Application guide

Security control with AXIS Device Manager

Version 1.3

Last updated: June 1, 2023

Table of contents

1. Introduction **3**

1.1 Three layers of cybersecurity protection 3

1.2 Purpose of this document 3

1.3 About AXIS Device Manager 3

2. Device inventory **4**

3. Account and password policy **5**

4. Firmware upgrades **6**

5. Additional hardening **7**

6. Certificate Authority Service **7**

7. Certificate lifecycle management **8**

8. Conclusion **10**

1. Introduction

The importance of cybersecurity continues to increase in the surveillance and security sectors. Effective cybersecurity demands ensuring depth of defense to properly protect your IP network at every level – from the products you choose and the partners you work with to the requirements they – and you – set.

1.1 Three layers of cybersecurity protection

We deliver three layers of cybersecurity protection:

1. Security management: requires applying the security controls you need to mitigate the threats you face. It can be divided in two parts: security controls and cost-effective management. Security controls are safeguards or countermeasures employed to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems or other assets.

2. Vulnerability management: encompasses everything Axis does to apply cybersecurity best practices in the design, development and testing of our products to minimize the risk of flaws that could be exploited. When vulnerabilities are discovered, we manage them; we fix critical vulnerabilities promptly and we issue security advisories.

3. Learning and collaboration: is about Axis, you and the partners involved in your IP network gaining and sharing a clear and common understanding of the threats you face, their potential impacts and how to protect your network.

1.2 Purpose of this document

This application guide describes how AXIS Device Manager can be used to harden your system and increase security. It focuses on key aspects and describes recommendations.

1.3 About AXIS Device Manager

AXIS Device Manager is an on-premise tool that delivers an easy, cost-effective and secure way to manage all major installation, security and maintenance device management tasks (see table below). It is suitable for managing up to a couple thousand Axis devices on one site — or several thousand devices on multiple sites. AXIS Device Manager enables you to efficiently deploy cybersecurity controls to protect your network devices and align them to a security infrastructure.

Device management functions, AXIS Device Manager

Installation	Maintenance
> Assign IP address	> Device status
> Export device list and keep track of assets*	> Collect device data
> User and password management*	> Configure devices and copy configurations to multiple devices
> ACAP management	> Connect to multiple servers/systems
> Upgrade firmware based on LTS or Active*	> Restore points
> HTTPS certificate management*	> Restore factory default settings
> Manage IEEE 802.1 certificates*[1]	> Replace device
> Device tagging	> Certificate renewal and management*
	> Cybersecurity hardening*

**Indicates cybersecurity control function*

[1] *Active Directory Certificate Services not currently supported; validated for FreeRADIUS running on Linux*

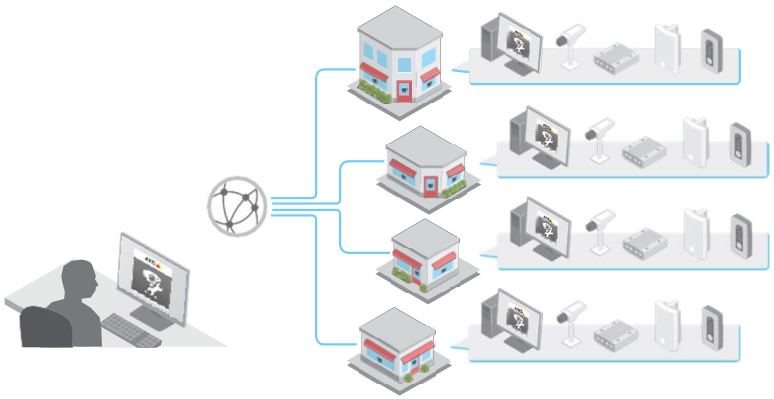


Figure 1. Multi-site management

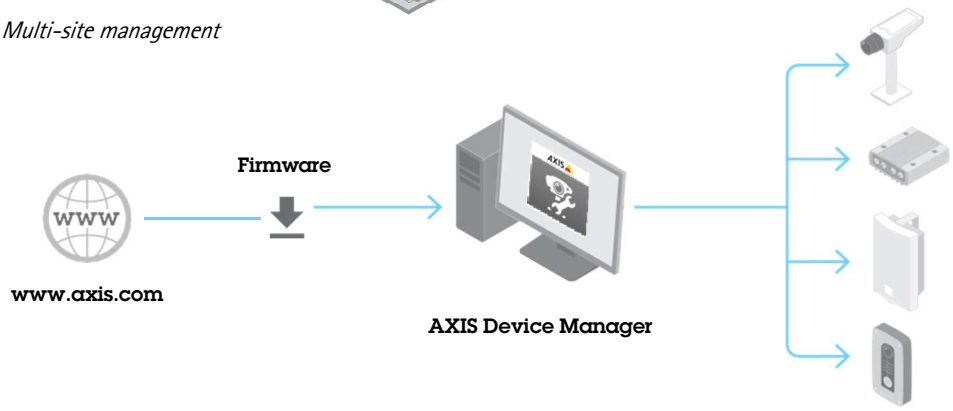


Figure 2. Firmware upgrade

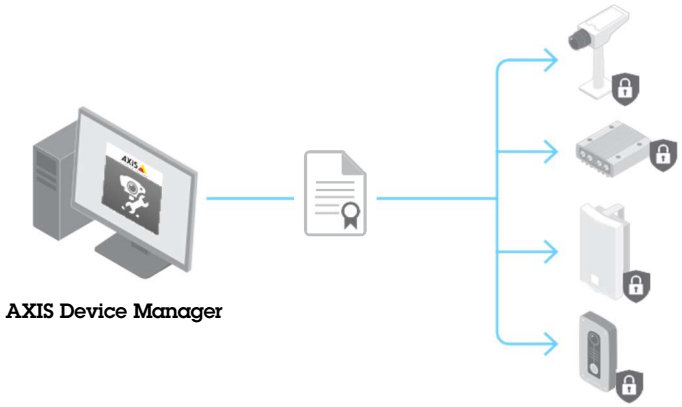


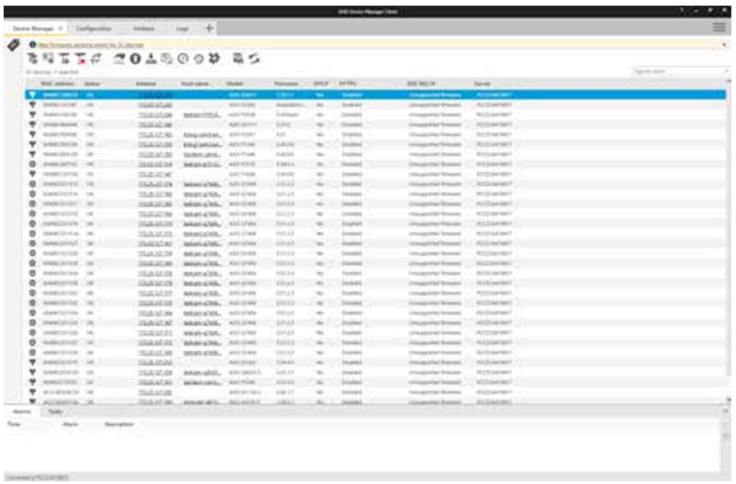
Figure 3. Certificate management

2. Device inventory

A fundamental aspect of ensuring the security of an enterprise network is maintaining a complete inventory of the devices on it. When creating or reviewing an overall security policy, it is important to have knowledge and clear documentation about each device and not just critical assets. That is because any single overlooked device can be a means of entry for attackers. You can't protect devices which you overlook or are not fully aware of.

Device inventory represents an essential step in securing an enterprise network. AXIS Device Manager helps you as it:

> Lets you easily access a current, complete inventory of your network devices when working with audits and incident responders
> Provides a complete list of your devices; sort by: total number, type, model numbers, etc.
> Gives you status of each device on your network



AXIS Device Manager provides a clear view of your inventory of devices.

Recommendations
AXIS Device Manager provides an automated means to gain access to a real-time inventory of Axis network devices. It lets you automatically identify, list and sort your devices. As important, it lets you use tags so that you can group and sort devices based on your own criteria. This makes it easy to gain an overview of and document all Axis devices on your network.

3. Account and password policy

Authentication and privilege control is an important part of protecting network resources. Implementing policy helps reduce the risk of accidental or deliberate misuse over a longer period of time. A key part is to reduce the risk of compromised passwords. Strong passwords are important. However, device passwords can spread within an organization. When they do, you lose control over who may access them. AXIS Device Manager helps you easily manage multiple accounts and passwords for Axis devices.

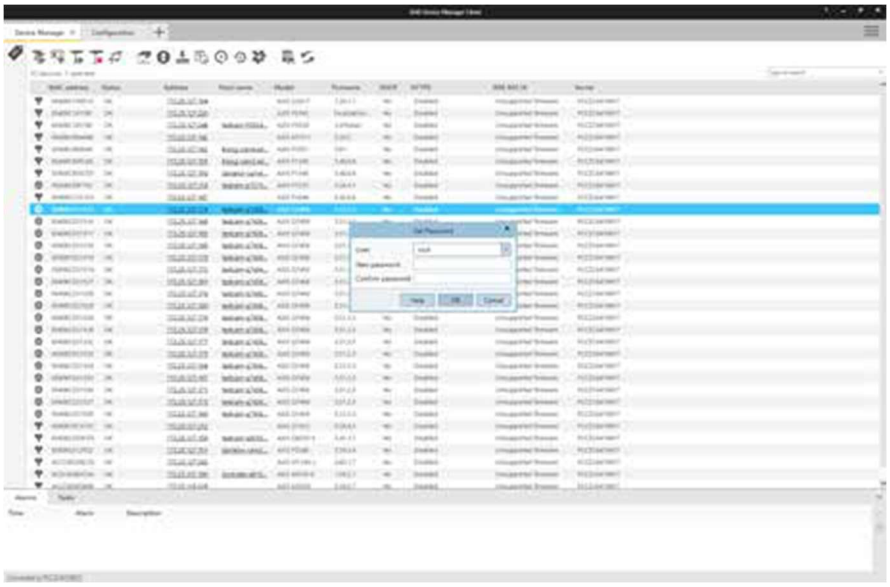
Why you should have more than one user account in devices
> You control privilege levels for different user types (machines and humans)
> You reduce risk of compromising the root (master) password
> You can reset credentials for one user type without impacting other users

Working with privileges in AXIS Device Manager
In AXIS Device Manager, Axis devices can support multiple accounts and belong to three different privileges levels: viewer, operator and administrator. Here is how privileges can be managed for Axis network cameras.

Users with viewer privileges may access video and control PTZ. Those with operator rights may optimize camera settings and video stream profiles. Administrators can administrate accounts, modify network settings and control a number of services in the device. Each role accessing the camera should have its own account.

Recommended steps to follow

> Before adding cameras to the VMS it is recommended to add the cameras to AXIS Device Manager.
> In AXIS Device Manager, select all cameras and create a new user account called "vms" or similar and set a strong password. The privileges need to align with the requirements of the VMS, this may be either operator or administrator (check with manufacturer).
> Add the devices to the VMS with the "vms" account and the password you defined
> Go back to AXIS Device Manager and select all cameras again and reset (change) the "root" account password with a new strong password. The "root" account password should only be known to a limited number of individuals (those who use AXIS Device Manager).
> When someone within the organization needs to use a web browser to access a device for maintenance or troubleshooting tasks, do not give them the root password. Use AXIS Device Manager to create a new (temporary) account for selected device(s) with either administrator or operator privileges. When their task is complete, use AXIS Device Manager to remove the temporary account.
> AXIS Device Manager supports local administrators as well as domain users and groups. You can use a local administrator if the AXIS Device Manager client will only be accessed from the same machine hosting the AXIS Device Manager server. It is recommended to use domain users if the person maintaining the system will use remote clients.



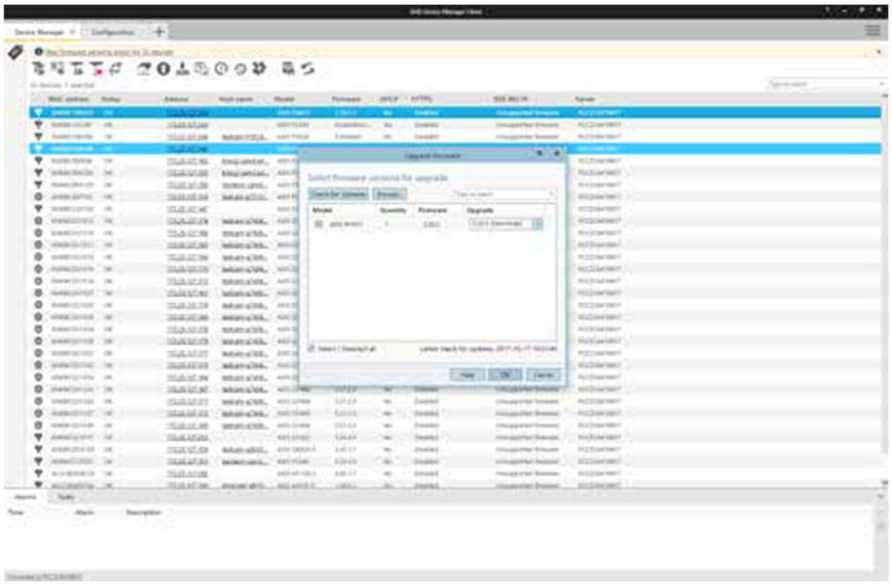
Changing user roles and passwords in AXIS Device Manager.

4. Firmware upgrades

Latest firmware versions include patches for known vulnerabilities. It is essential to always use the latest software because attackers may try to exploit any known vulnerabilities. As important, rapid deployment of new firmware boosts operational capabilities and removes bottlenecks related to manually rolling out new release upgrades. AXIS Device Manager connects to www.axis.com and downloads the latest applicable firmware or service releases. If you prefer to not download directly to your network from the internet, you can save upgrades to an USB stick and then upload them to your AXIS Device Manager client. It also shows if new firmware are available and lets you quickly deploy them on Axis devices.

Why you should always run the latest firmware versions

> Your network and devices are protected with the latest patches against known vulnerabilities, especially critical ones
> Your devices are updated for the latest performance improvements as well as resolve any known bugs or flaws
> You gain immediate access to the latest features and functionality enhancements



Upgrading firmware with AXIS Device Manager is simplified thanks to on-screen notifications and intuitive dialog boxes.

5. Additional hardening

A good user/password policy, as well as running devices with up-to-date firmware versions, will mitigate common risks for devices. The Axis Hardening Guide describes additional measures to reduce risks within large and critical organizations. This includes disabling services that may not be used and enabling services that can help detect and monitor indication of an attack or breach.

AXIS Device Manager simplifies the process of deploying some of these policies. Axis provides a configuration template for basic recommended settings; see more at:

www.axis.com/support/faq//FAQ116386

How to harden devices according to the Axis Hardening Guide

> Download the hardening template configuration file from www.axis.com/files/tech_notes/harden_device_with_AXIS_Device_Manager.zip
> Review the READ_ME.txt file
> Edit configuration file to choose relevant items
> Select devices
> Right-click and select "Configure Devices | Configure..."
> Click "Configuration File" and select the downloaded file
> Adjust settings as needed

6. Certificate Authority Service

Certificate Authority (CA) is a service that issues digital certificates to servers, clients or users. A CA can be public or private. Publicly trusted CAs, such as Comodo and Symantec (formerly Verisign), are typically used for public services such as public web sites and email.

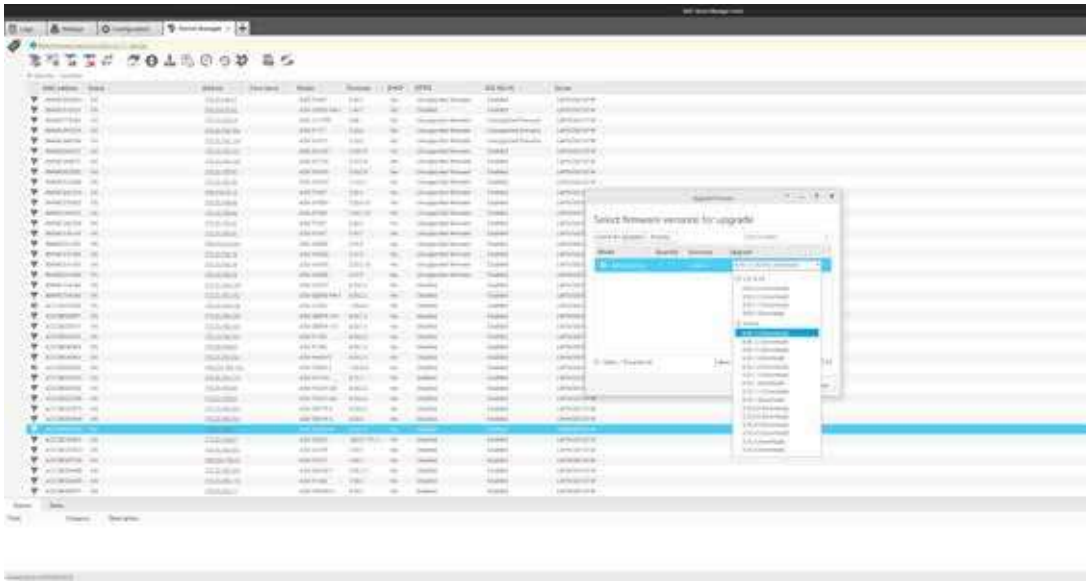
A private CA (typically active directory/certificate service) issues certificates for internal/private network services. In a video management system this is primarily for Hyper Text Transfer Protocol Secure (HTTPS) (network encryption) and IEEE 802.1x (network access control). AXIS Device Manager includes a CA service for Axis devices and can operate as either a private root CA or private intermediate CA; part of an enterprise Public Key Infrastructure (PKI).

CA-signed certificates are used for both IEEE 802.1x (client) and HTTPS (server) certificates.

HTTPS
HTTPS is the secure version of HTTP over which communications between a client and a server are encrypted. Self-signed certificates are sufficient to achieve an encrypted connection. There is no difference in the encryption level between self-signed and CA-signed certificates. The difference is that self-signed certificates do not protect against network spoofing, where an attacking computer tries to impersonate a legitimate server. CA-signed certificates add a trust point for clients to authenticate that it is accessing a trusted device. Note that the video client (VMS) needs to support requesting video over HTTPS (RTP over RTSP over HTTPS) in order to encrypt video.

IEEE 802.1X
Referred to as 802.1X, this standard prevents unauthorized network devices from accessing the local network. A device needs to authenticate itself before it is allowed access to the network (and its resources). There are different authentication methods that can be used, such as: MAC address (MAC filtering), user/password or client certificate. The system owner decides which method to use; the appropriate choice depends on threats, risk, and cost.

Operating an 802.1X infrastructure is an investment. It requires managed switches and additional servers, typically a RADIUS (Remote Authentication Dial-In User Service). Using client certificates requires a CA (private or public) that can issue client certificates. In most cases the infrastructure needs personnel to maintain and monitor it.



Certificate configuration in AXIS Device Manager.

7. Certificate lifecycle management

Certificate lifecycle management is a means of cost-efficiently handling all processes and tasks related to issuing, installing, inspecting, remediating and renewing certificates over a long period of time. AXIS Device Manager enables you to efficiently manage certificates by allowing administrators to:

> Issue CA-signed certificates when no other CA is available
> Easily manage IEEE 802.1X certificates
> Easily manage HTTPS certificates
> Monitor certificate expiration dates
> Easily renew certificates prior to expiration

Recommendations of private root and intermediate CA
It is not recommended to expose Axis devices as public servers targeting the public. That's why using a public CA for private resources is not cost-effective.

For HTTPS, the VMS server is the only client that needs to validate it is accessing a trusted camera. Operator clients will never access the cameras directly as live and recorded video is provided by the VMS server. In this situation there is limited value to incorporate camera server certificates in an existing enterprise PKI.

Using AXIS Device Manager as a private CA is the most cost-effective solution. After a root CA certificate is generated, install the AXIS Device Manager certificate in the VMS server's certificate store. If there are other clients accessing cameras directly (for maintenance or troubleshooting), install the AXIS Device Manager root CA in these clients as well.

For 802.1X, the camera needs a client certificate in order to authenticate itself to a RADIUS server. It is recommended to have the administrator for the Enterprise PKI/CA generate an Intermediate CA certificate and export this as a PKCS#12 (P12) certificate that can be installed in AXIS Device Manager.

For support in setting up a FreeRADIUS server, please go to the Technical papers tab at www.axis.com/products/axis-device-manager/support-and-documentation.

Figure 4

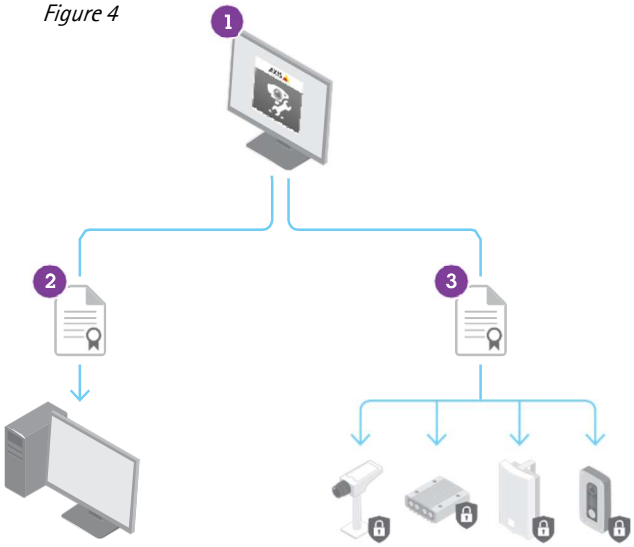


Figure 4, managing HTTPS certificates involves:
1) generating intermediate or root CA certificate in AXIS Device Manager; 2) exporting CA certificate to the VMS, and 3) uploading server certificates to the devices.

Figure 5

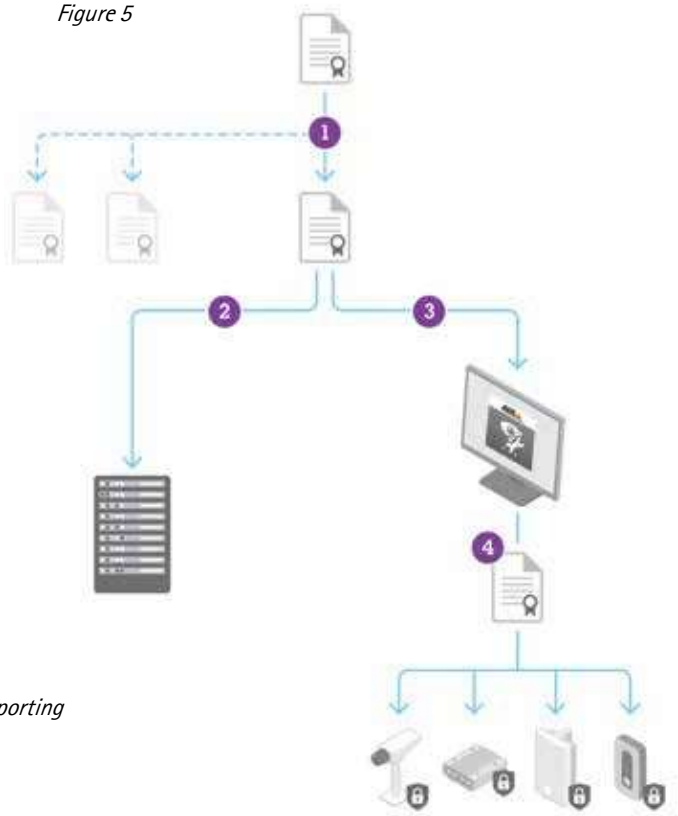


Figure 5, using a Private CA: Managing IEEE 802.1X certificates involves: 1) generating intermediate CA and client certificate; 2) installing CA certificate on the Radius server; 3) importing CA certificate in AXIS Device Manager and 4) uploading CA and client certificates to the devices.

Figure 6

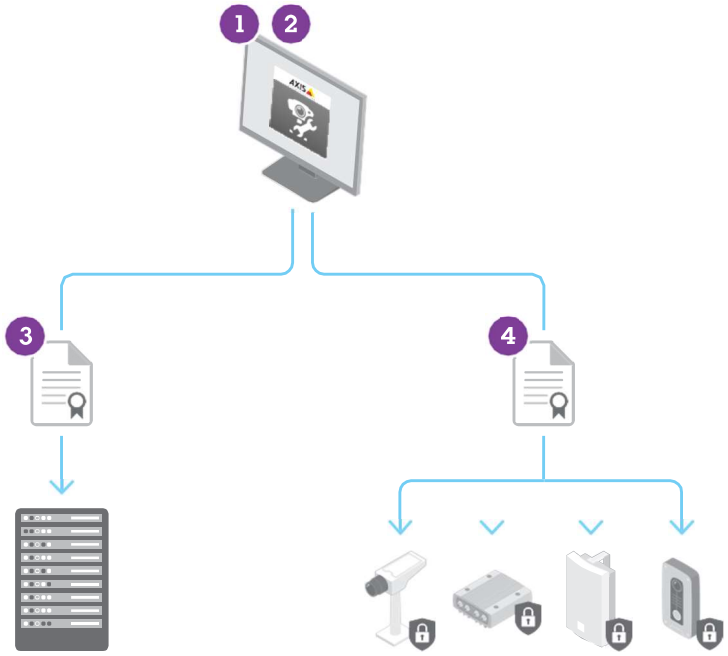


Figure 6, using AXIS Device Manager as a CA: To manage IEEE 802.1X certificates: 1) generate the root CA certificate in AXIS Device Manager; 2) import the authentication CA certificate in AXIS Device Manager; 3) install the CA certificate on the Radius server; 4) upload the CA authentication and client certificates to the devices.

8. Conclusion

Security management and security control are important parts of implementing an effective cybersecurity approach. Each is a continuous process that demands maintaining clear status and following proper actions to mitigate any potential threat that may impact your IP network. AXIS Device Manager offers you a tool to both manage your devices as well as increase the security of your network. Contact your local Axis representative or go to www.axis.com for more information or support.

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, and audio systems. Axis has more than 3,000 dedicated employees in over 50 countries and collaborates with partners worldwide to deliver customer solutions. Founded in 1984, Axis is a Sweden-based company listed on the NASDAQ Stockholm under the ticker AXIS.

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

AXIS COMMUNICATIONS