

**AXIS 247S
Video Server
User's Manual**

About This Document

This manual is intended for administrators and users of the AXIS 247S. It includes instructions for using and managing the Video Server on your network. Previous experience of networking will be of use when installing and using this product. Some knowledge of UNIX or Linux-based systems would also be beneficial, for developing shell scripts and applications. Later versions of this document will be posted to the Axis Website, as required. See also the product's online help, available via the Web-based interface.

Safety Notices Used In This Manual

Caution! - Indicates a potential hazard that can damage the product.
Important! - Indicates a hazard that can seriously impair operation.
Do not proceed beyond any of the above notices until you have fully understood the implications.

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.

Legal Considerations

Camera and audio surveillance can be prohibited by laws that vary from country to country. Check the laws in your local region before using this product for surveillance purposes. This product includes one (1) MPEG-4 decoder license. To purchase further licenses, contact your reseller.

Electromagnetic Compatibility (EMC)

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Re-orient or relocate the receiving antenna. Increase the separation between the equipment and receiver. Connect the equipment to an outlet on a different circuit to the receiver. Consult your dealer or an experienced radio/TV technician for help. Shielded (STP) network cables must be used with this unit to ensure compliance with EMC standards.

USA - This equipment has been tested and found to comply with the limits for a Class B computing device pursuant to Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his/her own expense will be required to take whatever measures may be required to correct the interference.

Europe - CE This digital equipment fulfills the requirements for radiated emission according to limit B of EN55022/1998, and the requirements for immunity according to EN55024/1998 residential, commercial, and light industry.

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.

Trademark Acknowledgments

Ethernet, Internet Explorer, Linux, Microsoft, Mozilla, OS/2, UNIX, Windows, WWW are registered trademarks of the respective holders. QuickTime™ is a trademark of Apple Computer, Inc., registered in the U.S. and other countries. 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 Services

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 staff by logging in to your private support area
- visit the Axis Support Web at www.axis.com/techsup/

Safety Notice - Battery Replacement

The Video Server uses a 3.0V CR2032 Lithium battery as the power supply for its internal real-time clock (RTC). This battery will, under normal conditions, last for a minimum of 5 years. Low battery power affects the operation of the RTC, causing it to reset at every power-up. A log message will appear when battery replacement is required.

The battery should not be replaced unless required!
If the battery does need replacing, observe the following points:

Caution!

- Danger of Explosion if battery is incorrectly replaced
- Replace only with the same or equivalent battery, as recommended by the manufacturer.
- Dispose of used batteries according to the manufacturer's instructions.

AXIS 247S Video Server User's Manual
Dated: April 2007
Copyright© Axis Communications AB, 2007

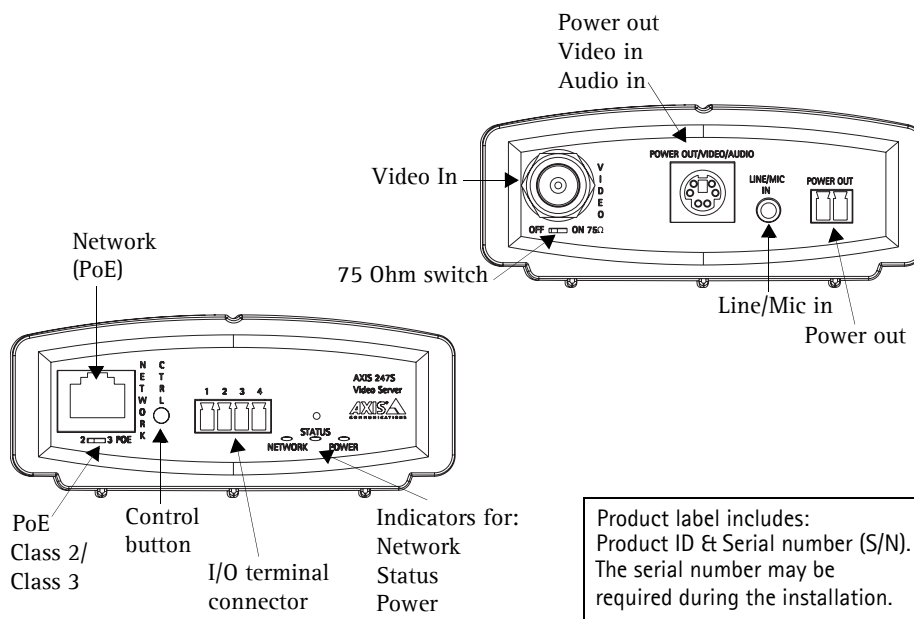
Revision 1.1
Part No: 29114

Table of contents

| | |
|---|----|
| Product Description | 4 |
| Using the Video Server | 5 |
| Accessing the Video Server | 5 |
| Video and Audio Streams | 7 |
| Video Stream Types | 7 |
| MPEG-4 protocols and communication methods | 8 |
| The AXIS Media Control | 8 |
| How to stream MPEG-4 | 8 |
| Other methods of accessing the video stream | 9 |
| Configuring the Video Server | 11 |
| Accessing the Setup tools | 11 |
| Video & Image Settings | 12 |
| Image Settings | 12 |
| Video Source Settings | 13 |
| Advanced - MPEG-4 Settings | 13 |
| Overlay/Mask Settings | 13 |
| Audio | 15 |
| Audio Settings | 15 |
| Live View Config | 16 |
| Layout | 16 |
| HTML Examples | 17 |
| External Video | 17 |
| Sequence Mode | 17 |
| Event Configuration | 18 |
| Event Servers | 18 |
| Event Types | 19 |
| Port Status | 21 |
| System Options | 22 |
| Security | 22 |
| Date & Time | 24 |
| Network - Basic TCP/IP Settings | 24 |
| Network - Advanced TCP/IP Settings | 26 |
| SOCKS | 27 |
| QoS (Quality of service) | 27 |
| SMTP (email) | 27 |
| SNMP | 28 |
| UPnP™ | 28 |
| RTP (Multicast)/MPEG-4 | 28 |
| Bonjour | 28 |
| Ports & Devices | 28 |
| Maintenance | 28 |
| Support | 29 |
| Advanced | 29 |
| Unit Connectors | 31 |
| Connection diagram | 31 |
| Troubleshooting | 33 |
| Checking the Firmware | 33 |
| Upgrading the Firmware | 33 |
| Support | 34 |
| Technical Specifications | 37 |
| Optimizing your system | 39 |
| Frame rates - Motion JPEG | 39 |
| Bandwidth | 40 |
| Glossary | 41 |
| Index | 43 |

Product Description

Video Server Connectors



Network Connector - The Video Server connects to the network via a standard, shielded network cable, and automatically detects the speed of the local network segment (10BaseT/100BaseTX Ethernet). PoE Supported.

Control Button - Press this button to restore the factory default settings, as described in *Resetting to the Factory Default Settings*, on page 30, or to install using AXIS Internet Dynamic DNS Service (see www.axiscam.net).

I/O Terminal connector - The I/O terminal connector provides the physical interface to 1 digital transistor output, 1 digital input and an auxiliary connection point for DC power. See *Unit Connectors*, on page 31 for more information.

Indicators - After completion of the startup and self test routines, the multi-colored Network, Status, Power Indicators flash as follows:

| 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. |
| | 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. |

Video Input - Coaxial BNC connector supporting a single composite video source. The physical connection is made using 75 Ohm coax video cable with a recommended maximum length of 800 feet (250 meters).

Mini-DIN - 6 pin Mini-DIN connector for power out, video in and audio in. See *Unit Connectors*, on page 31 for more information and a detailed description.

Line/Mic In - 3.5mm input for a mono microphone, or for line-in mono signal (only the left channel is used from a stereo signal).

Power out - Used to power a camera or other auxiliary equipment 12V DC, max. load 5W (420mA).

For more information on these connectors, please refer to *Unit Connectors*, on page 31.

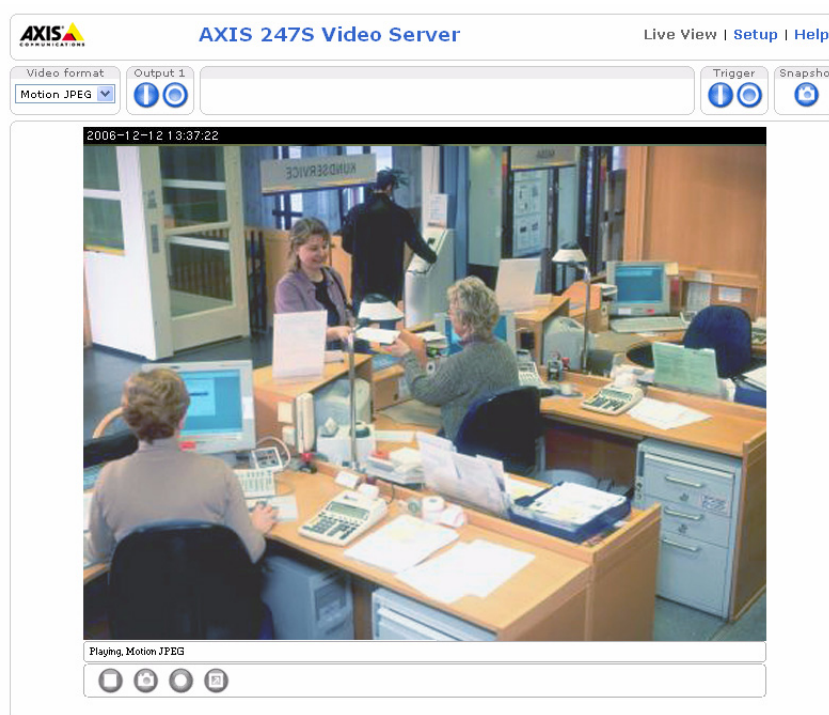
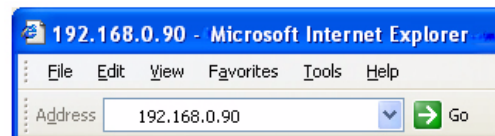
Using the Video Server

The Video Server can be used with most standard operating systems and browsers. The recommended browser is Internet Explorer with Windows, and Mozilla with other operating systems. See also the *Technical Specifications*, on page 37.

Note: For information on installing the Video Server, please refer to the Installation Guide.

Accessing the Video Server

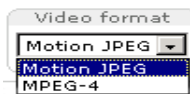
1. Start your browser.
2. Enter the IP address or host name of the Video Server in the Location/Address field of your browser.
3. Enter the user name and password set by the administrator.
4. A video image is displayed in your browser.



- Note:**
- To view streaming video in Microsoft Internet Explorer, you must set your browser to allow the AXIS Media Control (AMC) to be installed on your computer. AMC is required to use audio in the AXIS 247S. AMC also provides an MPEG-4 decoder for viewing MPEG-4 video streams. This decoder is installed the first time an MPEG-4 video stream is accessed. Please note that the product administrator may have disabled the installation of the decoder, as a license is required for each instance. See page 17 for more information.
 - If your workstation restricts the use of additional software components, the Video Server can be configured to use a Java applet for updating JPEG images. Please see the online help for more information.

The Live View page

If your Video Server 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:



The Video Format drop-down list allows the video format on the Live View page to be temporarily changed.

The **Output buttons** control an output directly from the Live View page. These buttons are configured under **Setup > Live View Config > Layout**.



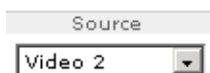
Pulse - click this button to activate the port for a defined period of time, e.g. to switch on a light for 20 seconds.



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



These buttons start/stop the **Sequence Mode**. This mode is created in **Setup > Live View Config > Sequence mode** and automatically displays the view from 2 or more video sources at set intervals.



From the **Source** list, select the desired video image(s). The list can contain internal video sources or external video sources.



The **Action buttons** trigger an event directly from the Live View page. These buttons are configured under **Setup > Live View Config > Layout**. Click these buttons to manually start and stop events.



Use the **Snapshot** button to capture a snapshot of the image currently being displayed in the window. Right-click on the image to save it in on your computer.

The **AMC viewer toolbar** (AXIS Media Control) is available in **Microsoft Internet Explorer only** and displays the following buttons:



The **Play/Stop** buttons start and stop the media stream.



The **Record** button is used to record the current video stream (MPEG-4 only). The Record function and the target directory for saving snapshots can be configured from AMC (AXIS Media Control), which is available from the Windows Control Panel (Internet Explorer only).



The **Snapshot** button takes a snapshot of the currently displayed image. The Snapshot function and the target directory for saving snapshots can be configured from AMC (AXIS Media Control), which is available from the Windows Control Panel (Internet Explorer only).



Click the **View Full Screen** button and the video image will fill the entire screen area. No other windows will be visible. Press Esc (Escape) on your keyboard to cancel full screen view.

Audio controls



Click the **Sound/Mute** button to switch the sound on and off.



Use the slider to control the volume (0 - 100).

Note that these AMC toolbar functions can also be accessed by right-clicking in the image.

Video and Audio Streams

The Video Server provides several different video and audio stream formats. The type to use depends on your requirements and on the properties of your network.

The Live View page in the Video Server provides access to Motion JPEG and MPEG-4 video and audio streams, as well as to single JPEG images. Other applications and clients can also access these video and audio streams/images directly, without going via the Live View page.

Video Stream Types

Motion JPEG

This format uses standard JPEG still images in 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 also provides excellent image quality and access to each and every individual image contained in the stream.

Note also that multiple clients accessing Motion JPEG streams can use different image settings.

MPEG-4

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

The MPEG-4 standard provides scope for a large range of different coding tools for use by various applications in different situations, and the Video Server provides certain subsets of these tools. These are represented as **Video object types**, which are selected for use with different viewing clients. The supported video object types are:

- **Simple** - sets the coding type to H.263
- **Advanced Simple** - in Axis products, this sets the coding type to MPEG-4 Part 2

AMC (AXIS Media Control) supports both object types, whilst e.g. QuickTime™ requires the Simple object type.

When using MPEG-4 it is also possible to control the bit rate, which in turn allows the amount of bandwidth usage to be controlled. CBR (constant bit rate) is used to achieve a specific bit rate by varying the quality of the MPEG-4 stream. When using VBR (variable bit rate), the quality of the video stream is kept as constant as possible, at the cost of a varying bit rate.

- Notes:**
- MPEG-4 is licensed technology. The Video Server includes one license for the decoder required for viewing in AMC. Installing additional unlicensed copies of this decoder is prohibited. To purchase more decoder licenses, contact your Axis reseller.
 - All clients viewing the MPEG-4 stream must use the same image settings.

MPEG-4 protocols and communication methods

To deliver live streaming video over IP networks, various combinations of transport protocols and broadcast methods are employed.

- RTP (Real-Time Transport Protocol) is a protocol that allows programs to manage the real-time transmission of multimedia data, via unicast or multicast.
- RTSP (Real-Time Streaming Protocol) serves as a control protocol, to negotiate which transport protocol to use for the stream. RTSP is thus used by a viewing client to start a unicast session, see below.
- UDP (User Datagram Protocol) 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.
- Unicasting is communication between a single sender and a single receiver over a network. This means that the video stream goes independently to each user, and each user gets their own stream. A benefit of unicasting is that if one stream fails, it only affects one user.
- Multicast is bandwidth-conserving technology that reduces bandwidth usage by simultaneously delivering a single stream of information to multiple network recipients. This technology is used primarily on delimited networks (intranets), as each user needs an uninterrupted data flow and should not rely on network routers.

The AXIS Media Control

The recommended method of accessing live video (MPEG-4 and/or Motion JPEG) and audio from the Video Server is to use the AXIS Media Control (AMC) in Microsoft Internet Explorer in Windows. This ActiveX component is automatically installed on first use, after which it can be configured by opening the AMC Control Panel applet from the Windows Control Panel. Alternatively, right-click the video image in Internet Explorer.

How to stream MPEG-4

Deciding on the combination of protocols and methods to use depends on your viewing requirements, and on the properties of your network. Setting the preferred method(s) is done in the control applet for AMC, which is found in the Windows Control Panel. When this has been set, AMC will test all the selected methods in the specified order, until the first functioning one is found.

RTP+RTSP

This method (actually RTP over UDP and RTSP over TCP) should be your first consideration for live video, especially when it is important to always have an up-to-date video stream, even if some images do get dropped. This can be configured as multicast or unicast.

Multicasting provides the most efficient usage of bandwidth, especially when there are large numbers of clients viewing simultaneously. Note however, that a multicast broadcast cannot pass a network router unless the router is configured to allow this. It is thus not possible to multicast over e.g. the Internet.

Unicasting should be used for video-on-demand broadcasting, so that there is no video traffic on the network until a client connects and requests the stream. However, if more and more unicast clients connect simultaneously, the server will at some point become overloaded. There is also a maximum of 20 simultaneous viewers to be considered.

RTP/RTSP

This unicast method is RTP tunneled over RTSP. This can be used to exploit the fact that it is relatively simple to configure firewalls to allow RTSP traffic.

RTP/RTSP/HTTP or RTP/RTSP/HTTPS

These two methods can also be used to traverse firewalls. Firewalls are commonly configured to allow the HTTP protocol, thus allowing RTP to be tunneled.

Other methods of accessing the video stream

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

- If supported by the client, the Video Server can use Motion JPEG server push to display video. This option maintains an open HTTP connection to the browser and sends data as and when required, for as long as required.
- As single JPEG images in a browser. Enter e.g. the path: `http://<ip>/axis-cgi/jpg/image.cgi?resolution=CIF`
- Windows Media Player. This requires AMC and the MPEG-4 decoder to be installed. The paths that can be used are listed below, in the order of preference.
- Unicast via RTP: `axrtpu://<ip>/mpeg4/#/media.amp`
- Unicast via RTSP: `axrtsp://<ip>/mpeg4/#/media.amp`
- Unicast via RTSP, tunneled via HTTP: `axrtsphhttp://<ip>/mpeg4/#/media.amp`
- Unicast via RTSP, tunneled via HTTPS: `axrtsphhttps://<ip>/mpeg4/#/media.amp`
- Multicast: `axrtpm://<ip>/mpeg4/#/media.amp`

- Notes:**
- <ip> = IP address.
 - # = video source number. This is set to 1 if omitted.

Other MPEG-4 clients

Although it may be possible to use other clients to view the MPEG-4 stream, it is not guaranteed to work in all cases.

For some other clients, e.g. QuickTime™ the Video Object Type must be set to *Simple*. It may also be necessary to adjust the advanced MPEG-4 settings.

To assess the video stream from e.g. QuickTime™ the following path can be used:

`rtsp://<ip>/mpeg4/#/media.amp`

This path is for all supported methods, and the client will negotiate with the Video Server to determine exactly which transport protocol to use.

- Notes:**
- <ip> = IP address.
 - # = video source number. This is set to 1 if omitted.

Audio transmission methods

The audio stream can be accessed in the Live View page when viewing either Motion JPEG or MPEG-4.

Using Motion JPEG

The basic transmission method of audio used in conjunction with Motion JPEG video streaming is transmission over HTTP. The video and audio streams are not synchronized when using Motion JPEG so the streams may be slightly out of sync. The latency in any stream should be low, but this will depend on the network infrastructure.

Using MPEG-4

When using MPEG-4, audio is streamed using the same protocol as the video stream.

When audio is transmitted using MPEG-4, the Axis product sends synchronization information along with the streams to the client that is performing the synchronization.

Note: Audio is streamed from the client to the server over HTTP when using Motion JPEG and MPEG-4.

Accessing the Audio Streams

In addition to accessing audio in the Live View page using AMC, audio from the Video Server can also be accessed in the following ways:

HTTP-API

You can read about accessing audio for the other protocols through the HTTP-API at <http://www.axis.com/techsup>

QuickTime/Windows Media Player

It is possible to use QuickTime and Windows Media Player to listen to the audio stream using the same methods to access video streams.

Java Applet

The Java applet supports simplex audio.

Configuring the Video Server

This section describes how to configure the Video Server and is intended for:

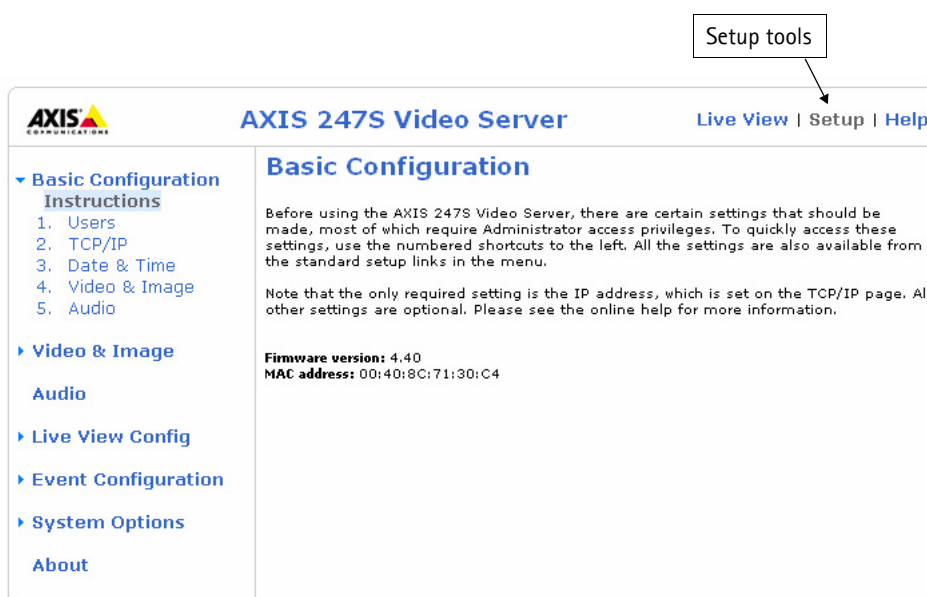
- **administrators**, who have unrestricted access to all the Setup tools
- **operators**, who have access to the Video & Image, Audio, Live View Config and Event Configuration settings.

The Video Server is configured from the **Setup link**, in a standard browser (see also the Technical Specifications on page 37).


Accessing the Setup tools

Follow the instructions below to access the Setup Tools from a browser.

1. Start the browser and enter the IP address or host name of the Video Server in the location/address field.
2. The Live View page is now displayed. Click **Setup** to display the **Setup tools**.



Video & Image Settings

The following descriptions show examples of the available features in the Video Server. For details of each setting, please refer to the online help available from each page. Click  to access the online help.

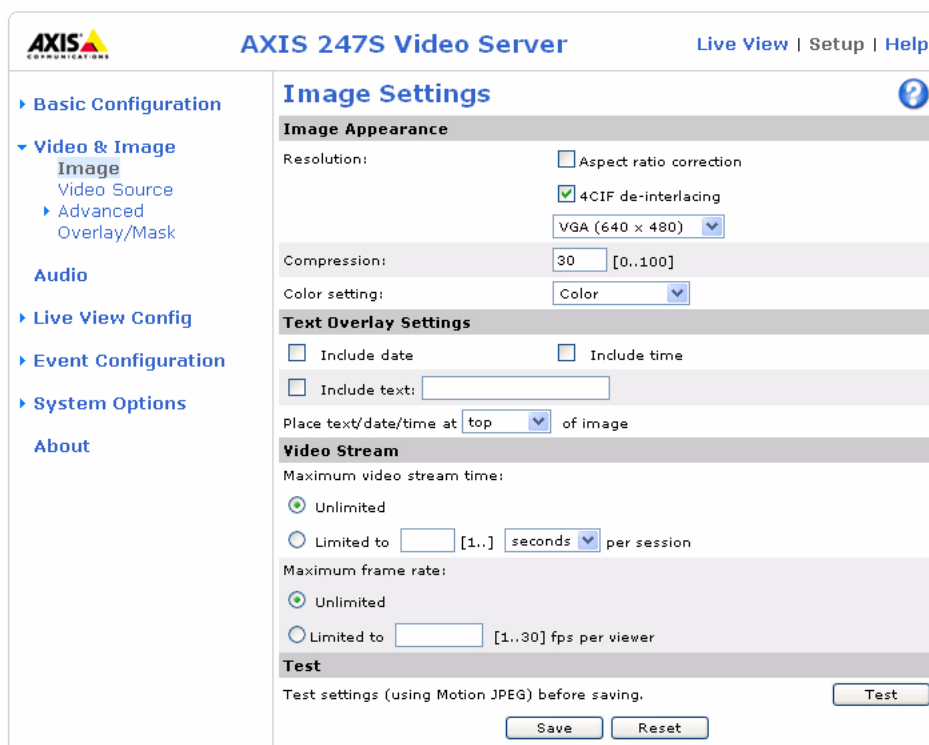


Image Settings

Image Appearance

Modify the **Image Appearance** to optimize the video images according to your requirements.

All configuration of images and overlays will affect the performance of the Video Server, depending on the usage and the available bandwidth.

- High resolution generates larger files
- Lower compression improves image quality, but generates larger files
- Black & White uses less bandwidth than Color

See also the specifications for frame rates and bandwidth on page 39.

Text Overlay Settings

Include date, time and/or text of your choice to be viewed on the image. The position of the text is set either to the top or the bottom of the image.

Video Stream

The **Maximum video stream time** can be set as *Unlimited*, or a **maximum stream time** per session in seconds, minutes or hours can be defined. When the set time has expired, a new stream can be started by refreshing the page in the Web browser. Note that the maximum video stream time does not apply to clients connecting via multicast.

To avoid bandwidth problems on the network, the **frame rate** allowed to each viewer can also be limited. Select either *Unlimited* or define a maximum frame rate per viewer.

Test

For a preview of the image and overlay settings before saving, click **Test**. When you are satisfied with the settings, click **Save**.

Video Source Settings

Eliminate any black borders surrounding the image, by making **Offset adjustments**. See the online help for more information.

Advanced - MPEG-4 Settings

Tools for adjusting the MPEG-4 settings and for controlling the video bit rate.

The MPEG-4 standard provides many different coding tools for various applications in different situations. As most MPEG-4 clients do not support all of these tools, it is usual to instead define and use subsets for different clients or groups of clients. These settings allow you to define the type of viewing client to use.

Adjusting the maximum bit rate and setting it to variable or constant is a good way of controlling the bandwidth used by the MPEG-4 video stream.

For more information on these advanced settings, please see the online help.

Overlay/Mask Settings

Overlay/Mask Type

Overlay/Mask Type allows you to place an overlay, or up to three privacy masks over the video image:

- Upload and place an image as an overlay - usually used to provide extra information in the video image.
- Place up to three privacy masks - up to 3 configurable masks can be used to conceal different areas of the video image.

Selecting the overlay/mask type from the menu will display further settings available for the selected type. See the online help for further information.



Note: If you need to see an area of the video that is covered by an overlay or mask, a privacy mask cannot be bypassed. An overlay image, however, can be bypassed via the AXIS VAPIX. See the Video Developer section on the Axis Web site for more information.

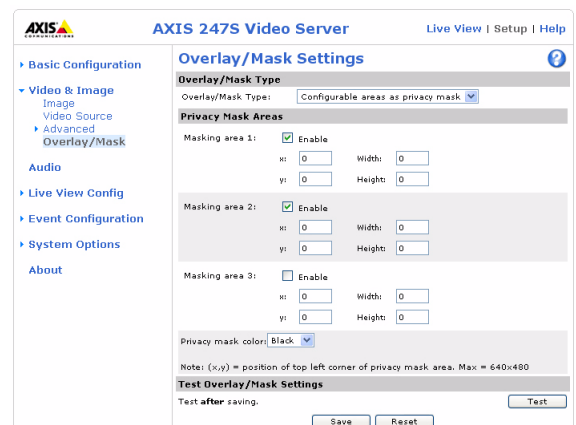
Upload and use an overlay image

To upload an overlay image:

1. Select **Uploaded image as overlay** in the drop-down list for **Overlay/Mask Type**. New options appear.
2. In the field **Upload own image**, click the **Browse** button and locate the image file on your computer or server.
3. Click the **Upload** button and follow the on-screen instructions.

To use an already uploaded image:

1. Select an uploaded image from the **Use image** drop-down list.
2. Place the image at the required location by entering the x and y coordinates.
3. Click **Save**.



Overlay image requirements:

| Image Formats | Image Size |
|--|---|
| <ul style="list-style-type: none"> Windows 24-bit BMP (full color) Windows 4-bit BMP (16 colors) | The height and width of the overlay image in pixels must be exactly divisible by 4. |

Overlay image limitations:

- The maximum overlay image size supported by the Video Server is the same as the maximum image resolution. See Technical Specifications, on page 37.
- When a text overlay is also used, this reduces the amount of space available to the overlay image. To keep the text readable at lower resolutions, the text overlay occupies proportionally more of the image at lower resolutions.
- If the overlay is initially positioned so that part of it is outside the video image, it will be relocated so that it appears over the video image, i.e. it is always the entire image that is displayed.

Please see the online help  for more information.

Use a Privacy Mask

To use privacy masks to hide different areas of the video image:

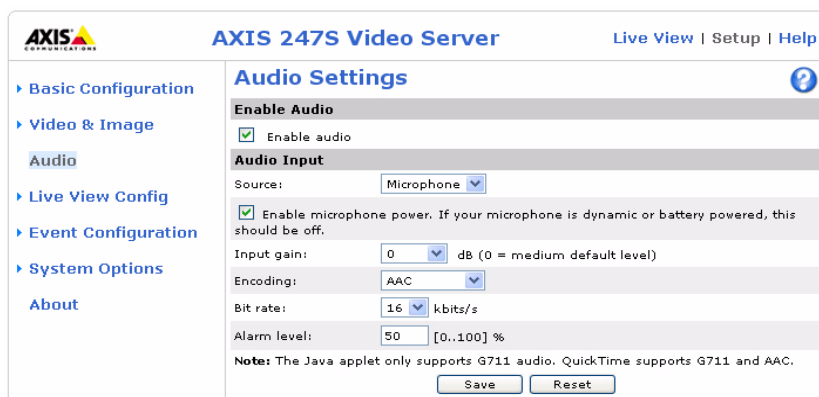
1. Select **Configurable areas as privacy mask** in the drop-down list for **Overlay/Mask Type**. New options appear.
2. Enter the (x,y) coordinates of the top left hand corner of the mask, and the height and width to define the masks' placement and size.
3. Select the privacy masks' color: black, grey, white, or red.
4. Click in the box beside **Enable** to enable one or more of the masks you have defined and click on **Save**.

Audio

The AXIS 247S can transmit audio to clients using e.g. an external microphone. See **Setup > Audio** to access the audio settings page.

Audio Settings

This section describes how to configure the basic audio settings for the AXIS 247S.



Enable Audio

Enable audio - Check this box to enable audio functionality.

Audio Input

Source - Select Microphone for an external microphone or Line for a Line in device, e.g. an audio mixer for multiple microphones or a microphone with a built-in amplifier.

The **Enable microphone power** option provides DC power for the external microphone. If you use a small electret condenser microphone such as a clip-on mic or a PC microphone, this option needs to be enabled.

To use a high impedance dynamic microphone, DC power should not be enabled. DC power will not harm the microphone, but if you are uncertain, try switching it off and on. DC power is enabled by default. To use a professional microphone requiring 48V phantom power, you need an external power supply and must use a balanced-unbalanced converter (audio transformer) in between.

If there are problems with the sound input being too low or high, it is possible to adjust the **input gain** for the connected microphone.

Select the desired audio **Encoding** format, AAC, G711, G726.

Depending on the selected encoding, set the desired **Bit rate** (audio quality). The settings depend on the available bandwidth and the required audio quality, i.e. a high bit rate setting requires more bandwidth.

Alarm level - Event types in the AXIS 247S can be set to use this level as a trigger. Each individual event type can be configured to trigger if the sound level rises above or falls below the set value.

The alarm level can be set in the range 0-100%, where 0% is the most sensitive and 100% the least sensitive.

Live View Config

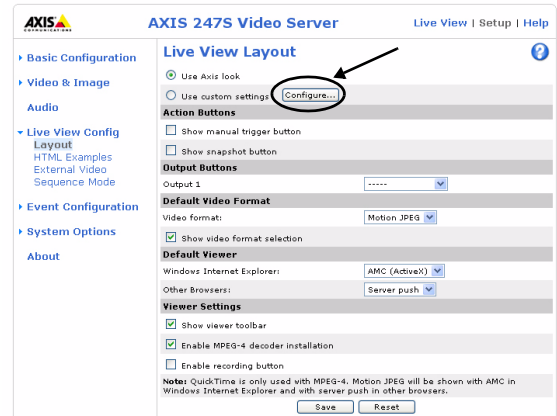
Layout

These are the tools for deciding the layout of the Live View page.

The layout can be set in 3 ways:

- Use Axis look - the layout is unchanged.
- Use custom settings - modify the default page with your own colors, images etc. Click the **Configure** button and see the following page.
- Own Home Page - Upload and use your own custom made page as the default web page. Click the **Configure** button and see the following page.

The other settings on this page concern which other features to include, e.g. buttons and links. See page 17 for more information.



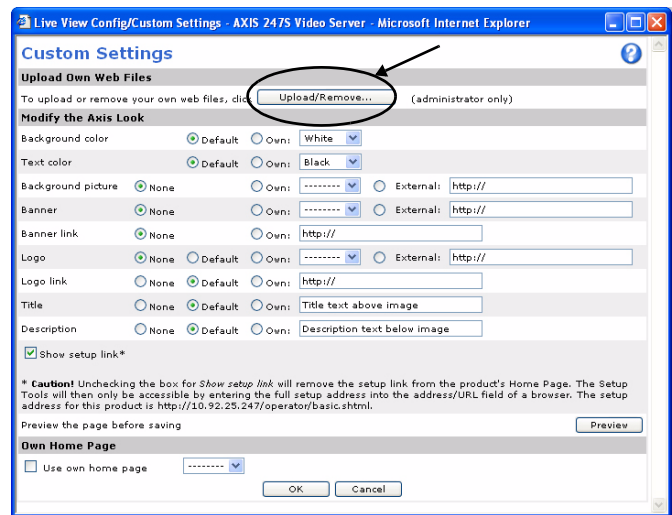
Customizing the default page

The appearance of the default Video Server Live View page can be customized to suit your own requirements, or you can upload and use your own home page. To upload your own files, click the **Upload/Remove** button and see the description below.

Upload Own Web Files

Your own web files, background picture, color etc. must first be uploaded to the Video Server in order to be available for selection in the **Custom Settings** setup dialog. Once uploaded, the files are shown in the drop-down list.

1. Enter the path to the file, e.g. a file located on your workstation or click the **Browse** button.
2. Select the user level for the uploaded file. Setting the user access level means that you have complete control over which pages can be viewed by which users.
3. When the path is shown correctly in the text field, click the **Upload** button.



The setup address is `http://<ip address>/operator/basic.shtml`

All uploaded files are shown in the list in the lower section of the page. To remove a file, check the box provided next to it and then click the **Remove** button.

- To use your uploaded file, click the radio button and select the file from the drop-down list by **Own**.
- To use an external file located somewhere other than in the Video Server, click the radio button and enter the URL by **External**:

Own Home Page

To use a previously uploaded web page as the default page, check the checkbox, select the page from the drop-down list and click **OK**.

Action Buttons

These buttons can be used to manually trigger and stop an event from the Live View page. See *Event Configuration*, on page 18. The snapshot button allows you to take a snapshot of the video stream and save it to a computer.

Output Buttons

These buttons are used to control the outputs on the Video Server and thus the equipment connected to them, e.g. to switch a light on or off:

- The Pulse button activates the port for a defined period
- Active/Inactive displays 2 buttons, one for each action (on/off)

Default Video Format

Select the default format to use on the Live View page. Checking the box for Show video format selection displays a drop-down list on the Live View page allowing you to temporarily change the format.

Default Viewer

Select from the drop-down list the viewer you wish to use for your web browser. Please see the online help for more information.

Viewer Settings

Checking the **Show viewer toolbar** box displays the AMC toolbar under the video stream in Microsoft Internet Explorer.

By checking the **Enable MPEG-4 decoder installation** box, it is also possible for the Administrator to enable or disable the installation of the MPEG-4 decoder. This is used to prevent the installation of unlicensed copies. Further decoder licenses can be purchased from your Axis dealer.

Default Viewer for Motion JPEG

Select the appropriate radio button to define the method for viewing moving video images, depending on your browser and settings.

Please see the online help  for more information.

HTML Examples

You can add live video from your Video Server to your own web site. The Video Server can send Motion-JPEG or MPEG-4 images to up to 10 simultaneous connections, although an administrator can restrict this to fewer. This does not affect or include the number of multicast viewers.

Enter the **Image Type**, **Image size** and other settings to suit your web page and click **Update**.

External Video

You can add links to other Axis network devices available over the network. These sources can be displayed on the Live View page, just as if they were video sources connected directly to the Video Server.

Click the **Add** button to open the External Video Source Setup dialog, which is used to make all the necessary settings.

Example of a path to an external video source:


```
http://192.168.0.125/axis-cgi/mjpeg/video.cgi
```

Sequence Mode

The live view page can be configured to rotate through selected internal and/or external video sources, in order or randomly.



Select the desired video sources and enter the time in seconds to display each source (up to 59 minutes). Click **Save**.

The Sequence buttons will appear on the Live View page to allow the viewer to start and stop the sequence mode. Please see the online help  for more information.

Event Configuration


This section describes how to configure the Video Server for alarm handling. Various actions can be configured to run when certain types of events occur.

| | | |
|-------------------------------|--|--|
| Event type | A set of parameters describing how and when the Video Server is to perform certain actions | |
| Triggered Event (see page 19) | - the circumstances that start an event | e.g. at a signal from an external device, such as a door switch or a motion sensor |
| Scheduled Event (see page 20) | - the circumstances that start an event | e.g. at a pre-programmed time |
| Action | - what occurs when the event runs | e.g. video images uploaded to an FTP server, email notification sent, etc. |

Event Servers

Event Servers are used for e.g. receiving uploaded image files and/or notification messages. To set up an Event server for your Video Server, go to **Setup > Event Configuration > Event Servers** and enter the required information according to the selected server type.

| Server type | Purpose | Information required |
|-------------|--|--|
| FTP Server | <ul style="list-style-type: none"> receives uploaded images | <ul style="list-style-type: none"> Descriptive name of your choice User Name and Password (to FTP server) Upload path, e.g. images/ Port number Use passive mode if there is a firewall between the Video Server and FTP server Use temporary file if your FTP server doesn't allow an existing file to be overwritten by a new file with the same name. |
| HTTP Server | <ul style="list-style-type: none"> receives uploaded images receives notification messages | <ul style="list-style-type: none"> Descriptive name of your choice URL (address) User Name and Password (to HTTP server) Proxy address/Proxy port (if required) Proxy User Name and Password (if required) |
| TCP Server | <ul style="list-style-type: none"> receives notification messages | <ul style="list-style-type: none"> Descriptive name of your choice User Name and Password (for TCP server) Port number |

For details on each setting, please refer to the online help  available from each web page.

Note: Pre-trigger and Post-trigger buffers will be lost if the connection to the event server fails.

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

An event in the AXIS 247S is when a **trigger** is activated, causing a certain action to be performed. The event is the set of parameters (or conditions) that specifies how and when which actions will be performed. A common event is when an Input/output is activated when triggered by an alarm.

This section describes how to configure the AXIS 247S to perform certain actions when an event (e.g. an alarm) occurs.

Event Types

An Event Type is a set of parameters describing how and when the Video Server is to perform certain actions.

Example: If somebody walks past the connected camera, and an event has been configured to act on this, the Video Server can e.g. record and send video images to an FTP server, or send a notification email to a pre-configured email address with a pre-configured message. Video images can be sent as an attachment with the email.

Triggered Event

A triggered event is activated by e.g:

- a push button connected to an input port on the Video Server
- a manually activated action e.g. from an action button in the web interface
- a lost signal from a video source
- detected movement in a configured motion detection window
- the sound level if it rises above or drops below the set alarm level
- on restart (reboot) after e.g. power loss

How to set up a triggered event

This example describes how to set the Video Server to upload images when the main door is opened:

1. Click **Add triggered** on the Event types page.
2. Enter a descriptive **name** for the event, e.g. Main door.
3. Set the **priority** - High, Normal or Low (see online help files).
4. Select which **Video Source** the event is to act on, e.g. Video 1 on Main door.
5. Set the **Respond to Trigger...** parameters when the event is to be active, e.g. only after office hours
6. Select the trigger alternative from the **Triggered by...** drop-down list, e.g. an Input port with a connected sensor if the door is opened.
7. Set the **When Triggered...** parameters, i.e. set what the Video Server should do if the main door is opened, e.g. upload images to an FTP server.
8. Click **OK** to save the event in the Event Types list.

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

Pre-trigger and Post-trigger buffers

This function is very useful when checking to see what happened immediately before and after a trigger, e.g. 2 minutes before and after a door was opened. Check the **Upload images** checkbox under **Event Types > Add Triggered... > When triggered...** to expand the web page with the available options.

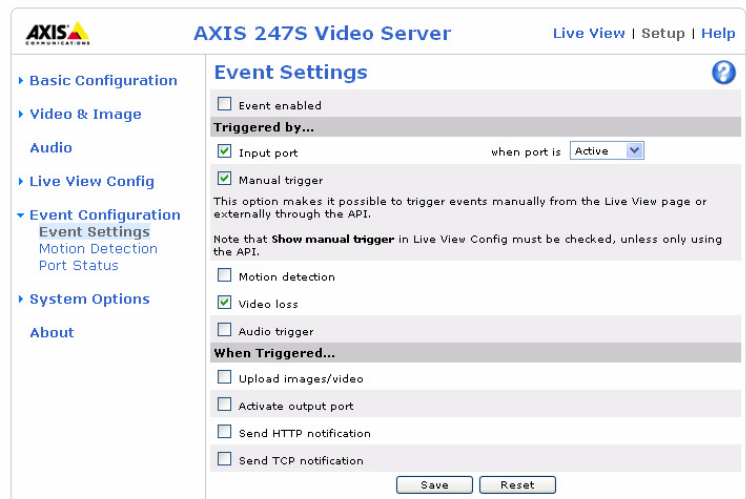
Buffer size - up to 9 MB

The maximum length of time of the pre-/post-buffer depends on the selected image size and frame rate.

Include pre-trigger buffer - images stored internally in the server from the time immediately preceding the trigger. Check the box to enable the pre-trigger buffer, enter the desired length of time and specify the required image frequency.

Include post-trigger buffer - contains images from the time immediately after the trigger. Configure as for pre-trigger.

Note: If the pre- or post-buffer is too large for the Video Server's internal memory, the frame rate will be reduced and individual images may be missing. If this occurs, an entry will be created in the unit's log file.



Continue image upload (unbuffered) - enable the upload of images for a fixed length of time. Specify the length of time for the uploaded recording, in seconds, minutes or hours, or for as long as the trigger is active. Finally, set the desired image frequency to the maximum (the maximum available) or to a specified 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.

Scheduled Event

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

How to set up a scheduled event

This example describes how to set the Video Server to send an email notification with saved images from a set time:

1. Click **Add scheduled** on the **Event types** page.
2. Enter a descriptive **name** for the event, e.g. Scheduled email.
3. Set the **priority** (High, Normal or Low).
4. Select the **video source** i.e. the source the event should act on, e.g. Video 2 in Storage room.
5. Set the **Activation Time** parameters (24h clock) when the event should be active, e.g. start on Sundays at 13.00 with a duration of 12 hours.
6. Set the **When Activated...** parameters i.e. set what the Video Server should do at the specified time e.g. send uploaded images to an email address.

Click **OK** to save the Event in the Event Types list.

Motion Detection

The motion detection feature is used to generate an alarm whenever movement occurs (or stops) in the video image. A total of 10 Include and/or Exclude windows can be configured.

- **Included** windows target specific areas within the whole video 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 will appear in the list of available triggers, for triggering events. See the section on *Event Configuration* above.

Note: Using the motion detection feature may decrease the overall performance of the Video Server.

How to configure Motion Detection

1. Click **Motion Detection** in the **Event Configuration** menu.
2. Click the **Configure Included Window** radio button.
3. Click **New**, or if using the Java Applet, click **Add Window**.
4. Enter a descriptive name under **Window name**.
5. Adjust the size (drag the bottom right-hand corner) and position (click on the text at the top and drag to the desired position).
6. Adjust the Object size, History and Sensitivity profile sliders (see table below for details). Any detected motion within an active window is then indicated by red peaks in the **Activity** window (the active window has a red frame).
7. Click **Save**.

To exclude parts of the Include window, click the **Configure Excluded Windows** button and position the Exclude window as required, within the Include window.

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 region 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 region will trigger motion detection for a very short period | Only very bright objects on a dark background will trigger motion detection |
| Default value | Low | Medium to High | Medium to High |

Examples:

- Avoid triggering on small objects in the video image by setting the object size level to high.
- 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, low sensitivity can be selected. In other cases, a high sensitivity level is recommended.

Port Status

Under **Event Configuration > Port Status** there is a list showing the status for the connected input/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**.

System Options

Security

User access control is enabled by default, when the administrator sets the root password on first access. New users are authorized with user names and passwords, or the administrator can choose to allow anonymous viewer login to the Live View page, as described below:

Users - the user list displays the authorized users and access levels:

| | |
|----------------------|---|
| Viewer | Provides the lowest level of access, which only allows the user access to the Live View page |
| Operator | An Operator can view the Live View page, create and modify event types and adjust certain other settings. The Operator does not have access to the Systems Options configuration pages. |
| Administrator | An administrator has unrestricted access to the Setup Tools and can determine the registration of all other users. |

User Settings - check the corresponding checkboxes to enable:

- **Anonymous viewer login** - allows any viewer direct access to the Live View page.

IP Address Filtering

Checking the **Enable IP address filtering** box enables the IP address filtering function. Up to 256 IP address entries may be specified (a single entry can contain multiple IP addresses). Click the **Add** button to add new filtered addresses.

When the IP address filter is enabled, addresses added to the list are set as allowed or denied addresses. All other IP addresses not in this list will then be allowed or denied access accordingly, i.e. if the addresses in the list are allowed, then all others are denied access, and vice versa. See also the online help for more information.

Note that users from IP addresses that will be allowed must also be registered with the appropriate access rights (**Viewer, Operator or Administrator**). This is done from **Setup > System Options > Security > Users**.

Referrals - to prevent unauthorized sources from including the video stream from the Video Server into external Web pages, check the **Referrals** box and enter the IP address or Host name of the computer that hosts the Web pages with the included video stream. Multiple IP addresses/host names can be defined and are separated by semicolons(;

- Notes:**
- If the referrals feature is enabled and you wish to also allow normal access to the Live View page, the product's own IP address or host name must be added to the list of allowed referrers.
 - Restricting referrers has no effect on an MPEG-4 video stream. To restrict an MPEG-4 stream, IP address filtering must be enabled.
 - Restricting referrers is of greatest value when not using IP address filtering. If IP address filtering is used, then the allowed referrers are automatically restricted to those allowed IP addresses.

HTTPS

For greater security, the Video Server can be configured to use HTTPS (Hypertext Transfer Protocol over SSL (Secure Socket Layer)). That is, all communication that would otherwise go via HTTP will instead go via an encrypted HTTPS connection.

Certificate - to use HTTPS for communication with the Video Server, a **Certificate** must be created using one of these methods:

- A self-signed certificate can be created in the Video Server, but this does not guarantee the same level of security as an official certificate.
- An official certificate issued by a CA (Certificate Authority). A CA issues and manages security credentials and public keys for message encryption.

1. Click either **Create self-signed certificate** or **Create Certificate Request** and enter the required information in the provided fields
2. Click **OK**.

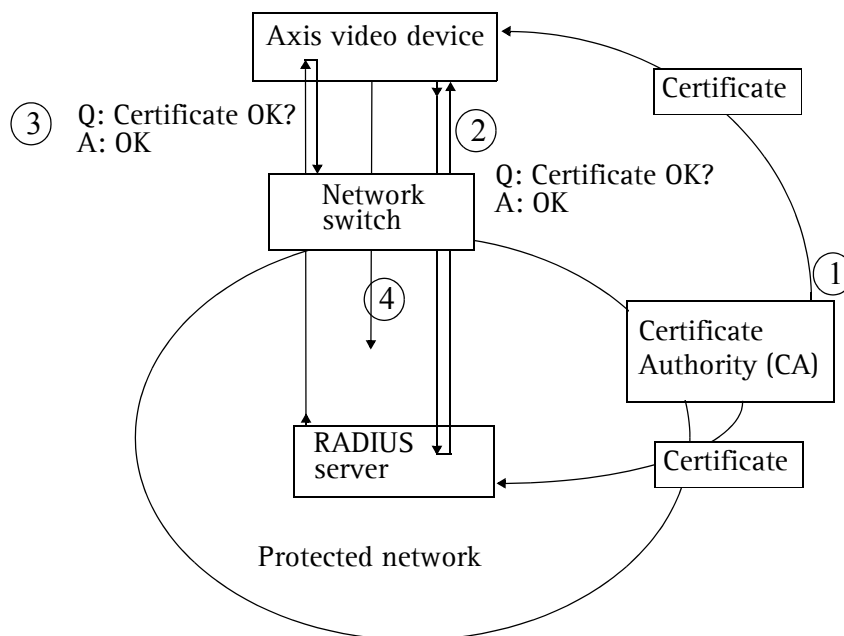
3. **Create self-signed certificate** generates and installs a certificate which will be displayed under **Installed Certificate**.
Create Certificate Request generates a PEM formatted request which you copy and send to a CA for signing. When the signed certificate is returned, click **Install signed certificate...** to install the certificate in the Video Server.
4. Set the **HTTPS Connection Policy** for the administrator, Operator and Viewer to enable HTTPS connection (set to HTTP by default)

Please refer to the home page of your preferred CA for information on where to send the request etc. For more information, please see the online help [?](#)

802.1X - Network Admission Control

IEEE 802.1X is an IEEE standard for port-based Network Admission Control. It provides authentication to devices attached to a network port (wired or wireless), establishing a point-to-point connection, or, if authentication fails, preventing access on that port. 802.1X is based on EAP (Extensible Authentication Protocol).

The authentication process



1. A CA server provides the required signed certificates.
2. The Axis video device requests access to the protected network at the network switch. The switch forwards the video device's CA certificate to the RADIUS server, which then replies to the switch.
3. The switch forwards the RADIUS server's CA certificate to the video device, which also replies to the switch.
4. The switch keeps track of all responses to the validation requests. If all certificates are validated, the Axis video device is allowed access to the protected network via a preconfigured port.

In a 802.1X enabled network switch, clients equipped with the correct software can be authenticated and allowed or denied network access at the Ethernet level.

Clients and servers in an 802.1x network may need to authenticate each other by some means. In the Axis implementation this is done with the help of digital certificates provided by a **Certification Authority**. These are then validated by a third-party entity, such as a **RADIUS server**, examples of which are Free Radius and Microsoft Internet Authentication Service.

To perform the authentication, the RADIUS server uses various EAP methods/protocols, of which there are many. The one used in the Axis implementation is EAP-TLS (EAP-Transport Layer Security).

The AXIS network video device presents its certificate to the network switch, which in turn forwards this to the RADIUS server. The RADIUS server validates or rejects the certificate and responds to the switch, and sends its own certificate to the client for validation. The switch then allows or denies network access accordingly, on a preconfigured port.

RADIUS

RADIUS (Remote Authentication Dial In User Service) is an AAA (Authentication, Authorization and Accounting) protocol for applications such as network access or IP mobility. It is intended to work in both local and roaming situations.

CA servers

In cryptography, a Certification Authority (CA) is an entity that provides signed digital certificates for use by other parties, and thus acts a trusted third party.

There are many commercial CA's that charge for their services. Institutions and governments may have their own CA, and there are free CA's available.

Date & Time

Current Server Time - displays the current date and time (24h clock). The time can be displayed in 12h clock format in overlay images.

New Server Time - Select your time zone from the drop-down list and check the daylight saving time changes, if desired.


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 Video Server will obtain the time from an NTP server every 60 minutes. Specify the NTP server's IP address or host name.

Note: Note that if using a host name for the NTP server, a DNS server must be configured under TCP/IP settings. See **Network > Advanced TCP/IP Settings** below.

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

Date & Time Format Used in Images - specify the formats for the date and time (12h or 24h) displayed in the Live View 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 file formats.

Network - Basic TCP/IP Settings

Your Axis Video Server supports 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 can be set automatically via DHCP, or a static IP address can be set manually.

If IPv6 is enabled, your video server will 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.

Notes:


- DHCP is a protocol for automatic IP address assignment on a network. IP address assignment via DHCP may lead to the situation where the IP address changes and you lose contact with the video server. Configure the options for notification of IP address change (under Services) to receive notification from the video server when the IP address changes.
- Alternatively, if your DHCP server can update a DNS server, you can access the AXIS 247S by host name which is always the same, regardless of the IP address.

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 2 minutes after the unit is started, or as soon as an IP address is set.
 - Pinging the unit will still be possible when this service is disabled.

AXIS Internet Dynamic DNS Service - If the Video Server has been registered with the Axis Internet Dynamic DNS service and the IP address for the product changes, the service is updated to reflect the change. Check the box to enable/disable automatic updates.

The domain name currently registered at the Axis Internet Dynamic DNS service for your product can at any time be removed. To do this click **Settings...** and follow the instructions. For more information, please refer to the online help 

Network - 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 Video Server. Multiple domains can be separated by semicolons (;). The host name is always the first part of a Fully Qualified Domain Name, e.g. 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.


NTP

Obtain NTP server address via DHCP - use a DHCP server to automatically find an NTP server to synchronize clock of the Video Server with the other devices on the network

Use the following NTP server address - use the host name or IP address of a specific NTP server for time synchronization.

Host Name Configuration

The Video Server 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 the online help 

Link-Local Address

This is enabled by default and assigns the Video Server an additional IP address for use with UPnP™. The Video Server 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

The default HTTP port number (80) can be changed to any port within the range 1024-65535. This is useful for e.g. simple port mapping.

HTTPS

The default HTTPS port number (443) can be changed to any port within the range 1024-65535. This is useful for e.g. simple port mapping.

NAT traversal

Use NAT traversal when your video server is located on an intranet and you want to make it available from the other side of a NAT router.

FTP

The FTP server running in the Video Server enables the upload of e.g. new firmware, user applications, etc. Check the box to enable the service.

RTSP


The RTSP protocol allows a connecting client to start an MPEG-4 stream. Enter the RTSP port number to use. The default setting is 554.

Network Traffic

The default setting is Auto-negotiate which means that the correct speed is automatically selected. If necessary, you can set the connection speed by selecting it from the drop-down list.

Maximum bandwidth - Specify, in Mbit/s or kbit/s, the maximum bandwidth that the Video Server is allowed to use on your network. This is a useful function when connecting your Video Server to busy or heavily loaded networks. The default setting is **Unlimited**.

Note: When using MPEG-4 as the video format, remember that setting a maximum bandwidth value here may create problems for individual video streams if the maximum value is less than the sum of the bit rates set for the video streams.

For more information, please see the online help 

SOCKS

SOCKS is a networking proxy protocol. The Video Server 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 Video Server is located on a local network behind a firewall, but notifications, uploads, alarms, etc., need to be sent to a destination outside the local network (e.g. to the Internet).

QoS (Quality of service)

Quality of Service (QoS) provides the means to guarantee a certain level of a specified resource to selected traffic on a network. Quality can be defined as e.g. a maintained level of bandwidth, low latency, no packet losses, etc. 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 e.g. reserve a fixed amount of bandwidth for these types of traffic. The following types of traffic are marked:

- live video
- live audio
- event/alarm traffic
- 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 which 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 addresses for your primary and secondary mail servers in the fields provided, to enable event and error email messages from the Video Server to predefined addresses, via SMTP.

If the mail server requires SMTP authentication, check the box for **Use authentication to log in to this server** and enter the user name and password used for logging in. Several different methods of authentication are available. See the online help for more information.

SNMP

The Simple Network Management Protocol (SNMP) allows the remote management of network devices. Select the version of SNMP to use, depending on the level of security required. Select the version of SNMP to use, by checking the appropriate box. The three levels of security are:

- SNMP V1 - includes no security
- SNMP V2c - uses very simple security, e.g. community name as password
- SNMP V3 - provides encryption and secure passwords. Use with HTTPS.

If using V1 and V2c, enter the community name for read-only access to all supported SNMP objects (except the root password and other objects that require write access). Default value = public. You can also specify the community name for read/write access to all supported SNMP objects (except read-only objects).

Default value = pass.

If using HTTPS enter the password if it has not already been set. To set the password again, the Video Server must be reset to the factory default settings.

UPnP™

The Video Server includes support for UPnP™ in Windows ME and Windows XP. UPnP™ is enabled by default.

Note: UPnP™ must be installed on your workstation if running Windows XP. To do this, open the Control Panel from the **Start Menu** and select **Add/Remove Programs**. Select **Add/Remove Windows Components** and open the **Networking Services** section. Click **Details** and then select **UPnP™** as the service to add.

RTP (Multicast)/MPEG-4

These settings are the IP address, port number, and Time-To-Live value to use for the media stream(s) in multicast MPEG-4 format. Only certain IP addresses and port numbers should be used for multicast streams. For more information, please see the online help. [?](#)

Bonjour

When Bonjour is enabled, the video server is automatically detected by operating systems and clients that support this protocol.

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 31.

Maintenance

- **Restart** - The unit is restarted without changing any of the settings. Use this method if the unit is not behaving as expected.
- **Restore** - The unit is restarted and most current settings are reset to factory default values. The settings that will not be reset are as follows:
 - the boot protocol (DHCP or static)
 - the static IP address
 - the default router
 - the subnet mask
 - the system time
- **Default** - The default button should be used with caution. Pressing this will return all of the Video Server's settings to the factory default values (including the IP address)

Upgrade Server - See *Upgrading the Firmware*, on page 33.

Backup - To take a backup of all of the parameters, and any user-defined scripts, click this button. If necessary, it is then possible to return to a previous configuration if settings are changed and there is unexpected behavior.

Restore - click the **Browse** button to locate the saved backup file (see above) and then click the **Restore** button. The settings will be restored to the previous configuration.

Note: Backup and Restore can only be used on the same unit running the same firmware. This feature is not intended for multi-configurations or for firmware upgrades.

Support

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

The **System Overview** gives a quick look over the status of the video server.

Logs & Reports - when contacting Axis support, please be sure to provide a valid Server Report with your query.

Information - The **Log report** and the **Parameter List** also provide valuable information for troubleshooting and when contacting Axis' support service.

Configuration:

Log Level for Log Files - from the drop-down list, select the level of information to be added to the Log file

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

Advanced

Scripting is an advanced function that provides the possibility 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 fully understand the consequences. Note that Axis support does not provide assistance for problems with customized scripts.

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

Plain Config - this function is for the advanced user with experience of Axis Video Server configuration. All parameters can be set and modified from this page, including the audio encoding format. Help is available from the standard help pages.

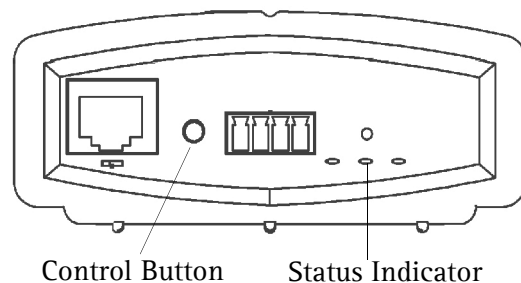
Resetting to the Factory Default Settings

To reset the Video Server to the original default settings, go to the **System Options > Maintenance** web page (described in *Maintenance*, on page 28) or use the control button on the Video Server, as described below:

Using the Control Button

Follow the instructions below to reset the Video Server to the factory default settings using the Control Button.

1. Switch off the Video Server by disconnecting power.
2. Press and hold the Control Button while reconnecting the power.
3. Keep the Control button pressed until the **Status Indicator** displays yellow (this may take up to 15 seconds).
4. Release the Control Button.
5. When the Status Indicator changes to Green (may take up to 1 minute), the process is complete and the Video Server has been reset.
6. Re-install the Video Server, as described in the Installation Guide.



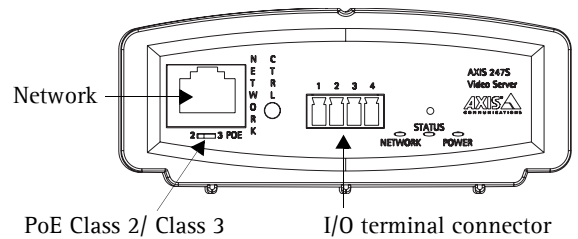
Unit Connectors

Network connector - RJ-45 Ethernet connector. Supports Power over Ethernet (PoE). Shielded cables recommended.

PoE switch - Power over Ethernet (IEEE 802.3af), selectable power classification:

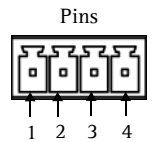
- Class 2 (max 7W)
- Class 3 (max 13W)

Note: If the connected analog camera is not powered by the video server, select PoE class 2 to optimize the load on the PoE switch. PoE class 3 is the default setting.



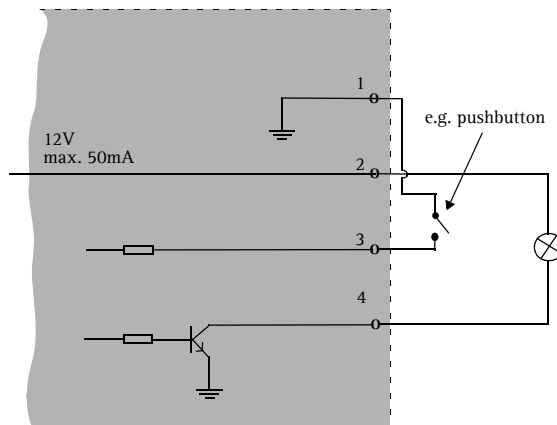
I/O terminal connector - Used in applications for e.g. motion detection, event triggering, time lapse recording and alarm notifications:

- 1 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 Event Configuration > Port Status) if the alarm device is activated.
- 1 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 Event Configuration > Port Status).



| Function | Pin | I/O Terminal Connector Pin Description | Specifications |
|-------------------|-----|--|---|
| GND | 1 | | |
| Power | 2 | Can be used to power auxiliary equipment. | 12V DC, Max load = 50mA |
| Digital Input | 3 | Connect to GND to activate, or leave floating (or unconnected) to deactivate. | Must not be exposed to voltages greater than 10V DC |
| Transistor Output | 4 | Uses an open-collector NPN transistor with the emitter connected to the GND pin. If used with an external relay, a diode must be connected in parallel with the load, for protection against voltage transients. | Max load = 50mA Max voltage = 24V DC (to the transistor) |

Connection diagram



BNC connector - Connect a 75 ohm coaxial video cable (max. length 800 feet (250 meters)).

Note: If the video source is to be connected in parallel with other equipment using a BNC T adaptor, disable the input termination by setting the 75 ohm switch to OFF. Failure to do so may cause reduced image quality.

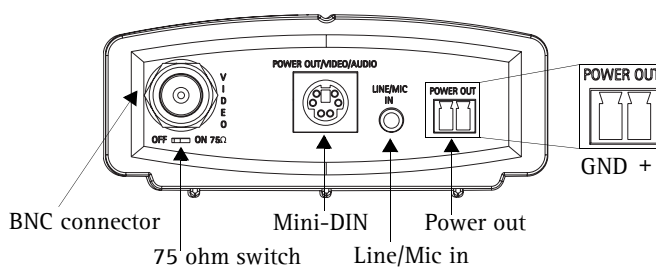
Mini-DIN - 6 pin Mini-DIN connector for power out, video in and audio in:

| Function | Pin | Mini-DIN Pin Description | Mini-DIN Connector |
|-----------|-------|---|--------------------|
| Power out | 1 | 12V DC, max. load 5W (420mA) | |
| Audio in | 3 | Mono microphone or a line-in | |
| Video in | 5 | Video connection (Not S-video or Y/C video) | |
| GND | 2,4,6 | Ground on pins 2, 4 and 6. | |

Important!

- There are two alternative connections available for power out, video in and audio in, providing flexible installation. Do not connect more than one video/audio source as the AXIS 247S is a one-channel video server and can only accommodate one video/audio stream.
- The AXIS 247S can deliver a maximum of 5W (420mA) to a camera (from power out or Mini-DIN connector) and 50mA from the I/O terminal connector.

Line/Mic in - 3.5mm input for a mono microphone, or a line-in mono signal (left channel stereo signal).



Power out - Used to power a camera or other auxiliary equipment 12V DC, max. load 5W (420mA)

Note: It is also possible to connect power to the AXIS 247S using an AXIS PS-K power adaptor connected to the Power out terminal connector. **DO NOT** connect the PS-K power supply if the AXIS 247S is connected to a PoE switch.

Troubleshooting

Checking the Firmware

Firmware is software that determines the functionality of the Video Server. One of your first actions when troubleshooting a problem should be to check the currently installed version. The latest version may contain a correction that fixes your particular problem. The current firmware version in your Video Server can be seen under Setup > Basic Configuration.

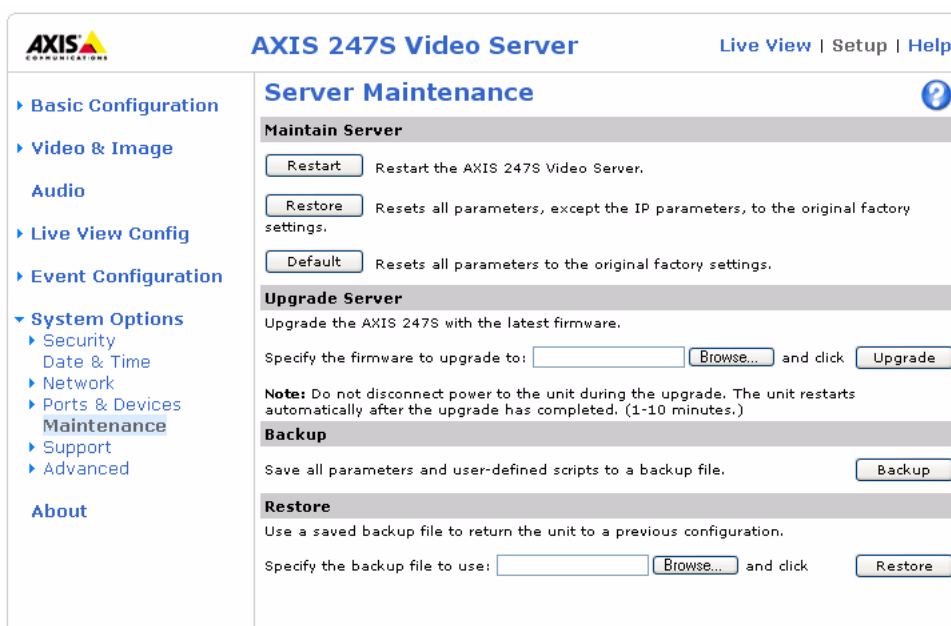
Upgrading the Firmware

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

New firmware can be downloaded to the Video Server over the network.

Note: Pre-configured and customized settings will be retained for use when the new firmware is running (provided the features are available in the new firmware) although this is not guaranteed by Axis Communications.

1. Save the firmware file to your computer. The latest version of the Video Server firmware is available free of charge from the Axis Web site at www.axis.com/techsup or from your local distributor.
2. Go to Setup > System Options > Maintenance in the Video Server's Web pages.
3. In the Upgrade Server section and browse to the desired firmware file on your computer. Click Upgrade.



- Notes:**
- Always read the upgrade instructions available with each new release, before updating the firmware.
 - After starting the process, you should always wait at least 20 minutes before restarting the Video Server, even if you suspect the procedure has failed.
 - Your dealer reserves the right to charge for any repair attributable to faulty updating by the user.

Emergency Recovery Procedure

If power or the network connection to the Video Server is lost during the upgrade, the process will fail and the unit will become 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 underside label on the product casing.

1. **Unix/Linux** - From the command line, type the following:

```
arp -s <IP address of Video Server> <Serial number> temp
ping -s 408 <IP address of Video Server>
```

Windows - From a command/DOS prompt, type the following:

```
arp -s <IP address of Video Server> <Serial number>
ping -l 408 -t <IP address of Video Server>
```

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 Video Server's IP address. In the page that appears, use the **Browse** button to select the upgrade file to use, e.g. axis247s.bin. Then click the **Load** button to restart the upgrade process.
4. After the upgrade has completed (1-10 minutes), the unit will automatically restart and show a steady green on the Power and Status LEDs and flashing green or amber on the Network LED.
5. Reinstall the Video Server.

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

Support

If you contact Axis support, please help us help you resolve your problems expediently by providing a server report, log file and a brief description of the problem.

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

Log file - go to **Setup > System Options > Logs & Reports**. The Log file records events within the unit since the last restart of the system and can prove a useful diagnostic tool for troubleshooting.

Symptoms, Possible Causes and Remedial Actions

Problems setting the IP address

| | |
|---|---|
| Using ARP/Ping – the IP address must be set within two minutes after power has been applied to the Video Server | Restart the server and try again. Ensure also the ping length is set to 408. (See AXIS 247S Video Server Installation Guide) |
| The Video Server is located on a different subnet. | If the IP address intended for the Video Server 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 for an IP address on the same subnet as the computer you are performing the installation from. |
| The IP address is being used by another device | Disconnect power from the Video Server. Run the Ping command (in a Command/DOS window, type <code>ping <IP address of unit></code>) 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 receive: Request timed out - this means that the IP address is available for use with your Video Server. In this case, check all cabling and reinstall the unit. |

The Video Server cannot be accessed from a Web browser

| | |
|---|--|
| Cannot log in | If the Video Server has been configured to use HTTPS, check that the protocol in the URL used to access the unit is correct. You may need to type this in manually (i.e. http or https) in the browser's address field. |
| The IP address has been changed by DHCP | 1) Move the Video Server to an isolated network or to one with no DHCP or BOOTP server. Set the IP address again, using the ARP Ping command. 2) Access the unit and disable BOOTP and 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 will now have 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. |

Cannot send notifications, uploads, alarms, etc, to a destination outside the local network

| | |
|---------------------|---|
| Firewall protection | The Video Server can be configured to use a SOCKS server to reach networks on the other side of a firewall/proxy server |
|---------------------|---|

Your Video Server is accessible locally, but not externally

| | |
|---|--|
| Firewall protection | Check the Internet firewall with your system administrator. |
| Default routers required | Check if you need to configure the default router settings. |
| The Internet site is too heavily loaded | Use a script on your web server to relay images from the Video Server to the Internet. |

The Power indicator is not constantly lit

| | |
|---------------------|--|
| Problem with PoE | Check the PoE switch |
| Faulty power supply | Verify that you are using an AXIS PS-K power supply. |

The Status indicator is flashing red and the server is inaccessible

| | |
|---|--|
| A firmware upgrade has been interrupted or the firmware has been damaged in some other way. | A rescue firmware is running in the product. First, set the IP address using AXIS IP utility or ARP and Ping, See AXIS 247S Video Server Installation Guide. Then, using a browser, access the unit and download the latest firmware to the product, see <i>Upgrading the Firmware</i> , on page 33. |
|---|--|

No images displayed in the Web interface

| | |
|---|--|
| Problem with AMC (<i>Internet Explorer only</i>) | To enable the updating of images in Microsoft Internet Explorer, set your Web 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 Video Server to use a Java applet for updating the images under Live View Config > Layout > Default Viewer for Internet Explorer. See the online help for more information. |

Video Image Problems

| | |
|--------------------------------------|---|
| Image too dark or too light. | Check that the termination dip switch for the video source is set to the correct position. See also the online help on Video Source Settings |
| Black borders around the video image | Adjust the X and/or Y offset, in the Video Source Settings. See the online help for information. |
| Problems uploading own files | There is only limited space available for the upload of your own files. Try deleting one or more existing files, to free up space |
| 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 e.g. pre-buffers, motion detection, high resolution images, high frame rates, etc., will reduce the performance of the Video Server. |
| Slow performance | Slow performance may be caused by e.g. heavy network traffic, multiple users accessing the unit, low performance clients, use of features such as Motion Detection, Event handling. |

| | |
|--|---|
| Bad snapshot images | |
| Display incorrectly configured on your workstation | In Display Properties, configure your display to show at least 65000 colors, i.e. at least 16-bit. Using only 16 or 256 colors on your display will produce dithering artifacts in the image. |
| Incorrect exposure in images | |
| Incorrect line termination | If the Video Server is to be connected in loop through with other equipment, disable the input termination by turning the corresponding DIP switch to OFF. |
| Problems with the MPEG-4 format | |
| Lower frame rate than expected. | Check with the administrator that there is enough bandwidth available. Check also the settings for bit rate control, in the Video & Image > Advanced > MPEG-4 settings. Using an inappropriate video object type can also affect the frame rate. See the online help for more information. Check in the AMC control panel applet (MPEG-4 tab) that video processing is not set to Decode only I frames . Lower the image resolution. Reduce the number of applications running on the client computer. |
| No MPEG-4 displayed in the client. | Check that the correct network interface is selected in the AMC control panel applet (network tab). Check that the relevant MPEG-4 connection methods are enabled in the AMC control panel applet (network tab). In the AMC control applet, select the MPEG-4 tab and click the button Set to default MPEG-4 decoder. |
| No multicast MPEG-4 displayed in the client. | Check with your network administrator that the multicast addresses used by the Video Server are valid for your network. Check with your network administrator to see if there is a firewall preventing viewing. |
| Multicast MPEG-4 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 MPEG-4 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. This is done on the MPEG-4 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 MPEG-4 and Motion JPEG. | Modify the settings for your graphics adapter. Please see the adapter's documentation for more information. |
| No audio | |
| Incorrect setup. | Check that the sound card in the PC and the connections to the speaker and microphone are working. Ensure that the mute button is not pressed and the volume settings are correct. |
| Post Content Length in proxy server. | The Post Content Length set in the proxy server is too low. Set the value of the Post Content Length in your proxy server to 1MB or more. You may need to contact your system administrator to do this. |
| Firewall or router settings. | AXIS 247S works locally, but not externally. Check the Internet firewall settings with your system administrator or reconfigure the default router settings. |
| DC power not enabled for microphone. | If the microphone has a built-in amplifier then the DC power must be enabled on the Audio Settings page. |
| Audio volume too low/high | |
| Volume settings incorrect. | The volume of the microphone connected to the AXIS 247S is either too high or too low. Change the volume for the microphone in the Live View page. |
| Input and output gain set incorrectly. | Change the input gain for the microphone to adjust the audio levels on the Audio Settings page. |
| Poor audio quality | |
| Too many users. | Too many users/clients listening to audio from the AXIS 247S may adversely affect the sound quality. |
| CPU overloaded. | Reduce the number of listeners and viewers and decrease the image resolution and compression. |

For additional assistance, please contact your reseller or check the product's support pages on the Axis Website at www.axis.com/techsup

Technical Specifications

| Item | Specification |
|----------------------------|---|
| Models | <ul style="list-style-type: none"> • AXIS 247S |
| Video compression | <ul style="list-style-type: none"> • Motion JPEG • MPEG-4 Part 2 (ISO/IEC 14496-2) with motion estimation • Profiles: Advanced Simple Profile and Simple Profile |
| Resolutions | <ul style="list-style-type: none"> • 4CIF, VGA, 2CIF, CIF, QVGA, QCIF • max 704x480 (NTSC) 704x576 (PAL) • min 160x120 (NTSC) 176x144 (PAL) |
| Frame rate (NTSC/PAL) | <ul style="list-style-type: none"> • Motion JPEG: Up to 30/25 fps at 4CIF • MPEG-4: Up to 30/25 fps at VGA, 27/23 fps at 4CIF |
| Video streaming | <ul style="list-style-type: none"> • Simultaneous Motion JPEG and MPEG-4 • Controllable frame rate and bandwidth • Constant and variable bit rate (MPEG-4) |
| Image settings | <ul style="list-style-type: none"> • Compression levels: 11 (Motion JPEG) /23 (MPEG-4) • Rotation: none • Aspect ratio correction • Color: color, black & white • Overlay capabilities: time, date, text or image or privacy mask • De-interlace filter |
| Audio | <p>One-way audio</p> <ul style="list-style-type: none"> • AAC LC 8-32 kbit/s, • G.711 PCM 64kbit/s, • G.726 ADPCM 32 or 24 kbit/s <p>Simplex or audio off</p> |
| Security | <ul style="list-style-type: none"> • Multiple user access levels with password protection • IP address filtering • HTTPS encryption • IEEE 802.1X authentication |
| Users | <ul style="list-style-type: none"> • 20 simultaneous viewers |
| Alarm and event management | <ul style="list-style-type: none"> • Events triggered by video motion detection, external inputs, audio detection, video loss, or according to a schedule • Image upload over FTP, email, HTTP • Notification over TCP, email, HTTP, external outputs • Pre- and post alarm buffer of 9 MB (approx. 4 min of CIF resolution video at 4 frames per second) |
| Connectors | <ul style="list-style-type: none"> • Analog composite video BNC input, NTSC/PAL autosensing • Ethernet 10BaseT/100BaseTX, RJ-45 • IO/ terminal block: <ul style="list-style-type: none"> • 1 alarm input • 1 alarm output • Power Out terminal block: <ul style="list-style-type: none"> • Power feed to the camera - or - • alternative power supply for the video server • 3.5 mm jack for Mic in (max 80 mVpp) -or- <ul style="list-style-type: none"> • Line in (max 6.4 Vpp, mono) • 6 pin Mini-DIN alternative connection for: <ul style="list-style-type: none"> • Video in • Audio in • Power out |
| Processors and memory | <ul style="list-style-type: none"> • CPU, Video processing and compression: ARTPEC-A chip • RAM: 32MB • Flash memory: 8 MB • Battery backed up real-time clock |
| Power | <ul style="list-style-type: none"> • Power over Ethernet (IEEE 802.3af) with (dip-switch) selectable power classification: <ul style="list-style-type: none"> • Class 2: max 1.4 W for powering the camera • Class 3: max 5.0 W for powering the camera (AXIS 247S uses max 5.0 W) • Alternative power connection over terminal block: 7 - 15 V |
| Operating conditions | <ul style="list-style-type: none"> • 0 - 50 °C (41 - 122 °F) • Humidity 20 - 80% RH (non-condensing) |

| Item | Specification |
|--|---|
| Minimum web browsing requirements | <ul style="list-style-type: none"> • Pentium III CPU 500 MHz or higher, or equivalent AMD, 128 MB RAM, AGP graphics card 32 MB RAM, Direct Draw • Windows XP, 2000, DirectX 9.0 or later • Internet Explorer 6.x or later For other operating systems and browsers, see www.axis.com/techsup |
| System integration support | <ul style="list-style-type: none"> • Open API for application integration, including AXIS VAPIX API*, AXIS Media Control SDK* • Quality of Service (QoS) Layer 3, DiffServ Model • Embedded Linux operating system * Available at www.axis.com |
| Supported protocols | IPv4/v6, HTTP, HTTPS, SSL/TLS*, TCP, ICMP, QoS, SNMPv1/v2cv/v3 (MIB-II), RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP, Bonjour, ARP, DNS, DynDNS, SOCKS, NTP, etc. More information on protocol usage available at www.axis.com *This product includes software developed by the Open SSL Project for use in the Open SSL Toolkit. |
| Approvals - EMC | <ul style="list-style-type: none"> • EN 55022 Class B • EN 55024 • EN 61000-3-2 • EN 61000-3-3 • FCC Part 15 Subpart B Class B • VCCI Class B • C-tick AS/NZS CISPR22:2002 • ICES-003 Class B |
| Approvals - Safety | <ul style="list-style-type: none"> • Safety: EN60950-1 |
| Dimensions | <ul style="list-style-type: none"> • HxWxD = 41 x 98 x 99 mm (1.6" x 3.8" x 3.9") • Weight: 214g (0.47 lb) |
| Complimentary Software | <ul style="list-style-type: none"> • AXIS Media Control (AMC) - ActiveX component software required for Microsoft Internet Explorer, installed automatically on first use. • Optional: AXIS IP Utility - Windows installation |
| MPEG-4 licensing | License for one MPEG-4 encoder and one MPEG-4 decoder included. Additional licenses available from Axis dealers. |
| Video management software (not included) | AXIS Camera Station - Surveillance application for viewing, recording and archiving video from up to 25 cameras. |
| Accessories (not included) | Camera cable, 10m, from 6 pin mini-DIN connector to RCA (video in, RCA to BNC adapter also included), RCA (audio in), Mini DC jack (power out). MPEG-4 Decoder multi-user license pack. |

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 will affect both. If the load on the CPU reaches its maximum, this will also affect the frame rate.

The following factors are among the most important to consider:

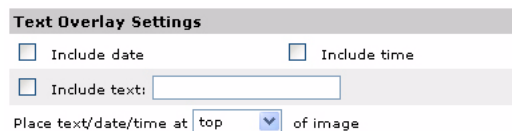
- High image resolutions and/or lower compression levels result in larger images. Bandwidth affected.
- Access by large numbers of Motion JPEG and/or unicast MPEG-4 clients. Bandwidth affected.
- Simultaneous viewing of different streams (resolution, compression, etc.) by different clients. Frame rate and bandwidth affected.
- Accessing both Motion JPEG and MPEG-4 video streams simultaneously. Frame rate and bandwidth affected.
- Heavy usage of event settings affects the 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 lowers perceived performance. Frame rate affected.
- Access by large number of audio clients using full-duplex mode. Bandwidth affected.

Optimizing your system

To see the bandwidth and frame rate currently required by the video stream, the Video Server provides a tool that can be used to display these values directly in the video image.

To do this, special format strings are added as part of a text overlay. Simply add **#r** (average frame rate in fps) and/or **#b** (average bandwidth in Kbps) to the overlay.

For detailed instructions, please see the online help for **Video & Image > Text Overlay Settings**, and the help for **File Naming & Date/Time Formats**.



Important!

- The figures displayed here are the values as delivered by the server. If other restrictions are currently in force, (e.g. bandwidth limitation) these values might not correspond to those actually received by the client.
- For Motion JPEG, these values will only be accurate as long as no frame rate limit has been specified.

Frame rates - Motion JPEG

The following test results show the frame rates in frames/second (fps) for Motion JPEG streams from the Video Server, using a compression level of 50%. Note that these values are guidelines only - actual values may vary.

| Resolution | fps (NTSC/PAL) |
|------------|----------------|
| 4CIF | 30/25 |
| 2CIF | 30/25 |
| CIF | 30/25 |
| QVGA | 30/25 |
| QCIF | 30/25 |

Frame rates - MPEG-4

The following test results show the frame rates in frames/second (fps) for MPEG-4 streams from the Video Server. Note that these values are guidelines only - actual values may vary.

The MPEG-4 test conditions:

- Compression level = 50%
- Video Object Type = Advanced Simple
- GOV structure = IP*

| Resolution | fps (NTSC/PAL) |
|------------|----------------|
| 4CIF | 27/23 |
| VGA | 30/25 |
| 2CIF | 30/25 |
| CIF | 30/25 |
| QVGA | 30/25 |
| QCIF | 30/25 |

*Note that setting the GOV structure to use "I-frames only" will increase the frame rate.

Bandwidth

As there are many factors affecting bandwidth, it is very difficult to predict the required amounts. The settings that affect bandwidth are:

- the image resolution
- the image compression
- the frame rate
- the MPEG-4 object type
- the MPEG-4 GOV structure
- the analog cameras connected to the Video Server
- the audio settings

There are also factors in the monitored scene that will affect the bandwidth. These are:

- the amount of motion
- the image's complexity
- the lighting conditions.

For MPEG-4, if there is only limited bandwidth available, and if this is more important than the image quality, using a constant bit rate (CBR) is recommended. Use a variable bit rate (VBR) if the image quality needs to be maintained at a higher level. If supported on the network, consider also using MPEG-4 multicasting, as the bandwidth consumption will be much lower.

Glossary

- Active Speaker** - a speaker with a built-in power amplifier.
- ActiveX** - A control (or set of rules) used by a browser. ActiveX controls are often downloaded and installed automatically as required.
- AMC** - AXIS Media Control. The control required for viewing video images in Internet Explorer. Installs automatically on first use.
- API** - Application Programming Interface. The Axis API can be used for integrating Axis products into other applications.
- ARP** - Address Resolution Protocol. Used to associate an IP address to a hardware MAC address. A request is broadcast on the local network to find out what the MAC address is for the IP address.
- ARTPEC** - Axis Real Time Picture Encoder - used for image compression.
- 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.
- BOOTP** - A protocol that can automatically configure a network device (give it an IP address).
- Bonjour** - Also known as zero-configuration networking, Bonjour enables automatic discovery of computers, devices, and services on IP networks. Bonjour allows devices to automatically discover each other without the need to enter IP addresses or configure DNS servers. Bonjour is developed by Apple Computer Inc.
- CGI** - Common Gateway Interface. A set of rules (or a program) that allows a Web Server to communicate with other programs.
- Client/Server** - Describes the network relationship between two computer programs, in which one, the client, makes a service request from another - the server.
- DC-Iris** - This special type of iris is electrically controlled by the Axis camera, to automatically regulate the amount of light allowed to enter.
- dB (Decibels)** - A unit to measure sound level changes. A 3dB change is the smallest level change we can hear. A 3dB change is actually twice or half the audio power level. A gain of 0dB will leave the signal level unchanged.
- De-interlacing** - De-interlacing is the process taking a stream of interlaced frames and converting it to a stream of progressive frames.
- DSL** - Digital Subscriber Line. A means of transferring data via standard phone lines.
- Ethernet** - A widely used networking standard.
- ETRAX** - Axis' own microprocessor.
- Firewall** - A virtual barrier between a LAN (Local Area Network) and other networks, e.g. the Internet.
- FTP** - File Transfer Protocol. Used for the simple transfer of files to and from an FTP-server.
- Full-duplex** - Transmission of data, e.g. audio, in two directions simultaneously.
- G.711** - G.711 is the international standard for encoding telephone audio on 64 kbps channel. It is a pulse code modulation (PCM) scheme operating at 8 kHz sample rate.
- G.726** - Frequently used speech-compression algorithm in telecommunications due to its high perceived speech quality and low resource requirements.
- Half-duplex** - A half-duplex link communicates in one direction at a time only, much like a walkie-talkie. Two way communication is possible, but not simultaneously.
- HTTP** - Hypertext Transfer Protocol. The set of rules for exchanging files (text, images, sound, video, and other files) on the World Wide Web.
- HTTP-S (HTTPS)** - An extension to the HTTP protocol to support sending data securely over the World Wide Web.
- Intranet** - A private network limited to an organization or corporation. Usually closed to external traffic.
- IP** - Internet Protocol. See TCP/IP.
- IP address** - A unique number used by a computer on the network to allow it to be identified and found.
- ISMA** - Internet Streaming Media Alliance.
- JPEG** - A standard image format, used widely for photographs. Also known as JPG.
- LAN** - A local area network (LAN) is a group of computers and associated devices that typically share common resources within a limited geographical area.
- Linux** - A popular operating system that is "open source" and practically free of charge.
- Lux** - A standard unit for light measurement.
- Mbit/s** - Megabits per second. A unit for measuring speeds in networks. A LAN might run at 10 or 100 Mbit/s.
- MPEG-4** - A video compression standard that makes good use of bandwidth, and which can provide DVD-quality video streams at less than 1 Mbit/s.
- Multicast** - A bandwidth-conserving technology that reduces bandwidth usage by simultaneously delivering a single stream of information to multiple network recipients.
- PEM** - Privacy Enhanced Mail. An early standard for securing electronic mail. The PEM-format is often used for representing an HTTPS certificate or certificate request.
- Ping** - A small utility used for sending data packets to network resources to check that they are working and that the network is intact.
- Pre/post alarm image** - The images from immediately before and after an alarm.
- 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.
- (QoS) Quality of Service** - QoS provides the means to guarantee a certain level of a specified resource to selected traffic on a network. Quality can be defined as e.g. a maintained level of bandwidth, low latency, no packet losses, etc.
- 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 is often included as part of a network switch (see below).
- RTP** - Real-Time Transfer Protocol. A transfer protocol designed for the delivery of live content, e.g. MPEG-4.
- 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.
- Simplex** - In simplex operation, a network cable or communications channel can only send information in one direction; it's a "one-way street".
- SMTP** - Simple Mail Transfer Protocol is the protocol used to send e-mail across the Internet. SMTP authentication is a way of allowing people outside of a domain to use an SMTP server when sending e-mail.
- SNMP** - Simple Network Management Protocol. An application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite.
- Subnet Mask** - An IP address consists of two components: the network address and the host address. "Subnetting" enables a network administrator to further divide the host part of the address into two or more subnets. The subnet mask identifies the subnet to which an IP address belongs.

Switch - Whilst a simple hub transmits all data to all devices connected to it, a switch only transmits the data to the device it is specifically intended for.

TCP/IP - Transmission Control Protocol/Internet Protocol. A suite of network protocols that determine how data is transmitted. TCP/IP is used on many networks, including the Internet. TCP keeps track of the individual packets of information and IP contains the rules for how the packets are actually sent and received.

UDP - The User Datagram Protocol is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is also known as UDP/IP.

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

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

Web server - A program on a computer that delivers the resources (usually web pages) requested by the web user (the client).

Index

802.1X authentication 23

A

Action 18
 Action buttons 6, 17
 Active/Inactive 6, 17
 Administrators 11, 22
 Advanced TCP/IP settings 26
 Alarm 18, 21, 31
 Allowed IP addresses 22
 AMC 8
 Anonymous viewers 22
 ARP/Ping 25
 Audio transmission 9
 AXIS Internet Dynamic DNS Service 25

B

Backup 28
 Bandwidth 7, 40
 Basic TCP/IP settings 24
 Buffers 19

C

Constant bit rate 7
 Control button 4, 30
 Customize 16

D

Date & Time 24
 Default Viewer 17
 Default viewer 17
 DIP switch 4
 DNS configuration 26

E

Email server 27
 Emergency recovery 33
 Enable ARP/Ping 25
 Event servers 18
 Events 18
 External video 17
 External video sources 6

F

Factory default settings 30
 Frame rates 12, 39
 FTP server 18

H

Host name 26
 HTML examples 17
 HTTP port number 26

HTTP server 18
 HTTP-API 10
 HTTPS 22

I

I/O Ports 28
 I/O terminal connector 4
 Include Windows 21
 Input 31
 Internal video sources 6
 IP address filtering 22

L

Line out 4
 Line/Mic in 4
 Live view config 16
 Live View page 11
 Logs & Reports 29

M

Maximum bandwidth 27
 Motion Detection 21, 31
 Motion JPEG 7, 9
 MPEG-4 7, 9
 MPEG-4 clients 9
 MPEG-4 protocols 8
 MPEG-4 settings 28
 Multicasting 8

N

Network indicator 4
 Network settings 24
 Network traffic 26

O

Operators 22
 Output 31
 Output buttons 6, 17
 Overlays 12
 Own home page 16
 Own web files 16

P

Pinout - I/O connectors 31
 PoE 4
 Port Status 21
 Ports & Devices 28
 Post-trigger buffer 19
 Power over Ethernet 4
 Pre-trigger buffer 19
 Pulse 6, 17

R

Recovery 33

Referrals 22
 Restart 28
 Restore 28
 RTP 8, 28
 RTSP 8, 26

S

Scheduled event 18
 Security 22
 Sequence mode 6, 17
 Services 24
 SMTP settings 27
 Snapshot 6
 SOCKS server 27
 Specifications 37
 Streaming MPEG-4 8
 Support 29
 Synchronization 9
 System options 22

T

TCP server 18
 TCP/IP settings 24
 Triggered event 18
 Troubleshooting 33

U

UDP 8
 Unicasting 8
 Upgrade Server 28
 UPnP 28
 Users 22

V

Variable bit rate 7
 Video input 4
 Video source 6, 13
 Video streams 7, 9, 12