

ARTISAN®
TECHNOLOGY GROUP

Your **definitive** source for quality pre-owned equipment.

Artisan Technology Group
(217) 352-9330 | sales@artisantg.com | artisantg.com

Full-service, independent repair center
with experienced engineers and technicians on staff.

We buy your excess, underutilized, and idle equipment
along with credit for buybacks and trade-ins.

Custom engineering
so your equipment works exactly as you specify.

- Critical and expedited services
- In stock / Ready-to-ship
- Leasing / Rentals / Demos
- ITAR-certified secure asset solutions

Expert team | Trust guarantee | 100% satisfaction

All trademarks, brand names, and brands appearing herein are the property of their respective owners.

Visit our website - *Click HERE*

USER'S MANUAL

AXIS Q1755 Network Camera

AXIS Q1755-E Network Camera

Notices

This manual is intended for administrators and users of the AXIS Q1755/-E Network Camera, and is applicable for firmware release 5.01 and later. It includes instructions for using and managing the camera on your network. Previous experience of networking will be of use when using this product. Some knowledge of UNIX or Linux-based systems may also be beneficial for advanced users, for developing shell scripts and applications. Later versions of this document will be posted to the Axis Website, as required. See also the product's online help, available via the Web-based interface. The AXIS Q1755/-E support ONVIF v1.0. For more information about ONVIF go to www.onvif.org For more information about enabling ONVIF go to the developers page at www.axis.com

Liability

Every care has been taken in the preparation of this manual. 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.

Intellectual Property Rights

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

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

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

Equipment Modifications

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

Trademark Acknowledgments

Apple, Boa, Bonjour, Ethernet, Internet Explorer, Linux, Microsoft, Mozilla, Netscape Navigator, OS/2, Real, SMPTE, QuickTime, UNIX, Windows, WWW are registered trademarks of the respective holders. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Axis Communications AB is independent of Sun Microsystems Inc.
UPnP™ is a certification mark of the UPnP™ Implementers Corporation.

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 firmware updates
- find answers to resolved problems in the FAQ database. Search by product, category, or phrases
- report problems to Axis support by logging in to your private support area
- visit Axis Support at www.axis.com/techsup

AXIS Q1755/-E Network Camera User's Manual
Rev. 1.4
Copyright© Axis Communications AB, 2008 - 2011
November 2011 Part no. 45216

Contents

Product Description 4
Key features 4
Overview 5
Accessing the Camera 7
Access from a browser 7
Setting the root password 8
Access from the internet 8
The Live View page 9
Video Streams 11
How to stream H.264 11
Motion JPEG 12
Alternative methods of accessing the video stream 12
Basic Setup 13
Video & Audio 14
Stream Profiles 16
Camera Settings 16
Focus and zoom 17
Overlay Image 17
Privacy mask 17
Audio Settings 18
Audio Clips 19
Live View Config 20
Layout 20
PTZ (Pan Tilt Zoom) 23
Installing PTZ devices 23
Installing the PTZ driver 23
PTZ Configuration 24
PTZ Controls 26
Applications 28
Events 29
Event Servers 29
Event Types 29
Gatekeeper 31
Camera tampering 31
Motion Detection 32
Port Status 33
Recording List 34
Continuous Recording 35
System Options 36
Security 36
Audio Support 37
Date & Time 38
Network 38
Storage - Disk Management 42
Ports & Devices 43
LED Settings 44
Maintenance 44
Support 44
About 46
Resetting to the Factory Default Settings 46
Unit connectors 47
LED indicators 49
Troubleshooting 50
Checking the Firmware 50
Upgrading the Firmware 50
Technical Specifications 55
General performance considerations 57
Glossary of Terms 58

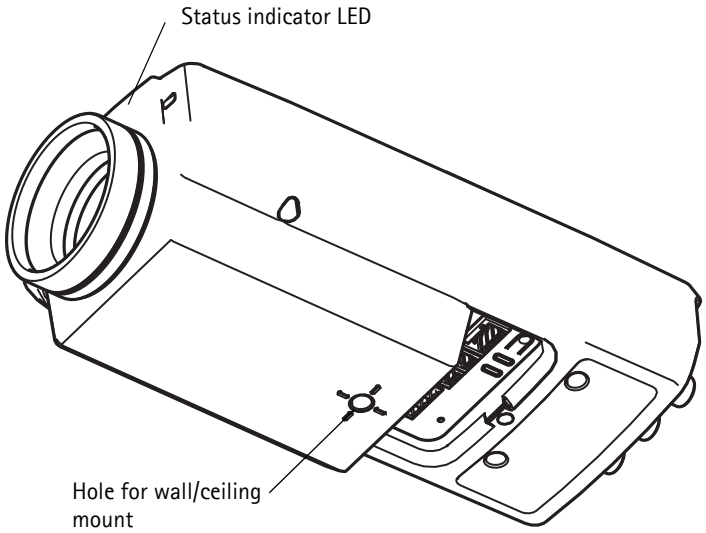
Product Description

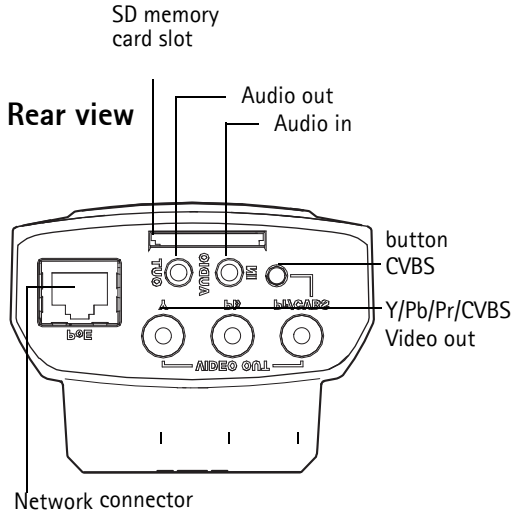
This manual applies to the AXIS Q1755/-E Network Cameras. The information provided here applies to all models, except where otherwise indicated.

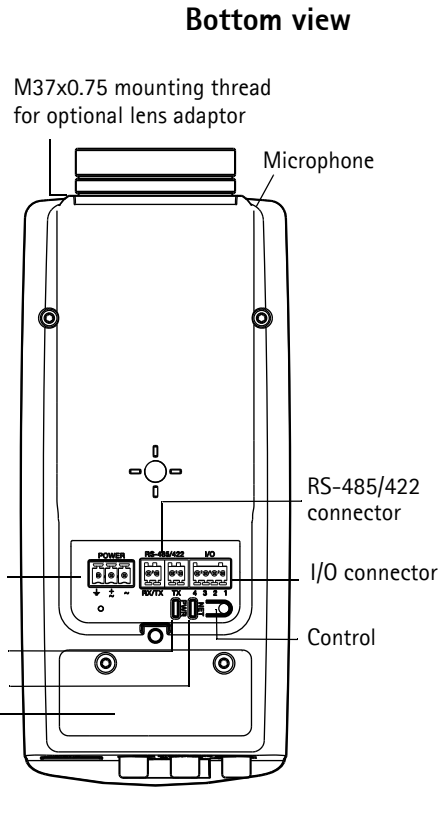
Key features

- **HDTV quality**
  With HDTV performance, AXIS Q1755/-E deliver outstanding image quality and full fps in H.264. This is beneficial for video surveillance systems where very clear images and greater image detail are required.
- **Zoom and autofocus**
  AXIS Q1755/-E have 10x optical zoom, 12x digital zoom and autofocus and can immediately zoom in to the desired field of view in perfect focus.
- **Local storage**
  The camera comes with a built-in slot for an SDHC memory card, enabling storage of several days of recordings, without any external equipment.
- **Power over Ethernet**
  AXIS Q1755/-E support Power over Ethernet (IEEE 802.3af) reducing installation costs by eliminating the need for power cables. AXIS Q1755-E can alternatively be powered by High Power over Ethernet. AXIS Q1755 can alternatively be powered by 8–20 V DC or 20–24 V AC.
- **Intelligent video capabilities**
  AXIS Q1755/-E offer intelligent capabilities such as the new Gatekeeper functionality, enhanced video motion detection, two-way audio including audio detection and detection of camera tampering attempts like blocking or spray-painting. The camera also provides capacity for third party analytics modules.
- **Outdoor-ready (AXIS Q1755-E)**
  AXIS Q1755-E is designed for quick and easy installation in demanding indoor and outdoor environments. There is no need to purchase and mount a separate outdoor housing. It eliminates the cost and complexity of pre-mounting a camera in an enclosure and minimizes the risk of incorrect mounting, it also helps to ensure optimal camera performance.
- **Arctic Temperature Control (AXIS Q1755-E)**
  Arctic Temperature Control allows the camera to not only function at -40 °C (-40 °F) but also power up at that temperature.
- **ONVIF**
  This 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.

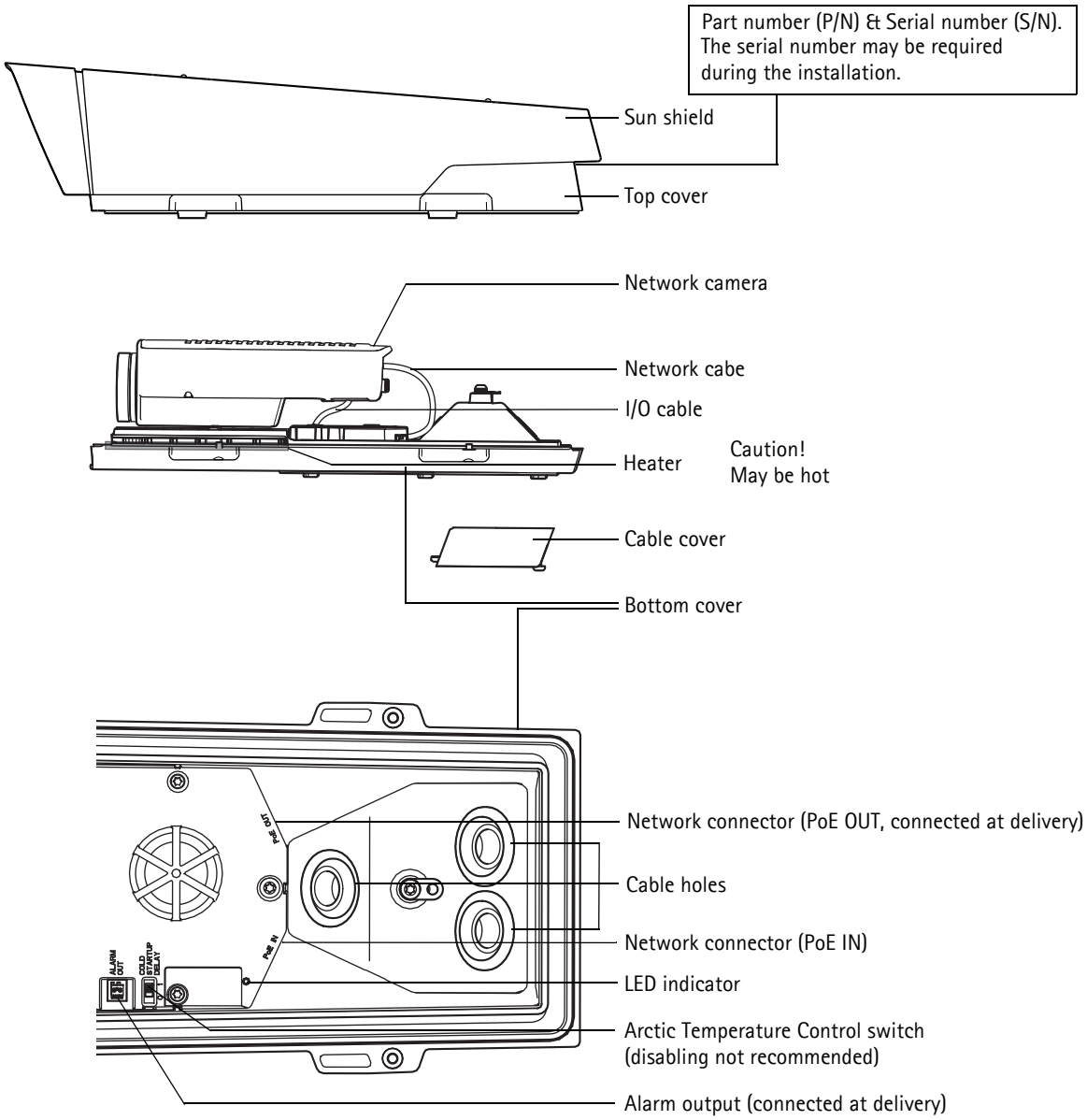
Overview


Status indicator LED
Hole for wall/ceiling mount


SD memory card slot
Rear view
Audio out
Audio in
button
CVBS
Y/Pb/Pr/CVBS Video out
Network connector


Bottom view
M37x0.75 mounting thread for optional lens adaptor
Microphone
RS-485/422 connector
Power connector
I/O connector
Control
Power indicator LED
Network indicator LED
Part number (P/N) & Serial number (S/N). The serial number may be required during the installation.

AXIS Q1755-E


Part number (P/N) & Serial number (S/N). The serial number may be required during the installation.
Sun shield
Top cover
Network camera
Network cabe
I/O cable
Heater
Caution! May be hot
Cable cover
Bottom cover
Network connector (PoE OUT, connected at delivery)
Cable holes
Network connector (PoE IN)
LED indicator
Arctic Temperature Control switch (disabling not recommended)
Alarm output (connected at delivery)

Accessing the Camera

Refer to the installation guide supplied with your product in order to install the AXIS Q1755/-E Network Camera.

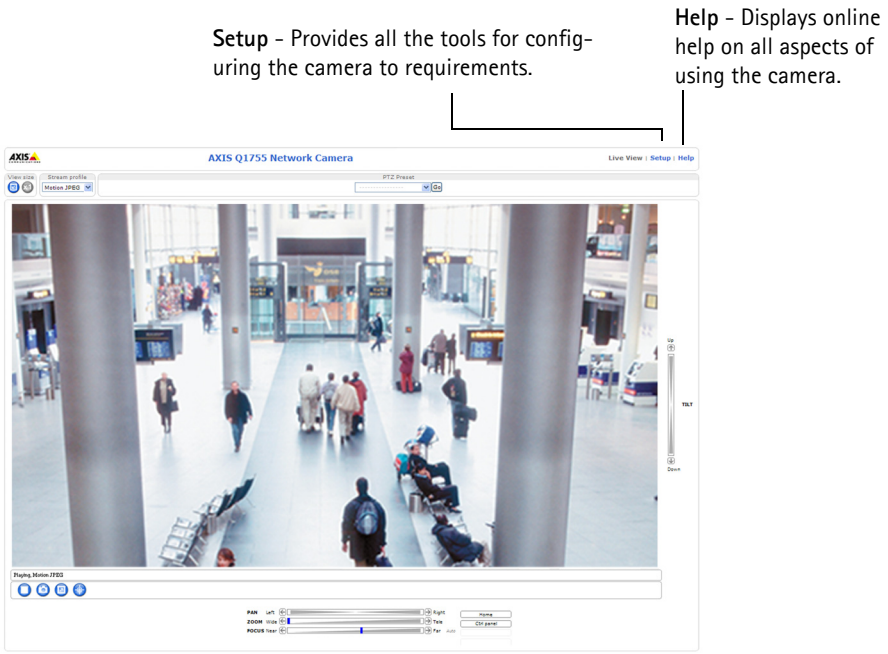
The network camera can be used with most standard operating systems and browsers. The recommended browser is Microsoft Internet Explorer with Windows, Safari with Macintosh and Firefox with other operating systems. See *Technical Specifications,* on page 55

Notes:

- To view streaming video in Microsoft Internet Explorer, set your browser to allow the installation of AMC and install AXIS Media Control (AMC) on your workstation.
- QuickTime™ is also supported for viewing streaming H.264 video and audio.
- If your workstation restricts the use of additional software components, the camera can be configured to use a Java applet for viewing Motion JPEG.
- The network camera includes one (1) decoder license for viewing H.264 video streams. This is automatically installed with AMC. The administrator can disable the installation of the H.264 decoder, to prevent installation of unlicensed copies.

Access from a browser

1. Start a browser (Internet Explorer, Firefox).
2. Enter the IP address or host name of the camera in the **Location/Address** field of your browser.
   To access the camera from a Macintosh computer (Mac OSX), click on the Bonjour tab and select the AXIS Q1755 from the drop-down list.
3. If this is the first time you are accessing the camera, see *Access from the internet,* on page 8. Otherwise enter your user name and password, set by the administrator.
4. The camera's **Live View** page appears in your browser.



Note:

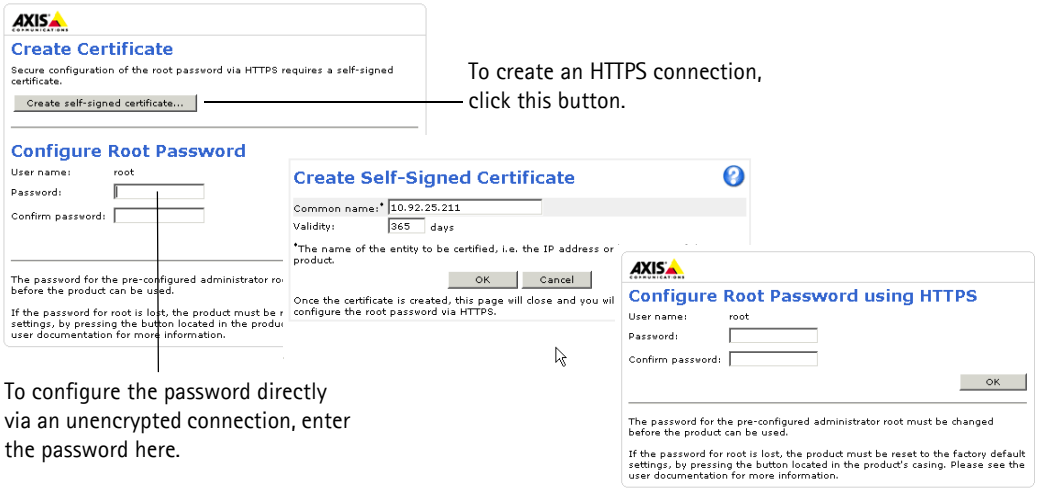
The layout of the Live View page may have been customized to specific requirements. Consequently, some of the examples and functions featured here may differ from those displayed on your own Live View page.

Setting the root password

To gain access to the product, the password for the default administrator user root must be set. This is done in the 'Configure Root Password' dialog, which is displayed when the network camera is accessed for the first time. To prevent network eavesdropping when setting the root password, this can be done via an encrypted HTTPS connection, which requires an HTTPS certificate (see note below).

Note:

HTTPS (Hypertext Transfer Protocol over SSL) is a protocol used to encrypt the traffic between web browsers and servers. The HTTPS certificate controls the encrypted exchange of information



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

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

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

Notes:

- The default administrator user name **root** cannot be deleted.
- If the password for root is lost or forgotten, the network camera must be reset to the factory default settings. See page 46.
- If prompted, click Yes to install AXIS Media Control, which allows viewing of the video stream In Internet Explorer. You will need administrator rights on the computer to do this. If using Windows Vista you must also run Internet Explorer as administrator; right-click the Internet Explorer icon and select **Run as administrator**.

Access from the internet

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

For more information, please see *NAT traversal (port mapping) for IPv4*, on page 40. See also the AXIS Internet Dynamic DNS Service at www.axiscam.net For Technical notes on this and other topics, visit the Axis Support web at www.axis.com/techsup

The Live View page

If your network camera has been customized to meet specific requirements the buttons and other items described below may or may not be displayed on the Live View page. The following provides an overview of each available button:

General controls



View size - Click these buttons to scale the image down to 800 pixels wide or to full scale. Only available in Motion JPEG.



The **Stream Profile** drop-down list allows you to select a customized or pre-programmed stream profile on the Live View page. Stream profiles are configured under Video & Audio > Stream Profiles, see *Stream Profiles*, on page 16 for more information.



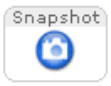
Pulse - Click this button to activate the output for a defined period of time, such as switching a light on for 20 seconds.



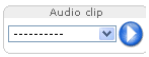
Active/Inactive - Click these buttons to manually start and stop a connected device - e.g. switch a light on/off.



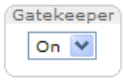
The Manual **Trigger** buttons can trigger an event directly from the Live View page. This button is configured under Events.



The **Snapshot** button saves a snapshot of the video image currently on display. Right-click on the video image to save it in JPEG format on your computer. This button is primarily intended for use when the AXIS Media Control viewer toolbar is not available.



Audio clip - Audio clips can be played when an event occurs or manually from the **Live View** page.



Enable/disable the **Gatekeeper** by selecting On or Off from the drop-down list. The Gatekeeper is configured under **Setup > Events > Gatekeeper**.

AXIS Media Control toolbar

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



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



The **Stop** stops the media stream being played.



The **Snapshot** button takes a snapshot of the current view. The location where the image is saved can be specified in the AMC Control Panel.



Click the **View Full Screen** button and the video view 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 media stream. The location where the recording is saved can be specified in the AMC Control Panel.

AMC Audio controls
AMC audio buttons control the speakers and microphone connected to the client computer. The buttons are only visible when audio is enabled.



Speaker buttons – Click to switch the sound on or off.



Microphone buttons - Click to switch the sound on or off.



Use the slider to control the **volume** on the speaker and microphone.



Half-duplex mode
The **Talk/Listen button** is used to switch between sending and receiving audio. The button can be configured from the Audio tab in the AMC Control panel:

- Push-To-Talk mode: Click and hold the button to talk/send, release the button to listen.
- Toggle mode: Click once to switch between talking and listening.

Simplex – Network Camera speaker only mode
To send audio, the Talk and Microphone buttons must both be enabled. Click either button to stop audio transmission.

Pan/Tilt/Zoom controls

If a PTZ device is installed, the Live View page also displays controls for the PTZ device. See *PTZ Controls*, on page 25 for more information.

Video Streams

The network camera provides several image and video stream formats. Your requirements and the properties of your network will determine the optimal use.

The Live View page in the network camera provides access to H.264 and Motion JPEG video streams, and to the list of available stream profiles. Other applications and clients can also access these video streams/images directly, without going via the Live View page.

How to stream H.264

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

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

<table>
<tr><td>Unicast RTP</td><td>This unicast method (RTP over UDP) should be your first consideration for live unicast video, especially when it is important to always have an up-to-date video stream, even if some images are dropped.</td><td rowspan="3">Unicasting is used for video-on-demand broadcasting, so that there is no video traffic on the network until a client connects and requests the stream.

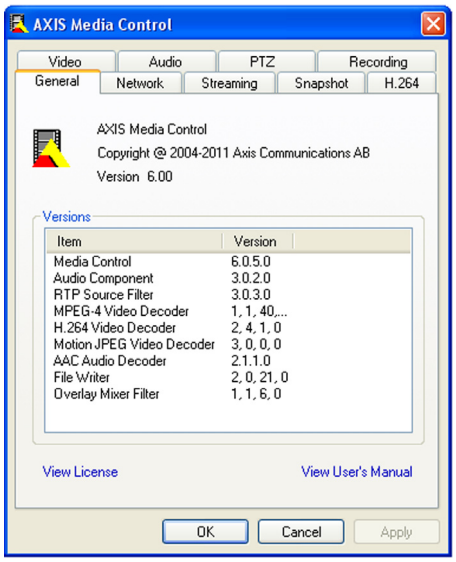
Note that there are a maximum of 10 simultaneous unicast connections.</td></tr>
<tr><td>RTP over RTSP</td><td>This unicast method (RTP tunneled over RTSP) is useful as it is relatively simple to configure firewalls to allow RTSP traffic.</td></tr>
<tr><td>RTP over RTSP over HTTP</td><td>This unicast method can be used to traverse firewalls. Firewalls are commonly configured to allow the HTTP protocol, thus allowing RTP to be tunneled.</td></tr>
<tr><td>Multicast RTP</td><td colspan="2">This method (RTP over UDP) should be used for live multicast video. The video stream is always up-to-date, even if some images are dropped.
Multicasting provides the most efficient usage of bandwidth when there are large numbers of clients viewing simultaneously. A multicast broadcast cannot however, pass a network router unless the router is configured to allow this. It is not possible to multicast over the Internet, for example. Note also that all multicast viewers count as one unicast viewer in the maximum total of 10 simultaneous connections.</td></tr>
</table>

AMC negotiates with the camera to determine the transport protocol to use in the order listed above. This order can be changed and the options disabled, to suit specific requirements.

Important!

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

AXIS Media Control (AMC)



The recommended method of accessing live video from the network camera is to use the AXIS Media Control (AMC) in Microsoft Internet Explorer in Windows.

The AMC control panel can be used to configure various video and audio settings. Please see the readme file included in the tool for more information.

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

- Windows Control Panel (from the Start menu)
- Alternatively, right-click the video image in Internet Explorer and click **Settings** to access the AMC window.

Motion JPEG

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 network camera is to use the AXIS Media Control (AMC) in Microsoft Internet Explorer in Windows.

Alternative methods of accessing the video stream

Video/images from the network camera can also be accessed in the following ways:

- Motion JPEG server push (if supported by the client, Firefox, for example). This option maintains an open HTTP connection to the browser and sends data as and when required, for as long as required.
- Still JPEG images in a browser. Enter the path - http://<ip>/axis-cgi/jpg/image.cgi
- Windows Media Player. This requires AMC and the H.264 viewing client to be installed. The paths that can be used are listed below in the order of preference:
  - Unicast via RTP: axrtpu://<ip>/axis-media/media.amp
  - Unicast via RTSP: axrtsp://<ip>/axis-media/media.amp
  - Unicast via RTSP, tunneled via HTTP: axrtsphttp://<ip>/axis-media/media.amp
  - Multicast: axrtpm://<ip>/axis-media/media.amp

<ip> = IP address

- To access the video stream from **QuickTime™** the following paths can be used:
  - rtsp://<ip>/axis-media/media.amp
  - rtsp://<ip>/axis-media/media.3gp

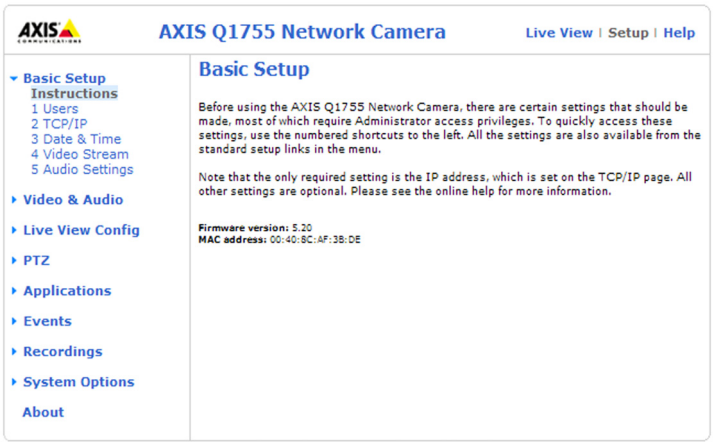
Notes:

- The network camera supports QuickTime 6.5.1 and later
- QuickTime adds latency to the video and audio stream (up to 3 seconds)
- It may be possible to use other players to view the H.264 stream using the paths above, although Axis does not guarantee this
- For input parameters to media.amp, refer to the VAPIX Application Programming Interface (API). See www.axis.com/developer for more information.

Basic Setup

Basic Setup provides shortcuts to the settings that should be made before using the network camera:

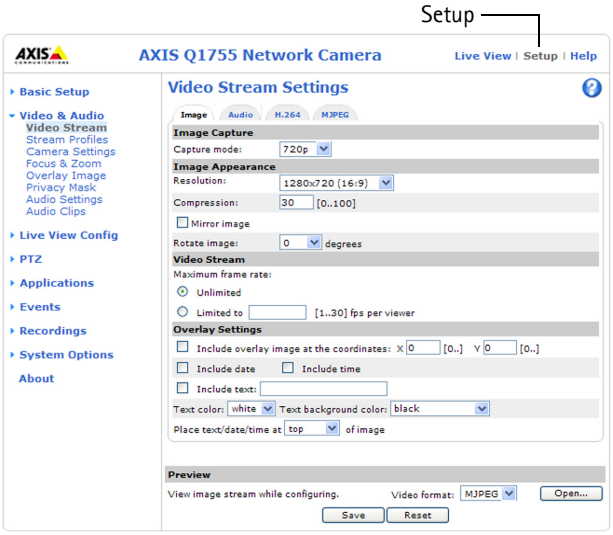
1. Users, see page 36.
2. TCP/IP, see page 38.
3. Date & Time, see page 38.
4. Video Stream, see page 11.
5. Audio Settings, see page 15.



Video & Audio

Click to access the online help that explains the Setup tools.

Video Stream



The video stream settings appear under four different tabs:

- Image
- Audio
- H.264
- MJPEG

Preview

For a preview of the image before saving, select the **Video Format** and click **Open...**

The **pixel counter** shows the number of pixels in an area of the image and can be use to ensure that the size of the image fulfills certain requirements, for example for face recognition. 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 satisfied with the settings, click **Save**.

Image

Image Capture

Capture mode - Select HDTV resolution, either 720p (progressive scan) or 1080i (interlaced with the option of de-interlacing).

- 720p provides a better quality video stream especially when capturing motion and is recommended for all resolutions except 1920x1080
- 1080i provides a larger image, but may contain motion artifacts and should only be used with 1920x1080 resolution

Note:

If component video out (analog video out) is used, make sure that the connected HDTV screen supports 1080i resolution if 1080i is the intended HDTV resolution.

Image Appearance

Use these settings to modify the image resolution and compression. Setting the compression level affects the image quality and the amount of bandwidth required; the lower the compression, the higher the image quality with higher bandwidth requirements. The image can also be mirrored (reversed) or rotated.

Note:

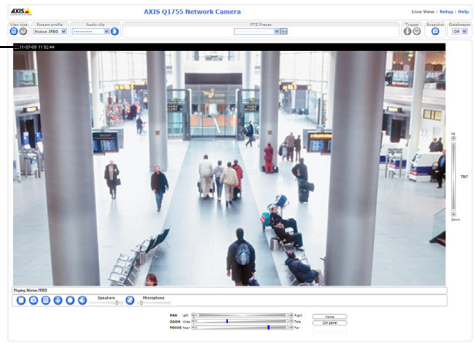
The default compression value of 30 gives a good image quality and a considerable bandwidth reduction compared to an uncompressed video stream

Video Stream

To avoid bandwidth problems on the network, the **frame rate** allowed to each viewer can be limited. Select the **Unlimited** radio button to allow the highest available frame rate or select the **Limited to...** radio button and enter a value (1-30) fps in the field.

Text Overlay Settings

Use these settings to include a text, date, and time as overlay in the video stream. Click for information on available options.



Preview

For a preview of the image before saving, select video format and **Open**. When satisfied with the settings, click **Save**.

Audio

Check the **Enable Audio** box to enable audio.

Note:

The checkbox **Enable Audio Support** under **System Options > Security > Audio Support** must also be checked to enable sound in the product. See **Audio Support,** on page 32**.**

Configuration settings from **Video & Audio > Audio Settings** are displayed under **Current Audio Settings**. See *Audio Settings,* on page 18 for more information on the audio settings.

H.264

GOV Settings

The GOV structure describes the composition of the H.264 video stream which consists of 2 image forms, I-images and P-images. An I-image is a complete image, whereas a P-image is only the differences in the image as compared with the previous image. The GOV length determines how many P-images are sent before the next complete I-image is sent.

Setting the GOV-length to a higher value may save some bandwidth but if there is congestion on the network, there may be noticeable decay in the video quality. Setting the GOV-length to a lower value increases the video quality, in this case.

GOV length should not be higher than the set frame rate when using a pre-trigger buffer see *Pre- and post-trigger buffers*, on page 30.

Bit Rate Control

The bit rate can be set as **Variable Bit Rate** (VBR) or **Constant Bit Rate** (CBR). VBR adjusts the bit rate according to the image complexity, using up bandwidth for increased activity in the image, and less for lower activity in the monitored area.

CBR allows you to set a fixed **Target bit rate** that consumes a predictable amount of bandwidth. As the bit rate would usually need to increase for increased image activity, but in this case cannot, the frame rate and image quality are affected negatively. To partly compensate for this, it is possible to prioritize either the frame rate or the image quality whenever the bit rate needs to be increased. Not setting a priority means the frame rate and image quality are equally affected.

Note:

To determine a reasonable bit rate, go to **Setup > Video & Audio > Video Stream > Image**. Under **Text Overlay Settings**, check the **Include text** checkbox and enter the code **#b** in the **Include text**: field. The current bit rate will display as a text overlay on the Live View page.

To preview the image stream while configuring the GOV settings and Bit rate control, select **Open...** under **Preview.**

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. Defining the frame size as **Unlimited** provides consistently good image quality at the expense of increased bandwidth and storage usage during low light. Limiting the frame size optimizes bandwidth and storage usage, but may give poor image quality.

Stream Profiles

There are four pre-programmed stream profiles available for quick set-up. These settings can be adjusted and new, customized profiles can be created. Each profile has a descriptive name, describing its usage and/or purpose. The profiles can be accessed from the Live View page.

- To create a new stream profile, click **Add...** to bring up the **Stream Profile Settings** dialog.
  1. Enter a unique name and a description for your profile.
  2. Select a **Video encoding** (H.264 or MJPEG) from the drop-down list.
  3. Modify the stream settings under the **Image, Audio, H.264** and **MJPEG** tabs. See *Video Stream,* on page 14**.**
  4. Click **OK** to save the profile.
- To copy an existing stream profile, click **Copy...** and enter a new name. Change the stream profile settings as above.
- To modify an existing stream profile, click **Modify...** and change the settings as above. The original settings for the pre-programmed profiles can always be restored by clicking **Restore**.
- To remove a stream profile, click **Remove**. Pre-programmed profiles cannot be removed.

Camera Settings

This page provides access to the image settings for AXIS Q1755/-E.

Image Appearance

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

Sharpness – Controls the amount of sharpening applied to the image.

IR cut filter – Set this filter to **Off** to allow the camera to 'see' infrared light, making the image clearer in low light conditions, e.g. at night. If set to **Auto**, the camera will automatically switch between IR cut filter **On** and **Off**, according to the current lighting conditions.

Rotate image – AXIS Q1755 is designed to be installed with the logotype facing down but if the installation requires another position, the image can be rotated to the correct orientation. Select the appropriate value from the drop-down list. Please see the online help files for a description of each available setting.

White balance

This is used to compensate for the different colors present in different light sources, to make the colors in the image appear the same. AXIS Q1755/-E can be set to automatically identify the light source and compensate for its color. Alternatively, the type of light source can be manually selected from the drop-down list.

Exposure Settings

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

Enable Backlight compensation – Backlight compensation makes the subject appear clearer when the image background is too bright, or the subject too dark.

Exposure control – this setting is used to adapt to the amount/type of light being used. Available settings are Manual Shutter, Manual Iris or Manual where all settings are available.

Max exposure time – this setting defines the max exposure time if **Exposure control** is set to **Auto**.
Once satisfied, click **Save.** Click **View** to view the video stream with the current configuration.
Please see the online help files for a description of each available setting.

View Image Settings

Click **View...** to view the video stream with the current configuration. Once satisfied, click **Save.**

Focus and zoom

The camera's maximum zoom level can be limited if required.

Zoom tele limit - Select a value from the drop-down list and click the **Go to** button to check the selected limit.

The camera has automatic focus and will refocus when the image changes. This setting is enabled by default. Set the near focus limit (Focus near limit) to avoid focusing on objects too close to the camera.

Overlay Image

An overlay image is a static image superimposed over the video image. The overlay image can be used to provide extra information, or to mask a part of the video image. See the online help for supported image formats and sizes.

To use your own image, e.g. a logo, it must first be uploaded to AXIS Q1755/-E. Click **Browse** and locate the image file on the computer. Click **Upload**. When uploaded, the file can be selected in the Use overlay image drop-down list.

To place the overlay image at specific coordinates in the live view image, check **Include overlay image at the coordinates** and enter the X and Y coordinates.

Once satisfied, click **Save.** Click **View** to view the overlay image in the video stream.

Privacy mask

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

Privacy Mask List

The Privacy Mask List shows all the masks that are currently configured in AXIS Q1755/-E Network Camera and if they are enabled.

Add/Edit Mask

To define a new mask:

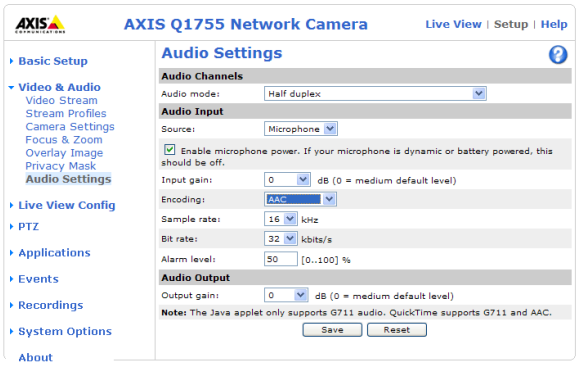
1. Click **Add.** A rectangle appears on the image.
2. Use the mouse to move the rectangle. To resize, click and pull in any edge.
3. Enter a descriptive name in the **Mask name** field.
4. Click **Save**.

To edit a privacy mask, select the mask and reshape or move as needed.

To change the **Privacy mask color**, select the new color from the drop-down list.

Audio Settings

This section describes how to configure the basic audio settings for the network camera. The audio functionality is enabled under **Video & Audio > Video Stream > Audio.**



Audio Channels

Audio mode - The available audio modes are

- **Half duplex**. Audio can be transmitted in both directions between the network camera and the client computer, but only in one direction at a time. You must actively transmit/receive sound using the **Talk/Listen** button available on the Live View page (see *AXIS Media Control toolbar,* on page 9). In Push-To-Talk mode, click and hold the button to speak and release it when finished speaking. In Toggle mode, click once to switch between speaking and listening.

  Note:

  The Talk/Listen button mode is configured from the Audio tab in the AMC control panel (see *AXIS Media Control (AMC),* on page 12).

- **Simplex – Network Camera speaker only**. Audio is transmitted from the client to AXIS Q1755/-E and played by the speaker connected to the camera. To send audio, the **Talk** and **Microphone** buttons in the AMC toolbar must both be enabled. Click either button to stop audio transmission.
- **Simplex – Network Camera microphone only**. Audio captured by the microphone connected to the network camera is transmitted from the camera to one or more clients.

Audio Input

An external microphone or a line source can be connected to the Audio in the connector of the network camera. If an external microphone or line source has been connected, the internal microphone will be automatically disconnected. The audio source must be set to **Microphone** or **Line** depending on the connected device.

Notes:

- To prevent unauthorized listening, the internal microphone can be disabled by inserting a plug in the Audio in connector.
- The internal microphone on AXIS Q1755-E cannot be used.

The **Enable microphone power** option provides DC power for an external microphone. If using a small electret condenser microphone such as a clip-on microphone or a PC microphone, enable this option.

Notes:

- If Enable microphone power is unchecked (disabled), the internal microphone is also disabled.
- To use a high impedance dynamic microphone, do not enable microphone power. Microphone power will not harm the microphone; if you are uncertain, try switching it off and on. To use a professional microphone requiring 48V phantom power, you need an external power supply and a balanced-unbalanced converter (audio transformer) in between.

If the sound input is too low or too high, adjust the **input gain** for the microphone attached to the network camera.

Select the desired audio **Encoding** format G711 µ-law, G726 or AAC.

Select the required **Sample rate** (number of times per second the sound is sampled). The higher the sample rate, the better the audio quality and the greater the bandwidth required.

Changing the **Bit rate** changes the audio compression level and hence audio quality. A higher bit rate can improve audio quality but requires more bandwidth.

The network camera can be set to trigger an event if the incoming sound level rises above, falls below, or passes the set **Alarm level**.

Audio Output

If the sound from the speaker is too low or too high, adjust the **output gain** for the active speaker attached to the network camera.

When satisfied with the settings, click **Save**, or click **Reset** to revert to previously saved settings.

Note:

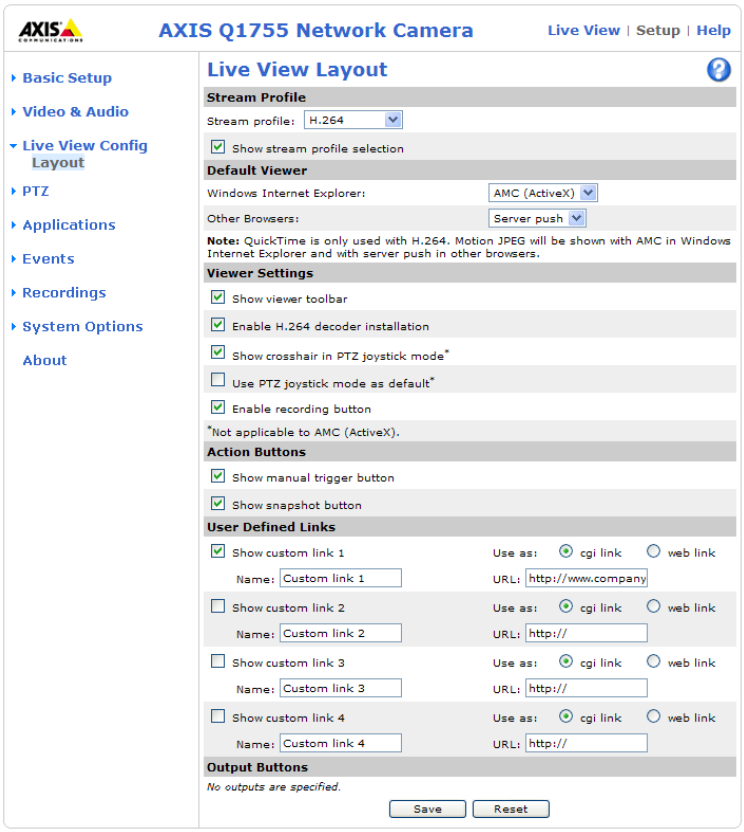
To receive synchronized video in H.264 and audio, it is recommended that the time settings in the camera and client computer are synchronized with an NTP Server. This is enabled in the camera under **System Options > Date & Time**. Please refer to the help pages for more information.

Audio Clips

Audio clips can be played when an event occurs or manually from the Live View page. Audio clips are created either by recording sound using the camera's microphone or by uploading a sound file to the camera. Audio clips that have been added to the network camera are listed in the Audio Clip List page. You can add new clips, play, download, modify and remove clips. Refer to the online help for further information.

Live View Config

Layout



Stream Profile

From the **Stream Profile** drop-down list, select the stream profile that is to be used for the Live View page. Listed are the standard stream profiles as well as the ones created under **Video & Audio > Stream Profiles**.

Show stream profile selection – Uncheck this checkbox to remove the Stream profile drop-down list from the Live View page.

See the online help files on this page for more information.

Default Viewer

From the drop-down lists, select the default method for viewing video images for your browser. The camera attempts to show the video images in the selected video format and viewer. If this is not possible, the camera overrides the settings and selects the best available combination.

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

Viewer Settings

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

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

Enable **Show crosshair in PTZ joystick mode** and a cross will indicate the center of the image in PTZ joystick mode.

Check **Use PTZ joystick mode as default** to enable joystick mode. The mode can be changed temporarily from the PTZ control panel.

Check **Enable recording button** to enable recording from the Live View page. The recordings are saved to the location specified in the AMC Control Panel, see *AXIS Media Control (AMC)*, on page 12.

Action Buttons

Check the boxes to display the action buttons on the Live View page.

The **manual trigger button** can be used to manually trigger and stop an event. See *Events*, on page 29.

The **snapshot button** can be used to save a snapshot from the video stream. This button is mainly intended for use with browsers other than Internet Explorer, or when not using AXIS Media Control to view the video stream. AXIS Media Control for Internet Explorer has its own snapshot button.

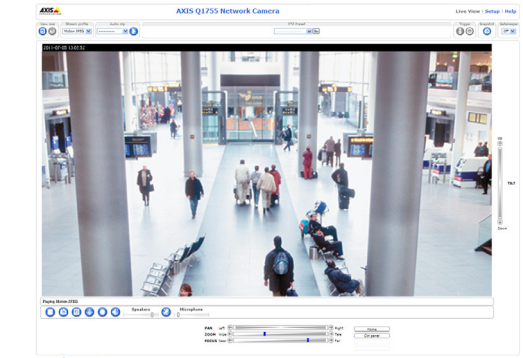
User Defined Links

User defined links can link to web pages, or can be used to run scripts or activate and control external devices connected to the network camera. Once configured, the links appear on the Live View page.

To set up a link, check the **Show custom link** box, select the cgi or web link radio button, enter the URL and a descriptive name in the provided field.

A link defined as a web link will open in a new window, while a cgi link will run for example a script in the background.

User defined cgi links can be used to issue API requests. For more information on the VAPIX Application Programming Interface (API), see the Video developer pages at Axis Web site www.axis.com/developer



User defined link

Output Buttons

The output buttons are used to manually activate and inactivate the output port, for example, to switch a light on and off. To display the output buttons on the Live View page, select the type of control to use for the port from the drop-down list:

- Pulse - Activates the output for a defined period of time
- Active/Inactive - Displays two buttons, one for each action (on/off)

See also *Ports & Devices*, on page 43.

Input/output ports are specified at **System Options > Ports & Devices > I/O Ports**

PTZ (Pan Tilt Zoom)

Installing PTZ devices

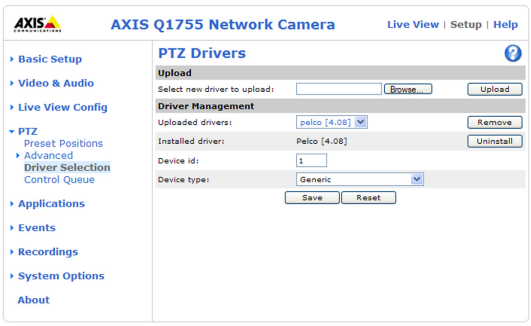
This Axis product supports several PTZ devices. Please see www.axis.com for a complete list of supported devices, and to obtain the correct driver. Follow the instructions below to install a PTZ device.

Installing a PTZ device is accomplished in two steps:

- Installing the PTZ driver (Pelco is already installed)
- Setting up the COM Port, See "COM Port" on page 39.

Installing the PTZ driver

1. Go to **PTZ** > **Driver Selection**.



2. Under **Upload**, click **Browse...** to find the driver. The driver has the file extension .ptz (e.g. driver.ptz).
3. Click **Upload**. If the driver was successfully uploaded, it will be available under **Driver Management** > **Uploaded drivers**.
4. From the **Uploaded drivers** drop-down list, select the driver to install and click **Save**.
5. Enter the **Device ID**, select the **Device Type** from the drop down list and click **Save**.
6. Set up the COM Port for the PTZ driver. See *COM Port*, on page 32 for instructions.

Notes:

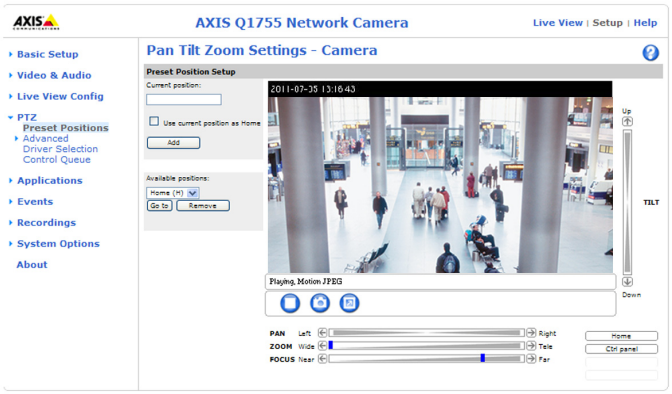
- After a PTZ driver has been installed, **PTZ** > **Advanced** > **Device** will contain additional driver specific settings that can be configured for the PTZ device.
- Advanced users and application developers can also use the Axis Application Programming Interface and HTTP specification for generic control of PTZ devices using CGI commands or a TCP/IP client. Refer to the Axis website at www.axis.com/developer for further information.

Uninstalling a PTZ driver

1. Go to **PTZ** > **Driver Selection**
2. Click **Uninstall**

PTZ Configuration

Once a PTZ driver has been installed, additional sub menus will appear in the menu to the left under PTZ.



Preset Positions

A preset position is a pre-defined camera view that can be used to quickly steer the camera to a specific location.

From **Preset Position Setup**, use the (Pan/Tilt) Zoom control to steer the camera view to the required position. When satisfied with the camera's position, enter a descriptive name. Click **Add** to save the camera position as a preset position.

On the **Live View** page, the camera view can be moved to a preset position at any time by selecting the preset's name from the **Source** drop-down list. Preset positions are also used as actions to triggered and scheduled **events**.

One preset can be set as the Home position, which is readily accessible by clicking the **Home** button on the Live View page and in the Preset Position Setup. To set the Home position, steer the camera to the desired position and check the **Use current position as Home** box. The position's name will have (H) added to the end, for example, Office Entrance (H).

Note:

The error "503 service unavailable" occurs if another user is accessing a different Motion JPEG stream configuration, for example via the Live View page. Only one Motion JPEG configuration is available at a time.

Advanced (Pan/Tilt)

A Pan/Tilt device can be used in order to pan and tilt the camera via controls on the web pages. The Pan/Tilt device controls can be modified from this page.

Device

Video Source 1 - Device ID is the RS-485 address of the connected P/T unit and the presented value must correspond to the value of the address switches in the connected PT unit, see the documentation for the connected unit for more information.

Driver Specific Settings for Video Source 1 - depending on the installation, it may be necessary to change the direction of the pan or tilt. Check **Flip pan** and **Flip tilt** to change direction.

Extended Driver Specific Settings for Video Source 1 - see the help file for a description of each setting.

Controls

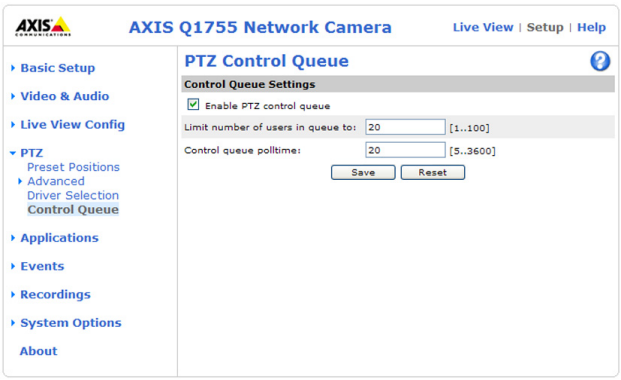
Driver-specific Panel Shortcut Command Buttons can be created to provide direct access to auxiliary commands provided by the PTZ driver. The buttons will be displayed in the PTZ control panel which is opened by clicking Ctrl Panel on the Live View page.

The pan, tilt, zoom, focus and iris controls can be disabled by unchecking the boxes under **Enable/Disable controls**.

See also *PTZ Controls*, on page 26, and *Control panel*, on page 27

Control Queue

The PTZ control queue gives one user exclusive access to the PTZ controls for a limited amount of time, placing other users in queue. To keep their place in the queue, waiting clients must regularly poll the network camera. The polltime and the maximum number of users allowed in the queue can be configured on this page.



A user who belongs to a group (see *Security,* on page 27) with a higher PTZ priority can go before other users in the queue and take control of the network camera. The order of priority for taking control of the queue is:

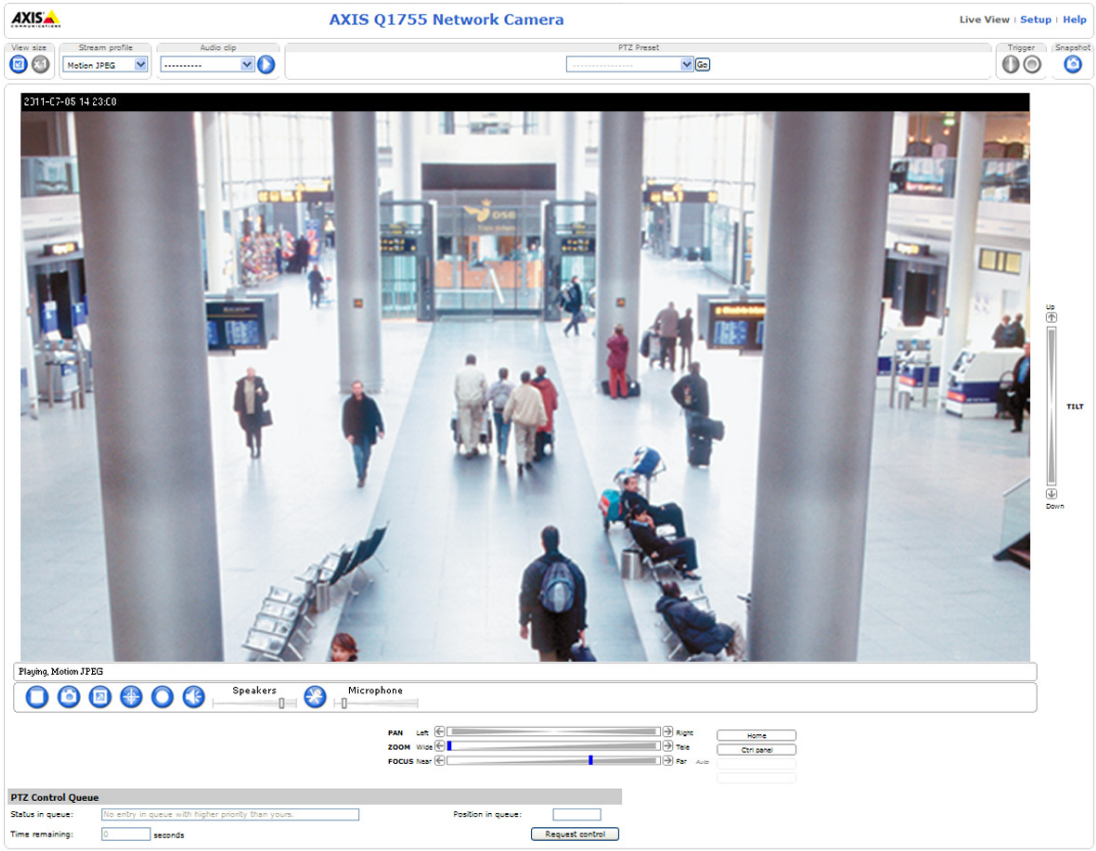
1. **Administrators** – An administrator takes over PTZ control regardless of who is first in queue. The administrator will be removed from the queue 60 seconds after their last PTZ control command.
2. **Event** – The network camera can be configured to go to a preset position when triggered by an alarm (see *Events,* on page 29). 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 to the next viewer in queue.

Notes:

- To identify the different users in the user group, the web browser must be set to enable cookies.
- The administrator can enable/disable PTZ control for selected users.

PTZ Controls

If the network camera has been appropriately configured, the Live View page displays the controls available for the installed Pan Tilt Zoom (PTZ) device. The administrator can enable/disable the controls for specified users under **System Options > Security > Users > User List**.



The controls shown depends on the PTZ device. The most common controls are:

- the Pan bar – moves the camera to the right and left
- the Tilt bar – tips the camera up and down
- the Zoom bar – zooms the view in and out. Note that this is only available if the camera is fitted with a zoom lens
- the Iris bar – adjusts the brightness of the image

Clicking on the bars themselves or on the arrows at the end of the bars moves the camera to a new position. The type of movement and the location of this new position depends on the type of PTZ driver.

When controlling the camera using a **relative** PTZ driver (see the bars in the illustration above) the new position is relative to the previous position, for example, left of, below, or above. Clicking the bar further from the center results in a larger movement.

In contrast, when using an **absolute** driver, each position on the bar (see right) represents a defined position in the device's range of movement, with the center of the bar representing the point midway between the two extremes of movement.



Clicking a position directly on the bar moves the camera directly to the new position in one smooth movement. Clicking on the arrows at the ends of a bar causes an incremental change.

Using CGI links to control PTZ devices

User-defined CGI links on the Live View page can be used to issue API (Application Programming Interface) requests, such as PTZ commands. These links are configured in the Live View Layout settings, see *User Defined Links,* on page 22.

PTZ control modes

The PTZ device can also be controlled using **click-in-image** movement, which has two different types of navigation - **Center** and **Joystick.**



Click the **Center mode** button and click on a position in the image to center the camera view on that position.



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

Note:

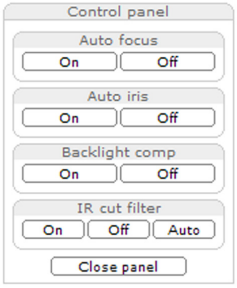
There is also joystick support in AXIS Media Control (AMC).

Control panel



Click the **Ctrl panel** button to access the PTZ control panel. The buttons available in the control panel depend on the installed PTZ driver.

- **Auto focus** – automatically adjust the image focus
- **Auto iris** – automatically adjust the amount of light reaching the image sensor
- **Backlight comp** – enabling backlight compensation makes the subject clearer if the image background is too bright, or if the subject is too dark.
- **IR cut filter** – when set to off, the camera will be able to "see" infrared (IR) light, for example at night; it increases light sensitivity. The image is shown in black & white when the IR cut filter is off. Set to Auto to automatically turn the filter off when the available amount of visible light falls below the minimum requirement.
- **Driver-specific shortcut command buttons** can also appear in the control panel, see *Advanced (Pan/Tilt),* on page 24.



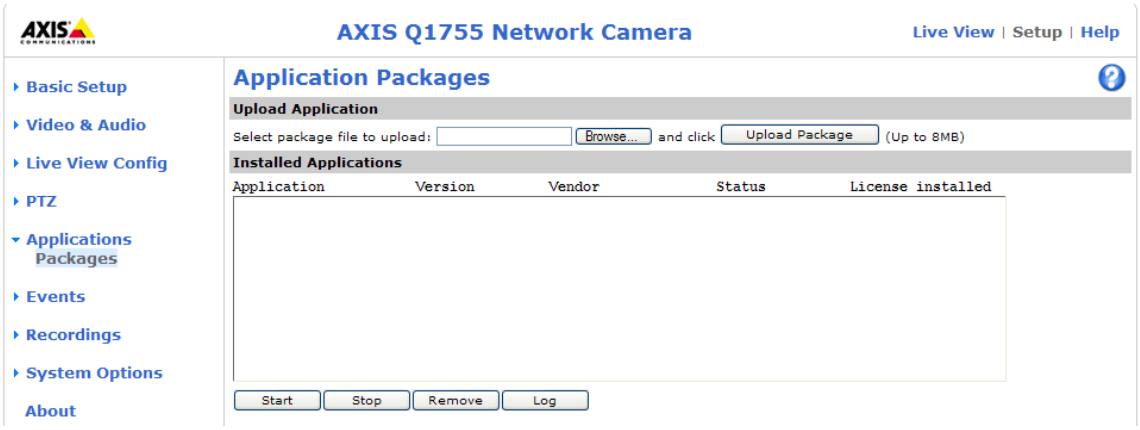
PTZ Control Queue

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. For more information see *Control Queue*, on page 25.



Applications

Application Packages



The Applications feature allows you to upload third party applications for use on this device. Listed under **Applications** > **Packages** are the applications that have already been installed. Click on the name to view the menu options - **Settings**, **License** and **About**.

Settings - This is dependent on the application.

License - Once uploaded some applications need a license to run, and a license code is required for the uploaded application. If there is an Internet connection in the camera, **Automatic Installation** appears in the web page. If there is no Internet connection to the camera, go to www.axis.com to acquire a License key file. You will need a license code and the device's serial number to receive a license key.

About - Details support for this application. To upload an application, browse to the package and click **Upload Package**.

Installed Applications - A list of installed applications with information about the version, and the vendor; the status of the application (running or not running), and information about the license (if installed).

Start/Stop - Start or stop the application.

Remove - To delete an application, select it and click **Remove**.

Log - To generate a log of the application happenings, select an application and click **Log**. This log is helpful when requesting support from the application's vendor.

Events

Pre-defined parameters, known as an **Event** or **Event type** can trigger certain actions in the camera. A common Event type is an alarm that causes the camera to upload images. Many Event types use an **Event Server**, to receive uploaded images.

An Event that is triggered by a signal, such as a door switch, motion detection, or system event, is called a **triggered event**, see page 30.

A **scheduled event** runs at pre-programmed times.

An **Action** refers to what happens when the Event occurs.

This section describes how to configure the camera to perform certain actions when Events occur.

Event Servers

Event Servers are used to receive uploaded image files and/or notification messages. To set up Event Server connections in your camera, go to **Setup > Events > Event Servers** and enter the required information for the required server type.

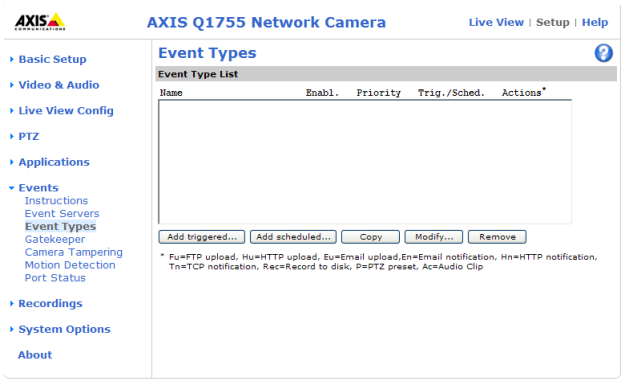
Server type	Purpose	Information required
FTP Server	• Receives uploaded images	• Descriptive name • Network address and Upload path • User Name and Password
HTTP Server	• Receives notification messages • Receives uploaded images	• Descriptive name • URL (IP address or host name) • User Name and Password • Proxy settings
TCP Server	• Receives notification messages	• Descriptive name • Network address (IP address or host name) • Port number

For details on each setting, see the online help available from each web page.

When the setup is complete, the connection can be tested by clicking the **Test** button (the connection test takes approximately 10 seconds).

Event Types

An **Event type** describes how and when the camera is to perform certain actions.



Example: If somebody passes in front of the camera and an Event has been configured to detect and respond to motion, the camera can record and save images to an FTP server, and can send a notification e-mail to an e-mail address. Images can be sent as e-mail attachments.

Triggered Event

A triggered event can be activated by:

- Input ports
- A manual trigger – using the manual trigger button on the Live View page or through the VAPIX® Application Programming Interface (API)
- IR cut filter
- Movement in a motion detection window
- Audio – when the sound level rises above or falls below the alarm level (configured under **Video & Audio > Audio Settings**, see page 15).
- On boot – for example after power loss
- Camera tampering, see page 31.
- Disk full – when the local storage disk (SD memory card) has less than 1MB free memory
- Pan Tilt Zoom

How to set up a triggered event

The following example describes how to set up a triggered event.

1. Click **Add triggered...** on the **Event Types** page. The **Triggered Event Type Setup** page appears.
2. Enter a descriptive **Name** for the Event, such as Door open.
3. Set the **Priority** - High, Normal or Low.
4. Set the **Respond to Trigger...** parameters to define when the Event is active, for example, after office hours.
5. Select the Input ports alternative from the **Triggered by...** drop-down list and specify the state (active, inactive or change) that the input must enter for the Event to be triggered.
6. Set the **When Triggered...** parameters, that is define what the camera will do if the door is opened. To upload images, select **Save stream** and enter the required information. See *Save stream, on page 30*.
7. Click **OK** to save the Event in the Event types list.

Please see the online help for descriptions of each available option.

Note:

Up to 10 Event types can be configured in the camera, and up to three of these can be configured to upload images. File names can be formatted according to specific requirements. See File Naming & Date/Time Formats in the online help.

Save stream

To upload images to an FTP or HTTP server, or to send images by email, check the **Save stream** box.

Image frequency – Set the image frequency to a desired frame rate. The frame rate will be the best possible, but might not be as high as specified, especially if uploading via a slow connection.

Pre- and post-trigger buffers

This function is very useful when checking to see what happened immediately before and/or after a trigger, for example, 20 seconds before and after a door was opened. All uploaded images are JPEG images.

Include pre-trigger buffer – Contains images from the time immediately preceding the trigger. Check the box to enable the pre-trigger buffer and specify the buffer length in seconds, minutes or hours.

Include post-trigger buffer – Contains images from the time immediately after the trigger. The post-trigger buffer is configured in the same way as the pre-trigger buffer.

Notes:

- Pre-trigger and post-trigger buffers will be lost if the connection to the Event server fails.
- The maximum length of the pre-/post-buffer depends on the video image size and selected frame rate.
- If the pre- or post-buffer is too large for the camera's internal memory, the frame rate is reduced and individual images may be missing. If this occurs, an entry is created in the unit's log file
- If the trigger releases often, set your post buffer to a higher amount of time to rather record one longer media stream than several shorter to improve memory card performance.

Continue image upload (unbuffered) – Upload video images for a fixed length of time or for as long as the trigger is active.

Select type – Upload images to an FTP or HTTP server, send images by e-mail or save the video stream to the local storage disk.

Create folder – Images uploaded to FTP and HTTP servers can be saved to designated folders. Folders can for example be named using the current date and time, see File Naming & Date/Time Formats in the online help.

Base file name – Used to name all uploaded images. Add a suffix or use your own file format to give the images unique names, see File Naming & Date/Time Formats in the online help.

Use stream profile – Select the stream profile to upload, send as e-mail or save to the local disk. For HTTP, FTP and Email only MJPEG stream profiles are available.

Scheduled Event

A **Scheduled event** can be activated at preset times, in a repeating pattern on selected weekdays.

How to set up a scheduled event:

The following example describes how to configure the camera to save images from pre-programmed time periods.

1. Click **Add scheduled...** on the **Event Types** page.
2. Enter a descriptive **Name** for the Event, such as Scheduled e-mail upload.
3. Set the **Priority** (High, Normal or Low).
4. Set the **Activation Time** parameters (24h clock) for the Event. For example, select **Recurrence pattern** and let the Event start on Sundays at 13.00 with a duration of 12 hours.
5. Set the **When Activated...** parameters, that is, define what the camera should do when the Event is active. To upload images, select **Save stream** and enter the required information. See *Save stream, on page 30*.
6. Click **OK** to save the Event in the Event Types list.

Please see the online help for descriptions of each available option.

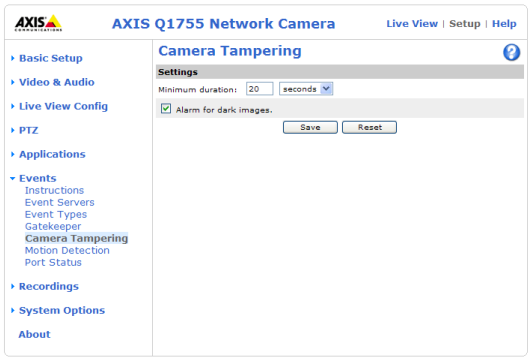
Gatekeeper

The Gatekeeper monitors an area such as an entrance gate and can zoom in and take a snapshot of, for example, a license plate, triggered by movement in the area. The camera will then automatically zoom out to the Home position and continue to overview the monitored area. Follow the online instructions to configure the Gatekeeper.

Camera tampering

The camera tampering application generates an alarm whenever the camera is repositioned, or when the lens is covered, sprayed, or severely defocused.

First, you must create an Event, see *How to set up a triggered event, on page 30*, for the camera to send an alarm.



Settings

The **Minimum duration** parameter sets the minimum tampering period, that is an alarm will not be triggered until this period has lapsed, even if the tampering conditions are otherwise met. This can help prevent false alarms for known conditions that affect the image.

If the camera lens is sprayed or covered so that the camera live view becomes dark, it will not be possible to distinguish this situation from other situations where the same effect is seen, such as when lighting conditions change.

When the **Alarm for dark images** parameter is enabled, alarms are generated for all cases where the lights are either dimmed or turned off, or if the lens is sprayed, covered, or rendered severely out of focus. If not enabled, no alarm will be sent.

After you define these settings, click **Save**.

Motion Detection

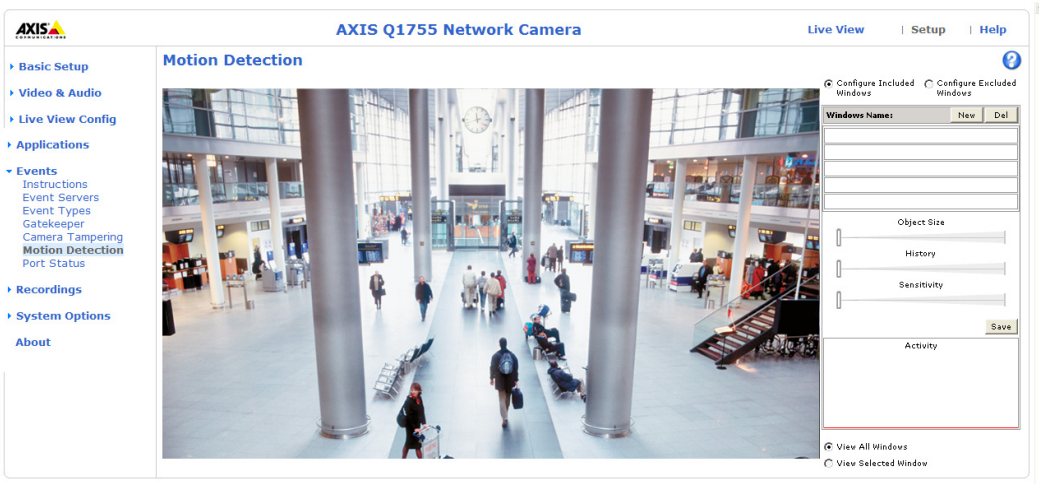
Motion detection is used to generate an alarm whenever movement occurs (or stops) in the camera's field of view. A total of 10 Include and/or Exclude windows can be configured.

- **Included** windows target specific areas within the whole image
- **Excluded** windows define areas within an Include window that should be ignored (areas outside Include windows are automatically ignored)

Once configured, the motion detection windows appear in the list of available triggers, for triggering Events. See *How to set up a triggered event, on page 30*.

Note:

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



Set up a motion detection include window

1. Go to **Events > Motion Detection**.
2. Create a new motion detection window:
   a.Using AXIS Media Control (Internet Explorer): Select the radio button Configure Included Windows and click **New**. Select the new window in the list of windows and enter a descriptive name.
   b. Using the Java applet: Click Add Window. Select the Include radio button and enter a descriptive name in the field.
3. Adjust the size (drag the bottom right-hand corner) and position (click on the text at the top and drag to the desired position) of the active window.
4. Adjust the **Object Size**, **History** and **Sensitivity** profile sliders (see table below for details). Any detected motion within an active window is indicated by red peaks in the **Activity** window (the active window has a red frame).
   Click **Save**.

Note:

To exclude parts of the Include window, select the Exclude option and position the Exclude window as required, within the Include window.

To delete an Include or Exclude window:

a. Using AXIS Media Control (Internet Explorer): Select the window in the list of windows and click **Del**.
b. Using the Java applet: Select the window and click on the cross in the upper right corner.

Please see the online help for descriptions of each available option.

	Object Size	History	Sensitivity
High level	Only very large objects trigger motion detection	An object that appears in the "include window" will trigger the motion detection for a long period	Ordinary colored objects on ordinary backgrounds will trigger the motion detection
Low level	Even very small objects trigger motion detection	An object that appears in the "include window" will trigger motion detection for only a very short period	Only very bright objects on a dark background trigger motion detection
Default value	Low	High	High

Examples:

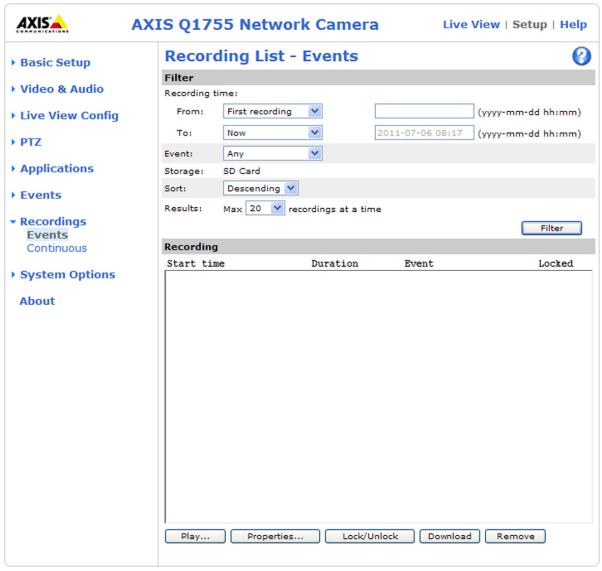
- Avoid triggering on small objects in the video image by setting the **object size** level to high.
- Use several small Motion Detection windows rather than one large window, if triggers on small movements or objects are desired.
- To reduce the number of triggers if there is a lot of movement during a short period of time, select a high **history** level.
- To only detect flashing light, select low **sensitivity**. In other cases, a high **sensitivity** level is recommended.

Port Status

Under **Events > Port Status** there is a list showing the status for the camera's input and output. This is for the benefit of **Operators** who have no access to the System Options section.

Example: If the Normal state for a push button connected to an input is set to **Open circuit –** as long as the button is not pushed, the state is **inactive**. If the button is pushed, the state of the input changes to **active**.

Recording List



The Network Camera can be set to record continuously or as result of a triggered or scheduled event. See *Continuous Recording, on page 35* and *Event Types, on page 29* for more information. The Recording List window contains a list of recordings made to the local storage. It shows each recording's start time, length, the Event type used to start the recording, and if the recording is locked so that it can neither be deleted nor recorded over.

To view a recording, select it from the list and click the **Play** button.

For detailed recording and video information, select an individual recording from the list and click the **Properties** button.

Use the **Lock/Unlock** button to control whether a recording can either be removed or overwritten. If the recording is important and needs to be saved for future use, locking the recording can help prevent its accidental removal.

Recordings can be downloaded by selecting one or more recordings and clicking **Download**. The package downloaded is a zip file containing a minimum of 3 files, of which the .mkv or Matroska file is the actual recording.

Note

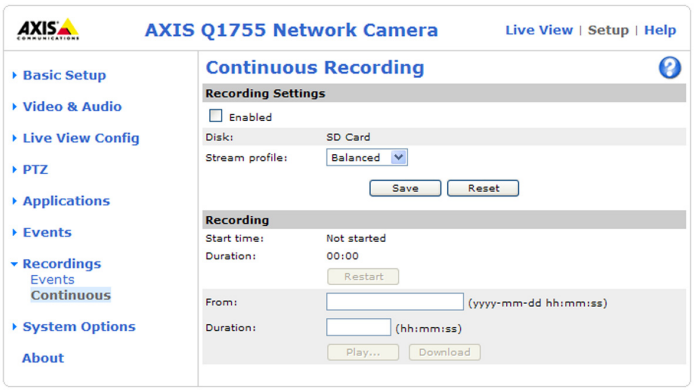
To play recordings in Windows Media Player download and install AXIS Matroska File Splitter from www.axis.com/techsup/software/ For more information on Matroska files see the online help .

The **Remove** button is used to delete unlocked recordings.

Filter - Use the filter to narrow down the list according to certain criteria such as a particular time frame. Note that certain filters may take a long time to complete.

For more information on filters see the online help .

Continuous Recording



The AXIS Q17 Series Network Camera can be configured to continuously save video to local storage. Automatic Disk Cleanup should be enabled when using Continuous Recording to prevent the local storage from becoming full. See *Storage - Disk Management, on page 42*.

Recording Settings

Enabled - Must be checked to record continuously.

Disk - Shows as SD Card for this product.

Stream Profile - Select a stream profile to use for recordings. For more information, see *Stream Profiles, on page 18*.

Note: The recording will be restarted and all previous continuous recordings will be removed if Stream profile is changed.

Click **Save** to activate these settings.

Recording

Start time - Shows the time the current continuous recording began. If no continuous recording is taking place the status will display as Not started.

Duration - Shows the length of the current continuous recording.

Restart - Click to start a new recording.

Note:
All previous continuous recording data will be removed.

From - To play or download the recording from a point in time, enter the year, month, day and the time in hours and minutes.

Duration - Enter the amount of the recording to play or download in hours, minutes and seconds.

Play... - Click this button to open a window to play the selected amount of the continuous recording.

Download - Click this button to download the recorded video. The package downloaded is a zip file containing a minimum of 3 files, of which the .mkv or Matroska file is the actual recording. The zip file is named after the time set in the **From** field.

Notes:

- The zip file will contain at least the time period selected. The first matroska file contains the start time, and the last matroska contains at least the stop time
- To play recordings in Windows Media Player download and install AXIS Matroska File Splitter from www.axis.com/techsup/software/

System Options

Security

Users

User access control is enabled by default. An administrator can set up other users, by giving these user names and passwords. It is also possible to allow anonymous viewer login, which means that anybody may access the Live View page, as described below:

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

Viewer	Provides the lowest level of access, which only allows access to the Live View page.
Operator	An operator can view the Live View page, create and modify events, and adjust certain other settings. Operators have no access to System Options.
Administrator	An administrator has unrestricted access to the Setup tools and can determine the registration of all other users.

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

User Settings

- Check the checkbox to enable **anonymous viewer login** to allow any viewer direct access to the Live View page.
- Check the checkbox to enable **anonymous PTZ control login** to allow anonymous users to join a queue for gaining control of the PTZ controls.
- **Enable Basic Setup** - before using the AXIS Q1755/-E Network Camera, there are certain settings that should be made, most of which require Administrator access privileges. To quickly access these settings, use the Basic Setup in the menu. All settings are also available from the standard setup links in the menu. Basic Setup is enabled by default but can be disabled and removed from the menu.

IP Address Filter

Enable IP Address Filtering to allow or deny access to the network cameras**.** Once enabled, the IP addresses in the list are allowed or denied access according to the choice made in the drop-down list **Allow/Deny the following IP addresses.**

The administrator can add up to 256 IP address entries to the list (a single entry can contain multiple IP addresses). The users from these IP addresses need to be specified in the user list with the appropriate access rights. This is done from **Setup > System Options > Security > Users**.

HTTPS

The network cameras support encrypted browsing using HTTPS.

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

A signed certificate can be obtained from an issuing Certificate Authority by clicking the **Create Certificate Request** button. When the signed certificate is returned, click the **Install signed certificate** button to import the certificate. The properties of any certificate request currently resident in the camera or installed can also be viewed by clicking the **Properties...** button. The HTTPS Connection Policy must also be set in the drop-down lists to enable HTTPS in the camera.

For more information, refer to the online help .

IEEE 802.1X

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

To access a network protected by IEEE 802.1X, devices must authenticate themselves. The authentication is performed by a third-party entity called an authentication server, typically a RADIUS server, examples of which are FreeRADIUS and Microsoft Internet Authentication Service. In Axis implementation, the network device and the authentication server authenticate themselves with the help of digital certificates using EAP-TLS (Extensible Authentication Protocol - Transport Layer Security). The certificates are provided by an Certification Authority (CA). You need:

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

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

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

Certificates

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

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

Settings

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

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

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

Enable IEEE 802.1X - Check the box to enable the IEEE 802.1X protocol.

Audio Support

Enable audio support - allow clients to retrieve audio streams from the camera. See also *Audio Settings, on page 18* for information on how to configure the audio settings.

Note:

This parameter will enable/disable all audio functionality in the camera, even in configured events and profiles with audio.

Date & Time

Current Server Time – Displays the current date and time (24h clock). The time can be displayed in 12h clock format in the overlay (see below).

New Server Time – Select your time zone from the drop-down list. If you want the server clock to automatically adjust for daylight savings time, select the **Automatically adjust for daylight saving time changes**.

Note:

The time zone setting only applies when the device's time is synchronized with an NTP server.

From the **Time Mode** section, select the preferred method to use for setting the time:

- **Synchronize with computer time** - sets the time from the clock on your computer.
- **Synchronize with NTP Server** - the camera will obtain the time from an NTP server.
- **Set manually** - this option allows you to manually set the time and date.

Note:

If using a host name for the NTP server, a DNS server must be configured under **TCP/IP** settings.
See ***Basic TCP/IP Settings***, below.

Date & Time Format Used in Images - specify the formats for the date and time (12h or 24h) displayed in the video streams. Use the predefined formats or use your own custom date and time formats. See **File Naming & Date/Time Formats** in the online help for information on how to create your own date and time formats.

Network

Basic TCP/IP Settings

AXIS Q1755/-E support both IP version 4 and IP version 6. Both versions may be enabled simultaneously, and at least one version must always be enabled. When using IPv4, the IP address for the camera can be set automatically via DHCP, or a static IP address can be set manually. If IPv6 is enabled, the network cameras receive an IP address according to the configuration in the network router. There are also options for setting up notification of changes in the IP address, and for using the AXIS Internet Dynamic DNS Service. For more information on setting the IP address, please see the online help.

Network Settings

Click the **View** button for an overview of the IP configuration of the network camera.

IPv4 Address Configuration

Check the **Enable IPv4** box to enable IPv4.

Obtain IP address via DHCP – Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a network. DHCP is enabled by default. Although a DHCP server is mostly used to set an IP address dynamically, it is also possible to use it to set a static, known IP address for a particular MAC address.

Note:

DHCP should only be enabled if your DHCP server can update a DNS server, which then allows you to access the network camera by name (host name). If DHCP is enabled and you cannot access the unit, run AXIS IP Utility to search the network for connected Axis products or reset the network camera to factory default settings and then perform the installation again.

Use the following IP address – To use a static IP address for the network camera, check the radio button and then make the following settings:

- **IP address** - Specify a unique IP address for your AXIS Q1755/-E. (To check if the IP address you intend to use is available or not, click the Test button)
- **Subnet mask** - Specify the mask for the subnet the AXIS Q1755/-E is located on
- **Default router** - Specify the IP address of the default router (gateway) used for connecting devices attached to different networks and network segments.

IPv6 Address Configuration

Check the **Enable IPv6** box to enable IPv6. Other settings for IPv6 are configured in the network router.

Services

Enable ARP/Ping setting of IP address - The IP address can be set using the ARP/Ping method, which associates the unit's MAC address with an IP address. Check this box to enable the service. Leave disabled to prevent unintentional resetting of the IP address.

Notes:

- The ARP/Ping service is automatically disabled two minutes after the unit is started, or as soon as an IP address is set. In order to reset the IP address, the camera must be restarted to activate ARP/Ping for an additional two minutes.
- Pinging the unit is still possible when this service is disabled.

Enable AVHS – AXIS Video Hosting System (AVHS) 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 please go to www.axis.com. If AVHS is not to be used this option can be disabled.

- **One-click enabled** - Press the camera's control button (see *Hardware Overview, on page 5*) until the status LED blinks green to install the camera using an AVHS service. Once registered the camera stays connected to the AVHS service. If the camera is not registered within 24 hours after the button is pressed, the camera will disconnect from the AVHS service.
- **Always** - The camera will constantly attempt to connect to the AVHS service over the Internet. Once registered the camera will stay connected to the service. This option can be used when the camera is already installed and it is not convenient to use the one-click installation.

AXIS Internet Dynamic DNS Service - Use the AXIS Internet Dynamic DNS service to assign a host name for easy access to your network camera (requires Internet access).

Click **Settings...** to register the camera with the Axis Internet Dynamic DNS service, or to modify the existing settings (requires access to the Internet). The domain name currently registered at the Axis Internet Dynamic DNS service for your product can at any time be removed.

For more information, please refer to the online help.

Advanced TCP/IP Settings

DNS Configuration

DNS (Domain Name Service) provides the translation of host names to IP addresses on your network.

Obtain DNS server address via DHCP - Automatically use the DNS server settings provided by the DHCP server. Click the **View** button to see the current settings.

Use the following DNS server address - Enter the desired DNS server by specifying the following:

- **Domain name** - enter the domain(s) to search for the host name used by the network cameras. 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.
- **DNS servers** - enter the IP addresses of the primary, and secondary DNS servers.

Note:

Adding a secondary DNS server is not mandatory.

NTP Configuration

Obtain NTP server address via DHCP - Check this radio button to automatically look up and use the NTP server settings as provided by DHCP. Click the **View** button to see the current settings.

Use the following NTP server address – to create manual settings, check this radio button and enter the host name or IP address of the NTP server.

Host Name Configuration – The network cameras can be accessed using a host name, instead of an IP address. The host name is usually the same as the assigned DNS Name.

For more information, please see *Security, on page 36*.

Link-Local IPv4 Address

This is enabled by default and assigns the network cameras an additional IP address for use with UPnP™. The camera can have both a Link-Local IP and a static/DHCP-supplied IP address at the same time - these will not affect each other.

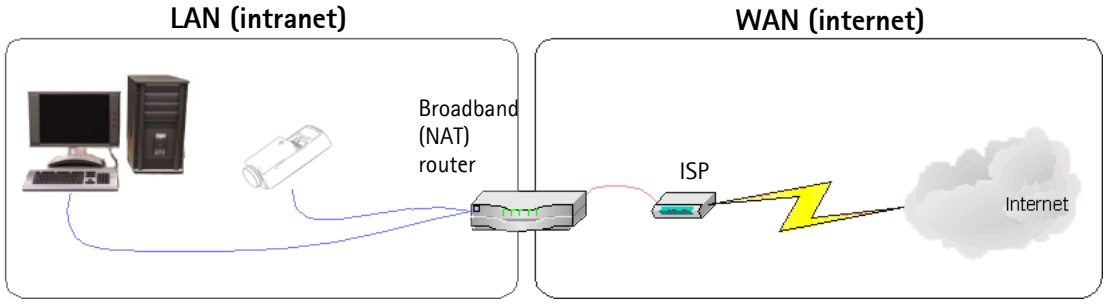
HTTP and HTTPS

The default HTTP/HTTPS port numbers (80 and 443 respectively) can be changed to any port within the range 1024-65535. This is useful for simple security port mapping, for example.

NAT traversal (port mapping) for IPv4

A broadband 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 broadband routers are pre-configured to stop attempts to access the private network (LAN) from the public network/Internet.

Use **NAT traversal** when your network cameras are 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 camera.



Notes:

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

Enable/Disable - When enabled, the network cameras attempt to configure port mapping in a NAT router on your network, using UPnP™. Note that UPnP™ must be enabled in the camera (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 provided.

If a router is not manually specified, the network cameras automatically search for NAT routers on your network. If more than one router is found, the default router is selected.

Alternative HTTP port - Select this option to manually define an external HTTP port. Enter the port number in the field provided. If no port is entered here a port number is automatically selected when NAT traversal is enabled.

Notes:

- An alternative HTTP port can be used/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 network camera enables the upload of new firmware and user applications. Check the box to enable the service.

RTSP

The RTSP protocol allows a connecting client to start an H.264 stream. Check the box to enable the server and enter the RTSP port number to use. The default setting is 554. Note that H.264 video streams will not be available if this service is not enabled.

SOCKS

SOCKS is a networking proxy protocol. The Axis network camera can be configured to use a SOCKS server to reach networks on the other side of a firewall/proxy server. This functionality is useful if the network camera is located on a local network behind a firewall and notifications, uploads, alarms and such need to be sent to a destination outside the local network (such as the Internet). See the online help for more information.

QoS (Quality of Service)

Quality of Service (QoS) guarantees a certain level of a specified resource to selected traffic on a network. Quality can be defined as a maintained level of bandwidth, low latency, and no packet losses. The main benefits of a QoS-aware network can be summarized as:

- The ability to prioritize traffic and thus allow critical flows to be served before flows with lesser priority.
- Greater reliability in the network, thanks to the control of the amount of bandwidth an application may use, and thus control over bandwidth races between applications.

The QoS in Axis network video products marks the data packets for various types of network traffic originating from the product. This makes it possible for network routers and switches to reserve a fixed amount of bandwidth for these types of traffic. The network cameras mark the following types of traffic:

- video
- audio
- event/alarm
- management network traffic

QoS Settings – For each type of network traffic supported by your Axis network video product, enter a DSCP (Differentiated Services Codepoint) value. This value is used to mark the traffic's IP header. When the marked traffic reaches a network router or switch, the DSCP value in the IP header tells the router or switch the type of treatment to apply to this type of traffic, for example, how much bandwidth to reserve for it. Note that DSCP values can be entered in decimal or hex form, but saved values are always shown in decimal.

For more information on Quality of Service, please see the Axis support web at www.axis.com/techsup

SMTP (email)

Enter the host names (or IP addresses) and port numbers for your primary and secondary mail servers in the fields provided, to enable the sending of notifications and image email messages from the camera to predefined addresses via SMTP.

If your mail server requires authentication, check the box for **Use authentication to log in to this server** and enter the necessary information. See the online help for more information.

SNMP

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

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

SNMP v1/v2

Select either SNMP v1 that includes no security, or SNMP v2c that uses very simple security.

The community name can be specified as a password for read or read/write access to all supported SNMP objects. The community is the group of network devices using SNMP. The default password for the **Read Community** is **public** and the default password for the **Write community** is **write**.

Traps for SNMP v1/v2

Traps are used by the camera to send messages to a management system for important events or status changes.

If **Enable traps** is selected, enter the email address where the trap message is to be sent as well as the **Trap community** that should receive the message.

There are four types of traps available for AXIS Q1755/-E.

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

SNMP v3

SNMP V3 - provides encryption and secure passwords. HTTPS must be enabled. To use traps with SNMP v3 an SNMP v3 management application is required.

If the **Enable SNMP v3** option is enabled, provide the Initial user password. Note that the initial password is activated only when HTTPS is enabled and can only be set once.

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

When SNMP configuration is ready, click **Save** to use the new settings or **Reset** to return to the default values.

UPnP™

The network camera includes support for UPnP™. UPnP™ is enabled by default, and the network camera then is automatically detected by operating systems and clients that support this protocol.

RTP/H.264

These settings are the port range, IP address, port number (video and audio), and Time-To-Live value to use for the video stream(s) in multicast H.264 format. Only certain IP addresses and port numbers should be used for multicast streams. For more information, please see the online help .

Bonjour

The network cameras include support for Bonjour. When enabled, the camera is automatically detected by operating systems and clients that support this.

Storage - Disk Management

Disk Management is used to setup and manage local storage devices. Local storage can be used to save video streams from triggered, scheduled or continuous recordings. For information on how to use the local storage with Triggered and Scheduled Event Type Setup and Continuous Recordings see the online help .

Storage Device

Once a formatted SD card has been inserted in the SD memory card slot, it is automatically mounted and information such as the available space and the size of the storage device is shown. The disk is full when there is less than 1000KB of space left on the memory card.

Disks are normally preformatted when purchased, if a SD Card needs to be formatted click the **Format** button to format the disk. Any previous data stored on the disk will be lost. Mounting is done automatically when a new memory card is inserted, or when the system boots. The only time you need to do a manual mount, is when you have executed an unmount command and the memory card has not been ejected and reinserted.

Status shows as follows:

- **OK** - The storage device is mounted and working correctly
- **connected** - The storage device is present but not mounted
- **disconnected** - The storage device is not present.
- **failed** - A problem has been discovered.

If the status shows as failed, click **Check disk** to see if the problem can be found and then try **Repair**. As a final measure the storage device might need to be reformatted. If there is important data on the storage device, see *Troubleshooting, on page 49*.

Read only shows the status of write-protect tab on the memory card. The status **no** means the tab is in the write-enabled mode and recordings can be saved to the memory card. The status **yes** means the memory card's tab is in the write-protected/read-only position, or there is a system error and recordings cannot be saved to the memory card.

Important!

To prevent loss of data, click **Unmount** before removing a storage device.

Storage Device Settings

Storage Device Settings is used to configure removal of recorded video.

Automatic disk cleanup

To avoid filling up local storage, Automatic disk cleanup can be set to continually remove older recordings to create more space.

Once enabled, automatic disk cleanup can be set to remove recordings that are older than a set number of days or weeks and when a percentage of the disk is full. For longer or continuous recordings, the oldest part of the recording is removed, it is recommended to have a time and date overlay in the video for proper tracking of recordings. See *Overlay Settings, on page 17*.

Note:

For continuous recording to work properly, do not set the limit to more than 80% full.

Interrupted recordings with an Unknown status, partial recordings and any other recording that has not been removed by disk cleanup can be removed manually from the **Recording List** using the **Remove** button.

Check **Lock disk** to stop writing to the disk and protect recordings from being removed. A locked disk cannot be formatted.

Ports & Devices

I/O Ports

The pinout, interface support and the control and monitoring functions provided by this connector are described in *Unit connectors*, on page 47.

COM Port

This page contains settings for the RS-485/RS-422 serial interface. The RS-485 and RS-422 ports support several operational modes:

Generic TCP/IP - Allows the network camera to receive data and send commands via TCP/IP.

Generic HTTP - Allows the network camera to receive data and send commands via HTTP.

Pan Tilt Zoom - Used for control of a PTZ device. A PTZ device requires a driver. See *Installing PTZ devices*, on page 21 for more information. Drivers can be obtained from www.axis.com

See also *Unit connectors, on page 47*.

LED Settings

The Status indicator LED on the camera can be set to flash at a configurable interval (or to not light up at all) when the unit is accessed. For a listing of all LED behavior, see page 49, or the online help. Note that the LED does not flash when the stream is retrieved using H.264 multicast.

Maintenance

Restart – The camera is restarted without changing any settings.

Restore – The unit is restarted and most current settings are reset to factory default values. The settings that do not reset are:

- the boot protocol (DHCP or static)
- the static IP address
- the default router
- the subnet mask

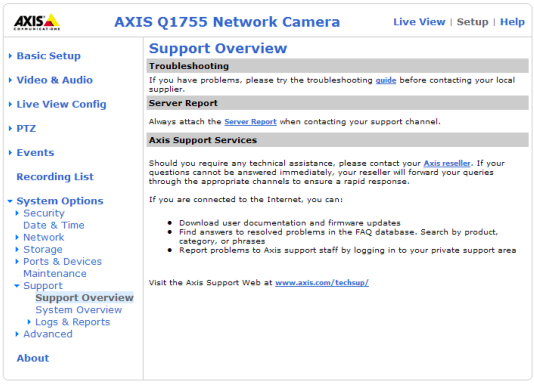
Default - the default button should be used with caution. Pressing this returns the camera's settings to the factory default values (including the IP address).

Upgrade Server - See *Upgrading the Firmware*, on page 50.

Support

Support Overview

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



System Overview

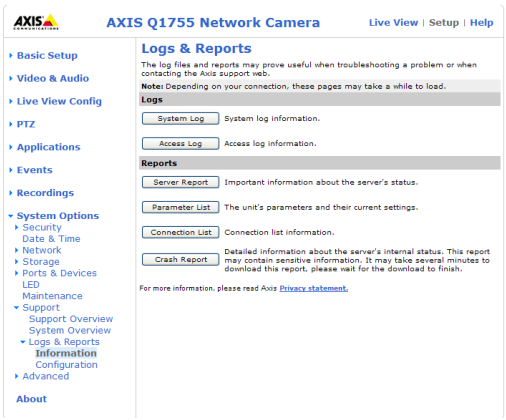
System Overview provides an overview of the status and settings. Information that can be found here includes the camera's firmware version, IP address, security, event and image settings and recent log items. Many of the captions are also links to the proper **Setup page** to conveniently make adjustments in the camera's settings.

Logs & Reports

When contacting Axis support, please be sure to provide a valid Server Report with your query. The Access Log is automatically included in the server report.

Information

The **Server Report** and **Parameter List** may prove useful when troubleshooting a problem or when contacting the Axis support web.



- **System Log** - Provides information about system events.
- **Access Log** - By default, the Access Log lists all failed attempts to access the camera but can be configured to list all connections to the camera, whether successful or not. Go to **Support > Logs & Reports > Configuration** and select the desired level of information from the list. See *Configuration, on page 45* for more information.
  The Access Log is useful for various purposes such as tracking all access to the camera, simple web attraction tracking, system analysis and troubleshooting.
- **Server Report** - Provides information about the server status and should always be included when requesting support.
- **Parameter List** - Shows the unit's parameters and their current settings.
- **Connection List** - Lists all clients that are currently accessing video and audio. It is also used for system analysis and troubleshooting.

Configuration

From the drop-down lists, select the size and level of information to be added to the **System Log** and **Access Log** files.

The default information level for the Access Log is set to Critical & Warnings, i.e. failed connections. However, in an error situation and when requesting support, set it to the highest information level - Critical & Warnings & Info.

For the Log Level for Email, select from the drop-down list the level of information to send as email and enter the destination email address.

Advanced

Scripting is an advanced function that enables you to customize and use scripts. This function is a very powerful tool.

Caution!

Improper use may cause unexpected behavior or even cause loss of contact with the unit. If a script does cause problems, reset the unit to its factory default settings. A backup file may be of use to return the unit to its latest configuration.

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

For more information, please visit the Video Developer pages at www.axis.com/developer

File Upload

Files (e.g. web pages and images) can be uploaded to AXIS Q1755/-E and used as custom settings. Uploaded files are accessed through http://<ip address>/local/<user>/<file name> where <user> is the selected user access group (viewer, operator or administrator) for the uploaded file.

Plain Config

Plain Config is for the advanced user with experience of Axis network camera configuration. All parameters can be set and modified from this page. Help is available from the standard help pages.

About

Here you can find basic information about your network camera. You can also view third party software licenses.

Resetting to the Factory Default Settings

To reset the camera to the original factory default settings, go to the **System Options > Maintenance** web page (as described in *Maintenance, on page 44*) or use the **Control button** on the side of the camera (see page 5) as described below:

Using the Control Button

This will reset all parameters, including the IP address, to the Factory Default settings:

1. Disconnect power from the camera.
2. Press and hold the Control button and reconnect power.
3. Keep the Control button pressed until the Status indicator displays amber (this may take up to 15 seconds).
4. Release the Control button. When the Status indicator displays green (which can take up to 1 minute) the process is complete and the camera has been reset. All parameters are set to factory default value.

Note:

For other methods of setting the IP address, please refer to the product's Installation Guide that accompanies the product, or download a copy from www.axis.com

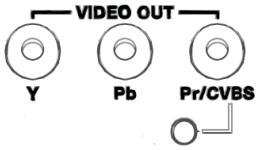
Unit connectors

Network – RJ-45 Ethernet connector. Supports PoE (Power over Ethernet, class 3). Using shielded cables is recommended.

Audio in – 3.5mm input for a mono microphone, or a line-in mono signal (left channel is used from a stereo signal).

Audio out – 3.5mm output for audio (line level), can be connected to a public address (PA) system or an active speaker with a built-in amplifier. A pair of headphones can also be connected. A stereo connector must be used for audio out.

Video Out – RCA connectors for component or composite video out.

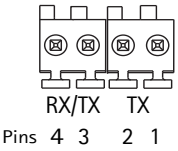


- Component video out (Y/Pb/Pr) for HDTV video, e.g. an entrance camera connected to an HDTV screen
- Composite video out (CVBS) - for easy installation using a video monitor. CVBS is available for 2 minutes after pressing the button and should only be used during installation.

RS-485/422 – two 2-pin terminal blocks for RS-485/422 serial interface used to control auxiliary equipment, e.g. PT devices.

The RS-485/422 serial port can be configured as follows:

RS-485/422



- Bidirectional RS-485 half-duplex port for data transmission using two wires, one combined RX/TX pair.
- Bidirectional RS-485 full-duplex port for data transmission using four wires, one RX pair and one TX pair.
- Unidirectional RS-422 port for transmitting or receiving data using two wires, RX- or TX pair.
- Bidirectional RS-422 full-duplex port for data transmission (point-to-point) using four wires, one RX pair and one TX pair.

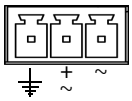
Function	Pin	Notes
RS 485/422TX(A)	1	TX pair for RS-422 and 4-wire RS-485
RS 485/422TX(B)	2	
RS-485A alt RS-485/422RX(A)	3	RX pair for all models (combined RX/TX for 2-wire RS-485)
RS-485B alt RS-485/422RX(B)	4	

SD memory card slot – SD and SDHC memory card can be used for local recording and removable storage.

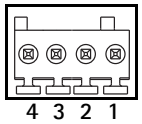
Lens – M37x0.75 mounting thread for optional lens adaptor, for example wide-angle adaptor, tele adaptor or lens filter. Remove the existing lens cover and retain for future use. Attach the adaptor securely to the camera casing.

Power – 3-pin terminal block 8-20 VDC or 20-24 VAC.

Use a limited power source, such as a mains adaptor, which rated power output does not exceed either 100 W or 5 A.



I/O terminal connector – Used in applications for e.g. motion detection, event triggering and alarm notifications. In addition to an auxiliary power and a GND pin, the AXIS Q1755/-E has 2 pins that can be configured as either input or output. These pins provide the interface to:



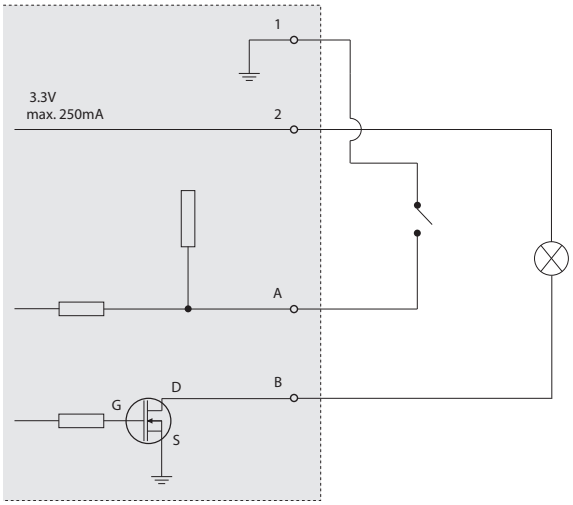
- Transistor output - For connecting external devices such as relays and LEDs. Connected devices can be activated by AXIS VAPIX API, output buttons on the **Live View** page or by an **Event Type**. The output will show as active (shown under **Events > Port Status**) if the alarm device is activated.
- Digital input - An alarm input for connecting devices that can toggle between an open and closed circuit, for example: PIRs, door/window contacts, glass break detectors, etc. When a signal is received the state changes and the input becomes active (shown under Events > Port Status.)

Notes:

- The I/O connector on AXIS Q1755-E is connected to the housing electronics at delivery and will trigger an input port event to indicate a fan or heater error when activated. See *Events,* on page 29, for information on how to set up an event.
- For information on how to connect external devices, refer to the Installation Guide supplied with the product.

Function	Pin number	Notes	Specifications
GND	1	Ground	
3.3 V DC Power	2	Can be used to power auxiliary equipment. **Note**: This pin can only be used as power out.	Max load = 250 mA
Configurable (Input or Output)	3-6	Digital input – Connect to GND to activate, or leave floating (unconnected) to deactivate.	0 to +40 V DC
		Digital output – Internal connection to ground when activated, floating (unconnected) when deactivated. If used with an external relay, a diode must be connected in parallel with the load, for protection against voltage transients.	Max. load =100 mA Max. voltage = + 40 V DC

The following connection diagram gives an example of how to connect an auxiliary device to the network camera.



LED indicators

LED	Color	Indication
Network	Green	Steady for connection to a 100 Mbit/s network. Flashes for network activity.
	Amber	Steady for connection to 10 Mbit/s network. Flashes for network activity.
	Unlit	No network connection.
Status	Green	Steady green for normal operation. Note: The Status LED can be configured to be unlit during normal operation, or to flash only when the camera is accessed. To configure, go to **Setup > System Options > LED.** See the online help files for more information.
	Amber	Steady during startup, during reset to factory default or when restoring settings.
	Red	Slow flash for failed upgrade.
Power	Green	Normal operation.
	Amber	Flashes green/amber during firmware upgrade.

Note:

Please refer to the product's Installation Guide for information on the LED indicators for the housing electronics (fan/heater).

Troubleshooting

Checking the Firmware

Firmware is software that determines the functionality of the network cameras. 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 your camera is displayed on the page **Setup > Basic Setup** or under **About.**

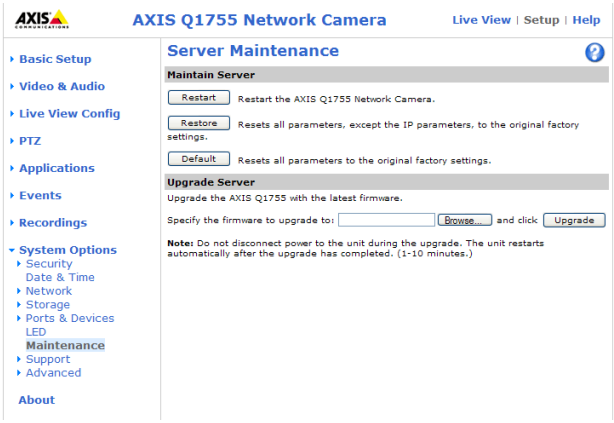
Upgrading the Firmware

When you upgrade your camera with the latest firmware from the Axis Web site, your camera receives the latest functionality available. Always read the upgrade instructions and release notes available with each new release, before updating the firmware.

Note:

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. Always read the instructions and release notes available with each new release, before upgrading the firmware.

1. Save the firmware file to your computer. The latest version of the firmware is available free of charge from the Axis website at **www.axis.com/techsup**
2. Go to **Setup > System Options > Maintenance** in the camera's web pages.
3. In the **Upgrade Server** section, browse to the desired firmware file on your computer. Click **Upgrade**.



Notes:

- After starting the upgrade process, always wait at least 5-10 minutes before restarting the camera, even if you suspect the upgrade has failed.
- Your dealer reserves the right to charge for any repair attributable to faulty upgrading by the user.
- AXIS Camera Management can be used for multiple upgrades. Please see the Axis website at www.axis.com for more information.

Emergency Recovery Procedure

If power or the network connection to the camera is lost during the upgrade, the process fails and the unit becomes unresponsive. A flashing red Status LED indicates a failed upgrade. To recover the unit, follow the steps below. The serial number is found on the label attached to the bottom of the camera.

1. **UNIX/Linux** - From the command line, type the following:
   arp -s <IP address of camera> <serial number> temp
   ping -s 408 <IP address of camera>

   Windows - From a command/DOS prompt, type the following:
   arp -s <IP address of camera> <serial number>
   ping -l 408 -t <IP address of camera>
2. If the unit does not reply within a few seconds, restart it and wait for a reply. Press CTRL+C to stop Ping.
3. Open a browser and type in the camera's IP address. In the page that appears, use the **Browse** button to select the upgrade file to use, for example, axisq1755.bin. Then click the Load button to restart the upgrade process.
4. After the upgrade is complete (1-10 minutes), the unit automatically restarts and shows a steady green on the Power and Status LEDs and flashing green or amber on the Network LED.
5. Reinstall the camera, referring to the installation guide.

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

Axis Support

If you contact Axis support (www.axis.com/techsup/), please help us to help you solve your problems expendiently by providing a Server Report and a detailed description of the problem.

The Server Report contains important information about the server and its software, as well as a list of the current parameters. Go to **Setup > System Options > Support > Support Overview** to generate a Server Report.

The **Log file** is available from **Setup > System Options > Support > Logs & Reports**. The Log file records events in the unit since the last system restart and can be a useful diagnostic tool when troubleshooting.

Symptoms, Possible Causes, and Remedial Action

Problems setting the IP address	
When using ARP/Ping	Try the installation again. The IP address must be set within two minutes after power has been applied to the camera. Ensure the Ping length is set to 408. See the Installation Guide.
The camera is located on a different subnet	If the IP address intended for the camera and the IP address of your computer are located on different subnets, you will not be able to set the IP address. Contact your network administrator to obtain an appropriate IP address.
The IP address is being used by another device	Disconnect the camera from the network. Run the Ping command. (In a Command/DOS window, type **ping** and the **IP address** of the unit). If you receive: **Reply from <IP address>: bytes = 32; time = 10 ms.....** - this means that the IP address may already be in use by another device on your network. You must obtain a new IP address and reinstall the unit. If you see: **Request timed out** - this means that the IP address is available for use with your camera. In this case, check all cabling and reinstall the unit.
Possible IP address conflict with another device on the same subnet	The static IP address in the camera is used before the DHCP server sets a a dynamic address. This means that if the same default static IP address is also used by another device, there may be problems accessing the camera. To avoid this, set the static IP address to 0.0.0.0.
The camera cannot be accessed from a browser	
Problems with ONVIF	If ONVIF is not working as expected, it may be that for security reasons ONVIF was disabled when the camera was accessed over VAPIX. To enable ONVIF, reset the product to Factory default settings (page 46).
The IP address has been changed by DHCP	If the camera and client are on the same network, Run AXIS IP Utility to locate the camera. Identify the camera using its model or serial number Alternatively: 1) Move the camera to an isolated network or to one with no DHCP or BOOTP server. Set the IP address again, using the AXIS IP Utility (see the Installation Guide) or the ARP/Ping commands. 2) Access the unit and disable DHCP in the TCP/IP settings. Return the unit to the main network. The unit now has a fixed IP address that will not change. 3) As an alternative to 2), if dynamic IP address via DHCP or BOOTP is required, select the required service and then configure IP address change notification from the network settings. Return the unit to the main network. The unit now has a dynamic IP address, but will notify you if the address changes.
Other networking problems	Test the network cable by connecting it to another network device, then Ping that device from your workstation. See instructions above.
Camera is accessible locally, but not externally	
Broadband router configuration	To configure your broadband router to allow incoming data traffic to the camera, enable the NAT-traversal feature which will attempt to automatically configure the router to allow access to the camera. This is enabled from **Setup > System Options > Network > TCP/IP Advanced**.
Firewall protection	Check the Internet firewall with your system administrator.
Default routers required	Check if you need to configure the default router settings.
Problems with the H.264 format	
No H.264 displayed in the client	Check that the correct network interface is selected in the AMC control panel applet (network tab).
	Check that the relevant H.264 connection methods are enabled in the AMC control panel applet (network tab).
	In the AMC control applet, select the H.264 tab and click the button Set to default H.264 decoder.
No multicast H.264 displayed in the client	Check with your network administrator that the multicast addresses used by the camera are valid for your network.
	Check with your network administrator to see if there is a firewall preventing viewing.

Multicast H.264 only accessible by local clients	Check if your router supports multicasting, or if the router settings between the client and the server need to be configured. The TTL (Time To Live) value may need to be increased.
Poor rendering of H.264 images	Color depth set incorrectly on clients. Set to 16-bit or 32-bit color.
	If text overlays are blurred, or if there are other rendering problems, you may need to enable Advanced Video Rendering from the H.264 tab in the AMC control panel applet.
	Ensure that your graphics card is using the latest device driver. The latest drivers can usually be downloaded from the manufacturer's web site.
Color saturation is different in H.264 and Motion JPEG	Modify the settings for your graphics adapter. Please see the adapter's documentation for more information.
Lower frame rate than expected	Reduce number of applications running on the client computer.
	Limit the number of simultaneous viewers.
	Check with the system administrator that there is enough bandwidth available. See also the online help.
	Check in the AMC control panel applet (H.264 tab) that video processing is not set to **Decode only I frames**.
	Lower the image resolution.
Why do I not get 30 frames per second?	See the section *General performance considerations, on page 57*.
Image degeneration	Decrease the GOV length, see the online help for more information.
The Power indicator is not constantly lit	
Faulty power supply	Check that you are using an AXIS PS-P power supply.
The Status and Network indicator LEDs are flashing red rapidly	
Hardware failure	Contact your Axis dealer.
The Status indicator LED is flashing red and the camera is inaccessible	
A firmware upgrade has been interrupted or the firmware has otherwise been damaged	See the *Emergency Recovery Procedure* above.
No images displayed on web page	
Problem with AMC. (*Internet Explorer only*)	To enable the updating of video images in Microsoft Internet Explorer, set your browser to allow ActiveX controls. Also, make sure that AXIS Media Control (AMC) component is installed on your workstation.
Installation of additional ActiveX component restricted or prohibited	Configure your camera to use a Java applet for updating the video images under **Live View Config > Layout > Default Viewer** for Internet Explorer. See the online help for more information.
Video/Image problems, general	
Image too dark or too light	Check the video image settings. See the online help on Video and Image Settings.
Missing images in uploads	This can occur when trying to use a larger image buffer than is actually available. Try lowering the frame rate or the upload period.
Slow image update	Configuring pre-buffers, motion detection, high-resolution images, or high frame rates, will affect the performance of the camera.
Poor performance	Poor performance may be caused by heavy network traffic, multiple users accessing the unit, low performance clients, use of features such as Motion Detection, Event handling, Image rotation other than 180 degrees.
Poor quality snapshot images	
Screen incorrectly configured on your workstation	In Display Properties, configure your screen to show at least 65000 colors, that is, at least 16-bit. Using only 16 or 256 colors will produce dithering artifacts in the image.
Overlay/Privacy mask is not displayed	
Incorrect size or location of overlay or privacy mask.	The overlay or privacy mask may have been positioned incorrectly or may be too large. Refer to **Overlay Image Requirements and Limitations** in the online help for more information.

Browser freezes	
Older browsers	Update your browser and Java to latest versions.
Problems uploading files	
Limited space	There is only limited space available for the upload of your own files. Try deleting existing files to free up space.
Motion Detection triggers unexpectedly	
Changes in luminance	Motion detection is based on changes in luminance in the image. This means that if there are sudden changes in the lighting, motion detection may be triggered mistakenly. Lower the sensitivity setting to avoid problems with luminance.
No audio	
Incorrect setup	Check the sound card in the PC. Ensure that the mute button is not pressed and the volume settings are correct.
No audio or very poor audio quality	Check that the correct Audio Input source is selected under **Setup > Audio > Source**. Select Microphone for the internal microphone or for a connected external microphone. Select Line for a connected line in source.
Audio volume too low/high	
Volume settings incorrect	The volume of the microphone is either too high or too low. Change the volume for the microphone in the toolbar on the Live View page.
Poor audio quality	
CPU overloaded	Reduce the number of listeners and viewers and decrease the image resolution and compression.
Unsynchronized audio and video	It is recommended that the camera's time setting is synchronized with an NTP Server. This is enabled under **System Options > Date & Time**.
Distorted audio	Check that the correct Audio Input source is selected under **Setup > Audio Settings > Source**. Select Microphone for the internal microphone or for a connected external microphone. Select Line for a connected line in source.

For further assistance, please contact your reseller or see the support pages on the Axis website at www.axis.com/techsup

Technical Specifications

Function/group	Item	Specification
Camera	Models	• AXIS Q1755 50 Hz/60 Hz • AXIS Q1755-E 50 Hz/60 Hz
	Image sensor	1/3" Progressive Scan CMOS 2 Megapixel
	Lens	• f 5.1 - 51 mm, F1.8 - 2.1 • Auto day/night IR filter, autofocus • Near focus limit: 10mm (wide) or 800mm (tele) • Angle of view, horizontal: 50° – 5.4° • M37x0.75 mounting thread for optional lens adaptor
	Minimum illumination	Color: 2 lux at 30IRE, F1.8 B/W: 0.2 lux at 30IRE, F1.8
	Shutter time	1/10000s to 1/2s
	Zoom	10x optical and 12x digital, total 120x
Video	Video compression	• H.264 Baseline profile • Motion JPEG
	Resolutions	• HDTV 1080i 1920x1080 • HDTV 720p 1280x720
	Frame rate H.264	30/25 fps in all resolutions
	Frame rate Motion JPEG	30/25 fps in all resolutions
	Video streaming	• Multi-stream H.264 and Motion JPEG: simultaneous, individually configured streams in max. resolution at 30/25 fps • Controllable frame rate and bandwidth • VBR/CBR H.264 • Max 10 simultaneous clients
	Image settings	• Compression, brightness, sharpness, white balance, exposure control, backlight compensation, rotation • Mirroring of images • Text and image overlay • Privacy mask
Audio	Audio streaming	Two-way, full duplex
	Audio compression	• AAC LC 8/16 kHz • G.711 PCM 8 kHz • G.726 ADPCM 8 kHz • Configurable bit rate
	Audio Input/Output	External microphone or line input, line output AXIS Q1755: Built-in microphone
Network	Security	Password protection, IP address filtering, HTTPS encryption*, IEEE 802.1X network access control, digest authentication, user access log *This product includes software developed by the Open SSL Project for use in the Open SSL Tool kit (www.openssl.org)
	Supported protocols	IPv4/v6, HTTP, HTTPS, SSL/TLS*, QoS Layer 3 DiffServ, FTP, SMTP, Bonjour, UPnP, SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, etc. *This product includes software developed by the Open SSL Project for use in the Open SSL Tool kit (www.openssl.org)

Function/group	Item	Specification
System Integration	Application Programming Interface	• Open API for software integration, including VAPIX® from Axis Communications*, AXIS Media Control SDK*, event trigger data in video stream, the ONVIF specification available at www.onvif.org • Quality of Service (QoS) layer 3, DiffServ Model • Embedded Linux operating system *Available at www.axis.com
	Intelligent Video	Video motion detection, active tampering alarm, audio detection, Gatekeeper
	Alarm triggers	Video motion detection, active tampering alarm, audio detection, temperature and external input
	Alarm events	• File upload via FTP, HTTP and email • Notification via email, HTTP and TCP • External output activation
	Video buffer	96 MB pre- and post alarm
	Video access from web browser	• Camera live view • Video recording to file (ASF) • Customizable HTML pages • Windows 7, Windows Vista, XP, 2000, 2003 server • DirectX 9c or higher • For other operating systems and browers see www.axis.com/techsup
General	Casing	AXIS Q1755: Metal (zink) AXIS Q1755-E: IP66- and NEMA 4X-rated, IK10 impact-resistant aluminum enclosure
	Processors, memory	• ARTPEC-3, 256 MB RAM, 128 MB Flash • Battery backed-up real-time clock
	Power	• AXIS Q1755: 8 – 20 V DC max 11,2 W, 20 - 24 V AC max 17,4 VA or Power over Ethernet IEEE 802.3af Class 3 • AXIS Q1755-E: Power over Ethernet IEEE 802.3af Class 3 or High Power over Ethernet
	Connectors	• RJ-45 10BASE-T/100BASE-TX PoE, terminal block for power, I/O terminal block for two configurable inputs/outputs • 3.5 mm mic/line in, 3.5 mm line out • RS485/RS422 • Video out: 3x RCA Y/Pb/Pr (HD), 1x RCA Composite (SD)
	Local Storage	SD/SDHC memory card slot (memory card not included)
	Operating conditions	• AXIS Q1755: 0 °C to 45 °C (32 °F to 113 °F) Humidity 20-80% RH (non-condensing) • AXIS Q1755-E: -40 °C to 45 °C (-40 °F to 113 °F) with High Power over Ethernet, -30 °C to 45 °C (-22 °F to 113 °F) with Power over Ethernet IEEE 802.3af Class 3 Arctic Temperature Control enables camera start-up at temperatures as low as -40 °C (-40 °F) with High PoE
	Approvals	• EN 55022 Class B • EN 61000-3-2 • EN 61000-3-3 • EN 55024 • EN 61000-6-1 • EN 61000-6-2 • EN 60950-1 • FCC Part 15, Subpart B, Class B • VCCI, Class B ITE • KCC Class B • C-tick AS/NZS CISPR 22 • ICES-003, Class B • AXIS Q1755-E: IP66, NEMA 250 Type 4X, IK10

Function/group	Item	Specification
	Dimensions (HxWxD)	AXIS Q1755: 58 x 79 x 186 mm (2.3" x 3.1" x 7.3") AXIS Q1755-E including sunshield: 87/120 x 140/161 x 404 mm (3.4/4.7" x 5.5/6.4" x 15.9")
	Weight	AXIS Q1755: 1.0 kg (2.2 lb) excl. power supply AXIS Q1755-E: 3.5 kg (7.7 lb.)
	Included accessories	Mounting and connector kits, Installation Guide, CD with installation tools, recording software and User's Manual, Windows decoder 1-user license
	Video management software (not included)	• AXIS Camera Station - Video management software for viewing and recording up to 50 cameras • See www.axis.com/partner/adp_partners.htm for more software applications via partners • AXIS Q1755-E: wall mount bracket, sunshield, 5 m (16 ft.) Ethernet cable
	Optional accessories	• YP3040 PT Motor • AXIS T8412 Installation Display • AXIS T90A Illuminators • AXIS Power over Ethernet Midspan 1-port, AXIS T8123 High PoE Midspan 1-Port • AXIS Camera Station and video management software from Axis' Application Development Partners • AXIS Q1755: Various housings • AXIS Q1755-E: Mounting accessories

General 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 it is slow response in the UI, latency in images, too low FPS (contrary to settings), this will also affect the frame rate.

The following factors are among the most important to consider:

- High image resolutions and/or lower compression levels result in larger images. Bandwidth affected.
- Access by large numbers of Motion JPEG and/or unicast H.264 clients. Bandwidth affected.
- Simultaneous viewing of different streams (resolution, compression, etc.) by different clients. Frame rate and bandwidth affected.
- Accessing both Motion JPEG and H.264 video streams simultaneously. Frame rate and bandwidth affected.
- Heavy usage of event settings affects the camera's CPU load. Frame rate affected.
- Enabled motion detection. Frame rate and bandwidth affected.
- Heavy network utilization due to poor infrastructure. Bandwidth affected.
- Viewing on poorly performing client PC's lowers perceived performance. Frame rate affected.

Glossary of Terms

ActiveX – A standard that enables software components to interact with one another in a networked environment, regardless of the language(s) used to create them. web browsers may come into contact with ActiveX controls, ActiveX documents, and ActiveX scripts. ActiveX controls are often downloaded and installed automatically as required.

Angle – The field of view, relative to a standard lens in a 35mm still camera, expressed in degrees, e.g. 30°. For practical purposes, this is the area that a lens can cover, where the angle of view is determined by the focal length of the lens. A wide-angle lens has a short focal length and covers a wider angle of view than standard or telephoto lenses, which have longer focal lengths.

ARP (Address Resolution Protocol) – This protocol is used to associate an IP address to a hardware MAC address. A request is broadcast on the local network to discover the MAC address for an IP address.

ARTPEC (Axis Real Time Picture Encoder) – This chip is used for image compression.

ASIC (Application Specific Integrated Circuit) – A circuit designed for a specific application, as opposed to a general purpose circuit, such as a microprocessor.

Aspect ratio – A ratio of width to height in images. A common aspect ratio used for television screens and computer monitors is 4:3. High-definition television (HDTV) uses an aspect ratio of 9:16.

Autoiris (DC-Iris) – This special type of iris is electrically controlled by the camera, to automatically regulate the amount of light allowed to enter.

Bitmap – A bitmap is a data file representing a rectangular grid of pixels. It defines a display space and color for each pixel (or 'bit') in the display space. This type of image is known as a 'raster graphic.' GIFs and JPEGs are examples of image file types that contain bitmaps.

Because a bitmap uses this fixed raster method, it cannot easily be rescaled without losing definition. Conversely, a vector graphic image uses geometrical shapes to represent the image, and can thus be quickly rescaled.

Bit rate – The bit rate (in kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit and not distance/time unit.

Bonjour – Also known as zero-configuration networking, Bonjour enables devices to automatically discover each other on a network, without having to enter IP addresses or configure DNS servers. Bonjour is a trademark of Apple Computer, Inc.

Broadband – In network engineering terms, this describes transmission methods where two or more signals share the same carrier. In more popular terminology, broadband is taken to mean high-speed data transmission.

CCD (Charged Coupled Device) – This light-sensitive image device used in many digital cameras is a large integrated circuit that contains hundreds of thousands of photo-sites (pixels) that convert light energy into electronic signals. Its size is measured diagonally and can be 1/4", 1/3", 1/2" or 2/3".

CGI (Common Gateway Interface) – A specification for communication between a web server and other (CGI) programs. For example, a HTML page that contains a form might use a CGI program to process the form data once it is submitted.

CIF (Common Intermediate Format) – CIF refers to the analog video resolutions 352x288 pixels (PAL) and 352x240 pixels (NTSC). See also *Resolution*.

Client/Server – Client/server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfils the request. Typically, multiple client programs share the services of a common server program. A web browser is a client program that requests services (the sending of web pages or files) from a web server.

CMOS (Complementary Metal Oxide Semiconductor) – A CMOS is a widely used type of semiconductor that uses both negative and positive circuits. Since only one of the circuit types is on at any given time, CMOS chips require less power than chips using just one type of transistor. CMOS image sensors also allow processing circuits to be included on the same chip, an advantage not possible with CCD sensors, which are also much more expensive to produce.

Codec – In communications engineering, a codec is usually a coder/decoder. Codecs are used in integrated circuits or chips that convert e.g. analog video and audio signals into a digital format for transmission. The codec also converts received digital signals back into analog format. A codec uses analog-to-digital conversion and digital-to-analog conversion in the same chip.

Codec can also mean compression/decompression, in which case it is generally taken to mean an algorithm or computer program for reducing the size of large files and programs.

Compression – See *Image compression*.

CVBS – analog video format (composite video).

DC-Iris (Autoiris) – This special type of iris is electrically controlled by the camera, to automatically regulate the amount of light allowed to enter.

DHCP (Dynamic Host Configuration Protocol) – DHCP is a protocol that lets network administrators automate and centrally manage the assignment of Internet Protocol (IP) addresses to network devices in a network.

DHCP uses the concept of a 'lease' or amount of time that a given IP address will be valid for a computer. The lease time can vary, depending on how long a user is likely to require the network connection at a particular location.

DHCP also supports static addresses for e.g. computers running web servers, which need a permanent IP address.

DNS (Domain Name System) – DNS is used to locate and translate Internet domain names into IP (Internet Protocol) addresses. A domain name is a meaningful and easy-to-remember name for an Internet address. For example the domain name www.example.com is much easier to

remember than 192.0.34.166. The translation tables for domain names are contained in Domain name servers.

Domain Server - Domains can also be used by organizations who wish to centralize the management of their (Windows) computers. Each user within a domain has an account that usually allows them to log in to and use any computer in the domain, although restrictions may also apply. The domain server is the server that authenticates the users on the network.

Duplex - See *Full-duplex*.

Ethernet - Ethernet is the most widely installed local area network technology. An Ethernet LAN typically uses special grades of twisted pair wires. The most commonly installed Ethernet systems are 10BASE-T and 100BASE-T10, which provide transmission speeds up to 10 Mbps and 100 Mbps respectively.

ETRAX (Ethernet Token Ring AXIS) - Axis' own microprocessor.

Factory default settings - These are the settings that originally applied for a device when it was first delivered from the factory. If it should become necessary to reset a device to its factory default settings, this will, for many devices, completely reset any settings that were changed by the user.

Firewall - A firewall works as a barrier between networks, e.g. between a Local Area Network and the Internet. The firewall ensures that only authorized users are allowed to access the one network from the other. A firewall can be software running on a computer, or it can be a standalone hardware device.

Focal length - Measured in millimeters, the focal length of a camera lens determines the width of the horizontal field of view, which in turn is measured in degrees.

FTP (File Transfer Protocol) - An application protocol that uses the TCP/IP protocols. It is used to exchange files between computers/devices on networks.

Frame - A frame is a complete video image. In the 2:1 interlaced scanning format of the RS-170 and CCIR formats, a frame is made up of two separate fields of 262.5 or 312.5 lines interlaced at 60 or 50 Hz to form a complete frame, which appears at 30 or 25 Hz. In video cameras with a progressive scan, each frame is scanned line-by-line and not interlaced; most are also displayed at 30 and 25 Hz.

Frame rate - The frame rate used to describe the frequency at which a video stream is updated is measured in frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Full-duplex - Transmission of data in two directions simultaneously. In an audio system this would describe e.g. a telephone systems. Half-duplex also provides bi-directional communication, but only in one direction at a time, as in a walkie-talkie system. See also *Simplex*.

Gain - Gain is the amplification factor and the extent to which an analog amplifier boosts the strength of a signal. Amplification factors are usually expressed in terms of power. The decibel (dB) is the most common way of quantifying the gain of an amplifier.

Gateway - A gateway is a point in a network that acts as an entry point to another network. In a corporate network for example, a computer server acting as a gateway often also acts as a proxy server and a firewall server. A gateway is often associated with both a router, which knows where to direct a given packet of data that arrives at the gateway, and a switch, which furnishes the actual path in and out of the gateway for a given packet.

GIF (Graphics Interchange Format) - GIF is one of the most common file formats used for images in web pages. There are two versions of the format, 87a and 89a. Version 89a supports animations, i.e. a short sequence of images within a single GIF file. A GIF89a can also be specified for interlaced presentation.

GOV (Group Of VOPs) - A group of VOPs is the basic unit of an H.264 video stream. The GOV contains different types and numbers of VOPs (I-VOPs, P-VOPs) as determined by the GOV length and GOV structure. See also *VOP*.

GOV length - The GOV length determines the number of images (VOPs) in the GOV structure. See also *GOV* and *VOP*.

GOV structure - The GOV structure describes the composition of an H.264 video stream, as regards the type of images (I-VOPs or P-VOPs) included in the stream, and their internal order. See also *GOV* and *VOP*.

H.264 - A standard for video compression, also known as MPEG-4 Part 10.

Half-duplex - See *Full-duplex*.

HDTV - High-definition television, high resolution digital video.

HTML (Hypertext Markup Language) - HTML is the set of "markup" symbols or codes inserted in a file intended for display in web browser. The markup tells the browser how to display the page's words and images for the user.

HTTP (Hypertext Transfer Protocol) - HTTP is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the web. The HTTP protocol runs on top of the TCP/IP suite of protocols.

Hub - A (network) hub is used to connect multiple devices to the network. The hub transmits all data to all devices connected to it, whereas a switch will only transmit the data to the device it is specifically intended for.

IEEE 802.11 - A family of standards for wireless LANs. The 802.11 standard supports 1 or 2 Mbit/s transmission on the 2.4 GHz band. IEEE 802.11b specifies an 11 Mbit/s data rate on the 2.4 GHz band, while 802.11a allows up to 54 Mbit/s on the 5 GHz band.

Image compression - Image compression minimizes the file size (in bytes) of an image. Two of the most common compressed image formats are JPEG and GIF.

Interlacing - Interlaced video is video captured at 50 pictures (known as fields) per second, of which every 2 consecutive fields (at half height) are then combined into 1 frame.

Interlacing was developed many years ago for the analog TV world and is still used widely today. It provides good results when viewing motion in standard TV pictures, although there is always some degree of distortion in the image.

To view interlaced video on e.g. a computer monitor, the video must first be de-interlaced, to produce progressive video, which consists of complete images, one after the other, at 25 frames per second. See also *Progressive scan*.

IP (Internet Protocol) – The Internet Protocol is a method transmitting data over a network. Data to be sent is divided into individual and completely independent "packets." Each computer (or host) on the Internet has at least one address that uniquely identifies it from all others, and each data packet contains both the sender's address and the receiver's address.

The Internet Protocol ensures that the data packets all arrive at the intended address. As IP is a connectionless protocol, which means that there is no established connection between the communication end-points, packets can be sent via different routes and do not need to arrive at the destination in the correct order.

Once the data packets have arrived at the correct destination, another protocol - Transmission Control Protocol (TCP) - puts them in the right order. See also *TCP*.

IP Address – An IP address is simply an address on an IP network used by a computer/device connected to that network. IP addresses allow all the connected computers/devices to find each other and to pass data back and forth.

To avoid conflicts, each IP address on any given network must be unique. An IP address can be assigned as fixed, so that it does not change, or it can be assigned dynamically (and automatically) by DHCP.

An IP address consists of four groups (or quads) of decimal digits separated by periods, e.g. 130.5.5.25. Different parts of the address represent different things. Some part will represent the network number or address, and some other part will represent the local machine address.

See also *IP (Internet Protocol)*.

I-VOP – See *VOP*.

JPEG (Joint Photographic Experts Group) – Together with the GIF file format, JPEG is an image file type commonly used on the web. A JPEG image is a bitmap, and usually has the file suffix '.jpg' or ".jpeg." When creating a JPEG image, it is possible to configure the level of compression to use. As the lowest compression (i.e. the highest quality) results in the largest file, there is a trade-off between image quality and file size.

kbit/s (kilobits per second) – A measure of the bit rate, i.e. the rate at which bits are passing a given point. See also *Bit rate*.

LAN (Local Area Network) – A LAN is a group of computers and associated devices that typically share common resources within a limited geographical area.

Linux – Linux is an open source operating system within the UNIX family. Because of its robustness and availability, Linux has won popularity in the open source community and among commercial application developers.

MAC address (Media Access Control address) – A MAC address is a unique identifier associated with a piece of networking equipment, or more specifically, its interface with the network. For example, the network card in a computer has its own MAC address.

Manual iris – This is the opposite to an autoiris, i.e. the camera iris must be adjusted manually to regulate the amount of light allowed to reach the image sensor.

Mbit/s (Megabits per second) – A measure of the bit rate, i.e. the rate at which bits are passing a given point. Commonly used to give the 'speed' of a network. A LAN might run at 10 or 100 Mbit/s. See also *Bit rate*.

Monitor – A monitor is very similar to a standard television set, but lacks the electronics to pick up regular television signals.

Motion JPEG – Motion JPEG is a simple compression/decompression technique for networked video. Latency is low and image quality is guaranteed, regardless of movement or complexity of the image. Image quality is controlled by adjusting the compression level, which in turn provides control over the file size, and thereby the bit rate.

High-quality individual images from the Motion JPEG stream are easily extracted. See also JPEG.

Megapixel – See *Pixel*.

MPEG (Moving Picture Experts Group) – The Moving Picture Experts Group develops standards for digital video and audio compression. It operates under the auspices of the International Organization for Standardization (ISO). The MPEG standards are an evolving series, each designed for a different purpose.

MPEG-2 – MPEG-2 is the designation for a group of audio and video coding standards, and is typically used to encode audio and video for broadcast signals, including digital satellite and Cable TV. MPEG-2, with some modifications, is also the coding format used by standard commercial DVD movies.

Multicast – Bandwidth-conserving technology that reduces bandwidth usage by simultaneously delivering a single stream of information to multiple network recipients.

Network connectivity – The physical (wired or wireless) and logical (protocol) connection of a computer network or an individual device to a network, such as the Internet or a LAN.

NTSC (National Television System Committee) – NTSC is the television and video standard in the United States. NTSC delivers 525 lines at 60 half-frames/second.

NWay – A network protocol that automatically negotiates the highest possible common transmission speed between two devices.

PAL (Phase Alternating Line) – PAL is the dominant television standard in Europe. PAL delivers 625 lines at 50 half-frames/second.

Ping – Ping is a basic network program used diagnostically to check the status of a network host or device. Ping can be used to see if a particular network address (IP address or host name) is occupied or not, or if the host at that address is responding normally. Ping can be run from e.g. the Windows Command

prompt or the command line in UNIX.

Pixel - A pixel is one of the many tiny dots that make up a digital image. The color and intensity of each pixel represents a tiny area of the complete image.

PoE (Power over Ethernet) - Power over Ethernet provides power to a network device via the same cable as used for the network connection. This is very useful for IP-Surveillance and remote monitoring applications in places where it may be too impractical or expensive to power the device from a power outlet.

PPP (Point-to-Point Protocol) - A protocol that uses a serial interface for communication between two network devices. For example, a PC connected by a phone line to a server.

PPTP (Point-to-Point Tunneling Protocol) - A protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. In this way a corporation can effectively use a WAN (Wide Area Network) as a large single LAN (Local Area Network). This kind of interconnection is known as a virtual private network (VPN).

Pre/post alarm images - The images from immediately before and after an alarm. These images are stored in a buffer for later retrieval.

Progressive scan - Progressive scan, as opposed to interlaced video, scans the entire picture, line by line every sixteenth of a second. In other words, captured images are not split into separate fields as in interlaced scanning.

Computer monitors do not need interlace to show the picture on the screen, but instead show them progressively, on one line at a time in perfect order, i.e. 1, 2, 3, 4, 5, 6, 7 etc., so there is virtually no 'flickering' effect. In a surveillance application, this can be critical when viewing detail within a moving image, such as a person running. A high-quality monitor is required to get the best from progressive scan. See also *Interlacing*.

Protocol - A special set of rules governing how two entities will communicate. Protocols are found at many levels of communication, and there are hardware protocols and software protocols.

Proxy server - In an organization that uses the Internet, a proxy server acts as an intermediary between a workstation user and the Internet. This provides security, administrative control, and a caching service. Any proxy server associated with a gateway server, or part of a gateway server, effectively separates the organization's network from the outside network and the local firewall. It is the firewall server that protects the network against outside intrusion.

A proxy server receives requests for Internet services (such as web page requests) from many users. If the proxy server is also a cache server, it looks in its local cache of previously downloaded web pages. If it finds the page, it is returned to the user without forwarding the request to the Internet. If the page is not in the cache, the proxy server, acting as a client on behalf of the user, uses one of its own IP addresses to request the page from another server over the Internet. When the requested page is returned, the proxy server forwards it to the user that originally requested it.

P-VOP - See *VOP*.

Resolution - Image resolution is a measure of how much detail a digital image can hold: the greater the resolution, the greater the level of detail. Resolution can be specified as the number of pixel-columns (width) by the number of pixel-rows (height), e.g. 320x240.

Alternatively, the total number of pixels (usually in megapixels) in the image can be used. In analog systems it is also common to use other format designations, such as CIF, QCIF, 4CIF, etc.

RTCP (Real-Time Control Protocol) - RTCP provides support for real-time conferencing of groups of any size within an intranet. This support includes source identification and support for gateways like audio and video bridges as well as multicast-to-unicast translators.

RTCP offers quality-of-service feedback from receivers to the multicast group as well as support for the synchronization of different media streams.

RTP (Real-Time Transport Protocol) - RTP is an Internet protocol for the transport of real-time data, e.g. audio and video. It can be used for media-on-demand as well as interactive services such as Internet telephony.

RTSP (Real Time Streaming Protocol) - RTSP is a control protocol, and a starting point for negotiating transports such as RTP, multicast and Unicast, and for negotiating codecs.

RTSP can be considered a 'remote control' for controlling the media stream delivered by a media server. RTSP servers typically use RTP as the protocol for the actual transport of audio/video data.

Router - A device that determines the next network point to which a packet should be forwarded on its way to its final destination. A router creates and/or maintains a special routing table that stores information on how best to reach certain destinations. A router is sometimes included as part of a network switch. See also *switch*.

Server - In general, a server is a computer program that provides services to other computer programs in the same or other computers. A computer running a server program is also frequently referred to as a server. In practice, the server may contain any number of server and client programs. A web server is the computer program that supplies the requested HTML pages or files to the client (browser).

Sharpness - This is the control of fine detail within a picture. This feature was originally introduced into color TV sets that used notch filter decoders. This filter took away all high frequency detail in the black and white region of the picture. The sharpness control attempted to put some of that detail back in the picture. Sharpness controls are mostly superfluous in today's high-end TVs. The only logical requirement for it nowadays is on a VHS machine.

Simplex - In Simplex operation, a network cable or communications channel can only send information in one direction.

SMTP (Simple Mail Transfer Protocol) - SMTP is used for sending and receiving e-mail. However, as it is 'simple,' it is limited in its ability to queue messages at the receiving end, and is usually used with one of two other protocols, POP3 or

IMAP. These other protocols allow the user to save messages in a server mailbox and download them periodically from the server.

SMTP authentication is an extension of SMTP, whereby the client is required to log into the mail server before or during the sending of email. It can be used to allow legitimate users to send email while denying the service to unauthorized users, such as spammers.

SNMP (Simple Network Management Protocol) – SNMP forms part of the Internet Protocol suite, as defined by the Internet Engineering Task Force. The protocol can support monitoring of network-attached devices for any conditions that warrant administrative attention.

Sockets – Sockets are a method for communication between a client program and a server program over a network. A socket is defined as 'the endpoint in a connection.' Sockets are created and used with a set of programming requests or 'function calls' sometimes called the sockets application programming interface (API).

SSL/TSL (Secure Socket Layer/Transport Layer Security) These two protocols (SSL is succeeded by TSL) are cryptographic protocols that provide secure communication on a network. SSL is commonly used over HTTP to form HTTPS, as used e.g. on the Internet for electronic financial transactions. SSL uses public key certificates to verify the identity of the server.

Subnet/subnet mask – A subnet is an identifiably separate part of an organization's network. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network (LAN). Having an organization's network divided into subnets allows it to be connected to the Internet with a single shared network address.

The subnet mask is the part of the IP address that tells a network router how to find the subnet that the data packet should be delivered to. Using a subnet mask saves the router having to handle the entire 32-bit IP address; it simply looks at the bits selected by the mask.

Switch – A switch is a network device that connects network segments together, and which selects a path for sending a unit of data to its next destination. In general, a switch is a simpler and faster mechanism than a router, which requires knowledge about the network and how to determine the route. Some switches include the router function. See also *Router.*

TCP (Transmission Control Protocol) – TCP is used along with the Internet Protocol (IP) to transmit data as packets between computers over the network. While IP takes care of the actual packet delivery, TCP keeps track of the individual packets that the communication (e.g. requested a web page file) is divided into, and, when all packets have arrived at their destination, it reassembles them to re-form the complete file.

TCP is a connection-oriented protocol, which means that a connection is established between the two end-points and is maintained until the data has been successfully exchanged between the communicating applications.

Telnet – Telnet is a simple method with which to access another network device, e.g. a computer. The HTTP protocol and the FTP protocols allow you to request specific files from remote computers, but do not allow you logon as a user of that computer. With Telnet, you log on as a regular user with whatever privileges you may have been granted for specific applications and data residing on that computer.

UDP (User Datagram Protocol) – UDP is a communications protocol that offers limited service for exchanging data in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP). The advantage of UDP is that it is not required to deliver all data and may drop network packets when there is e.g. network congestion. This is suitable for live video, as there is no point in re-transmitting old information that will not be displayed anyway.

Unicast – Communication between a single sender and a single receiver over a network. A new connection is established for each new user.

URL (Uniform Resource Locator) – An "address" on the network.

Varifocal lens – A varifocal lens provides a wide range of focal lengths, as opposed to a lens with a fixed focal length, which only provides one.

VPN (Virtual Private Network) – This creates a secure "tunnel" between the points within the VPN. Only devices with the correct "key" will be able to work within the VPN. The VPN network can be within a company LAN (Local Area Network), but different sites can also be connected over the Internet in a secure way. One common use for VPN is for connecting a remote computer to the corporate network, via e.g. a direct phone line or via the Internet.

VOP (Video Object Plane) – A VOP is an image frame in an H.264 video stream. There are several types of VOP:

- An I-VOP is complete image frame.

- A P-VOP codes the differences between images, as long as it is more efficient to do so. Otherwise it codes the whole image, which may also be a completely new image.

WAN (Wide-Area-Network) – Similar to a LAN, but on a larger geographical scale.

W-LAN (Wireless LAN) – A wireless LAN is a wireless local area network that uses radio waves as its carrier: where the network connections for end-users are wireless. The main network structure usually uses cables.

Web server – A web server is a program, which allows web browsers to retrieve files from computers connected to the Internet. The web server listens for requests from web browsers and upon receiving a request for a file sends it back to the browser.

The primary function of a web server is to serve pages to other remote computers; consequently, it needs to be installed on a computer that is permanently connected to the Internet. It also controls access to the server whilst monitoring and logging server access statistics.

WEP (Wireless Equivalent Privacy) – A wireless security protocol, specified in the IEEE 802.11 standard, which is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to that usually expected of a wired LAN. Security is at two different levels; 40-bit and 128-bit encryption. The higher the bit number, the

more secure the encryption.

WPA-PSK (Wi-Fi Protected Access - Pre-Shared Key) - This wireless encryption method uses a pre-shared key (PSK) for key management. Keys can usually be entered as manual hex values, as hexadecimal characters, or as a Passphrase. WPA-PSK provides a greater degree of security than WEP.

YPbPr - analog video signal for component video.

Zoom lens - A zoom lens can be moved (zoomed) to enlarge the view of an object to show more detail.

A
Absolute PTZ driver 26
Active/Inactive 22
Alarm 32, 47
AMC 7
ARP/Ping 39
Audio 15
Audio input 18
Audio output 19
Audio Settings 18
AVHS 39
AXIS Media Control 18

B
Backup 44
Bit Rate 15
Bonjour 7
Buffer Size 30

C
Camera tampering 31
CGI links 27
Click-in-image 27
COM Port 44
Continuous Recording 35
Control Button 46
Control panel 24, 27
Control queue 25, 27

D
Date & Time 38
Default Viewer 21
Disk Management 42
DNS Configuration 39
DNS Server 39
Domain Name 39

E
Emergency Recovery 50
Enable ARP/Ping 39
Event Servers 29
Events 29

F
Factory Default Settings 46
Frame Rate 14
FTP Server 29

G
Gatekeeper 31
GOV Settings 15

H
H.264 14, 15
HDTV 4, 14, 47
Host Name 40
HTTP Server 29
HTTPS 8, 36, 40

I
I/O Ports 43
Input 47
Installing PTZ devices 23
IP Address Filtering 36

L
Lens 47
Live View 9
Live View Config 20
Logs & Reports 44

M
Motion Detection 32, 47

N
NAT traversal 8, 40
Network Settings 38
NTP Server 38

O
ONVIF 2, 4, 52
Output 47
Output Buttons 22

P
Pan/Tilt/Zoom 26
Pinout - I/O connectors 47
Port Status 33
Ports & Devices 43
Pre- and post-trigger buffers 30
Preset Positions 24
PTZ commands 27
PTZ control panel 24, 27
PTZ control queue 25, 27
Pulse 22

Q
QuickTime 12, 21

R
Recording List 34
Recovery 50
Referrals 36
Relative PTZ driver 26
Restore 44

S
Save stream 30
Scheduled Event 31
Security 36
Server Time 38
Snapshot button 9
SNMP 42
Storage 42

Support 44
System Options 36

T

TCP Server 29
TCP/IP Settings 38
Time Mode 38
Troubleshooting 50

U

Upgrade Server 44
UPnP 40, 42
Users 36

V

Video Stream 14

Artisan Technology Group is an independent supplier of quality pre-owned equipment

Gold-standard solutions

Extend the life of your critical industrial, commercial, and military systems with our superior service and support.

We buy equipment

Planning to upgrade your current equipment? Have surplus equipment taking up shelf space? We'll give it a new home.

Learn more!

Visit us at **artisantg.com** for more info on price quotes, drivers, technical specifications, manuals, and documentation.

Artisan Scientific Corporation dba Artisan Technology Group is not an affiliate, representative, or authorized distributor for any manufacturer listed herein.

We're here to make your life easier. How can we help you today?

(217) 352-9330 | sales@artisantg.com | artisantg.com

ARTISAN® TECHNOLOGY GROUP