Setting up an IP-Surveillance system using Axis cameras and AXIS Camera Station software

March 20, 2007

TABLE OF CONTENTS

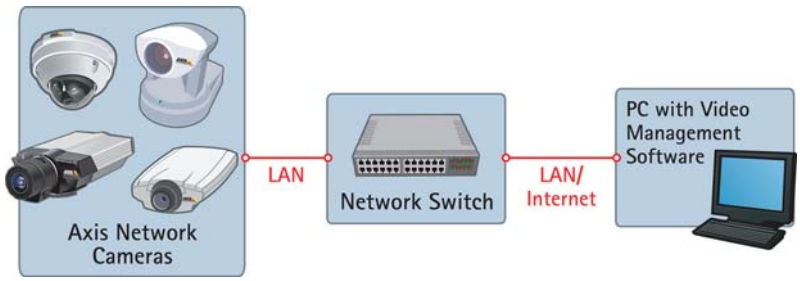
This document is a guide to setting up an IP-Surveillance system in a small- to medium-sized security installation. It provides an overview of network video's functionalities and benefits, and outlines considerations and recommendations for implementing such a system.

1 Introduction to an IP-Surveillance system

This chapter provides an overview of what is involved in an IP-Surveillance system, the benefits of network video, the importance of defining your surveillance application and legal considerations to take into account when setting up an IP-Surveillance system in your area.

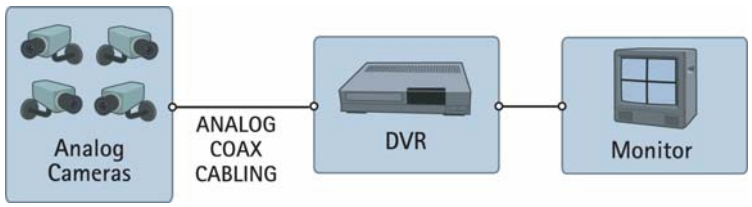
1.a What is IP-Surveillance?

IP-Surveillance is a term for a security system that gives users the ability to monitor and record video and/or audio over an IP (Internet Protocol-based) computer network such as a local area network (LAN) or the Internet. In a simple IP-Surveillance system, this involves the use of a network camera (or an analog camera with a video encoder/video server), a network switch, a PC for viewing, managing and storing video, and video management software. (A more detailed discussion of the components is provided in Chapter 2.)



An IP-Surveillance or network video system

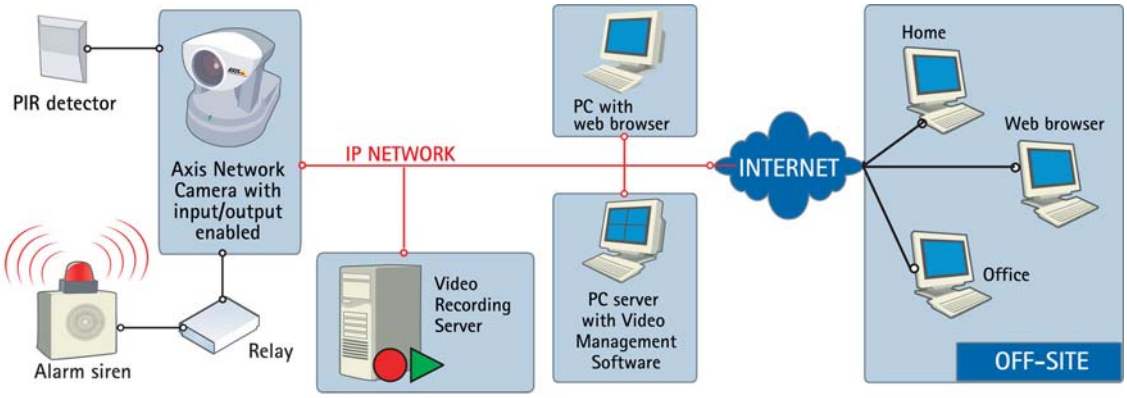
Unlike analog video systems that use dedicated point-to-point analog cabling from the camera location to the viewing/recording station, IP-Surveillance (or network video) uses the IP network technology as the backbone for transporting information. In an IP-Surveillance application, digitized video and/or audio streams can be sent to any location—even around the world, if desired—via a wired and/or wireless IP network, enabling video monitoring and recording from anywhere with network access.



An analog video system that incorporates a DVR (digital video recorder)

While an analog video system is for the most part a one-directional signal carrier that ends at the recording device, a network video system is bi-directional (allowing information to be sent and received) and can be an integrated part of a larger, scalable system. A network camera, for instance, can send video and audio to a user, as well as receive from the user audio and data instructions that could, for example, activate doors or external alarms. In addition, a network video system can communicate with

several applications in parallel and perform various tasks such as detecting motion or sending different streams of video. Such a system provides for greater performance possibilities and flexibility.



An IP-Surveillance or network video system with alarm integration

Because of the digital nature and method of video distribution, IP-Surveillance provides a host of benefits and advanced functionalities that gives you greater control and management of live and recorded video, as well as alarm events. This makes the system highly suited to security surveillance applications. The advantages include:

1) **Remote accessibility:** You can access live and recorded video at any time and from virtually any networked location in the world. Multiple, authorized users at different locations may be able to access live or recorded video. This is advantageous if your company wants a third-party, such as a security firm, to benefit from and have access to the video. In a traditional analog CCTV system, you need to be in a specific, on-site monitoring location to view and manage video, and off-site video access would not be possible without some additional equipment, such as a video encoder or a network DVR (digital video recorder).

2) **High image quality:** High image quality is essential in a security surveillance application. You want to be able to clearly capture an incident in progress and identify persons or objects involved. In a network video system, the quality of images produced can be more easily retained than in an analog surveillance system. With an analog video system, the captured images are degraded with every conversion that the images make between analog and digital formats and with the cabling distance. The further the analog video signals travel, the weaker they become. In a fully digital IP-Surveillance system, images from a network camera are digitized once and they stay digital with no unnecessary conversions and no image degradation due to distance traveled. In addition, digital images can be more easily stored and retrieved than is the case with the use of analog video tapes.

   A network camera using progressive scan technology is also better suited to depicting moving objects clearly because the whole image is presented at one time. With an analog video signal, two consecutive interlaced fields of lines are presented to form an image, and when objects move between the image capture of the two interlaced fields, blurriness results.

Progressive scan

Analog interlaced scan

A megapixel network camera (i.e. one that delivers an image comprised of 1 million or more pixels) can also offer resolutions greater than what an analog camera can offer, which means that more detail or larger areas can be covered.

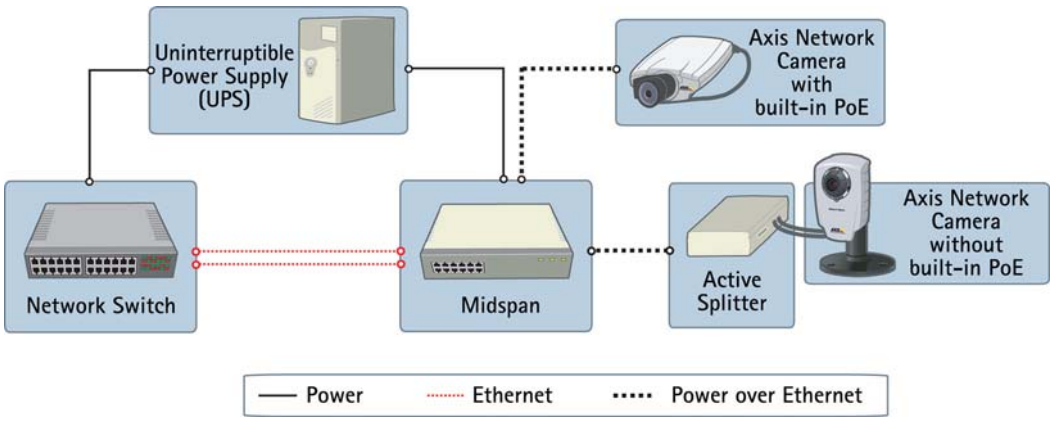
3) **Easy, future-proof integration:** Network video products based on open standards can be easily integrated with computer and Ethernet-based information, audio and security systems, video management and application software, and other digital devices. For instance, a network camera can be linked to specialized software programs that could, for example, integrate video with a Point of Sales system, or analyze the visual and/or audio data to detect wanted persons in a crowd or unauthorized access to specific areas.

Integration with Point of Sales system

4) **Scalable and flexible:** An IP-Surveillance system can grow with your needs. You can add as many network video products to the system as desired without significant or costly changes to the network infrastructure. You can place and network the products from virtually any location, and the system can be as open or as closed as you wish.

5) **Cost-effective:** An IP-Surveillance system has a lower total cost of ownership than a traditional analog CCTV surveillance. Management and equipment costs are lower since back-end applications and storage run on industry standard, open systems-based servers—not on proprietary hardware such as a DVR in the case of an analog CCTV system. Additional cost savings come from the infrastructure used. IP-based video streams can be routed around the world using a variety of interoperable infrastructure. IP-based networks such as LANs and the Internet, and various connection methods such as wireless are much less expensive alternatives than traditional coax and fiber needed for an analog CCTV system. In addition, an IP infrastructure can be leveraged for other applications across the organization.

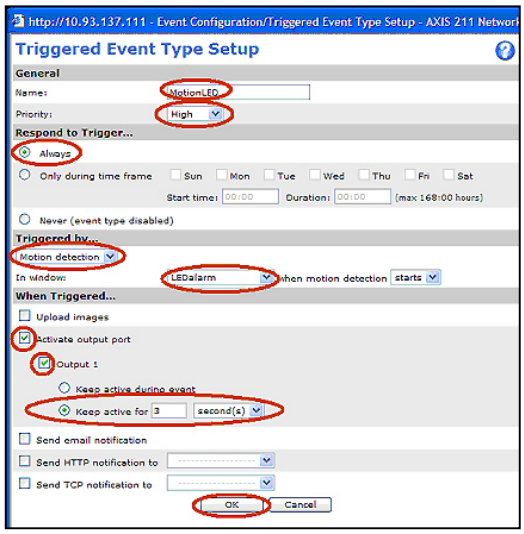
Furthermore, Power over Ethernet (PoE) technology, which cannot be applied in an analog video system, can be used in a network video system to increase savings and reliability.



PoE enables networked devices to receive power from a PoE-enabled switch or midspan through the same standard cable that transmits data and video. Hiring a certified electrician and installing a separate power line are not needed—a big advantage, particularly in difficult-to-reach areas. With PoE, network cameras will also be able to receive centralized backup power from a server room with an Uninterruptible Power Supply; so in the event of a power failure, the cameras will still be able to operate. (See diagram above.)

6) **Distributed intelligence or analytics:** There is often too much video recorded and lack of time to properly analyze them. Advanced network cameras with built-in intelligence or analytics take care of this by reducing the amount of uninteresting video recorded and enabling programmed responses.

Advanced network cameras have such features as built-in video motion detection, audio detection alarm, tampering detection, I/O connections, and alarm and event management functionalities. These features enable users to program and instruct the cameras on when to send video—and at what frame rate and resolution; when to activate external mechanisms such as alarms, lights and doors; when and how to alert operators; and where to send video for recording and storage—whether it be local and/or off-site for security purposes. The intelligent network camera is never idle. It is constantly on guard, analyzing inputs and waiting for an impulse to kick-start an action or series of actions.



Intelligent algorithms such as number plate recognition and people counting can also be integrated into a network camera unit. Intelligence at the camera level enables a more productive and effective means of surveillance than is possible with a centralized system. Network bandwidth usage and storage needs are reduced since only actionable information is sent over a network. In addition, less computing power is required from the recording server.

A security personnel's ability to protect people, property and assets can be enhanced by the flexibility and power of IP-Surveillance technology. IP-Surveillance systems have been installed in indoor/outdoor and private/public spaces; for example, in stores, homes, day care centers, schools, banks, government

offices, factories, warehouses, railway/subway stations and airports.

1.b Overview of an IP-Surveillance system

An IP-Surveillance system can be as simple or as sophisticated as your needs require. In a simple scenario, you have a PC, where you want to view and record video. You have an Ethernet cable between a PC and a network switch (which allows different devices to connect to each other and share, for instance, a common Internet connection) and a cable from the switch to the camera location. You then need equipment that can capture video and send a video stream over the network. This can be a network camera, or an analog camera connected to a video encoder/server.

A network camera or a video encoder connects directly to the network—not to a PC as is the case with a web camera. Once the network camera (or analog camera and video encoder) is installed and configured, you can view and record live video using a web browser on a local PC or a remote PC via the Internet. If you want to access and record video from many cameras simultaneously, it is advisable to install a video management software on the recording PC.

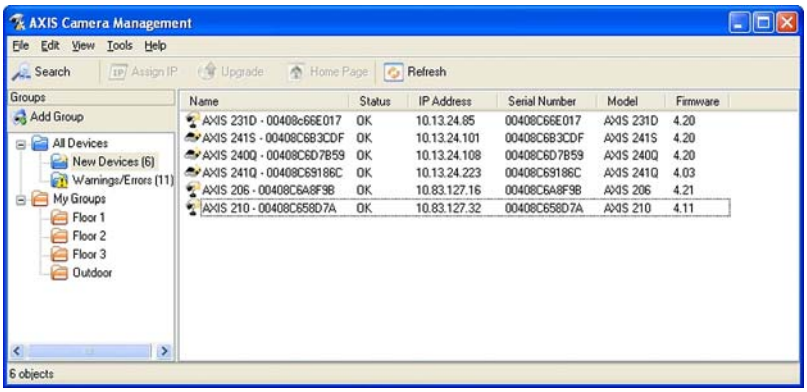
As mentioned earlier, an IP-Surveillance system is easy and cost-effective to scale up. It is also flexible, and each component of the system can be customized to your needs. The following is a brief overview of the components that can be tailored to your application:

a) Network camera/video encoder: A wide variety of network cameras and video encoders are available. Network cameras range from fixed cameras to pan/tilt/zoom and dome cameras, and may be designed for use indoors or outdoors. Both network cameras and video encoders may offer a variety of features such as: 1) different video compression methods (e.g. Motion JPEG and MPEG-4) delivered separately or simultaneously to optimize bandwidth and image quality; 2) input/output ports for connection to external devices such as sensors and alarms; 3) built-in intelligence such as video motion detection; 4) sophisticated alarm and event management functions that can communicate with different devices and applications simultaneously, and can send separate video streams in different resolutions, at different frame rates and to different places; and 5) comprehensive security features.

b) Network: There are many ways to design and secure a network for IP-Surveillance. In addition, a network can be as small or as extensive as your requirements, and it can be wired, wireless or a combination of both. It is also easy to increase the bandwidth capacity of your network simply by adding switches/routers. And different technologies can be used to optimize bandwidth usage. Furthermore, a wired network can deliver not only data, but also power, to indoor network cameras using Power over Ethernet technology. This simplifies installation and provides cost savings.

c) Hardware (server and storage): The hardware requirements of an IP-Surveillance system are not complex. Simply use standard components found in the IT industry. Today's PC, with a Pentium processor and Windows operating system, is able to run a video management software, and record and store video from up to 25 cameras. If the hard disk on the actual server running the recording application is not enough, there are solutions that enable you to increase storage space and achieve increased flexibility and recoverability. As larger hard drives are produced at lower costs, it is becoming less expensive to store large amounts of video.

d) Software: A wide range of software is available to help you in the preparation, installation and management of an IP-Surveillance system. For example, you can use the AXIS Design Tool, which helps you estimate how much bandwidth your network video system will require, and installation software such as the AXIS Camera Management (free download), which makes it easier for you to find, install and configure the video products on the network. A video management software is also recommended. It will allow you to, among other things, centrally manage and configure the network video products to your viewing, recording and security preferences.

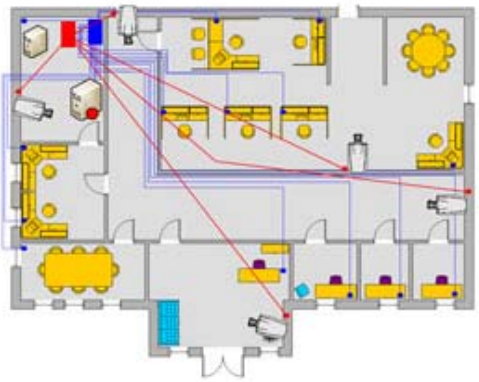


AXIS Camera Management software

A more detailed discussion of the components and the considerations to make when selecting equipment is provided in Chapter 2.

1.c Defining your surveillance application

The first and most important step in implementing a video surveillance installation is determining the goal of your surveillance application. It is a good idea to map out where you want video surveillance to take place and for what purpose (i.e. surveillance overview, identification, people counting). This will determine the type and number of network cameras, as well as other components to install and can influence the overall cost of the installation. More information about how to select a network camera and other components is covered in Chapter 2.



1.d Legal considerations

Video surveillance can be restricted or prohibited by laws that vary from country to country. It is advisable to check the laws in your local region before installing a video surveillance system.

There may be legislation or guidelines covering the following:

a) License. You may need to register or get a license from an authority to conduct video surveillance, particularly in public areas.

b) Purpose of the surveillance equipment. Is it in accordance with what is permitted by the laws in your area?

c) Position or location of the equipment. Is it positioned or located in such a way that it only monitors the spaces which the equipment is intended to cover, and if unintended areas are covered, would you have to consult with the owners of such spaces? There may be rules covering areas where video surveillance is prohibited; for example, toilets and changing rooms in a retail environment.

d) Notification. You may have to place signs to warn the public that they are entering a zone covered by surveillance equipment and there may be rules regarding the signage.

e) Quality of images. There may be rules regarding the quality of images, which can affect what may be permitted or acceptable for use as evidence in court.

f) Video format. Police authorities may require that the video format be ones that they can handle.

g) Information provided in recorded video. Video recordings, for instance, may be required to have time and date stamped.

h) Processing of images. There may be rules regulating how long images should be retained, who can view such images and where recorded images can be viewed. You may have to keep an audit log.

i) There may be requirements for drawings of where cameras are placed.

j) Personnel training. There may be regulations that require operators to be trained in security and disclosure policies, as well as privacy issues.

k) Access to and disclosure of images to third parties. There may be restrictions on who can access the images and how images can be shown. For example, if video is to be disclosed to the media, images of individuals may have to be disguised or blurred.

l) Recording of sound. A permit may be required for recording sound in addition to video.

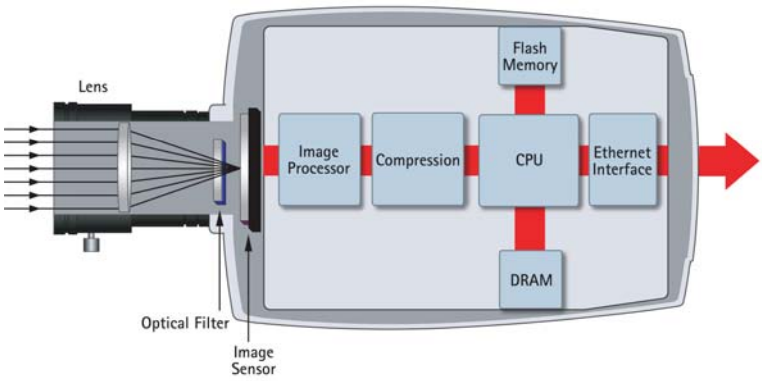
m) Regular system checks. There may be guidelines on how often and thorough a company should perform system checks to make sure all equipment are operating as they should.

2 Component considerations

This chapter describes the major components of an IP-Surveillance system, and provides guidelines for selecting equipment. The components covered in this chapter include network camera, video encoder/server, network switch, server hardware and video management software.

2.a Network camera

A network camera can be described as a camera and computer combined in one unit. It has a compression chip, an operating system, a built-in web server, FTP (File Transfer Protocol) server, FTP client, e-mail client, alarm management and much more. A network camera, unlike a web camera, does not need to be attached to a PC; it operates independently and connects, as with a PC, directly to an IP network. It can be placed wherever there is a network connection. The network camera captures and sends live images, enabling authorized users to locally or remotely view, store and manage video over a standard IP-based network infrastructure.



Inside an Axis network camera

Back of an Axis network camera

All types of network cameras are available today, and no matter what your needs are, there is a network camera available to meet them. Although analog cameras are available in a similar variety, network cameras can now offer more benefits, including better image quality and greater installation flexibility. For some special applications, such as very high image resolution or wireless needs, network cameras are the only option.

The following sections provide an overview of the types of network cameras available, the network camera features to consider and how to select a network camera.

a) Types of network cameras:

Network cameras fall into categories and types. They are:

- **Category: Indoor or outdoor**. Outdoor network cameras must have an auto iris to regulate how much light is received. Many outdoor cameras require a protective housing. Others may already be designed with a protective enclosure. Housings are also available for indoor cameras that require protection from harsh environments such as dust and humidity, and from vandalism or tampering.

- **Types: Fixed, pan/tilt/zoom, or dome**

Fixed cameras: Once a fixed camera is mounted, the camera's viewing angle is fixed. There are two types of fixed network cameras available:

The first is the traditional camera (with a body and lens) that clearly shows the direction the camera is pointing at and is ideal in situations where you want to the camera to be visible. Many cameras of this kind enable exchangeable lenses.

The second type is a fixed network dome camera, which is a fixed camera installed in a small dome housing. The design, as well as the fact that it is difficult to see where the camera is pointing, makes it ideal for discreet installations. This type of camera offers limited ability for changing lenses. Mounting of fixed cameras is usually on a wall.

Pan/tilt/zoom (PTZ): The camera's view can be remotely controlled, either manually or automatically, for panning from side to side, tilting up and down, and zooming in and out of an area or object. There are now mechanical as well as non-mechanical pan/tilt/zoom cameras:

In a mechanical PTZ camera, the direction of the camera's viewing angle is visible. Most PTZ cameras do not have full 360-degree pan and are not made for continuous automatic operations. Mounting is on a ceiling or wall.

In a non-mechanical PTZ camera, a megapixel sensor is used to enable the camera to have a viewing angle of 140 degrees to 360 degrees. The operator can select to pan, tilt and zoom the camera in any direction without involving any mechanical movement. It also offers immediate movement to a new position, which in a traditional PTZ camera can take up to 1 second. The advantages of such a camera include: no wear and tear since there are no moving parts, the viewing angle is not visible and it is ideal for discreet installations. To ensure a good image quality, pan and tilt should be limited to 140 degrees and zoom to 3x in camera with a 3 megapixel sensor. Mounting is on a wall.

Dome: Dome cameras can cover a wide area by enabling greater flexibility in pan, tilt and zoom functions, with a 360-degree pan and a tilt of usually 180 degrees. Dome cameras are ideal for use in discreet installations due to their design, mounting (particularly in drop-ceiling mounts as seen in the picture at right), and difficulty in seeing the camera's angle (dome coverings can be clear or smoked). A network dome camera also provides mechanical robustness for continuous operation in guard tour mode, where the camera continuously moves between presets. Mounting is usually on a ceiling.

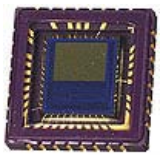
b) Feature considerations:

- **Image sensor**: Two types of image sensor technologies are available for use in network cameras: CCD (charge-coupled device) and CMOS (complementary metal-oxide semiconductor). Each has its own advantages.

  CCD sensors have been used in cameras for more than 20 years and present many advantageous qualities; among them, better light sensitivity than CMOS sensors. This higher light sensitivity translates into better images in low light conditions.

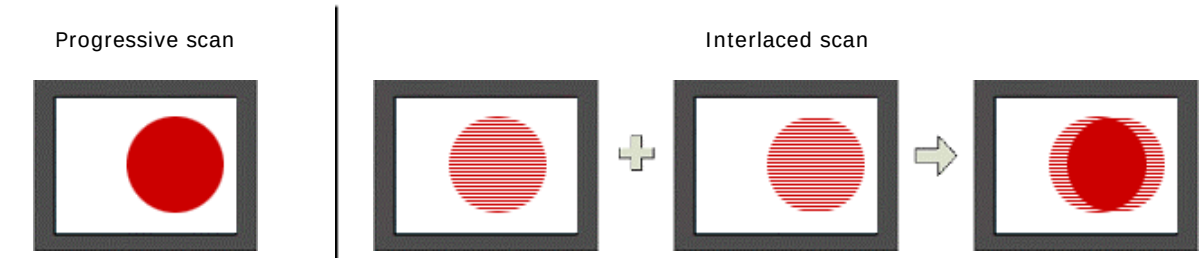
CCD

  Recent advances in CMOS sensors bring them closer to their CCD counterparts in terms of image quality. CMOS sensors lower the total cost for cameras since they contain all the logics needed to build cameras around them. They make it possible for manufacturers to produce smaller-sized cameras. Megapixel CMOS sensors are also available, enabling network cameras to provide megapixel resolution.



CMOS

- **Progressive scan**: This technology, present in advanced network cameras, enables moving objects to be seen more clearly since it involves exposing, capturing and presenting an entire image at one time, rather than splitting an image into two separate fields, as with analog interlaced scanning technology. With interlaced technology, an image is formed when two consecutive interlaced fields of lines are presented. When objects move between the image capture of the two interlaced fields, blurriness results.



- **Automatic day/night functionality**: This feature is incorporated into some outdoor cameras and enables the automatic removal of the infrared (IR) cut filter that is incorporated into all color cameras. When there is light, the camera delivers color video. In dark conditions, the camera makes use of invisible, infrared light present in all objects to capture images and deliver infrared-sensitive black and white video. Infrared or day/night cameras are particularly useful in outdoor environments or situations that restrict the use of artificial light. These situations include discreet and covert surveillance applications.

- **Lens**: Different types of lens are available on network cameras. Lenses may be *fixed* (the focal length or horizontal field of view is fixed), *varifocal* (allows for the manual adjustment of the focal length) or *zoom* (allows the camera to stay in focus when zooming in on objects). Varifocal and zoom lenses offer focal lengths that range from telephoto to wide angle. A lens' iris, which controls the amount of light coming into the camera, can be manually adjusted (for indoor cameras) or automatically controlled (for outdoor cameras). An auto iris lens can be controlled by the camera's processor (DC-controlled), or by video signal.

Varifocal lens


Fixed lens

- **Lens changeable**: Changeable lens gives users the option of using other lenses (such as telephoto or wide angle) that may be more appropriate for a particular application. You will need to know if the camera's original lens is C-mount or CS-mount so that the new lens you purchase fits the same type of mount. Today, almost all surveillance cameras and lenses sold are CS-mount types.

  When choosing the size of a new lens, you will also need to know the size of the image sensor. If a lens is made for a smaller sensor than the one actually fitted inside the camera, you will have black corners in the image. If a lens is made for a larger sensor than the one fitted inside the camera, the angle of view will be smaller than the default angle of the lens since part of the information will be "lost" outside of the sensor.

- **Minimum illumination / light sensitivity**: Network cameras come with lux specifications. Lux is the measurement unit for light. One lux is the equivalent of light from a candle. At least 200 lux is needed to capture good quality images. A high-quality camera might be specified to work down to 1 lux but this does not mean that you will get a good image at 1 lux. Different manufacturers also use different references when they specify the light sensitivity of a camera, so it is important to look at captured images to make a comparison.

Environment: lux

- Strong sunlight: 100,000
- Full daylight: 10,000
- Normal office light: 500
- Poorly lit room: 100

- **Type of video compression**: Two of the most common types of video compressions are MPEG-4 and Motion JPEG. MPEG-4 and Motion JPEG each employ a different technique to reduce the amount of data transferred and stored in a network video system. Each format has its advantages and disadvantages.

  MPEG-4 transmits only parts of an image that differ from an earlier referenced image. At high frame rates and particularly with scenes that have static areas, MPEG-4 requires less bandwidth and storage than with Motion JPEG. MPEG-4 is a licensed technology, so if a network camera supports MPEG-4, be sure to find out if the MPEG-4 license fee is already included in the product's purchase price. MPEG-4 provides support for synchronized audio, whereas Motion JPEG does not.

MPEG-4 image sequence

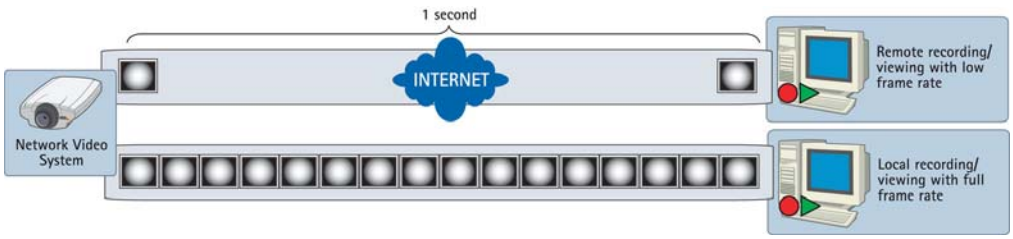
Motion JPEG image sequence

With Motion JPEG, each image is a complete JPEG compressed image and is simple to encode and decode. One of the advantages of Motion JPEG is that it guarantees the image quality that you set (either high or low) regardless of movement or image complexity. Motion JPEG has low latency and is license free. However, Motion JPEG files are usually larger than those compressed with the MPEG-4 standard.

When looking at video compression, it is important to select the compression that best suits your application. One of the best ways to maximize the benefits of both standards is to look for network video products that can deliver simultaneous MPEG-4 and Motion JPEG streams. Axis network video products, for example, provide the two video compression formats, giving users the flexibility to both maximize image quality for recording and reduce bandwidth needs for live viewing. With limited bandwidth, you may want to view at full frame rate or 30/25 (NTSC/PAL) frames per second (fps) with MPEG-4 and record with guaranteed quality using Motion JPEG.

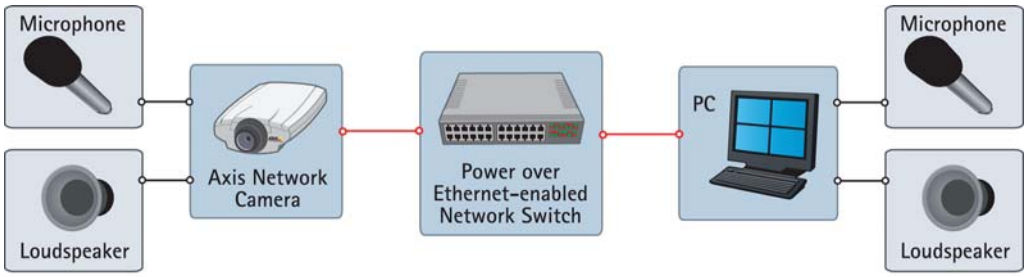
- **Video resolution**: A VGA resolution is 640x480 pixels. (Computer screens have resolutions in VGA or multiples of VGA.) Another common format is 4CIF (704x480 pixels in NTSC / 704x576 pixels in PAL standard). Megapixel cameras provide high resolutions of at least 1280x960 pixels and are used for applications that require the ability to see fine details or cover a large area. A network camera's ability to deliver a specified number of frames per second may vary depending on the resolution.

- **Frames per second**: There may be different frame rates specified for different resolutions. Full-motion video is 30 frames per second in NTSC video standard (in North America/Japan) and 25 frames per second in PAL video standard (Europe). Full frame rate on all cameras at all times is more than what is required for most applications. With the configuration capabilities and built-in intelligence of network cameras, frame rates under normal conditions can be set lower, e.g. one to three frames per second, to dramatically decrease storage requirements. In the event of an alarm, i.e. if video motion detection or an external sensor is triggered, the recording frame rate can be automatically increased. It is also possible to send video with different frame rates to different recipients. (See diagram below.)



- **Video motion detection**: Video motion detection monitors changes in the camera's field of view and if a change occurs (e.g. an intruder enters the scene), an alarm condition is generated. This function can be a built-in feature of a network camera or a feature of a video management software. Using the built-in video motion detection feature in a network camera reduces bandwidth use since no video is delivered on the network unless video motion is detected.

- **Audio support**: A network camera with audio support comes either with a built-in microphone or an input for an external microphone. Speakers may be built in or external. An audio feature enables users to remotely listen in on an area and communicate instructions, orders or requests to visitors or intruders. Audio can also be used as an independent detection method. When sound above a certain level is detected, video recordings and alarms can be triggered.



  Audio modes may be simplex (audio is sent either by the operator or the camera) or duplex (audio is sent to and from the operator simultaneously). Audio can be compressed and integrated into the video stream, and sent over a network for monitoring and/or recording. There are many audio compression formats. The higher the compression level, the more latency is introduced. If synchronized audio and video is a priority, the preferred compression standard is MPEG.

- **Input and output (I/O) ports**: Input/output connectors enable external devices to be connected to a network camera. Inputs to a camera (e.g. a door contact, infrared motion detector, glass break sensor or shock sensor) enable the camera to react to an external event by, for example, initiating the sending and recording of video. Outputs enable the camera to control external devices such as activating alarms, triggering door locks, generating smoke or turning on lights.

  I/Os also allow you to save storage space. For example, if you want to simply capture the identity of a person at an entrance, you do not need the camera to continually send video. You can set up the system in such a way that the camera is triggered to capture and send the necessary image frames only when the door opens.

- **Alarm and event management**: Pre- and post-alarm image buffers within a network camera can save and send images collected before and after an alarm occurs. Once an alarm or event is detected, a network camera can send notifications via e-mail, TCP, HTTP and upload of images via e-mail, FTP and HTTP.

- **Security and management**: At a basic level, a video surveillance network camera should provide different levels of password-protected access to a network camera. For instance, some authorized users may only have access to view images from specific cameras; others have operator-level access, and a few have access to administer all settings in a network camera.

Beyond multi-level password protection, a network camera may offer HTTPS encryption for secure communication; IP address filtering, which allows you to define the IP addresses that have access rights to the camera, as well as the IP addresses that the camera is allowed to send video to; and IEEE802.1X for port-based authentication.

- **Power over Ethernet (PoE)** (IEEE 802.3af): When a network camera supports this feature, it means that the camera can receive power through the same cable as for data. It reduces cabling requirements and installation costs.

- **Internet Protocol version 6 (IPv6)**: Some video encoders may offer support for IPv6 addresses in addition to IPv4 addresses as insurance against the growing shortage of IPv4 addresses.

- **Other specialized features:** Network cameras may be specially designed to be tamper or vandal resistant. These kinds of cameras are useful in areas where they may be vandalized.

  For some network dome cameras, a specialized feature may be the ability to use a joystick for pan/tilt/zoom control.

c) How to select a network camera:

1) **Define the scene and application needs.** To determine the type of network cameras required, as well as the number of cameras needed to adequately cover an area, you first need to determine the scene or environment and the goal of the surveillance application.

   Consider:

   a) Environment: This will determine whether you need an outdoor or indoor camera, whether the camera needs to be tamper or vandal proof, and whether special housing is required. Consider also the lighting requirements: Is there adequate light to obtain a good quality image? Do you need to add light sources? How light sensitive should the camera be?

   b) Area of coverage: A PTZ or dome camera is able to cover a wider area than a fixed network camera. The bigger the area, the more cameras are needed.

   c) Application: Determine the kind of surveillance you want to conduct (overt/covert—this will help you in selecting cameras that offer a non-discreet or discreet installation). Determine also the kind of image you want to capture: overview or close-up for identification purposes.

      The purpose will determine the placement of the camera, the type of camera and camera features required (e.g. progressive scan, megapixel for exceptional details, audio, security features) and lens

Overview

Close-up

adjustment/type (normal, telephoto or wide angle).

A security operator using a PTZ or dome camera can cover a large area and capture different images for different purposes. In many cases, different cameras will be needed to capture images for different purposes (i.e. one camera providing a full overview image for capturing an incident in action, and another camera for close-up views of a person/object for identification purposes).

d) Viewing and recording needs: Determine when and how often you need to view and record: day, night and/or weekends? This will determine the features you need to consider; i.e. frame rate capabilities, type of video compression (e.g. MPEG-4 for live viewing and Motion JPEG for recording), bandwidth saving features such as video motion detection, and alarm management functions.

2) **Image quality.** Not all network cameras are created equal. A key determinant of a network camera is image quality. When assessing image quality, be sure to consider a network camera's light sensitivity, the crispness of moving objects and the level of clarity. Read through a camera's datasheet and, most importantly, field test a few cameras before making a decision.

3) **Compatibility with a range of software.** Find out if the network camera is able to work with an extensive range of video management software. A network camera with an open, application programming interface enables a large variety of software vendors to write programs for the cameras. This will increase your choices in software applications and will ensure that you are not tied to a single vendor. Your choice of network camera should never limit vendor options and functionalities.

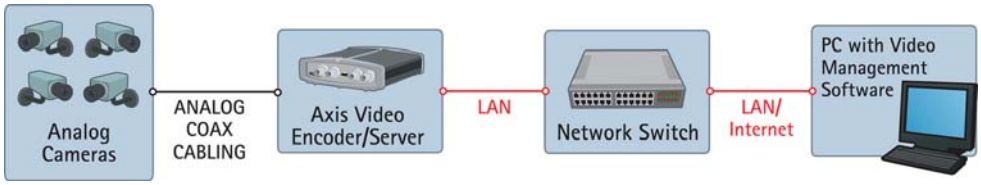
4) **Select a vendor that will be a long-term partner.** Does the company have a large installed base of cameras, focuses on network camera technology and offers you local representation and support? As your needs change and grow, you want to choose a camera from a vendor where the innovation, support, upgrades and product path will be there for the long term.

Axis offers the widest range of network cameras on the market. They include indoor/outdoor, day/night, and fixed, pan/tilt/zoom, and dome cameras. In addition to network cameras, Axis also offers video encoders, network digital video recorders and video management software. A wide range of accessories are also available: protective housings, IR illuminators, Power over Ethernet midspans and active splitter, connectors and cables, lenses and lens accessories, power accessories, as well as third-party accessories.

Before you set out to order or buy many network cameras, it is a good idea to buy one and test its quality. Try out an Axis network camera with a free AXIS Camera Station video management software, which is packaged with every network camera purchase and is also downloadable on Axis' web site at (www.axis.com). AXIS Camera Station One provides simultaneous viewing and recording of high-quality MPEG-4 and Motion JPEG video from a single surveillance camera.

2.b Video encoder/server

If you already have existing analog CCTV surveillance cameras and want to move to an IP-based surveillance system, you can still make use of your analog investments by adding a video encoder/server. Simply connect a video encoder to analog cameras. The encoder converts analog signals into digital video and sends them over an IP network, enabling users to remotely monitor the cameras, as well as record and store video on standard PC servers. A video encoder brings new functionality to analog equipment and eliminates the need for dedicated equipment such as coaxial cabling, analog monitors and digital video recorders.



The video encoder/server migrates the analog cameras into an IP-based video solution

Front and back image of an Axis video encoder

A video encoder typically provides between one and four connections to analog cameras, as well as an Ethernet port to connect to the network. Like network cameras, it contains a built-in web server, a compression chip, an operating system and processing power for local intelligence. Besides digitizing analog signals, a video encoder can support a host of other functions: for example, digital inputs and outputs (I/O, which can trigger the encoder to start sending images or to activate alarms and devices such as lights and doors), audio, and serial port(s) for serial data or control of pan/tilt/zoom cameras and devices. With image buffering, a video encoder can also send pre- and post-alarm images.

A video encoder can be connected to a wide variety of specialized cameras, such as a highly sensitive black and white camera, a miniature or a microscope camera, in addition to fixed, dome, indoor, outdoor and pan/tilt/zoom analog cameras.

In a system involving many analog cameras, a video encoder rack together with “blades” (video encoders without their casings) can be used. Placing blade video encoders in racks allows them to be managed centrally with a common power supply and in some cases, a common Ethernet cable. One standard 19-inch rack can digitize up to 48 analog cameras.

19-inch video encoder rack

With analog cameras where coaxial cables have not been pulled to a central location, it is best to use stand-alone video encoders positioned close to each camera. This method reduces installation costs since it can take advantage of existing network cabling to transmit video, instead of running coaxial cables to a central location. It also eliminates the loss in image quality that would occur if video were to be transferred over long distances through coaxial cabling. A video encoder produces digital images, so there is no reduction in image quality due to the distance traveled.

Considerations to make when selecting a video encoder:
(See also guidance provided in the previous section under network cameras.)

- Image quality: Can the video encoder provide high-quality, deinterlaced digital video? The deinterlace filter eliminates the artifacts (a series of horizontal lines) caused by analog interlaced scanning technology.

- Resolution: What are the resolutions needed?

- Frame rate and compression: Do you require the ability to view and/or record at full frame rate? Do you require compression with Motion JPEG and/or MPEG-4?

- Ease of installation, management and upgradeability.

- Ease of integration: Can it integrate with different types of analog cameras, for example, pan/tilt/zoom cameras?

- With a rack solution: How many analog channels can the rack handle? How many channels with full frame rate and full resolution can the system provide?

- Alarm management features: Do you require I/Os, video motion detection, image upload, scheduled and triggered event functionality with alarm notification?

- Reliability: How reliable is the video encoder/rack solution? When connecting to multiple analog CCTV cameras, it is crucial that the video encoder/rack solution can be relied upon.

- Security: What are the available security features? Security features may include multiple user access levels; HTTPS encryption, which provides a secure channel between the video encoder and application; IEEE 802.1X, which allows a network to be secured with port-based authentication; and IP address filtering.

- Quality of Service (QoS): Does the video encoder support Quality of Service? QoS helps secure the necessary bandwidth for streaming video and control commands over a network.

- Software: Is the video encoder supported by a range of application software?

- Future proof: Some video encoders may offer support for IPv6 (Internet Protocol version 6) addresses in addition to IPv4 addresses as insurance against the growing shortage of IPv4 addresses.

2.c Network

The next consideration to make is assessing your network needs.

Network switches allow devices such as network cameras, servers and PCs to communicate with each other to share information and, in some cases, a common Internet connection. Network designs can take many forms and may vary in terms of performance and security.

First, determine what your company is using the network for and how congested your local area network (LAN) or wide area network (WAN) is.

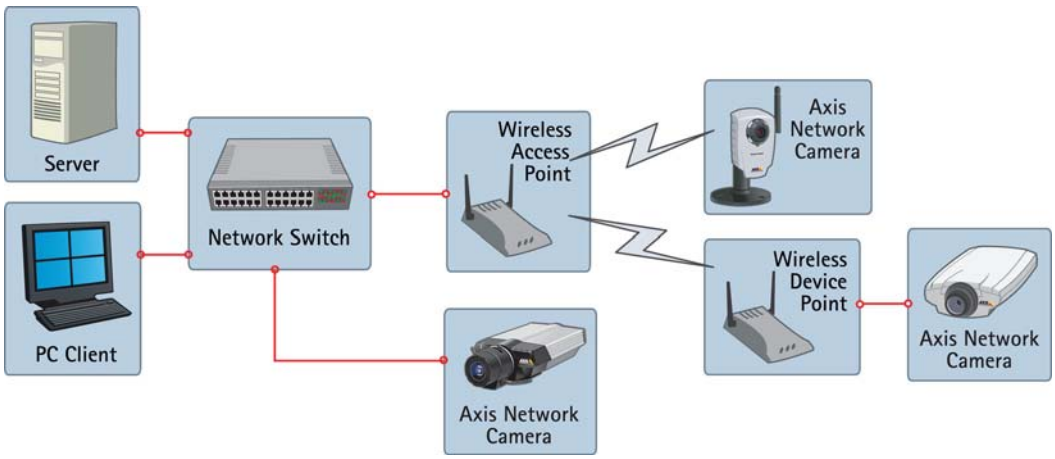
If you are implementing a smaller surveillance system involving 8 to 10 cameras, you should be able to use a basic 100-megabit (Mbit) network switch without having to consider bandwidth limitations. Most companies can implement a surveillance system of this size using their existing network.

If you are implementing 10 cameras or more, you should try to estimate the load on the network using a few rules of thumb:

- A camera will use approx. 2 to 3 megabits of bandwidth when configured to deliver high-quality images at a high frame rate.

- With more than 12 to 15 cameras, you should consider using a switch with a gigabit (Gbit) backbone. If a gigabit-supporting switch is used, the server running the video management software should have a gigabit network adapter installed.

Determine the pattern of congestion levels over a given period to find out if you have to install additional bandwidth capacity on your network or whether you can make use of the same network as for general business activities. It may be that the network traffic drops off during nighttime and weekends—the times when you may want to activate the surveillance system. The usage pattern will help you to determine whether you can a) simply use the same network infrastructure for your general purpose needs as for your surveillance needs, or b) use a combination of existing general purpose network as well as a new network for IP-Surveillance. If additional network capacity is needed, new cabling is normally not needed since adding a switch or reconfiguring the patch panel may solve the problem. One tool that helps estimate bandwidth usage is the AXIS Design Tool, which is available at http://www.axis.com/products/video/design_tool/. See also section 5.d for more about bandwidth control.



Network including both wired and wireless connections

Wireless networks

When running a cable between a LAN and a network camera is impractical, difficult or expensive, a wireless solution using a wireless access point—also called a device bridge or wireless router—is a good option. Wireless technology can be useful, for example, in historic buildings where the installation of cables would damage the interior; within facilities where there is a need to move cameras to new locations on a regular basis, such as in a supermarket; or in outdoor installations. Wireless technology can also be used to bridge sites without expensive ground cabling.

Security in wireless networks

Securing a wireless network should be addressed. Otherwise, everyone with a wireless device present within the area covered by the network will be able to participate in the network and use shared services. The most commonly used standard today is WEP (Wireless Equivalent Privacy), which adds RSA RC4-based encryption to the communication, and prevents people without the correct key from accessing the network. But as the key itself is not encrypted, it is possible to 'pick the lock,' so this should be seen only as a basic level of security. A new standard, the WPA (WiFi Protected Access), significantly increases security by taking care of some of the shortcomings in the WEP standard with, for instance, the addition of an encrypted key.

When using wireless cameras for surveillance, there are a few rules of thumb:

- Enable the user/password login in the cameras
- Enable the encryption in the wireless router/cameras
- Since wireless routers do not have the same bandwidth capacity as a normal switch, no more than four to five cameras should be connected to a wireless access point.

2.d Hardware (storage needs)

Similar to the way a PC can "save" documents and other files, video can be stored on a server or PC hard disk. Specialized equipment is not needed because a storage solution does not differentiate video data—it is viewed as any other large group of files that is stored, accessed and eventually deleted. However, video storage puts new strains on storage hardware because it may be required to operate on a continual basis, as opposed to during normal business hours with other types of files. In addition, video by nature generates very large amounts of data, creating high demands on the storage solution.

Calculating the storage needs

In order to appropriately calculate the storage requirements of a network surveillance system, there are a number of elements to factor in, such as the number of cameras required in your installation, the number of hours a day each camera will be recording, how long the data will be stored, and whether the system uses motion detection or continuous recording. Additional parameters such as frame rate, compression, image quality and complexity should also be considered.

The type of video compression employed also effects storage calculations. Systems employing Motion JPEG compression vary storage requirements by changing the frame rate, resolution and compression. If MPEG compression is used, then bit rate is the key factor determining the corresponding storage requirements.

Fortunately, there are formulas for calculating the amount of storage to buy. These formulas are different for Motion JPEG and MPEG-4 compressions because Motion JPEG consists of one individual file for each image, while MPEG-4 is a stream of data, measured in bits per second. The formulas are as follows:

Motion JPEG calculation:

Image size x frames per second x 3600s = Kilobyte (KB) per hour/1000 = Megabyte (MB) per hour

MB per hour x hours of operation per day / 1000 = Gigabyte (GB) per day

GB per day x requested period of storage = Storage need

Camera	Resolution	Image size (KB)	Frames per second	MB/hour	Hours of operation	GB/day
No.1	CIF	13	5	234	8	1.9
No.2	CIF	13	15	702	8	5.6
No.3	4CIF	40	15	2160	12	26

Total for the 3 cameras and 30 days of storage = 1002 GB

MPEG-4 calculation:

Bit rate / 8(bits in a byte) x 3600s = KB per hour / 1000 = MB per hour

MB per hour x hours of operation per day / 1000 = GB per day

GB per day x requested period of storage = Storage need

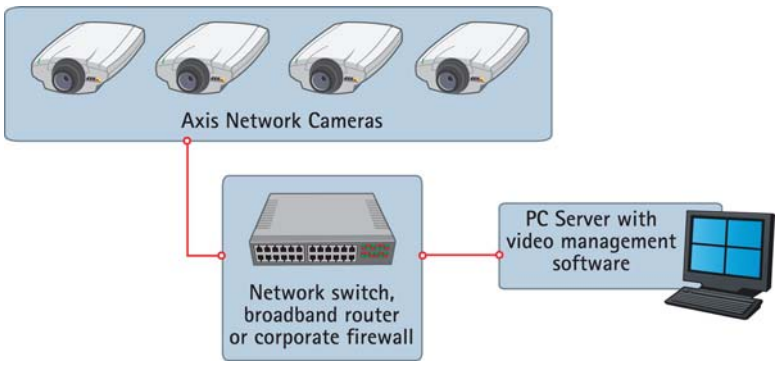
(Note: The formula does not take into account the complexity of the image, which is an important factor that can influence the size of storage required.)

Camera	Resolution	Bit Rate (Kbit/s)	Frames per second	MB/hour	Hours of operation	GB/day
No.1	CIF	170	5	76.5	8	0.6
No.2	CIF	400	15	180	8	1.4
No.3	4CIF	880	15	396	12	5

Total for the 3 cameras and 30 days of storage = 204 GB

Storage Options

Storage solutions depend on a PC's or server's ability to store data. As larger hard drives are produced at lower costs, it is becoming less expensive to store video. There are two ways to approach hard disk storage. One is to have the storage attached to the actual server running the application, called a direct attached storage. The other is a storage solution where the storage is separate from the server running the application, called a network-attached storage (NAS) or a storage area network (SAN).



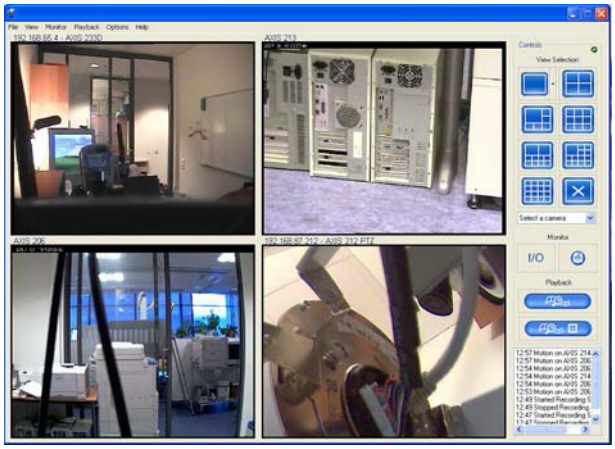
Direct attached storage

Direct attached storage is probably the most common solution for hard disk storage in small to medium-sized IP-Surveillance installations (See image above). The hard disk is located in the same PC server that runs the video management software. The PC and the number of hard disks it can hold determine the amount of storage space available. Most standard PCs can hold between two and four hard disks. With today's technology, each disk can store approximately 300 gigabytes of information for a total capacity of approximately 1.2 terabytes (one thousand gigabytes).

For information about NAS and SAN, please see Chapter 8.

2.e Video management software

Video management software is an important component of an IP-Surveillance system because it effectively manages video for live monitoring and recording. Video management requirements differ depending on the number of cameras, performance requirements, platform preferences, scalability, and the ability to integrate with other systems. Solutions typically range from single PC systems to advanced client/server-based software that provides support for multiple, simultaneous users and thousands of cameras.



There are common features in almost every video management software, no matter the type or size:

- **Simultaneous viewing and recording of live video from multiple cameras:** Video management enables multiple users to view several different cameras at the same time, and allow recordings to take place simultaneously. Video management software can also increase the resolution for cameras with activity or alarms. The system can be utilized for different purposes and even different departments (e.g. a store's IP-Surveillance system can be used by one individual for security purposes, while another uses it for studying store traffic).

- **Several recording modes:** Continuous, on alarm and/or video motion detection, and scheduled (which can combine continuous and on alarm recording instructions). Video motion detection defines activity by analyzing data and differences in a series of images. Video motion detection can be performed at the camera level, which is preferred, or reside in the software. The software can provide the motion detection functionality to network cameras or video encoders that do not have this feature built in.

- **Alarm management functions:** For example, parameters can be established so that alarms are not sent during hours of normal activity, such as from 8 a.m. to 9 p.m., Monday through Friday. Therefore, if motion is detected at 3 a.m. on a Saturday, the system knows that this activity is not normal, and can send e-mails or text messages to alert the proper authorities.

- **Frame rate control:** Video management enables users to set the recording frame rate of selected cameras, and pre-determine that if activity is detected, the recording frame rate would increase, and if there is no motion, the rate would decrease.

- **Camera management:** Video management systems allow users to administer and manage cameras from a single interface. This is useful for tasks such as detecting cameras on the network, managing IP addresses, and setting resolution, compression and security levels. Cameras are often located in distant or hard-to-reach locations, making it impractical for the administrator to visit every location and individually upgrade every camera. Video management systems provide access to every camera on the network and will automatically administer firmware upgrades.

Some video management software may also include full duplex, real-time audio support, as well as analytical tools that improve image details or provide helpful information to users. Programs with image enhancers, for example, can improve the image quality of video taken in poor weather conditions such as rain, snow, fog and smoke. Facial and licence plate recognition programs are used to detect suspects or criminals by enabling snapshots of faces or license plates to be compared with images in a database.

Video management software can be installed on a PC server platform. Most video management systems are available for the Windows operating system, but there are also options for UNIX, Linux and Mac OS. Open platform solutions run on “off-the-shelf” hardware, with components selected for maximum performance. The systems are also fully scalable because cameras can be added one at a time, and there is no limit to the number that can be added or managed. Open systems are suitable for scenarios where large numbers of cameras are deployed. They also make it easier to add functionality to the system, such as increased or external storage, firewalls, virus protection and intelligent video algorithms.

Some video management systems use a web interface to access the video from any type of computer platform. Web interfaces allow video to be managed online from anywhere in the world, using the proper safeguards such as password protection and IP address filtering.

Video management systems based on open platforms have another advantage in that they can be more easily integrated with access control devices, building management systems, industrial control systems and audio. This allows users to manage video and other building controls through a single program and interface. Integrating a video surveillance system with access control systems allows video to be captured at all entrance and exit points and for pictures in a badge system to be matched against images of the person actually using the access card.

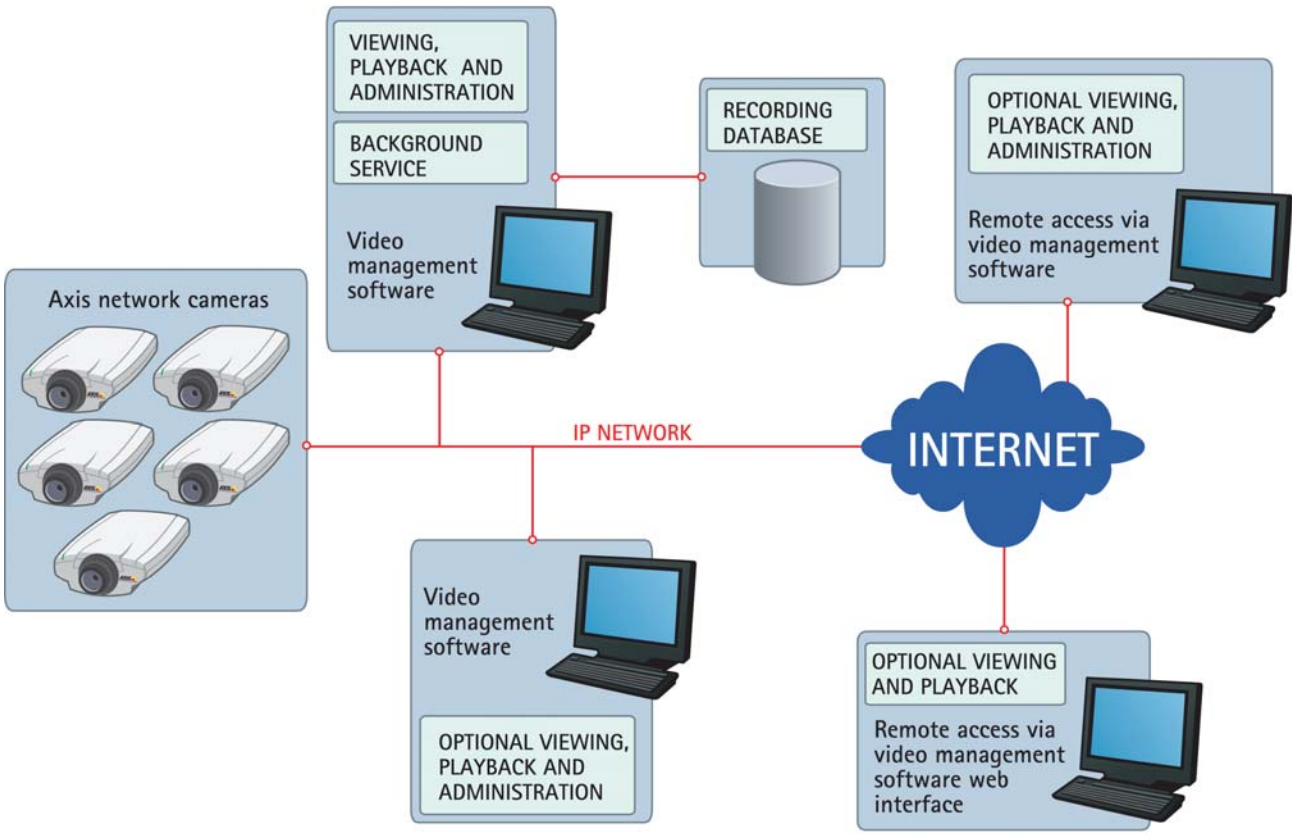
Video management systems also enable video to be integrated into industrial automation systems or BMS, such as heating, ventilation, and air conditioning systems. To do this, digital inputs and outputs (I/O) provide data to the system or the network cameras for functionalities such as controlling the heating or lighting in a room when it is not in use. I/O can be configured to record video or send alarms in response to external sensors. This allows remote monitoring stations to become immediately aware of a change in the monitored environment.

AXIS Camera Station

An example of a video management software is the AXIS Camera Station. AXIS Camera Station is specially designed to manage Axis network cameras and video encoders to provide multi-camera viewing, high-quality recording, alarm notification, multi-view playback and remote access capabilities.

The software lets you monitor multiple cameras at the same time, and simultaneously, record video either a) continuously, b) on alarm and/or video motion detection, or c) based on a schedule, wherein you can combine both continuous and triggered recording instructions. The software can also send alerts if video motion detection or an external alarm input is triggered. You can instruct the program to display a video pop-up, send e-mail notifications, or trigger an external alarm device. The software’s multi-view playback feature allows users to view simultaneous recordings from different cameras to get a comprehensive picture of an event. An events search function lets you search recordings for motion and activities triggered by external alarms. An event log can display a list of errors, while an audit log keeps track of all user actions. In addition to the normal functions of the AXIS Camera Station, an optional component called the AXIS Image Enhancer can be purchased and installed in the program. The AXIS

Image Enhancer improves the quality of images in poor visibility conditions, such as fog, smoke, rain and snow.



The AXIS Camera Station runs as a background service on a Windows PC with XP Professional, 2000 or 2003 Server. This means that even when you're logged off the PC that is running the software, the AXIS Camera Station program is still operating. The software supports recordings in both Motion JPEG and MPEG-4 for optimized quality and bandwidth. Digital recordings are saved directly onto the hard disk(s) of the local PC server running the AXIS Camera Station. On this PC, all normal operations, such as viewing, playback and administration, can be done. Meanwhile, a free Windows client can be installed on any PC on the same or outside the local network for remote viewing, playback and administration. This means that the 'server' can be placed anywhere; for example, in the server room or basement. In addition, the software enables remote viewing and playback via the Internet using any web browser.

A base license is required to run the AXIS Camera Station and allows for a specified number of cameras to be used with the program. Additional camera licenses, as well as software upgrade licenses, are available for purchase at your local Axis reseller.

More details about the AXIS Camera Station are covered in latter half of this document.

3 Mounting surveillance cameras

This chapter provides recommendations on how to best achieve useable, high-quality, surveillance video based on camera positioning and environmental considerations.

The following are some guidelines:

- **Surveillance objective**

  When positioning a surveillance camera, it is important to keep in mind the kind of image you would like to capture. If the aim is to get an overview of an area to be able to track the movement of people or objects, make sure you are using a suitable camera and that it is placed in a position that achieves this goal.

  Rotakin

  If the intention is to be able to identify a person or object, you will need a suitable camera that is positioned or focused in a way that will capture the level of detail needed for identification purposes. It may be favorable to place a camera in a high position to limit tampering. However, a lower placement may improve identification of faces or detailed objects, avoiding a "bird's eye" perspective. Local police authorities may also be able to provide guidelines on how best to position a surveillance camera. A letter chart, with varying letter sizes (attached as an appendix in this document), can be used as an indicator of the level of detail an installed camera can provide. A spinning Rotakin (see device at right) may also be used to test how well a camera displays moving objects.

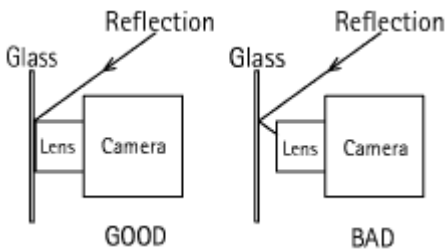
- **Housing**

  If a camera is to be mounted outdoors or in a relatively hostile environment, it needs a protective (weatherproof and/or vandal-proof) housing. Camera housings come in different sizes and qualities and some versions have built-in fans (for cooling) and/or heaters. There are vandal-resistant cameras that are already designed with an IP66-rated casing and have a built-in heater and fan, such as the AXIS 225FD Network Camera. In such a case, no additional housing accessory is required.

  
  Outdoor casing suitable for use with Axis network cameras.

- **Reflections**

  If a camera is mounted behind a glass in a housing, the lens must be placed close to the glass. Otherwise, reflections from the camera and the background will appear in the image. To reduce reflection, special coatings can be applied on any glass used in front of the lens.

- **Secure support**
  A camera should be placed on stable supports to minimize camera movement. As PTZ cameras move around, the action can cause image interference if the camera mounting is not properly secured. In outdoor situations, sturdy mounting equipment should always be used to avoid vibrations caused by strong winds.

- **Use lots of light / Add light if needed**
  The most common reason for poor quality images is lack of light. Generally, the more light, the better the images. With too little light, the images will become blurred and dull in color. You can easily and cost-effectively add strong lamps in both indoor and outdoor situations to give you the light conditions necessary for capturing good images.

  Environment: lux
  - Strong sunlight: 100,000
  - Full daylight: 10,000
  - Normal office light: 500
  - Poorly lit room: 100

  Lux is the standard unit of measurement for light. The table at right shows the available light in different kinds of conditions. At least 200 lux is needed to capture good quality images. A high-quality camera might be specified to work down to 1 lux, which means that you can capture an image at 1 lux, but it may not be of high quality. Different manufacturers use different references when they specify the light sensitivity of a camera, and this makes it difficult to compare cameras without first testing them and comparing the images captured.

  When using external, artificial lighting in outdoor environments, reflections and/or shadows should be avoided.

  For covert security or in areas where the presence of artificial light is unwanted, you can choose to use an IR-sensitive, black and white camera, or an automatic, day/night camera. In a day/night camera, color video is delivered during light conditions, while at night, the camera makes use of invisible, infrared light energy that is reflected by objects to generate IR-sensitive, black and white video. An IR illuminator, which provides infrared light, can also be used in conjunction with an IR-camera or a day/night camera to further enhance a camera's ability to produce high-quality video in low-light or nighttime conditions.

IR-sensitive network camera with IR illuminator attached below the camera housing

- **Avoid direct sunlight**
  Direct sunlight should always be avoided. Direct sunlight will "blind" the camera and can reduce the performance of the image sensor chip. If possible, position the camera with the sun shining from behind the camera.

- **Bright areas in the images should be avoided** as they might become overexposed (bright white) and objects can then appear too dark. This problem typically occurs when attempting to capture an object in front of a window. To solve this problem, simply reposition the camera or draw the curtains and close blinds if possible.

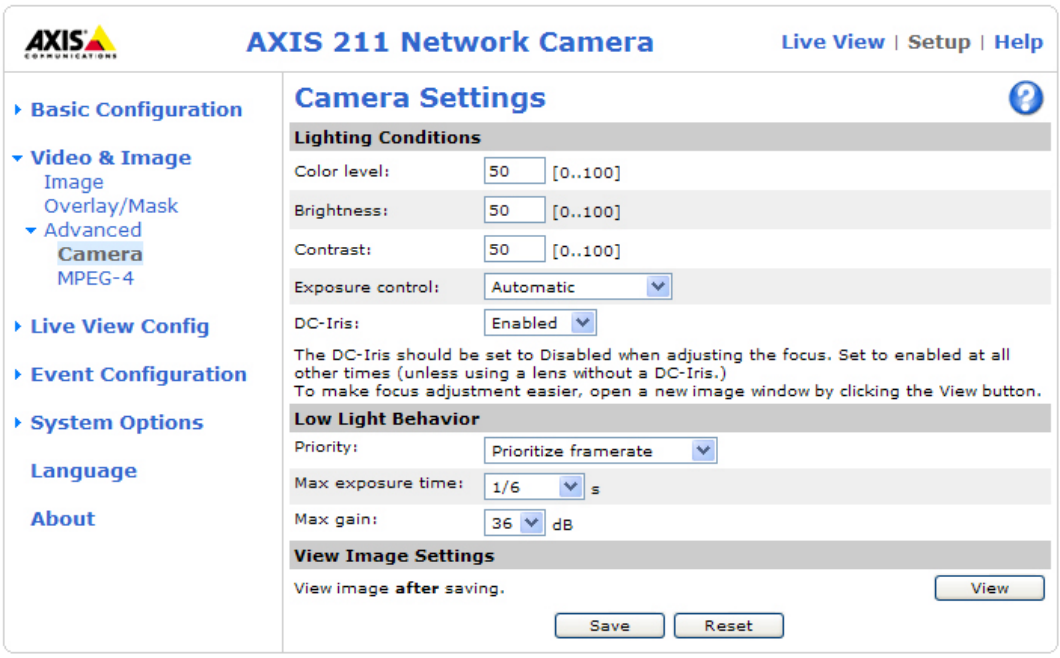
Avoid very bright areas in an image by changing the camera position.

Advanced cameras include the feature to compensate for back light.

- **Contrast**
  In outdoor environments, viewing too much of the sky results in too much contrast. The camera will adjust in order to achieve a proper light level for the sky. Consequently, the object/landscape of interest will appear too dark. One way to solve this problem is to mount the camera high above the ground, using a pole if needed.

- **Lenses**
  An auto iris lens should always be used for outdoor applications. An auto iris lens automatically adjusts the amount of light that reaches the image sensor. This optimizes the image quality and protects the image sensor from being damaged by strong sunlight.

- **Adjust camera settings**
  It is important to adjust the white balance settings for different environments (indoor/outdoor/fluorescent), as well as for brightness and sharpness.



Example of a camera user interface showing options for advanced camera settings

When deciding upon the exposure, a fast shutter speed or shorter exposure time is recommended when capturing rapid movement or when a high frame rate is required. A longer exposure time will improve image quality but it may lower the total frame rate and result in increased motion blur. In Axis network cameras, an automatic exposure setting means the frame rate will increase or decrease with the amount of available light. It is only as the light level decreases that you need to have artificial light or prioritize frame rate or image quality.

The following chapters outline how a small- to mid-sized IP-Surveillance system can be implemented using Axis network video products and AXIS Camera Station software.

4 Server selection

This chapter discusses general server recommendations, hard disk selection, network-attached storage and RAID as they relate to the installation of the AXIS Camera Station software and its hard disk cleanup procedure.

4.a General server recommendations for AXIS Camera Station

TARGET CAMERAS	REQUIRED SERVER				
	FPS	Hard disks	Bandwidth (Mbit)	CPU (GHz)	RAM
5	5	1	100	2	512
	10	1	100	2.5	512
	20	1	100	3	512
10	5	2	100	2.5	512
	10	2	100	3	512
	20	2	100	3.4	768
15	5	2	100	3	512
	10	3	1000	3.4	768
	20	3	1000	Xeon dual 3.0	768
20	5	3	100	3.4	768
	10	4	1000	Xeon dual 2.8	768
	20	4	1000	Xeon dual 3.0	1024
25	5	3	100	Xeon dual 2.8	768
	10	4	1000	Xeon dual 3.0	1024
	20	4	1000	Xeon dual 3.4	1024

The table above outlines the recommendations for server requirements in implementing an IP-Surveillance system using the AXIS Camera Station as the video management software. The recommendations are not minimum requirements.

Notes:

- The calculations are based on viewing and recording video with a 640x480 resolution and a 25 percent compression rate using Motion JPEG. Using multiple cameras and higher frame rates will raise the requirements for the server.

- The CPU recommendation is based on Pentium4 / Xeon dual processors. Other options such as Dual Core might lower the CPU requirement.
- Using MPEG-4 recording will lower the bandwidth usage and use less hard disk.
- For best performance and stability, use local hard disks for primary storage. Network storage or USB/Firewire disks should only be used for archiving (secondary storage).
- Software-based RAID systems should not be used since performance bottlenecks could result.
- The disk drive (normally C:) where Windows and AXIS Camera Station are installed should have enough disk space for the AXIS Camera Station log files. Allow at least 1 GB free disk space for the log files.

4.b Hard disks

When selecting hard disks for your surveillance solution, keep in mind that the recording of a continuous stream of video from multiple cameras will add more load on the hard drive than a standard office PC or mail server.

There are three main hard drive solutions on the market:

1. SCSI
2. Serial ATA
3. IDE

SCSI is the best solution in terms of reliability (and also the most expensive), followed in order by Serial ATA and IDE. Note that Serial ATA and IDE are made for office desktops and not for 24-hour server operation as a surveillance solution demands. Since it is difficult to predict how long such hard disks will last, it is recommended that Serial ATA and IDE disks be installed in such a way that they are easy to replace in case of failure.

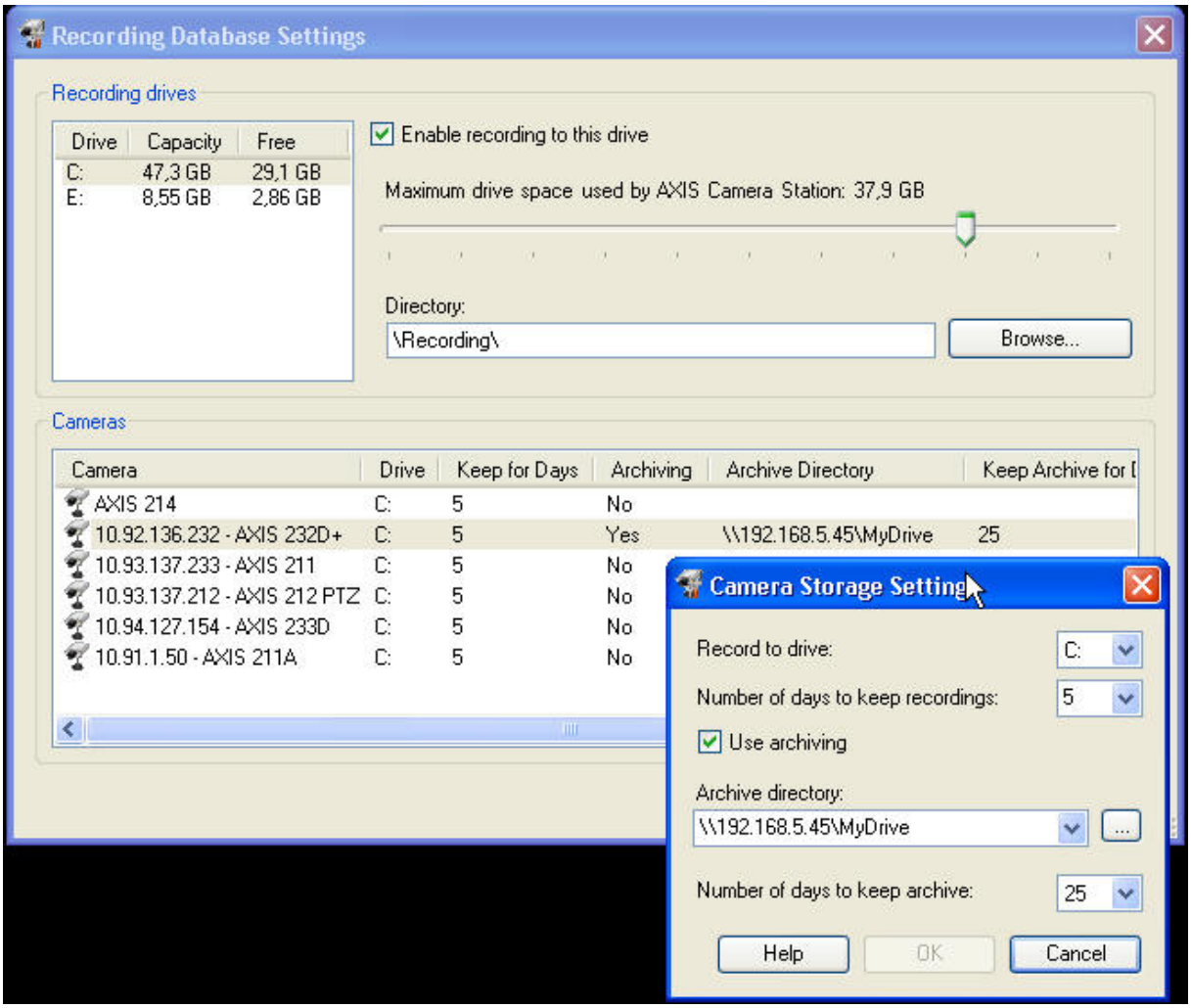
4.c Network-attached storage (NAS) and RAID

AXIS Camera Station can use NAS as a media to store recordings. The software enables two levels of storage:

1) Primary hard drive (always the local hard disk)
2) Archive (local disks or network-attached drive/remote hard drive)

AXIS Camera Station will always record video initially on the primary hard drive. The video will remain there for the number of days specified in the configuration. If no archive drive is specified, the recorded video will be deleted when they are older than the number of days specified.

If an archive drive is enabled, video recordings from the primary drive will be moved to the archive drive when the recordings become too old. They will stay in the archive for the number of days specified in the archive setup.



AXIS Camera Station: Recording database settings

Most customers use only the primary drive configuration. The reasons for using the archive option are: 1) for storing video for more days than the primary hard disk can hold, and 2) for securing recordings on another server or location.

When using remote disks or network-attached storage, you should ensure that the necessary bandwidth is available to move your recordings from the AXIS Camera Station server to the archive drives. If network-attached storage is used, you will also have to consider that live streams from the cameras are running while data from the local drive are moved to the NAS.

Using Redundant Array of Independent Disks (RAID) setup

RAID—which is a method of arranging hard drives in such a way that the operating system sees them as one large, logical hard disk—can be used to secure your recordings and configuration, but it must be implemented with caution.

RAID is mostly configured in three different ways:

RAID Level	Characteristics
RAID-0	Data is being striped (divided) over two or several hard disks for improved read/write speed but no redundancy. There is no advantage of using this setup with the AXIS Camera Station.
RAID-1	This is also known as disk mirroring since all hard disks are mirrored one by one. At least two disks duplicate data. Both disks can be read at the same time. Write performance as for single disk storage.
RAID-5	Minimum of three hard disks. One of the hard disks is used to mirror the others (in theory).

When RAID 1 or 5 is used, data is written twice, over two hard disks (one for the primary data disk and one for the mirror disk). This has an impact on performance since all disk writes are doubled in a RAID setup. When multiple cameras are streaming data to the hard drives, the RAID controller will handle the load using buffers and distribute the data to the disks. Since the hard disk write is doubled and there is a limit of how many write per second the setup can handle, a RAID setup can become a bottleneck in a surveillance scenario if it is not implemented correctly.

There are three usual ways to implement RAID:

1) A software solution that can configure two or more hard disks into a RAID setup. This is a very slow implementation and should never be used for surveillance.
2) The CPU comes with an on-board RAID solution. This is a hardware implementation that may have limited performance and should be used with caution.
3) Full hardware implementation with a separate RAID controller. This is the only recommended way to implement RAID for a surveillance solution. Make sure you use a well-known and well-proven RAID technology, as your surveillance solution will rely on it.

4.d The AXIS Camera Station hard disk cleanup procedure

While the AXIS Camera Station recording engine is running, some procedures are continuously executed to ensure that your hard disks do not become full. The procedures include:

1) Comparing *primary recorded images* with current date and configured “days to record.” If the saved recordings have passed the number of days that they should be stored in the primary hard drive, the images are removed. (If archive is enabled, the images are moved to archive and then deleted eventually.)
2) Comparing *archived images* with current date and configured “days to archive.” If the recordings are older than the number of days specified for storage, then the images are deleted.
3) Freeing up space on the primary hard drive for current recordings. If the space available on the primary drive is less than what is specified in the configuration, an emergency cleanup is invoked. This means that the oldest recordings from all cameras are deleted and space is freed up for current recordings. (No emergency cleanup can be performed on archive disks due to limitations in the network or Windows.)

5 AXIS Camera Station installation and configuration

This chapter provides an overview of the AXIS Camera Station installation and configuration processes covering registration, camera setup, recording methods, bandwidth control and security.

5.a Installing AXIS Camera Station

AXIS Camera Station should be installed on a dedicated, stand-alone PC from where you wish to run the main administration of your cameras and video encoders.

The installation process involves:

1) Accepting the license agreement.

2) Selecting the preferred language and where the program should be installed.

3) Accepting that the TCP port 11007 be opened in the firewall to enable incoming requests from AXIS Camera Station Client when prompted.

4) Then the program is installed.

5) The first time the program is activated, it will ask you to register your license. The license key can only be used on one computer. Once the license key is registered, it cannot be used again. Therefore, the AXIS Camera Station must be installed on the target computer when activating the software.

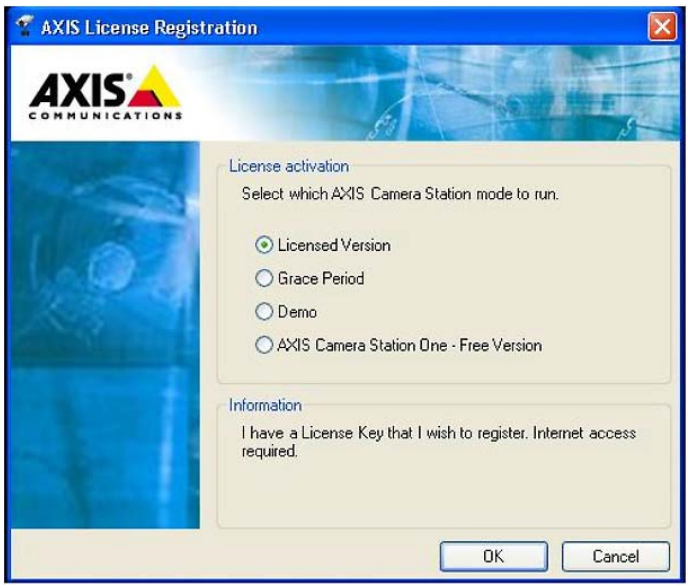
   You can choose to activate, either automatically or manually, one of four AXIS Camera Station alternatives:

   a) Licensed Version

   b) Grace Period (which allows you to use the software for five days)

   c) Demo (30-day trial version for four cameras. When the period expires, you will be required to register the software)

   d) AXIS Camera Station One - Free Version.



5.b Setting up a camera in AXIS Camera Station

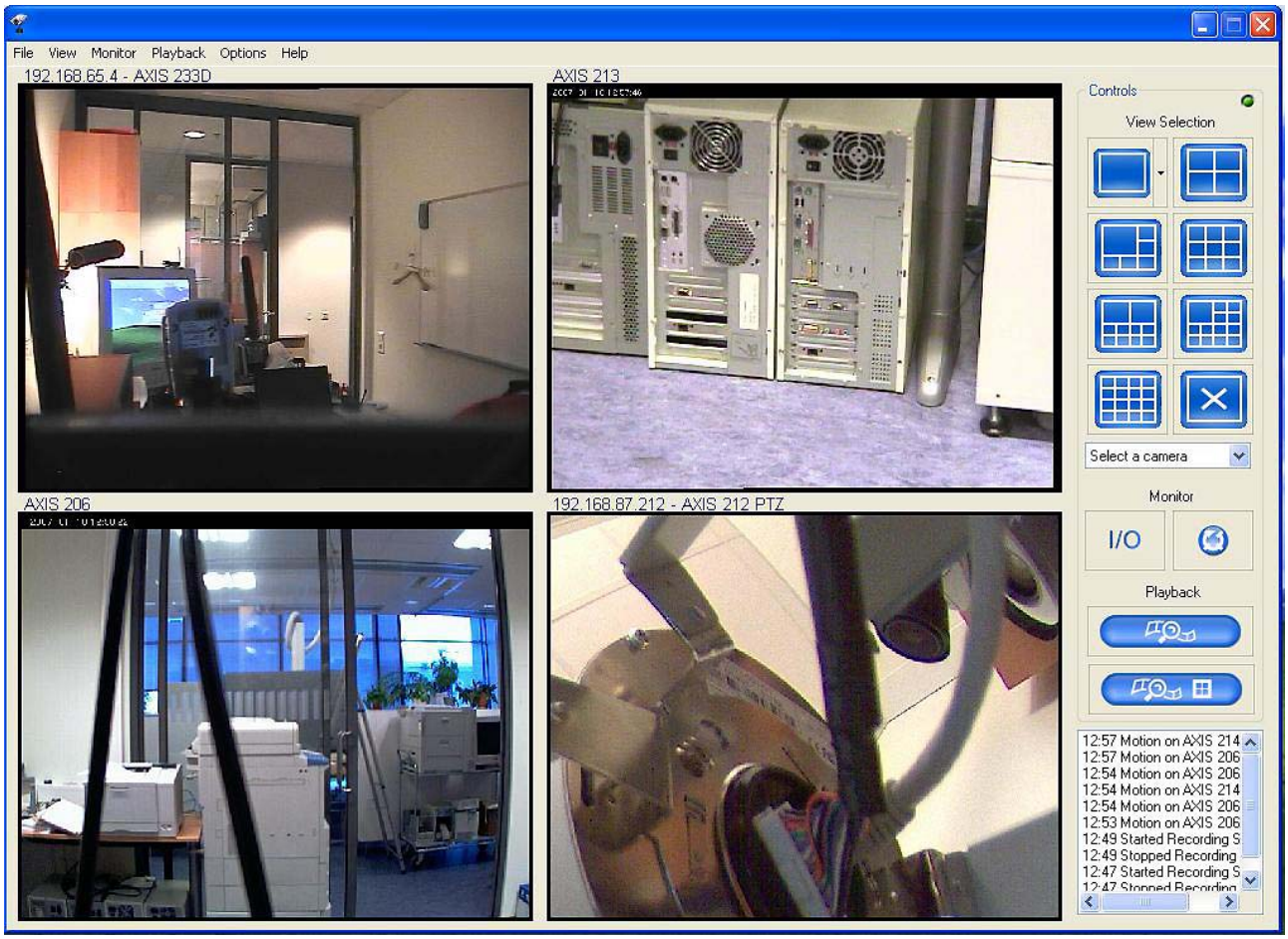
After installing the AXIS Camera Station, it must be configured for your network cameras and video encoders. The first time the software is configured, a search function automatically finds and installs the network cameras/video encoders on your network. If there are more cameras/video encoders on your network than you have a license for, a dialog box opens automatically to show a list of video products on your network. Then you simply check the boxes for the cameras/video encoders you would like to import into the AXIS Camera Station.

To add a network camera or video encoder at a later date, you can either manually enter the LAN and WAN IP addresses of the camera/video encoder, or click a Search button to get a list of video products on your network. The LAN IP address is used to access the camera within the LAN, while the WAN IP address is used when accessing the camera from outside the local network; for example, over the Internet.

Then choose a master user name and password if the cameras are set up to use a common user name and password, or enter a specific user name and password for a specific camera.

Customize the view in AXIS Camera Station

AXIS Camera Station offers a number of different layouts to view one or many cameras simultaneously. Select one of the layouts and arrange cameras in the view by clicking on the position in the view and then the desired camera in the list of cameras/video encoders shown. You can also drag and drop a camera to the desired position in the view. Then select the frame rate and video compression format.



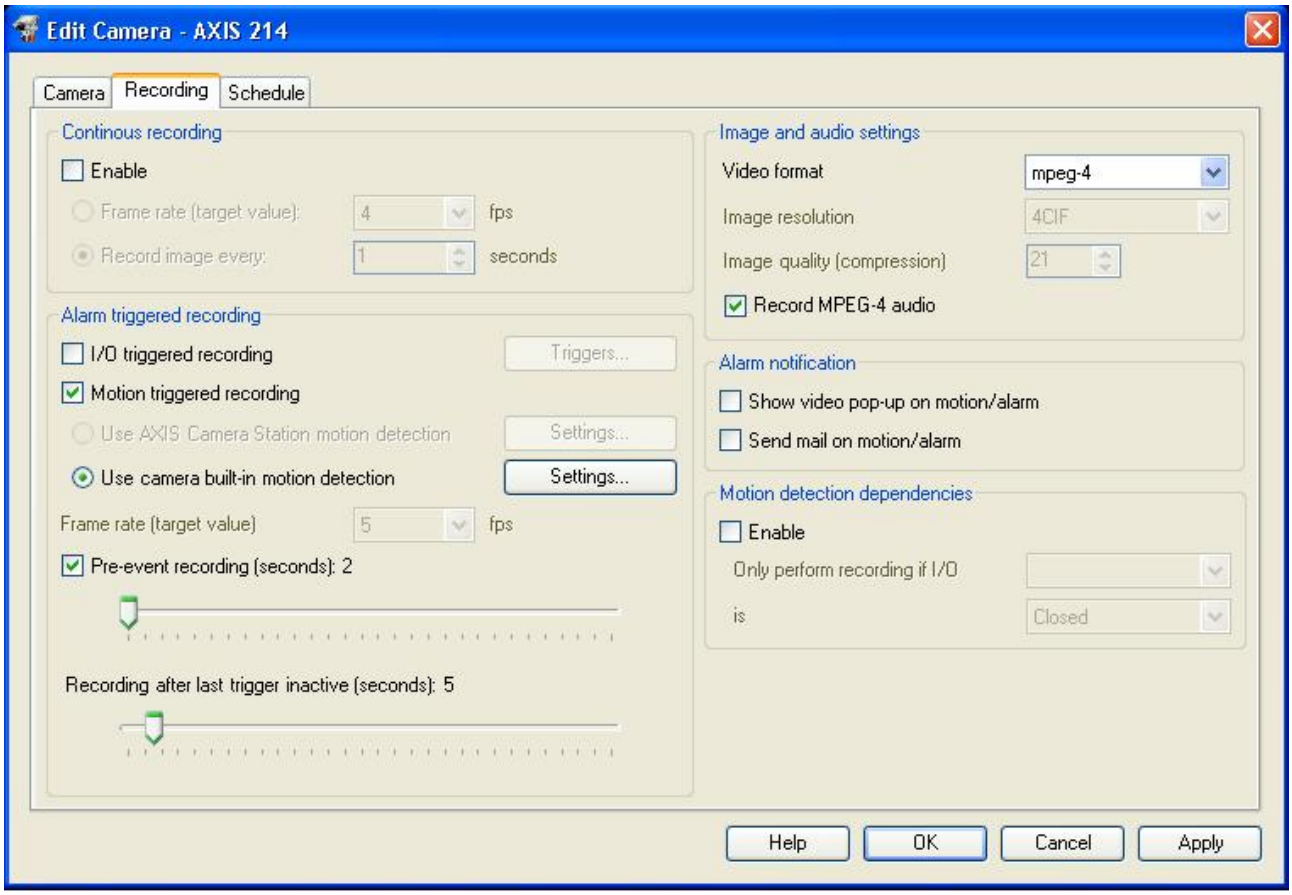
5.c Recording methods

For each camera, you can select one of three recording methods to use:

1) continuous

2) triggered by motion or alarm

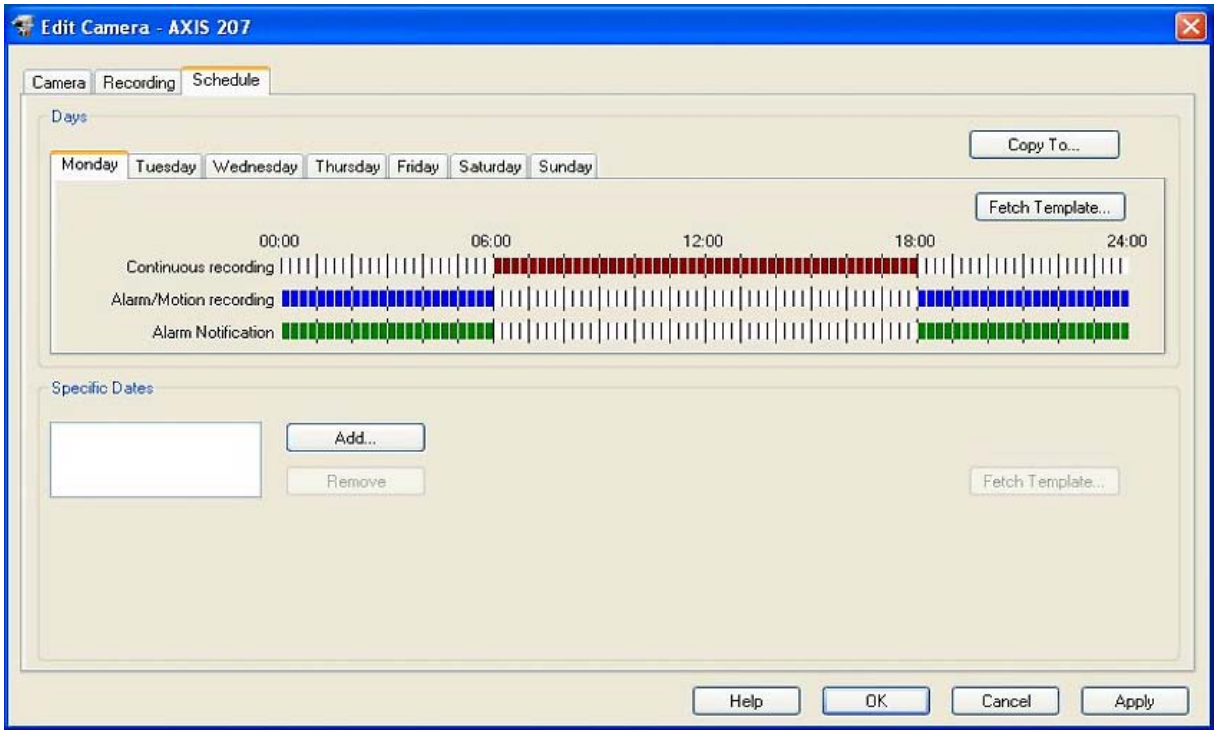
3) scheduled, which can combine both continuous and triggered recording instructions



In continuous recording, you can set how many frames per second and how often (i.e. every few seconds between images) the camera should send images to the software for recording. Continuous recording uses more disk space than an alarm-triggered recording.

In alarm-triggered recording, you can set up video motion detection using either the AXIS Camera Station or the network camera's built-in motion detection. Using the camera's built-in motion detection reduces bandwidth usage and processing load on the server. With recordings triggered by external inputs (I/O triggered recording), simply define the alarm for the selected camera(s) that will record when the alarm is triggered. You can also determine the length of the pre- and post-alarm image buffers by setting how many seconds you want to record before and after an alarm is triggered. This will provide you with a more comprehensive picture of an event. Recording only when motion or alarm is detected will save hard disk space compared with continuous recording.

With scheduled recordings, you can set up timetables for both continuous recording and alarm/motion recording.



Scheduled recording settings

Once the type of recording method is selected, you can determine the quality of the recordings by setting the video format (Motion JPEG/MPEG-4), resolution and level of image compression. These settings will affect the amount of bandwidth used, as well as the size of storage space required.

The AXIS Camera Station's background service automatically starts running upon system start-up. When the background service is running, recording will continue even after a user has logged out from the PC where AXIS Camera Station is installed.

5.d Calculating your hard disk requirements

Network video products utilize network bandwidth based on their configuration. Bandwidth usage depends on five criteria:

1) image resolution (the higher the resolution, the more bandwidth is required)

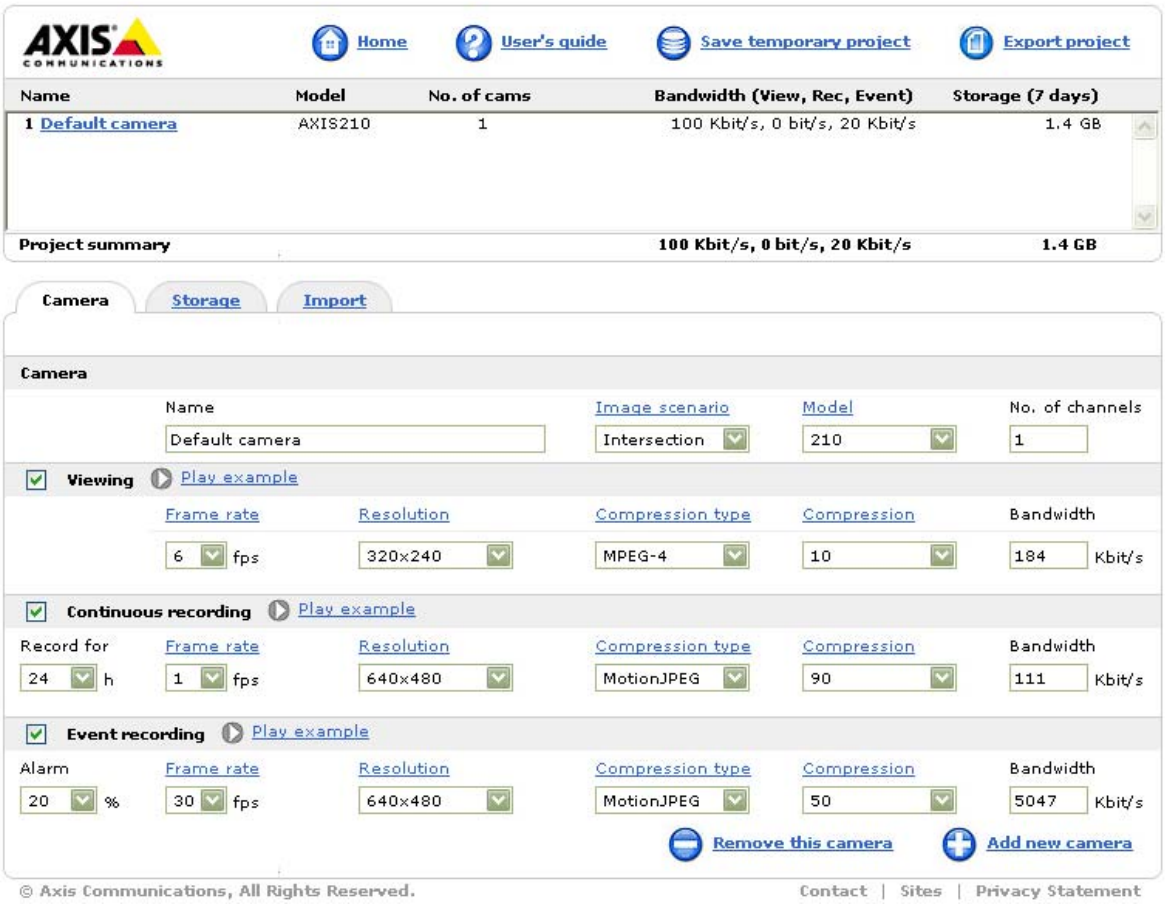
2) compression type (Motion JPEG often requires more bandwidth than MPEG-4)

3) compression ratio (the higher the compression, the lower the bandwidth usage)

4) frame rate (the higher the frame rate, the higher the bandwidth usage)

5) image complexity (the more complex, the higher the bandwidth usage)

The above criteria can be set either in the AXIS Camera Station software or in the network camera or video encoder product itself. A simulation-based calculation tool called the AXIS Design Tool is available on http://www.axis.com/products/video/design_tool/ (or on a DVD) and helps provide guidance on a network video product's bandwidth and storage requirements based on the five criteria mentioned earlier.



AXIS Design Tool user interface

You can reduce the use of bandwidth if you record only when motion or alarm is detected compared with continuous recording. The most efficient use of bandwidth and storage space is if you set the AXIS Camera Station to record using the camera/video encoder's built-in video motion detection and the MPEG-4 compression format. Note that while the AXIS Camera Station enables MPEG-4 recording, setting the frame rate, motion detection and image quality in MPEG-4 compression must be done in the network camera/video encoder itself.

5.e Security aspects

A high level of security can be implemented in the AXIS Camera Station. The software can inherit the Windows user database (local or LDAP/Domain) and you can grant or deny users access to a specific camera. This feature allows you to use your current user database without having to set up and maintain a separate database of users.

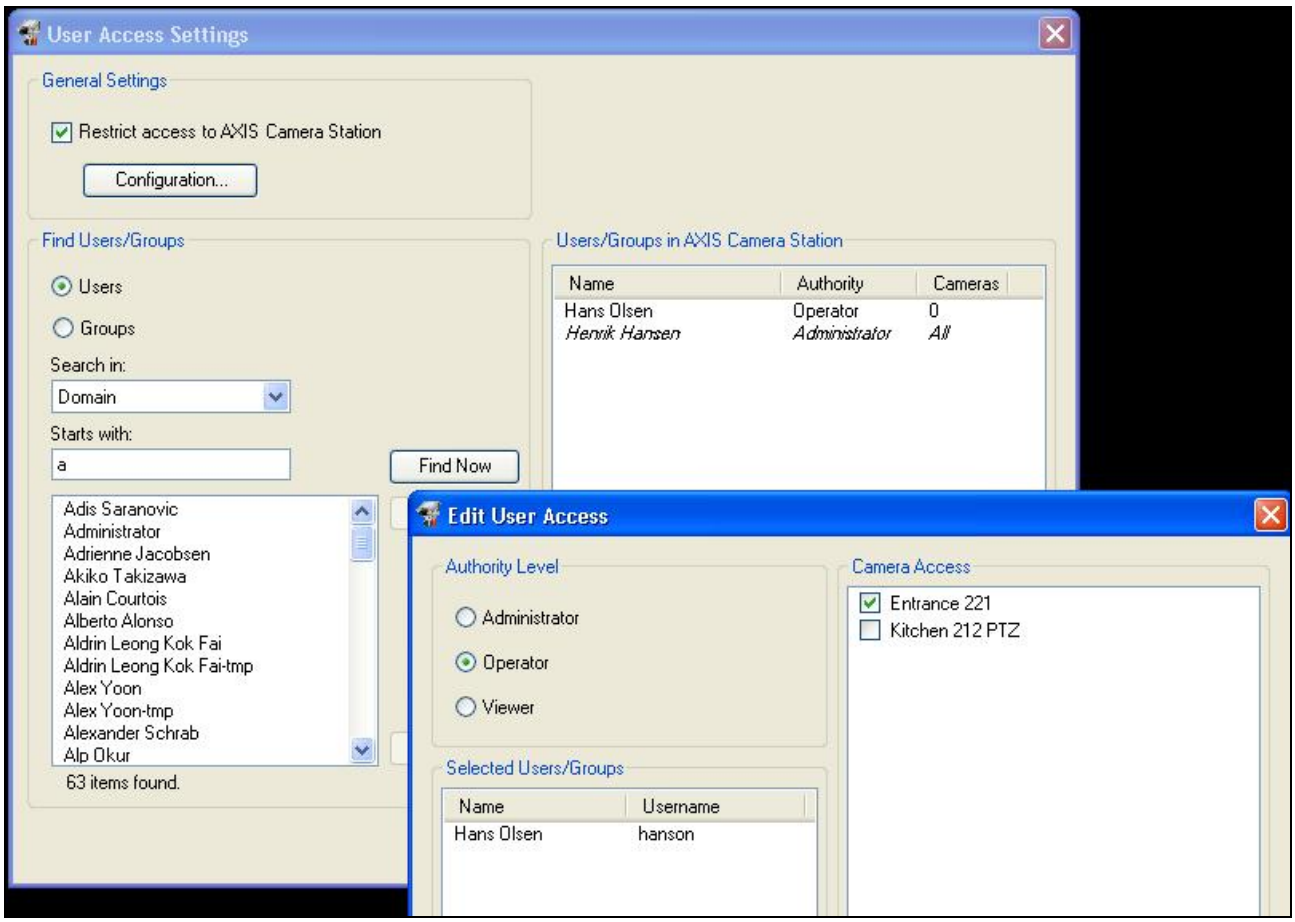
Once a user is defined, you select the user-access level. Three levels are available:

1) Administrator – full access to all of AXIS Camera Station's functionalities

2) Operator – Access to all functionalities (including recorded events) except the configuration pages under Options

3) Viewer – Access only to live video

Then select the password and choose which cameras the user will be allowed to access.



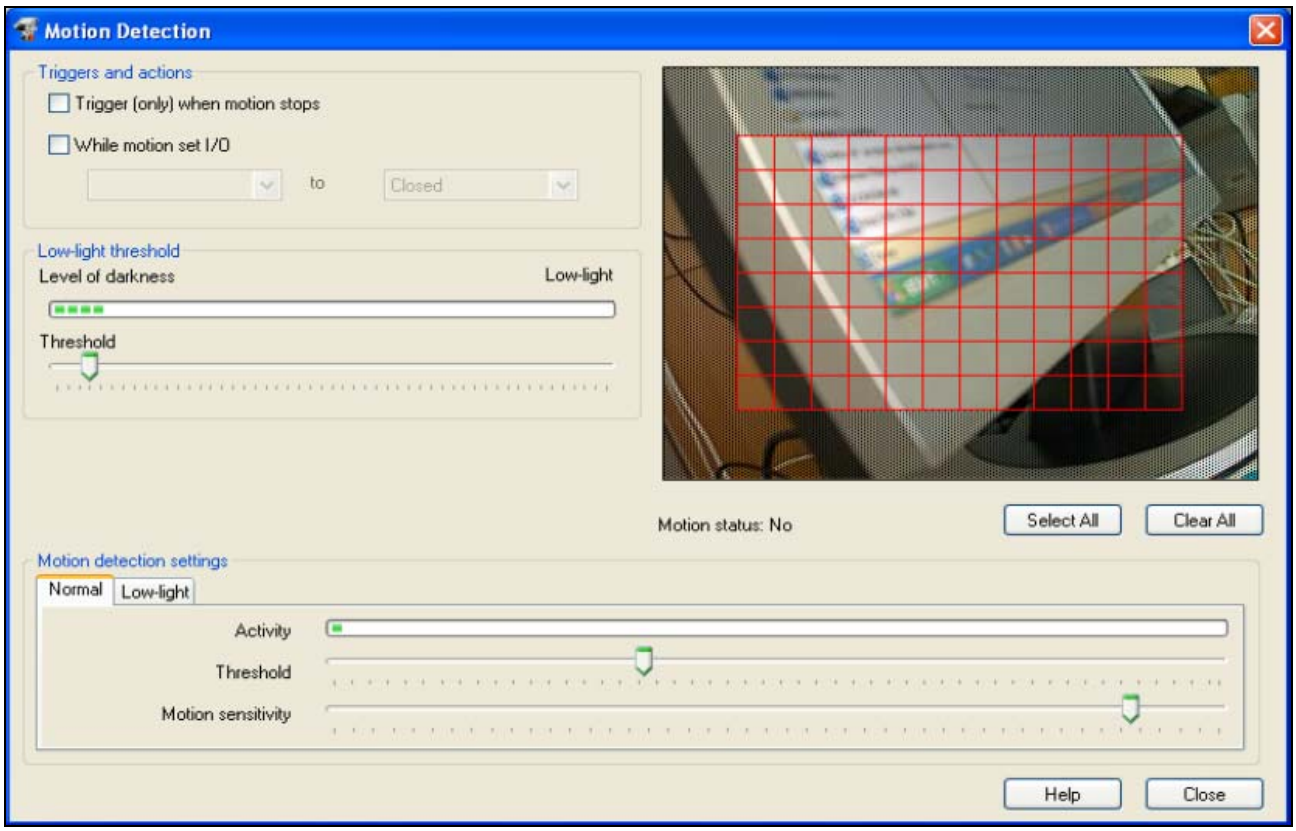
6 Video motion detection

This chapter describes the video motion detection function in the AXIS Camera Station and in the network camera or video encoder.

6.a AXIS Camera Station video motion detection

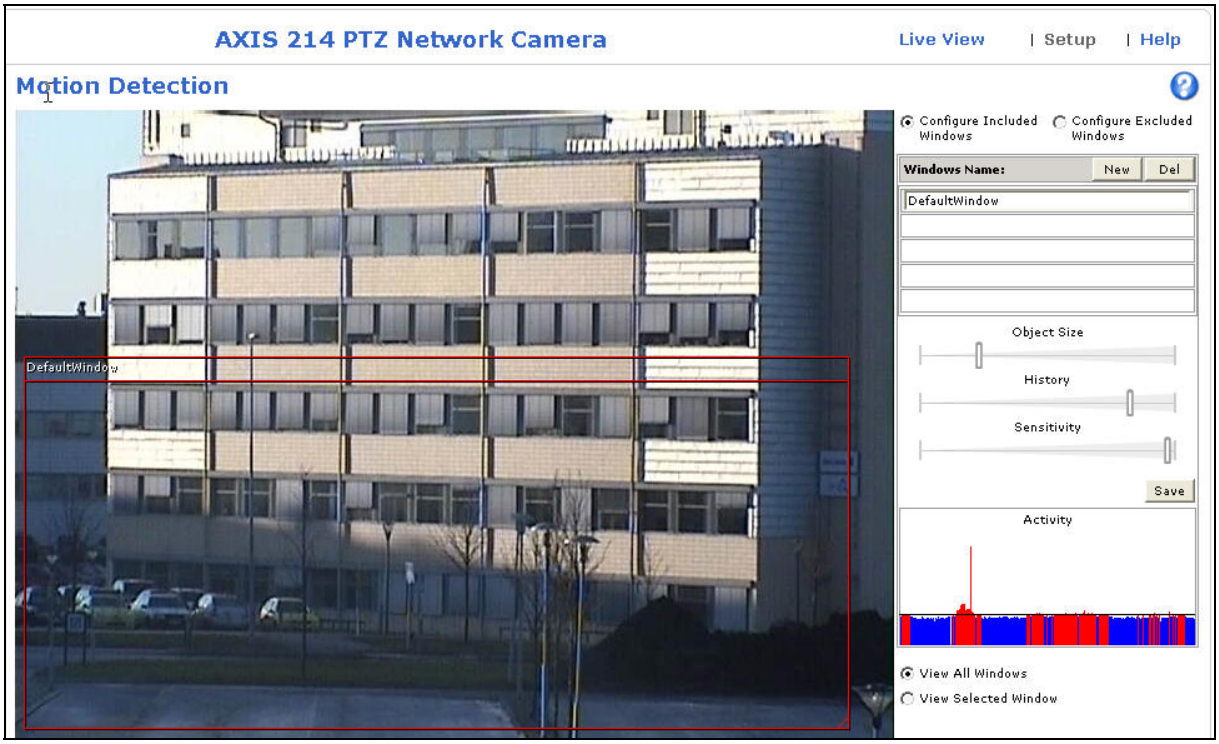
The AXIS Camera Station's video motion detection feature works by retrieving an image several times every second and comparing the differences in a specified area of the image.

The AXIS Camera Station allows you to set the motion detection grid in the area where you want motion to be detected. In addition, you can set up different motion detection sensitivities for low or normal light conditions. Once motion is detected, you can instruct the AXIS Camera Station to trigger an external alarm (such as a door to open/close, a light to turn on/off), instruct recordings from selected cameras, and send e-mail alerts. The software can also be instructed to trigger alerts when motion stops, which is helpful, for example, in factory situations.



6.b Built-in video motion detection in camera/video encoder

The built-in video motion detection feature in Axis network cameras or video encoders can be used to generate an alarm whenever movement occurs (or stops) in the video image. You can configure a number of “included” windows (a specific area in an image where you want motion to be detected), as well as “excluded” windows (areas within an “included” window that should be ignored).



When configuring for video motion detection, you can adjust the size of the window where you want motion to be detected and drag the window to the desired position. You can then adjust sliders for the object size (how large should the object be in order for the trigger to activate), history (how far back in time should the reference point for motion detection be), and sensitivity (how big should a change in the pixels be in order to trigger an alarm).

Any detected motion within an active window is then indicated by red peaks in the activity window (the active window has a red frame).

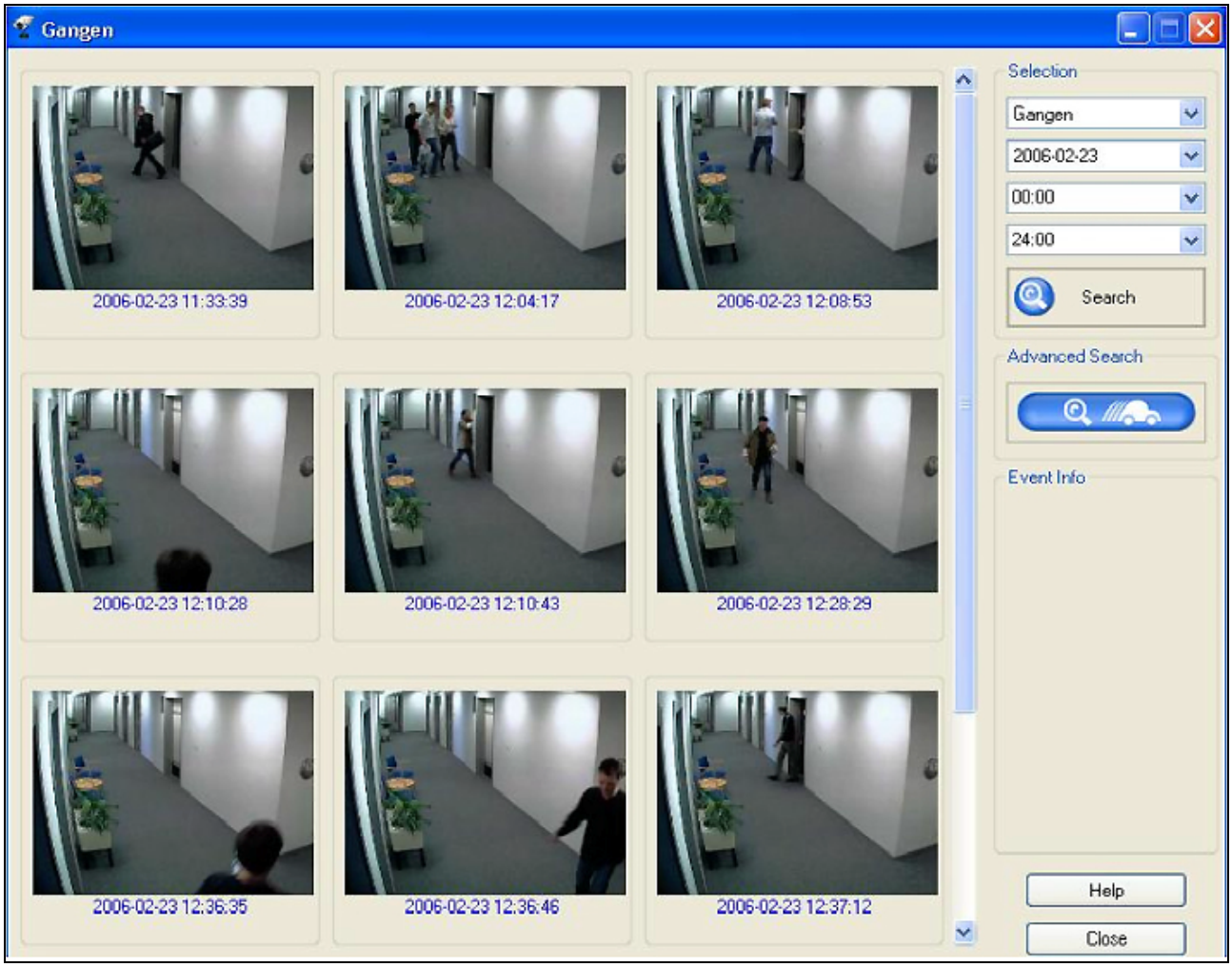
7 Daily operation

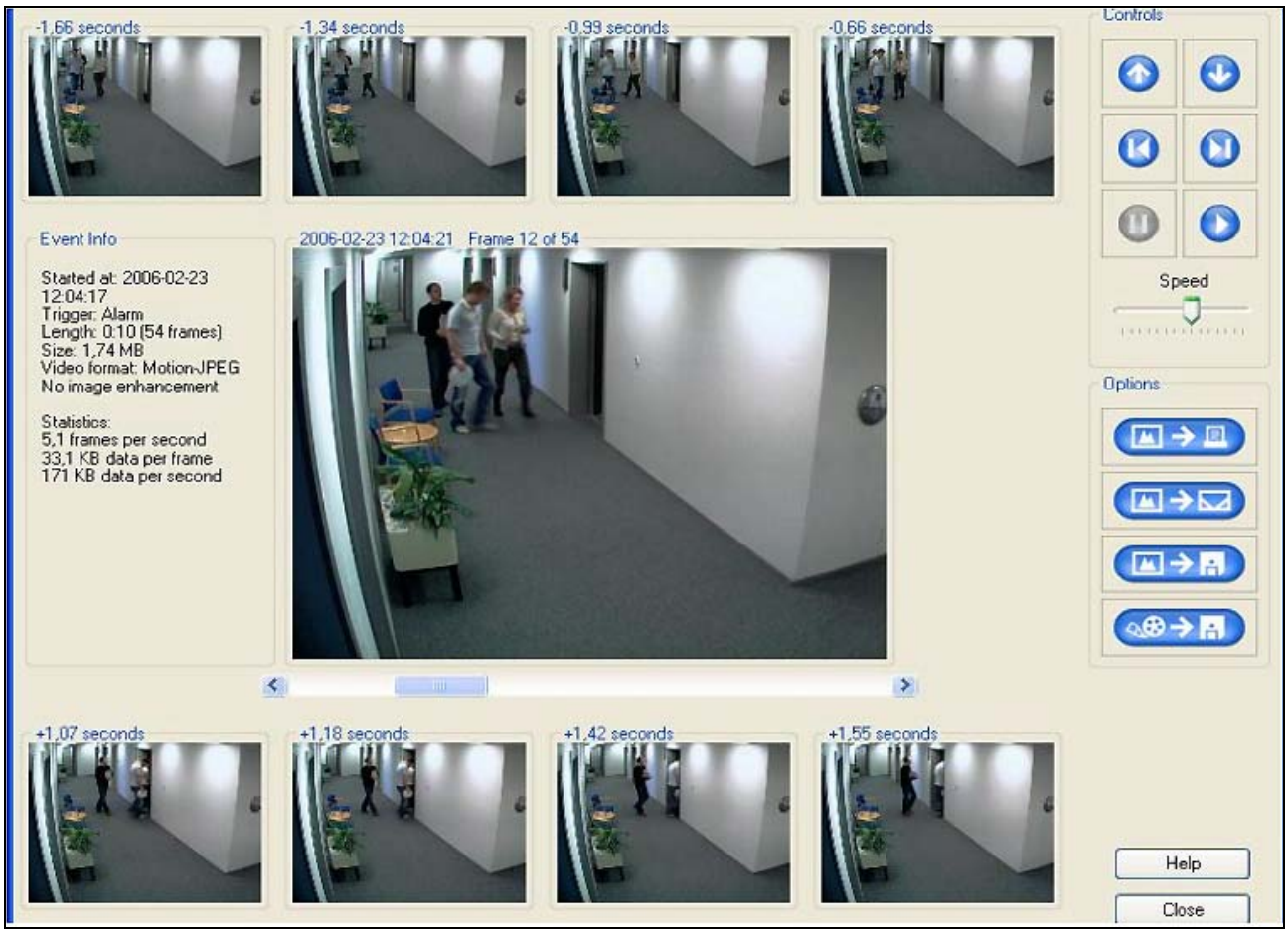
This chapter describes the functions in the AXIS Camera Station that may be used on a daily basis: events search, live image viewing, log files and configuration check, as well as remote connections.

7.a Events search

AXIS Camera Station offers easy ways to search for recorded events in Event Search and 4-Camera Playback. An event is a recording that is triggered by an alarm or schedule. 4-Camera Playback enables a user to view simultaneous recordings from different cameras to obtain a comprehensive picture of an event.

To search, simply select a camera and the date and time, and you will get sample images of all events found. Double-clicking on the image plays the recorded sequence.





7.b Live images and PTZ controls

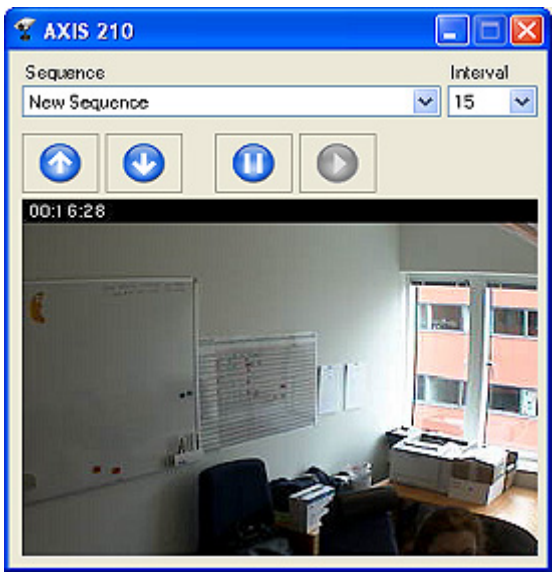
The AXIS Camera Station provides four different ways to view live images:

1) Split view

2) 1 camera pop-up (or pop-up on motion detection)

3) Monitor mode (full screen)

4) Camera sequence (A camera sequence is a pre-defined “tour” that automatically switches to all of the cameras included in the tour.)



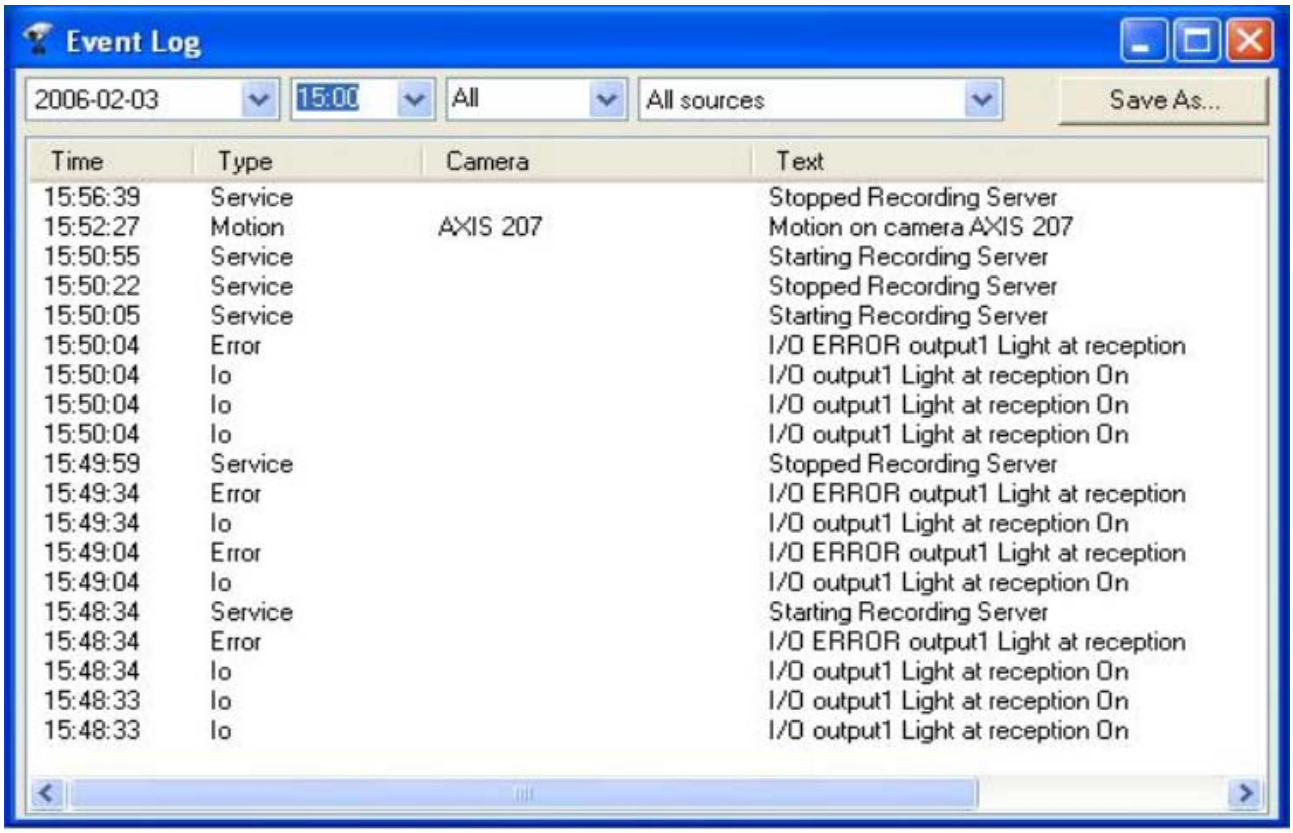
1 camera pop-up

The AXIS Camera Station also enables pan/tilt/zoom (PTZ) control when working with a PTZ or dome network camera. The software allows you to control the PTZ function of the camera by 1) clicking on a display keypad, 2) using a mouse (you can click in the image to move the camera or zoom in using the mouse scroll wheel), or 3) using the AXIS 295 Video Surveillance Joystick. In addition, if the camera is equipped with audio capability, the audio controls will be automatically shown in the AXIS Camera Station program.

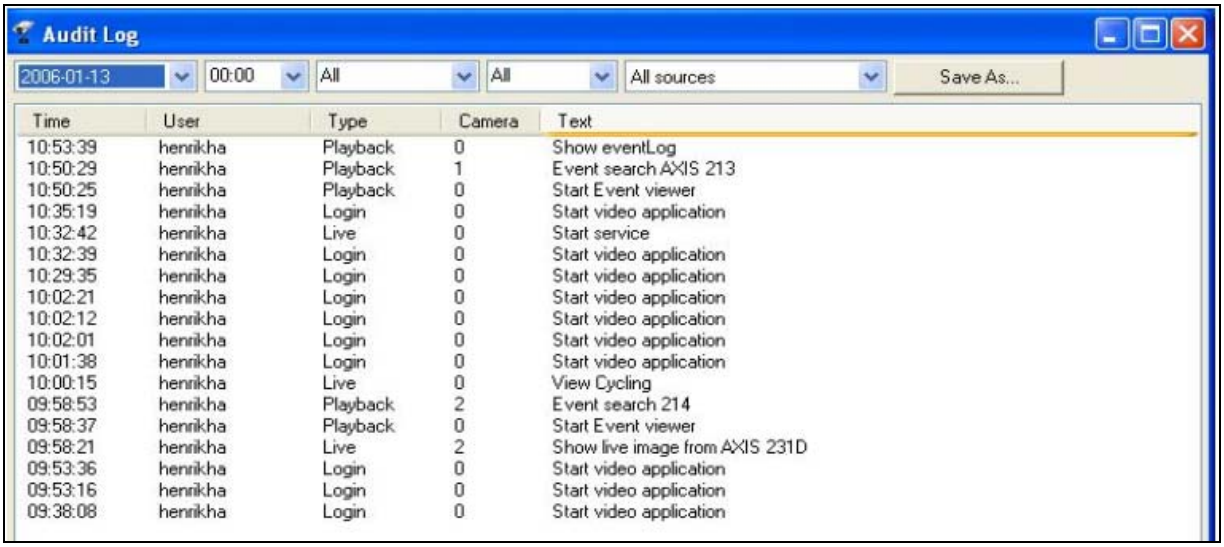
7.c Log files

The AXIS Camera Station provides two types of log files: event and audit.

The event log provides a list of camera and server events based on date, time, type and source of the events. You can sort or search, for example, for a list of errors or when motion is detected.

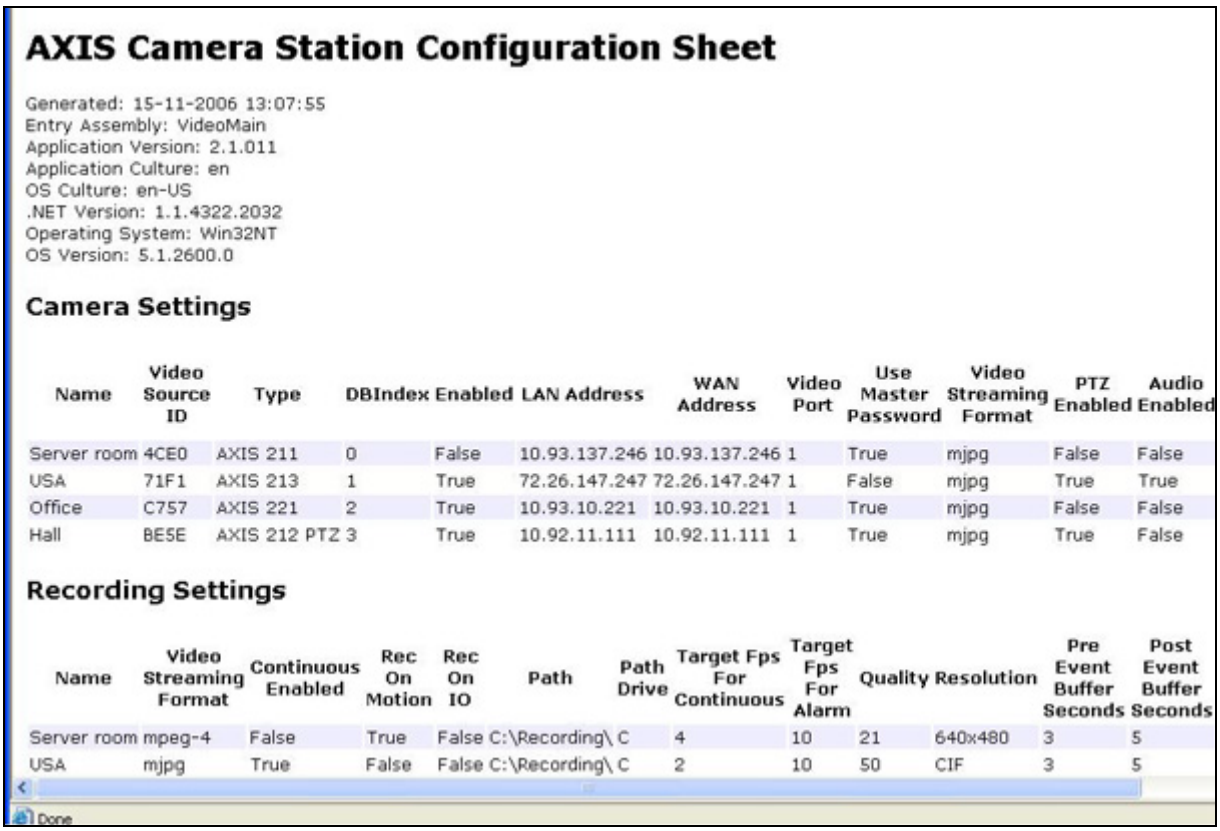


The audit log allows you to generate a list of user actions based on the user, time, type of activity and camera. All user activities are logged in the AXIS Camera Station. You can filter and sort all fields in the generated list.



7.d Configuration overview

For maintenance purposes, the AXIS Camera Station's Configuration Sheet enables you to obtain, in one place, an overview of all your camera and recording configurations.



AXIS Camera Station Configuration Sheet

Generated: 15-11-2006 13:07:55
Entry Assembly: VideoMain
Application Version: 2.1.011
Application Culture: en
OS Culture: en-US
.NET Version: 1.1.4322.2032
Operating System: Win32NT
OS Version: 5.1.2600.0

Camera Settings

Name	Video Source ID	Type	DBIndex	Enabled	LAN Address	WAN Address	Video Port	Use Master Password	Video Streaming Format	PTZ Enabled	Audio Enabled
Server room	4CE0	AXIS 211	0	False	10.93.137.246	10.93.137.246	1	True	mjpg	False	False
USA	71F1	AXIS 213	1	True	72.26.147.247	72.26.147.247	1	False	mjpg	True	True
Office	C757	AXIS 221	2	True	10.93.10.221	10.93.10.221	1	True	mjpg	False	False
Hall	BE5E	AXIS 212 PTZ	3	True	10.92.11.111	10.92.11.111	1	True	mjpg	True	False

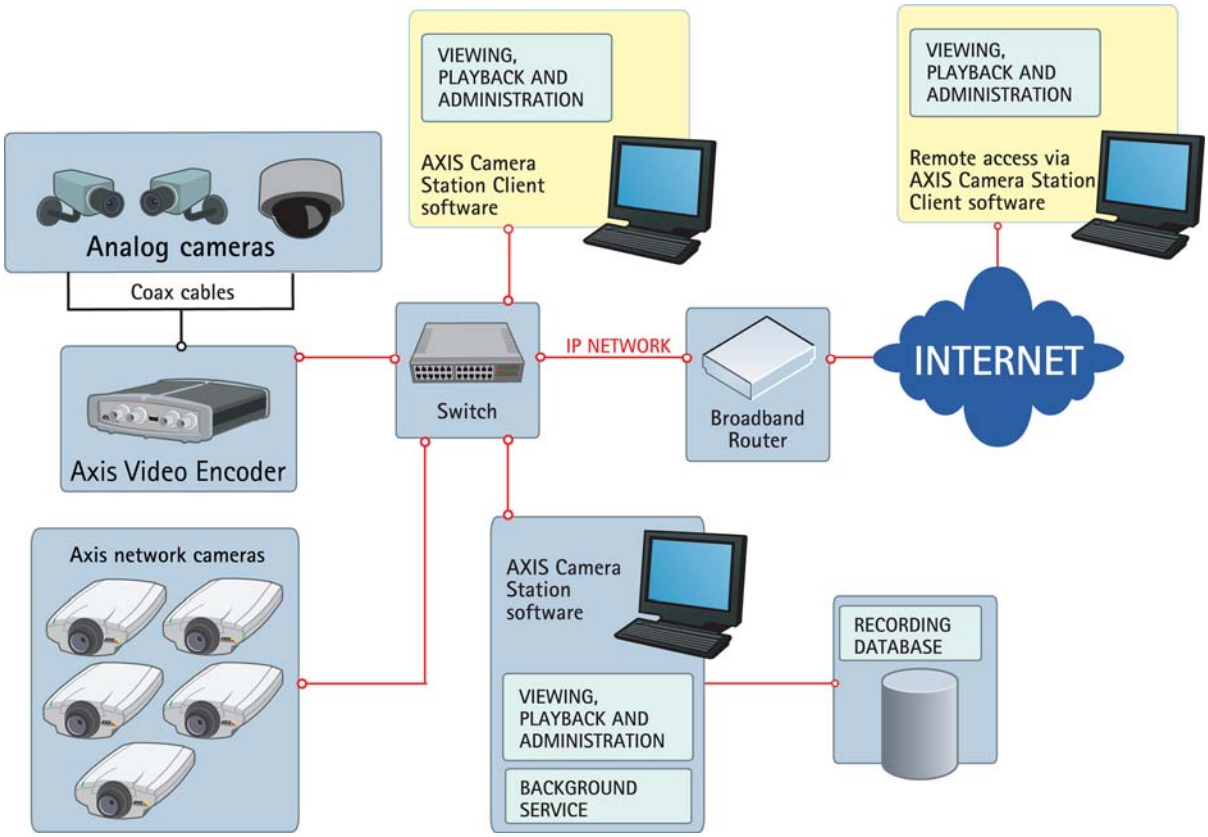
Recording Settings

Name	Video Streaming Format	Continuous Enabled	Rec On Motion	Rec On IO	Path	Path Drive	Target Fps For Continuous	Target Fps For Alarm	Quality	Resolution	Pre Event Buffer Seconds	Post Event Buffer Seconds
Server room	mpeg-4	False	True	False	C:\Recording\	C	4	10	21	640x480	3	5
USA	mjpg	True	False	False	C:\Recording\	C	2	10	50	CIF	3	5

Done

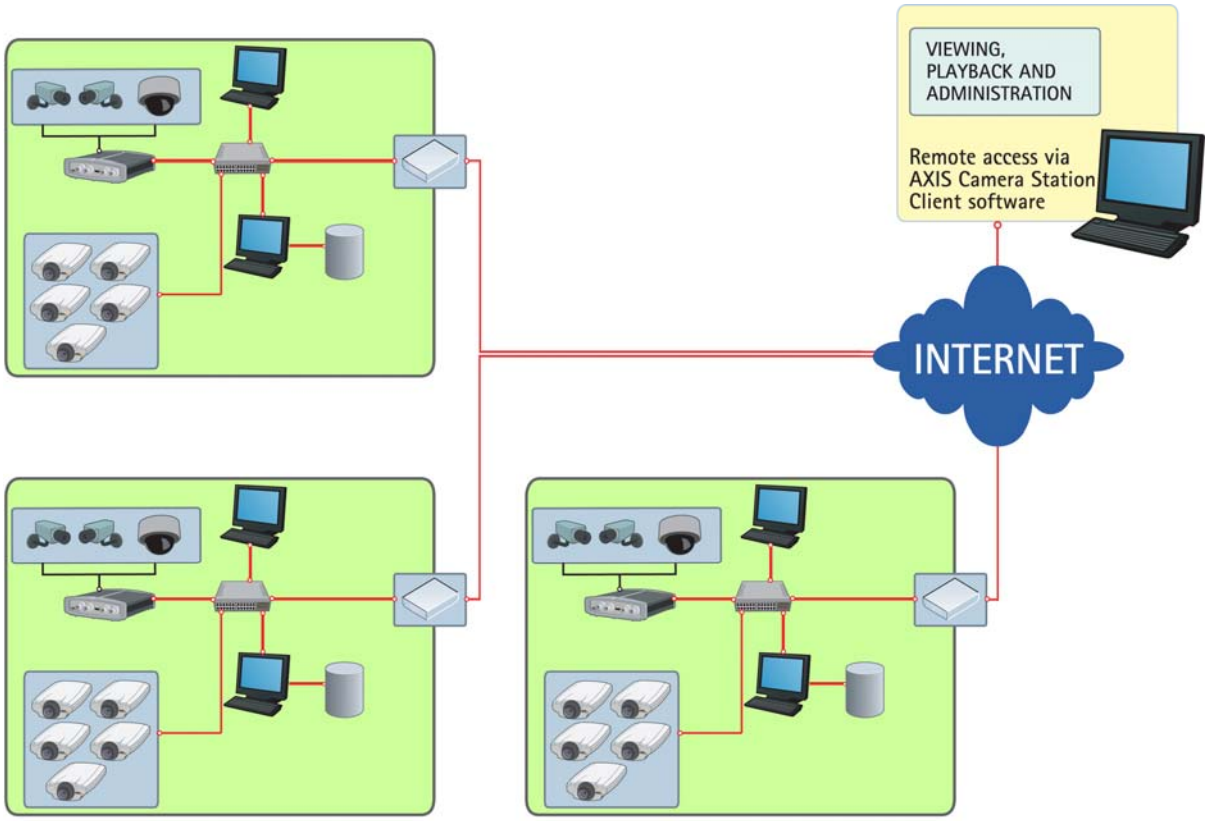
7.e Remote connections

Using AXIS Camera Station's Windows client software



Using AXIS Camera Station's Windows client software

The AXIS Camera Station client application is used for remote operations on client workstations and allows you to perform the same tasks using the same user interface as on the computer with the AXIS Camera Station installed. The client application lets you work as if you are operating directly on the AXIS Camera Station PC. Once the application is installed, you simply enter the IP address or host name of the server PC where AXIS Camera Station is installed and, if required, enter the user name and password. The client will download and inherit the camera settings from the AXIS Camera Station. From the same client, you can also switch between different AXIS Camera Station servers.

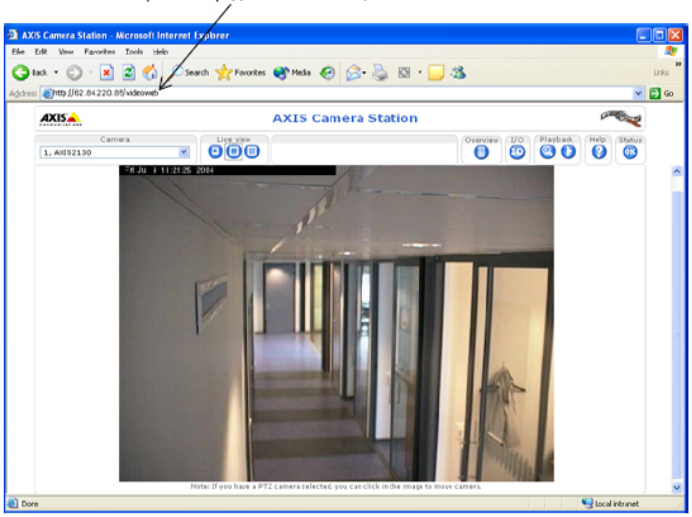


You can also switch between different AXIS Camera Station servers using the client software

Using the AXIS Camera Station web application

A web browser can be used on client workstations to view cameras and perform simple operations, such as reviewing or playing back recordings. Once web access has been enabled in the software, clients can access camera views from a browser by typing http://<server IP address>/VideoWeb in the Address field.

Example: http://10.13.6.128/VideoWeb



8 Scaling up your surveillance system

The AXIS Camera Station enables you to easily add more cameras to the system, while the client application allows you to work with multiple AXIS Camera Station servers.

8.a Adding more cameras

AXIS Camera Station allows you to easily add cameras to the system simply by using the Add function. You can add as many cameras to the system as the purchased license allows. If the number of cameras exceeds the number allowed under license, simply purchase an add-on license.

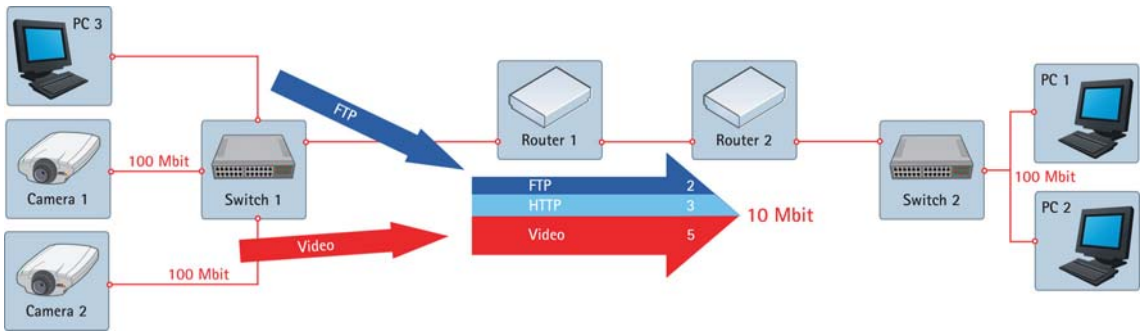
8.b Network considerations

If you are implementing 10 cameras or more, you should try to estimate the load on the network using a few rules of thumb:

- A camera will use approx. 2 to 3 megabits of bandwidth when configured to deliver high-quality images at a high frame rate.

- With more than 12 to 15 cameras, you should consider using a switch with a gigabit backbone. If a gigabit-supporting switch is used, the server running the video management software should have a gigabit network adapter installed.

Consider also using Quality of Service (QoS) on your network. Quality of Service enables reservation of network capacity and prioritization of mission-critical surveillance. Some Axis network video products support QoS.



The above is an example of a QoS aware network, where Router 1 has been configured to devote a certain amount of maximum bandwidth usage to streaming video, FTP traffic, and HTTP and all other traffic. The maximum usage applies only when there is congestion on the network. If there is unused bandwidth available, any type of traffic can take advantage of it. (In an ordinary or non-QoS network, there is no reserved bandwidth usage for different types of traffic, so when there is network congestion, there is no guarantee that video streams will be able to maintain the desired frame rate.)

8.c Server considerations

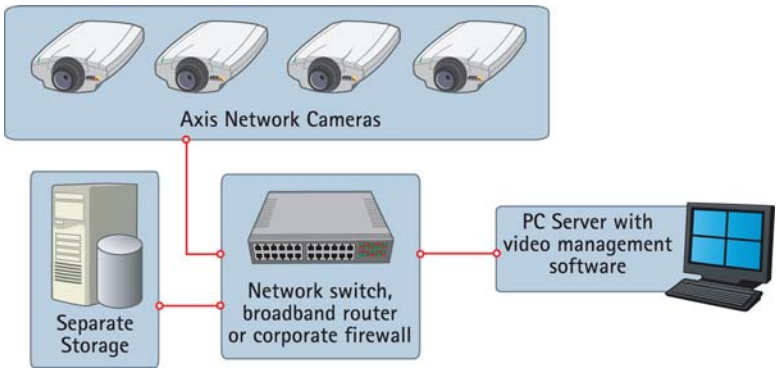
If you are adding more cameras, you should monitor the server's CPU usage so that it doesn't exceed limitations. One hard disk is suitable for storing recordings from six to eight cameras. With more than eight cameras, at least two hard disks should be used to split the load. For 25 or more cameras, the use of a second server is recommended. The AXIS Camera Station Client will be able to switch between different AXIS Camera Station servers.

No. of cameras	Considerations
1 to 8	1 disk
9 to 16	2 disks
17 to 25	3 disks
25+	2 servers

For more information, please refer to the hardware recommendation sheet on page 32

8.d Storage considerations

When the amount of stored data and management requirements exceed the limitations of a direct attached storage, a network-attached storage (NAS) or storage area network (SAN) allows for increased storage space, flexibility and recoverability.



Network-attached storage

NAS provides a single storage device that is directly attached to a LAN and offers shared storage to all clients on the network. A NAS device is simple to install and easy to administer, providing a low-cost storage solution. However, it provides limited throughput for incoming data because it has only one network connection, which can become problematic in high-performance systems.

SANs are high-speed, special-purpose networks for storage, typically connected to one or more servers via fiber. Users can access any of the storage devices on the SAN through the servers, and the storage is scalable to hundreds of terabytes. Centralized storage reduces administration and provides a high

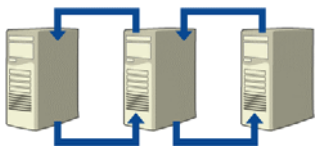
performance, flexible storage system for use in multi-server environments. In a SAN system, files can be stored block by block on multiple hard disks. Technologies such as Fiber Channel are commonly used, providing data transfers at four gigabits per second. This type of hard disk configuration allows for very large and scalable solutions where large amounts of data can be stored with a high level of redundancy.

Redundant Storage

SAN systems build redundancy into the storage device. Redundancy in a storage system allows for video, or any other data, to be saved simultaneously in more than one location. This provides a backup for recovering video if a portion of the storage system becomes unreadable. There are a number of options for providing this added storage layer in an IP-Surveillance system, including a Redundant Array of Independent Disks (RAID), data replication, server clustering and multiple video recipients.

RAID -- RAID is a method of arranging standard, off-the-shelf hard drives such that the operating system sees them as one large hard disk. A RAID set up spans data over multiple hard disk drives with enough redundancy so that data can be recovered if one disk fails. There are different levels of RAID - ranging from practically no redundancy to a full-mirrored solution in which there is no disruption and no loss of data in the event of a hard disk failure.

Data replication -- This is a common feature in many network operating systems. File servers in the network are configured to replicate data among each other providing a back up if one server fails.



Server clustering -- A common server clustering method is to have two servers work with the same storage device, such as a RAID system. When one server fails, the other identically configured server takes over. These servers can even share the same IP address, which makes the so-called "fail-over" completely transparent for users.

Multiple video recipients -- A common method to ensure disaster recovery and off-site storage in network video is to simultaneously send the video to two different servers in separate locations. These servers can be equipped with RAID, work in clusters, or replicate their data with servers even further away. This is an especially useful approach when surveillance systems are in hazardous or not easily accessible areas, such as in mass-transit installations or industrial facilities.

The variety of storage options available for IP-Surveillance systems makes it crucial to consider the different ways the information will be used and stored for the long term. As hard drive technology continues to advance, it is important to utilize open standards to ensure that storage is scalable and future proof. In addition, advances in IP-Surveillance, such as intelligent video algorithm, will make it even more critical to select open storage devices that can handle combinations of data from different sources. Storage systems should be able to accommodate new and upcoming applications so that equipment investments are not lost as technology advances.

9 Conclusion

We hope this document has been helpful in providing guidelines for implementing an IP-Surveillance system. While there are many considerations to take into account, it is relatively easy to set up and operate an Axis IP-Surveillance system once you have defined your application requirements and determined the components you require.

Setting up an AXIS IP-Surveillance system – Quick checklist:

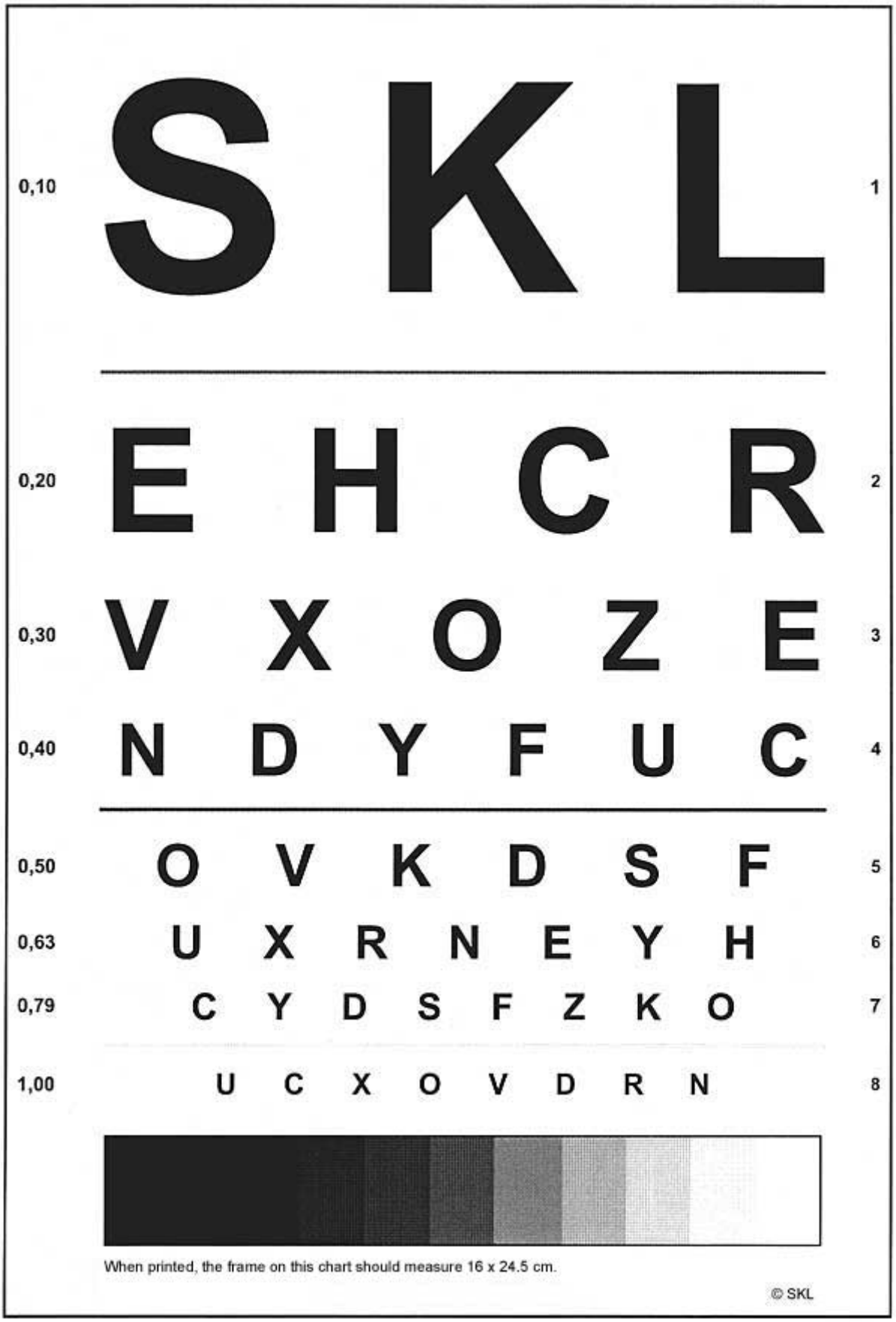
- ❑ Define your surveillance needs
  - o Draw a plan of your installation
  - o Select points of interest to view (area of coverage)
  - o Position each camera: define what you want to be able to capture with each camera
  - o Consider environment: light conditions
  - o Consider cabling to cameras
  - o Position the recording server
- ❑ Network camera and/or video encoder selection
  - o Image quality requirements: resolution, compression and frame rate
  - o Light sensitivity and lens selection (re: camera)
  - o Outdoor/indoor, fixed/PTZ/dome camera
  - o Consider needs such as Power over Ethernet (PoE), video motion detection, audio…
  - o Housing, mounting and other accessories
  - o Buy and try: Buy one camera to test its quality
- ❑ Hardware components
  - o Additional switches (PoE, wireless options)
  - o Additional light sources
  - o Power supplies and eventually UPS
  - o Server for video management software
  - o Hard drives (local disks, SAN, RAID, etc.)
- ❑ Software
  - o Select a software package for your required functionality
  - o Purchase licenses that fit the number of cameras
  - o Specify image quality and frame rate requirements for each camera
  - o IP address range for cameras and servers
  - o Calculate hard disk usage
  - o Configure your cameras and their recording settings
  - o Configure video motion detection settings
  - o Grant user access and authentications
- ❑ Operations and maintenance
  - o Check recorded events for all your cameras
  - o Check motion detection settings again
  - o Check hard disk free space and eventually adjust recording options

10 About Axis

Axis is an IT company offering network video solutions for professional installations. The company is the global market leader in network video, driving the ongoing shift from analog to digital video surveillance. Axis products and solutions focus on security surveillance and remote monitoring, and are based on innovative, open technology platforms.

Axis is a Swedish-based company, operating worldwide with offices in 18 countries and cooperating with partners in more than 70 countries. Founded in 1984, Axis is listed on the Nordic List, Mid Cap and Information Technology exchanges. For more information about Axis, please visit our web site at www.axis.com.

Appendix: Letter chart. (Place the letter chart at the distance where you want an image to be captured. Rows 5 and 6 should be clear for recognition purposes; rows 7 and 8 and most gray shades should be clear for identification purposes.)



Printed with permission from SKL – Statens kriminaltekniska laboratorium