WHITE PAPER

Identity and access management in video surveillance systems

Axis recommendations

March 2021

Table of Contents

1 Summary

Identity and access management comprises policies for safeguarding that people and systems have the appropriate access to system resources. This includes maintaining integrity over time, for example, ensuring that passwords are not leaked, and that accesses are revoked when no longer needed.

In video surveillance systems, the default approach should be that identity and access management is handled in management software, such as a VMS (video management system) or AXIS Device Manager.

Management software should use an administrator account with its own credentials to access the cameras. This account should be unique and not shared.

Site operators should have individual accounts in the management software, but no individuals should have direct access to the cameras. In case there are very good reasons for allowing direct access to cameras, this should be limited to temporary access.

Furthermore, administrative tasks on a camera should be performed using HTTPS. Video streaming should use HTTPS or SRTP (Secure RTP). A decision to use HTTPS for video streaming should be balanced between the need to protect the video stream and the need to prioritize system performance.

2 Introduction

Identity and access management is about making sure that the right individuals and systems have access to the right system resources. It is a fundamental cybersecurity measure for preventing unauthorized access. One of its main challenges is maintaining integrity over time. This includes ensuring that passwords have not been leaked and that individuals who should no longer have access indeed have their access revoked.

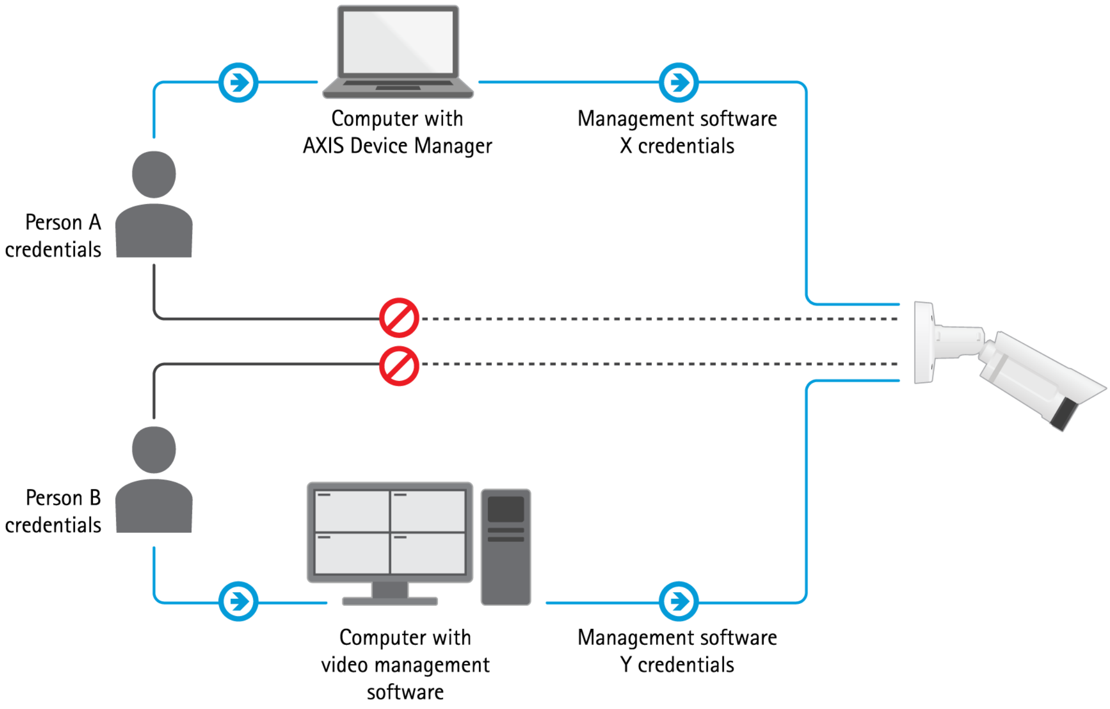
This white paper provides recommendations for identity and access management in video surveillance systems.

3 Background

Identity and access management typically involves *authentication*, *authorization*, and *roles*.

- **Authentication.** Verifying that an entity is who it states to be. Achieved by, for example, using passwords.
- **Authorization.** Controlling which entities are allowed to perform specific functions.
- **Roles.** Grouping of entities based on what they are authorized to do.

4 Management software



In video surveillance systems, identity and access management should primarily be exercised by management software. This could typically be a VMS (video management system) or AXIS Device Manager. Individuals should not have direct access to cameras. The reasons are that, typically:

- identity and access management is easier to handle in management software than in cameras,

- a system often contains many more cameras than instances of management software,
- the management software is on a network and operating system where there is support for IT management practices such as Active Directory, and
- individuals need direct access to the management software but not to the cameras.

Exceptions from this general approach may be needed in various situations or systems, but management via software should be the default solution if there are no strong reasons against it.

5 Authentication

The default authentication mechanism in Axis cameras is Digest Authentication using passwords.

All administrative tasks on a camera should be performed using HTTPS. To be able to use HTTPS, devices require firmware 5.70 (or a later version) for cameras, or 1.25 (or a later version) for access control products and audio products. Devices with firmware 7.20 and onwards are pre-configured with a self-signed certificate but it is recommended to replace this certificate with a CA-signed certificate. For more details about HTTPS certificate management, see: *https://www.axis.com/files/tech_notes/adm_https_cert_guide_en.pdf*

The decision to use HTTPS for video streaming is based on a balance between the need to protect the video stream and the need to prioritize system performance. If available, SRTP (Secure RTP) can be used for secure video streaming. If neither SRTP nor HTTPS is used for video streams, then Digest Authentication is used. Basic authentication should never be allowed. For more on authentication, see Axis Hardening guide.

5.1 Password policies

Different sites and organizations can have different policies, including password policies. The setup of the system should accommodate these policies.

Typically, each management software should have its own credentials (user and password) to devices. Site operators should also have individual accounts in the management software. This is important to maintain proper identity management and it enables adjustments to be made later, when roles might have changed. It is also a way to facilitate the enforcement of additional policies, for example, that passwords must be changed regularly or that reuse of previous passwords is not allowed.

6 Authorization and roles

Axis cameras do support different roles like Administrator, Operator, and Viewer, with different authorization levels. However, management software should use an administrator account to access the cameras. This account should be unique and not shared. Ideally, the password for this account should be generated by the management software itself and remain unknown to all individuals.

Management software should not use the default root account. This account can be used as a backup account by the system owner - use strong passwords that are stored safely and never shared. In systems with a policy to not allow default users, the root account should be "locked" by setting the password to a strong random password which is then discarded.

7 If direct access to cameras is needed

If there are reasons for allowing direct access to cameras, this should preferably be limited to temporary access. A new user account should be created on the camera with the appropriate role for what needs to be done. Once the direct access is no longer needed, this user account should be deleted.

T10165828/EN/M1.3/2103

About Axis Communications

Axis enables a smarter and safer world by creating network solutions that provide insights for improving security and new ways of doing business. As the industry leader in network video, Axis offers products and services for video surveillance and analytics, access control, intercom and audio systems. Axis has more than 3,800 dedicated employees in over 50 countries and collaborates with partners worldwide to deliver customer solutions. Axis was founded in 1984 and has its headquarters in Lund, Sweden.

For more information about Axis, please visit our website *axis.com*.