

AXIS Device Manager

Introduzione

La sicurezza informatica diventa sempre più importante nei settori della sicurezza e della sorveglianza. Per una sicurezza informatica efficace è necessario garantire una profondità di difesa sufficiente a proteggere adeguatamente la rete IP a ogni livello, dai prodotti e dai partner scelti, ai requisiti stabiliti dal cliente e dai suoi partner.

Questa guida descrive come utilizzare AXIS Device Manager per rendere più sicuro il sistema e aumentare la sicurezza. Si concentra sugli aspetti chiave e descrive le raccomandazioni.

Gestione del ciclo di vita del dispositivo

Noi di Axis siamo consapevoli dell'importanza di una solida base di sicurezza per l'intero ciclo di vita del dispositivo. Il nostro impegno per la sicurezza informatica garantisce che i nostri prodotti e le nostre soluzioni forniscano una solida protezione contro le potenziali minacce.

Implementazione

Axis offre dispositivi sicuri per progettazione con funzioni di sicurezza integrate, come meccanismi di avvio sicuri, sistema operativo firmato e archiviazione crittografata. Inoltre, AXIS Device Manager aiuta gli installatori e gli amministratori di sistema a configurare e distribuire in modo sicuro i dispositivi, garantendo una configurazione sicura fin dall'inizio.

Servizio attivo

Durante la fase operativa, Axis offre aggiornamenti regolari del software del dispositivo e patch di sicurezza per proteggere dalle vulnerabilità. AXIS Device Manager consente inoltre il monitoraggio e la manutenzione da remoto, permettendo una rapida risoluzione dei problemi e tempi di inattività minimi. Inoltre, le nostre guide all'hardening forniscono consigli per configurare i dispositivi in modo da soddisfare specifici requisiti di sicurezza.

Smaltimento

Quando è il momento di dismettere o sostituire i dispositivi, AXIS Device Manager facilita la dismissione sicura cancellando i dati sensibili e ripristinando i dispositivi alle impostazioni di fabbrica. Ciò garantisce che nessuna informazione riservata rimanga sul dispositivo, proteggendo i dati dell'utente e impedendo l'accesso non autorizzato.

AXIS Device Manager

AXIS Device Manager è uno strumento locale che fornisce un modo semplice, economico e sicuro dal punto di vista informatico per gestire tutte le principali attività di installazione, di sicurezza e manutenzione (vedere la tabella seguente). Lo strumento è adatto per gestire fino a un paio di migliaia di dispositivi Axis in un singolo sito o per diverse migliaia di dispositivi distribuiti in più siti. AXIS Device Manager consente di implementare in modo efficiente i controlli di sicurezza informatica per proteggere i dispositivi di rete e allinearli a un'infrastruttura di sicurezza.

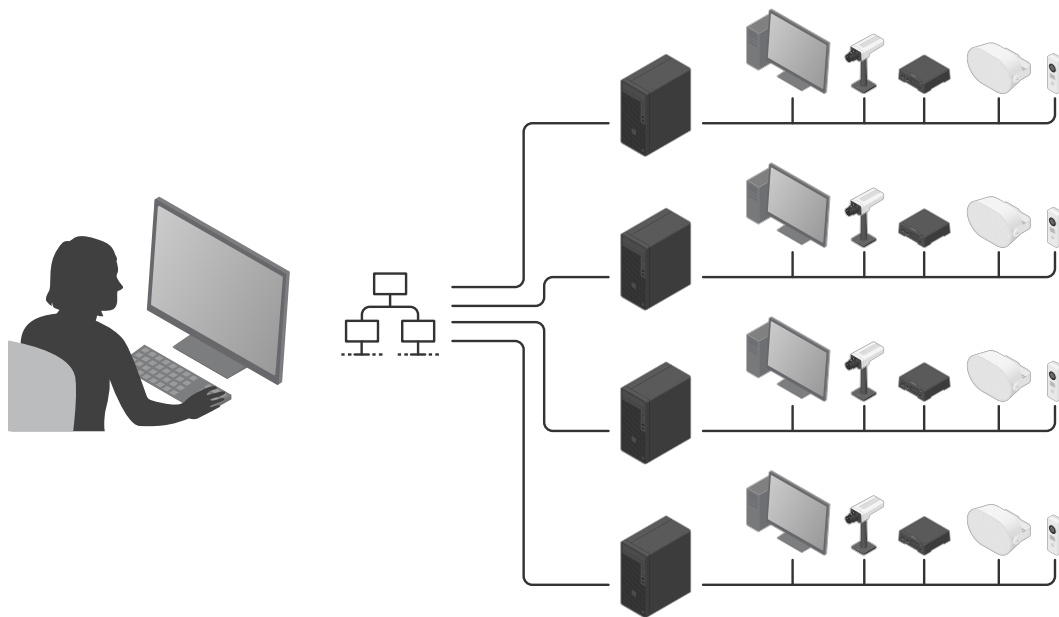
Funzioni di gestione dei dispositivi, AXIS Device Manager

Installazione	Manutenzione
Assegnazione di un indirizzo IP	Stato dispositivi
Esportazione dell'elenco dei dispositivi e traccia delle risorse*	Raccolta dei dati dei dispositivi
Gestione degli utenti e delle password*	Configurazione e copia delle configurazioni su più dispositivi
Gestione ACAP	Connessione a più server/sistemi
Aggiornamento del sistema operativo AXIS, basato su LTS o Active*.	Punti di ripristino

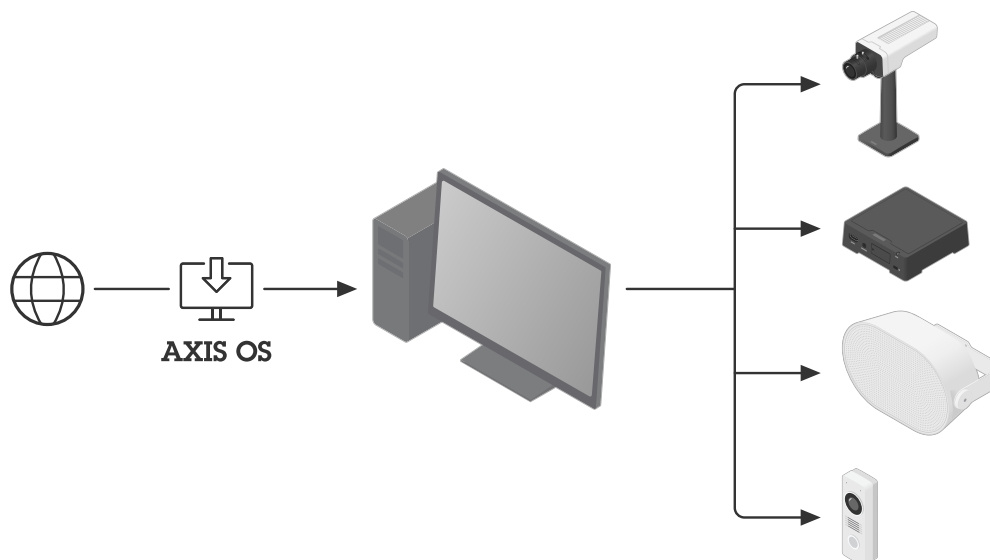
Gestione dei certificati HTTPS*	Ripristino dei valori predefiniti di fabbrica
Gestire i certificati IEEE 802.1*/**	Sostituire il(i) dispositivo(i)
Tagging dispositivi	Rinnovo e gestione dei certificati*
	Protezione avanzata della sicurezza informatica*

* Indica la funzione di controllo della sicurezza informatica.

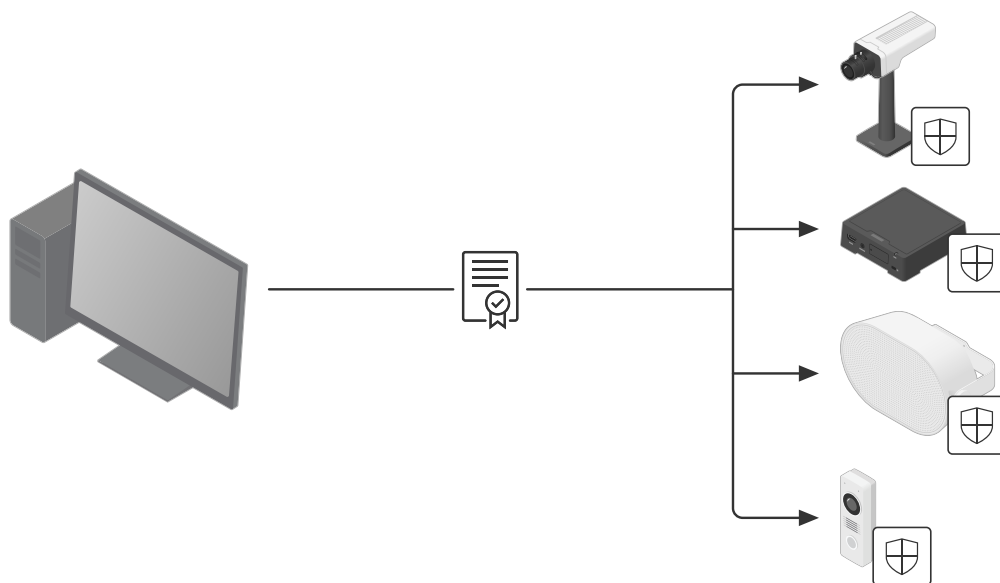
** I servizi di certificazione di Active Directory non sono attualmente supportati. Convalidato per FreeRADIUS in esecuzione su Linux.



Gestione di più siti.



AXIS OS upgrade (Aggiornamento di AXIS OS).



Gestione dei certificati.

Inventario del dispositivo

Un aspetto fondamentale per garantire la sicurezza di una rete aziendale è mantenere un inventario completo dei dispositivi che risiedono nella rete. Quando si crea o si rivede un criterio di sicurezza generale, è importante disporre chiaramente delle conoscenze e della documentazione per ciascun dispositivo e non solo sulle risorse critiche. Questo perché ogni dispositivo sottovalutato può essere un varco per i malintenzionati. Non è possibile proteggere i dispositivi che si ignorano o di cui non si è pienamente a conoscenza.

L'inventario dei dispositivi rappresenta un passaggio fondamentale per la protezione della rete aziendale. AXIS Device Manager può essere d'aiuto in questo senso:

- Consente di accedere facilmente a un inventario corrente e completo dei dispositivi di rete quando si lavora con controlli e operatori di incidenti.
- Fornisce un elenco completo dei dispositivi, che possono essere ordinati per numero totale, tipo, numeri di modello, ecc.
- Fornisce lo stato di ogni dispositivo nella rete.
- Aiuta a pianificare il futuro, mostrando la data prevista per la fine del supporto software del dispositivo e indicando quali prodotti più recenti possono essere utilizzati in sostituzione.

Device Manager

Configuration

Logs

Hotkeys

+

Manage devices

250 devices, 1 selected

Type to search

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
ACCC8EEB2B4	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
ACCC8EE24018	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
ACCC8EDC1601	OK	10.21.66.50	AXIS M3215-LVE	10.12.289	Yes	Disabled	ADM	2023-02-26 (3Y)	2029-12-31	AXIS M3215-LVE

Connected to ADM

Alarms and Tasks

AXIS Device Manager fornisce una chiara visione dell'inventario dei dispositivi.

AXIS Device Manager fornisce i mezzi automatizzati per accedere all'inventario dei dispositivi di rete Axis in tempo reale. Consente di identificare, elencare e ordinare automaticamente i dispositivi. Altrettanto importante è la possibilità di utilizzare i tag per raggruppare e ordinare i dispositivi in base ai propri criteri, semplificando la visione d'insieme e la documentazione di tutti i dispositivi Axis presenti sulla rete.

Criteri di account e password

L'autenticazione e il controllo dei privilegi è una parte importante della protezione delle risorse di rete. Il criterio di implementazione aiuta a ridurre il rischio di uso improprio accidentale o intenzionale per un periodo di tempo. Imporre l'uso di password robuste è un compito fondamentale, ma lo è anche ridurre il rischio di password compromesse. Le password dei dispositivi spesso si diffondono all'interno di un'organizzazione e quando ciò accade si perde il controllo sugli utenti che possono accedervi. AXIS Device Manager consente di gestire facilmente più account e password per i dispositivi Axis.

Perché si deve avere più di un account utente nei dispositivi:

- Controllare i livelli di privilegio per diversi tipi di utenti (macchine e persone).
- Ridurre il rischio di compromettere la password root (master).
- Poter reimpostare le credenziali per un tipo di utente senza influire sugli altri.

Utilizzo dei privilegi in AXIS Device Manager

I dispositivi Axis supportano più account, ognuno dei quali ha uno dei tre diversi livelli di privilegio:

- **Viewers (Visualizzatori):** Questi utenti hanno accesso al video e ai Comandi PTZ.
- **Operators (Operatori):** Gli utenti con diritti di operatore possono ottimizzare le impostazioni della telecamera e i profili del flusso video.
- **Amministratori:** Gli amministratori possono gestire gli account, modificare le impostazioni di rete e controllare un numero di servizi nel dispositivo.

Ogni ruolo che accede alla telecamera deve avere un proprio account. Ad esempio, si potrebbe configurare il ruolo "Personale della sala di controllo" con il livello di privilegio "operatore", mentre il ruolo "Personale di pattugliamento" potrebbe necessitare solo del livello di privilegio "visualizzatore".

Passaggi consigliati

- Prima di aggiungere le telecamere al VMS, aggiungere le telecamere ad AXIS Device Manager.
- In AXIS Device Manager, selezionare tutte le telecamere e creare un nuovo account utente chiamato "vms" o nome simile e impostare una password complessa. I privilegi devono essere allineati con i requisiti del VMS – che potrebbero essere l'operatore o l'amministratore (verificare con il produttore).
- Aggiungere i dispositivi al VMS con l'account e la password creata.
- Tornare ad AXIS Device Manager – selezionare nuovamente tutte le telecamere e reimpostare (modificare) la password dell'account "root" con una nuova password complessa. La password dell'account "root" deve essere nota solo a un numero limitato di persone (coloro che utilizzano AXIS Device Manager).
- Quando qualcuno deve utilizzare un browser Web per accedere a un dispositivo per attività di manutenzione o risoluzione dei problemi, **non** fornire loro la password root. Invece, utilizzare AXIS Device Manager per creare un nuovo account (temporaneo) per il dispositivo selezionato (i dispositivi selezionati) con privilegi di amministratore o operatore. Una volta completato l'intervento, utilizzare AXIS Device Manager per eliminare l'account temporaneo.
- AXIS Device Manager supporta amministratori locali e utenti e gruppi di dominio. È possibile utilizzare un amministratore locale se si accede al client AXIS Device Manager solo dalla stessa macchina che ospita il server AXIS Device Manager. Si consiglia di utilizzare gli utenti di dominio se la persona che si occupa della manutenzione del sistema utilizzerà i client remoti.

Device Manager

Configuration

Logs

Hotkeys

+

Manage devices

250 devices, 4 selected

MAC address	Status	Address
ACCC8EF37017	OK	10.21.66.4
ACCC8EF34AD0	OK	10.21.66.228
ACCC8EECD1E9	OK	10.21.68.61
ACCC8EECD123	OK	10.21.68.60
ACCC8EEB2B4	OK	10.21.66.209
ACCC8EEBCBD4	OK	10.21.66.194
ACCC8EEB910F	OK	10.21.66.210
ACCC8EEA73E8	OK	10.21.66.134
ACCC8EE89BF7	OK	10.21.66.53
ACCC8EE8935A	OK	10.21.66.52
ACCC8EE80DB4	OK	10.21.66.54
ACCC8EE80849	OK	10.21.68.55
ACCC8EE80816	OK	10.21.68.56
ACCC8EE56609	OK	10.21.68.80
ACCC8EE521A2	OK	10.21.66.5
ACCC8EE49D90	OK	10.21.66.211
ACCC8EE2401B	OK	10.21.66.208
ACCC8EE1C43F	OK	10.21.66.207
ACCC8EE10192	OK	10.21.66.230
ACCC8EE06247	OK	10.21.66.203
ACCC8EDE17A8	OK	10.21.66.213
ACCC8EDC1601	OK	10.21.66.50

User Management

Select method and action

Method

☒ Manually enter credentials, operate on selected devices
 ☐ Use a CSV file

Operation

☒ Set password
 ☐ Add user
 ☐ Remove user
 ☐ List users of selected and accessible devices

Help

< Back

Next >

Cancel

Type to search

End of software support	Device replacements
No information	No information
2029-12-31	AXIS Q1809-LE
No information	No information
No information	No information
2027-12-31	AXIS M1135 Mk II
2029-12-31	AXIS P3265-V
2027-12-31	AXIS M1137 Mk II
2027-12-31	No information
2029-12-31	AXIS P1388 AXIS P1388-B
2029-12-31	AXIS P1387 AXIS P1387-B
2027-12-31	AXIS M3085-V
2027-12-31	AXIS M3085-V
2027-12-31	AXIS M3085-V
2025-02-01	AXIS Q6075-E
2033-12-31	No information
2027-12-31	AXIS M3215-LVE
No information	No information
2033-12-31	No information
2026-11-30	AXIS M3125-LVE
2029-12-31	AXIS P3265-LVE
No information	No information
No information	No information

Connected to ADM

Alarms and Tasks 0

Modifica dei ruoli utente e delle password in AXIS Device Manager.

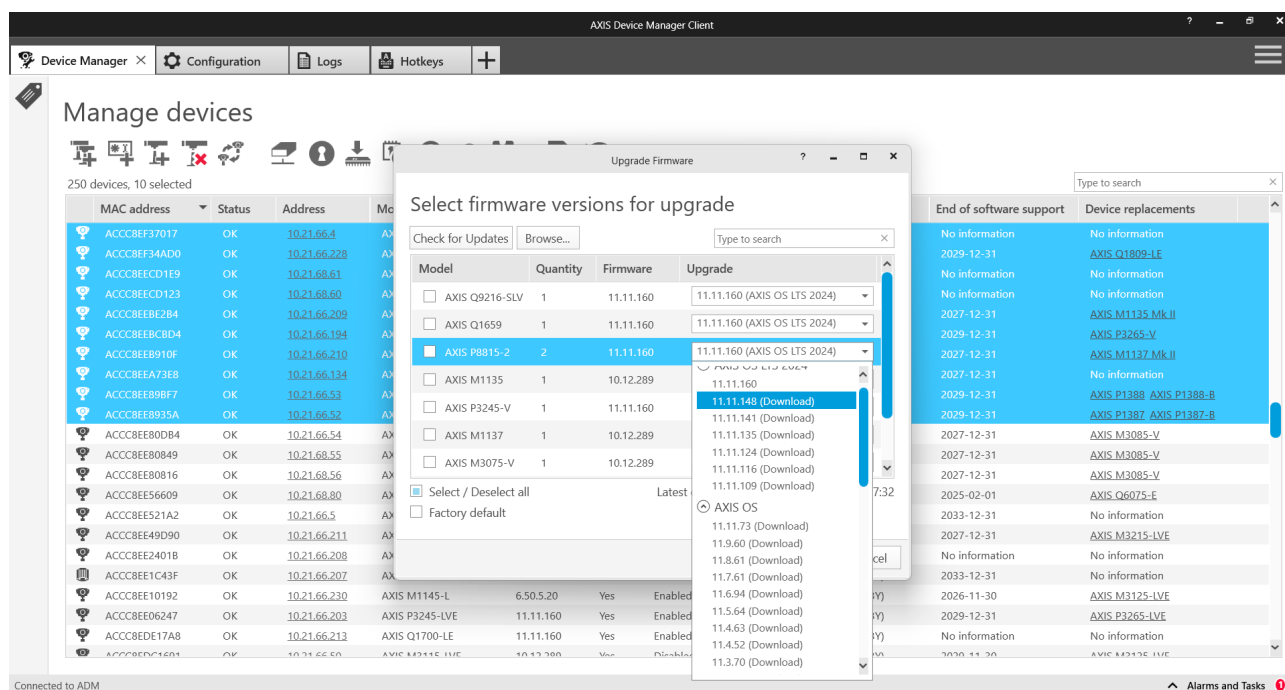
7

Aggiornamenti AXIS OS

Le versioni aggiornate di AXIS OS includono patch per le vulnerabilità note. È fondamentale utilizzare sempre il software più recente perché i malintenzionati potrebbero tentare di sfruttare vulnerabilità note. Altrettanto importante è la rapidità di distribuzione di una nuova versione del sistema operativo di AXIS, che aumenta le capacità operative ed elimina i rallentamenti collegati al roll-out manuale degli aggiornamenti delle nuove release. AXIS Device Manager si collega a www.axis.com e scarica le ultime versioni del sistema operativo AXIS o dei servizi applicabili. Se si preferisce non scaricare direttamente sulla rete da Internet, è possibile salvare gli aggiornamenti su una chiavetta USB e caricarli sul client AXIS Device Manager. Viene indicato anche se sono disponibili nuove versioni del sistema operativo AXIS e consente di distribuirli rapidamente sui dispositivi Axis.

Perché si devono sempre eseguire le ultime versioni del sistema operativo AXIS:

- La rete e i dispositivi sono protetti con le ultime patch contro vulnerabilità note, specialmente quelle critiche.
- I dispositivi vengono aggiornati con gli ultimi miglioramenti delle prestazioni e per risolvere bug e difetti.
- Si ottiene accesso immediato alle ultime funzionalità e ai miglioramenti delle funzionalità.



L'aggiornamento di AXIS OS con AXIS Device Manager è semplice grazie alle notifiche sullo schermo e alle finestre di dialogo intuitive.

Protezione aggiuntiva

L'adozione di un buon sistema per utenti e password e l'utilizzo di versioni aggiornate del sistema operativo AXIS consentono di ridurre i rischi comuni per i dispositivi. La *Guida all'hardening di AXIS* descrive ulteriori misure per ridurre i rischi all'interno di organizzazioni grandi e importanti. Questo include la disattivazione di servizi che potrebbero non essere utilizzati e l'abilitazione di servizi che possono aiutare a rilevare e monitorare i segnali di un attacco o di una violazione. AXIS Device Manager semplifica il processo di distribuzione di alcuni di questi sistemi. Axis fornisce un modello di configurazione per le impostazioni raccomandate di base.

Come proteggere i dispositivi con la Guida alla protezione Axis:

- Leggete la *Guida all'hardening di AXIS* e scaricare il file del modello alla fine del documento.
- Modificare il file di configurazione per selezionare gli elementi pertinenti.
- Selezionare i dispositivi nell'inventario di AXIS Device Manager.
- Fare clic con il pulsante destro del mouse e selezionare "Configure Devices > Configure..." (Configura dispositivi - Configura).
- Fare clic su "File di configurazione" e selezionare il file scaricato.
- Regolare le impostazioni in base alle esigenze.

Servizio di autorità di certificazione

A Autorità di certificazione (CA) è un servizio che rilascia certificati digitali a server, client o utenti. Una CA può essere pubblica o privata. Le CA pubbliche attendibili, come Comodo e Symantec (in precedenza Verisign), vengono in genere utilizzate per servizi pubblici quali siti Web pubblici ed e-mail.

Un CA privato (in genere un servizio di directory/certificato attivo) rilascia certificati per i servizi di rete interni/privati. In un sistema di gestione video, questo serve principalmente per la Crittografia HTTPS della rete e per il controllo degli accessi alla rete IEEE 802.1X. AXIS Device Manager include un servizio CA per i dispositivi Axis e può funzionare sia come CA private root che come CA intermedio privato; come parte di un'infrastruttura a chiave pubblica (PKI) aziendale.

I certificati firmati dalla CA sono utilizzati per i certificati IEEE 802.1X (client) e HTTPS (server).

HTTPS

HTTPS è la versione sicura di HTTP su cui vengono crittografate le comunicazioni tra un client e un server. I certificati autofirmati sono sufficienti per ottenere una connessione crittografata. Non vi è alcuna differenza nel livello di crittografia tra i certificati autofirmati e i certificati firmati dalla CA. La differenza è che i certificati autofirmati non proteggono dallo spoofing di rete, in cui un computer attaccante tenta di impersonare un server legittimo. I certificati firmati da CA aggiungono un punto di fiducia per i client per autenticare che stanno accedendo a un dispositivo fidato. Si noti che il client video (VMS) deve supportare la richiesta di video su HTTPS (RTP su RTSP su HTTPS) per poter crittografare il video.

IEEE 802.1X

Spesso definito semplicemente 802.1X, questo standard impedisce ai dispositivi di rete non autorizzati di accedere alla rete locale. Un dispositivo deve autenticarsi prima di poter accedere alla rete (e alle sue risorse). È possibile utilizzare diversi metodi di autenticazione: indirizzo MAC (filtraggio MAC), utente/password o certificato client. Il proprietario del sistema decide quale metodo usare e la scelta appropriata dipende da minacce, rischi e costi.

La gestione di un'infrastruttura 802.1X è un investimento. Richiede switch gestiti e server aggiuntivi, in genere un RADIUS (servizio utente di accesso remoto per l'autenticazione remota). L'utilizzo dei certificati client richiede una CA (privata o pubblica) in grado di rilasciare certificati client. Nella maggior parte dei casi l'infrastruttura ha bisogno di personale per gestirla e monitorarla.

The screenshot shows the AXIS Device Manager Client interface. The main window is titled 'Manage devices' and displays a list of 250 devices, with 6 selected. The list includes columns for MAC address, Status, and Address. A 'Secure communication' dialog box is open, showing options to 'Enable' or 'Disable' HTTPS, IEEE 802.1X, or both. The 'Enable' section has three radio buttons: 'Enable or renew HTTPS', 'Enable or renew IEEE 802.1X', and 'Enable or renew HTTPS and IEEE 802.1X'. The 'Disable' section has three radio buttons: 'Disable HTTPS', 'Disable IEEE 802.1X', and 'Disable HTTPS and IEEE 802.1X'. The 'Enable or renew HTTPS and IEEE 802.1X' option is selected. The dialog box also includes 'Help', '< Back', 'Next >', and 'Cancel' buttons. In the background, a table lists device details including MAC address, model, IP address, and status.

MAC address	Status	Address
ACCC8EF37017	OK	10.21.66.4
ACCC8EF34AD0	OK	10.21.66.22
ACCC8EECD1E9	OK	10.21.68.61
ACCC8EECD123	OK	10.21.68.61
ACCC8EEB2B4	OK	10.21.66.21
ACCC8EEBCB04	OK	10.21.66.19
ACCC8EEB910F	OK	10.21.66.21
ACCC8EEA73E8	OK	10.21.66.11
ACCC8EE89BF7	OK	10.21.66.51
ACCC8EE8935A	OK	10.21.66.52
ACCC8EE80DB4	OK	10.21.66.54
ACCC8EE80849	OK	10.21.68.55
ACCC8EE80816	OK	10.21.68.56
ACCC8EE56609	OK	10.21.68.80
ACCC8EE521A2	OK	10.21.66.5
ACCC8EE49D90	OK	10.21.66.21
ACCC8EE2401B	OK	10.21.66.20
ACCC8EE1C43F	OK	10.21.66.20
ACCC8EE10192	OK	10.21.66.23
ACCC8EE06247	OK	10.21.66.203
ACCC8EDE17A8	OK	10.21.66.213
ACCC8EDC1601	OK	10.21.66.50

Configurazione dei certificati in AXIS Device Manager.

Gestione del ciclo di vita dei certificati

La gestione del ciclo di vita dei certificati è un mezzo per gestire in modo efficiente dal punto di vista dei costi tutti i processi e le attività relative all'emissione, all'installazione, all'ispezione, alla correzione e al rinnovo dei certificati nel tempo. AXIS Device Manager consente di gestire in modo efficiente i certificati permettendo agli amministratori di:

- Rilasciare certificati firmati dal CA quando non sono disponibili altri CA
- Gestire facilmente i certificati IEEE 802.1X
- Gestire facilmente i certificati HTTPS
- Controllare le date di scadenza del certificato
- Rinnovare facilmente i certificati prima della scadenza

Consigli per i CA private root e intermedi

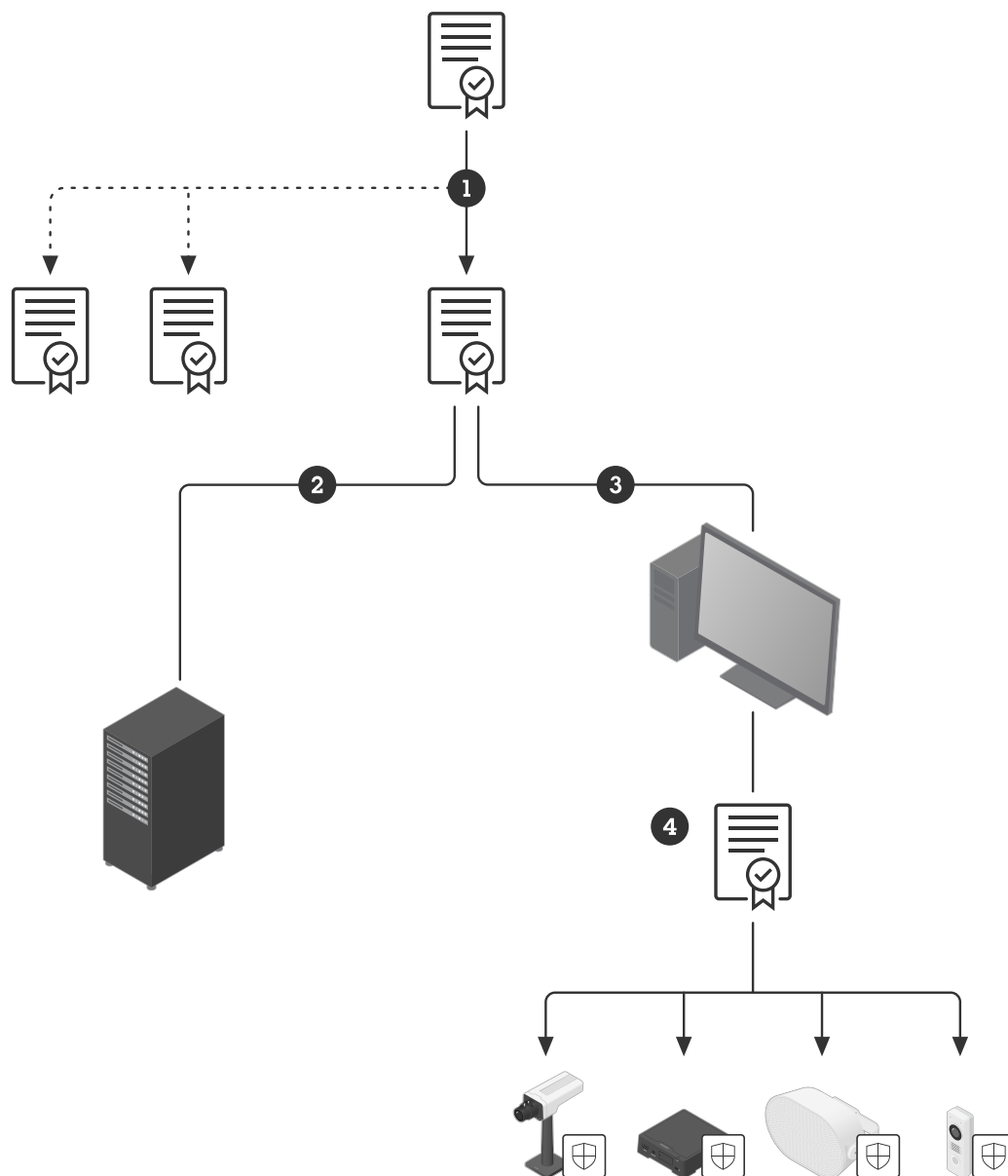
Non è consigliabile esporre i dispositivi Axis come server pubblici destinati al pubblico. Questo è il motivo per cui l'utilizzo di un CA pubblico per le risorse private non è economicamente conveniente.

Per HTTPS, il server VMS è l'unico client che deve convalidare l'accesso a una telecamera attendibile. I client operatore non accedono mai direttamente alle telecamere poiché i video in diretta e registrati sono forniti dal server VMS. In una tale situazione il valore per incorporare i certificati dei server delle telecamere in una PKI aziendale esistente è limitato.

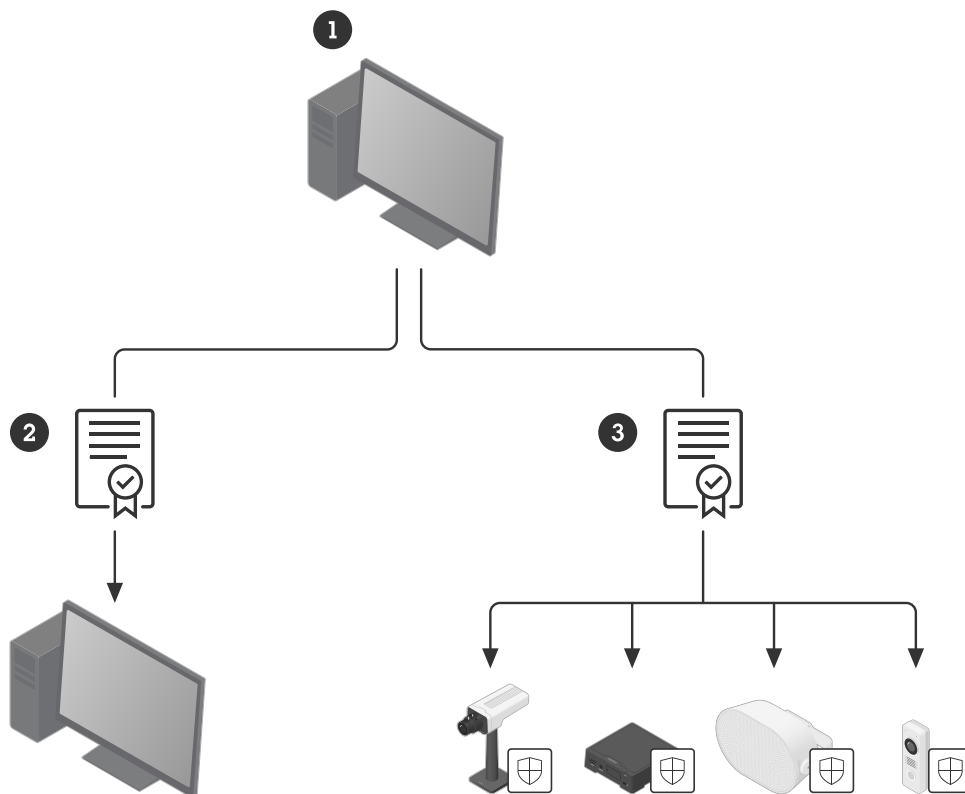
L'uso di AXIS Device Manager come CA privata è la soluzione più conveniente. Dopo aver generato un certificato CA radice, installare il certificato AXIS Device Manager nell'archivio certificati del server VMS. Se ci sono altri client che accedono direttamente alle telecamere (per la manutenzione o la risoluzione dei problemi), installare CA root di AXIS Device Manager anche in questi client.

Per 802.1X, la telecamera necessita di un certificato client per autenticarsi su un server RADIUS. Si consiglia di chiedere all'amministratore della PKI/CA aziendale di generare un certificato CA intermedio ed esportarlo come certificato PKCS#12 (P12) che può essere installato in AXIS Device Manager.

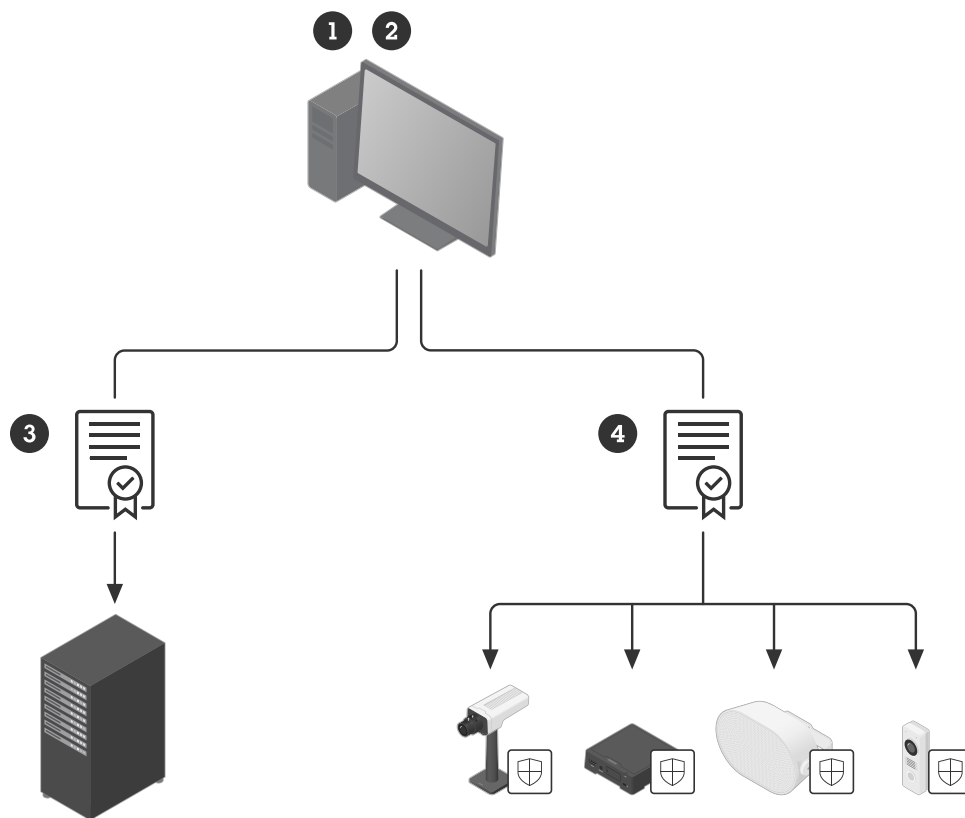
Per assistenza nell'impostazione di un server FreeRADIUS, visitare la sezione *Documenti tecnici* per AXIS Device Manager



La gestione di certificati HTTPS prevede: 1) la generazione del certificato CA intermedio o radice in AXIS Device Manager; 2) l'esportazione del certificato CA nel VMS e 3) il caricamento dei certificati del server nei dispositivi.



Utilizzo di un CA privato. La gestione di certificati IEEE 802.1X prevede: 1) la generazione del certificato cliente e CA intermedio; 2) l'installazione del certificato CA sul server Radius; 3) l'importazione del certificato CA in AXIS Device Manager e 4) il caricamento dei certificati CA e client nei dispositivi.



Utilizzo di AXIS Device Manager come CA. Per gestire i certificati IEEE 802.1X: 1) generare il certificato CA root in AXIS Device Manager; 2) importare il certificato CA di autenticazione in AXIS Device Manager; 3) installare il certificato CA sul server Radius; 4) caricare i certificati CA di autenticazione e client sui dispositivi.

Conclusioni

La gestione e il controllo della sicurezza sono parti importanti dell'implementazione di un approccio efficace alla sicurezza informatica. Si tratta di un processo continuo che richiede il mantenimento di uno stato chiaro e l'adozione di azioni appropriate per mitigare qualsiasi potenziale minaccia che possa avere un impatto sulla rete IP. AXIS Device Manager offre uno strumento per gestire i dispositivi e aumentare la sicurezza della rete. Contattare il rappresentante Axis locale o visitare il sito www.axis.com per ulteriori informazioni o supporto.

T10231485_it

2025-09 (M4.2)

© 2025 Axis Communications AB