AXIS 211M

Network Camera

User's Manual

SES-1017
10,701,321

About this Document

This manual is intended for administrators and users of the AXIS 211M Network Camera, and is applicable for software release 4.49 and later. It includes instructions for using and managing the camera on your network. Previous experience of networking will be of use when using this product. Some knowledge of UNIX or Linux-based systems may also be beneficial, for 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.

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

Legal Considerations

Video 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.

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

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

Japan – This is a class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

Australia – This electronic device meets the requirements of the Radio communications (Electromagnetic Compatibility) Standard AS/NZS CISPR22:2002.

Equipment Modifications

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

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

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

Support

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

Safety Notice - Battery Replacement

The AXIS 211M uses a 3.0V CR2032 Lithium battery as the power supply for its internal real-time clock (RTC). Under normal conditions this battery will 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 the battery needs replacing.

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

RoHS

This product complies with both the European RoHS directive, 2002/95/EC, and the Chinese RoHS regulations, ACPEIP.

WEEE Directive

The European Union has enacted a Directive 2002/96/EC on Waste Electrical and Electronic Equipment (WEEE Directive). This directive is applicable in the European Union member states.

The WEEE marking on this product (see right) or its documentation indicates that the product must not be disposed of together with household waste. To prevent possible harm to human health and/or the environment, the product must be disposed of in an approved and environmentally safe recycling process. For further information on how to dispose of this product correctly, contact the product supplier, or the local authority responsible for waste disposal in your area.

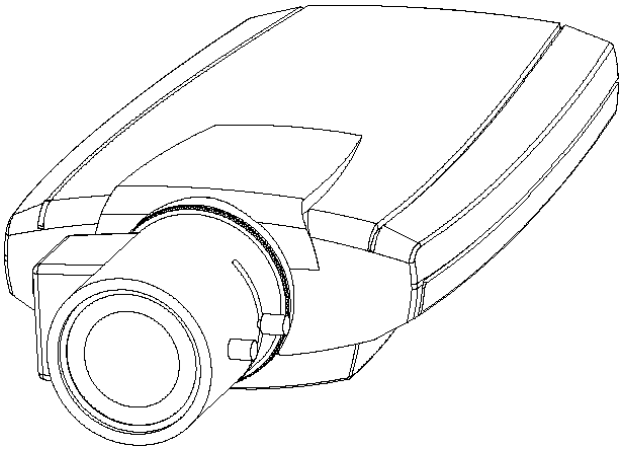
Business users should contact the product supplier for information on how to dispose of this product correctly. This product should not be mixed with other commercial waste.

AXIS 211M User's Manual Rev 2.1
February 2010 Part no. 38375
Copyright© Axis Communications AB, 2007 - 2010

Product Features 4
Key features 4
Overview 5
Using the Network Camera 7
Set the password 7
Accessing the AXIS 211M from the Internet 8
Video Stream 11
How to stream MPEG-4 11
MPEG-4 clients 12
Motion JPEG 12
Configuration 13
To configure the camera 13
AXIS Media Control 13
Video and Image settings 14
Image Appearance 14
Overlay/Mask Settings 15
Advanced - Camera Settings 15
Advanced - MPEG-4 Settings 16
Audio Settings 17
Enable Audio 17
Audio Channels - Audio mode 17
Audio Output 18
Live View Config 20
HTML Examples 23
External Video 23
Sequence Mode 23
Event Configuration 25
Event Servers 25
Configuring Event Types 25
Motion Detection 27
Port Status 28
System Options 29
Security 29
Date & Time 30
Network - Basic TCP/IP Settings 31
Network - Advanced TCP/IP Settings 31
SOCKS 33
QoS (Quality of Service) 33
SMTP (email) 34
SNMP 34
UPnP™ 34
RTP / MPEG-4 34
Bonjour 34
Ports & Devices 34
LED Settings 35
Maintenance 35
Support 35
Advanced 36
Resetting to the Factory Default Settings 36
I/O Terminal Connector 37
Connection diagram 38
Troubleshooting 39
Technical Specifications 43
Optimizing your system 45
Glossary of Terms 46

Product Features

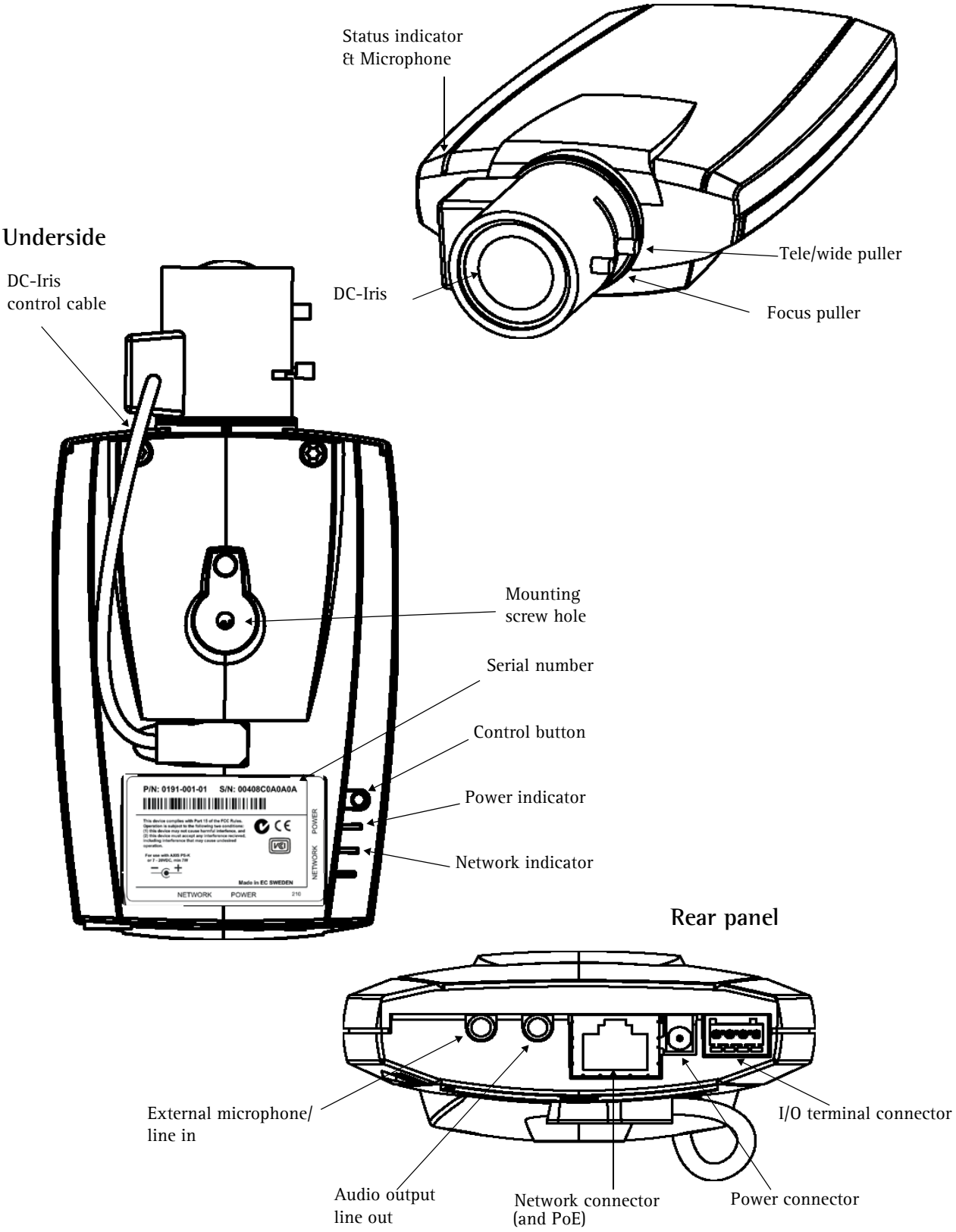
The AXIS 211M is a high performance megapixel network camera, designed for professional video surveillance. Owing to its high quality megapixel sensor, it delivers crisp and clear images, perfect for identification of objects and persons.



Key features

- Superior image quality, with maximum resolution 1280x1024.
- Video streams from the camera available on the network as real-time, full frame rate Motion JPEG and/or MPEG-4 video streams.
- Video Motion Detection - this can be used to trigger image uploads, for example, when there is activity in the video image.
- Scheduled image uploads.
- IP address filtering and multilevel password protection.
- Alarm input and output, which can be connected to various external devices such as door sensors and alarm bells.
- Multiple video resolutions.
- Simultaneous access by up to 20 viewers when using Motion JPEG. If MPEG-4 multicast is used, the number of viewers is unlimited, but each viewer still needs a separate MPEG-4 license. One license is included in the product, additional licenses can be purchased separately.
- Privacy masking allows the concealment of parts of the image that should not be viewable. Up to 3 areas can be configured as masked areas.
- Built-in web server that provides full access to all features via a standard web browser.
- Built-in scripting tool that allows the creation of basic applications. For advanced functionality, the cameras can be accessed via the AXIS HTTP API (more info at www.axis.com/developer).

Overview



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

Audio output/line out - Audio output (line level) can be connected to a public address (PA) system or an active speaker with a built-in amplifier. A stereo connector must be used for the audio out.

Power Connector - For connection of the PS-K power adapter (included).

I/O Terminal Connector - The I/O terminal connector provides the physical interface to one transistor output, one digital input and an auxiliary connection point for DC power. For more information, see *I/O Terminal Connector,* on page 37.

Network connector - The AXIS 211M connects to the network via a standard network cable, and automatically detects the speed of the local network segment (10BaseT/100BaseTX Ethernet). This socket can also be used to power the AXIS 211M via Power over Ethernet (PoE).

Serial Number - This number is used during installation.

Control Button - Press this button to install using the AXIS Internet Dynamic DNS Service as described in the AXIS 211M Installation Guide or to restore the factory default settings, as described on page 36.

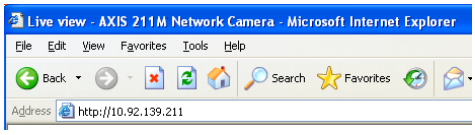
LED Indicators - After completion of the startup and self test routines, the multi-colored Network, Status, and Power LED indicators flash as follows:

LED	Color	Description
Network	Green	Steady for connection to 100 Mbit/s network. Flashes for network activity.
	Amber	Steady for connection to 10 Mbit/s network. Flashes for network activity.
	Unlit	No connection **Note:** The Network LED can be configured to be unlit during normal operation. See the online help files for more information. Go to **Setup > System Options > LED settings**.
Status	Green	Shows steady green for normal operation. **Note:** The Status LED can be configured to be unlit during normal operation, or to flash only when the camera is accessed. See the online help files for more information. Go to **Setup > System Options > LED settings**
	Amber	Steady during startup, 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.

Using the Network Camera

This document includes instructions for using and managing the AXIS 211M. For instructions on how to install the AXIS 211M on your network refer to the Installation Guide which is supplied with the product in the printed format or in PDF format from the Axis Web site at http://www.axis.com
The AXIS 211M can be used with most standard operating systems and browsers. The recommended browser is Microsoft Internet Explorer with Windows, Safari with Macintosh, and Firefox with other operating systems.

Accessing the AXIS 211M

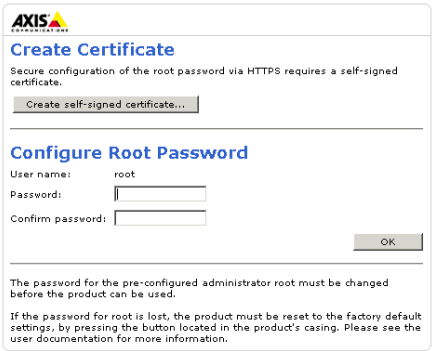


1. Start a Web browser.
2. Enter the IP address or host name of the camera in the browser's **Location/Address** field.
3. Enter the user name and password set by the administrator.
4. A video image is displayed in your Web browser.

Notes:
- To be able to view streaming video in Microsoft Internet Explorer, you must set your Web browser to allow ActiveX controls. If your working environment restricts the use of additional software components, you can configure the AXIS 211M to use a Java applet for updating images. Please refer to the online help files for more information.
- The layout of the **Live View** page may have been customized to specific requirements. Consequently, some of the examples and functions featured here may differ from those displayed on your own Live View page.

Set the password

When accessing the AXIS 211M for the first time, the '**Configure Root Password**' dialog appears.



1. Enter a password and then re-enter it, to confirm the spelling. Click **OK**.

Note: Before you enter your password at this point, you can secure configuration of the root password via HTTPS by creating a self-signed certificate. To do so, click the **Create self-signed certificate...** button in the **Create Certificate** window, and then proceed as follows.

2. Enter the user name **root** in the dialog as requested.
   Note: The default administrator user name **root** cannot be deleted.
3. Enter the password as set above, and click **OK**. If the password is lost, the AXIS 211M must be reset to the factory default settings. See page 36.
4. If required, click **Yes** to install AMC (AXIS Media Control), which allows viewing of the video stream in Internet Explorer. You will need administrator rights on the computer to do this.

Accessing the AXIS 211M from the Internet

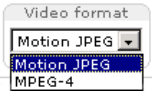
Once configured, your AXIS 211M is accessible on your local network (LAN). To access the camera from the Internet, network routers must be configured to allow incoming traffic, which is usually done on a specific port. To do this, enable the NAT-traversal feature, which will attempt to automatically configure the router to allow access to the camera. This is enabled from Setup > System Options > Network > TCP/IP Advanced.

For more information, see *NAT traversal (port mapping),* on page 32. See also the AXIS Internet Dynamic DNS Service at www.axiscam.net or, for Technical notes on this and other topics, visit the Axis Support Web at www.axis.com/techsup

The Live View Page

Depending on whether or not the Live View page has been customized, the buttons described below may or may not be visible.

View size buttons are available for Motion JPEG. Scale the image to an 800 pixel width and return the image to full scale.



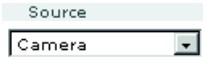
The Video Format drop-down list allows the video format on the Live View page to be temporarily changed.

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

Pulse - click this button to activate the output 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 and 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 external video source. Note that Sequence Mode must be stopped before selecting a source from this list.

The **Trigger buttons** can trigger an event directly from the **Live View** page. These are configured under **Setup > Live View Config > Layout**.

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

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

Play/Stop button - starts and stops the live video stream.

Snapshot button - saves a snapshot of the video image currently being displayed. The Snapshot function and the target directory for saving snapshots can be configured from the AMC Control Applet in the Windows Control Panel (Internet Explorer only).

View Full Screen button - makes the image fill the entire screen area. No other windows will be visible. Press **Esc** (Escape) on the keyboard to exit full screen.

Click the **Record** button to start an MPEG-4 recording (only available when viewing MPEG-4).

AMC audio controls

There are audio controls for controlling the client computer's speaker output. These controls are only available when audio is enabled, see *AXIS Media Control (AMC)*, on page 12 and *Audio Settings*, on page 17.

Click the **Speaker** and **Microphone** buttons to switch the sound off and on for the speaker and microphone, respectively.

Use the sliders to control the volume on the speaker and microphone. The volume can be set between 0 and 100.

When using **Half-duplex** mode, this button toggles between allowing you to speak and listen. The first icon indicates that you can talk and the speaker attached to the camera will play your voice. The second indicates that you will hear audio from the camera, but no audio will be sent to any web clients.

When in **Simplex** talk mode, the icon toggles between allowing you to speak and is dimmed when you do not want other clients to receive any audio.

Video Stream

The AXIS 211M provides several different image and video stream formats. The type you want to use depends on your requirements and on the properties of your network.

The **Live View** page in the AXIS 211M provides access to MPEG-4 and Motion JPEG video streams, as well as single JPEG images. Other applications and clients can also access these video streams/images directly, without going via the **Live View** page.

How to stream MPEG-4

This video compression standard makes good use of bandwidth, and can provide DVD-quality video streams at less than 1 Mbit/s. Note that the image settings of the MPEG-4 stream are the same for all clients.

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

Unicast RTP	This method (RTP over UDP) 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 are dropped.	Unicasting is used for video-on-demand broadcasting, so that there is no video traffic on the network until a client connects and requests the stream. Note: There is a maximum of 20 simultaneous viewers.
RTP over RTSP	This unicast method (RTP tunnelled over RTSP) is useful as it is relatively simple to configure firewalls to allow RTSP traffic.	
RTP over RTSP over HTTP	This unicast method can be used to traverse firewalls. Firewalls are commonly configured to allow the HTTP protocol, thus allowing RTP to be tunnelled.	
Multicast RTP	This method (RTP over UDP) 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 are dropped.	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.

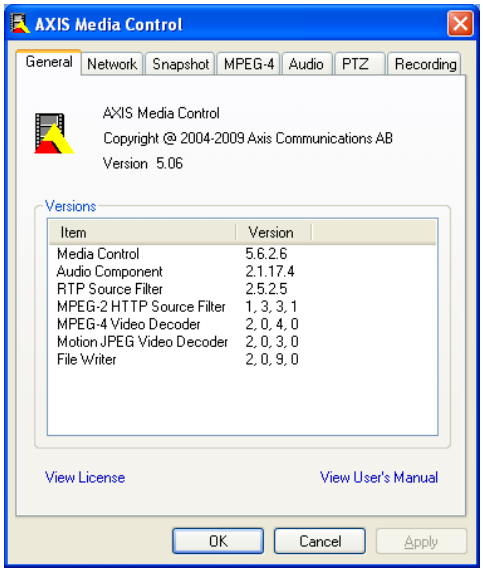
AMC will negotiate with the camera to determine exactly which transport protocol to use in the order listed above. This order can be changed and the options disabled, to suit any specific requirements.

Important!

MPEG-4 is licensed technology. The AXIS 211M includes one viewing client license. Installing additional unlicensed copies of the viewing client is prohibited. To purchase additional licenses, contact your Axis reseller.

MPEG-4 clients

AXIS Media Control (AMC)



The recommended method of accessing live video (MPEG-4 and Motion JPEG) from the AXIS 211M is to use the AXIS Media Control (AMC) in Microsoft Internet Explorer in Windows.

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

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

- Windows Control Panel (from the Start menu)

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

For more information on the AMC settings, please refer to the AXIS Media Control User's Manual available from the Axis Web site at http://www.axis.com from the Network Video link.

QuickTime™ & Real Player™

To access the video stream from, e.g. **QuickTime™** or **Real Player™** the following paths can be used:

- rtsp://<ip>/mpeg4/media.amp
- rtsp://<ip>/mpeg4/media.3gp

Notes:
- The AXIS 211M supports QuickTime 6.5.1 (or later) and Real Player 10.5 (or later)
- QuickTime adds latency to the video and audio stream (up to 3 seconds)
- It may be possible to use other players to view the MPEG-4 stream using the paths above, although this is not guaranteed by Axis Communications AB

Motion JPEG

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

The Motion JPEG stream uses considerable amounts of bandwidth, but provides excellent image quality and access to each and every individual image contained in the stream. The recommended method of accessing Motion JPEG live video from the AXIS 211M is to use the AXIS Media Control (AMC) in Microsoft Internet Explorer in Windows. Note also that multiple clients accessing Motion JPEG streams can use different image settings.

Alternative methods of accessing the video stream

Video/images from the AXIS 211M can also be accessed in the following ways:

- Motion JPEG server push (if supported by the client, e.g. Firefox). This option maintains an open HTTP connection to the browser and sends data as and when required, for as long as required. See *HTML Examples*, on page 23.
- Still JPEG images in a browser. Enter, e.g. the path: http://<ip>/axis-cgi/jpg/image.cgi?resolution=320x240
- Windows Media Player. This requires AMC and the MPEG-4 viewing client 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, tunnelled via HTTP: axrtsphttp://<ip>/mpeg4/media.amp
- Multicast: axrtpm://<ip>/mpeg4/media.amp

Note: <ip> = IP address

Configuration

This section describes how to configure the camera, and is intended for product **Administrators** and **Operators**. For a description of user access rights, see *Security,* on page 29.

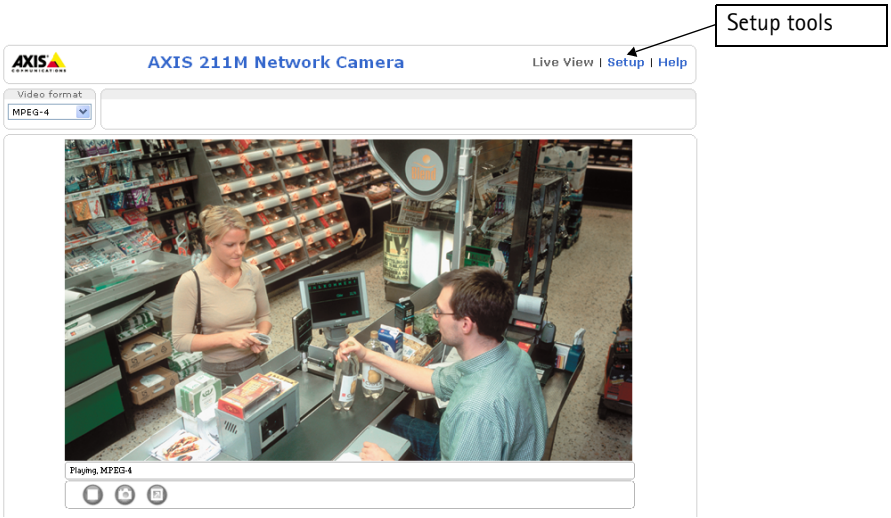
The camera is configured from the **Setup** link in your standard browser.

The descriptions below show examples of the features available in the AXIS 211M. For details of each setting, please refer to the online help available from the **Setup** link. Click ? to access the online help.

To configure the camera

Follow the instructions below to configure the camera from a browser.

1. Start your browser and enter the IP address or host name of the camera in the location/address field.
2. The **Live View** page appears. Click the **Setup** link on the top right of your web browser.



AXIS Media Control

The AXIS Media Control (AMC) is automatically installed the first time the camera is accessed from Microsoft Internet Explorer. The AMC control panel can be opened by right-clicking on the video image on the **Live View** page. The control panel can be used to configure various video and audio settings.

For more information, see the AMC User's Manual, available on the CD supplied with this product, or from www.axis.com/techsup

Video and Image settings

The following descriptions show examples of some of the features available in the AXIS 211M. For details of each setting, please refer to the online help available from the setup tools. Click ? to access the online help

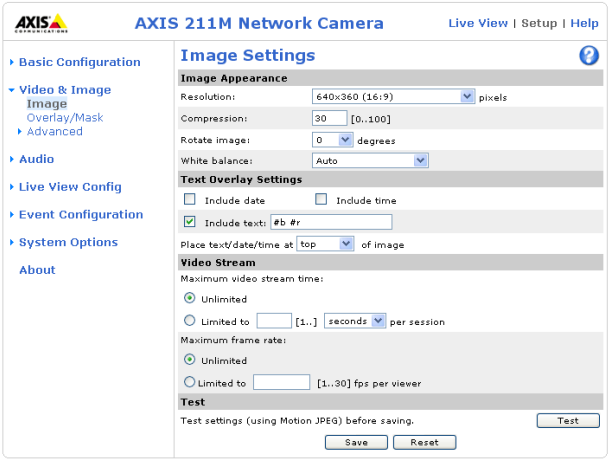


Image Appearance

Use these settings to change the image as required. The image can be rotated, the image resolution and compression can be adjusted, and the white balance can be changed.

Mirroring is the horizontal flipping of an image, that gives you another image perspective. This is a useful function when you need a direct view of the image, for example, in ATMs and door phones. The mirroring settings should be defined before you define the parameters for privacy masks and motion detection.

Resolution includes wide screen **16:9**, **partial** which stands for partial scan where an image is taken from the center region of the sensor for optimal frame rate in Motion JPEG/MPEG-4 and **full speed** which is a partial scan that has been scaled down to give full frame rate in Motion JPEG.

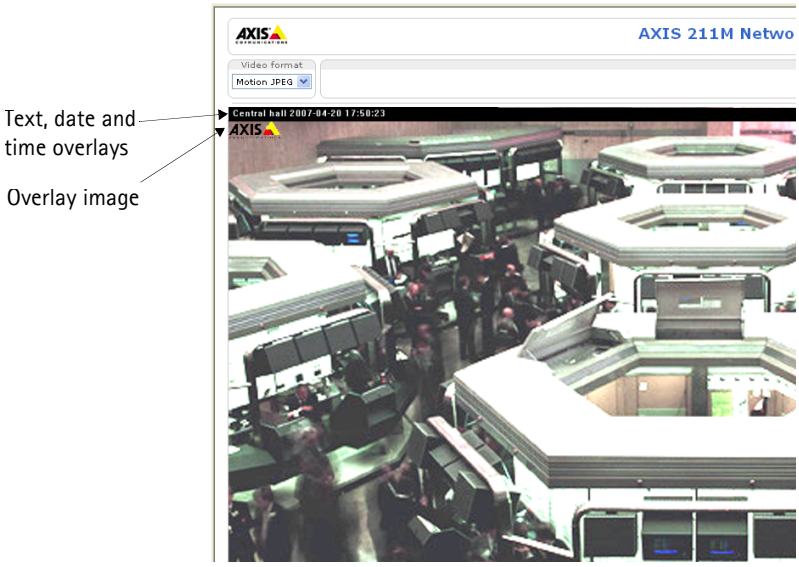
The configuration of the video image will affect the camera's overall performance, depending on how it is used and on the available bandwidth. Setting higher resolution and lower compression improves video image quality, but increases the amount of bandwidth used.

Please see the online help ? for further information on these settings.

Text Overlay Settings

Use these settings to include text and date and time overlays.

These overlays are included on one line, at the top or bottom of the video image.



Video Stream

Define the maximum **video stream time** per session in seconds, minutes or hours. When the set time has expired, a new stream can be started by refreshing the page in the browser. For unlimited video stream time, select the **Unlimited** radio button. Note that the maximum video stream time does not apply to clients connecting via multicast.

The **frame rate** allowed to each viewer can also be limited, to avoid bandwidth problems on the network. To allow the highest available frame rate, select the **Unlimited** radio button.

For a preview of the image before saving, click **Test**. When satisfied with the settings, click **Save**. Please note that the preview image will be in JPEG format, even though the settings are valid both for Motion JPEG and MPEG-4.

Please refer to the online help for more information. ?

Overlay/Mask Settings

Overlay/Mask Type

The following options are available for overlays and masks:

- Uploaded image as overlay
- Configurable areas as privacy mask

Uploaded image as overlay is a text and/or a static image superimposed over the video image, for extra information.

To upload an overlay image to the camera:

1. Select the type of overlay to use in **Overlay/Mask Type**.
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
• Windows 24-bit BMP (full color)	The height and width of the overlay image in pixels must be exactly divisible by 4.
• Windows 4-bit BMP (16 colors)	The height and width of the overlay image in pixels must be exactly divisible by 16.

There are a number of limitations when using overlay images, such as the size and positioning of images. Please refer to the online help for more information.

Configurable areas as privacy mask are configurable areas of solid color that can be used to block out certain parts of the video image.

Note: Make sure to set privacy masks while camera is set for full resolution to ensure full coverage of sensitive area.

Advanced - Camera Settings

This page contains settings for fine-tuning the video image. These include the color level, brightness, sharpness and exposure control. **DC-Iris** should always be enabled, except when focusing, or when using a non-DC-Iris lens.

Please see the online help for further information on these settings.

Low Light Behavior

Exposure priority - These settings define the balance between possible motion blur, noise and frame rate. Prioritize Image Quality to lower noise may reduce frame rate while increasing exposure time and thereby motion blur. A prioritized frame rate limits the exposure time in order to allow for full frame rate. This may raise the gain factor, creating possible noise or darker exposure.

Advanced - MPEG-4 Settings

GOV Settings

The GOV structure describes the composition of the MPEG-4 video stream. Setting the GOV-length to a high value saves considerably on bandwidth. The **Cyclic refresh** parameter gives a smoother bit rate and can be useful if bandwidth is limited.

Note: Cyclic refresh should not be enabled if **Event** handling is enabled and the file format is set to MPEG-4 in **Upload images/video** (see Setup > Event configuration > Event settings).

Bit Rate Control

Limiting the maximum bit rate is a good way of controlling the bandwidth used by the MPEG-4 video stream. Leaving the maximum bit rate as unlimited will provide consistently good image quality, but at the expense of increased bandwidth usage whenever there is more activity in the image. Limiting the bit rate to a defined value will prevent excessive bandwidth usage, but images will be lost when the limit is exceeded.

Note that a maximum bit rate can be used for both variable and constant bit rates.

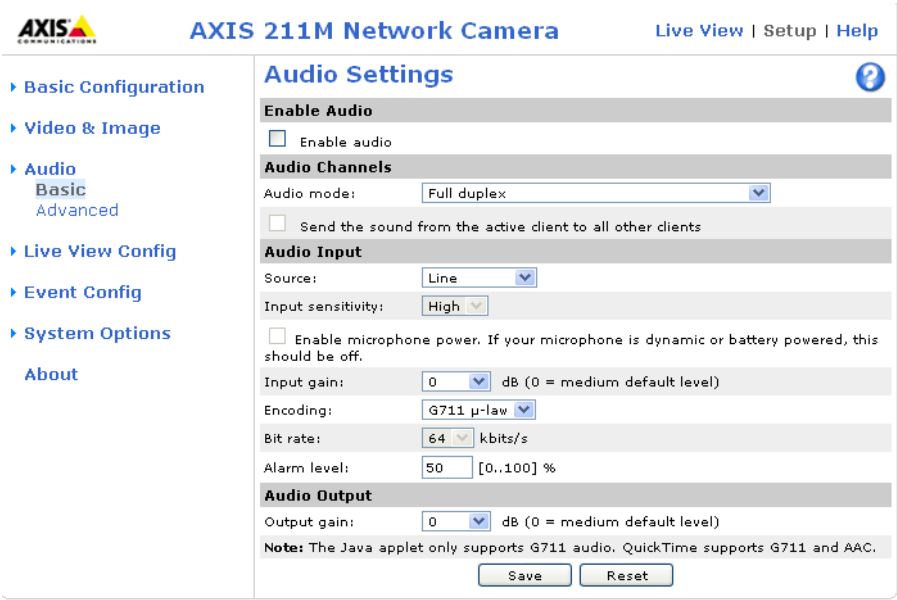
The bit rate type can be set as Variable Bit Rate (VBR) or Constant Bit Rate (CBR). VBR will adjust the bit rate according to the images' complexity, thus using a lot of bandwidth for a lot of activity in the image and less for lower activity in the monitored area.

CBR allows you to set a fixed Target bit rate that will consume a predictable amount of bandwidth, and which will not change whatever happens in the image.

As the bit rate would usually need to increase for increased image activity, but in this case cannot, the frame rate and image quality will be affected negatively. To go some of the way towards compensating for this, it is possible to prioritize either the frame rate or the image quality whenever the bit rate would normally need to be increased. Not setting a priority means the frame rate and image quality will be affected approximately equally.

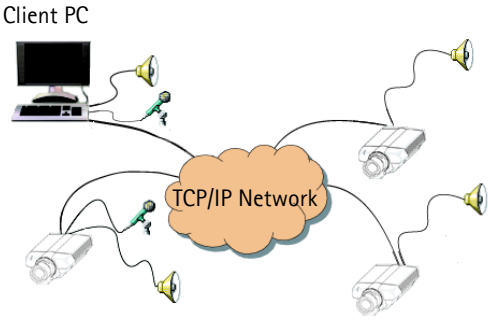
Audio Settings

The AXIS 211M can transmit audio to other clients using a connected external microphone or the internal microphone and can play audio received from other clients via connected speakers. This section describes how to configure the basic audio settings for the AXIS 211M, such as setting the communication mode and adjusting the sound levels in the microphone and speakers connected to the camera.



Note:

The speakers connected to the audio output must have a built-in amplifier, e.g. PC speakers.



Example of a network using AXIS 211M cameras to transmit audio and video across the network.

Enable Audio

Check this box to enable audio in the AXIS 211M.

Audio Channels - Audio mode

Full duplex mode is simultaneous two-way audio where you can transmit and receive audio at the same time.

Half duplex mode transmits and receives audio in both directions, but only in one direction at a time. This means that you must select when to receive or transmit audio with the push-to-talk button. To speak, press and hold the button (check that the microphone is not muted). When finished, release the button and you will receive audio from the other end of the connection.

Note that the push-to-talk button is configured from AMC. It is also possible to configure the push-to-talk button so that it toggles between speaking and listening modes.

When selecting **Simplex - Network Camera speaker only** mode, the speaker connected to the camera will play audio, but no audio will be transmitted from the camera to other web clients. This could be used to provide spoken instructions to a person seen in the camera. This mode requires you to use the push-to-talk button.

Simplex - Network Camera microphone only mode transmits audio only from the AXIS 211M to web clients. It will not receive audio from any other web clients. This can be used in remote monitoring, web attractions etc., to provide live audio, as well as video, of a monitored situation.

When using half duplex, the **Send the sound from the active client to all other clients** option transmits the audio signal from the client that is talking to all the other clients.

Audio Input

Audio from a connected microphone or a line source can be connected to the Audio in connector of the AXIS 211M. The audio source must be set to **Microphone** or **Line** depending on the connected device.

Note: To prevent unauthorized listening, the internal microphone can be disabled by inserting a plug in the Audio in connector.

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

Note: 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. The default value is DC power enabled. 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.

Set **Input sensitivity** to **High** or **Low** depending on the sound level in the monitored are. For example, if the AXIS 211M is installed in a noisy environment set the sensitivity to **Low**. When using an external microphone set the **Input sensitivity** to **High** if you are using an ordinary, unamplified microphone. Set the sensitivity to **Low** if the connected microphone has a built-in line amplifier.

Enable microphone power with electret microphones that have no battery. Do not use this setting with a dynamic or battery powered microphone.

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

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.

The AXIS 211M can be set to trigger an event if the incoming sound level rises above, falls below or passes the set value. The **Alarm level** is set between 0-100%.

Audio Output

If the sound from the speaker is too low or high, adjust the **output gain** for the active speaker attached to the AXIS 211M. When satisfied with the settings, click **Save**, or click **Reset** to revert to the previously saved settings.

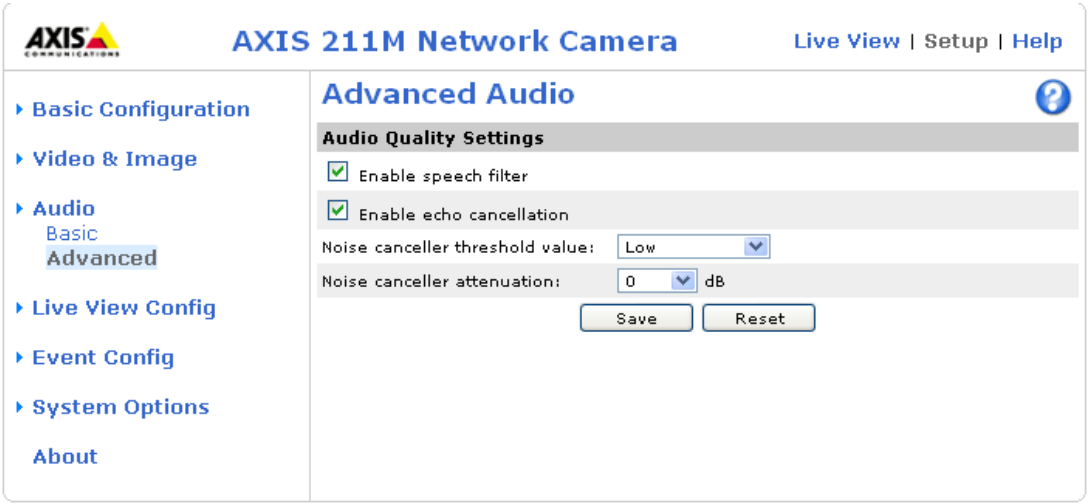
Advanced Audio

Advanced audio settings can improve audio quality by speech filtering, echo cancellation or setting the noise canceller threshold value or attenuation.

When enabled the **speech filter** reduces noise by filtering out all the frequencies below 100HZ and above 3500 Hz. This improves the sound quality if a person is close to the microphone when talking and will reduce background noises.

Enable echo cancellation to reduce acoustic echoing that can be caused by audio coming from a speaker being captured by a microphone.

Noise canceling is a way of reducing the background noise if the microphone, for example, is set up in a noisy environment and you are only interested in hearing a person who is talking close to the microphone. The **noise canceller attenuation** produces maximum noise reduction when set to 18dB of attenuation. Optimize the sound quality by listening to the sound and adjusting the attenuation level as required.

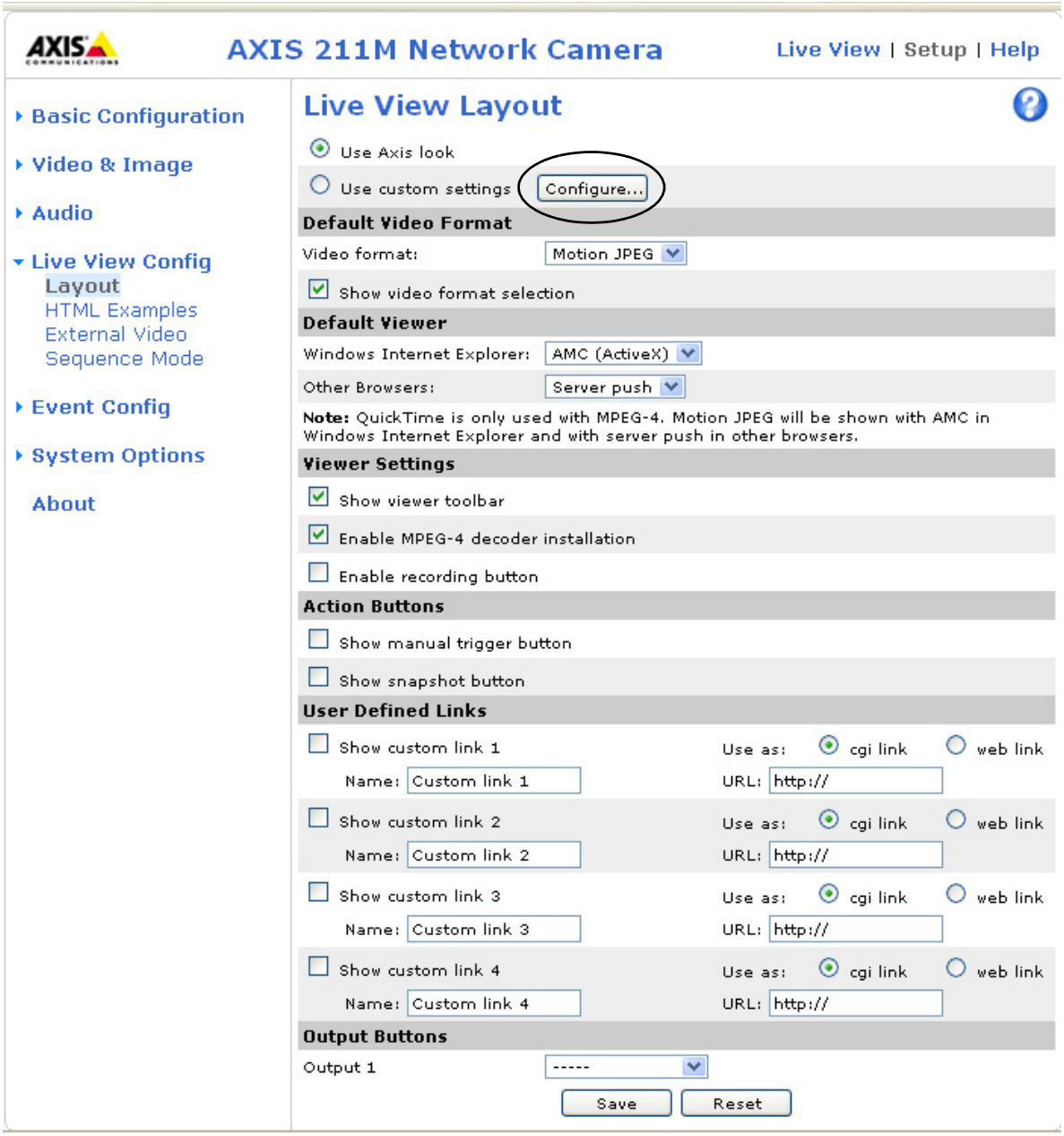


Live View Config

These are the tools for deciding the layout of the camera's **Live View** page. The layout can be set in 2 ways:

- Use **Axis look** - the layout is unchanged.
- Use **custom settings** - modify the default **Live View** page with your own colors, and images. Click the **Configure** button and see below.

The other settings on this page concern other features to include, such as buttons and links.



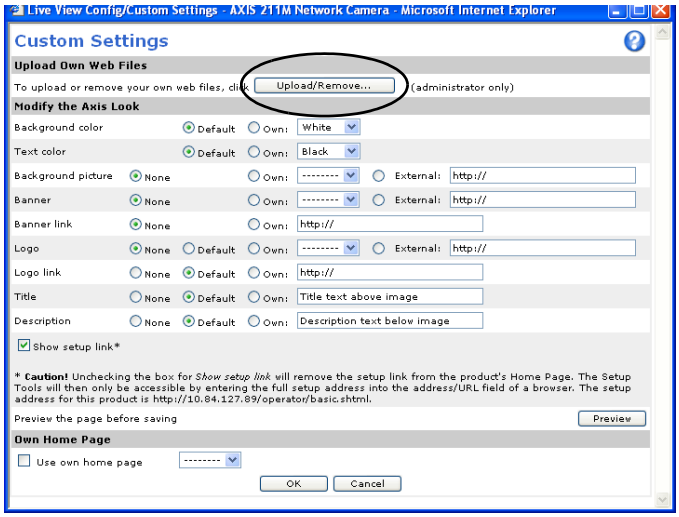
Custom settings

Adjust the settings under **Modify the Axis look**, to change the background picture, banner, or colors.

To use your own file for example a banner, first upload it (see the following page) or select **External** and enter the path to the file.

Deselecting the box option for **Show setup link** will remove the **Setup** link from the camera's Home Page. The menus will then only be accessible by entering the full setup address into the address/URL field of a browser, i.e.

http://<ip address>/operator/basic.shtml



Upload Own Web Files

Your own background pictures, banners and logos can either be located externally on a network server, or they can be uploaded to the AXIS 211M itself. Once uploaded, files appear in the drop-down lists for **Own** (file). Follow these instructions to upload a file.

1. Click the **Upload/Remove** button in the Custom settings dialog.
2. Enter the path to the file, e.g. a file located on your computer or click the **Browse** button.
3. Select the user level for the uploaded file. Setting the user access level means that you have complete control over users viewing specific pages.
4. When the path is shown correctly in the text field, click the **Upload** button.

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

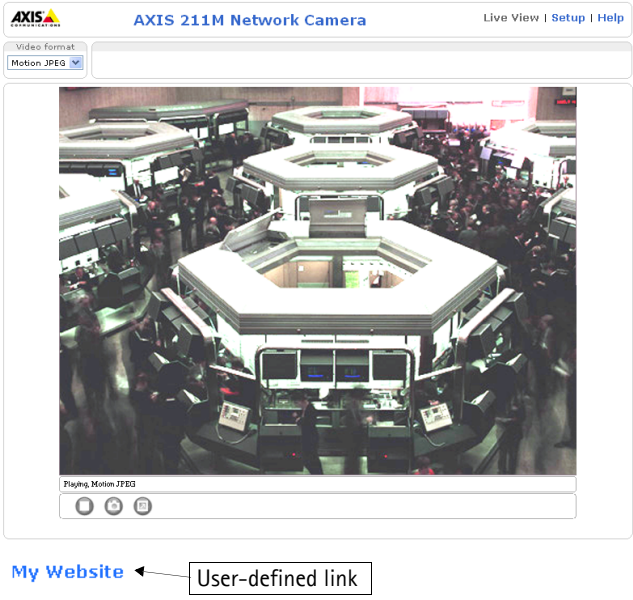
Own home page

On the **Live View Layout** web page, select the radio button **Use custom settings** and click **Configure**.

Check the box option **Use own home page** at the bottom of this dialog. To use a previously uploaded web page (see above) as the default home page, select the page from the drop-down list and click OK.

Default Video Format

Select default video format from the drop-down list. Check the box option to enable video format selection from the **Live View** Page.



Default Viewer

When using Microsoft Internet Explorer (IE) for Windows, select your preferred method of viewing moving images. The options are:

- AMC (ActiveX) - this is the best choice for fast image updating in Internet Explorer for Windows, but might not be possible on computers that have restriction on the installation of additional software.
- QuickTime - for use with MPEG-4 only, select this to use the QuickTime plug-in for Microsoft Internet Explorer.
- Java applet - this alternative uses a Java applet to update the images in the browser.
- Still Image - displays still images only. Hit the Refresh button in your browser to view a new image.

When using any browser other than Internet Explorer for Windows, select the appropriate method from the drop-down list for viewing images. The available options are similar to Internet Explorer except for Server Push. With this method, the camera maintains and controls an open HTTP connection to the browser and sends data as and when required for as long as required.

Please see the online help ? for more information.

Viewer settings

Show viewer toolbar - uncheck to remove the viewer toolbar from the **Live View** page.

Enable MPEG-4 decoder installation - enables/disables the installation of the MPEG-4 decoder included with AMC.

Enable recording button - enables recording directly from the **Live View** page. The recording is saved in the folder specified in the Recording tab in the AMC Control Applet. Note that this button is only available when viewing with AMC.

Action Buttons

These buttons can be used to manually trigger and stop an event from the **Live View** page. For more information, see Event servers, on page 30.

The snapshot button allows users to take a snapshot of the video stream and save it on a computer.

User Defined Links

Enter a descriptive name and enter the URL in the provided field. The link appears on the **Live View** page.

User defined CGI links can be used to issue HTTP API requests, such as PTZ commands.

Example:

1. Check Show custom link 1.
2. Enter a descriptive name, e.g. CAM START.
3. Select the Use as cgi link radio button and enter the cgi link in the field:
4. Check Show custom link 2.
5. Enter a descriptive name, e.g. CAM STOP.
6. Select the Use as cgi link radio button and enter the cgi link in the field:
7. These links will appear in the web interface and can be used to control the PTZ camera.

For more information on the Axis HTTP API, see the Support / Developer pages on the Axis Website at http://www.axis.com

Output Buttons

These buttons can then be used to manually start and stop an event from the **Live View** page, such as switching a light on/off:

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

HTML Examples

You can add live video from the camera to your own web site. The camera can transmit a Motion JPEG or unicast MPEG-4 stream to up to 20 simultaneous connections, although an administrator can restrict this to fewer. If multicast MPEG-4 is used, the video stream will be available to an unlimited number of viewers connected to the parts of the network where multicast is enabled. Please note that a separate MPEG-4 license is required for each viewer.

Enter the **Video Format**, **Image Type**, **Image size** and other settings to suit your Web page and click **Update.** The camera then generates the required source code for your configuration. Copy this code and paste it into your own Web page code.

External Video

The camera can also display video images from other Axis network cameras and video servers, directly on the **Live View** page. These are known as **External Video** sources. These external video sources are available from the drop-down list on the Live View page.

Click the **Add** button to open the External Video Source Setup dialog, which is used to make all the necessary settings. Enter the IP address or host name of the external video source you wish to add. Depending on the external source, select either MPEG-2, MPEG-4 or Motion JPEG as the type of video stream to receive.

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 cycle through the internal and selected 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 that appear on the **Live View** page are used to start and stop the sequence mode.

Please see the online help for more information.

Event Configuration

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

An event that is triggered by a signal, such as a door switch, motion detection, or system event, is called a triggered event.

A scheduled event runs at pre-programmed times.

An Action refers to what happens when the event occurs.

This section describes how to set up event servers and event types, i.e. how to configure the camera to perform certain actions when events (e.g. alarms) occur.

Event Servers

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

Server type	Purpose	Information required
FTP Server	• Receives uploaded images	• Descriptive name of your choice • Network address (IP address or host name) • User name and password (for FTP server) • Upload path e.g. images/ • Port number • Use passive mode if there is a firewall between the camera 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	• Receives notification messages • Receives uploaded images	• Descriptive name of your choice • URL (IP address or host name) • User name and password (for HTTP server) • Proxy address/Proxy port (if required) • Proxy User name and password (if required)
TCP Server	• Receives notification messages	• Descriptive name of your choice • Network address (IP address or host name) • Port number

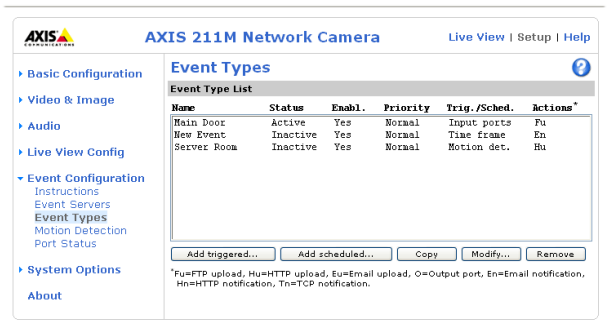
For details on each setting, please see the online help ? available from each web page.

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

Configuring Event Types

An **Event Type** describes how and when the camera will perform certain actions.

Example: If somebody passes in front of the camera and an event that uses motion detection has been configured to act on this, the camera can, e.g. record and save images to an FTP server, and/or send a notification e-mail to a pre-configured e-mail address with a pre-configured message. Images can be sent as e-mail attachments.



Triggered Event

A Triggered event can be activated by:

- **Input port** - a switch (e.g. a push button) connected to the camera
- **Manual trigger** - a manually activated action, e.g. from an action button in the web interface
- Detected movement in a configured **motion detection** window
- **Audio** alarm
- On restart (**reboot**) after, e.g. power loss

How to set up a triggered event

This example describes how to set the camera to upload images when, e.g 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 open.
3. Set the **priority** - High, Normal or Low (see the online help).
4. Set the **Respond to Trigger...** parameters for when the event will be active, e.g. only after office hours.
5. Select the trigger alternative from the **Triggered by...** drop-down list, e.g. select Input port, for the sensor connected to the door.
6. Set the **When Triggered...** parameters, i.e. define what the camera will do if the main door is opened e.g. upload images to an FTP server or send an e-mail.
7. Click **OK** to save the Event in the Event Types list.

Please use the online help ? for descriptions of each available option. Image file names can be formatted according to specific requirements, such as time/date or type of triggered event. See *File Naming & Date/Time Formats* under *Event Configuration*.

Note: Up to 10 event types can be configured in the camera, and up to 3 of these can be configured to upload images.

Pre-trigger and Post-trigger buffers

This function is very useful when checking to see what happened immediately before and/or after a trigger, e.g. up to 30 seconds before and/or after a door was opened. Check the **Upload images** checkbox under **Event Types > Add Triggered... > Triggered by...** to expand the web page with the available options. All uploaded images are JPEG images.

Include pre-trigger buffer - images stored internally in the camera 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:
- Pre-trigger and Post-trigger buffers will be lost if the connection to the event server fails.
- The maximum length of the pre-/post-buffer depends on the video image size and selected frame rate.
- If the pre- or post-buffer is too large for the camera's internal memory, the frame rate is reduced and no image is uploaded. If this occurs, an entry will be created in the unit's log file.

Continue image upload (unbuffered) - enables the upload of video 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 preset times, in a repeating pattern on selected weekdays.

Configuration example:

1. Click **Add scheduled** on the **Event types** page.
2. Enter a descriptive **name** for the event, e.g. "Scheduled e-mail upload."
3. Set the **priority** (High, Normal or Low).
4. Set the **Activation Time** parameters (24h clock) when the event will be active, e.g. start on Sundays at 13.00 with a duration of 12 hours.
5. Set the **When Activated...** parameters, i.e. set what the camera will do at the specified time, for example send uploaded images to an e-mail address.
6. Click **OK** to save the Event in the Event Types list.

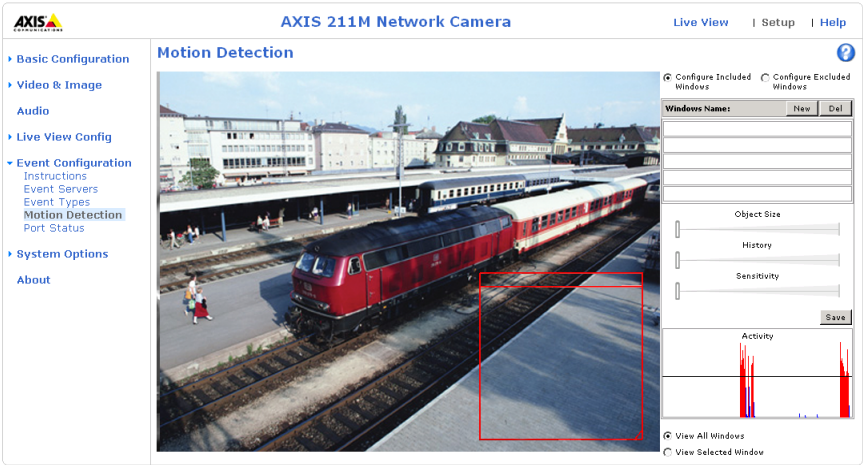
Please see the online help ? for descriptions of each available option.

Motion Detection

Motion detection 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 *How to set up a triggered event* above.



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

If AMC is not used, the Motion Detection web page may look different from the image here.

Configuring Motion Detection

1. Click **Motion Detection** in the **Event Configuration** menu.
2. Click the **Configure Included Window** radio button and click **New**.
3. Enter a descriptive name under **Window name**.
4. Adjust the size (drag the bottom right-hand corner) and position (click on the text at the top and drag to the desired position).
5. 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).
6. 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.

Object size, history and sensitivity:

	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 only 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 camera's input and output. This is for the benefit of **Operators**, who cannot access the System Options section.

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

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

System Options

Security

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

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

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

User Settings - check the relevant check boxes to enable:

- **Anonymous viewer login** - allows any viewer direct access to the Live View page.
- **Maximum number of simultaneous viewers** - enter a value here to restrict the number of unicast viewers accessing the unit. This is useful if you need to save on bandwidth. (Note that all multicast viewers count as 1 viewer.)

The AXIS 211M Network Camera supports different methods of user authentication:

HTTP Basic Authentication - This authenticates the user by requesting a user name and a password. The exchange of network credentials is in simple base64 coding and is not encrypted.

HTTP Digest Authentication - This method also requests a user name and password, but the exchange of credentials is encrypted, which secures it against eavesdropping.

IP Address Filtering

Checking the **Enable IP address filtering** box enables the IP address filtering function, whereby the IP addresses in the list of filtered addresses will be allowed or denied access to the AXIS 211M.

Up to 256 IP address entries may be specified (a single entry can contain multiple IP addresses). All other IP addresses not in this list will 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. Click the **Add** button to add new filtered addresses. See also the online help for more information.

Referrals - To prevent unauthorized clients from including the video stream from the cameras into external Web pages, check the Referrals checkbox and enter the IP address or Host name of the computer that hosts the Web pages with the included video stream. Several IP addresses/host names can be defined and are separated by semicolons (;). This option is only applicable to Motion JPEG video streams.

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

The AXIS 211M supports encrypted browsing using HTTPS.

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

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

In an 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 FreeRADIUS 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 (Remote Authentication Dial In User Service) - 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, thus acting 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 the Overlay (see below).

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

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

- **Synchronize with computer time** - sets the time from the clock on your computer.
- **Synchronize with NTP Server** - the camera will obtain the time from an NTP server every 60 minutes. The NTP Server can be set under **Network** > **TCP/IP** > **Advanced** or click on the **No server specified** link, see *NTP Configuration,* on page 32.
- **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 video streams.

Use the pre-defined formats or use your own custom date and time formats. See **Advanced File Naming & Date/Time Formats** in the online help ? for information on how to create your own file formats.

Network - Basic TCP/IP Settings

IP Address Configuration

The AXIS 211M 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 for the AXIS 211M can be set automatically via DHCP, or a static IP address can be set manually.

If IPv6 is enabled, the AXIS 211M 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 camera. Configure the options for notification of IP address change (under Services) to receive notification from the camera when the IP address changes.
- Alternatively, if your DHCP server can update a DNS server, you can access the AXIS 211M 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.

Options for notification of IP address change - If the IP address for the camera changes, e.g. automatically by DHCP, you can choose to be notified of the change. Click **Settings...** and enter the required information.

AXIS Internet Dynamic DNS Service - Use the AXIS Internet Dynamic DNS service to assign a host name for easy access to your AXIS 211M Network Camera (requires Internet access).

Click **Settings...** to register the AXIS 211M with the Axis Internet Dynamic DNS service, or to modify the existing settings (requires access to the Internet). The domain name currently registered at the Axis Internet Dynamic DNS service for your product can at any time be removed.

For more information, please refer to the online help.

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 AXIS 211M. 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 Configuration

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

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

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

Host Name Configuration

The AXIS 211M 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, see the online help.

Link-Local IPv4 Address

This is enabled by default and assigns the AXIS 211M an additional IP address for use with UPnP™. The AXIS 211M 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 security port mapping.

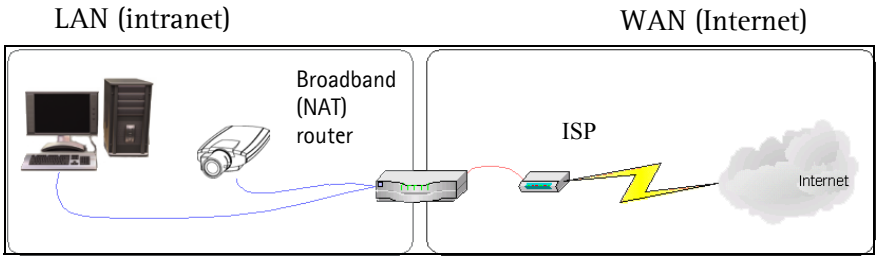
HTTPS

If applicable, enter the HTTPS port the AXIS 211M will use. The default setting (443) can be changed to any port within the range 1024-65535. HTTPS is used to provide encrypted web browsing.

NAT traversal (port mapping)

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

Use **NAT traversal** when your AXIS 211M is located on an intranet (LAN) and you wish to make it available from the other (WAN) side of a NAT router. With NAT traversal properly configured, all HTTP traffic to an external HTTP port in the NAT router will be forwarded to the camera.



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

Enable/Disable - When enabled, the AXIS 211M will attempt to configure port mapping in a NAT router on your network, using UPnP™. Note that UPnP™ must be enabled in the camera (see **System Options > Network > UPnP™**).

Use manually selected NAT router - Select this option to manually select a NAT router and enter the IP address for the router in the field provided.

If a router is not manually specified, the AXIS 211M will automatically search for NAT routers on your network. If more than one router is found, the default router will be selected.

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

Notes:
- An alternative HTTP port can be used/be active even if NAT traversal is disabled. This is useful if, e.g. your NAT router does not support UPnP™ and you need to manually configure port forwarding in the NAT router.
- If a manually selected port is already in use, another will automatically be selected.
- When the port is selected automatically it will be displayed in this field. This can be changed by entering a new port number and clicking Save.

FTP

The FTP server running in the AXIS 211M enables the upload of, e.g. new firmware, and user applications. Check the box to enable the service.

RTSP

The RTSP protocol allows a connecting client to start an MPEG-4 stream. Check the box to enable the service and enter the RTSP port number to use. The default setting (554) can be changed to any port within the range 1024-65535.

Network Traffic

Connection Type - 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.

SOCKS

SOCKS is a networking proxy protocol. The AXIS 211M 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 AXIS 211M is located on a local network behind a firewall, but notifications, uploads, and alarms 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 a maintained level of bandwidth, low latency, no packet losses. The main benefits of a QoS-aware network can be summarized as:

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

The QoS in Axis network video products marks the data packets for various types of network traffic originating from the product. This makes it possible for network routers and switches to, e.g. reserve a fixed amount of bandwidth for these types of traffic. The types of traffic marked by the camera are video, audio, event/alarm and management network traffic.

QoS DSCP 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 hexadecimal format, 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 the sending of notifications and image/video email messages from the camera to predefined addresses via SMTP.

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

SNMP

The Simple Network Management Protocol (SNMP) allows remote management of network devices. Depending on the level of security required, select the version of SNMP to use. The three levels of security are:

- SNMP V1 - includes no security.
- SNMP V2c - uses very simple security. The community name can be specified as a password for read or read/write access to all supported SNMP objects. The community is the group of network devices using SNMP.
- SNMP V3 - provides encryption and secure passwords. HTTPS must be enabled.

Traps for SNMP v1/v2/v3

Traps are used by the camera to send messages to a management system for important events or status changes. These settings are used with SNMP v1/v2/v3.

You can activate trap reporting, enter the IP address of the management server, and choose the trap community to use when sending a trap message to the management system.

UPnP™

The camera includes support for UPnP™, which is enabled by default. If also enabled on your computer, the camera will automatically be detected and a new icon will be added to "My Network Places."

Note: UPnP™ must also be enabled on your operating system. Refer to your operating systems help or user manual for more information.

RTP / MPEG-4

These settings are the port range, IP address, port number (video and audio), and Time-To-Live value to use for the video stream(s) in multicast 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

The AXIS 211M includes support for Bonjour. When enabled, the camera is automatically detected by operating systems and clients that support this.

Ports & Devices

I/O Ports - the pinout, interface support and the control and monitoring functions provided by this connector are described in *I/O Terminal Connector*, on page 37.

LED Settings

The Network Indicator LED can be enabled or disabled, according to requirements and the Status indicator LED can be set to flash at a configurable interval (or to not light up at all) whenever the unit is accessed. For a listing of all LED behavior, see page 6, or the online help.

Note that the Status LED does not flash when the stream is retrieved using MPEG-4 multicast.

Maintenance

•Restart - The camera is restarted without changing any of the settings.

•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

•Default - The default button should be used with caution. Pressing this will return all of the camera's settings to the factory default values (including the IP address).

Upgrade Server - See *Upgrading the Firmware*, on page 39.

Backup - To take a backup of all of the parameters, and any user-defined scripts, click this button. If necessary, it will then be possible to return to the previous settings, 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 the configuration of multiple units or for firmware upgrades.

Support

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

System Overview - is a quick look at the camera's status and settings. Information that can be found here includes the camera's Firmware version, IP address, Security, Optional Network Services, Event Settings, Image settings and Recent log items. Many of the captions are also links to the proper **Setup page** to conveniently make adjustments in the camera's settings.

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

Information

Logs, Server Report and **Parameter List** all provide valuable information for troubleshooting and when contacting Axis support.

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 means for customizing and using scripts.

Caution!

The scripting function is a very powerful tool. Improper use may cause unexpected behavior or even loss of contact with the unit. If a script does cause problems, reset the unit to its factory default settings (in which case, a previously saved backup file will be useful for returning the unit to its latest configuration). **Axis strongly recommends that you do not use this function unless you fully understand the consequences.** Axis support provides no assistance for 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 previous experience of configuring Axis cameras. All parameters can be set and modified from this page. Help is available via the links on the standard setup pages.

Resetting to the Factory Default Settings

To reset the camera to the original factory default settings, go to the **System Options > Maintenance** web page (as described in *Maintenance,* on page 35) or use the **Control** button on the rear of the camera (see the illustration on page 5) as described below:

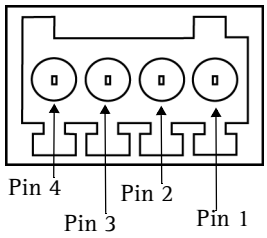
Using the Reset Button

To reset the camera to the factory default settings using the Reset Button:

1. Disconnect the power adapter, or the network cable if using PoE.
2. Press and hold the Reset button while reconnecting power.
3. Keep the Reset button pressed until the **Status Indicator** color changes to amber (which may take up to 15 seconds).
4. Release the Reset button.
5. When the Status Indicator changes to Green (which may take up to 1 minute), the process is complete and the camera has been reset. The unit will now have the default IP address 192.168.0.90

I/O Terminal Connector

The I/O terminal connector is used in applications such as motion detection, event triggering, time lapse recording and alarm notifications. It provides the interface to:

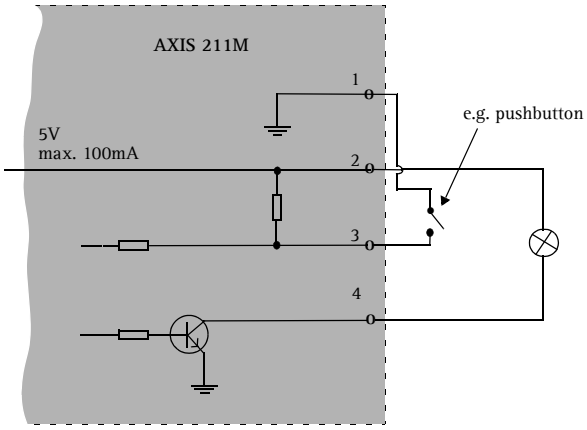


Terminal connector. Note that the pins are numbered 1-4, right to left.

- 1 transistor output - For connecting external devices such as relays and LEDs. Connected devices can be activated by the 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, and glass break detectors. When a signal is received the **state** changes and the input becomes active (shown under **Event Configuration > Port Status**).
- Auxiliary power and GND.

Function	Pin number	Notes	Specifications
GND	1		
5V DC Power	2	Can be used as an alternative power supply (7-20VDC) or to power auxiliary equipment +5VDC (100mA).	Max load = 100mA
Digital Input	3	Connect to GND to activate, or leave floating (or unconnected) to deactivate.	Must not be exposed to voltages greater than 20VDC
Transistor Output	4	Connects to GND when activated. If used with an external relay, a diode must be connected in parallel with the load for protection against voltage transients.	Max load =100mA Max voltage = 24VDC (to the transistor)

Connection diagram



Troubleshooting

Checking the Firmware

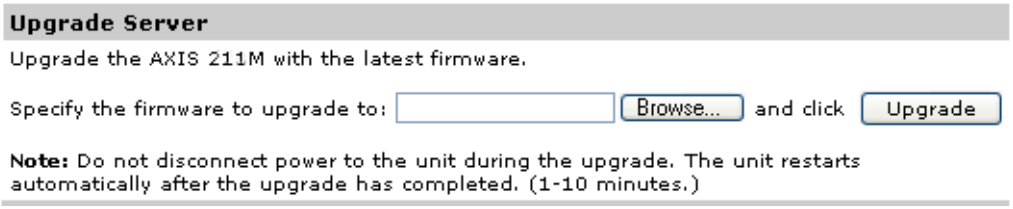
Firmware is software that determines the functionality of the AXIS 211M. One of your first actions when troubleshooting a problem should be to check the currently installed firmware version. The latest version may contain a correction that fixes your particular problem. The current firmware version in your camera can be seen on the page **Setup > Basic Configuration.**

Upgrading the Firmware

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

Note: Preconfigured and customized settings will be saved when the firmware is upgraded (providing 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 firmware is available free of charge from the Axis Web site at **www.axis.com/techsup**
2. Go to **Setup > System Options > Maintenance** in the camera's Web pages.
3. In the **Upgrade Server** section, browse to the desired firmware file on your computer. Click **Upgrade**.



Notes:
- **After starting the upgrade process, always wait at least 5-10 minutes before restarting the camera, even if you suspect the upgrade has failed.**
- **Your dealer reserves the right to charge for any repair attributable to faulty upgrading by the user.**
- **Always read the upgrade instructions available with each new release, before updating the firmware.**

Emergency Recovery Procedure

If power to the camera 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 label attached to the bottom of the camera.

1. If the unit does not reply within a few seconds, restart it and wait for a reply. Press CTRL+C to stop Ping.

Unix/Linux -From the command line, type the following: arp -s <IP address of camera> <Serial number> temp ping -s 408 <IP address of camera>	**Windows** - From a command/DOS prompt, type the following: arp -s <IP address of camera> <Serial number> ping -l 408 -t <IP address of camera>

2. Open a browser and type in the camera's IP address. In the page that appears, use the **Browse** button to select the upgrade file to use, e.g. axis211m.bin. Then click the Load button to restart the upgrade process.
3. 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.
4. Re-configure the camera.

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

Axis Support

If you contact Axis support, please help us to help you solve your problems, by providing the server report, the 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.

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

Symptoms, Possible Causes and Remedial Actions

Problems setting the IP address	
When using ARP/Ping.	Try the installation again. The IP address must be set within two minutes after running the ARP command. Ensure the Ping length is set to 408.
The camera is located on a different subnet.	If the IP address intended for the camera and the IP address of your computer are located on different subnets, you will not be able to set the IP address. Contact your network administrator to obtain an appropriate IP address.
The IP address is being used by another device.	Disconnect the camera from the network. Run the Ping command. (In a Command/DOS window, type **ping** and the **IP address** of the unit). If you receive: **Reply from <IP address>: bytes = 32; time = 10 ms.....** - this means that the IP address is already in use on your network. You must obtain a new IP address and reinstall the unit. If you see: **Request timed out** - this means that the IP address is available for use with your camera. In this case, check all cabling and reinstall the unit.
Possible IP address conflict with another device on the same subnet.	The static IP address in the camera is used before the DHCP server sets a a dynamic address. This means that if the same default static IP address is also used by another device, there may be problems accessing the camera. To avoid this, set the static IP address to 0.0.0.0.
The camera cannot be accessed from a Web browser	
The IP address has been changed by DHCP.	1) Move the camera to an isolated network, or to one with no DHCP or BOOTP server. Set the IP address again, using the AXIS IP Utility (see the Installation Guide) or the ARP/Ping commands. 2) Access the unit and disable DHCP in the TCP/IP settings. Return the unit to the main network. The unit now has a fixed IP address that will not change. 3) As an alternative to 2), if dynamic IP address via DHCP or BOOTP is required, select the required service and then configure IP address change notification from the network settings. Return the unit to the main network. The unit will now have a dynamic IP address, but will notify you if the address changes.
Proxy server.	If using a proxy server, try disabling the proxy setting in your browser.
Other networking problems.	Test the network cable and connectors by connecting it to another network device, then Ping that device from your workstation. See the instructions above.
Cannot log in.	Check that you are using the proper password. If HTTPS is enabled, ensure that the correct protocol (HTTP or HTTPS) is used when attempting to log in. You may need to manually type in http or https in the browser's address bar.
Incorrect host name.	Check that the host name and DNS server settings are correct. See the basic and advanced TCP/IP settings.
Cannot send notifications, uploads, alarms, etc, to a destination outside the local network	
Firewall protection.	The camera can be configured to use a SOCKS server to reach networks on the other side of a firewall/proxy server.
Your camera 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.
Poor or intermittent network connection.	
Network switch.	If using a network switch, check that the port on that device uses the same setting for the network connection type (speed/duplex) as set in the advanced TCP/IP settings. The Auto-Negotiate setting is recommended.

Video/Image problems - general

No images in browser (*Internet Explorer for Windows only*)	To enable the updating of video images in Microsoft Internet Explorer, set your browser to allow ActiveX controls. Also, make sure that AXIS Media Control (AMC) component is installed on your workstation.
Installation of additional ActiveX component restricted or prohibited.	Configure your camera to use a Java applet for updating the video images under Live View Config > Layout > Default Viewer for Internet Explorer. See the online help for more information.
Image too dark or too light.	Check the video image settings. See the online help on Video and Image Settings.
Missing images in uploads.	This can occur when trying to use a larger image buffer than is actually available. Try lowering the frame rate or the upload period.
Slow image update.	Configuring, e.g. pre-buffers, motion detection, high-resolution images, high frame rates, etc, will reduce the performance of the camera.
Poor performance.	Poor 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.
Image gradually gets darker or lighter.	When using the camera in locations lit by fluorescent lighting, check in the advanced image settings that the Exposure control is set to **Flicker-free**.
Image loses focus often.	Disable the DC-Iris lens in the settings for **Video & Image > Advanced**. Focus the camera following the instructions on page 9, and then enable the DC-Iris lens.
Images only shown in black & white.	Check the color level setting.
Blurred images.	Refocus the camera. Check in the Video & Image > Advanced - Camera Settings that DC-Iris is set to Enabled. If the images are still blurred adjust the metal ring until the image is sharp,
Rolling dark bands or flickering in image.	Try adjusting the Flicker-free exposure setting under advanced image settings. Note that the 'Hold Current'/Manual setting may cause unwanted effects.

Video/image problems - MPEG-4

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 that you have a recent MPEG-4 decoder installed. Check in the AMC control panel applet (MPEG-4 tab) that video processing is not set to **Decode only I frame**. Lower the image resolution. Reduce the number of applications running on the client computer Reduce the number of clients that have access to the AXIS 211M.
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 AXIS 211M are valid for your network.
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. If images are degrading, try decreasing the GOV length, see *Advanced - MPEG-4 Settings*, on page 16.
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.

The test image does not display as expected.

Image settings.	Not all settings have an effect on the test image. For more information, see the help on Image Settings.

The Power indicator is not constantly lit

Faulty power supply.	Check that you are using an AXIS PS-K power supply.
The Status indicator LED is flashing red and the camera is inaccessible	
A firmware upgrade has been interrupted or the firmware has otherwise been damaged.	See the *Emergency Recovery Procedure* above.
Poor quality snapshot images	
Screen incorrectly configured on your workstation.	In Display Properties, configure your screen to show at least 65000 colors, i.e. at least 16-bit. Using only 16 or 256 colors will produce dithering artifacts in the image.
Browser freezes	
Safari or Firefox 1.4 (or later) can sometimes freeze on a slow computer.	Lower the image resolution.
Problems uploading files	
Limited space.	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.
Overlay/Privacy mask is not displayed	
Incorrect size or location of overlay or privacy mask.	The overlay or privacy mask may have been positioned incorrectly or wrong resolution was used while positioning. Refer to the online help for information on the limitations when using image overlays and privacy masks.
Motion Detection triggers unexpectedly	
Changes in luminance.	Motion detection is based upon changes in luminance in the image. This means that if there are sudden changes in the lighting, motion detection may be mistakenly triggered. Lower the sensitivity setting to avoid problems with luminance.

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

Technical Specifications

Item	Specification
Image sensor	1/3" Micron Progressive Scan RGB CMOS 1.3 Megapixel
Lens	3.0 - 8.0 mm, F1.0, DC-iris, CS mount. Horizontal viewing angle: 35°-93°,
Minimum illumination	1lux, F1.0
Video compression	• Motion JPEG • MPEG-4 Part 2 (ISO/IEC 14496-2) with motion estimation, Profiles: Advanced Simple Profile level 0-5 and Simple Profile level 0-3
Resolutions	24 resolutions from 1280 x 1024 to 160 x 90 via API, 22 selections via configuration web page
Frame rate	Motion JPEG: • Up to 12 fps in 1280 x 1024 • Up to 20 fps at 1024 x 768 (partial scan) • Up to 30 fps at 800 x 600 (partial scan) MPEG-4: • Up to 8 fps at 1280 x 1024 • Up to 13 fps at 1024 x 768 (partial scan) • Up to 20 fps at 800 x 600 (partial scan) *Partial scan takes the data from the center region of the sensor and then scales it down to present an image at optimal frame rate.
Video streaming	• Simultaneous Motion JPEG and MPEG-4 • Controllable frame rate and bandwidth • Constant and variable bit rate (MPEG-4)
Image settings	• Compression levels: 100 • Rotation: 0°, 180° • Configurable color level, brightness, sharpness, contrast, white balance, exposure control • Mirroring • Overlay capabilities: time, date, text, image or privacy mask
Shutter time	1/4 to 1/15000 sec.
Audio	• Two-way (full and half duplex) or one-way or audio off. • Built-in microphone and external microphone input or line input. Mono audio output (line level) connects to active speaker with built-in amplifier. • Audio compression: G.711 PCM 64kbit/s, G.726 ADPCM 32 or 24 kbit/s, AAC LC 8-32kbit/s+R17
Security	• Multiple user access levels with password protection, IP address filtering, HTTPS encryption, Network control IEEE 802.1x • Digest authentication
Users	• 20 simultaneous users • Unlimited number of users using multicast (MPEG-4)
Alarm and event management	• Events triggered by built-in motion detection, audio detection, external input or according to a schedule. • Image upload over FTP, email and HTTP. Notification over TCP, email, HTTP and external outputs. • Pre- and post alarm buffer: up to 20 MB (250 images or more, in full 1280 x 1024 resolution in Motion JPEG)
Connectors	• RJ-45 for Ethernet 10BaseT/100BaseTX, Auto-MDIX • Terminal block for 1 alarm input, 1 output and alternative power connection • 3.5 mm jack for Mic or Line mono input • 3.5 mm jack for Line mono output.
Casing	Plastic
Processors, memory, clock	• CPU, video processing and compression: ARTPEC-A • RAM: 64 MB • Flash: 8 MB • Battery backed-up real-time clock
Power	7-20 V DC max 5 W PoE IEEE802.3af Class 2
Operating conditions	0 - 45 °C (32 – 113 °F) Humidity 20 - 80% RH

Item	Specification
Installation, management and maintenance	AXIS Camera Management tool on CD and web-based configuration Configuration of backup and restore Firmware upgrades over HTTP or FTP, firmware available at www.axis.com
Video access from Web browser	Camera live view, Video recording to file (ASF), Sequence tour for up to 20 Axis video sources Customizable HTML pages
Minimum requirements	Pentium III CPU 500 MHz or higher, or equivalent AMD,128 MB RAM, AGP graphics card 32 MB RAM, Direct Draw Windows 2000 or later Internet Explorer 6.x or later For other operating systems and browsers see www.axis.com/techsup
System integration support	Open API for application integration including AXIS VAPIX API*, AXIS Media Control SDK*, event trigger data in video stream 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, QoS, SNMPv1/v2c/v3 (MIB-II), RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, ICMP DHCP, UPnP, Bonjour, ARP, DNS, DynDNS, SOCKS, IEEE802.1X. 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 Tool kit (www.openssl.org)
Video management software (not included)	AXIS Camera Station - Surveillance application for viewing, recording and archiving up to 25 cameras See www.axis.com/partner/adp_partners.htm for more software applications via partners
Accessories (included)	Power supply 9 V DC, stand, connector kit, Installation Guide, CD with installation tool, software and User's Manual, MPEG-4 licenses (1 encoder, 1 decoder), MPEG-4 decoder (Windows)
Accessories (not included)	Housings for adverse indoor/outdoor environments Power over Ethernet midspans AXIS 292 Network Video Decoder MPEG-4 Decoder multi-user license pack
Approvals	EN 55022 Class B, EN 61000-3-2, EN 61000-3-3, EN 55024, FCC Part 15 Subpart B Class B, ICES-003 Class B VCCI Class B, C-tick AS/NZS CISPR22, EN 60950-1 Power supply: EN 60950, UL, cUL
Dimensions (HxWxD) and weight	44 x 88 x 172 mm (1.7" x 3.5" x 6.8") 244 g (0.5 lb) excl. power supply

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.

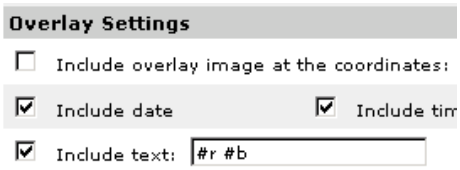
The following factors are among the most important to consider:

- 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) 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 camera's CPU load. Frame rate affected.
- Enabled motion detection. Frame rate and bandwidth affected.
- Heavy network utilization due to poor infrastructure. Bandwidth affected
- Viewing on poorly performing client PC's lowers perceived performance. Frame rate affected.

Optimizing your system

To see the bandwidth and frame rate currently required by the video stream, the AXIS 211M 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 > Overlay Settings**, and the help for **File Naming & Date/Time Formats**.

Glossary of Terms

802.1x - 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).

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

AF (Autofocus) - A system by which the camera lens automatically focuses on a selected part of the subject.

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

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

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

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

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

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

AVI (Audio Video Interleave) - A video format that supports simultaneous playback of audio and video.

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

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

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

Bluetooth - Bluetooth is an open standard for wireless transmission of voice and data between mobile devices (PCs, handheld computers, telephones and printers).

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

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

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

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

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

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

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

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

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

Compression - See *Image Compression*.

Contrast - Defines the degree of difference between the lightest and darkest parts of an image or video stream.

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

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

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

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

DNS (Domain Name System) - DNS is used to locate and translate Internet domain names into IP (Internet Protocol) addresses. A domain name is a meaningful and easy-to-remember name for an Internet address. For example the domain name www.example.com is much easier to remember than 192.0.34.166. The translation tables for domain names are contained in Domain name servers.

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

Duplex - See *Full-duplex*.

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

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

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

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

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

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

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

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

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

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

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

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

GOV (Group Of VOPs) - A group of VOP's is the basic unit of an MPEG-4 video stream. The GOV contains different types and numbers of VOP's (I-VOP's, P-VOP's, etc) as determined by the GOV length and GOV structure. See also *VOP*.

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

GOV structure - The GOV structure describes the composition of an MPEG-4 video stream, as regards the type of images (I-VOP's or P-VOP's) included in the stream, and their internal order. See also *GOV* and *VOP*.

Half-duplex - See *Full-duplex*.

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

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

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

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

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

Interlacing - Interlaced video is video captured at 50 pictures (known as fields) per second, of which every 2 consecutive fields (at half height) are then combined into 1 frame. Interlacing was developed many years ago for the analog TV world and is still used widely today. It provides good results when viewing motion in standard TV pictures, although there is always some degree of distortion in the image.

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

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

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

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

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

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

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

See also *IP (Internet Protocol)*.

I-VOP - See *VOP*.

IPv6 (Internet Protocol version 6) - A set of specifications designed as improvements to the current IP Version 4. Network hosts and intermediate nodes with either IPv4 or IPv6 can handle packets for either level of the Internet Protocol.

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

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

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

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

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

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

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

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

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

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

Megapixel - See *Pixel*.

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

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

MPEG-4 - MPEG-4 is a group of audio and video coding standards and related technology. The primary uses for the MPEG-4 standard are web (streaming media) and CD distribution, conversational (videophone), and broadcast television.

Most of the features included in MPEG-4 are left to individual developers to decide whether to implement them or not. This means that there are probably no complete implementations of the entire MPEG-4 set of standards. To deal with this, the standard includes the concept of "profiles" and "levels", allowing a specific set of capabilities to be defined in a manner appropriate for a subset of applications.

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

Multiplexer - A multiplexer is a high-speed switch that provides full-screen images from up to 16 analog cameras. Multiplexers can playback everything that happened on any one camera with no interference from the other cameras on the system.

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

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

OEM (Original Equipment Manufacturer) - This is a designation for companies that manufacture equipment which is then marketed and sold to other companies under their own names.

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

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

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

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

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

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

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

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

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

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

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

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

P-VOP - See *VOP*.

Quality of Service (QoS) - 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.

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

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

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

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

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

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

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

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

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

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

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

SMTP (Simple Mail Transfer Protocol) – SMTP is used for sending and receiving e-mail. However, as it is "simple," it is limited in its ability to queue messages at the receiving end, and is usually used with one of two other protocols, POP3 or IMAP. These other protocols allow the user to save messages in a server mailbox and download them periodically from the server.

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

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

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

SSL/TLS (Secure Socket Layer/Transport Layer Security)

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

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

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

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

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

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

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

TVL (TV Lines) – A method of defining resolutions in analog video.

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

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

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

USB – (Universal Serial Bus) A plug-and-play interface between a computer and peripheral devices, e.g. scanners, printers, etc.

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

VAPIX – AXIS VAPIX is considered to be the global application programming interface (API) standard, in the rapidly growing field of Network Video based on IP.

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

VOP (Video Object Plane) – A VOP is an image frame in an MPEG-4 video stream. There are several types of VOP:

- An I-VOP is complete image frame.

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

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

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

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

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

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

WINS (Windows Internet Naming Service) - Part of the Microsoft Windows NT Server, WINS manages the association of workstation names and locations with IP addresses, without the user or administrator having to be involved in each configuration change.

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

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

A
Accessing the video stream 12
ActiveX Controls 7
Administrator 13
Alarm 18, 27, 37
Alarm level 18
AMC viewer toolbar 9
ARP/Ping 31
Audio 6, 10
Audio input 18
Audio output 18
Auxiliary Power 37
AXIS Media Control 17

B
Backup 35
Bit Rate 16, 18
Buffers 26

C
Configuration 13
Control Button 6
Custom settings 20, 21

D
Date & Time 30
DNS Configuration 31
DNS Server 31, 32
Domain Name 32

E
Emergency recovery 39
Enable ARP/Ping 31
Event servers 25
Event types 25
Events 25
External video 23
External video source 9

F
Factory default settings 36
Firmware 39
Frame Rate 14
FTP Server 25
Full duplex 17
Full screen button 9

G
GOV Settings 16

H
Half duplex 17
Host Name 32
HTML examples 23
HTTP Server 25
HTTPS 30

I
I/O Ports 34
I/O Terminal Connector 6
Include Windows 27
Input 37
IP address filtering 29

L
LED indicators 6
Line in 5
Line out 6
Live View 13
Live View Config 20
Live View page 9
Logs & Reports 35

M
Maintenance 35, 36
Microphone 5
Motion Detection 37
Motion detection 28
Motion JPEG 12
MPEG-4 4
MPEG-4 recording 9
MPEG-4 Settings 16
Multicast 11

N
NAT traversal 32
Network connector 6
Network Settings 31
Noise canceller attenuation 19
Notification of IP address change 31
NTP Server 30

O
Output 37
Output buttons 9
Own home page 21
Own web files 21

P
Pinout - I/O connectors 37
Port status 28
Ports & Devices 34
Power Connector 6
Power over Ethernet 6
Pre/post trigger buffer 26
Pulse 9
Push to talk 17

Q
QoS 33
QuickTime 12

R
Real Player 12
Record button 9

Recovery 39
Restore 35

S
Scheduled event 27
Security 29
Sequence mode 9
Serial Number 6
Server Time 30
Services 31
Simplex 17
Snapshot button 9
SNMP 34
Support 35
System options 29
System Overview 35

T
TCP Server 25
TCP/IP Settings 31
Text overlay 15
Time Mode 30

U
Upgrade Server 35
Upgrading the firmware 39
Uploading web files 21
UPnP 32, 34
Users 29

V
Video Stream 11, 14