WHITE PAPER

Video data as evidence

Securing video data integrity with AXIS Camera Station

July 2021

AXIS COMMUNICATIONS

Table of Contents

1 Summary

Video data that is of high quality, credible, and not tampered with can be used as evidence. The best practices for handling video data as evidence by using AXIS Camera Station:

- Design, configure, and validate your system properly to provide the image, recording, and security that you want
- Perform regular maintenance
- Handle any evidence according to set procedures

2 Introduction

Surveillance video is practically tailor-made for use as evidence in court. An event caught "on tape", so to speak, can't be denied – or can it? Well, a judge would probably accept video data that is of high quality, credible, and not tampered with.

But there are also cases where the evidential value of video is inadvertently reduced. For example, surveillance footage with time gaps, where people or vehicles suddenly disappear or "jump" in the image, might not be considered sufficiently trustworthy to be used as evidence. Video could also be questioned if its metadata, such as timestamps or the camera's MAC address, doesn't make sense. Any suspicion that video might have been edited, deleted, or tampered with can reduce the video owner's credibility.

This white paper presents advice on how to manage video as evidence. More specifically, it describes the role of the video management software (VMS) AXIS Camera Station in the evidence chain, as well as the role of the video owner.

Figure 1. Video surveillance in strategic places can provide valuable evidence, if correctly set up and managed

3 Best practices for handling video data as evidence

Companies and organizations that use video surveillance need to have processes and procedures in place that determine how to handle and store video data. To be fully prepared for when one of your cameras captures an incident, you need to make sure that video is protected from being overwritten, tampered with, or stolen. It must also be possible to export the footage safely to secure storage and hand it over to law enforcement.

But the production of high-quality video evidence is a process that starts with a purposeful designing of your video system. It is also of the utmost importance that you keep your system up-to-date and keep track of any irregularities. This chapter presents the steps in this process, and how they can be followed with the help of AXIS Camera Station and its toolbox AXIS Camera Station Integrator Suite.

If you produce surveillance video according to these principles about system design, system maintenance, and handling of incidents, it will comply with current cybersecurity requirements and, most probably, provide value as evidence, should that be needed.

Figure 2. AXIS Camera Station software facilitates both the setup, the daily operation, and the strategic management of a video surveillance system

3.1 Design your system properly...

A video surveillance system should be designed with care. You must select equipment according to your needs and set it up to provide the image that you want, the type of recording that you want, and the security that you want. AXIS Site Designer provides significant assistance for these purposes.

3.1.1 To provide the image that you want

The image quality depends on the camera and its placement. The resolution of the image, or more specifically, the pixel density across the scene of events, can be calculated if you know the camera model, lens, and the camera's distance and angle to the scene. For an adequate pixel density across the face of a person in the scene, you may have to deploy more cameras or use cameras with higher resolution. You must investigate the field of view, lighting requirements, and other parameters for specific cameras on your specific site. This can all be smoothly designed in AXIS Site Designer.

3.1.2 To provide the recording that you want

For recording your video, you should use high-performing, validated hardware with redundancy. To increase system reliability, AXIS Camera Station supports fail-over recording by temporarily storing images on the network camera SD card. If you use VMD (video motion detection) analytics, make sure that recordings become long enough to provide value in verifying the whole incident. Motion detection recording that

is not optimally calibrated may exhibit time gaps and disjointed footage. Continuous recording may be a better choice in many cases, but it requires a lot more storage as well as a constant availability of sufficient bandwidth.

3.1.3 To provide the security that you want

You should provide the system with the physical security needed to prevent unauthorized access. All hardware elements, including cameras, network equipment and cables, servers, data storage, power devices, and cables should be protected. Security measures could include keeping the server room a restricted-access area, locking the server cabinet, racking the server in the cabinet, disabling physical ports on the server, and keeping network cables unexposed.

You should also strive to provide the system with the cybersecurity needed to minimize the risks of data abuse, data tampering attempts, and malicious attacks. So-called hardening can be partly provided by software tools and technology, which ensures that the system meets current security standards. But hardening also requires the owner of the system to apply a cybersecurity mindset and work actively to propagate it in the organization. For example, all users of the system must be aware of the importance of using strong, hard-to-guess passwords and be careful not to reveal them. User accesses should also be minimized, as well as user permissions, for instance by using the least-privileged user accounts approach. It is the responsibility of the owner of the system to educate their personnel about best practices and ensure that these are successfully implemented. An authorized integrator can harden the system, but some cybersecurity measures can be effective only with the active cooperation of the people using the system.

One important way to reach overall increased cybersecurity is to protect your video using encrypted data transport. For data transport between the client and the server, AXIS Camera Station uses AES encryption for video, audio, and metadata and TLS 1.2 encryption for other data. AXIS Camera Station can be configured to also encrypt, via HTTPS, the data streams between the cameras and the server. Other best practices for protecting software includes the disabling of any unused services, using IP/MAC address filtering, accommodating IEEE 802.1X, accommodating SNMP monitoring, setting the correct date and time along with a trusted NTP server (to secure the accuracy of timestamps in your video metadata), and using only Axis Secure Remote Access for remote connections (instead of port forwarding or remote desktop). For detailed cybersecurity measures and recommendations, see Axis cybersecurity hardening guide.

3.1.4 Configure and validate your system

It is possible to configure key parts of the system already when designing it using AXIS Site Designer, with specific camera names, resolutions, and retention times. When your system is designed and installed, configurations set in AXIS Site Designer can be automatically imported to AXIS Camera Station, from where you can continue to tweak and adjust the settings if desired.

After actual installation is completed you can validate your system using AXIS Installation Verifier, which is part of the AXIS Camera Station Integrator Suite. The installation verifier tests the system in normal mode as well as night mode, to verify that there is sufficient bandwidth during low-light operation when noise levels are higher and more bandwidth is needed. AXIS Installation Verifier then performs a stress test by steadily increasing the data volume generated in the system until the first bottleneck is found. This will reveal the system spare capacity and indicate if system improvements are needed.

3.2 Perform regular maintenance

When your system is up and running, you need to keep monitoring and updating it.

Make sure that hardware, as well as software, keeps performing as expected. Inspect the video quality, clean the camera lenses according to a schedule, check that there has been no physical tampering and

that the field of view and direction of the cameras remain the way they should. Study system logs on a regular basis, since they provide information about logins, connections, and device issues. AXIS Camera Station provides notifications upon many discovered irregularities and records them in the system logs. Forward logs to read-only remote storage, in particular after any important incident has occurred. Axis also provides an online system health monitoring as part of the Integrator Suite, which allows you to monitor all your installations and provides system status to facilitate service and maintenance.

Both hardware and software (operating system and VMS) should be updated on a regular basis. By always using the latest software and firmware versions, your system will benefit from the latest security patches and bug fixes. Ideally, the VMS finds all software and firmware updates automatically, and either prompt the update installation, or just update automatically. Any software that you download should come from trusted sources.

3.3 Handle any evidence according to set procedures

If you have applied the principles about designing and maintaining your surveillance system properly, AXIS Camera Station should be able to provide credible evidence of any incidents captured by your cameras. Then, you need to have procedures in place for how to proceed.

You must follow any advice from law enforcement. In case of a serious crime, the law enforcement organization in charge has the right to decide how evidence should be protected, and you need to follow their instructions.

In other cases, the main process is to securely export the evidence. This means to be able to provide it outside of your system in the same untampered form, with preserved credibility, as inside.

The exporting should be handled by a designated operator, preferably together with a witness. This operator could be an external professional, hired solely for the purpose of providing and documenting a credible export. Using a third, independent party for the export could minimize the risk for the video owner of being suspected of tampering with the evidence. The operator must make sure to export video that covers the actual incident but also provides enough information about any events leading up it, as well as any aftermath.

The selected video clips can be exported to read-only disks, such as CD-R, DVD-R or Blu-ray (-R), which can then be handed to law enforcement. An alternative is to export the video clips to zip files with encryption and password protection. The files can be digitally signed with a signature that is hashed with the user's password. To confirm the hash and check with the file's current hash, the signature must be entered in AXIS File Player. If the hashes match, no data has been changed in that file.

Axis also provides AXIS Camera Station Incident Report, which functions as an advanced export tool for operators. The tool must be set up in advance, by an administrator providing data such as incidents tags and export location. The Incident Report then automates the exporting, allowing to export videos organized in incidents, using tags as folder names. The location might be set to a local resource, for example network-attached storage (NAS) or a remote resource, for example cloud storage if that is accessible via SMB protocol. The report will consist of video files, snapshots in .jpg (created in AXIS Camera Station manually by the operator when convening the report), bookmarks in .txt, and all information gathered in a report in .pdf format.

4 Cybersecurity resources

Axis applies cyber hardening in the design, development, and testing of devices to minimize the risk of flaws that could be exploited in an attack. We follow industry best practices in cybersecurity, for example

regarding the management of security vulnerabilities, the requirements for safe data transmission and storage, and encryption. We strive to make it easy and cost-efficient for you to apply the appropriate security controls, and our devices support encryption and security management.

While Axis as a manufacturer and provider of the system makes the best effort to offer the most complete and secure system or solution, you, as the end user, have a large responsibility to apply security best practices on your end. Axis provides several tools, guides, and tutorials to help you. See www.axis.com/cybersecurity, where you can find, for example, hardening guides, security management information, and blog posts about cybersecurity.

T10169774/EN/M2.2/2107

About Axis Communications

Axis enables a smarter and safer world by creating solutions for improving security and business performance. As a network technology company and industry leader, Axis offers solutions in video surveillance, access control, intercom, and audio systems. They are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 4,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden