr>
<td></td>
<td>• Enable dynamic DNS updates.</td>
</tr>
<tr>
<td></td>
<td>• Enter DNS name for each channel (same DNS name for all channels).</td>
</tr>
<tr>
<td></td>
<td>• Enter Alternative HTTP port for each channel (different port numbers).</td>
</tr>
<tr>
<td></td>
<td>• Enable NAT traversal (port mapping) for IPv4.</td>
</tr>
<tr>
<td></td>
<td>On the router:</td>
</tr>
<tr>
<td></td>
<td>• Check that UPnP is enabled.</td>
</tr>
<tr>
<td></td>
<td>• Configure port-forwarding for the Alternative HTTP ports entered on the camera.</td>
</tr>
</tbody>
</table>

### Problems with streaming H.264

<table>
<thead>
<tr>
<th>Problems with AXIS Media Control (Internet Explorer only)</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<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 14.</td>
</tr>
<tr>
<td>In the AMC Control Panel, select the H.264 tab and click Set to default H.264 decoder.</td>
<td>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.</td>
</tr>
<tr>
<td>Check with your network administrator to see if there is a firewall preventing viewing.</td>
<td>Poor rendering of H.264 images</td>
</tr>
<tr>
<td>Color saturation is different in H.264 and Motion JPEG</td>
<td>Modify the settings for your graphics adapter. Refer to the adapter's documentation for more information.</td>
</tr>
<tr>
<td>Lower frame rate than expected</td>
<td>See Performance Considerations on page 57.</td>
</tr>
<tr>
<td>Limit the number of simultaneous viewers.</td>
<td>Check with the network administrator that there is enough bandwidth available.</td>
</tr>
<tr>
<td>Check in the AMC Control Panel (H.264 tag) that video processing is NOT set to Decode only key frames.</td>
<td>Lower the image resolution.</td>
</tr>
<tr>
<td>The maximum frames per second is dependent on the utility frequency (60/50 Hz) of the Axis product. See Technical Specifications on page 56.</td>
<td>Product does not start up</td>
</tr>
</tbody>
</table>
# AXIS Q3709-PVE Network Camera

## Troubleshooting

### Video and image problems, general

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Black image with text indicating inadequate power supply</td>
<td>Check cables and restart power sourcing equipment.</td>
</tr>
<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>Insufficient power</td>
<td>The camera requires a midspan or network switch that supports 30W PoE Class 4. Make sure that the camera is connected to a 30W port on the network switch.</td>
</tr>
</tbody>
</table>

### Motion Detection triggers unexpectedly

<table>
<thead>
<tr>
<th>Issue</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>Issue</th>
<th>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 33.</td>
</tr>
</tbody>
</table>

### Product does not function

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The ambient temperature is too low. Certain hardware functions are suspended.</td>
<td>Wait until the product is sufficiently heated.</td>
</tr>
</tbody>
</table>
**AXIS Q3709-PVE Network Camera**

**Technical Specifications**

### Camera

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image sensor</td>
<td>3 x 1/2.3” progressive scan CMOS</td>
</tr>
<tr>
<td>Lens</td>
<td>3 x lenses, fixed focus, 5.0 mm, F2.8 Combined horizontal angle of view: 180°</td>
</tr>
<tr>
<td>Day and night</td>
<td>Automatically removable infrared-cut filter</td>
</tr>
<tr>
<td>Minimum illumination</td>
<td>Color: 2 lux, F2.8</td>
</tr>
<tr>
<td></td>
<td>B/W: 0.4 lux, F2.8</td>
</tr>
<tr>
<td>Shutter time</td>
<td>1/23250 s to 2/5 s</td>
</tr>
<tr>
<td>Camera angle adjustment</td>
<td>Pan +/- 180°</td>
</tr>
<tr>
<td></td>
<td>Tilt 18°–75°</td>
</tr>
</tbody>
</table>

### Video

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video compression</td>
<td>H.264 (MPEG-4 Part 10/AVC) Baseline, Main and High Profiles</td>
</tr>
<tr>
<td></td>
<td>Motion JPEG</td>
</tr>
<tr>
<td>Resolutions</td>
<td>3 x (3840x2880 to 320x240)</td>
</tr>
<tr>
<td>Frame rate</td>
<td>3 x 4K Ultra HD: Up to 25/30 fps with power line frequency 50/60 Hz</td>
</tr>
<tr>
<td></td>
<td>3 x 11 MP: Up to 16/20 fps with power line frequency 50/60 Hz</td>
</tr>
<tr>
<td></td>
<td>3 x 5 MP (16:9): Up to 25/30 fps with power line frequency 50/60 Hz</td>
</tr>
<tr>
<td></td>
<td>3 x 5 MP (4:3): Up to 16/20 fps with power line frequency 50/60 Hz</td>
</tr>
<tr>
<td>Video streaming</td>
<td>Multiple, individually configurable streams in H.264 and Motion JPEG</td>
</tr>
<tr>
<td></td>
<td>Controllable frame rate and bandwidth</td>
</tr>
<tr>
<td></td>
<td>VBR/CRBR H.264</td>
</tr>
<tr>
<td>Image settings</td>
<td>Compression, Color, Brightness, Sharpness, Contrast, White balance, Exposure control, Exposure zone, Backlight compensation, WDR – dynamic contrast, Fine tuning of behavior at low light, Text and image overlay, Privacy mask, Capture alignment</td>
</tr>
<tr>
<td>Pan/Tilt/Zoom</td>
<td>Digital PTZ, Preset positions, Guard tour</td>
</tr>
</tbody>
</table>

### Network

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Password protection, IP address filtering, HTTPS encryption, IEEE 802.1X network access control, Digest authentication, User access log, Centralized Certificate Management, Cross-Origin Resource Sharing</td>
</tr>
<tr>
<td>Supported protocols</td>
<td>IPv4/IPv6, HTTP, HTTPS*, SSL/TLS*, QoS Layer 3 DiffServ, FTP, CIFS/SMB, SMTP, Bonjour, UPnP™, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, SFTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH</td>
</tr>
</tbody>
</table>

### System Integration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Programming Interface</td>
<td>Open API for software integration, including VAPIX® and AXIS Camera Application Platform; specifications at <a href="http://www.axis.com">www.axis.com</a> ONVIF Profile S, specification at <a href="http://www.onvif.org">www.onvif.org</a></td>
</tr>
<tr>
<td>Analytics</td>
<td>Video motion detection, Active tampering alarm</td>
</tr>
<tr>
<td></td>
<td>Support for AXIS Camera Application Platform enabling installation of AXIS Video Motion Detection 3, AXIS Cross Line Detection, AXIS Digital Autotracking and third-party applications, see <a href="http://www.axis.com/acap">www.axis.com/acap</a></td>
</tr>
<tr>
<td>Event triggers</td>
<td>Analytics, Edge storage events</td>
</tr>
<tr>
<td>Event actions</td>
<td>File upload: FTP, SFTP, HTTP, HTTPS, network share and email</td>
</tr>
<tr>
<td></td>
<td>Notification: email, HTTP, HTTPS, TCP and SNMP trap</td>
</tr>
<tr>
<td></td>
<td>Video recording to edge storage</td>
</tr>
<tr>
<td></td>
<td>Pre- and post-alarm video buffering</td>
</tr>
<tr>
<td></td>
<td>Overlay text</td>
</tr>
</tbody>
</table>
### AXIS Q3709-PVE Network Camera

#### Technical Specifications

<table>
<thead>
<tr>
<th>Built-in installation aids</th>
<th>Pixel counter</th>
</tr>
</thead>
</table>

#### General

<table>
<thead>
<tr>
<th>Casing</th>
<th>IP66- and NEMA 4X-rated, IK10 impact-resistant aluminum casing with transparent, polycarbonate cover and dehumidifying membrane Encapsulated electronics Captive screws (resistorx 30) Color: White NCS S1002-B For repainting instructions and impact on warranty contact your Axis partner.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>3 GB RAM, 768 MB Flash</td>
</tr>
<tr>
<td>Power</td>
<td>Power over Ethernet IEEE 802.3at Type 2 Class 4, max. 23.1 W, typical 16.7 W</td>
</tr>
<tr>
<td>Connectors</td>
<td>RJ45 10BASE-T/100BASE-TX/1000BASE-T</td>
</tr>
<tr>
<td>Edge storage</td>
<td>Support for recording to dedicated network-attached storage (NAS)</td>
</tr>
<tr>
<td>Operating conditions</td>
<td>-40 °C to 55 °C (–40 °F to 131 °F) Arctic Temperature Control: Start-up as low as –40 °C (–40 °F) Humidity 10–100% RH (condensing)</td>
</tr>
<tr>
<td>Storage conditions</td>
<td>–40 °C to 65 °C (–40 °F to 149 °F)</td>
</tr>
<tr>
<td>Dimensions</td>
<td>205 x 205 x 172 mm (8.1 x 8.1 x 6.8 in)</td>
</tr>
<tr>
<td>Weight</td>
<td>2.2 kg (4.8 lb) including weather shield</td>
</tr>
<tr>
<td>Included accessories</td>
<td>RJ45 Push–pull connector (IP66), L-key, Weather shield, Installation Guide, Windows decoder 3-user license</td>
</tr>
<tr>
<td>Optional accessories</td>
<td>Axis Mounts AXIS PoE+ Midspans AXIS T8604 Media Converter Switch AXIS T8129 PoE Extender AXIS T8415 Wireless Installation Tool AXIS P8221 Network I/O Audio Module RJ45 IP66-rated cables with premounted connector (Cat 6) For more accessories, see <a href="http://www.axis.com">www.axis.com</a></td>
</tr>
<tr>
<td>Video management software</td>
<td>AXIS Camera Companion, AXIS Camera Station, Video management software from Axis’ Application Development Partners available on <a href="http://www.axis.com/techsup/software">www.axis.com/techsup/software</a></td>
</tr>
<tr>
<td>Warranty</td>
<td>Axis 3-year warranty and AXIS Extended Warranty option, see <a href="http://www.axis.com/warranty">www.axis.com/warranty</a></td>
</tr>
</tbody>
</table>

**a. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (www.openssl.org), and cryptographic software written by Eric Young (eay@cryptsoft.com).**

**Environmental responsibility:**

www.axis.com/environmental-responsibility

#### 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.
AXIS Q3709-PVE Network Camera

Technical Specifications

The following factors are among the most important to consider:

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