Anwendungsleitfaden

Sicherheitskontrollen mit AXIS Device Manager

Version 1.0

Inhalt

1. Einführung **3**

1.1 Drei Schutzebenen für Cybersicherheit 3

1.2 Zweck dieses Dokumentes 3

1.3 Über AXIS Device Manager 3

2. Geräteinventar **4**

3. Konto- und Kennwortrichtlinie **5**

4. Firmware-Aktualisierungen **7**

5. Zusätzliches Härten **7**

6. Zertifizierungsstellenservice **8**

7. Verwaltung der Gültigkeit des Zertifikats **9**

8. Zusammenfassung **10**

1. Einführung

Cybersicherheit gewinnt in der Überwachungs- und Sicherheitsbranche immer mehr an Bedeutung. Seit die Überwachungs- und Sicherheitsbranche die Infrastruktur auf IP-Ethernet umgestellt hat, ist das Thema Cybersecurity in den Fokus gerückt. Für einen effektiven Schutz der System- und Netzwerkkomponenten ist ein mehrstufiger Schutz unabdingbar. Der Endkunde erwartet eine sachgerechte Auswahl der Komponenten und eine fundierte Beratung durch den Partner.

1.1 Drei Schutzebenen für Cybersicherheit

Wir bieten drei Schutzebenen für Cybersicherheit:

1. Sicherheitsverwaltung: Die Basis für eine sichere IT-Landschaft ist eine Risikoanalyse. Sie beschreibt die denkbaren Angriffsszenarien und die zu erwartenden Ausfälle und Schäden. Dabei sind sowohl die materiellen als auch die ideellen Schäden zu berücksichtigen. Um solche Vorfälle und Schäden zu vermeiden, sind Sicherheitsrichtlinien festzulegen. Sicherheitsrichtlinien beschreiben die Maßnahmen, die notwendig sind, um die Systeme zu schützen. Sie stützen sich üblicherweise auf Vorgaben von Verwaltungswerkzeugen und Kontrollprozessen.

2. Schwachstellenvermeidung: Bereits bei der Projektierung und der Entwicklung von Produkten achtet Axis auf die Vermeidung von Sicherheitslücken. Ziel ist es, potentielle Angriffsziele frühzeitig zu erkennen und zu vermeiden. Werden wider Erwarten zu einem späteren Zeitpunkt Schwachstellen entdeckt, schließen wir diese zeitnah, informieren umfänglich über die Sicherheitsrisiken und empfehlen notwendige Gegenmaßnahmen.

3. Lernen und Zusammenarbeit: Um die Cyber-Bedrohung richtig einschätzen und eine sichere IT-Umgebung aufbauen zu können, ist ein gutes Grundverständnis der komplexen Thematik notwendig. Mit klassischen Trainings, Online-Kursen und Whitepapers bietet Ihnen Axis einen breite Palette an Möglichkeiten zum Aufbau des notwendigen Wissens.

1.2 Zweck dieses Dokumentes

Dieser Anwendungsleitfaden beschreibt die Nutzung des AXIS Device Managers mit dem Ziel, die IT-Sicherheit zu erhöhen. Dies sind nur Empfehlungen, die unter Berücksichtigung der Risikoanalyse und in Absprache mit dem Kunden umgesetzt werden können.

1.3 Über AXIS Device Manager

AXIS Device Manager ist ein einfaches, kostenfreies und zuverlässiges Werkzeug zur Verwaltung von Axis-Geräten in einem lokalen Netzwerk. Alle wichtigen Installationen sowie das gesamte operative Gerätemanagement lassen sich damit verwalten (siehe Tabelle unten). Das Programm eignet sich bestens zur Verwaltung von mehreren Tausend Axis-Geräten an unterschiedlichen Standorten. AXIS Device Manager ermöglicht eine einfache Implementierung von Sicherheitsfunktionen auf Axis-Endgeräte im Netzwerk. Damit lassen sich entsprechende Schutzmaßnahmen aus den Sicherheitsrichtlinien einfach umsetzen.

Funktionen zur Geräteverwaltung mit AXIS Device Manager

Installation	Wartung
> Zuweisen einer IP-Adresse > Geräteliste exportieren und Vermögenswerte im Blick behalten* > Benutzer- und Kennwortverwaltung* > ACAP-Verwaltung > Aktualisieren der Firmware* > Verwaltung von HTTPS-Zertifikaten* > Verteilung von IEEE 802.1x Zertifikaten* > Geräte-Kennzeichnung	> Gerätestatus > Gerätedaten sammeln > Geräte konfigurieren und diese Konfigurationen auf mehrere Geräte anwenden > Verbindung zu mehreren Servern/Systemen herstellen > Wiederherstellungspunkte > Zurücksetzen auf werksseitige Standardeinstellung > Gerät ersetzen > Erneuerung und Verwaltung von Zertifikaten* > Cybersecurity Hardening*

**Hinweis auf Funktion zur Kontrolle der Cybersicherheit*

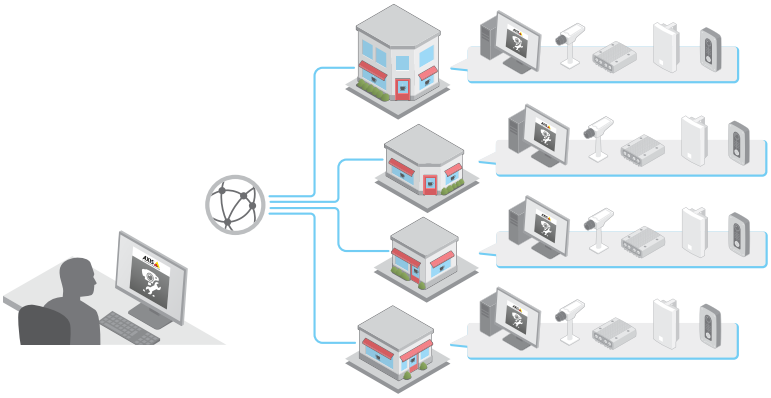


Abbildung 1. Multisite-Management

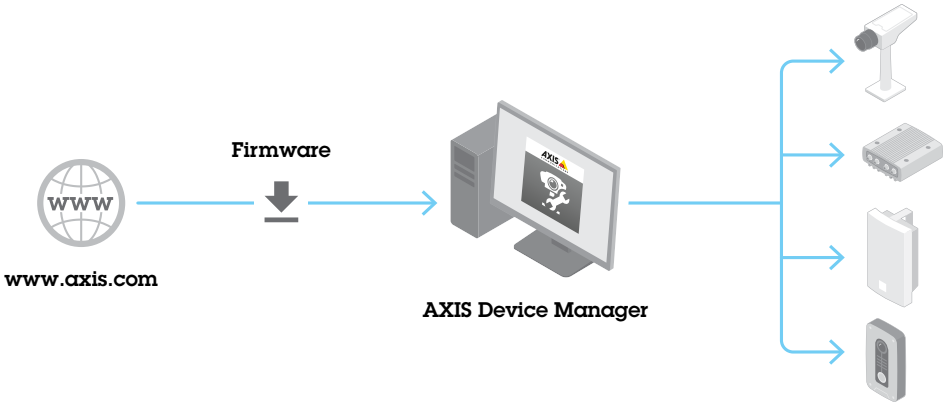


Abbildung 2. Firmware-Aktualisierung

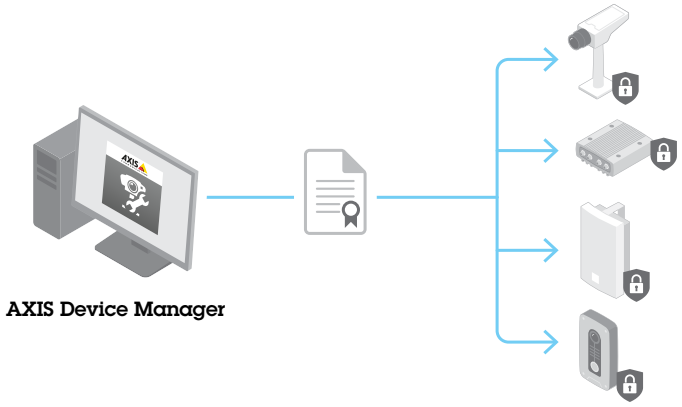


Abbildung 3. Zertifikatsverwaltung

2. Geräteinventar

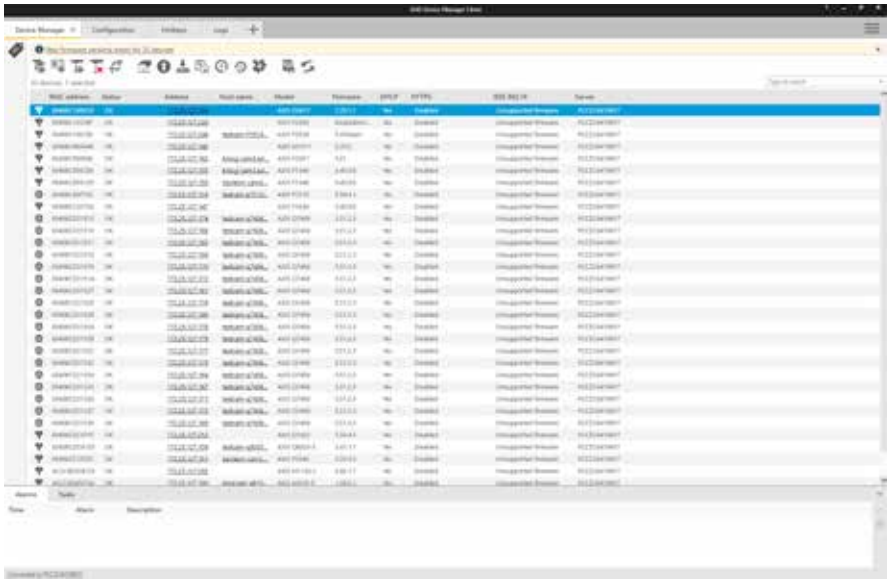
Die Inventarisierung der Netzwerkgeräte ist die Basis für den Aufbau einer umfassenden und sicheren IT-Landschaft. Die Vorzüge des AXIS Device Managers:

> Sie erhalten eine aktuelle und vollständige Liste aller Axis Netzwerkgeräte, die Sie zum Beispiel bei IT-Sicherheitsüberprüfungen und für die Arbeit der IT-Sicherheitsreaktionsteams nutzen können.
> Die Liste aller Axis-Geräte im Netzwerk lässt sich zum Beispiel nach der kompletten Anzahl, dem Typ oder der Modellnummer sortieren.
> Sie erhalten die Statusinformation zu jedem gefundenen Axis-Netzwerkgerät.

Die Inventarisierung der Geräte ist ein wesentlicher Schritt zu einem sicheren Firmennetzwerk. Die Vorzüge von AXIS Device Manager:

> Ermöglicht Ihnen den einfachen Zugriff auf ein aktuelles, vollständiges Inventar Ihrer Netzwerkgeräte bei der Arbeit mit Prüfern und Notfall-Einsatzteams
> Sie erhalten eine vollständige Liste Ihrer Geräte, sortiert nach Gesamtzahl, Typ, Modellnummer usw.
> Sie erhalten den Status jedes Geräts in Ihrem Netzwerk

Empfehlungen
AXIS Device Manager bietet eine automatisierte Methode, um in Echtzeit Zugriff auf das gesamte Inventar an Axis-Netzwerkgeräten zu erhalten. Sie können Ihre Geräte automatisch identifizieren, auflisten und sortieren. Sie können Tags verwenden, die es Ihnen erlauben, Geräte anhand Ihrer eigenen Kriterien zu gruppieren und zu sortieren. Sie erhalten problemlos einen Überblick über alle Axis-Geräte in Ihrem Netzwerk und können diese dokumentieren.



AXIS Device Manager verschafft Ihnen einen Überblick über Ihr Geräteinventar.

3. Konto- und Kennwortrichtlinie

Authentifizierung und Zugriffsrechte sind maßgeblich zum Schutz von Netzwerkkomponenten. Dies sollte in den IT-Sicherheitsrichtlinien festgelegt sein, um das Risiko für den ungewollten Missbrauch von Geräten über einen längeren Zeitraum hinweg zu reduzieren. Eine Schüsselfunktion dabei stellen Kennworte dar. Nur starke Kennworte, die nicht einfach zu erraten sind, bieten auch einen Schutz. Verbreiten sich die Kennworte in einem Unternehmen, ist nicht mehr nachvollziehbar, wer auf welches Gerät zugegriffen hat. AXIS Device Manager bietet Ihnen die Möglichkeit, individuelle Benutzerkonten, Kennwörter und Zugriffsrechte einfach und zentral zu verwalten.

> Sie legen die Zugriffsrechte für verschiedene Benutzertypen fest (Systeme und Menschen)
> Sie reduzieren das Risiko, dass das Systemkennwort (root) offengelegt wird
> Sie können die Anmeldedaten einzelner Benutzer zurücksetzen, ohne dass andere Anwender betroffen sind

Darum sollten Sie in Ihren Geräten mehr als nur ein Benutzerkonto einrichten:
> Sie kontrollieren Berechtigungsstufen für verschiedene Benutzertypen (Maschinen und Menschen)
> Sie reduzieren das Risiko, das Root-(Master-)Kennwort zu gefährden
> Sie können Anmeldedaten für einen Benutzertyp zurücksetzen, ohne dass sich das auf andere Benutzer auswirkt

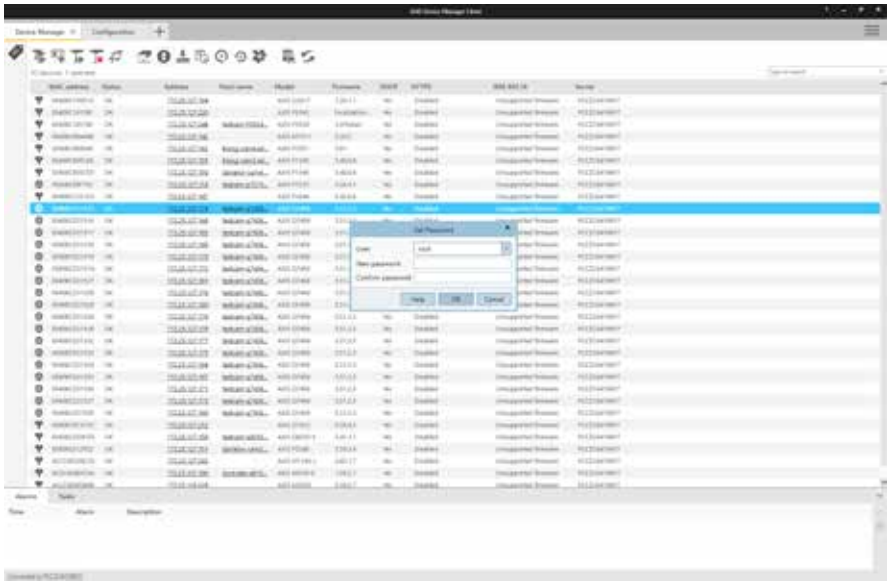
Arbeit mit Privilegien in AXIS Device Manager
Der AXIS Device Manager erlaubt die Zuordnung von verschiedenen Benutzerkonten mit unterschiedlichen Zugriffsrechten: Viewer, Operator und Administrator. So können die Zugriffsrechte auf einer Axis Kamera verwaltet werden:

Auf Axis Geräten können verschiedene Rollen vergeben werden. Für die Nutzung der Rollen ist es sinnvoll, individuelle Benutzerkonten anzulegen und damit entsprechende Rechte zu verknüpfen.

> Benutzer mit Viewer-Rechten können Zugriff auf das Live-Video und die PTZ-Steuerung erhalten.
> Benutzer mit Operator-Rechten können die Kameraeinstellungen und die Video-Streaming-Profile ändern.
> Anwender mit Administrator-Rechten können Benutzerrechte, Netzwerkeinstellungen oder Netzwerkdienste ändern.

Empfohlene Schritte

> Wir empfehlen, Kameras erst zum AXIS Device Manager und dann zur Videoverwaltungssoftware hinzuzufügen.
> Wählen Sie im AXIS Device Manager alle Kameras aus und erstellen Sie ein neues Benutzerkonto mit einer Bezeichnung wie „VMS" und legen Sie ein starkes Kennwort fest. Die Berechtigungen müssen mit den Anforderungen an die Videoverwaltungssoftware übereinstimmen, das kann entweder der Operator oder der Administrator sein (mit Hersteller abklären).
> Fügen Sie die Geräte mit dem Konto „VMS" und dem festgelegten Kennwort zur Videoverwaltungssoftware hinzu.
> Gehen Sie zurück zum AXIS Device Manager und wählen Sie erneut alle Kameras aus. Ersetzen (Ändern) Sie das Kennwort für das „Root"-Konto durch ein neues starkes Kennwort. Das Kennwort für das „Root"-Konto sollten nur einige wenige Personen kennen (die Benutzer des AXIS Device Managers).
> Sollte eine Person im Unternehmen zur Wartung oder zur Fehlersuche über einen Webbrowser auf das Gerät zugreifen müssen, dann geben Sie dieser Person nicht das Root-Kennwort. Nutzen Sie AXIS Device Manager, um ein neues (temporäres) Konto, entweder mit Administratoren- oder Operator-Berechtigungen für ein oder mehrere ausgewählte Geräte zu erstellen. Löschen Sie nach Fertigstellung der Aufgabe das temporäre Konto über den AXIS Device Manager.
> AXIS Device Manager unterstützt lokale Administratoren sowie Domain-Benutzer und Gruppen. Sie können einen lokalen Administrator verwenden, wenn der Zugriff auf den AXIS Device Manager Client nur von derselben Maschine erfolgen soll, die auch den AXIS Device Manager Server hostet. Wir empfehlen, Domainbenutzer zu verwenden, wenn die Person, die das System betreut, Remote-Clients nutzt.



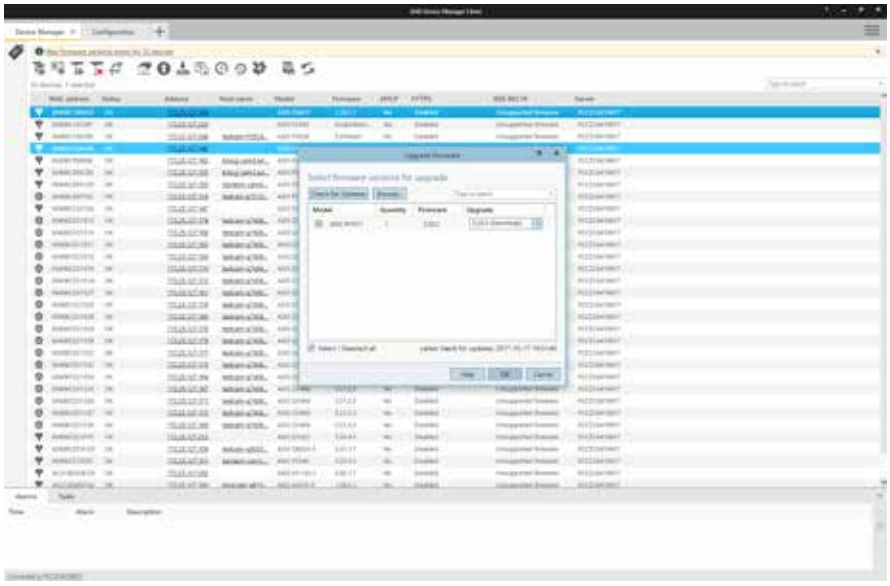
Verändern von Benutzer-Berechtigungen und Kennwörtern in AXIS Device Manager.

4. Firmware-Aktualisierungen

Die neuesten Firmware-Versionen enthalten Patches für erkannte Schwachstellen. Immer die neueste Software zu verwenden ist deshalb so wichtig, weil Angreifer alle bekannten Schwachstellen ausnutzen könnten. Die manuelle Verteilung einer neuen Firmware-Version auf einzelne Kameras kann zu längeren Betriebsunterbrechungen führen. Um diese zu vermeiden ist es wichtig, eine effiziente Methode zum Ausrollen der Updates zu nutzen. AXIS Device Manager stellt eine Verbindung zu www.axis.com her und lädt die neueste passende Firmware oder die neuesten Service-Release-Packs herunter. Wenn Sie keine direkten Downloads aus dem Internet auf Ihr Netzwerk durchführen möchten, können Sie die Upgrades auf einem USB-Stick speichern und anschließend auf Ihren AXIS Device Manager Client hochladen. Sie erhalten eine Mitteilung, wenn neue Firmware verfügbar ist und können diese rasch auf Ihre Axis-Geräte übertragen.

Darum sollten Sie immer die neuesten Firmware-Versionen verwenden:

> Ihr Netzwerk und Ihre Geräte sind mit den neuesten Patches vor Schwachstellen, insbesondere vor kritischen Schwachstellen, geschützt
> Ihre Geräte erhalten mit den Updates die neuesten Leistungsverbesserungen und Lösungen für bekannte Programmierfehler
> Sie erhalten sofortigen Zugriff auf die neuesten Features und Funktionsverbesserungen



Mitteilungen über das Benachrichtigungsfenster und intuitive Dialogfelder vereinfachen die Aktualisierung der Firmware.

5. Zusätzliches Härten

Eine gute Benutzer-/Kennwortrichtlinie sowie der Betrieb der Geräte mit aktuellen Firmware-Versionen verringern häufige Risiken für die Geräte. Der Axis Hardening Guide beschreibt zusätzliche Maßnahmen zur Verringerung von Risiken in großen und kritischen Umgebungen. Ein wichtiger Punkt dabei sind die Netzwerkdienste. Einzelne Netzwerk-Services stellen potenzielle Angriffsflächen dar, andere können zur Fehlererkennung und Behebung nützlich sein.

Axis bietet dazu eine cybersecurity-optimierte Kamerakonfiguration als Standard an. Diese lässt sich einfach und effizient auf alle Axis Kameras über den AXIS Device Manager verteilen. Mehr dazu unter: www.axis.com/products/axis-device-manager/support-and-documentation.

So härten Sie Geräte gemäß dem Axis Hardening Guide:

> Laden Sie die Vorlagendatei für die Hardening-Konfiguration von folgendem Link herunter: www.axis.com/products/axis-device-manager/support-and-documentation
> Bearbeiten Sie die Konfigurationsdatei durch Auswahl relevanter Punkte
> Wählen Sie die Geräte aus
> Wählen Sie nach einem Rechtsklick mit der Maus „Geräte konfigurieren | Konfigurieren ..."
> Klicken Sie auf „Konfigurationsdatei" und wählen Sie die heruntergeladene Datei aus
> Passen Sie die Einstellungen nach Bedarf an

6. Zertifizierungsstellenservice

Die Certificate Authority (CA) ist ein Dienst, der digitale Zertifikate an Server, Clients oder Benutzer ausgibt. Eine CA kann öffentlich oder privat sein. Öffentlich vertrauenswürdige CA wie Comodo und Symantec (früher Verisign) werden normalerweise für öffentliche Dienste wie öffentliche Websites und E-Mails verwendet.

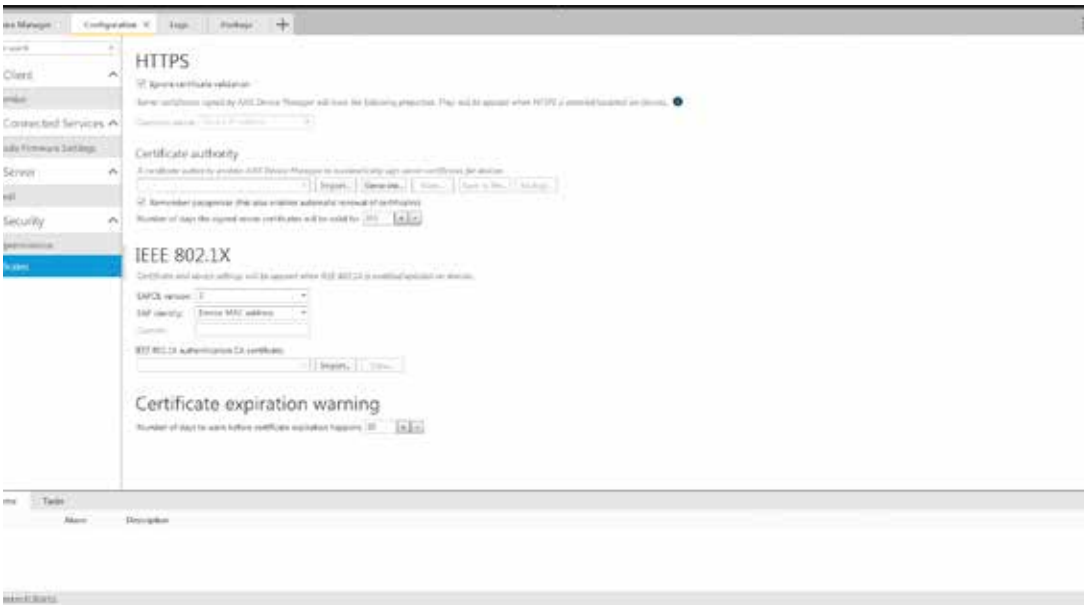
Ein privates CA (normalerweise eine Active Directory/ein Certificate Service) gibt Zertifikate für interne/private Netzwerkdienste aus. In einem Verwaltungssystem gilt dies vor allem für HTTPS (Hyper Text Transfer Protocol Secure) und IEEE 802.1x (Netzwerkzugriffskontrolle). AXIS Device Manger enthält einen CA-Dienst für Axis-Geräte, der entweder als privater Root-CA oder als privater Intermediate-CA ausgeführt werden kann. Er ist Teil einer Enterprise-PKI (Public Key Infrastructure).

CA-signierte Zertifikate finden Verwendung für IEEE 802.1x (Client) und HTTPS (Server) Zertifikate.

HTTPS
HTTPS ist die sichere Version von HTTP. Über dieses Protokoll wird die Kommunikation zwischen einem Client und Server verschlüsselt. Selbstsignierte Zertifikate sind ausreichend, um eine verschlüsselte Verbindung zu erreichen. Die Verschlüsselungsstufe unterscheidet sich bei selbstsignierten und CA-signierten Zertifikaten nicht. Der Unterschied besteht darin, dass selbstsignierte Zertifikate keinen Schutz gegen Netzwerk-Spoofing haben, bei dem ein angreifender Computer einen legitimen Server zu imitieren versucht. CA-signifizierte Zertifikate schaffen einen Vertrauenspunkt, der bestätigt, dass der Client auf ein vertrauenswürdiges Gerät zugreift. Beachten Sie, dass der Video-Client (Videoverwaltungssystem) das Abrufen von Video über HTTPs (RTP oder RTSP over HTTPS) unterstützen muss, um die Videoübertragung zu verschlüsseln.

IEEE 802.1X
Der als 802.1X bezeichnete Standard verhindert, dass nicht autorisierte Netzwerk-Geräte auf das lokale Netzwerk zugreifen. Ein Gerät muss sich selbst authentifizieren, bevor es Zugriff auf das Netzwerk (und seine Ressourcen) erhält. Dabei können verschiedene Authentifizierungsmethoden wie MAC-Adresse (MAC-Filterung), Benutzer/Kennwort oder Client-Zertifikat verwendet werden. Der Systemeigentümer entscheidet, welche Methode zum Einsatz kommt. Die passende Auswahl hängt von der Risikoanalyse, dem notwendigen Schutz und den damit verbundenen Kosten ab.

Eine 802.1X-Infrastruktur zu betreiben ist eine Investition. Verwaltbare Switches und zusätzliche Server, normalerweise ein RADIUS (Remote Authentication Dial-In User Service), sind dazu erforderlich. Die Nutzung von Client-Zertifikaten erfordert ein CA (privat oder öffentlich), das Client-Zertifikate ausgeben kann. In der Regel ist Personal erforderlich, um die Infrastruktur zu verwalten und zu überwachen.



Konfiguration des Zertifikats in AXIS Device Manager.

7. Verwaltung der Gültigkeit des Zertifikats

Das Certificate-Lifecycle-Management dient der Ausgabe, Installation, Überprüfung, dem Löschen und der Erneuerung von Zertifikaten über einen langen Zeitraum.
AXIS Device Manager ermöglicht es Ihnen, Zertifikate effizient zu verwalten. Administratoren können:

> CA-signierte Zertifikate ausgeben, wenn keine andere CA verfügbar ist
> problemlos IEEE 802.1X-Zertifikate verteilen
> HTTPS-Zertifikate einfach bereitstellen
> Ablaufdaten von Zertifikaten überwachen
> Zertifikate vor dem Ablauf einfach erneuern

Empfehlungen für private Root- und Intermediate-CA
Es ist nicht empfehlenswert, Axis-Geräten öffentlich signierte Zertifikate zuzuteilen, da diese niemals direkt mit dem Internet verbunden sind. Außerdem ist die Verwendung einer öffentlichen CA für private Ressourcen nicht billig.

Für HTTPS ist der VMS-Server der einzige Client, der überprüfen muss, dass er auf eine vertrauenswürdige Kamera zugreift. Operator-Clients erhalten niemals direkten Kamerazugriff, denn Live-Aufnahmen und aufgezeichnetes Video werden vom VMS-Server bereitgestellt. In dieser Situation gibt es einen begrenzten Wert zur Einbindung von Kameraserver-Zertifikaten in einer bestehenden Enterprise-PKI.

Am kostengünstigsten ist es, AXIS Device Manager als private CA zu nutzen. Installieren Sie nach dem Erstellen eines Root-CA-Zertifikats das AXIS Device Manager Zertifikat in dem Zertifikatsspeicher des VMS-Servers. Installieren Sie die AXIS Device Manager Root CA ebenfalls in diesen Clients, falls andere Clients (zur Wartung oder Fehlerbehebung) direkt auf Kameras zugreifen müssen.

Für 802.1X benötigt die Kamera ein Client-Zertifikat, um sich selbst bei einem RADIUS-Server zu authentifizieren. Wir empfehlen, dass der Administrator für Enterprise-PKI/CA ein Intermediate CA-Zertifikat erstellt und dieses als ein PKCS#12 (P12) Zertifikat exportiert, das im AXIS Device Manager installiert werden kann.

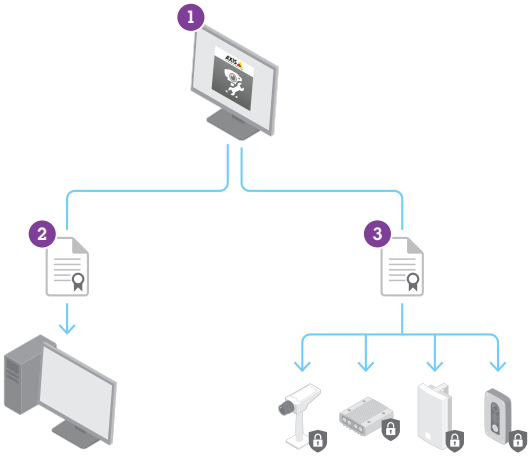


Abb. 4, links: Die Verwaltung von HTTPS-Zertifikaten beinhaltet:
1) Erstellen von Intermediate- oder Root-CA-Zertifikaten im AXIS Device Manager; 2) Export des CA-Zertifikats in das Videoverwaltungssystem sowie 3) Upload von Server-Zertifikaten in die Geräte.

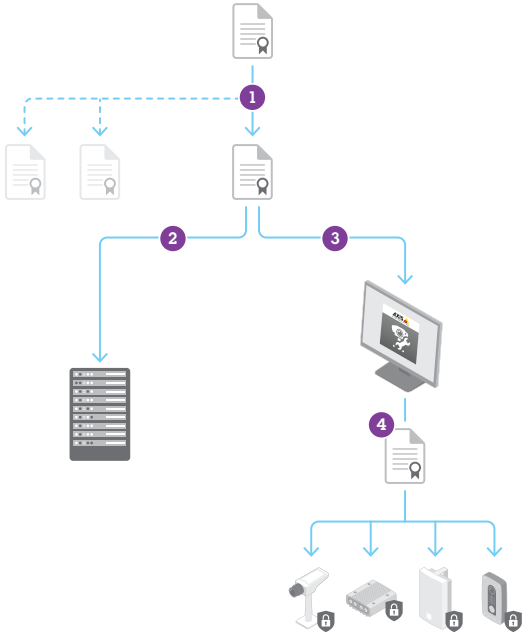


Abb. 5, rechts: Die Verteilung von IEEE 802.1X-Zertifikaten beinhaltet: 1) Erstellen eines Intermediate CA und Client-Zertifikats; 2) Installieren eines CA-Zertifikats auf den Radius-Server; 3) Import des CA-Zertifikats in AXIS Device Manager sowie 4) Upload der CA- und Client-Zertifikate in die Geräte.

8. Zusammenfassung

Sicherheitsverwaltung und Sicherheitsrichtlinien sind wichtige Bestandteile der Implementierung eines effektiven Konzepts für Cybersicherheit. Beides sind kontinuierliche Prozesse mit dem Ziel, die notwendigen Schutzmaßnahmen für die Netzwerkkomponenten an die aktuelle Bedrohungslage anzupassen. AXIS Device Manager verfügt über Funktionen, um Ihre Geräte zu verwalten und die Sicherheit Ihres Netzwerks zu erhöhen. Wenden Sie sich an Ihren lokalen Axis-Ansprechpartner oder besuchen Sie www.axis.com , um weitere Informationen zu erhalten.

Informationen zu Axis Communications

Axis bietet intelligente Sicherheitslösungen für den Schutz und die Sicherheit von Menschen, Unternehmen und Institutionen. Ziel von Axis ist es, zu einer sicheren, stabilen Welt beizutragen. Als Marktführer im Bereich Netzwerk-Video sorgt Axis durch die kontinuierliche Entwicklung innovativer Netzwerkprodukte für den technischen Fortschritt in der Branche. Die Axis-Produkte basieren allesamt auf einer offenen Plattform. Axis legt größten Wert auf die langfristigen Beziehungen mit seinen weltweiten Partnern und versorgt diese mit wegweisenden Netzwerkprodukten und technischem Know how für etablierte und neue Märkte. Die Kunden profitieren von diesem globalen Partnernetzwerk.

Axis beschäftigt über 2.700 engagierte Mitarbeiter in mehr als 50 Ländern und arbeitet mit über 90.000 Partnern zusammen. Das 1984 gegründete schwedische Unternehmen ist an der NASDAQ Stockholm unter dem Tickersymbol AXIS notiert.

Weitere Informationen über Axis finden Sie unter www.axis.com.

AXIS COMMUNICATIONS