# AXIS Device Manager

Benutzerhandbuch

# Einführung

Die Cybersicherheit gewinnt in den Bereichen Überwachung und Sicherheit zunehmend an Bedeutung. Eine wirksame Cybersicherheit erfordert eine ausreichende Verteidigungstiefe, um Ihr IP-Netzwerk auf jeder Ebene angemessen zu schützen, angefangen bei den von Ihnen ausgewählten Produkten und Partnern bis hin zu den von Ihnen und den Partnern festgelegten Anforderungen.

Diese Übersicht beschreibt, wie Sie AXIS Device Manager verwenden können, um Ihr System zu härten und die Sicherheit zu erhöhen. In diesem Dokument werden die wichtigsten Punkte vorgestellt und Empfehlungen erteilt.

## Lebenszyklus-Management für Geräte

Wir bei AXIS wissen, wie wichtig eine solide Sicherheitsgrundlage während des gesamten Lebenszyklus eines Geräts ist. Unser Engagement für Cybersicherheit sorgt dafür, dass unsere Produkte und Lösungen einen zuverlässigen Schutz vor potenziellen Bedrohungen bieten.

### Implementierung

Axis bietet Secure-by-Design-Geräte mit integrierten Sicherheitsfunktionen wie Secure Boot-Mechanismen, einem signierten Betriebssystem und verschlüsseltem Speicher. Darüber hinaus unterstützt AXIS Device Manager Installateure und Systemadministratoren bei der sicheren Konfiguration und Bereitstellung von Geräten und gewährleistet ein sicheres Setup von Anfang an.

### Aktive Wartung

Während der Betriebsphase bietet Axis regelmäßige Aktualisierungen der Gerätesoftware und Sicherheits-Patches zum Schutz vor Schwachstellen. AXIS Device Manager aktiviert auch die Fernüberwachung und -wartung und ermöglicht so eine schnelle Auflösung von Problemen und minimale Ausfallzeiten. Darüber hinaus bieten unsere Härtungsleitfäden Empfehlungen für die Konfiguration von Geräten zur Erfüllung bestimmter Sicherheitsanforderungen.

### Außerbetriebnahme

Wenn es an der Zeit ist, Geräte auszumustern oder zu ersetzen, erleichtert der AXIS Device Manager die sichere Außerbetriebnahme, indem er sensible Daten löscht und die Geräte auf ihre Werkseinstellungen zurücksetzt. Dadurch wird sichergestellt, dass keine vertraulichen Informationen auf dem Gerät verbleiben, die Benutzerdaten geschützt werden und ein unbefugter Zugriff verhindert wird.

## AXIS Device Manager

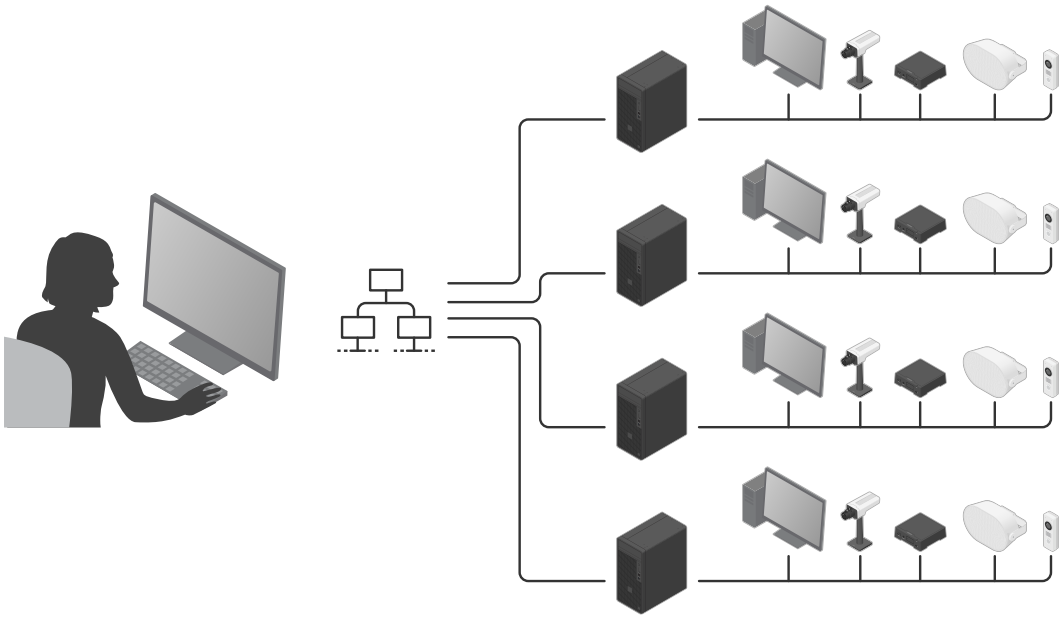
Der AXIS Device Manager ist ein am Standort eingesetztes Tool, mit dem sich schnell, kostengünstig und cybersicher alle wichtigen Verwaltungsaufgaben in den Bereichen Installation, Sicherheit und Wartung durchführen lassen (siehe die folgende Tabelle). Das Tool eignet sich für die Verwaltung von bis zu einigen Tausend Axis Geräten an einem einzigen Standort oder für mehrere Tausend Geräte, die über mehrere Standorte verteilt sind. AXIS Device Manager ermöglicht die effiziente Implementierung von Cybersicherheitskontrollen, um Ihre Netzwerkgeräte zu schützen und sie an eine Sicherheitsinfrastruktur anzugleichen.

**AXIS Device Manager – Geräteverwaltungsfunktionen**

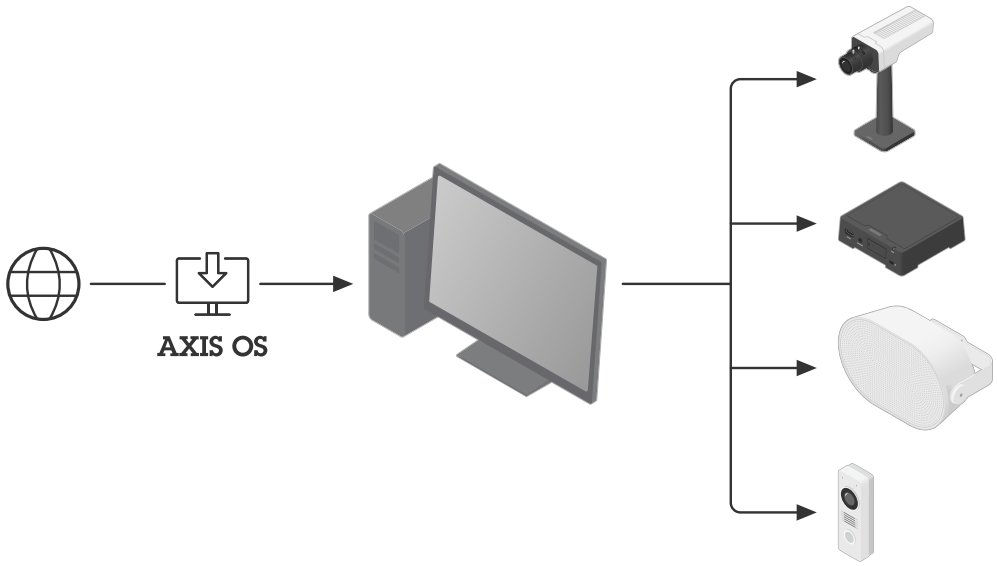
| Installation | Wartung |
|---|---|
| Zuweisen einer IP-Adresse | Gerätestatus |
| Gerätelisten exportieren und Inventar nachverfolgen* | Gerätedaten sammeln |
| Benutzer- und Kennwortverwaltung* | Geräte konfigurieren und Konfigurationen zu mehreren Geräten kopieren |
| ACAP-Verwaltung | Verbindung zu mehreren Servern/Systemen herstellen |
| Upgrade von AXIS OS, basierend auf LTS oder Active* | Wiederherstellungspunkte |

| | |
|---|---|
| Verwaltung von HTTPS-Zertifikaten* | Zurücksetzen auf werksseitige Standardeinstellung |
| Verwaltung von IEEE 802.1-Zertifikaten*/** | Geräte ersetzen |
| Geräte-Kennzeichnung | Erneuerung und Verwaltung von Zertifikaten* |
| | Cybersicherheit härten* |

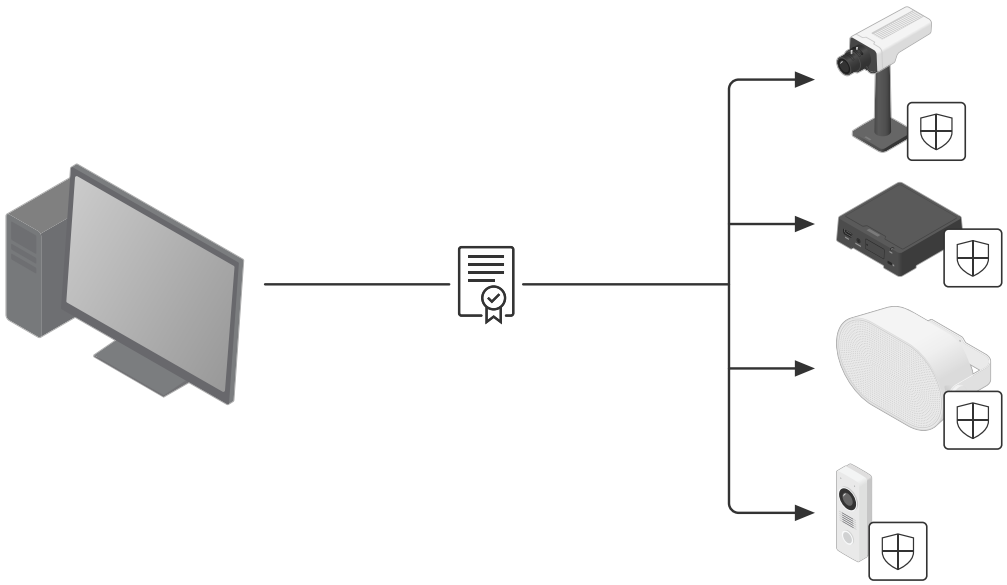
* Funktionsmerkmal der Cybersicherheit.
** Active Directory-Zertifikatsdienste werden derzeit nicht unterstützt. Validiert für FreeRADIUS unter Linux.



*Multisite-Management.*




*AXIS OS-Aktualisierung.*



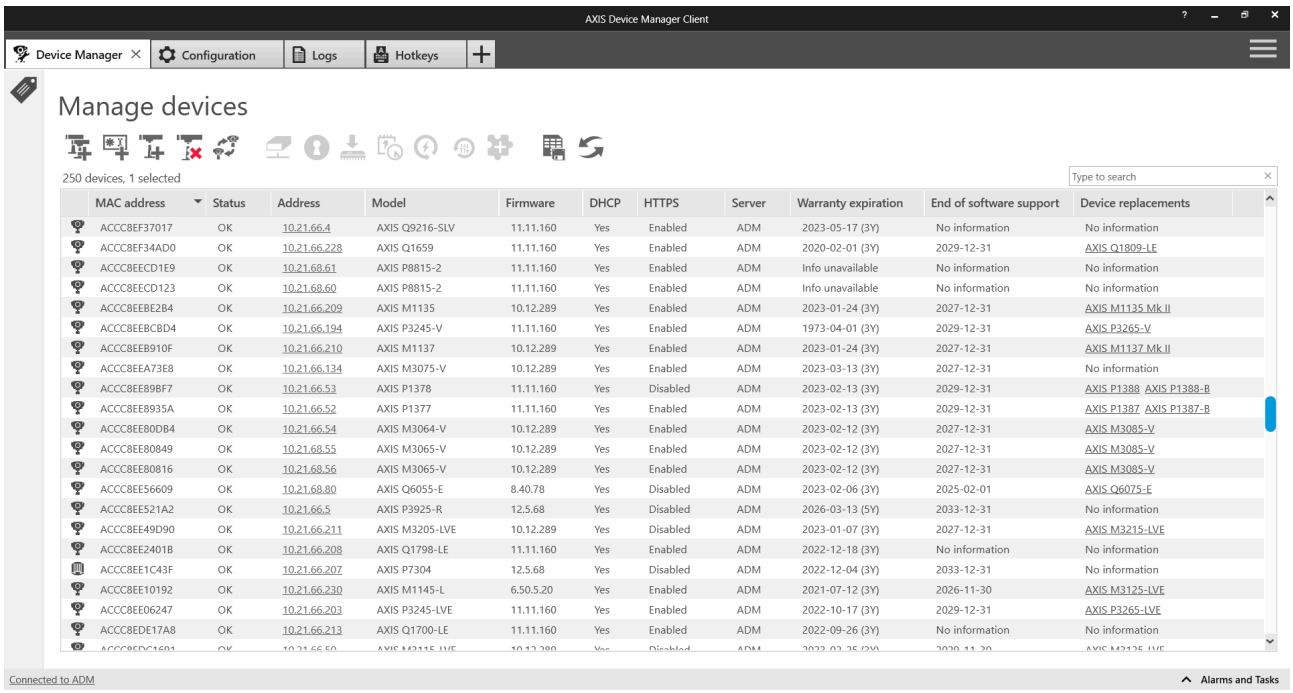
*Zertifikatverwaltung.*

## Geräteinventar

Ein grundlegender Aspekt eines sicheren Unternehmensnetzwerks ist das jederzeit aktuelle und vollständige Geräteinventar. Zum Erstellen oder Überarbeiten von Sicherheitsrichtlinien sind sauber dokumentierte Informationen zu allen Geräten und nicht nur zu kritischen Elementen unerlässlich. Denn bereits ein übersehenes Gerät kann zum kritischen Angriffspunkt werden. Übersehene oder nur halb wahrgenommene Geräte können nicht geschützt werden.

Die Inventarisierung von Geräten ist ein wesentlicher Schritt zur Sicherung eines Unternehmensnetzwerks. AXIS Device Manager kann Ihnen dabei helfen:

- Für Arbeiten mit Prüfberichten und Sicherungsdiensten immer die aktuelle und vollständige Inventarliste Ihrer Netzwerk-Geräte bereitstellt.
- Sie erhalten eine vollständige Liste Ihrer Geräte, sortiert nach: Gesamtzahl, Typ, Modellnummer usw.
- Den Status aller Ihrer Netzwerk-Geräte anzeigt.
- Hilft Ihnen bei der Vorausplanung, indem es anzeigt, wann der Zeitplan für die Unterstützung der Gerätesoftware ausläuft und welche neueren Produkte als Ersatz verwendet werden können.




*Der AXIS Device Manager stellt Ihr Geräteinventar klar und übersichtlich dar.*

Der AXIS Device Manager erstellt automatisch und in Echtzeit Inventare der Axis Netzwerk-Geräte. Er identifiziert und sortiert Ihre Geräte automatisch und stellt sie in Listenform dar. Genauso wichtig ist, dass Sie Geräte mit Hilfe von Tags nach Ihren eigenen Kriterien gruppieren und sortieren können. So können Sie sich leicht einen Überblick über alle Axis Geräte in Ihrem Netzwerk verschaffen und diese dokumentieren.

## Richtlinien für Benutzerkonten und Kennwörter

Die Benutzerauthentifizierung und das Verwalten von Zugriffsrechten sind für den Schutz von Netzwerkressourcen wichtig. Das Umsetzen dieser Richtlinien verringert langfristig das Risiko fahrlässigen oder vorsätzlichen Missbrauchs. Die Verwendung robuster Kennwörter zu erzwingen, ist eine wichtige Aufgabe, aber auch das Risiko kompromittierter Kennwörter zu verringern. Gerätekennwörter werden oft innerhalb einer Organisation weitergegeben, und wenn dies der Fall ist, verlieren Sie die Kontrolle darüber, wer Zugriff darauf hat. AXIS Device Manager hilft Ihnen, mehrere Konten und Kennwörter für Axis Geräte einfach zu verwalten.

**Mehr als ein Benutzerkonto pro Gerät ist wichtig, denn:**

- Die Zugriffsebene lässt sich an den Benutzertyp (Mensch oder Maschine) anpassen.
- Das Root-Kennwort wird besser geschützt.
- Die Zugangsberechtigung für einen Benutzertyp kann ohne Auswirkung auf andere Benutzer zurückgesetzt werden.

**Mit dem AXIS Device Manager mit Zugriffsrechten arbeiten**

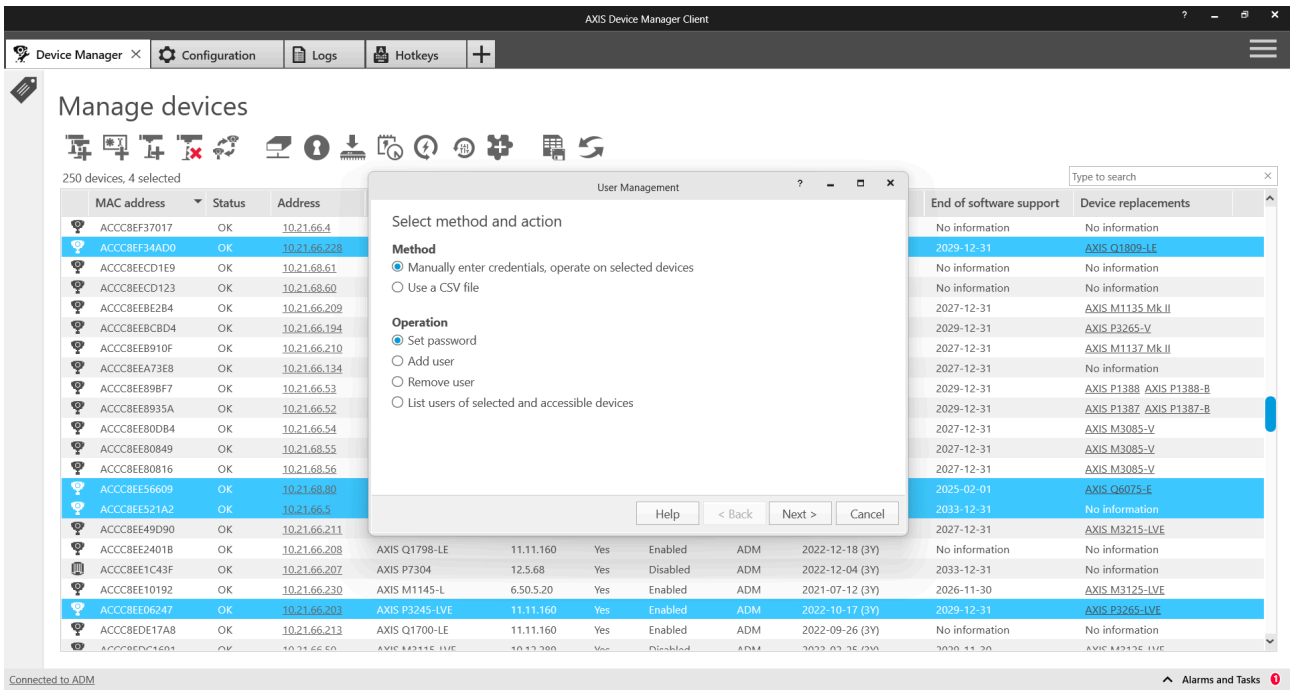
Axis Geräte unterstützen mehrere Konten, wobei jedes Konto eine von drei verschiedenen Berechtigungsstufen hat:

- **Viewers (Betrachter)**: Diese Benutzer haben Zugriff auf Video- und PTZ-Steuerung.
- **Operators (Bediener)**: Benutzer mit Bedienerrechten dürfen Kameraeinstellungen und Videostreamprofile optimieren.
- **Administratoren**: Administratoren dürfen Konten verwalten, Netzwerkeinstellungen ändern und Gerätedienste steuern.

Für jede dieser Zugriffsrollen wird ein eigenes Konto eingerichtet. Sie können zum Beispiel die Rolle „Kontrollraumpersonal" mit der Berechtigungsstufe „Bediener" konfigurieren, während die Rolle „Streifenpersonal" nur die Berechtigungsstufe „Betrachter" benötigt.

**Empfohlene Schritte**

- Zuerst die Kameras dem Axis Device Manager hinzufügen, dann die Kameras der VMS hinzufügen.
- Im AXIS Device Manager alle Kameras wählen und ein neues Benutzerkonto einrichten und mit einem Namen wie „vms" oder ähnlich versehen. Die Zugriffsrechte müssen den Vorgaben der VMS entsprechen, also entweder auf der Stufe Bediener oder Administrator (genaue Informationen beim Hersteller erfragen).
- Die Geräte der VMS unter dem eingerichteten Konto und dem entsprechenden Kennwort hinzufügen.
- Den AXIS Device Manager aufrufen, alle Kameras erneut wählen, das Root-Kennwort zurücksetzen und durch ein neues, sicheres Kennwort ersetzen. Das Kennwort für das Root-Konto muss so wenig Mitarbeitern wie möglich bekannt sein (nur den Benutzern des Axis Device Manager).
- Anderen Mitarbeitern für den Zugriff auf ein Gerät über die Weboberfläche zu Wartungszwecken oder zur Problembehebung auf **keinen** Fall das Root-Kennwort mitteilen. Stattdessen im AXIS Device Manager ein neues und kurzzeitiges Konto für ausgewählte Geräte und mit den Benutzerrechten Administrator oder Bediener einrichten. Nach Abschluss der Arbeiten im AXIS Device Manager das kurzzeitige Konto löschen.
- Der AXIS Device Manager unterstützt lokale Administratoren sowie Benutzer von Gruppen und Domains. Lokale Administratoren werden eingesetzt, wenn der Zugriff auf den Client des AXIS Device Manager ausschließlich über den Computer erfolgt, auf dem der Server des AXIS Device Manager installiert ist. Wir empfehlen die Verwendung von Domänenbenutzern, wenn die Person, die das System verwaltet, Remote-Clients verwenden wird.



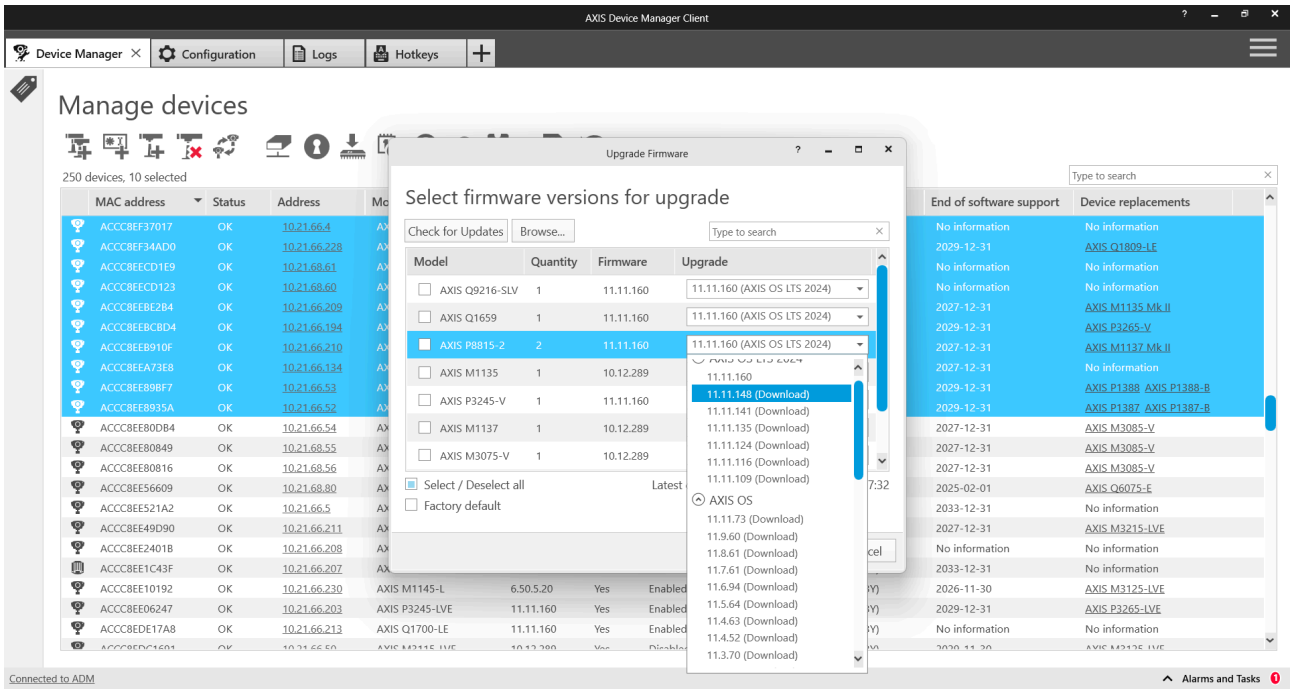

*Benutzerrollen und Kennwörter im AXIS Device Manager ändern*

## AXIS OS-Upgrades

Aktualisierte AXIS OS-Versionen enthalten Patches für bekannte Schwachstellen. Es ist wichtig, immer die aktuelle Software zu verwenden, damit bekannte Schwachstellen nicht ausgenutzt werden können. Ebenso wichtig ist die schnelle Bereitstellung einer neuen AXIS OS-Version, die die Bedienbarkeit verbessert und Engpässe bei der manuellen Einführung neuer Versionen beseitigt. AXIS Device Manager stellt eine Verbindung zu www.axis.com her und lädt die neuesten AXIS OS- oder Service-Versionen herunter. Alternativ lassen sich die Aktualisierungen statt direkt aus dem Internet in das Netzwerk auch über Zwischenspeichern auf USB-Speicher mit anschließender Installation auf dem Client des AXIS Device Manager durchführen. Der AXIS Device Manager informiert zudem über neue AXIS OS-Versionen und rollt sie auf Axis Geräte aus.

**Die aktuelle AXIS OS ist wichtig:**

- Sie schützt mit Patches Netzwerk wie Geräte insbesondere vor kritischen Schwachstellen.
- Zudem profitieren die Geräte von aktuellen Leistungssteigerungen und Fehlerbereinigungen.
- Die neuesten Funktionsmerkmale und Funktionssteigerungen stehen sofort bereit.




*AXIS OS lässt sich mit dem AXIS Device Manager dank Meldungen auf der Benutzeroberfläche und intuitiv zu bedienenden Dialogfeldern unkompliziert aktualisieren.*

## Zusätzliches Härten

Durch eine gute Benutzer- und Kennwortpolitik sowie die Verwendung aktueller AXIS OS-Versionen lassen sich die üblichen Risiken für Geräte verringern. In den *Axis Hardening Guide* werden weitere Maßnahmen beschrieben, die Risiken für große und sicherheitskritischen Organisationen verringern. Dazu gehört die Deaktivierung von Diensten, die möglicherweise nicht verwendet werden, sowie die Aktivierung von Diensten, die bei der Erfassung und Überwachung von Indikatoren für Angriffe oder Sicherheitsverletzungen helfen können. Der AXIS Device Manager vereinfacht die Bereitstellung einiger dieser Richtlinien. Axis bietet eine Konfigurierungsvorlage für die grundlegenden Einstellungen an.

Geräte mit dem Axis Härtungsleitfaden härten:

- Lesen Sie die Übersicht *AXIS Hardening Guide* und laden Sie die Vorlagendatei am Ende des Dokuments herunter.
- In der Konfigurationsdatei die relevanten Punkte wählen
- Wählen Sie Geräte im AXIS Device Manager-Bestand aus.
- Rechtsklicken und „Geräte konfigurieren > Konfigurieren...“ wählen
- Die Option Konfigurationsdatei anklicken und die heruntergeladene Datei wählen.
- Die Einstellungen nach Bedarf ändern.

## Zertifizierungsdienste

A Zertifizierungsstellen (Certificate Authorities – CAs) stellen digitale Zertifikate für Server, Clients und Benutzer aus. CAs sind öffentlich oder privat. Öffentliche CAs, wie Comodo und Symantec (vormals Verisign), werden in der Regel für öffentliche Dienste wie Websites und E-Mail-Dienste verwendet.

Private CAs (in der Regel Active Directory oder ein Zertifizierungsdienst) stellen Zertifikate für interne/private Netzwerke aus. In einem Videoverwaltungssystem dient dies in erster Linie der HTTPS-Netzwerkverschlüsselung und der IEEE 802.1x-Netzwerkzugriffskontrolle. AXIS Device Manager umfasst einen CA-Dienst für Axis Geräte und kann entweder als private Root-CA oder als private Zwischen-CA betrieben werden; als Teil einer unternehmensweiten Public Key Infrastructure (PKI).

Von CAs signierte Zertifikate werden sowohl für Clients (IEEE 802.1x) als auch für Server (HTTPS) eingesetzt.

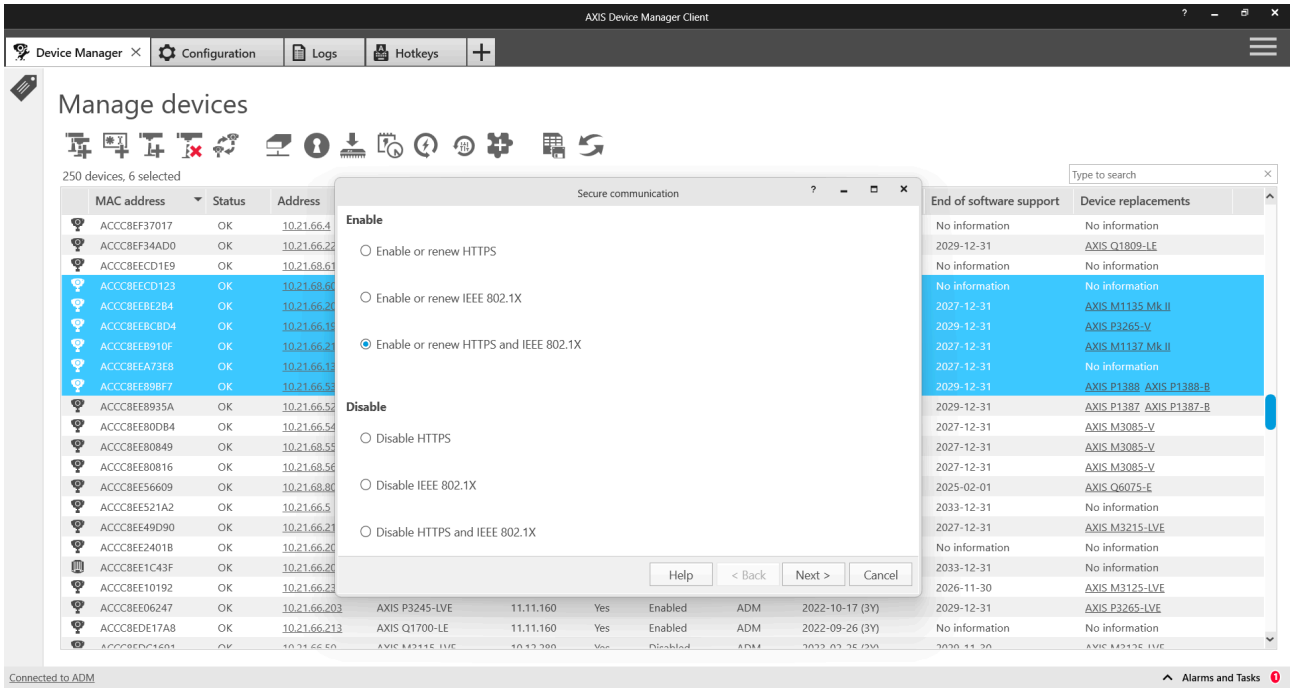
### HTTPS

HTTPS ist die sichere Version von HTTP. Mit ihm wird die Kommunikation zwischen Client und Server verschlüsselt. Selbstsignierte Zertifikate reichen zum Erstellen verschlüsselter Kommunikation aus. Die Verschlüsselungsgrad von selbstsignierten und von durch Zertifizierungsstellen ausgestellten Zertifikaten ist gleich. Der Unterschied besteht darin, dass selbstsignierte Zertifikate keinen Schutz vor Netzwerk-Spoofing bieten, bei dem ein angreifender Computer versucht, sich als legitimer Server auszugeben. Von einer Zertifizierungsstelle signierte Zertifikate fügen einen Vertrauenspunkt für Clients hinzu, um zu authentifizieren, dass der Zugriff auf ein vertrauenswürdiges Gerät erfolgt. Hinweis: Der Videoclient (VMS) muss Videoanfragen über HTTPS (RTP über RTSP über HTTPS) annehmen können, um Video verschlüsseln zu können.

### IEEE 802.1X

Der oft als kurzer 802.1X bezeichnete Standard verhindert den nicht autorisierten Zugriff von Netzwerk-Geräten auf das lokale Netzwerk. Geräte müssen sich authentifizieren, bevor ihnen der Zugriff auf das Netzwerk uns seine Ressourcen gestattet wird. Es können verschiedene Authentifizierungsmethoden verwendet werden: MAC Adresse (MAC-Filterung), Benutzer/Passwort oder Client-Zertifikat. Der Systembetreiber wählt die Methode. Die Wahl wird von den Kriterien Bedrohung, Risiken und Kosten bestimmt.

Eine auf 802.1X basierte Infrastruktur erfordert Investitionen. Erforderlich sind verwaltete Switches und weitere Server, in der Regel ein RADIUS (Remote Authentication Dial-In User Service). Die Verwendung von Clientzertifikaten erfordert eine CA (privat oder öffentlich), die Clientzertifikate ausstellen kann. In den meisten Fällen erfordert diese Infrastruktur Personal für die Pflege und Überwachung.




*Konfigurieren von Zertifikaten mit dem AXIS Device Manager*

## Zertifikatslebenszyklen verwalten

Die Verwaltung des Lebenszyklus von Zertifikaten ist ein Mittel zur kosteneffizienten Abwicklung aller Prozesse und Aufgaben im Zusammenhang mit der Ausstellung, Installation, Überprüfung, Korrektur und Erneuerung von Zertifikaten im Laufe der Zeit. AXIS Device Manager ermöglicht die effiziente Verwaltung von Zertifikaten, indem es Administratoren Folgendes ermöglicht:

- CA-signierte Zertifikate zu erstellen, falls keine CA verfügbar ist
- Unkomplizierte Verwaltung von IEEE 802.1x-Zertifikaten
- Unkomplizierte Verwaltung von HTTPS-Zertifikaten
- Ablauftermine der Zertifikaten zu überwachen
- Ablauftermine der Zertifikaten zu überwachen.

**Empfehlungen für private Root- und Zwischen-CAs**

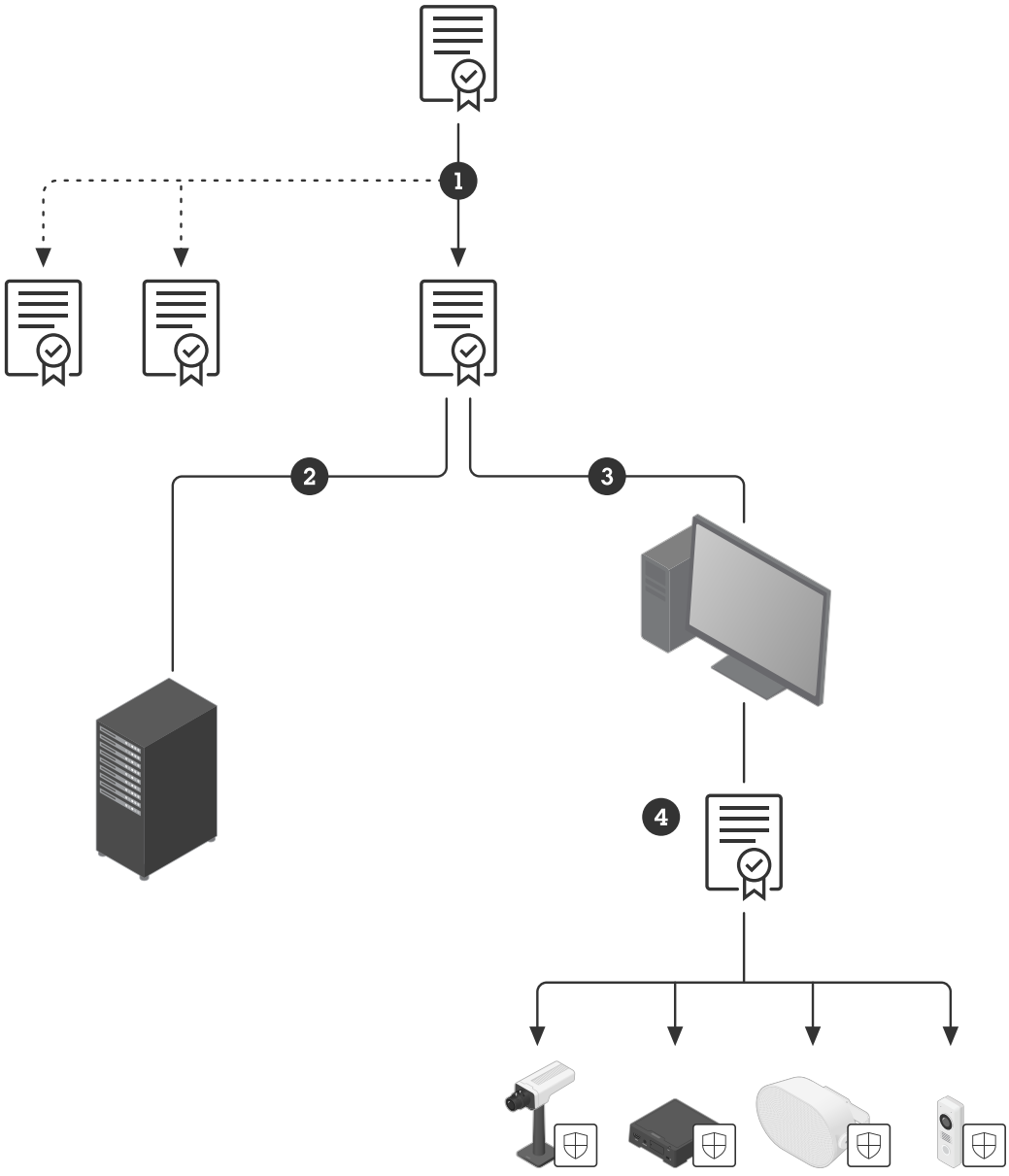
Axis Geräte sollen nicht als öffentliche Server zur Verfügung gestellt werden. Deshalb ist die Nutzung einer öffentlichen Zertifizierungsstelle auch nicht kosteneffizient.

Für HTTPS ist der VMS-Server der einzige Client, der sich beim Zugriff auf vertrauenswürdige Kameras authentifizieren muss. Die Clients der Bediener greifen nie direkt auf Kameras zu, da Livevideo und Aufzeichnungen vom VMS-Server bereitgestellt werden. Der Nutzen von in eine Enterprise PKI integrierten Kameraserverzertifikaten ist daher begrenzt

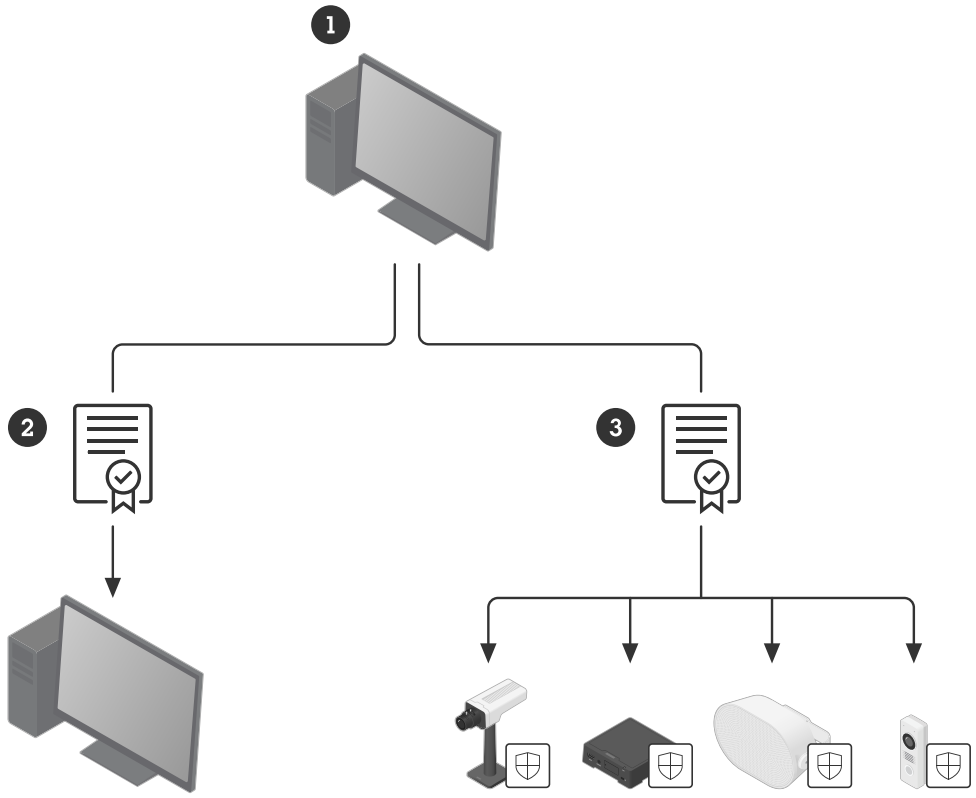
Die kostengünstigste Lösung ist der als private Zulassungsstelle verwendete AXIS Device Manager. Hierbei zuerst das Zertifikat für das Root-Konto erstellen. Dann das Zertifikat des AXIS Device Manager auf dem Server des VMS installieren. Falls weitere Clients direkt (zur Wartung und Problembehebung) auf die Kameras zugreifen, das Root-Zertifikat des AXIS Device Manager auch auf diesen Clients installieren.

Für 802.1X benötigen die Kameras Zertifikate, die sie gegenüber einem RADIUS-Server authentifizieren. Der Administrator sollte für das Enterprise-PKI/CA ein Zwischen-Zertifikat erstellen und dieses als ein Zertifikat des Typs PKCS#12 (P12) exportieren, das auf dem AXIS Device Manager installiert werden kann.

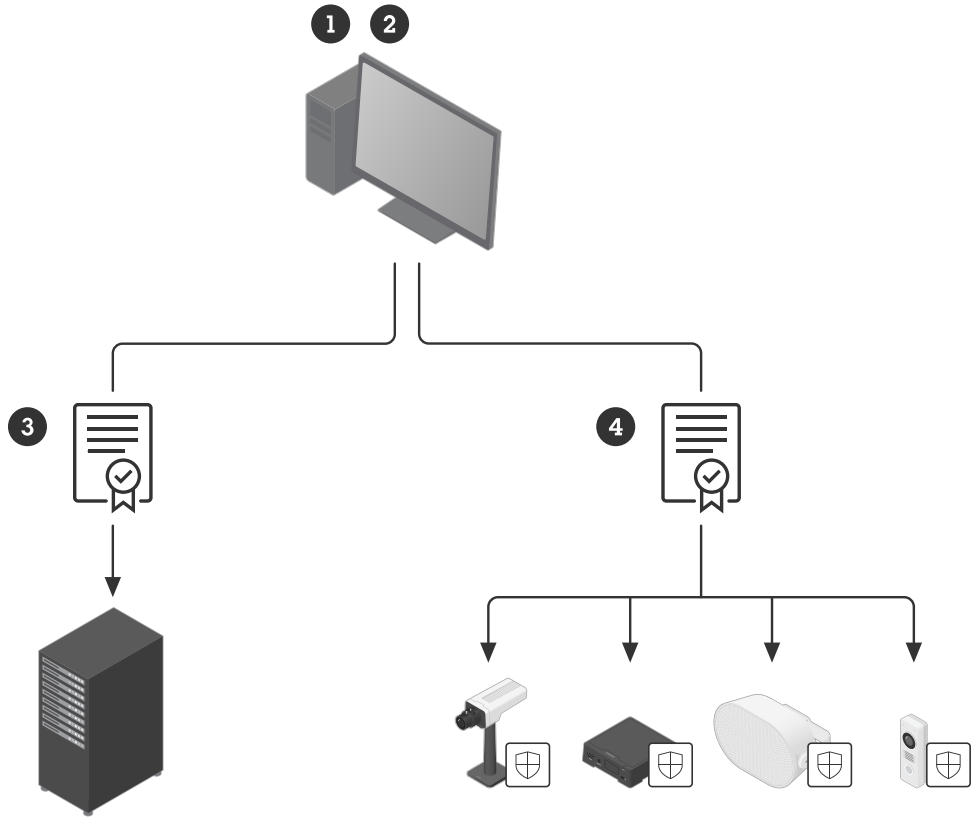
Unterstützung bei der Einstellung eines FreeRADIUS-Servers finden Sie im Abschnitt *Technische Unterlagen* für AXIS Device Manager




*Die Verwaltung von HTTPS-Zertifikaten beinhaltet: 1) Erstellen von Root- oder Zwischenzertifikaten in AXIS Device Manager. 2) Exportieren der Zertifikate auf die VMS. 3) Hochladen der Server-Zertifikate auf die Geräte.*




*Die Verwendung einer privaten CA. Die Verwaltung von IEEE 802.1X-Zertifikaten beinhaltet: 1) Erstellen von Zwischen- und Clientzertifikaten. 2) Installieren des Zertifikates auf dem RADIUS-Server. 3) Importieren des Zertifikats auf den Axis Device Manager. 4) Hochladen des CA-Zertifikats und der Clientzertifikate auf die Geräte.*



*Verwendung von AXIS Device Manager als CA. Verwaltung von IEEE 802.1X-Zertifikaten: 1) Generieren des root CA-Zertifikats in AXIS Device Manager; 2) Importieren des Authentifizierungs-CA-Zertifikats in AXIS Device Manager; 3) Installieren des CA-Zertifikats auf dem Radius-Server; 4) Hochladen der CA-Authentifizierungs- und Client-Zertifikate auf die Geräte.*

## Fazit

Sicherheitsmanagement und Sicherheitsmaßnahmen sind zum Erzielen effizienter Cybersicherheit unerlässlich. Es handelt sich dabei um einen kontinuierlichen Prozess, der die Aufrechterhaltung eines klaren Status und die Durchführung geeigneter Aktionen erfordert, um potenzielle Bedrohungen für Ihr IP-Netzwerk zu entschärfen. AXIS Device Manager bietet Ihnen ein Tool, mit dem Sie sowohl Ihre Geräte verwalten als auch die Sicherheit Ihres Netzwerks erhöhen können. Über Ihren Axis Händler oder *www.axis.com* erhalten Sie weitere Informationen und Unterstützung.

T10231485_de

2025-09 (M4.2)