AXIS Device Manager Security Guide

User manual

Introduction

The importance of cybersecurity continues to increase in the surveillance and security sectors. Effective cybersecurity requires ensuring a sufficient depth of defense to properly protect your IP network at every level, from the products and partners you choose, to the requirements both you and they set.

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

Device lifecycle management

At Axis, we understand the importance of a strong security foundation throughout the device's entire lifecycle. Our commitment to cybersecurity ensures that our products and solutions provide robust protection against potential threats.

Implementation

Axis provides secure-by-design devices with built-in security features, such as secure boot mechanisms, a signed operating system and encrypted storage. Additionally, AXIS Device Manager helps installers and system administrators securely configure and deploy devices, ensuring a secure setup right from the start.

Active service

During the operational phase, Axis offers regular device software updates and security patches to protect against vulnerabilities. AXIS Device Manager also enables remote monitoring and maintenance, allowing for swift issue resolution and minimum downtime. Furthermore, our Hardening Guides provide recommendations for configuring devices to meet specific security requirements.

Decommissioning

When it's time to retire or replace devices, AXIS Device Manager facilitates secure decommissioning by wiping sensitive data and restoring devices to their factory settings. This ensures that no confidential information remains on the device, protecting user data and preventing unauthorized access.

AXIS Device Manager

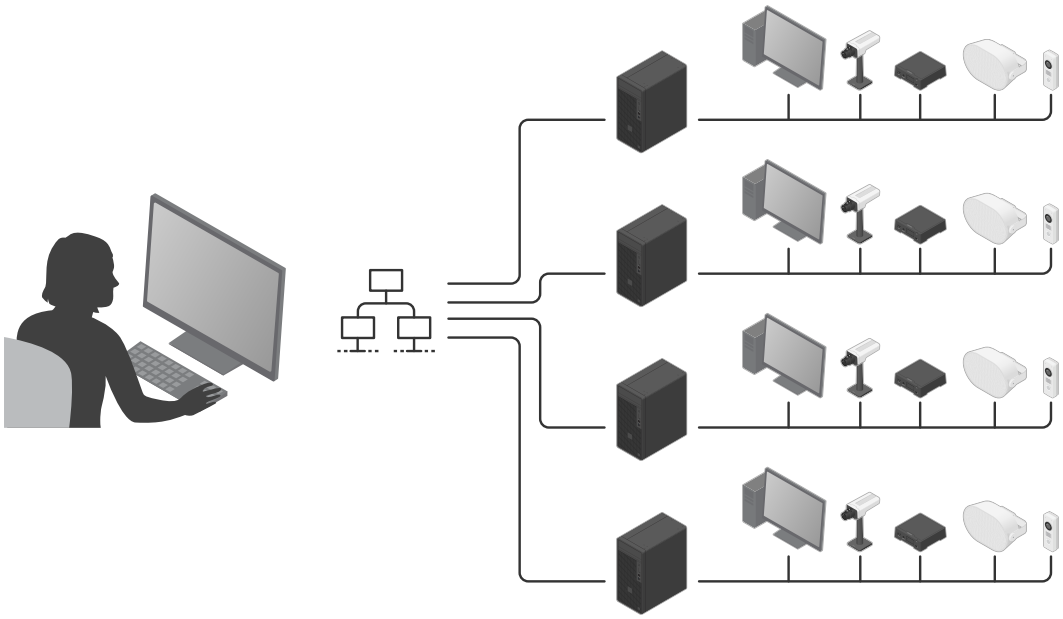
AXIS Device Manager is an on-premises tool that provides an easy, cost-effective and cyber-secure way to manage all major installation, security and maintenance tasks (see the table below). The tool is suitable for managing up to a couple of thousand Axis devices on a single site, or for several thousand devices spread over 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

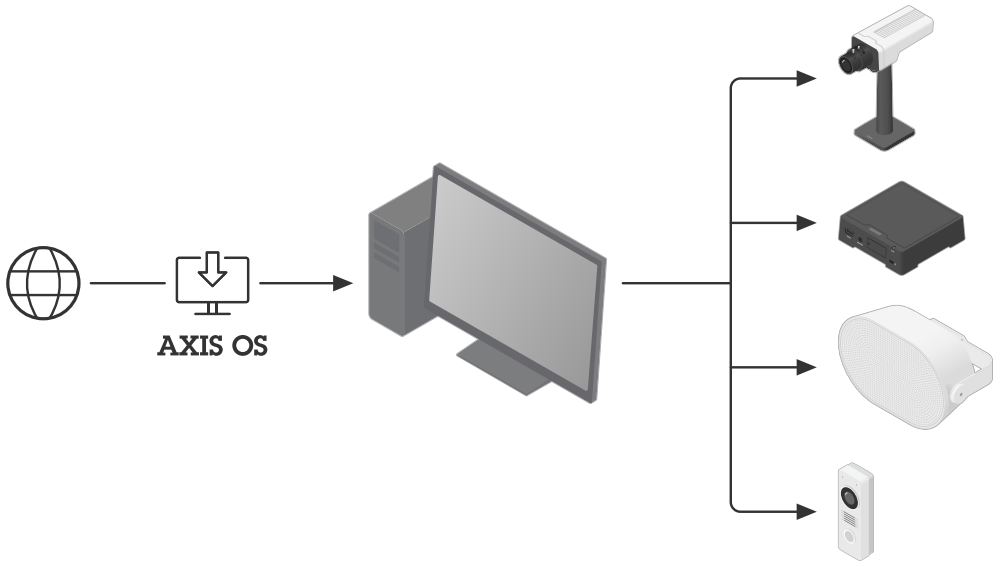
Installation	Maintenance
Assign IP address	Device status
Export device list and keep track of assets*	Collect device data
User and password management*	Configure devices and copy configurations to multiple devices
ACAP management	Connect to multiple servers/systems
Upgrade AXIS OS, based on LTS or Active*	Restore points
HTTPS certificate management*	Restore factory default settings
Manage IEEE 802.1 certificates*/**	Replace device(s)

Device tagging	Certificate renewal and management*
	Cybersecurity hardening*

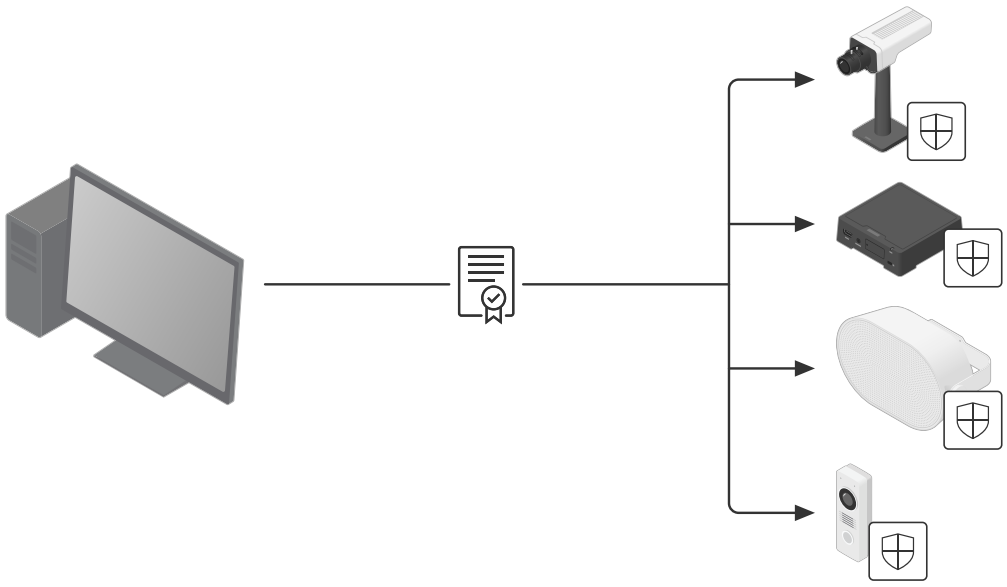
* Indicates cybersecurity control function.
** Active Directory Certificate Services not currently supported. Validated for FreeRADIUS running on Linux.



Multi-site management.



AXIS OS upgrade.



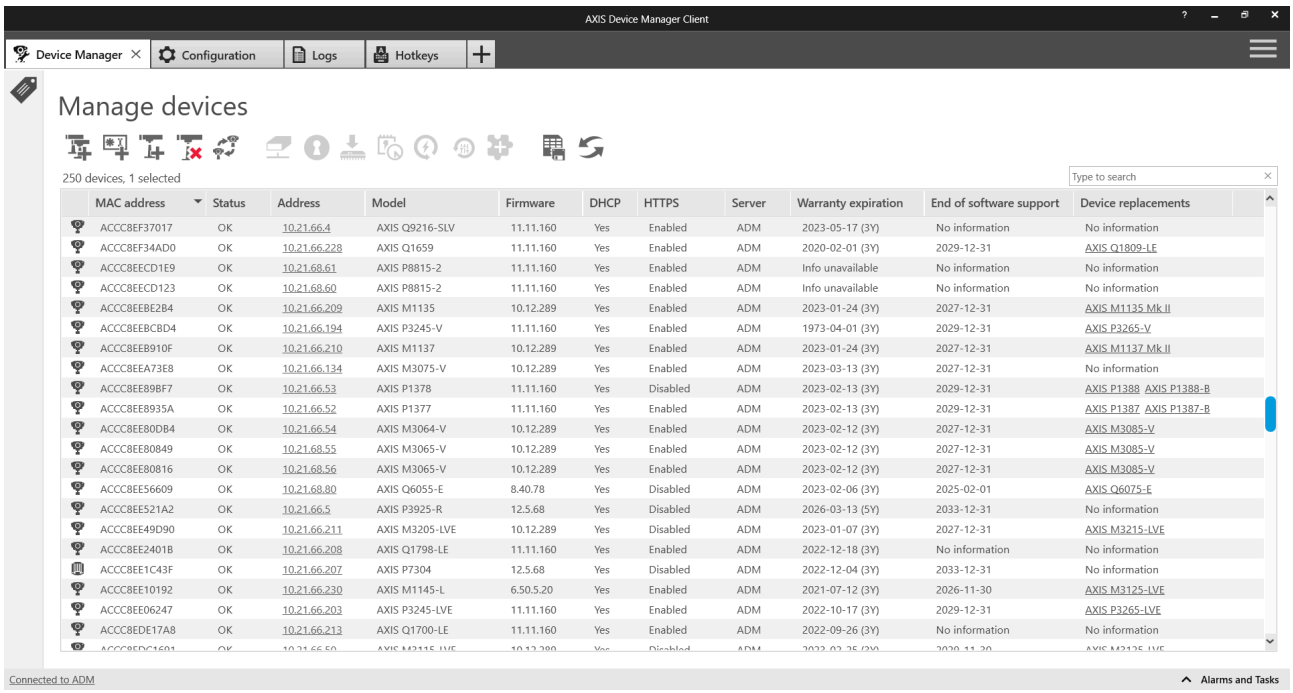
Certificate management.

Device inventory

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

A device inventory represents an essential step in securing an enterprise network. AXIS Device Manager can help you here, as it:

- Gives you easy access to a current, complete inventory of your network devices when working with audits and incident responders.
- Provides a complete list of your devices, which can be sorted by total number, type, model numbers, etc.
- Gives you the status of every device on your network.
- Helps you plan ahead, by showing when device software support is scheduled to end, as well as listing which newer product(s) can be used as replacements.



MAC address	Status	Address	Model	Firmware	DHCP	HTTPS	Server	Warranty expiration	End of software support	Device replacements
ACCC8EF37017	OK	10.21.66.4	AXIS Q9216-SLV	11.11.160	Yes	Enabled	ADM	2023-05-17 (3Y)	No information	No information
ACCC8EF34AD0	OK	10.21.66.228	AXIS Q1659	11.11.160	Yes	Enabled	ADM	2020-02-01 (3Y)	2029-12-31	AXIS Q1809-LE
ACCC8EECD1E9	OK	10.21.68.61	AXIS P8815-2	11.11.160	Yes	Enabled	ADM	Info unavailable	No information	No information
ACCC8EECD123	OK	10.21.68.60	AXIS P8815-2	11.11.160	Yes	Enabled	ADM	Info unavailable	No information	No information
ACCC8EEBE2B4	OK	10.21.66.209	AXIS M1135	10.12.289	Yes	Enabled	ADM	2023-01-24 (3Y)	2027-12-31	AXIS M1135 Mk II
ACCC8EEBCBD4	OK	10.21.66.194	AXIS P3245-V	11.11.160	Yes	Enabled	ADM	1973-04-01 (3Y)	2029-12-31	AXIS P3265-V
ACCC8EEB910F	OK	10.21.66.210	AXIS M1137	10.12.289	Yes	Enabled	ADM	2023-01-24 (3Y)	2027-12-31	AXIS M1137 Mk II
ACCC8EEA73E8	OK	10.21.66.134	AXIS M3075-V	10.12.289	Yes	Enabled	ADM	2023-03-13 (3Y)	2027-12-31	No information
ACCC8EE89BF7	OK	10.21.66.53	AXIS P1378	11.11.160	Yes	Disabled	ADM	2023-02-13 (3Y)	2029-12-31	AXIS P1388 AXIS P1388-B
ACCC8EE8935A	OK	10.21.66.52	AXIS P1377	11.11.160	Yes	Enabled	ADM	2023-02-13 (3Y)	2029-12-31	AXIS P1387 AXIS P1387-B
ACCC8EE80DB4	OK	10.21.66.54	AXIS M3064-V	10.12.289	Yes	Enabled	ADM	2023-02-12 (3Y)	2027-12-31	AXIS M3085-V
ACCC8EE80849	OK	10.21.68.55	AXIS M3065-V	10.12.289	Yes	Enabled	ADM	2023-02-12 (3Y)	2027-12-31	AXIS M3085-V
ACCC8EE80816	OK	10.21.68.56	AXIS M3065-V	10.12.289	Yes	Enabled	ADM	2023-02-12 (3Y)	2027-12-31	AXIS M3085-V
ACCC8EE56609	OK	10.21.68.80	AXIS Q6055-E	8.40.78	Yes	Disabled	ADM	2023-02-06 (3Y)	2025-02-01	AXIS Q6075-E
ACCC8EE521A2	OK	10.21.66.5	AXIS P3925-R	12.5.68	Yes	Disabled	ADM	2026-03-13 (5Y)	2033-12-31	No information
ACCC8EE49D90	OK	10.21.66.211	AXIS M3205-LVE	10.12.289	Yes	Disabled	ADM	2023-01-07 (3Y)	2027-12-31	AXIS M3215-LVE
ACCC8EE2401B	OK	10.21.66.208	AXIS Q1798-LE	11.11.160	Yes	Enabled	ADM	2022-12-18 (3Y)	No information	No information
ACCC8EE1C43F	OK	10.21.66.207	AXIS P7304	12.5.68	Yes	Disabled	ADM	2022-12-04 (3Y)	2033-12-31	No information
ACCC8EE10192	OK	10.21.66.230	AXIS M1145-L	6.50.5.20	Yes	Enabled	ADM	2021-07-12 (3Y)	2026-11-30	AXIS M3125-LVE
ACCC8EE06247	OK	10.21.66.203	AXIS P3245-LVE	11.11.160	Yes	Enabled	ADM	2022-10-17 (3Y)	2029-12-31	AXIS P3265-LVE
ACCC8EDE17A8	OK	10.21.66.213	AXIS Q1700-LE	11.11.160	Yes	Enabled	ADM	2022-09-26 (3Y)	No information	No information

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

AXIS Device Manager provides the automated means to access a real-time inventory of Axis network devices. It lets you automatically identify, list and sort your devices. Equally importantly, it lets you use tags to group and sort devices based on your own criteria, making it easy to get an overview of and document all the Axis devices on your network.

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 time. Enforcing the use of robust passwords is a key task, but so is reducing the risk of compromised passwords. Device passwords often spread within an organization, and when they do you lose control over who has access to 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 the risk of compromising the root (master) password.
- You can reset credentials for one user type without impacting others.

Working with privileges in AXIS Device Manager

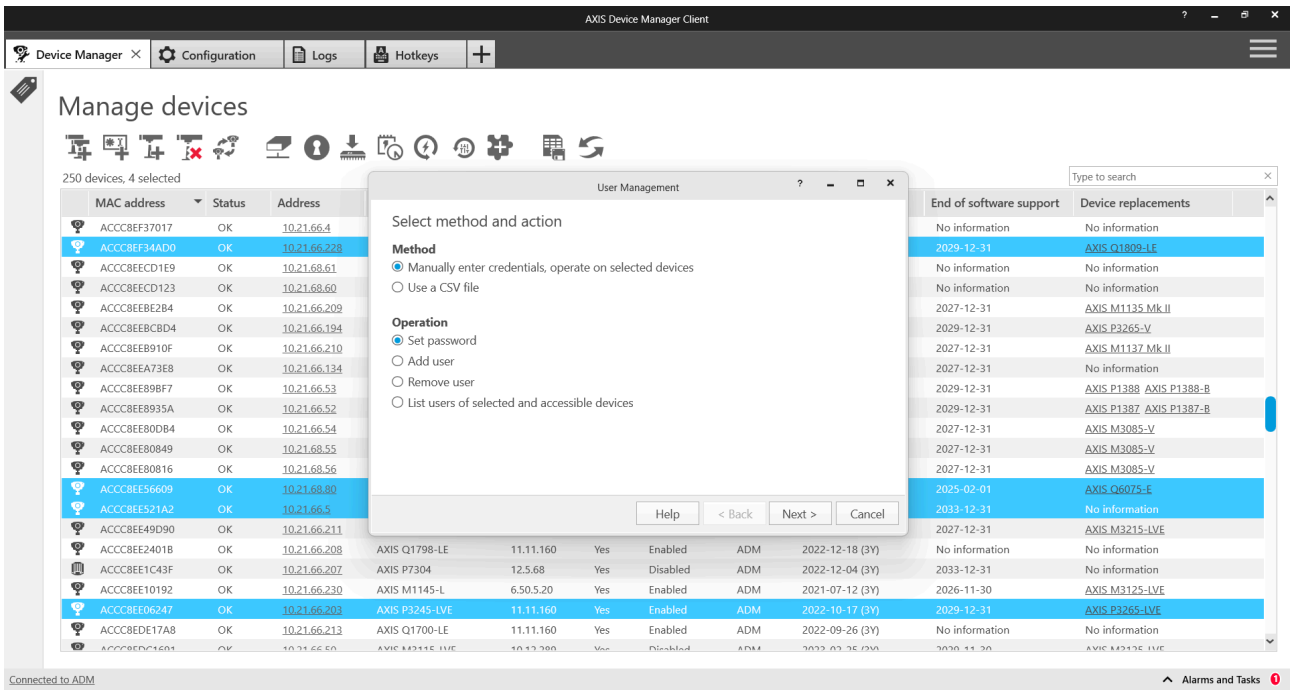
Axis devices support multiple accounts, with each account having one of three different privilege levels:

- **Viewers**: These users have access to video and PTZ control.
- **Operators**: Users with operator rights may optimize camera settings and video stream profiles.
- **Administrators**: Administrators can administer accounts, modify network settings and control a number of services in the device.

Each role accessing the camera should have its own account. For example, you might configure the role "Control room personnel" with the privilege level "operator", whereas the role "Patrolling staff" might only need the privilege level "viewer".

Recommended steps

- Before adding cameras to the VMS – 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 could be either operator or administrator (check with the manufacturer).
- Add the devices to the VMS with the account and password you created.
- Back in AXIS Device Manager – select all the cameras again and reset (change) the "root" account password with a new, strong password. The "root" account password should be known only to a limited number of individuals (those who use AXIS Device Manager).
- When someone needs to use a web browser to access a device for maintenance or troubleshooting tasks, do **not** give them the root password. Instead, use AXIS Device Manager to create a new (temporary) account for the selected device(s), with either administrator or operator privileges. When their work is complete, use AXIS Device Manager to delete 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. We recommend using domain users if the person maintaining the system will be using remote clients.



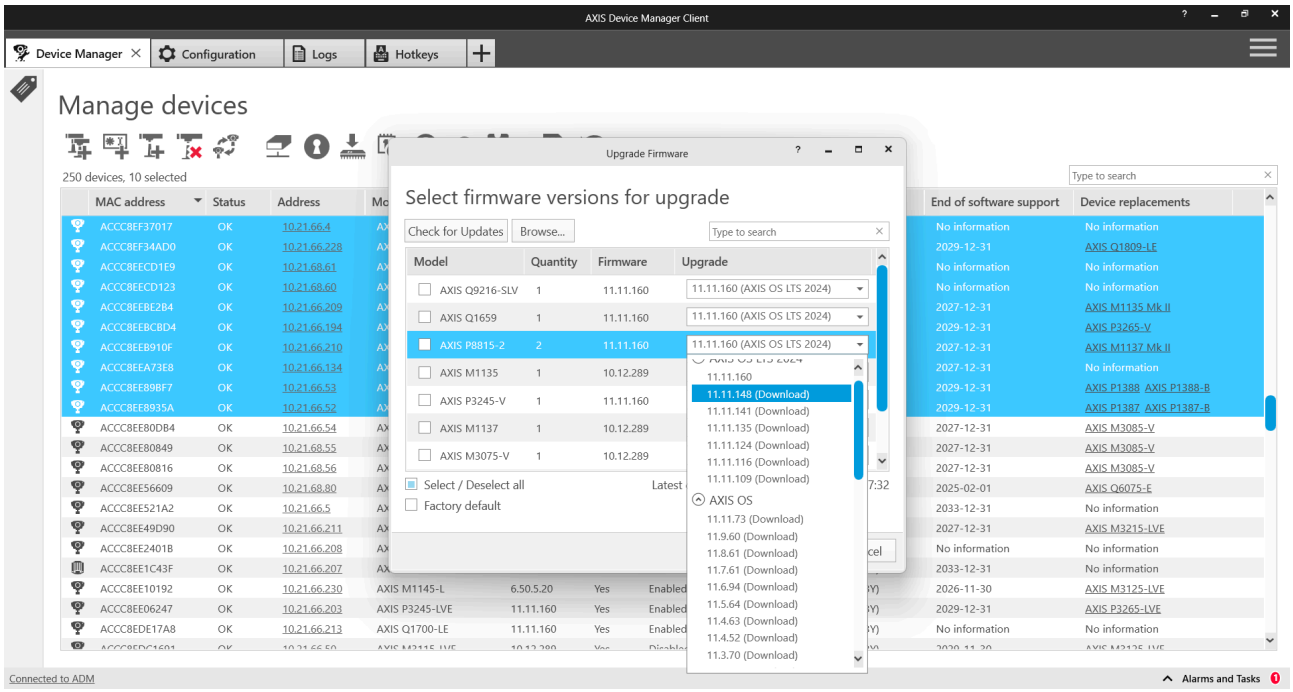
Changing user roles and passwords in AXIS Device Manager.

AXIS OS upgrades

Updated AXIS OS versions include patches for known vulnerabilities. It is essential to always use the latest software because attackers may try to exploit known vulnerabilities. Equally importantly, rapid deployment of a new AXIS OS version 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 AXIS OS 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 AXIS OS versions are available and lets you quickly deploy them on Axis devices.

Why you should always run the latest AXIS OS 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 fixes for bugs and flaws.
- You get immediate access to the latest features and functionality enhancements.



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

Additional hardening

Employing a good user- and password policy, as well as running up-to-date AXIS OS 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.

How to harden devices according to the Axis Hardening Guide:

- Read the *AXIS Hardening Guide* and download the template file at the end of the document.
- Edit the configuration file to select relevant items.
- Select devices in AXIS Device Manager inventory.
- Right-click and select "Configure Devices > Configure..."
- Click "Configuration File" and select the downloaded file.
- Adjust the settings as required.

Certificate Authority Service

A 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 an active directory/certificate service) issues certificates for internal/private network services. In a video management system this is primarily for 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 as a private intermediate CA; as part of an enterprise Public Key Infrastructure (PKI).

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

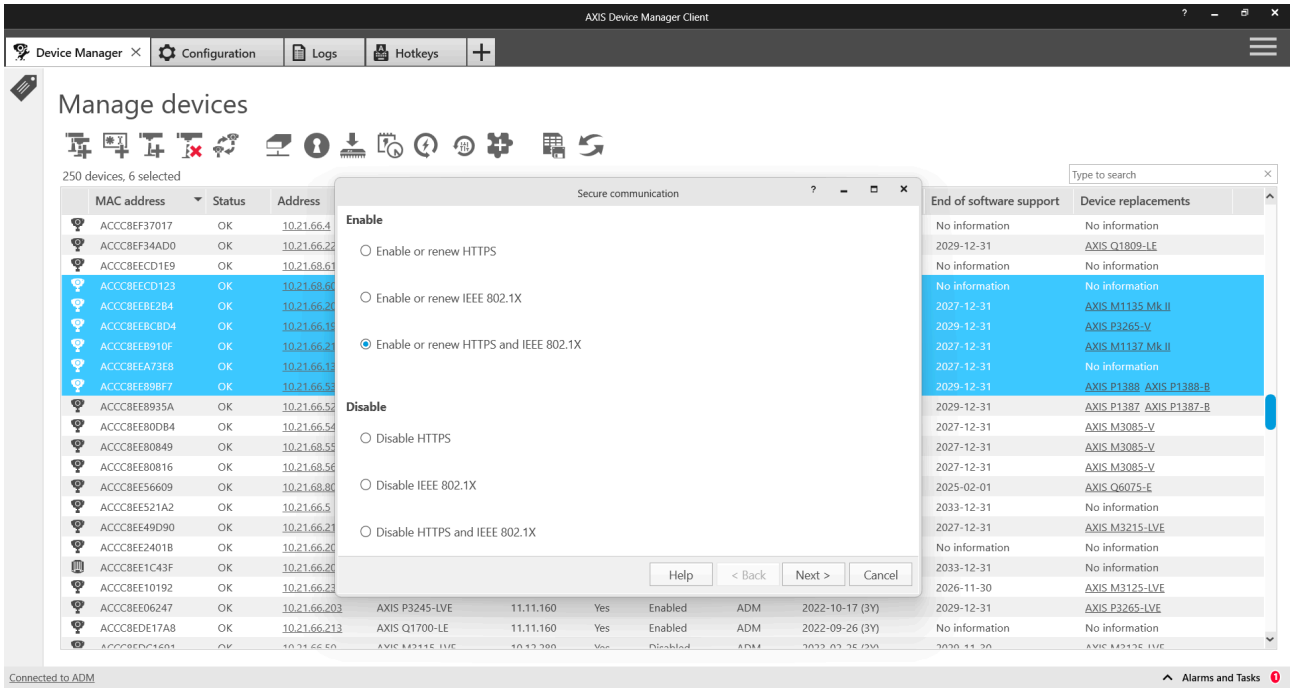
HTTPS

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, in which 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

Often referred to simply 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). Various authentication methods can be used: MAC address (MAC filtering), user/password or client certificate. The system owner decides which method to use; the appropriate choice depending on the threats, risks, and costs.

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 staff to maintain and monitor it.



Certificate configuration in AXIS Device Manager.

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 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 for private root and intermediate CAs

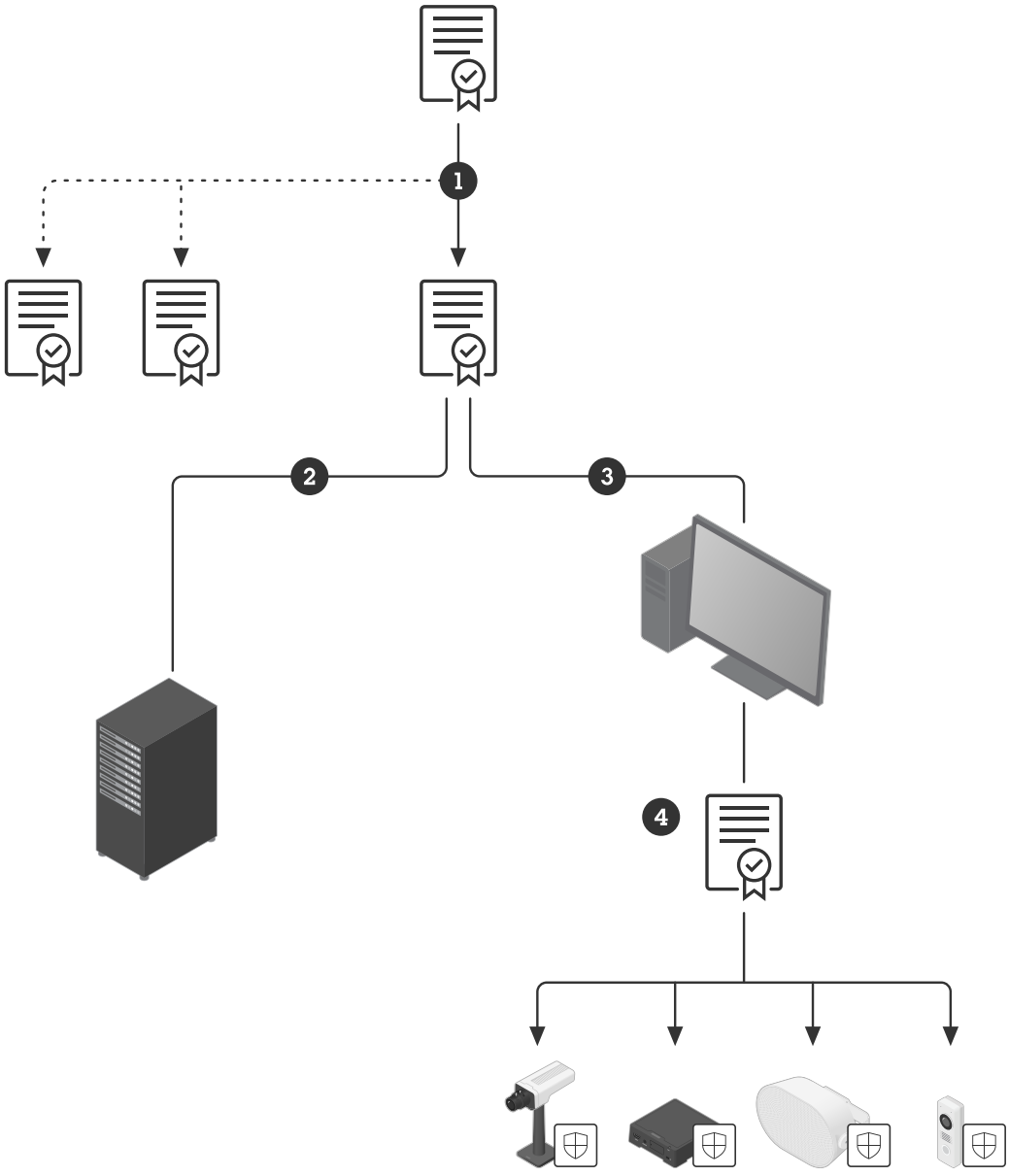
It is not recommended to expose Axis devices as public servers targeting the public. This is why using a public CA for private resources is not cost-effective.

For HTTPS, the VMS server is the only client that needs to validate that 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 in incorporating camera server certificates in an existing enterprise PKI.

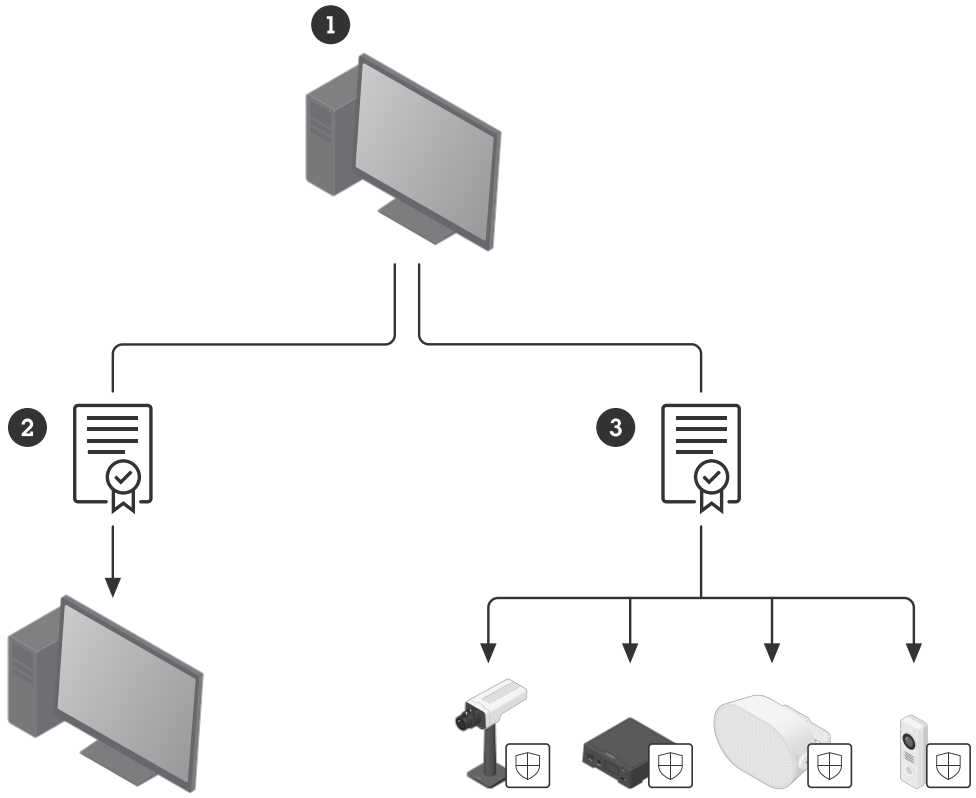
Using AXIS Device Manager as a private CA is the most cost-effective solution. After a root CA certificate is generated, install the AXIS Device Manager certificate in the VMS server's certificate store. If there are other clients accessing cameras directly (for maintenance or troubleshooting), install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

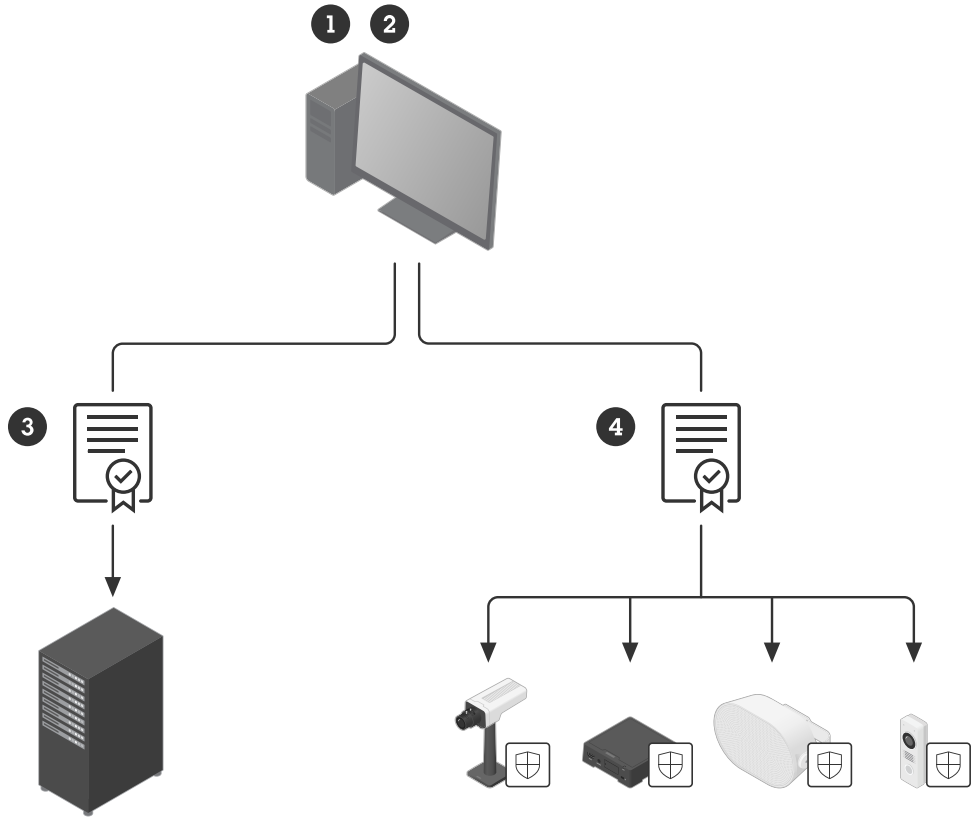
For support in setting up a FreeRADIUS server, please visit the *Technical papers section* for AXIS Device Manager



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.



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.



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.

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.

T10231485

2025-08 (M1.5)