AXIS Device Manager

Manuale dell'utente

Indice

Informazioni su AXIS Device Manager

AXIS Device Manager è un'applicazione software di installazione e gestione per prodotti Axis. Questo software può cercare automaticamente periferiche in rete, assegnare indirizzi IP, impostare password, visualizzare lo stato della connessione e gestire aggiornamenti firmware, certificati e la configurazione di più dispositivi.

AXIS Device Manager comprende:

- AXIS Device Manager Service Control: il server che gestisce tutte le comunicazioni con i prodotti Axis
- AXIS Device Manager Client: l'interfaccia utente front-end che abilita la gestione da remoto da internet o dalla rete aziendale

Allo stesso server possono essere connessi più client. Un client può essere connesso contemporaneamente a più server.

AXIS Device Manager è anche molto utile per irrobustire il sistema e aumentare la sicurezza. Per ulteriori informazioni, consultare la *Guida alla sicurezza di AXIS Device Manager.*

Impostazioni preliminari

Installazione del software

Per installare AXIS Device Manager 5, assicurarsi di disporre di tutti i diritti di amministratore sul computer in cui si esegue l'installazione, quindi procedere come segue:

1. *Andare alla pagina del dispositivo in axis.com e scaricare il file di installazione per l'app desktop AXIS Device Manager*
2. Eseguire il programma di installazione e seguire le istruzioni sullo schermo.

Nota

Se non è già installato, verrà installato il framework Microsoft .NET 4.8 (incluso nel file di installazione). L'operazione può durare alcuni minuti. Il framework Microsoft .NET 4.8 può essere installato anche tramite Windows Update prima dell'installazione di AXIS Device Manager.

Connessione a un server

Quando si avvia AXIS Device Manager per la prima volta, viene chiesto di connettersi a un server. Il server può essere eseguito sul computer locale o su un server remoto.

Per accedere come utente locale di Windows:

1. Selezionare **This computer (questo computer)**.
2. Selezionare **Log on as current user (accedi come utente corrente)** per accedere utilizzando le tue credenziali attuali.

Per accedere come un altro utente sul server o sul dominio:

- selezionare **Other user (altro utente)**.
- In **Other user (altro utente)**, inserire le credenziali dell'account.
- Selezionare **Remember me (ricordami)** per saltare questo passaggio la prossima volta che si esegue il client.
- Fare clic su **Log on (Accesso)**.

Nota

Per cancellare le credenziali salvate per tutti i server, andare a una schermata di accesso e selezionare **Delete saved passwords (eliminare le password salvate)**.

Per accedere a un server remoto:

1. Selezionare **Server remoto**.
2. Selezionare un server dall'elenco a discesa o inserire l'indirizzo IP o DNS nel relativo campo.
3. Inserisci le tue credenziali
4. Fare clic su **Log on (Accesso)**.

Nota

questa opzione non può essere usata se si accede a un server remoto da un computer che non fa parte di un dominio Windows.

Connessione a più server

È possibile collegarsi a più server con AXIS Device Manager. Una volta effettuato l'accesso a un server, è possibile passare da un server all'altro nel menu principale.

1. Andare al menu principale > Server > Nuova connessione
2. Scegliere se collegarsi al tuo computer o a un server remoto come descritto sopra.

Configurare il server

Dopo aver installato il server AXIS Device Manager sul computer, è possibile avviare e arrestare il server e modificare le relative impostazioni mediante Controllo del servizio.

Per configurare il server:

1. Per modificare le impostazioni, fare doppio clic sull'icona per aprire **Controllo del servizio AXIS Device Manager**
2. Spuntare la casella di controllo **Modify settings** (Modifica impostazioni)
3. Assegnare un nome al server. Nome del server identifica il server ed è visualizzato nel client AXIS Device Manager quando il client è collegato a più server. Il nome predefinito è quello del computer su cui è stata effettuata l'installazione del software.
4. Digitare la Porta HTTP. Il numero di porta HTTP predefinito è: 55762.
5. Digitare la porta TCP. Il numero di porta TCP predefinito è: 55764.

Nota

Il numero di porta del server deve essere compreso tra 1024 e 65533. Il numero di porta TCP sarà sempre equivalente al numero di porta del server + 2. Ad esempio, se il numero di porta del server è 55765, il numero di porta TCP sarà 55767.

Nota

Per installazioni più ampie, consigliamo AXIS Device Manager Service Administration. Si tratta di un'applicazione per consolle che può essere utilizzata a partire dal prompt dei comandi o da uno script batch per avviare e arrestare il servizio, eseguire backup del database, ecc. L'applicazione "AdmAdminConsole.exe" è situata nella directory di installazione del server.

Configurazione iniziale

Per iniziare è necessario fare queste cose:

- aggiungere dispositivi e creare account utente, vedere: *Aggiunta di dispositivi, on page 6*
- Fornire un rafforzamento della sicurezza informatica al tuo sistema. Vedere *Installazione certificati, on page 9*

Gestione dei dispositivi

Aggiunta di dispositivi

AXIS Device Manager cerca automaticamente la rete dei dispositivi connessi e tenta di accedere a tutti i dispositivi. Nell'elenco dei dispositivi trovati viene indicato l'indirizzo dei dispositivi (indirizzo IP o nome di host), il numero di serie, il modello e lo stato. Il numero di serie (S/N) è stampato sull'etichetta del prodotto.

Per aggiungere dispositivi dall'elenco:

1. Selezionare i dispositivi da aggiungere e fare clic su **Next (Avanti)**.
2. Selezionare **Use host name when possible (Usa nome host quando è possibile)**. Se un dispositivo viene aggiunto usando il suo nome host, quest'ultimo sarà utilizzato per tutte le ulteriori comunicazioni con il dispositivo. Se non è disponibile un nome host, verrà usato l'indirizzo IP.
3. Impostare la password per i dispositivi senza password. Se non si desidera impostare una password, selezionare **Skip (Salta)**.
4. Fare clic su **Next (Avanti)**.

Nella pagina "Pronto per l'aggiunta di dispositivi" vengono mostrati i dispositivi da aggiungere.

5. Fare clic su **Finish (Fine)** per aggiungere i dispositivi.

Rimuovi dispositivi

Per rimuovere dispositivi dall'elenco:

1. Andare a **User management (Gestione del dispositivo)**.
2. selezionare i dispositivi;
3. Fare clic con il pulsante destro del mouse e selezionare **Remove (Rimuovi)**.
4. Fare clic su **Sì**.

Sostituire i dispositivi

Per sostituire un dispositivo AXIS Device Manager, collegare un nuovo dispositivo e riutilizzare la configurazione di un dispositivo esistente. Il dispositivo sostituito verrà eliminato se la sostituzione ha esito positivo. Deve essere presente almeno un punto di ripristino per tale dispositivo, vedere *Creare punto di ripristino, on page 8*. Nessun punto di ripristino verrà trasferito al nuovo dispositivo.

1. Andare a **User management (Gestione del dispositivo)**.
2. Andare alla barra degli strumenti e fare clic sull'icona sostituisci dispositivo.
3. Selezionare un dispositivo da sostituire e fare clic su **OK**.
4. Selezionare il dispositivo che si vuole sostituire e fare clic su **OK**.
5. Fare clic su **Avanti** per ripristinare una configurazione di dispositivo dal più recente punto di ripristino.
6. Andare a **Parameters (Parametri) > Additional Settings (Impostazioni aggiuntive)** e selezionare i parametri e le impostazioni da applicare.
7. Fare clic su **Next (Avanti)**.
8. Fare clic su **Fine** per applicare le impostazioni.

Ripristina dispositivi

È possibile riportare uno o più dispositivi a punti di ripristino creati precedentemente. Per ripristinare dispositivi, ciascun dispositivo deve avere almeno un punto di ripristino disponibile. Per impostazione predefinita, ogni notte vengono creati e rimossi automaticamente punti di ripristino per tutti i dispositivi associati al server selezionato. Un numero predeterminato di recenti punti di ripristino automatici vengono mantenuti a scopo di ripristino.

Ripristino di dispositivi a un punto di ripristino precedente:

1. andare all'area di lavoro **Device Management (Gestione dispositivo)**.
2. Selezionare uno o più dispositivi da ripristinare.
3. Con il tasto destro del mouse cliccare e selezionare **Backup / Restore (Backup/ripristino) > Restore to a Previous Time (ripristinare in un momento precedente)** dal menu a discesa.
4. Selezionare un punto di ripristino sull'elenco dei punti di ripristino più recenti e fare clic su **Avanti**.
5. Verificare le impostazioni per ciascun dispositivo e fare clic su **Fine**.

Installare le app

Un'app è un software che può essere scaricato e installato sui dispositivi Axis. Le app possono essere installate sui dispositivi che supportano AXIS Camera Application Platform. Aggiungono funzionalità al dispositivo, ad esempio per il rilevamento, il riconoscimento, il tracking e il conteggio. Le app devono essere prima scaricate da *axis.com* o dal sito web del fornitore dell'app. Alcune applicazioni, inoltre, richiedono una versione AXIS OS o un modello di dispositivo specifici. Se l'app richiede una licenza, il file della chiave di licenza può essere installato contemporaneamente all'app o in un momento successivo mediante le pagine di configurazione del dispositivo. Se non si riesce a installare un'app, visitare il sito web *axis.com* e controllare che il modello del dispositivo e la versione di AXIS OS supportino AXIS Camera Application Platform.

Per installare un'app:

1. Andare all'indirizzo *axis.com* e scaricare l'app.
2. Andare a **Browse to Application** (Sfoglia per trovare l'app).
3. Fare clic su **Browse** (Sfoglia) e andare alla cartella dei download.
4. Selezionare l'app e fare clic su **Next** (Avanti)

Se l'app richiede una licenza per essere avviata, è necessario disporre di un file di licenza già scaricato; in caso contrario, fare clic su **No** e procedere al punto 8:

5. Selezionare **Yes** (Sì) e fare clic su **Next** (Avanti)
6. Fare clic su **Browse (Sfoglia)** e selezionare il file di licenza.
7. Fare clic su **Next (Avanti)**.
8. Selezionare il tipo di installazione desiderata:
   - **Downgrade dell'applicazione** consente di installare una versione precedente delle applicazioni.
   - **Sovrascrittura dell'applicazione** consente di reinstallare le applicazioni.

Nota

il downgrade o la sovrascrittura dell'applicazione consente di ripristinare le impostazioni dell'applicazione sui dispositivi.

Pronto per l'installazione
Vengono elencati i dispositivi sui quali verranno installate le app. Le app sono già installate su alcuni dispositivi, le applicazioni precedenti vengono sovrascritte. La sovrascrittura rimuove tutte le impostazioni dell'app.

9. Fare clic su **Finish** (Fine).

Configurazione

Gestione dei punti di ripristino

Un punto di ripristino è una configurazione di dispositivo salvata che può essere utilizzata per eseguire un backup e ripristinare le impostazioni del dispositivo. Ogni notte vengono creati punti di ripristino automatici per tutti i dispositivi riconfigurati che si trovano su un server. Se non è stata modificata alcuna impostazione su un dispositivo a partire dall'ultimo punto di ripristino, non verrà creato alcun nuovo punto di ripristino. Per ottenere la massima capacità di archiviazione, i punti di ripristino più vecchi vengono rimossi automaticamente. Un numero predeterminato di recenti punti di ripristino automatici vengono mantenuti a scopo di ripristino.

Creare punto di ripristino

Per creare un punto di ripristino manuale:

- andare all'area di lavoro **Device Management (Gestione dispositivo)**.
- Selezionare uno o più dispositivi da ripristinare.
- Fare clic con il pulsante destro del mouse e selezionare **Backup / Ripristino > Crea punti di ripristino**.
- Digitare una descrizione che identifichi il punto di ripristino.
- Fare clic su **OK**.

Nota

i punti di ripristino creati manualmente non vengono rimossi automaticamente.

Creazione automatica di punti di ripristino

Se è presente più di un server, selezionare il server da configurare sull'elenco dei server.

- Selezionare **Opzioni > Impostazioni punti di ripristino**.
- Selezionare **Crea automaticamente punti di ripristino** per abilitare la creazione automatica di punti di ripristino.
- Immettere il numero di punti di ripristino automatici da salvare e fare clic su **OK**.

Gestione di più credenziali

Questa funzionalità fornisce ad AXIS Device Manager le credenziali per un account amministratore dei dispositivi.

Digitare manualmente le credenziali del dispositivo

Se si sceglie di inserire manualmente le credenziali del dispositivo, queste verranno aggiornate in AXIS Device Manager per i dispositivi selezionati.

- Selezionare uno o più dispositivi
- Fare clic con il tasto destro del mouse e selezionare **Advanced (Avanzato) -> Enter Device Credentials (inserire le credenziali del dispositivo)** dal menu a discesa.

Nota

Le credenziali che non si possono verificare per il dispositivo non verranno aggiornate. É necessario usare la stessa password e lo stesso nome utente per tutti i dispositivi che partecipano a tale operazione.

Utilizzare un file CSV per le diverse credenziali

Utilizzando un file CSV è possibile utilizzare password e nomi utente separati per ciascun dispositivo. L'indirizzo MAC, l'indirizzo IP o l'indirizzo host vengono utilizzati per mappare le righe del file CSV con i dispositivi corrispondenti nel database di Axis Device Manager.

Quando si utilizza un file CSV, l'interfaccia utente chiede di specificare come interpretare le colonne del file CSV.

Nota

Come specificare a quale dispositivo appartiene una riga del file CSV.

Una colonna del file CSV deve contenere indirizzi MAC, indirizzi IP o indirizzi host, quindi è necessario specificare una colonna del file CSV da interpretare come indirizzo MAC, IP o host. Ciò è necessario per specificare a quale dispositivo appartengono i dati di una riga del file CSV. Inoltre, è possibile specificare una colonna da interpretare come nome del server. In questo modo, è possibile distinguere le righe del file CSV che si riferiscono a dispositivi di server Axis Device Manager diversi, ma con lo stesso indirizzo IP o host. Se non è necessaria questa distinzione, è inutile avere una colonna da interpretare come nome del server. In un'impostazione in cui un server utilizza lo stesso indirizzo IP o indirizzo host per diversi dispositivi, ma usa le porte per distinguerli l'uno dall'altro, è possibile specificare una colonna da interpretare come Porta. Se non è necessaria una distinzione sulla porta, di solito non c'è motivo di interpretare una colonna come Porta. Un'opzione per fornire la porta in una colonna dedicata è quella di indicare la porta insieme all'indirizzo IP o all'indirizzo dell'host. L'indirizzo IP o l'indirizzo dell'host deve essere seguito da due punti e dal numero di porta.

Installazione certificati

Informazioni su certificati

AXIS Device Manager fornisce le impostazioni per la gestione dei certificati client e server. I certificati client sono utilizzati per IEEE 802.1X e i certificati server sono utilizzati per HTTPS. Per applicare le modifiche, selezionare i dispositivi appropriati in Gestione dispositivo e quindi selezionare Abilita/Aggiorna nel menu contestuale.

Creare un'autorità di certificazione (CA)

Un'autorità di certificazione consentirà di abilitare HTTPS e IEEE 802.1X sui dispositivi senza alcun certificato server e client. L'autorità di certificazione indica ai dispositivi di creare certificati con le proprie chiavi private, firmarle e installarle

Per creare un'autorità di certificazione:

- Andare alla scheda **Configuration (Configurazione)**.
- Andare a **Security (Sicurezza) > Certificates (Certificati)**
- In **Certificate authority (Autorità di certificazione)**, fare clic su **Generate... (Genera...)**
- Digitare una passphrase e conformarla.
- Fare clic su **OK**.

La CA sarà ora generata e pronta per l'uso.

Nota

Il tuo certificato autofirmato root e la chiave privata, protetta da una passphrase di tua scelta. Un certificato generato da AXIS Device Manager ha una durata di 3 anni. Se si desidera che AXIS Device Manager rinnovi in automatico i certificati server/client, è necessario selezionare la casella **Remember passphrase (Ricorda passphrase)**. Se non è configurata un'autorità di certificazione sarà necessario creare certificati client e server al di fuori di AXIS Device Manager. Verranno quindi persi i vantaggi della gestione certificati automatica,

Importa - Utilizzando la funzionalità di Importazione, è possibile importare un'autorità di certificazione esistente di un certificato pubblico e una chiave privata. Sarà necessario fornire una passphrase.

Salva nel file - Salva il certificato pubblico dell'autorità di certificazione nei formati .cer o .crt. Il file non conterrà la chiave privata e non verrà quindi crittografato.

Backup - Il backup di un'autorità di certificazione è consigliato se si verifica un errore hardware. Se selezionato, verrà effettuato il backup del certificato e della chiave privata dell'autorità di certificazione utilizzato da Axis Device Manager. I dati di cui è stato eseguito il backup verranno protetti dalla passphrase utilizzata per generare l'autorità di certificazione.

Avviso di scadenza certificato Verrà creata una notifica di sistema se un certificato è scaduto o sta per scadere. Ciò verrà applicato a tutti i certificati installati sui dispositivi collegati, ad eccezione delle CA installate al di fuori di AXIS Device Manager. L'avviso apparirà come allarme di sistema, nella colonna dello stato in Gestione dispositivi, come icone nella finestra di dialogo "Visualizza certificati installati" e nell'area di lavoro Configurazione.

Specificare quando si desidera che AXIS Device Manager notifichi che i certificati stanno per arrivare alla data di scadenza. Per impostazione predefinita, i certificati server e client generati da AXIS Device Manager verranno automaticamente rinnovati sette giorni prima che deve apparire l'avviso di scadenza. Per ricevere la notifica di quando è impostata la scadenza dell'autorità di certificazione, è necessario selezionare "ricorda passphrase".

Abilitare HTTPS

Per abilitare HTTPS, è necessario che su ogni dispositivo sia presente un certificato del server. AXIS Device Manager può utilizzare un'autorità di certificazione (CA) per accedere e installare i certificati del server per i dispositivi.

È possibile farlo anche in modo manuale:

1. Andare alla scheda **Device manager (Gestione dispositivi)**
2. Fare clic con il tasto destro del mouse su questi dispositivi e scegliere **Install server certificates (Installare i certificati del server)** per ogni dispositivo nel menu contestuale.

Su ogni dispositivo può essere presente un solo certificato del server prima di abilitare HTTPS. I certificati in eccesso possono essere eliminati dal menu contestuale.

3. Dopo aver installato i certificati, è possibile abilitare HTTPS nel menu contestuale.

Nota

Può essere eseguita una connessione con HTTP se non è disponibile una connessione sicura (HTTPS). Questa operazione serve per poter configurare i dispositivi non ancora sicuri.

Ignora convalida certificato

AXIS Device Manager non si connetterà a un dispositivo se il relativo certificato non è convalidato. Il certificato del server deve essere firmato dall'autorità di certificazione attiva in AXIS Device Manager o convalidato tramite Windows Certificate Store. Selezionando Ignora convalida certificato, AXIS Device Manager non verrà convalidato se il certificato inviato al dispositivo è sicuro o meno.

Per far sì che AXIS Device Manager ignori la convalida del certificato.

- Andare alla scheda **Configuration (Configurazione)**.
- In **HTTPS**, abilitare **Ignore certificate validation (Ignora la convalida del certificato)**.

Abilita 802.1X

Per abilitare IEEE 802.1X, è necessario che su ogni dispositivo sia presente un certificato del client. AXIS Device Manager può utilizzare un'autorità di certificazione (CA) per accedere e installare i certificati del client per i dispositivi.

È possibile, inoltre, eseguire l'operazione manualmente in Gestione dispositivi facendo clic con il pulsante destro del mouse sui dispositivi e installando i certificati client per ciascun dispositivo nel menu contestuale. Su ogni dispositivo può essere presente un solo certificato del client prima di abilitare IEE 802.1X. I certificati in eccesso possono essere eliminati dal menu contestuale. Dopo aver installato i certificati, è possibile abilitare IEEE 802.1X nel menu contestuale.

Sarà, inoltre, necessario un certificato CA di autenticazione IEEE 802.1X per utilizzare il protocollo IEEE 802.1X.

Versione EAPOL - Selezionare la versione di Extensible Authentication Protocol (EAP) che si desidera utilizzare.

Identità EAP - Inserire l'indirizzo MAC del dispositivo, il nome host o il testo personalizzato.

Personalizzato - Inserire il testo che funzionerà come identità EAP.

Certificato CA di autenticazione IEEE 802.1X - Oltre al certificato client, deve essere installato un certificato CA di autenticazione IEEE 802.1X. Per attivare IEEE 802.1X, è necessario solo il certificato pubblico e non la chiave privata, non è quindi necessaria alcuna passphrase. Il certificato CA di autenticazione IEEE 802.1X verrà installato quando si abilita o si aggiorna IEEE 802.1X.

Importa - Selezionare un certificato dell'autorità di certificazione che verrà installato sui dispositivi e utilizzato per convalidare il server di autenticazione. Il certificato CA può essere creato dall'autorità di certificazione in AXIS Device Manager o derivare da una fonte esterna.

Visualizza - Dettagli del certificato CA utilizzati durante il processo di autenticazione IEEE 802.1X.

Nome comune - Selezionare l'identità del dispositivo EAP o l'indirizzo IP del dispositivo. Se il campo personalizzato viene lasciato vuoto, verrà selezionato il nome host. Se c'è un problema con il nome host, verrà usato l'indirizzo IP come nome comune.

Configura impostazioni SIP

Per configurare le impostazioni SIP e della porta sui dispositivi selezionati, utilizzare l'assistente di configurazione. L'assistente di configurazione consente di mantenere il valore già presente nel dispositivo o di inserire un valore da applicare a tutti i dispositivi selezionati. È anche possibile caricare valori da un file CSV per applicare valori specifici per il dispositivo ai dispositivi selezionati.

Utilizzare una riga nel file CSV per ciascun dispositivo e una colonna per ciascun parametro da impostare. L'assistente di configurazione consente di specificare quali valori devono essere recuperati.

Per utilizzare un file CSV per le impostazioni specifiche per il dispositivo di più dispositivi:

1. andare all'area di lavoro **Device Management (Gestione dispositivo)**.
2. Selezionare i dispositivi in cui si desidera eseguire la configurazione.
3. Fare clic con il tasto destro del mouse e selezionare **Configure devices > Advanced > SIP configuration > Settings** (Configura dispositivi, Avanzate, Configurazione SIP, Impostazioni).
4. Se si desidera utilizzare un file CSV, verificare di averne autorizzato l'uso. Altrimenti, andare al punto 5.
   4.1. Fare clic su **Browse** (Sfoglia) e selezionare il file CSV che si desidera utilizzare.
   4.2. Fare clic su Next (Avanti)
   4.3. Scegliere come denominare le colonne del file CSV nel menu a discesa.
   4.4. Selezionare l'indirizzo MAC, l'indirizzo IPv4 o l'indirizzo host per una colonna nel file CSV e associarli ai dispositivi nelle righe.
5. Fare clic su **Next (Avanti)**.
6. Selezionare una delle seguenti impostazioni SIP e porta:
   - **Enable SIP (Abilita SIP)**: Abilitare SIP sui dispositivi selezionati.
   - **Allow incoming SIP calls (Consenti chiamate SIP in entrata)**: Consentire le chiamate SIP in entrata sui tuoi dispositivi.
   - **SIP port (Porta SPI)** : Assegnare un numero porta utilizzato per le chiamate SIP.
   - **TLS port (Porta TLS)**: Assegnare un numero di porta utilizzato per la crittografia TLS.
   - **RTP start port (Porta di avvio RTP)**: Assegnare un numero di porta RTP per il traffico audio.
7. Fare clic su **Next (Avanti)**.
8. Selezionare una delle seguenti impostazioni audio e di chiamata:
   - **Audio direction** - Choose between **Send only**, **Receive only** o **Send and receive** (Direzione audio, Scegli tra, Invia solo, Ricevi solo, Invia e ricevi).
   - **DTMF payload type (Tipo di payload DTMF)**: scegliere il tipo di payload DTMF per trasportare cifre, toni e segnali DTMF.
   - **Calling timeout (Timeout chiamata)**: Scegliere il numero di secondi di attesa prima che una chiamata vada in timeout.

- **Incoming call timeout (Timeout chiamata in entrata)**: Scegliere il numero di secondi di attesa prima che una chiamata in entrata vada in timeout.
- **End calls after (Termina le chiamate dopo)** Scegliere il numero di secondi di attesa prima che una chiamata in arrivo venga automaticamente terminata. È anche possibile scegliere di consentire una durata illimitata delle chiamate.

9. Fare clic su **Next (Avanti)**.
10. Selezionare uno dei seguenti parametri di attraversamento di traduzione di indirizzi di rete (NAT):
    - **ICE Enable (Abilita ICE)**: Abilita la connessione interattiva (ICE) sui dispositivi selezionati.
    - **TURN Enable (Abilita TURN)**: Abilita l'attraversamento utilizzando i relay intorno alla traduzione degli indirizzi di rete (TURN).
    - **TURN server address (Indirizzo server TURN)**: inserire l'indirizzo del server TURN.
    - **TURN username (Nome utente TURN)**: Inserire il nome utente TURN.
    - **TURN password (Password TURN)**: Inserire la password TURN.
    - **STUN Enable (Abilita STUN)**: Abilita le utilità di attraversamento della sessione per la traduzione degli indirizzi di rete (STUN)
    - **STUN server address (Indirizzo server STUN)**: inserire l'indirizzo del server STUN.
11. Fare clic su **Next (Avanti)**.
12. Riesaminare la configurazione dei dispositivi elencati.
13. Se tutto è in ordine, fare clic su **Finish (Fine)**.

Gestione degli account SIP

In Axis Device Manager è possibile configurare le impostazioni SIP e aggiungere o rimuovere utenti SIP.

Aggiungere utenti SIP

Per aggiungere utenti SIP, è necessario specificarli in un file CSV. È possibile creare un modello nell'assistente di configurazione.

Per generare un modello:

1. andare all'area di lavoro **Device Management (Gestione dispositivo)**.
2. Selezionare i dispositivi in cui si desidera eseguire la configurazione.
3. Fare clic con il pulsante destro del mouse e selezionare **Configure devices > Advanced > SIP configuration > Add SIP accounts** (Configura dispositivi, Avanzate, Configurazione SIP, Aggiungi utenti SIP)
4. Fare clic su **Generate template (Genera modello)**
5. Selezionare una posizione in cui salvare il file CSV.
6. Aggiungere gli utenti al file. Utilizzare una riga per ogni utente che si desidera aggiungere a un dispositivo. Per aggiungere più utenti a un dispositivo.

Il file CSV ha il seguente layout:

Nome colonna	Descrizione	Obbligatorio/ Facoltativo	Note
deviceIdentifier	Indirizzo MAC, indirizzo IP o indirizzo host	obbligatorio	Questa colonna specifica a quale dispositivo si aggiunge l'utente. Può essere un indirizzo MAC, un indirizzo IPv4 o un indirizzo host.
attivo	Booleano	obbligatorio	
makeDefault	Booleano	obbligatorio	
answerAutomatically	Booleano	obbligatorio	
name	stringa	obbligatorio	
userId	stringa	obbligatorio	
dominio	stringa	Facoltativo	Se questa colonna non è presente nel file CSV, tutti gli utenti saranno impostati come Peer-to-peer. Se questa colonna è presente, l'utente sarà Peer-to-peer se la cella è vuota e Registrato se contiene qualcosa.
Password	stringa	obbligatorio	
authenticationId	stringa	obbligatorio	
callerId	stringa	obbligatorio	
registro	stringa	Facoltativo	
transportMode	udp o tcp	obbligatorio	In MVP1, TLS non è supportato.

Per aggiungere gli utenti ai dispositivi selezionati:

- andare all'area di lavoro **Device Management (Gestione dispositivo)**.
- Selezionare i dispositivi in cui si desidera eseguire la configurazione.
- Fare clic con il pulsante destro del mouse e selezionare **Configure devices > Advanced > SIP configuration > Add SIP accounts** (Configura dispositivi, Avanzate, Configurazione SIP, Aggiungi utenti SIP)
- Fare clic su **Browse (Sfoglia)**.
- Seleziona il file CSV a cui hai aggiunto gli utenti.
- Fare clic su **Next (Avanti)**
- Riesaminare la configurazione dei dispositivi elencati.
- Se tutto è in ordine, fare clic su **Finish (Fine)**.

Rimuovere utenti SIP

Per rimuovere tutti gli utenti SIP tranne quello predefinito sui dispositivi selezionati:

1. andare all'area di lavoro **Device Management (Gestione dispositivo)**.
2. Selezionare i dispositivi in cui si desidera eseguire la configurazione.
3. Fare clic con il pulsante destro del mouse e selezionare **Configure devices > Advanced > SIP configuration > Remove accounts** (Configura dispositivi, Avanzate, Configurazione SIP, Rimuovi utenti)
4. Nell'assistente di configurazione, selezionare **Remove all accounts except the default account on the selected devices (Rimuovere tutti gli utenti tranne quello predefinito sui dispositivi selezionati)**.
5. Fare clic su **Finish** (Fine).

Abilitare i metadati sui dispositivi

In questo caso d'uso abiliteremo i metadati su più dispositivi. Prima di eseguire questa operazione, si consiglia di provarla su un solo dispositivo per evitare problemi con più dispositivi contemporaneamente. Per abilitare i metadati su uno o più dispositivi:

1. andare all'area di lavoro **Device Management (Gestione dispositivo)**.
2. Selezionare i dispositivi su cui si desidera abilitare i metadati.
3. Fare clic con il tasto destro del mouse e selezionare **Configure devices > Advanced > Set configuration** (Configura dispositivi, Avanzate, Imposta configurazione).
4. Fare clic su OK
5. Selezionare **Set NTP servers** (Imposta server NTP) nel menu a discesa.
6. Nel menu a discesa **Uri**, controllare che il metodo sia **Post**.
7. Nel campo dell'indirizzo, aggiungere il seguente indirizzo: **axis-cgi/analyticsmetadataconfig.cgi**
8. Aggiungi il seguente codice in **Content** (Contenuto):

```
{ "apiVersion": "1.0", "context": "my context", "method": "setEnabledProducers", "params": { "producers": [ { "name": "objectanalytics", "videochannels": [ { "channel": 1, "enabled": true } ] } ] } }
```

9. Verificare che **Content-Type** (Tipo di contenuto) sia **application/json**
10. Fare clic su **Send (Invia)**.

Nota

Si noti che AXIS Device Manager non restituirà una risposta quando si utilizza il metodo sopra indicato. Controllare sempre che non vi siano errori nel riquadro **Tasks** (Attività). È inoltre possibile utilizzare un software dedicato come POSTMAN per testare l'API con funzionalità migliorate. Alcuni VMS potrebbero avere limitazioni che consentono un solo produttore alla volta, quindi potrebbe essere necessario disabilitare i produttori aggiuntivi utilizzando l'API sopra menzionata.

Gestione del software del dispositivo

Aggiornamenti AXIS OS

Le nuove versioni del sistema operativo AXIS OS possono essere ottenute in due modi:

- scaricate con AXIS Device Management (Gestione dispositivo AXIS) (è necessario l'accesso a internet)
- Importate da un file (ad esempio da un disco rigido o da una chiavetta di memoria).

Nota

Si consiglia di seguire il percorso di aggiornamento consigliato da AXIS OS. Per saperne di più: *https://help.axis.com/axis-os#upgrade-path*

Aggiornamento manuale del sistema operativo AXIS OS

1. Selezionare i dispositivi che si desidera aggiornare con una nuova versione del sistema operativo AXIS OS, fare clic con il tasto destro del mouse e selezionare **Upgrade firmware** (Aggiorna firmware).
2. Quando si riceve l'informazione che i dispositivi diventeranno inaccessibili durante l'aggiornamento, fare clic su **Yes** (Sì).
3. Per aggiornare l'elenco delle versioni del firmware disponibili per il download Nella finestra di dialogo **Upgrade firmware** (Aggiorna firmware), fare clic su **Check for Updates** (Controlla aggiornamenti).
4. Per accedere a uno o più file della versione del sistema operativo AXIS OS archiviati sul client locale, fare clic sul pulsante **Browse** (Sfoglia).
5. Selezionare i dispositivi e le versioni di AXIS OS che si desidera aggiornare.
6. Per impostare i dispositivi selezionati come predefiniti durante l'aggiornamento del sistema operativo AXIS OS, fare clic su **Factory default checkbox** (Casella di controllo condizioni di fabbrica). Questo è un requisito per il downgrade di alcune versioni del sistema operativo AXIS OS.
7. Fare clic su **OK** per avviare l'aggiornamento dei dispositivi selezionati nell'elenco.

Nota

Per impostazione predefinita, gli aggiornamenti di AXIS OS vengono eseguiti contemporaneamente per tutti i dispositivi selezionati. L'ordine di aggiornamento può essere modificato in **Configuration (Configurazione) > Connected Services (Servizi connessi) > Firmware upgrade settings (Impostazioni aggiornamento firmware)**.

Aggiornamenti automatici

L'impostazione predefinita di AXIS Device Manager 5 è di non controllare la presenza di aggiornamenti firmware, ma è possibile impostarla in modo da controllare automaticamente se gli aggiornamenti del sistema operativo AXIS OS sono disponibili sul server o su axis.com.

Per controllare manualmente gli aggiornamenti del sistema operativo AXIS OS, premere il pulsante **Check now (Controlla ora)** nel menu azione.

Ordine di aggiornamento del sistema operativo AXIS OS

Gli aggiornamenti del sistema operativo AXIS OS possono essere effettuati su tutti i dispositivi contemporaneamente o su un dispositivo dopo l'altro.

- Per aggiornare tutti i dispositivi in una sola volta, selezionare l'ordine di aggiornamento **Parallel (Parallelo)**
- Per aggiornare i dispositivi uno dopo l'altro, selezionare **Sequential (sequenziale)**. Questa opzione impiega più tempo ma evita che i dispositivi siano tutti offline allo stesso tempo. Se si verifica un problema durante l'aggiornamento, è inoltre possibile scegliere di interrompere un aggiornamento se si presenta un problema selezionando la casella **Cancel all remaining upgrades if one device fails (Annulla tutti gli aggiornamenti rimanenti in caso di errore di un dispositivo)** .

Risoluzione dei problemi

Distinta base del software

Per ottenere la distinta base del software (SBOM):

1. Andare *alla pagina di assistenza prodotti per AXIS Device Manager* su axis.com.
2. Fare clic su **Distinta base del software**.

Per ulteriori informazioni sulla SBOM, andare al *Portale AXIS OS* su axis.com.

Contattare l'assistenza

Quando contatti l'assistenza, crea prima un ticket e includi un file di report del sistema per facilitare la risoluzione di problemi specifici:

1. Vai al menu principale.
2. Andare a **Help (Aiuto) > System Report...(report di sistema...)**
3. Salvare il file del rapporto in una cartella selezionata.
4. Andare a *axis.com/support*.
5. Crea un ticket di assistenza.
6. Allegare il file al ticket di assistenza.

Nota

Per creare un rapporto di sistema da un sistema che non risponde:

1. Vai a `C:\ProgramData\Axis Communications\`
2. Archiviare il contenuto della cartella in un file .zip e allegarlo al ticket di assistenza.

Processo di escalation

Se avvengono problemi non risolvibili con questa guida, inoltrare il problema all'helpdesk online Axis, vedere *helpdesk online Axis*. Per permettere al nostro team di assistenza di capire il problema e risolverlo, si devono includere le seguenti informazioni:

- Una descrizione chiara su come riprodurre il problema o delle circostanze nelle quali si verifica.
- L'ora e il nome e l'indirizzo IP del dispositivo interessato dove si verifica il problema.
- AXIS Device Manager report di sistema generato direttamente dopo che si è verificato il problema. Il report di sistema deve essere generato dal client o dal server in cui è stato riprodotto tale problema.
- Schermate o registrazioni opzionali che mostrano il problema.
- Se serve, includere i file del database. Escluderli per velocizzare il caricamento.

Certi problemi richiedono informazioni supplementari che il team di assistenza richiede, se necessario.

Nota

Se il file supera i 100 MB, come ad esempio un'analisi di rete o i file di database, usare un servizio di condivisione file sicuro che si considera attendibile per inviare il file.

Informazioni aggiuntive	
Log livello di debug	A volte usiamo la registrazione al livello di debug per raccogliere altre informazioni. Eseguibile solo dietro richiesta di un tecnico dell'assistenza Axis. Si possono trovare istruzioni *nell'helpdesk online Axis*.
Analisi della rete	Se lo richiede il tecnico dell'assistenza, eseguire la generazione delle tracce di rete quando si crea il report del sistema. Prendere le tracce di rete

Informazioni aggiuntive	
	effettuate nel momento in cui si è verificato il problema se è riproducibile. I materiali comprendono: • Un'analisi di rete di 60 sec effettuata sulla telecamera (applicabile solo al firmware 5.20 e successivo) Usare il seguente comando VAPIX per cambiare login, indirizzo IP e durata (in secondi) se serve: `http://root:pass@192.168.0.90/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=60` • Un'analisi di rete di 10-30 sec effettuata sul server che mostra la comunicazione tra il server e la telecamera.
File del database	Nei casi in cui è necessario esaminare o riparare manualmente il database. Selezionare **Include database in the report (Includi database nel report)** prima di generare il report di sistema.
Schermate	Usa gli screenshot quando il problema riguarda la visualizzazione in diretta ed è relativo all'interfaccia utente. Ad esempio quando si vuole visualizzare una sequenza temporale per le registrazioni o quando il problema è difficile da descrivere.
Screen recordings (Registrazioni schermo)	Usare le registrazioni dello schermo quando è difficile descrivere il problema a parole, ad esempio quando sono interessate molte interazioni della UI per riprodurre il problema.

T10211981_it

2026-04 (M6.2)