Controllo di sicurezza con AXIS Device Manager

Versione 1.0

Indice

1. Introduzione

La cybersecurity diventa sempre più importante in settori come sicurezza e sorveglianza. Un'efficace sicurezza informatica richiede una profonda difesa per proteggere adeguatamente la rete IP a tutti i livelli, dai prodotti scelti e dai partner con cui si lavora ai requisiti che vengono impostati.

1.1 Tre livelli di protezione di sicurezza informatica

Sono tre i livelli di protezione di sicurezza informatica che offriamo:

1. Gestione della sicurezza: richiede controlli di sicurezza necessari per mitigare le minacce che si presentano. Può essere divisa in due parti: controlli di sicurezza e gestione economicamente efficace. I controlli di sicurezza sono misure di sicurezza o contromisure utilizzate per evitare, rilevare, neutralizzare o minimizzare i rischi per la sicurezza di proprietà fisiche, informazioni, sistemi informatici o altre risorse.

2. Gestione delle vulnerabilità: comprende tutto ciò che Axis fa per applicare le migliori procedure di sicurezza informatica nella progettazione, nello sviluppo e nel test dei nostri prodotti con lo scopo di minimizzare il rischio di errori. Quando vengono scoperte una o più vulnerabilità, le gestiamo e risolviamo prontamente, inviando inoltre avvisi di sicurezza.

3. Apprendimento e collaborazione: riguarda Axis, gli utenti ed i partner coinvolti nella rete IP, ottenendo e condividendo una chiara comprensione comune delle minacce, l'impatto che potrebbero avere e le modalità di protezione della rete.

1.2 Scopo del presente documento

Questa guida all'applicazione descrive come l'utilizzo di AXIS Device Manager rafforzi il sistema ed aumenti la sicurezza. Delinea gli aspetti chiave e descrive le raccomandazioni.

1.3 Informazioni su AXIS Device Manager

AXIS Device Manager è uno strumento semplice, economico e sicuro in grado di gestire tutte le principali attività dei dispositivi come la manutenzione, la sicurezza e l'installazione (vedere la tabella seguente). È adatto per gestire fino a un paio di migliaia di dispositivi Axis di un unico sito o migliaia di dispositivi su più siti. AXIS Device Manager consente di eseguire in modo efficente controlli di sicurezza informatica per proteggere i dispositivi di rete e allinearli ad un'infrastruttura di sicurezza.

Funzioni di AXIS Device Manager per la gestione dei dispositivi

Installazione	Manutenzione
> Assegnazione dell'indirizzo IP > Esportazione dell'elenco dei dispositivi e traccia delle risorse* > Gestione utenti e password* > Gestione ACAP > Aggiornamento del firmware* > Gestione dei certificati HTTPS* > Distribuzione dei certificati IEEE 802.1x* > Tagging dei dispositivi	> Stato dispositivo > Raccolta dei dati del dispositivo > Configurazione dei dispositivi e copia delle configurazioni in più dispositivi > Connessione a più server/sistemi > Punti di ripristino > Ripristino dei valori predefiniti di fabbrica > Sostituzione del dispositivo > Gestione e rinnovo dei certificati* > Protezione avanzata della sicurezza informatica*

**Indica la funzione di controllo della sicurezza informatica*

Figura 1. Gestione di più siti

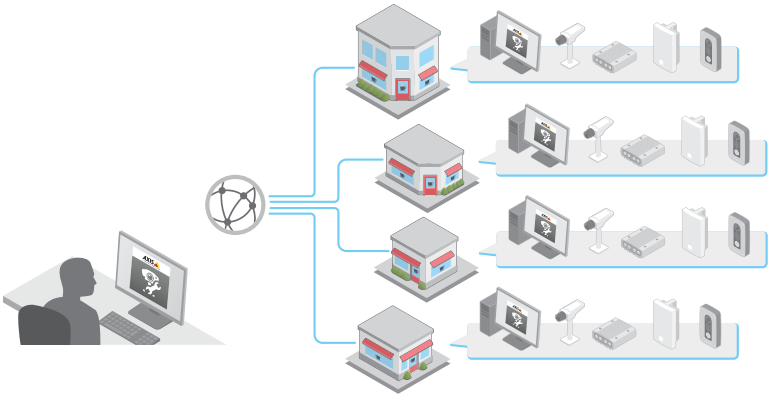


Figura 2. Aggiornamento del firmware

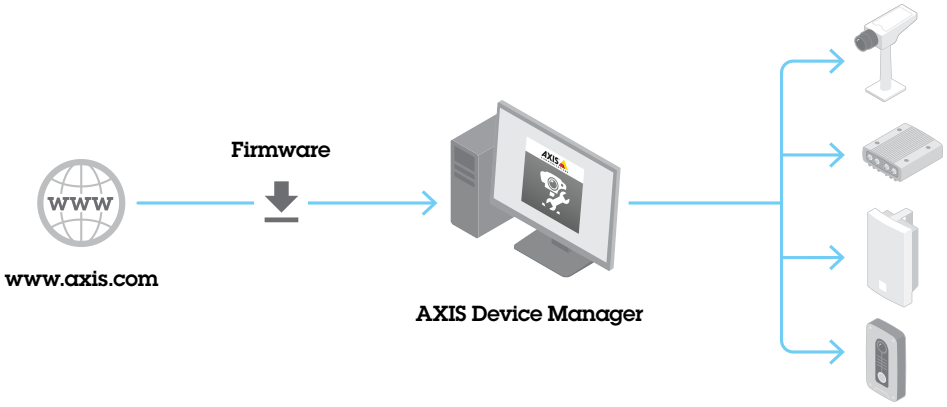
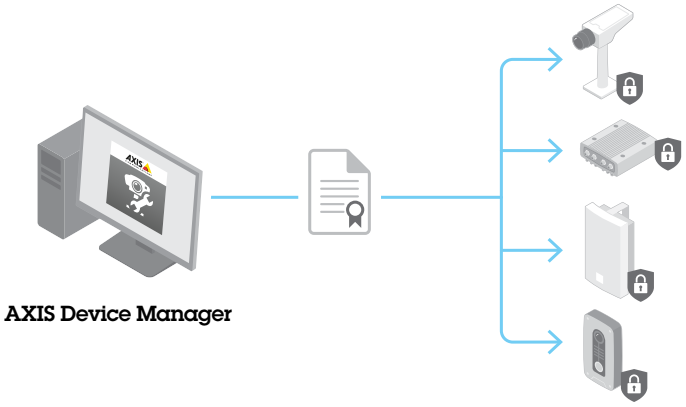


Figura 3. Gestione dei certificati



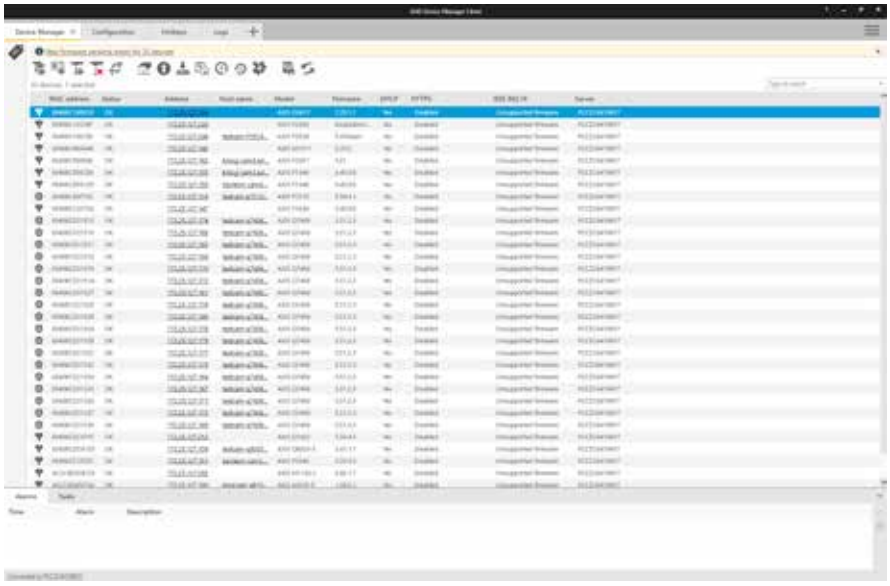
2. Inventario del dispositivo

Un aspetto fondamentale per garantire la sicurezza di una rete aziendale è mantenere un inventario completo di tutti i dispositivi. Durante la creazione o la revisione di policy di sircurezza, è importante disporre chiaramente delle conoscenze e della documentazione di ciascun dispositivo e non solo delle risorse critiche. Questo perché ogni singolo dispositivo può fungere da accesso 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 essenziale per la sicurezza di una rete aziendale. AXIS Device Manager aiuta in quanto:

> Consente di accedere facilmente all'inventario corrente e completo dei dispositivi di rete quando si lavora con controlli e operatori del pronto intervento
> Fornisce un elenco completo dei dispositivi, ordinati per: numero totale, tipo, numero di modello e così via.
> Fornisce lo stato di rete di ogni dispositivo

Suggerimenti
AXIS Device Manager consente di accedere automaticamente all'elenco di tutti i dispositivi di rete Axis in tempo reale. Consente di identificare, elencare e ordinare automaticamente i dispositivi. Inoltre, è possibile utilizzare i tag in modo da poter raggruppare e ordinare i dispositivi in base a criteri personali. In questo modo è facile ottenere una panoramica di tutti i dispositivi Axis nella rete.



AXIS Device Manager fornisce una chiara lista dei dispositivi.

3. Account e password

L'autenticazione ed il controllo dei privilegi è una parte importante della protezione delle risorse di rete che aiuta a limitare il rischio di uso improprio accidentale o intenzionale per un periodo di tempo più lungo. Una parte fondamentale è ridurre il rischio di compromettere le password. Le password complesse sono importanti. Tuttavia, le password del dispositivo possono diffondersi all'interno di un'organizzazione e quando accade, si perde il controllo su chi può accedervi. AXIS Device Manager aiuta a gestire facilmente più account e password per i dispositivi Axis.

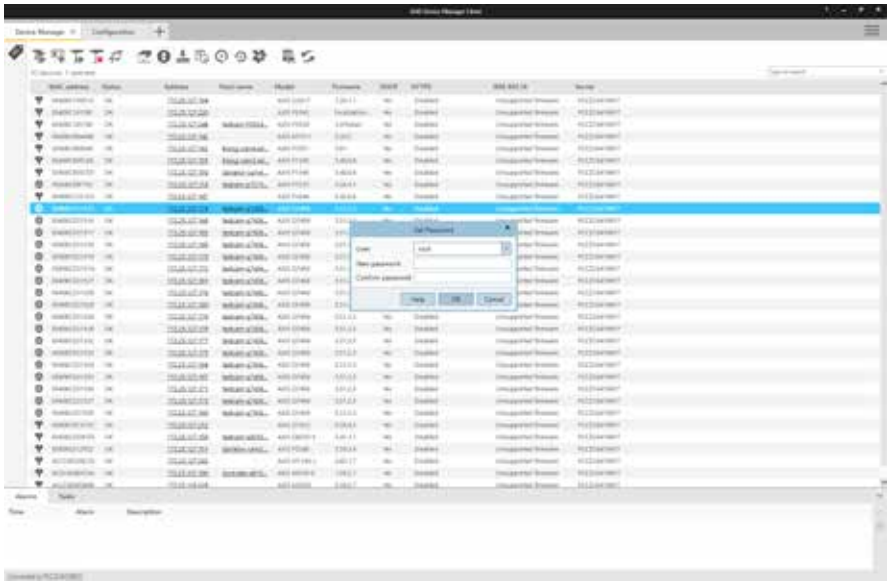
Perchè si dovrebbe avere più di un account nei dispositivi
> Poter controllare i livelli di autorizzazione per diversi tipi di utenti (macchine e persone)
> Ridurre il rischio di compromettere la password radice (master)
> Poter reimpostare le credenziali per un tipo di utente senza influire sugli altri

Utilizzo dei privilegi in AXIS Device Manager
In AXIS Device Manager, i dispositivi Axis possono supportare più account e appartengono a tre diversi livelli di autorizzazione: visitatore, operatore e amministratore. Di seguito viene descritto come è possibile gestire i privilegi per le telecamere di rete Axis.

I visitatori possono accedere al video e controllare PTZ. Le persone con diritti di operatore possono ottimizzare le impostazioni della telecamera e i profili del flusso video. 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.

Passaggi consigliati da seguire

> Si consiglia di inserire le telecamere ad AXIS Device Manager prima di aggiungerle al VMS
> Selezionare tutte le telecamere presenti in AXIS Device Manager e creare un nuovo account utente chiamato "vms" (o nome simile) ed impostare una password complessa. Le autorizzazioni devono essere allineate con i requisiti del VMS, operatore o amministratore (verificare con il produttore).
> Aggiungere i dispositivi al VMS con l'account "vms" e la password definiti
> Tornare ad AXIS Device Manager e selezionare nuovamente tutte le telecamere e reimpostare (modificare) la password dell'account "radice" con una nuova password complessa. La password dell'account "radice" deve essere nota solo ad un numero limitato di persone (coloro che utilizzano AXIS Device Manager).
> Quando qualcuno all'interno dell'organizzazione deve utilizzare un browser Web per accedere ad un dispositivo per attività di manutenzione o risoluzione dei problemi, non fornire loro la password radice. Utilizzare AXIS Device Manager per creare un nuovo account (temporaneo) per i dispositivi selezionati con privilegi di amministratore o operatore. Una volta completata l'attività, utilizzare AXIS Device Manager per rimuovere l'account temporaneo.
> AXIS Device Manager supporta amministratori locali, utenti e gruppi di dominio. È possibile utilizzare un amministratore locale solo se si accede al client AXIS Device Manager dalla stessa macchina che ospita il server AXIS Device Manager. Si consiglia di utilizzare gli utenti del dominio se la persona che gestisce il sistema utilizzerà client remoti.



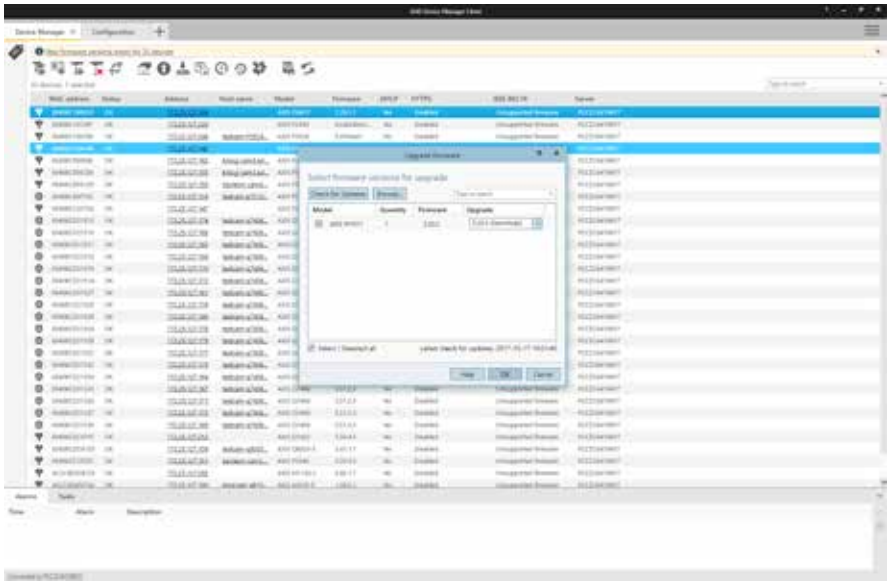
Modifica dei ruoli utente e delle password in AXIS Device Manager.

4. Aggiornamenti del firmware

Le ultime versioni del firmware includono patch per le vulnerabilità note. È fondamentale utilizzare sempre il software più recente perché i malintenzionati potrebbero tentare di sfruttare eventuali vulnerabilità note. Inoltre, la rapida installazione del nuovo firmware aumenta le capacità operative e rimuove i colli di bottiglia legati alla distribuzione manuale di nuove versioni. AXIS Device Manager si connette ad www.axis.com e scarica il firmware o le versioni di servizio più recenti applicabili. E' possibile sia eseguire un download attraverso internet direttamente sulla rete, sia salvare gli aggiornamenti su una chiavetta USB e caricarli sul client AXIS Device Manager. Mediante l'indicazione di disponibilità di nuovi firmware e consente di distribuirli rapidamente sui dispositivi Axis.

Perché si devono sempre eseguire gli aggiornamenti del firmware

> 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 eventuali bug o difetti conosciuti
> Si ottiene immediatamente la possibilità di accedere ai miglioramenti e alle ultime funzionalità



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

5. Protezione aggiuntiva

Una buona policy utente/password, così come il funzionamento dei dispositivi con versioni di firmware aggiornate,attenueranno i rischi più comuni legati ai dispositivi. La Guida alla protezione Axis descrive ulteriori misure per ridurre i rischi all'interno di organizzazioni importanti e di grandi dimensioni. Ciò include la disattivazione di servizi che non possono essere utilizzati e l'abilitazione di servizi che possono aiutare a rilevare e monitorare l'indicazione di un attacco o una violazione.

AXIS Device Manager semplifica il processo di distribuzione di alcuni di questi criteri. Axis fornisce un modello di configurazione per le impostazioni raccomandate di base. Per ulteriori informazioni vedere: www.axis.com/products/axis-device-manager/support-and-documentation.

Come proteggere i dispositivi grazie alla Guida alla protezione Axis

> Scaricare il file di configurazione del modello di protezione da www.axis.com/products/axis-device-manager/support-and-documentation
> Modificare il file di configurazione per scegliere gli elementi pertinenti
> Selezionare i dispositivi
> Fare clic con il pulsante destro del mouse e selezionare "Configura dispositivi | Configura..."
> Fare clic su "File di configurazione" e selezionare il file scaricato
> Regolare le impostazioni secondo le necessità

6. Certificate Authority Service

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.

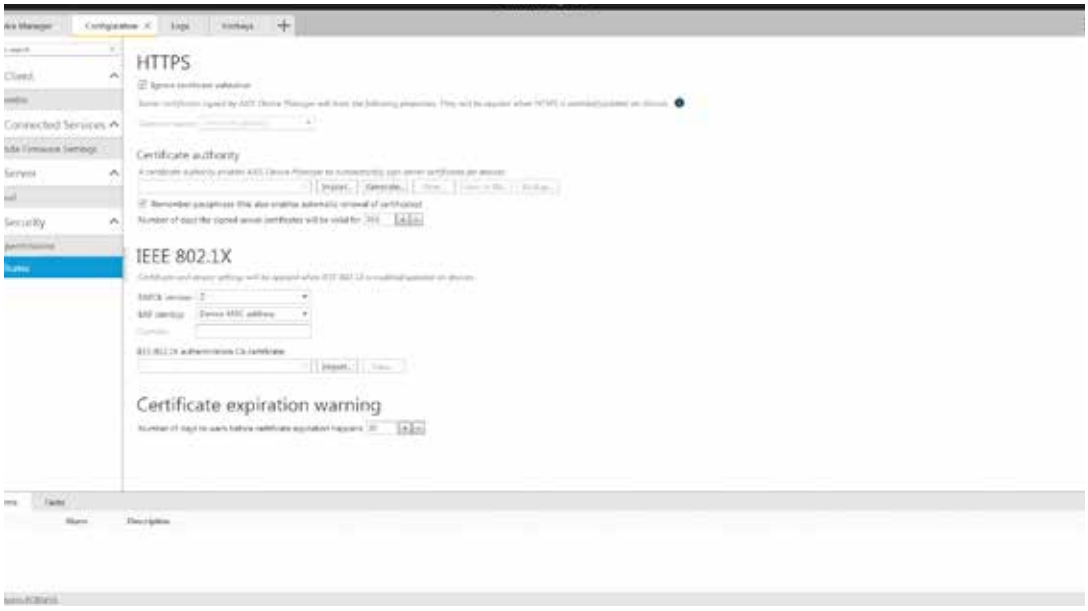
Una CA privata (in genere un servizio di directory/certificato) rilascia certificati per i servizi di rete interni/privati. In un sistema di gestione video, principalmente rilascia certificati per Hyper Text Transfer Protocol Secure (HTTPS) (crittografia di rete) e IEEE 802.1x (controllo di accesso alla rete) AXIS Device Manager include un servizio di CA per i dispositivi Axis e può operare come CA radice privata o CA intermedia privata, parte di una Public Key Infrastructure (PKI) aziendale.

I certificati firmati dalla CA sono utilizzati sia per i certificati IEEE 802.1x (client) che per 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 della rete, in cui un computer malintenzionato tenta di impersonare un server legittimo. I certificati firmati dalla CA aggiungono un punto di attendibilità ai client per l'autenticazione dell'accesso ad un dispositivo attendibile. 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
Chiamato anche 802.1X, questo standard impedisce ai dispositivi di rete non autorizzati di accedere alla rete locale. E' necessario autenticarsi prima di poter accedere alla rete (e alle sue risorse). Esistono diversi metodi di autenticazione che possono essere utilizzati, ad esempio: indirizzo MAC (filtro MAC), utente/password o certificato client. In seguito ad un'accurata valutazione di minacce, rischi e costi, il proprietario del sistema decide quale metodo utilizzare.

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 per poter essere monitorata e gestita, un'infrastruttura, ha bisogno di personale.



Configurazione dei certificati in AXIS Device Manager.

7. Gestione del ciclo di vita dei certificati

La gestione del ciclo di vita dei certificati è un mezzo per gestire in modo economico tutti i processi e le attività relative al rilascio, all'installazione, all'ispezione, al controllo e al rinnovo dei certificati per un lungo periodo di tempo. AXIS Device Manager consente di gestire in modo efficiente i certificati consentendo agli amministratori di:

> Rilasciare certificati firmati dalla CA quando non sono disponibili altre CA
> Distribuire facilmente i certificati IEEE 802.1X
> Distribuire facilmente i certificati HTTPS
> Controllare le date di scadenza del certificato
> Rinnovare facilmente i certificati prima della scadenza

Raccomandazioni della CA intermedia e radice privata
Non è consigliabile esporre i dispositivi Axis come server pubblici destinati al pubblico. Questo è il motivo per cui l'utilizzo di una CA pubblica 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 la CA radice 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.

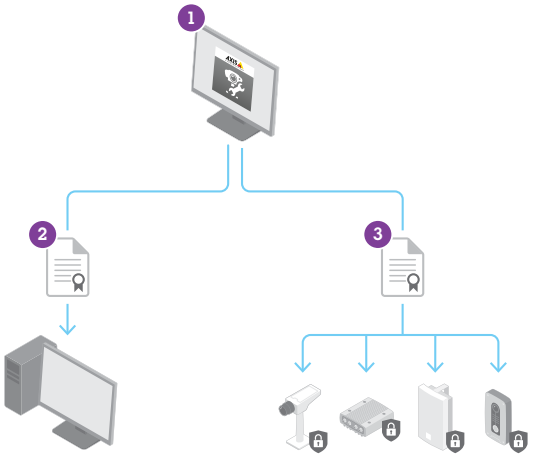


Figura 4, sinistra: La gestione dei certificati HTTPS implica:
1) la generazione del certificato CA intermedio o radice in AXIS Device Manager; 2) l'esportazione del certificato CA nel VMS e 3) il caricamento dei certificati del server nei dispositivi.

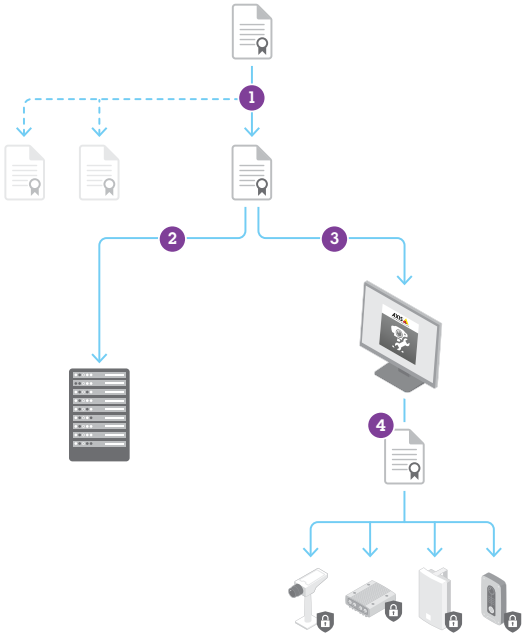


Figura 5, destra: La distribuzione dei certificati IEEE 802.1X implica: 1) la generazione del certificato cliente e CA intermedio; 2) l'installazione del certificato CA sul server Radius; 3) l'importazione del certificato CA in AXIS Device Manager e 4) il caricamento dei certificati CA e client nei dispositivi.

8. Conclusione

La gestione e il controllo della sicurezza sono parti importanti se si desidera un'efficiente sicurezza informatica. Si tratta di un processo continuo che richiede la gestione di uno stato chiaro e l'esecuzione 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 visitate il sito www.axis.com per ulteriori informazioni o supporto.

Informazioni su Axis Communications

Axis offre soluzioni di sicurezza intelligenti che consentono un mondo più intelligente e più sicuro. In qualità di leader del mercato dei video di rete, Axis è alla guida del settore lanciando continuamente prodotti di rete innovativi basati su una piattaforma aperta che offre un valore elevato ai clienti attraverso una rete di partner globale. Axis ha relazioni a lungo termine con i partner e fornisce loro le conoscenze e i prodotti di rete innovativi nei mercati nuovi ed esistenti.

Axis ha oltre 2.700 dipendenti dedicati in oltre 50 paesi in tutto il mondo, con il supporto di una rete globale di oltre 90.000 partner. Fondata nel 1984, Axis è una società con sede in Svezia, presente nelle quotazioni NASDAQ Stockholm con la sigla Axis.

Per ulteriori informazioni su Axis, si prega di visitare il nostro sito web su www.axis.com.

AXIS® COMMUNICATIONS