

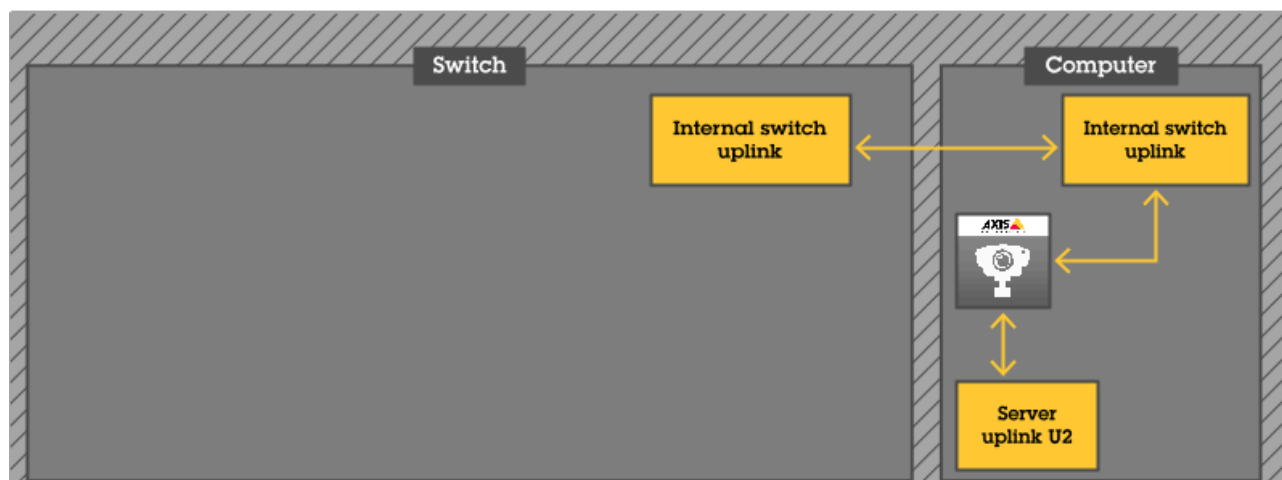
AXIS Camera Station S2108 Appliance

Informazioni sul dispositivo

AXIS Camera Station S2108 Appliance è una soluzione di registrazione completa con switch PoE integrato progettato per offrire una sorveglianza affidabile, con supporto per telecamere fino a risoluzione 4K. Per un'installazione rapida e semplice, i dispositivi sono preconfigurati e precaricati con il Software per la gestione di video AXIS Camera Station Video Management Software, comprese le licenze e tutti i software di sistema necessari. AXIS Camera Station offre un'interfaccia utente intuitiva che consente agli utenti di sfruttare appieno l'ampia gamma di telecamere di videosorveglianza e altri prodotti IP di Axis. Con il sistema operativo archiviato su un'unità SSD (Solid State Drive) e una garanzia hardware di 5 anni, questo apparecchio fornisce una soluzione di sorveglianza affidabile.

AXIS Camera Station S2108 Appliance comprende due componenti:

- **Switch:** switch con Power over Ethernet (PoE) integrato.
- **Computer:** precaricato con tutto il software che serve per la creazione di una soluzione di sorveglianza, compreso il software per la gestione video AXIS Camera Station.

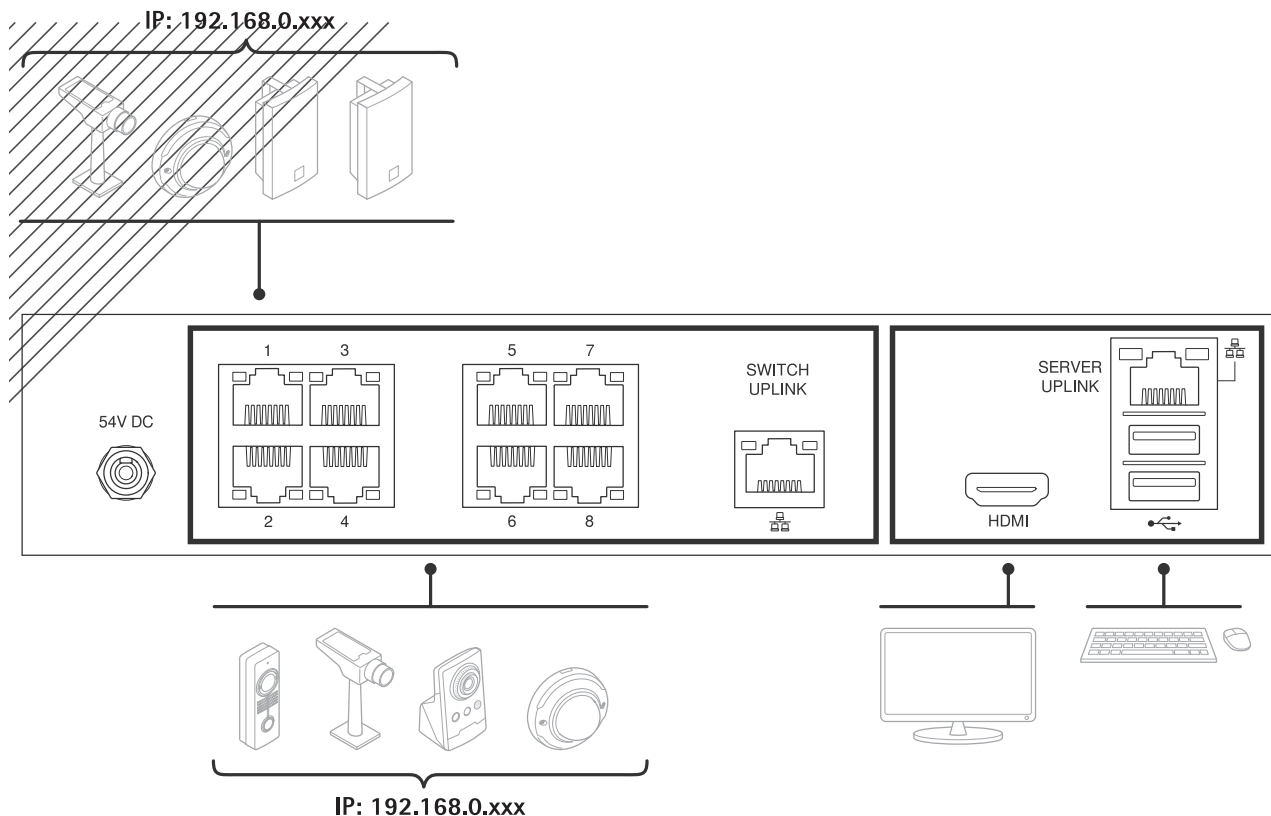


- Lo switch e il computer sono due componenti separati.
- Lo switch e il computer comunicano attraverso i connettori uplink interni: uno si trova sul circuito di alimentazione dello switch e l'altro sulla scheda madre del computer.
- L'uplink server rappresenta un'interfaccia di rete esterna capace di connettersi a una rete esistente.
- Non è possibile far comunicare direttamente i dispositivi connessi all'uplink server con i dispositivi collegati allo switch.
- Tramite AXIS Camera Station è possibile far comunicare i dispositivi connessi all'uplink server con i dispositivi collegati allo switch.

Esempi di setup

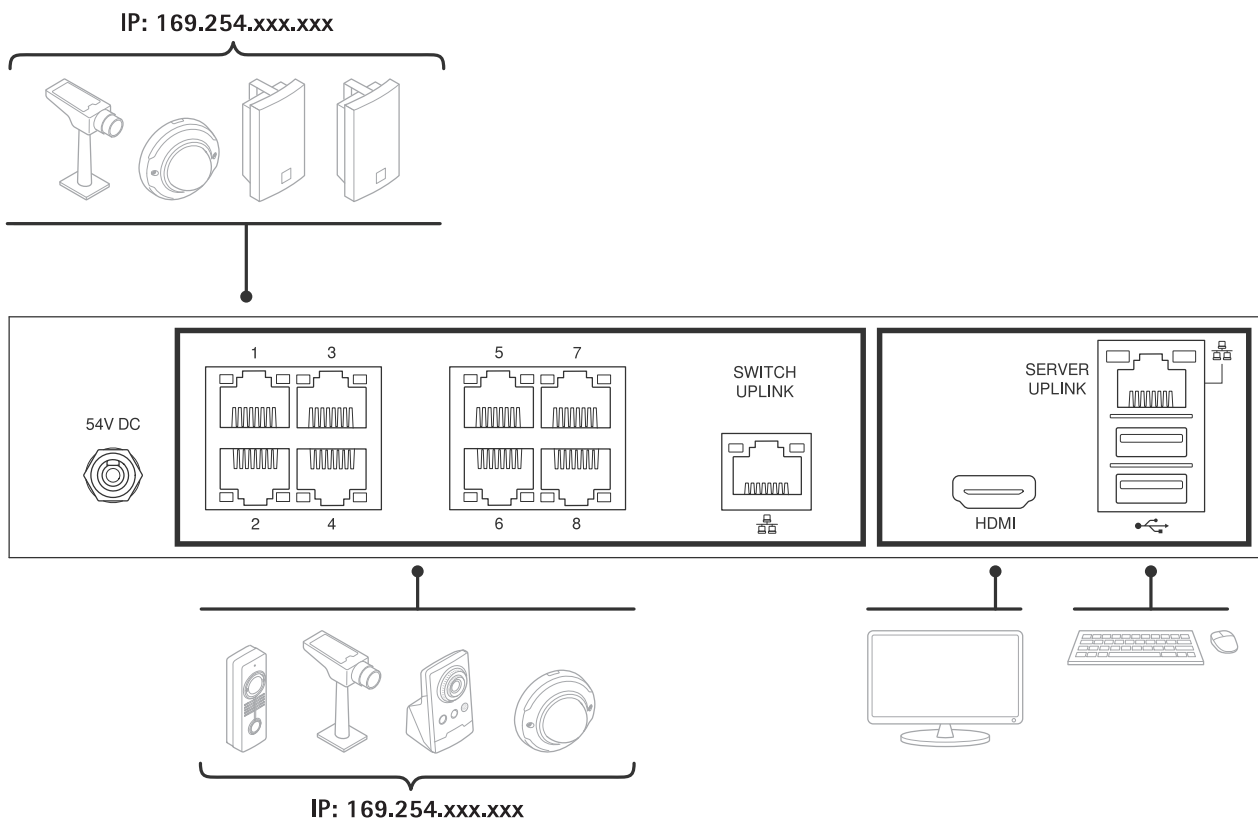
Assegnazione di un indirizzo statico a ciascun dispositivo

Hai la possibilità di creare una rete indipendente con l'assegnazione di un indirizzo IP statico a ciascun dispositivo e ad AXIS S2108 Appliance. Questa rete non avrà interconnettività ad un'altra rete esterna a meno che non ci sia corrispondenza dei parametri tra le reti. Il computer è lo stesso in grado di ottenere la connettività Internet attraverso la porta uplink del server. Non appena i dispositivi saranno connessi alle porte PoE alimentate, dovranno usare l'indirizzo di collegamento locale e necessiteranno di un set di indirizzi IP fissi che corrisponda ad AXIS S2108 Appliance.



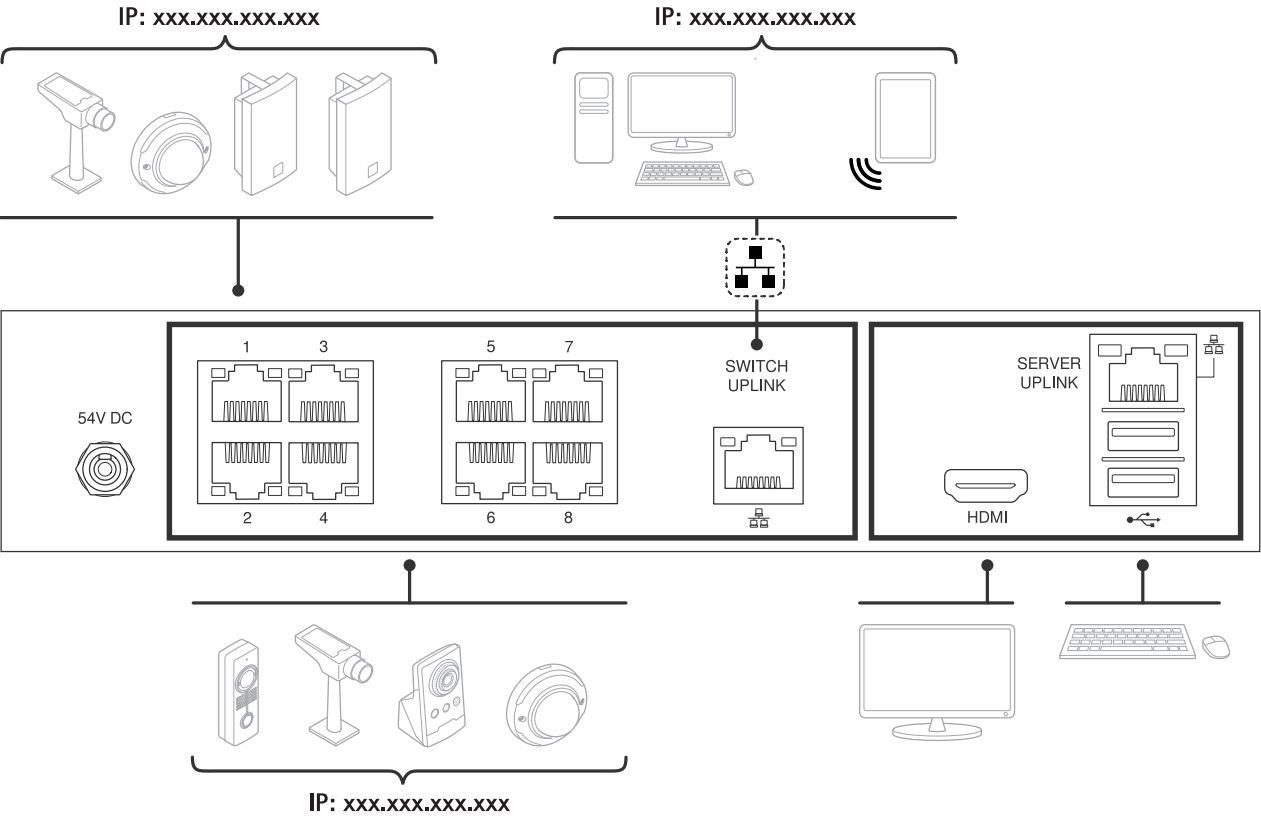
Utilizzo dell'indirizzo locale

Puoi creare una rete indipendente usando l'indirizzo di collegamento locale su ciascun dispositivo e AXIS S2108 Appliance. Questa rete non avrà interconnettività con un'altra rete esterna. Il computer è lo stesso in grado di ottenere la connettività Internet attraverso la porta uplink del server. Appena i dispositivi saranno connessi alle porte PoE alimentate, accetteranno l'indirizzo di collegamento locale e potranno essere trovati da AXIS Camera Station su AXIS S2108 Appliance.



Usare un server DHCP di un'altra rete

Puoi unire AXIS S2108 Appliance e dispositivi connessi avendo una rete esistente e un server DHCP collegati all'uplink switch. Così tutti i dispositivi connessi avranno un indirizzo IP compreso nell'intervallo del server DHCP. Nel caso la connettività Internet sia disponibile su quella rete, lo sarà anche per AXIS S2108 Appliance. In caso contrario, il computer è lo stesso in grado di ottenere la connettività Internet indipendentemente attraverso la porta uplink del server. Quando i dispositivi sono connessi alle porte PoE alimentate, assumono l'indirizzo DHCP se il server DHCP è attivo.



Impostazioni preliminari

Il flusso di lavoro standard per configurare un server del registratore AXIS Camera Station è:

1. *Installare il dispositivo*
2. Configurazione iniziale di Windows®: Dopo aver installato il dispositivo, la configurazione guidata consentirà l'impostazione di regione, lingua, layout della tastiera, account amministratore e relativa password.
3. Configurazione iniziale del registratore Axis: dopo la configurazione iniziale di Windows, AXIS Recorder Toolbox viene aperto e si verrà guidati attraverso alcuni passaggi per impostare le impostazioni di base e necessarie, ad esempio, nome del computer, data, ora e rete. Vedere *Configurazione iniziale del registratore Axis, on page 15*.
4. Configurare Windows®. Si consiglia di:
 - Aggiornare Windows® alla versione più recente. Vedere .
 - Creare un account utente standard. Vedere *Creare un account utente, on page 21*.
5. Aggiornare AXIS Camera Station alla versione più recente.
 - Se il sistema è online: aprire l'applicazione AXIS Recorder Toolbox e fare clic su **Update AXIS Camera Station (Aggiorna AXIS Camera Station)**.
 - Se il sistema è offline: andare in *axis.com* e scaricare l'ultima versione.
6. Avviare il client AXIS Camera Station.
7. *Connessione a un server AXIS Camera Station*
8. *Configurazione di AXIS Camera Station, on page 16*

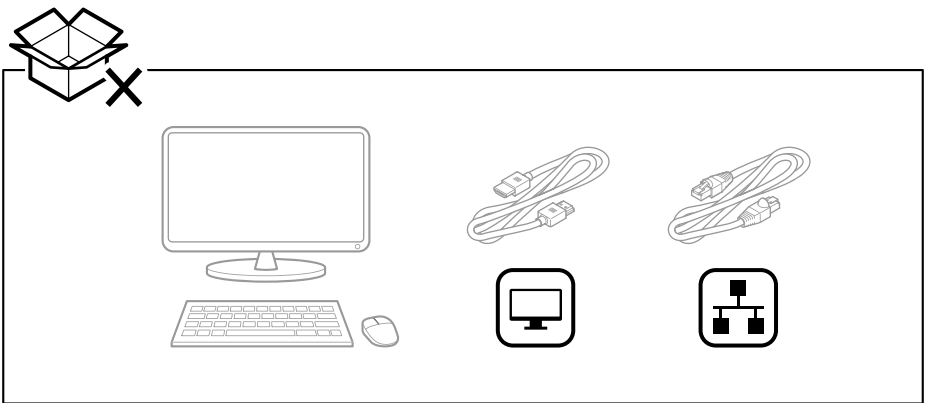
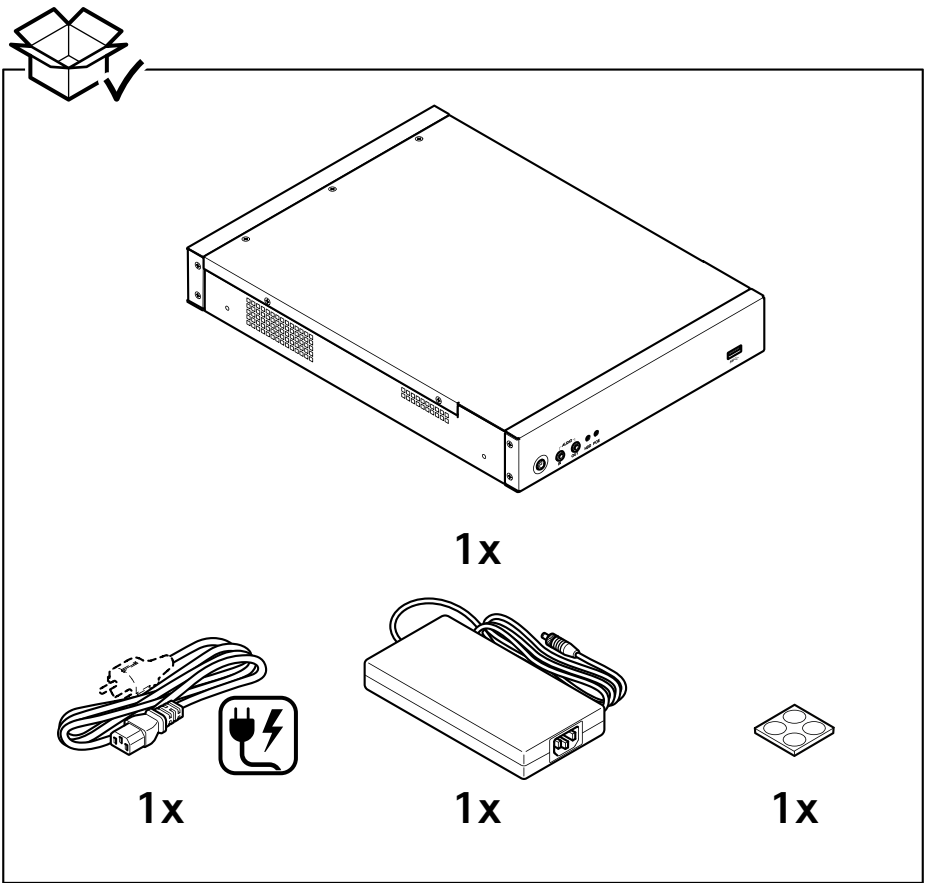
Installare il dispositivo

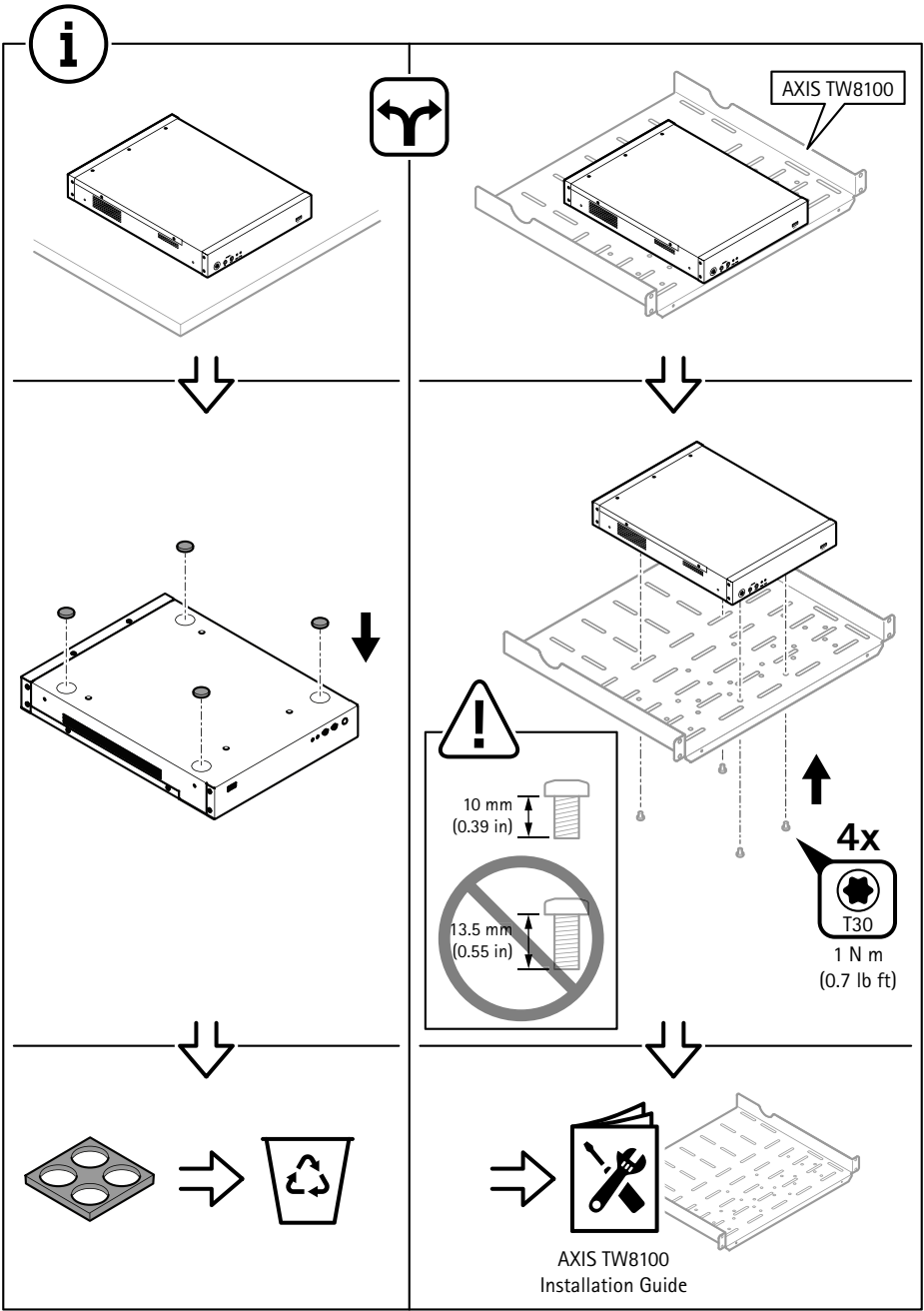
Operazioni preliminari all'installazione

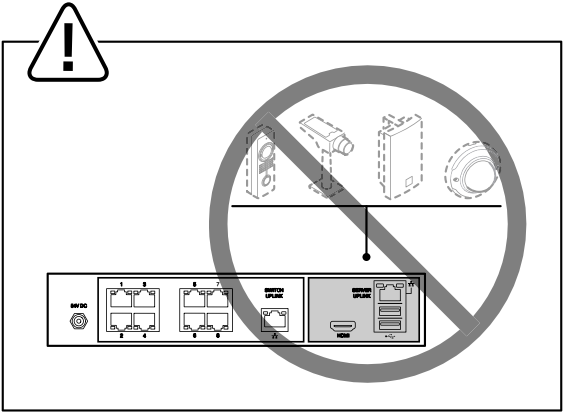
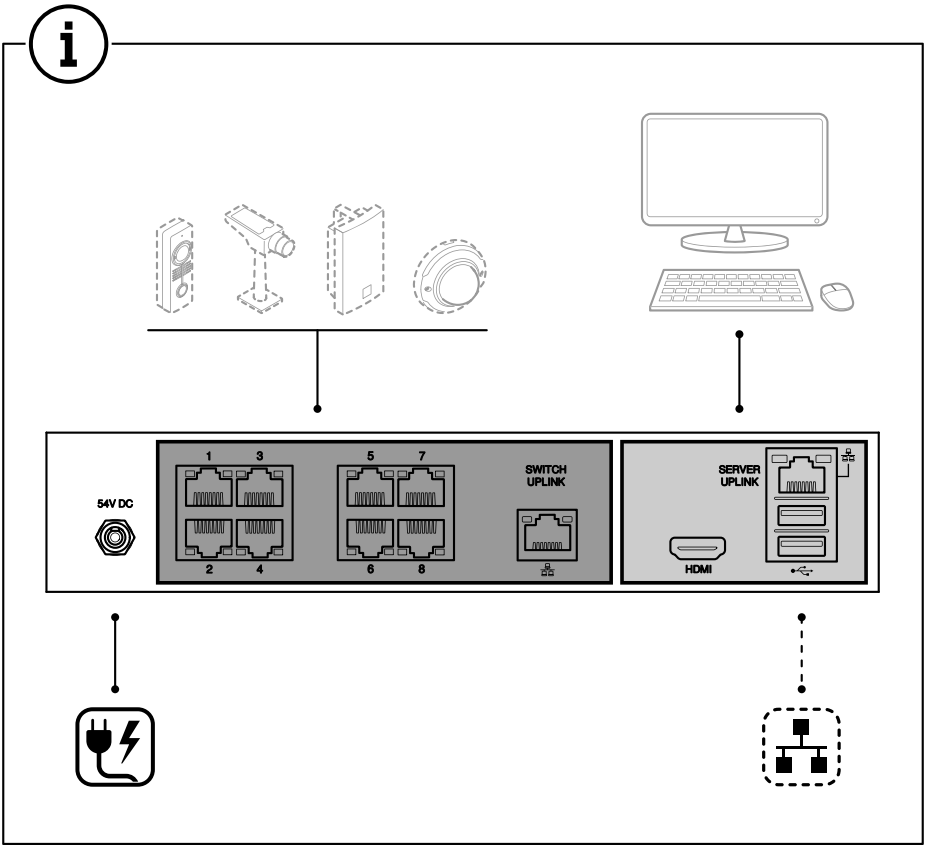
- Preparare gli accessori aggiuntivi utilizzati per l'installazione: monitor, mouse, tastiera e cavo di rete.
- Comprensione dell'uso di account utente diversi.

La tabella seguente elenca gli account utente che possono essere utilizzati per l'installazione, la configurazione e l'utilizzo del sistema Axis.

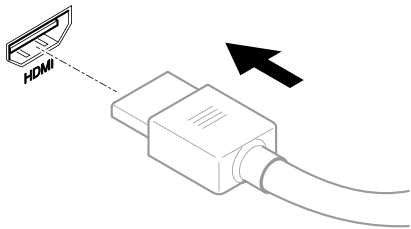
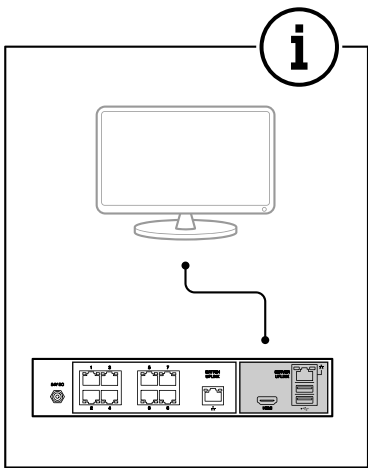
Account utente	Descrizione	Nota
MyAxis	Utilizzato per scaricare il software più recente, accedere al sistema di licenza, ad Axis Secure Remote Access e al monitoraggio dell'integrità del sistema.	Registrato da <i>my.axis.com</i> .
Windows®		
Amministratore Windows®	Privilegi di amministratore Windows®. Si consiglia di non utilizzarlo come amministratore di AXIS Camera Station.	Creato durante l'impostazione iniziale di Windows®.
Utente Windows® con privilegi di amministratore di AXIS Camera Station	Un utente Windows® con privilegi di amministratore in AXIS Camera Station per l'utilizzo da parte di un integratore di sistema o da un amministratore di sistema per la configurazione o la risoluzione dei problemi.	Creato nelle impostazioni di Windows®.
Utente di Windows® con privilegi di operatore o visualizzatore in AXIS Camera Station	Un utente Windows® con privilegi di operatore o visualizzatore in AXIS Camera Station.	Creato nelle impostazioni di Windows®.
Dispositivo		
Amministratore dispositivo	Utilizzato dall'amministratore per accedere alla telecamera dal Video Management System o dalla pagina Web del dispositivo.	Creato dalla pagina Web del dispositivo o quando si aggiunge il dispositivo ad AXIS Camera Station.



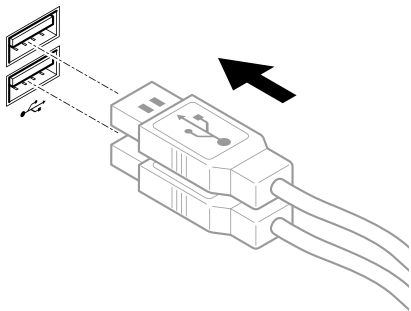
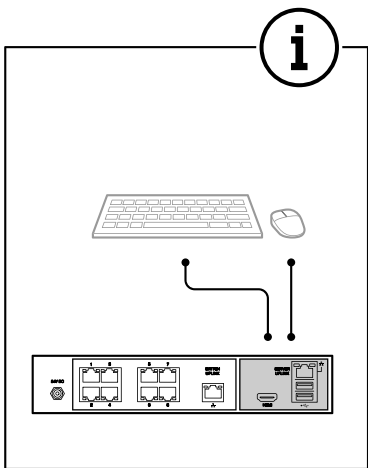




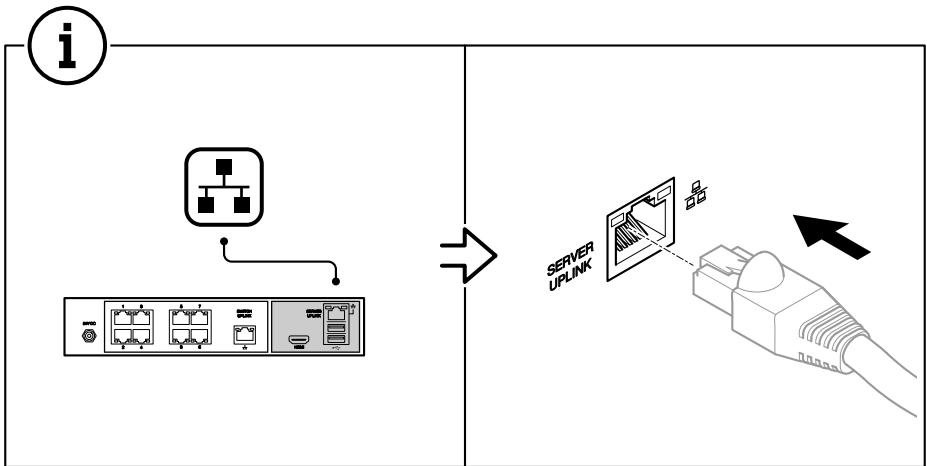
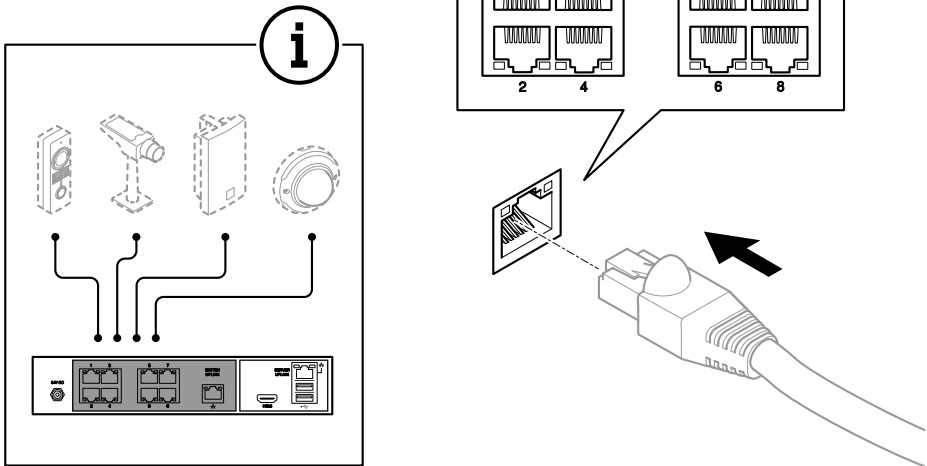
1.1



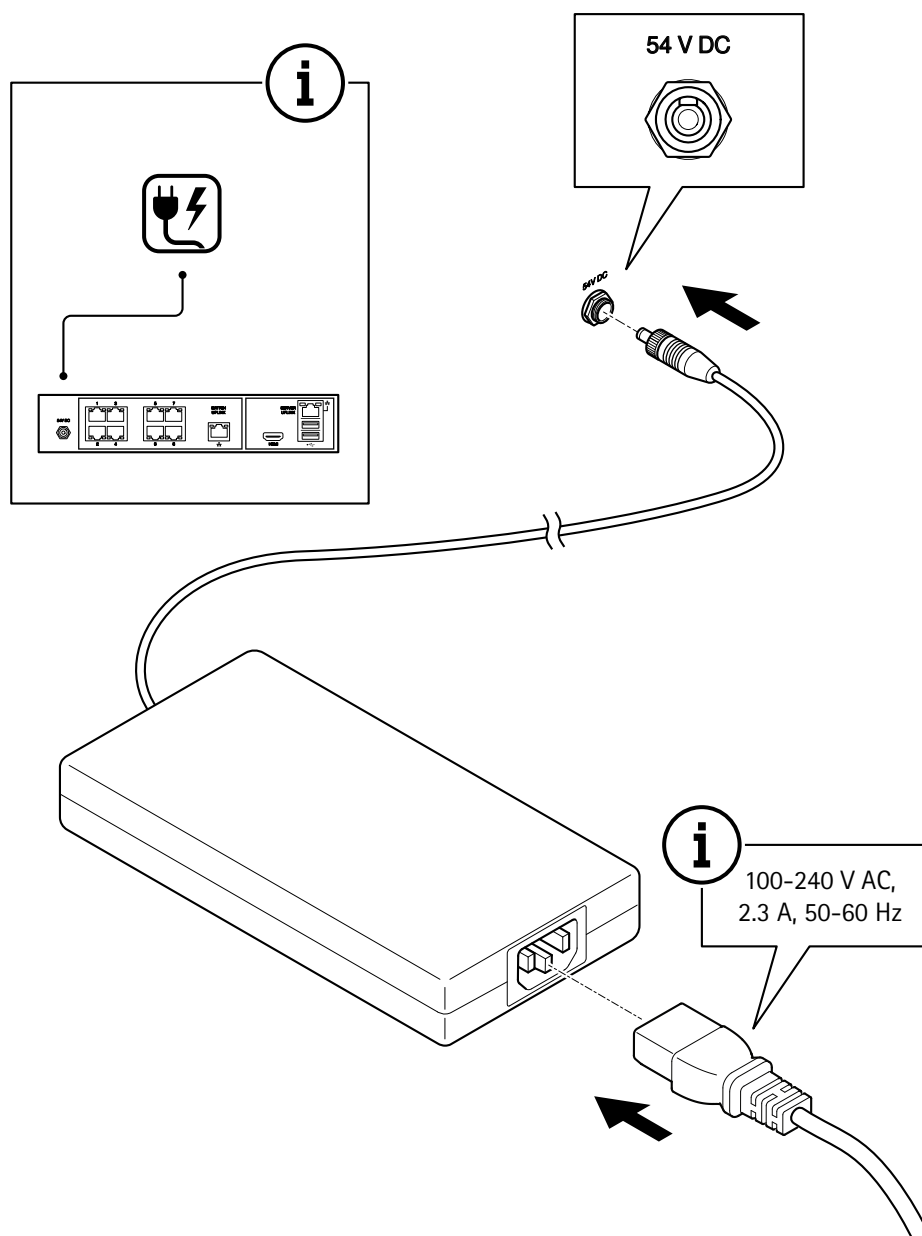
1.2



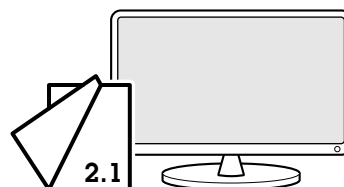
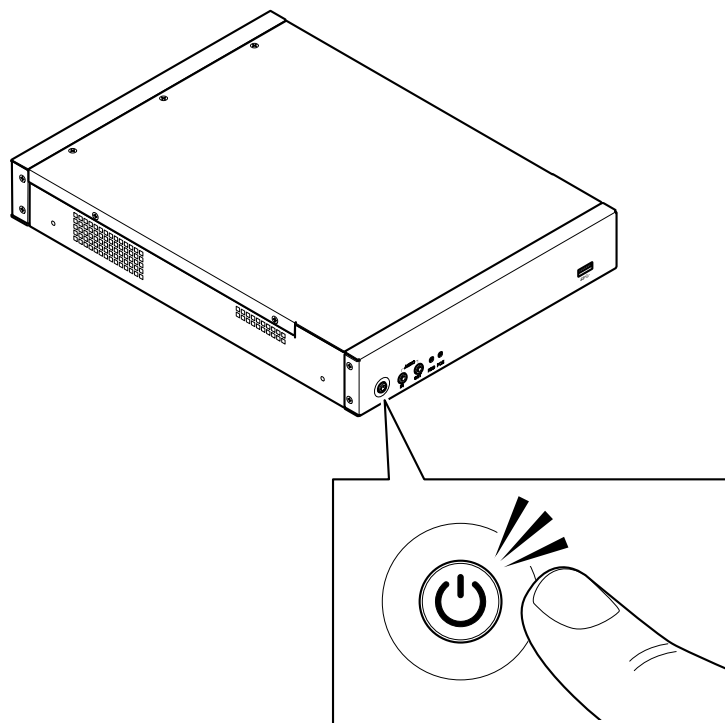
1.3



1.4



1.5



Configurare il dispositivo

Configurazione iniziale del registratore Axis

Dopo aver configurato Windows®, AXIS Recorder Toolbox viene aperto automaticamente e si avvia l'assistente alla configurazione iniziale. Con questo assistente alla configurazione, è possibile configurare diverse impostazioni di base e necessarie prima della gestione del dispositivo in AXIS Recorder Toolbox.

1. Seleziona il tema **Light (Chiaro)** o **Dark (Scuro)** e fai clic su **Next (Avanti)** (se è disponibile per il tuo dispositivo).
2. Se si desidera, cambiare il nome del computer e fare clic su **Next (Avanti)**.
3. In **Date and time (Data e ora)**, configurare le seguenti impostazioni e fare clic su **Next (Avanti)**.
 - Selezionare un fuso orario.
 - Per impostare un server NTP, selezionare **NTP server (Server NTP)** e immettere l'indirizzo del server NTP.
 - Per l'impostazione manuale, selezionare **Manual (Manuale)** e selezionare una data e un'ora.
4. In **Network settings (Impostazioni di rete)**, configurare le seguenti impostazioni e fare clic su **Next (Avanti)**.
 - Le opzioni **Use automatic IP settings (DHCP) (Utilizza impostazioni IP automatiche (DHCP))** e **Use automatic DNS settings (Utilizza le impostazioni DNS automatiche)** sono attivate per impostazione predefinita.
 - Se il dispositivo è connesso a una rete con un server DHCP, vengono visualizzati automaticamente l'indirizzo IP assegnato, la subnet mask, il gateway e il DNS preferito.
 - Se il dispositivo non è connesso a una rete o non è disponibile alcun server DHCP, immettere manualmente l'indirizzo IP, la subnet mask, il gateway e il DNS preferito in base ai requisiti di rete.
5. Fare clic su **Finish (Fine)**. Se è stato modificato il nome del computer, AXIS Recorder Toolbox richiederà di riavviare il dispositivo.

Accesso al server

Tramite il client AXIS Camera Station è possibile connettersi a più server o a un singolo server installati sul computer locale oppure in un'altra posizione nella rete. È possibile collegarsi ai server AXIS Camera Station in modi diversi:

Ultimi server utilizzati – Connettersi ai server utilizzati nella sessione precedente.

Questo computer – Collegarsi al server installato sullo stesso computer del client.

Server remoto – Vedere *Connessione a un server remoto, on page 16*.

AXIS Secure Remote Access – Vedere *Accedi ad AXIS Secure Remote Access, on page 16*.

Nota

Quando si tenta di connettersi a un server per la prima volta, il client controlla l'ID del certificato del server. Per assicurarsi che ci si stia connettendo al server corretto, verificare manualmente l'ID del certificato con quello visualizzato in AXIS Camera Station Service Control.

Elenco dei server	Per connettersi ai server da un elenco di server, selezionarne uno dal menu a discesa Server list (Elenco dei server) . Fare clic su  per creare o modificare gli elenchi di server.
Importa lista dei server	Per importare un file contenente un elenco di server esportati da AXIS Camera Station, fare clic su Import

	server list (Importa lista dei server) e andare a un file .msl.
Elimina password salvate	Per eliminare i nomi utente e le password salvati su tutti i server collegati, fare clic su Delete saved passwords (Elimina password salvate) .
Cambia le impostazioni proxy del client	Potrebbe essere necessario modificare le impostazioni proxy del client per connettersi a un server, fare clic su Change client proxy settings (Cambia le impostazioni proxy del client) .

Connessione a un server remoto

1. Selezionare **Server remoto**.
2. Selezionare un server dall'elenco a discesa **Remote server (Server remoto)** o immettere l'indirizzo IP o DNS. Se il server non è elencato, fare clic su  per aggiornare l'elenco di tutti i server remoti disponibili. Se il server è configurato in modo da accettare i client su una porta diversa dalla porta predefinita 55754, immettere l'indirizzo IP seguito dal numero di porta, ad esempio, 192.168.0.5:46001.
3. effettuare una delle seguenti operazioni:
 - Selezionare **Log in as current user (Accedi come utente corrente)** per accedere come utente corrente di Windows®.
 - Deselezionare l'opzione **Log in as current user (Accedi come utente corrente)** e fare clic su **Log in (Accedi)**. Selezionare **Other user (Altro utente)** e fornire un altro nome utente e password per accedere con credenziali diverse.

Accedi ad AXIS Secure Remote Access

Importante

Per migliorare la sicurezza e la funzionalità, stiamo passando da **Axis Secure Remote Access (v1)** ad **Axis Secure Remote Access v2**. La versione attuale verrà dismessa l'1 dicembre 2025, e si consiglia vivamente di effettuare l'aggiornamento ad **Axis Secure Remote Access v2** prima di tale data.

Cosa significa tutto ciò per il vostro sistema **AXIS Camera Station S2108 Appliance**?

- Dopo l'1 dicembre 2025, non sarà più possibile accedere da remoto al sistema utilizzando **Axis Secure Remote Access (v1)**.
- Per utilizzare **Axis Camera Remote Access v2**, è necessario eseguire l'aggiornamento ad **AXIS Camera Station Pro** versione 6.8. Questo aggiornamento è attualmente gratuito per tutti gli utenti di **AXIS Camera Station 5** fino all'1 marzo 2026.

Nota

- Il server non può aggiornare il client automaticamente durante un tentativo di connessione a un server attraverso **Axis Secure Remote Access**.
 - Se il server proxy si trova tra il dispositivo di rete e il server **AXIS Camera Station S2108 Appliance**, è necessario configurare le impostazioni proxy in Windows sul server **AXIS Camera Station S2108 Appliance** per accedere al server utilizzando **AXIS Secure Remote Access**.
1. Fare clic sul collegamento **Accedi ad AXIS Secure Remote Access**.
 2. Immettere le credenziali dell'account My Axis.
 3. Fai clic su **Accedi**.
 4. Fare clic su **Grant (Concedi)**.

Configurazione di AXIS Camera Station

In questo tutorial spiegheremo i passaggi di base per rendere operativo il sistema.

Operazioni preliminari:

- Configurare la rete a seconda dell'installazione. Vedere *Configurazione di rete*, on page 18.
- Se necessario, configurare le porte del server. Vedere *Configurazione della porta del server*, on page 19.
- Valutare eventuali problemi di sicurezza. Vedere *Considerazioni sulla protezione*.

Dopo aver effettuato le necessarie configurazioni, è possibile iniziare a lavorare con AXIS Camera Station:

1. *Avviare il video management system*, on page 17
2. *Aggiunta di dispositivi*, on page 17
3. *Configura metodo di registrazione*, on page 17
4. *Visualizzazione del video in diretta*, on page 17
5. *Visualizzazioni registrate*, on page 17
6. *Aggiunta di segnalibri*, on page 18
7. *Esportazione delle registrazioni*, on page 18
8. *Riproduzione e verifica delle registrazioni in AXIS File Player.*, on page 18

Avviare il video management system

Fare doppio clic sull'icona del client AXIS Camera Station per avviare il client. Quando si avvia il client per la prima volta, tenta di accedere al server AXIS Camera Station installato nello stesso computer del client.

Non è possibile collegarsi a più server AXIS Camera Station in modi diversi:

Aggiunta di dispositivi

Al primo avvio di AXIS Camera Station si apre la pagina Add devices (Aggiungi dispositivi). AXIS Camera Station cerca i dispositivi connessi nella rete e mostra l'elenco dei dispositivi trovati.

1. Selezionare le telecamere che si desidera aggiungere dall'elenco. Se non è possibile trovare la telecamera, fare clic su **Manual search (Ricerca manuale)**.
2. Fare clic su **Aggiungi**.
3. Selezionare **Configurazione rapida** o **Configurazione di Site Designer**. Fare clic su **Next (Avanti)**.
4. Utilizzare le impostazioni predefinite e verificare che il metodo di registrazione sia impostato su **None (Nessuno)**. fare clic su **Install (Installa)**.

Configura metodo di registrazione

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Metodo di registrazione**.
2. Selezionare una telecamera
3. Attivare l'opzione **Motion detection (Rilevamento movimento)** o **Continuous (Continua)** o entrambe.
4. fare clic su **Applica**;

Visualizzazione del video in diretta

1. Aprire una scheda **Live view (Visualizzazione in diretta)**.
2. Selezionare una telecamera per visualizzarne il video in diretta.

Visualizzazioni registrate

1. Aprire una scheda **Recordings (Registrazioni)**.
2. Selezionare la telecamera da cui visualizzare le registrazioni.

Aggiunta di segnalibri

1. Andare alla registrazione.
2. Nella sequenza temporale, ingrandire e ridurre e spostare la sequenza temporale per posizionare l'indicatore nella posizione desiderata.
3. Fare clic su .
4. Immettere un nome e una descrizione per il segnalibro. Utilizzare le parole chiave per facilitare la ricerca del segnalibro.
5. Selezionare **Impedisci eliminazione registrazione** per proteggere la registrazione.

Nota

Per rimuovere la protezione della registrazione, deselezionare **Prevent recording deletion (Impedisci eliminazione registrazione)** o eliminare il segnalibro.

6. Fare clic su **OK** per salvare il segnalibro.

Esportazione delle registrazioni

1. Aprire una scheda **Recordings (Registrazioni)**.
2. Selezionare la telecamera da cui esportare le registrazioni.
3. Fare clic su  per visualizzare i marcatori di selezione.
4. Trascinare gli indicatori per includere le registrazioni che si desidera esportare.
5. Fare clic su  per aprire la scheda **Export (Esporta)**.
6. Fare clic su **Export... (Esporta)**

Riproduzione e verifica delle registrazioni in AXIS File Player.

1. Andare alla cartella con le registrazioni esportate.
2. Fare doppio clic su **AXIS File Player**.
3. Fare clic su  per visualizzare le note della registrazione.
4. Per verificare la firma digitale:
 - 4.1. Andare a **Tools > Verify digital signature (Strumenti > Verifica firma digitale)**.
 - 4.2. Selezionare **Validate with password (Convalida con password)** e immettere la password.
 - 4.3. Fare clic su **Verify (Verifica)** per visualizzare i risultati della verifica.

Nota

- Una firma digitale differisce da video firmato. Un video firmato consente di risalire alla telecamera da cui proviene la registrazione, in modo da poter verificare che non sia stata oggetto di manomissione. Vedi *Video firmato* e il manuale per l'utente della telecamera per maggiori informazioni.
- Se i file memorizzati non sono collegati a un database di AXIS Camera Station (file non indicizzati), è necessario convertirli per renderli riproducibili in AXIS File Player. Contattare l'assistenza tecnica Axis per ricevere supporto riguardo la conversione dei file.

Configurazione di rete

Configurare le impostazioni proxy o firewall prima di utilizzare AXIS Camera Station se il client AXIS Camera Station, il server AXIS Camera Station e i dispositivi di rete collegati sono su reti diverse.

Impostazioni proxy client

Quando un server proxy separa il client e il server, configurare le impostazioni proxy del client.

1. Aprire il client AXIS Camera Station.
2. Fare clic su **Change client proxy settings (Cambia le impostazioni proxy del client)**.
3. Cambia le impostazioni proxy del client.
4. Fare clic su **OK**.

Impostazioni proxy del server

Quando un server proxy separa i dispositivi di rete e il server, configurare le impostazioni proxy del server.

1. Apri Controllo del servizio AXIS Camera Station.
2. Selezionare **Modify settings (Modifica impostazioni)**.
3. Nella sezione Impostazioni proxy, utilizzare l'**System account internet option (Opzione Internet account di sistema)** predefinita oppure selezionare **Use manual proxy settings (Utilizza impostazioni proxy manuali)**.
4. Fare clic su **Save (Salva)**.

NAT and Firewall (NAT e Firewall)

Quando un NAT, un firewall o un dispositivo simile separa il client e il server, configurare il NAT o il firewall per garantire che la porta HTTP, TCP e di streaming specificata in AXIS Camera Station Service Control possa passare attraverso il firewall o NAT. Contattare l'amministratore di rete per istruzioni su come configurare il NAT o il firewall.

Configurazione della porta del server

Il server AXIS Camera Station usa le porte 55752 (HTTP), 55754 (TCP), 55756 (comunicazione mobile) e 55757 (mobile streaming) per la comunicazione tra il server e client. Se necessario, le porte possono essere cambiate in AXIS Camera Station Service Control.

Considerazioni sulla protezione

Per impedire l'accesso non autorizzato alle telecamere e alle registrazioni:

- Usare password complesse per tutti i dispositivi di rete (telecamere, video encoder e dispositivi ausiliari).
- Installare il server, le telecamere, i video encoder e i dispositivi ausiliari di AXIS Camera Station S2108 Appliance su una rete protetta separata da una rete d'ufficio. È possibile installare il client AXIS Camera Station S2108 Appliance su un computer in un'altra rete, ad esempio una rete con accesso a Internet.
- Assicurarsi che tutti gli utenti dispongano di password complesse.

Ottenimento di una licenza per un sistema online

Sia il server che il client AXIS Camera Station devono avere la connessione a Internet.

1. andare a **Configuration (Configurazione) > Licenze > Management (Gestione)**.
2. Assicurarsi che **Manage licenses online (Gestisci licenze online)** sia attivo.
3. Accedi con l'account MyAxis.
4. La chiave di licenza è generata in automatico e appare in **License keys (Chiavi di licenza)**.
5. Se sono state acquistate chiavi di licenza separatamente, immettere la chiave di licenza in **Add license key (Aggiungi chiave di licenza)**.
6. Fare clic su **Aggiungi**.
7. Nel client AXIS Camera Station assicurarsi che le chiavi di licenza appaiano in **Configuration > Licenses > Keys (Configurazione > Licenze > Chiavi)**.

Ottenimento di una licenza per un sistema offline

1. andare a **Configuration (Configurazione) > Licenze > Management (Gestione)**.
2. Disattivare **Manage licenses online (Gestisci licenze online)**.
3. Fare clic su **Esporta file di sistema**.
4. Salvare il file di sistema su un'unità flash USB.
5. Accedi con l'account MyAxis.
6. Fare clic su **Upload system file (Carica file di sistema)** per il caricamento del file di sistema dall'unità flash USB.
7. La chiave di licenza è generata in automatico e mostrata in **License keys (Chiavi di licenza)**.
8. Se sono state acquistate chiavi di licenza separatamente, immettere la chiave di licenza in **Add license key (Aggiungi chiave di licenza)**.
9. Fare clic su **Aggiungi**.
10. In **License keys (Chiavi di licenza)**, fare clic su **Download license file (Scarica file di licenza)** e salvare il file nell'unità flash USB.
11. Nel client AXIS Camera Station Client, andare a **Configuration > Licenses > Management (Configurazione > Licenze > Gestione)**.
12. Fare clic su **Import license file (Importa file di licenza)** e selezionare il file di licenza nell'unità flash USB.
13. Assicurarsi che le chiavi di licenza appaiano in **Configuration > Licenses > Keys (Configurazione > Licenze > Chiavi)**.

Gestire gli account utente di Windows® locali

Creare un account utente

Per incrementare la sicurezza dei dati personali e delle informazioni, consigliamo di aggiungere una password per ogni account locale.

Importante

Una volta creata una password per un account locale, non dimenticarla. Se si perde la password per un account locale, è impossibile recuperarla.

1. Andare a **Settings > Accounts > Other people > Add someone else to this PC** (Impostazioni > Account > Altre persone > Aggiungi qualcun altro a questo PC).
2. Fare clic su **I don't have this person's sign-in information** (Non ho le informazioni di accesso di questa persona).
3. Fare clic su **Add a user without a Microsoft account** (Aggiungi un utente senza un account Microsoft).
4. Immettere un nome utente, una password e un suggerimento per la password.
5. Fare clic su **Next (Avanti)** e seguire le istruzioni.

Crea un account amministratore

1. Andare a **Settings > Accounts > Other people** (Impostazioni > Account > Altre persone).
2. Accedere all'account che si desidera modificare e fare clic su **Change account type** (Cambia tipo di account).
3. Andare a **Account type** (Tipo di account) e selezionare **Administrator** (Amministratore).
4. Fare clic su **OK**.
5. Riavviare il dispositivo e accedere con il nuovo account amministratore.

Creare un gruppo di utenti locale

1. Andare a **Computer Management** (Gestione del computer).
2. Andare a **Local Users and Groups > Group** (Utenti e gruppi locali > Gruppo).
3. Fare clic con il pulsante destro del mouse su **Group** (Gruppo) e selezionare **New Group** (Nuovo gruppo).
4. Immettere un nome per il gruppo e una descrizione.
5. Aggiungere membri al gruppo:
 - 5.1. Fare clic su **Aggiungi**.
 - 5.2. fare clic su **Avanzate**;
 - 5.3. Individuare gli account utente che si desidera aggiungere al gruppo e fare clic su **OK**.
 - 5.4. Fare di nuovo clic su **OK**.
6. Fare clic su **Create** (Crea).

Eliminare un account utente

Importante

Quando si elimina un account, si rimuove l'account utente dalla schermata di accesso. Inoltre saranno rimossi tutti i file, le impostazioni e i dati dei programmi memorizzati nell'account utente.

1. Andare a **Settings > Accounts > Other people** (Impostazioni > Account > Altre persone).
2. Accedere all'account che si desidera rimuovere e fare clic su **Remove** (Rimuovi).

Modificare la password di un account utente

1. Accedere con un account amministratore.
2. Andare a **User Accounts > User Accounts > Manage another account in sequence** (Account utente > Account utente > Gestire un altro account in sequenza).
Verrà visualizzato un elenco di tutti gli account utente nel dispositivo.
3. Selezionare l'account utente di cui si desidera modificare la password.
4. Fare clic su **Change the password** (Modifica la password).
5. Immettere la nuova password e fare clic su **Change password** (Cambia password).

Creare un disco di reimpostazione della password per un account utente.

Si consiglia di creare un disco di reimpostazione della password su un'unità flash USB. Così si può reimpostare la password. Senza un disco di reimpostazione password, non è possibile reimpostare la password.

Nota

Se si utilizza Windows® 10 o versione successiva, è possibile aggiungere domande di sicurezza all'account locale nel caso in cui la password venga dimenticata, in modo da non dover creare un disco di reimpostazione della password. Per fare questo, andare su **Start** e fare clic su **Settings > Sign-in options > Update your security questions** (Impostazioni > Opzioni di accesso > Aggiorna le domande di sicurezza).

1. Accedere al dispositivo con un account utente locale. Non è possibile creare un disco di reimpostazione della password per un account connesso.
2. Collegare un'unità flash USB vuota al dispositivo.
3. Dal campo di ricerca di Windows®, andare su **Create a password reset disk** (Creare un disco di reimpostazione della password).
4. Nell'assistente di configurazione **Forgotten Password** (Password dimenticata), fare clic su **Next** (Avanti).
5. Selezionare l'unità flash USB e fare clic su **Next** (Avanti).
6. Digitare la password attuale e fare clic su **Next** (Avanti).
7. Seguire le istruzioni visualizzate.
8. Rimuovere l'unità flash USB e conservarla in un luogo sicuro. Non è necessario creare un nuovo disco quando si modifica la password, anche se la si modifica più volte.

Gestire gli account utente di AXIS Camera Station

Autorizzazioni utente

Andare a **Configuration > Security > User permissions (Configurazione, Sicurezza, Autorizzazioni utente)** per visualizzare gli utenti e i gruppi che esistono in AXIS Camera Station S2108 Appliance.

Nota

Agli amministratori del computer su cui viene eseguito il server AXIS Camera Station S2108 Appliance vengono garantiti determinati privilegi di amministratore in AXIS Camera Station S2108 Appliance. Non è possibile cambiare o rimuovere i privilegi del gruppo degli Amministratori.

Prima di poter aggiungere un utente o un gruppo, controllare che siano registrati sul computer locale o che dispongano di un account di Windows® Active Directory. Per aggiungere utenti o gruppi, vedere *Aggiunta di utenti o gruppi*.

Quando un utente appartiene a un gruppo, gli vengono assegnate le autorizzazioni relative al ruolo più elevato tra quelle assegnate a lui individualmente e quelle assegnate al gruppo. Ad esempio, un utente che ha accesso alla telecamera X e che appartiene anche a un gruppo con accesso alle telecamere Y e Z può accedere a tutte e tre le telecamere.

	Indica se la voce si riferisce a un utente singolo.
	Indica che la voce rappresenta un gruppo.
Nome	Il nome utente visualizzato nel computer locale o in Active Directory.
Dominio	Il dominio di cui fa parte l'utente o il gruppo.
Ruolo	Il ruolo di accesso assegnato all'utente o al gruppo. I possibili valori sono: Amministratore, Operatore e Visualizzatore.
Dettagli	Informazioni dettagliate sull'utente come visualizzate su un computer locale o in Active Directory.
Server	Il server di cui fa parte l'utente o il gruppo.

Aggiunta di utenti o gruppi

Microsoft Windows® e i gruppi e gli utenti di Active Directory possono accedere a AXIS Camera Station S2108 Appliance. Per aggiungere un utente a AXIS Camera Station S2108 Appliance, è necessario aggiungere utenti o un gruppo a Windows®.

Per aggiungere un utente in Windows® 10 e 11:

- Premere il tasto Windows + X e selezionare **Computer Management (Gestione computer)**.
- Nella finestra **Computer Management (Gestione computer)**, spostarsi su **Local Users and Groups (Utenti e gruppi locali) > Users (Utenti)**.
- Fare clic con il tasto destro del mouse su **Users (Utenti)** e selezionare **New user (Nuovo utente)**.
- Nella finestra di dialogo a scomparsa, inserire i dettagli del nuovo utente e annullare **User must change password at next login** (L'utente deve modificare la password all'accesso successivo).
- Fare clic su **Create (Crea)**.

Se si usa un dominio di Active Directory, consultare l'amministratore di rete.

Aggiunta di utenti o gruppi

1. Andare in **Configuration (Configurazione) > Security (Sicurezza) > User permissions (Autorizzazioni utente)**.
2. Fare clic su **Aggiungi**. Gli utenti e i gruppi disponibili appaiono nell'elenco.

3. In **Scope (Ambito)**, scegliere dove si devono cercare utenti e gruppi.
4. In **Show (Mostra)**, selezionare per mostrare utenti o gruppi. I risultati della ricerca potrebbero non essere visualizzati qualora il numero di utenti o gruppi fosse eccessivo. Utilizzare il filtro per restringere i risultati.
5. Selezionare gli utenti o i gruppi e fare clic su **Aggiungi**.

Ambito	
Server	Selezionare per cercare utenti o gruppi sul computer locale.
Dominio	Selezionare per eseguire la ricerca di utenti o gruppi Active Directory.
Server selezionato	Se si è connessi a più server di AXIS Camera Station S2108 Appliance, selezionare un server per cercare utenti o gruppi su quel server.

Configurare un utente od un gruppo

1. Selezionare un utente o un gruppo nell'elenco.
2. In **Role (Ruolo)**, selezionare **Administrator (Amministratore)**, **Operator (Operatore)** o **Viewer (Visualizzatore)**.
3. Se si è selezionato **Operator (Operatore)** o **Viewer (Visualizzatore)**, è possibile configurare i privilegi utente o gruppo. Vedere *Privilegi utente o di gruppo*.
4. Fare clic su **Save (Salva)**.

Rimuovere un utente od un gruppo

1. Selezionare utente o gruppo.
2. Fare clic su **Remove (Rimuovi)**.
3. Nella finestra a comparsa, fare clic su **OK** per rimuovere l'utente o il gruppo.

Privilegi utente o di gruppo

Sono disponibili tre ruoli che si possono assegnare a un utente o a un gruppo. Per le modalità di definizione del ruolo per un utente o un gruppo, vedere *Aggiunta di utenti o gruppi*.

Amministratore – accesso completo all'intero sistema, incluso l'accesso ai video in diretta e registrati di tutte le telecamere, tutte le porte I/O e le viste. Questo ruolo è necessario per ottenere l'accesso alla configurazione di sistema.

Operatore – Selezionare telecamere, viste e porte I/O per ottenere l'accesso ai video dal vivo e registrati. Un operatore ha pieno accesso a tutte le funzionalità di AXIS Camera Station S2108 Appliance ad eccezione della configurazione del sistema.

Utente – Accesso a video dal vivo di telecamere, porte I/O e viste selezionate. Un visualizzatore non ha accesso ai video registrati o alla configurazione di sistema.

Telecamere

Per utenti o gruppi con ruolo **Operator (Operatore)** o **Viewer (Visualizzatore)** sono disponibili i seguenti privilegi di accesso.

Accesso	consente l'accesso alla telecamera e a tutte le relative funzioni.
Video	consente l'accesso al video dal vivo dalla telecamera.

Ascolta con audio	consente l'accesso per ascoltare l'audio dalla telecamera.
Parla con audio	consente l'accesso per parlare alla telecamera.
Registrazione manuale	Consentire l'avvio e l'interruzione delle registrazioni in modo manuale.
PTZ meccanico	consente accesso ai comandi PTZ meccanici. Disponibile solo per telecamere dotate di PTZ meccanico.
Priorità PTZ	imposta la priorità PTZ. Un numero inferiore indica una priorità più alta. Nessuna priorità assegnata è impostata su 0. Un amministratore ha la priorità più alta. Quando un ruolo con una priorità più elevata opera una telecamera PTZ, gli altri non possono utilizzare la stessa telecamera per 10 secondi per impostazione predefinita. Disponibile solo per telecamere con PTZ meccanico con Mechanical PTZ (PTZ meccanico) selezionato.

Viste

Per utenti o gruppi con ruolo **Operator (Operatore)** o **Viewer (Visualizzatore)** sono disponibili i seguenti privilegi di accesso. È possibile selezionare più viste e impostare i privilegi di accesso.

Accesso	Consentire l'accesso alle viste in AXIS Camera Station S2108 Appliance.
Modifica	Consente la modifica delle viste in AXIS Camera Station S2108 Appliance.

I/O

Per utenti o gruppi con ruolo **Operator (Operatore)** o **Viewer (Visualizzatore)** sono disponibili i seguenti privilegi di accesso.

Accesso	consente l'accesso completo alla porta I/O.
Leggi I'	Consente di visualizzare lo stato della porta I/O senza effettuare alcuna modifica.
Scrittura	Consente di effettuare una modifica dello stato della porta I/O.

Sistema

Non si può eseguire la configurazione dei privilegi di accesso riportati in grigio nella lista. Un segno di spunta indica che l'utente o il gruppo ha questo privilegio per impostazione predefinita.

Per utenti o gruppi con ruolo **Operator (Operatore)** sono disponibili i seguenti privilegi di accesso. **Take snapshots (Acquisisci istantanee)** è anche disponibile per il ruolo **Viewer (Visualizzatore)**.

Acquisisci istantanee	Consente di scattare istantanee in modalità di visualizzazione in diretta e in modalità di registrazione.
Esportazione delle registrazioni	consente di esportare le registrazioni.
Genera report dell'incidente	consente di generare i report dell'incidente.

Prevent access to recordings older than (Impedisci accesso a registrazioni precedenti a)	impedisce di accedere alle registrazioni precedenti al numero di minuti specificato. Gli utenti non possono trovare queste registrazioni quando effettuano una ricerca.
Accedi ad allarmi, attività e registri	Ricevere notifiche di allarme e permettere l'accesso alla barra Alarms and tasks (Allarmi e attività) e alla scheda Logs (Registri).
Access data search (Ricerca dati di accesso)	Consente di cercare i dati per tenere traccia di quanto è successo al momento di un evento.
Aggiungere categorie agli eventi	Consente l'aggiunta di categorie agli eventi nella scheda Recordings (Registrazioni).
Rimuovere le categorie dall'evento	Consente la rimozione di categorie dagli eventi nella scheda Recordings (Registrazioni).

Controllo accessi

Per utenti o gruppi con ruolo **Operator (Operatore)** sono disponibili i seguenti privilegi di accesso. **Access Management** (Gestione degli accessi) è a disposizione anche per il ruolo **Viewer (Visualizzatore)**.

Configurazione controllo degli accessi	Permette di configurare porte e zone, profili di identificazione, formati tessera e PIN, comunicazione criptata e multiserver.
Gestione degli accessi	Permette la gestione degli accessi e l'accesso alle impostazioni di Active Directory.

Per utenti o gruppi con ruolo **Viewer (Visualizzatore)** sono disponibili i seguenti privilegi di accesso.

Monitoraggio dell'integrità del sistema

Per utenti o gruppi con ruolo **Operator (Operatore)** sono disponibili i seguenti privilegi di accesso. **Access to system health monitoring** (Accesso a monitoraggio dell'integrità del sistema) è a disposizione anche per il ruolo **Viewer (Visualizzatore)**.

Configurazione di Monitoraggio dell'integrità del sistema	Consente la configurazione di monitoraggio dell'integrità del sistema.
Accesso a monitoraggio dell'integrità del sistema	Consente l'accesso al monitoraggio dell'integrità del sistema.

Gestire il dispositivo

Aggiornare i certificati Secure Boot

Microsoft ritirerà i certificati Secure Boot del 2011 nel giugno 2026 e li sostituirà con i nuovi certificati del 2023. Per preservare la sicurezza dell'unità di registrazione, installare i certificati del 2023 prima di tale data.

L'installazione dei certificati del 2023 richiede Windows 10 LTSC (Long-Term Servicing Channel) o Windows 11 LTSC. Se il dispositivo è ancora in garanzia ma utilizza Windows 10 SAC (Semi-Annual Channel) anziché una versione LTSC, rivolgersi all'assistenza tecnica di Axis. L'assistenza potrà indicare se è possibile effettuare l'aggiornamento a una versione LTSC prima di aggiornare il BIOS o effettuare qualsiasi modifica ai certificati.

Nota

Dopo giugno 2026, i dispositivi sprovvisti dei certificati del 2023 continueranno a funzionare normalmente, ma non riceveranno nuove protezioni di sicurezza per la fase iniziale di avvio, compresi gli aggiornamenti di Windows Boot Manager e gli elenchi di revoca relativi alle nuove vulnerabilità.

Controllare lo stato del certificato

Per verificare che i certificati del 2023 sono stati installati e che il bootloader di Windows è stato aggiornato, utilizzare uno dei seguenti metodi:

Metodo 1:

1. Aprire **Registry Editor (Editor di registro)**.
2. Andare a `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing`.
3. Controllare il valore **UEFICA2023Status**. Se il valore indica **Updated (Aggiornato)**, il certificato del 2023 è installato.

 (Default)	REG_SZ	(value not set)
 BucketHash	REG_SZ	5a3041a8e6c7476f988f369de06e65e224df7d53cf7f9...
 ConfidenceLevel	REG_SZ	No Data Observed - Action Required
 ConfidenceUpdateType	REG_DWORD	0x00000000 (0)
 LastParsedBucketDataVersion	REG_DWORD	0x0000000c (12)
 UEFICA2023Status	REG_SZ	Updated
 WindowsUEFICA2023Capable	REG_DWORD	0x00000002 (2)

Metodo 2:

1. Aprire **Windows Security (Sicurezza di Windows)**.
2. Andare a **Device security (Sicurezza dispositivo)**.
3. In **Secure boot (Avvio sicuro)**, verificare il messaggio di stato. Se il certificato è aggiornato, la scheda riporta la dicitura: "Secure Boot è attivo e sono stati applicati tutti gli aggiornamenti necessari al certificato. Non sono necessarie ulteriori modifiche al certificato."

Secure boot

Secure Boot is on and all required certificate updates have been applied.
No further certificate changes are needed.

Nota

La funzione Windows Security mostra lo stato del certificato solo se sul dispositivo è effettuata l'installazione dell'aggiornamento cumulativo del 14 aprile 2026 o una versione successiva. Se non viene visualizzato alcun messaggio relativo allo stato del certificato, aggiornare Windows oppure ricorrere al Metodo 1.

Azioni consigliate

Un aggiornamento del BIOS aggiorna il firmware con i certificati del 2023 in modo permanente. Si tratta del metodo più affidabile e lo consigliamo anche se è stata già effettuata l'installazione dei certificati tramite Windows Update.

Importante

Se si installano i certificati esclusivamente tramite Windows Update e successivamente si ripristinano le impostazioni di fabbrica delle chiavi di avvio sicuro (Secure Boot) del BIOS, i certificati andranno persi e il dispositivo non si avvierà con l'avvio sicuro (Secure Boot) attivo. Aggiornare il BIOS per rendere permanenti i certificati prima di reimpostare le chiavi di Secure Boot.

Aggiornare il certificato tramite il BIOS

Installare la versione del BIOS indicata per il modello oppure una versione successiva. È possibile scaricarli dalla pagina del prodotto su Axis.com:

Modello	Versione minima del BIOS
AXIS S2208	Da confermare
AXIS S2212	Da confermare
AXIS S2216	Da confermare
AXIS S2224	Da confermare
AXIS S2108	Z218-004
AXIS S2208 Mk II	Z670-005
AXIS S2212 Mk II	Z671-005
AXIS S2216 Mk II	Z672-005
AXIS S2224 Mk II	Z673-005

Aggiornare il certificato tramite Windows Update

Se per il proprio modello non è ancora disponibile un aggiornamento del BIOS, è possibile ottenere i certificati del 2023 tramite Windows Update.

Importante

I certificati installati in questo modo vengono memorizzati nel database Secure Boot corrente, non nel firmware. Se si ripristinano le chiavi di Secure Boot del BIOS alle impostazioni di fabbrica, si perderanno i certificati e il dispositivo potrebbe non essere in grado di avviarsi con Secure Boot attivo. Installare un aggiornamento del BIOS non appena ne sarà disponibile uno per il proprio modello, anche se questo metodo è stato già utilizzato.

Per utilizzare questo percorso:

1. Controllare che il dispositivo utilizzi Windows 10 LTSC o Windows 11 LTSC.
2. Installare tutti gli aggiornamenti di Windows rilasciati il 14 aprile 2026 o successivamente.
3. Andare a **Windows Security (Sicurezza di Windows) > Device security (Sicurezza dispositivo) > Secure Boot (Avvio sicuro)** per verificare lo stato del proprio certificato.
4. Se il certificato non viene aggiornato dopo l'installazione degli ultimi aggiornamenti, controllare il valore di registro **UEFICA2023Status**. Se il dispositivo continua a non essere idoneo all'aggiornamento automatico, aggiornare il BIOS oppure contattare l'assistenza tecnica di Axis.

Importante

Non revocare manualmente il certificato del 2011 finché non è stato verificato che tutti i supporti di ripristino, gli ambienti di avvio e i driver presenti nel proprio ambiente siano firmati con il certificato del

2023. Se si revoca il certificato del 2011 troppo in anticipo, il dispositivo non sarà in grado di avviarsi con la funzione Secure Boot attiva.

Controllo della versione corrente del BIOS

Per controllare il BIOS corrente:

1. Accendere il dispositivo e premere ripetutamente **DEL** fino a quando non viene visualizzato il logo Axis.
2. Il numero di versione è mostrato come prima voce in **Main (Principale)**.

Aggiornare il BIOS

Seguire le istruzioni contenute nella guida del BIOS, disponibile nella pagina di download del file del BIOS.

Aggiornare Windows®

Windows® controlla periodicamente la disponibilità degli aggiornamenti. Quando è disponibile un aggiornamento, il dispositivo lo scarica automaticamente, ma è necessario installarlo manualmente.

Nota

La registrazione verrà interrotta durante un riavvio pianificato del sistema.

Per verificare manualmente la disponibilità di aggiornamenti:

1. Andare a **Settings (Impostazioni) > Windows Update (Aggiornamento Windows)**.
2. Fare clic su **Check for updates (Controlla aggiornamenti)**.

Configurazione delle impostazioni di Windows® Update

Si può modificare come e quando Windows® esegue gli aggiornamenti secondo le proprie esigenze.

Nota

Tutte le registrazioni in corso si interrompono durante un riavvio pianificato del sistema.

1. Aprire l'app **Esegui**.
 - Andare a **Windows System > Run (Sistema Windows > Esegui)** o
2. Digitare `gpedit.msc` e fare clic su **OK**. Si apre l'Editor criteri gruppi locali.
3. Andare a **Computer Configuration > Administrative Templates > Windows Components > Windows Update (Configurazione computer > Modelli amministrativi > Componenti di Windows > Windows Update)**.
4. Configurare le impostazioni in base alle esigenze, vedere esempio.

Esempio:

Per scaricare e installare automaticamente gli aggiornamenti senza alcuna interazione dall'utente e fare in modo che il dispositivo venga riavviato, se necessario, fuori dall'orario di ufficio, utilizzare la configurazione seguente:

1. Aprire **Always automatically restart at the scheduled time (Riavvia sempre all'ora pianificata)** e selezionare:
 - 1.1. **Attivato**
 - 1.2. **The restart timer will give users this much time to save their work (minutes) (Il timer di riavvio darà agli utenti questo tempo per salvare il loro lavoro (minuti))**: 15.
 - 1.3. Fare clic su **OK**.
2. Aprire **Configure Automatic Updates (Configurare aggiornamenti automatici)** e selezionare:
 - 2.1. **Attivato**
 - 2.2. **Configure Automatic updates (Configurare aggiornamenti automatici)**: **Download automatico e pianificazione dell'installazione**

- 2.3. Schedule Install day (Pianifica giorno di installazione): Ogni domenica
- 2.4. Schedule Install time (Pianifica l'ora di installazione): 00:00
- 2.5. Fare clic su OK.
3. Aprire Allow Automatic Updates immediate installation (Consenti installazione immediata di aggiornamenti automatici) e selezionare:
 - 3.1. Attivato
 - 3.2. Fare clic su OK.

Gestione alimentazione

Lo switch presenta un power budget totale pari a 105 W. È la potenza massima in uscita per tutti i dispositivi connessi.

Nella gran parte dei casi, i dispositivi connessi consumano meno energia di quanto richiesto. Per l'ottimizzazione dell'uso dell'alimentazione, il controller PoE permette ai dispositivi connessi di richiedere un massimo di 125 W e limita simultaneamente l'uso effettivo dell'alimentazione a 105 W.

Ad esempio, lo switch è in grado di alimentare 8 dispositivi di classe PoE 3.

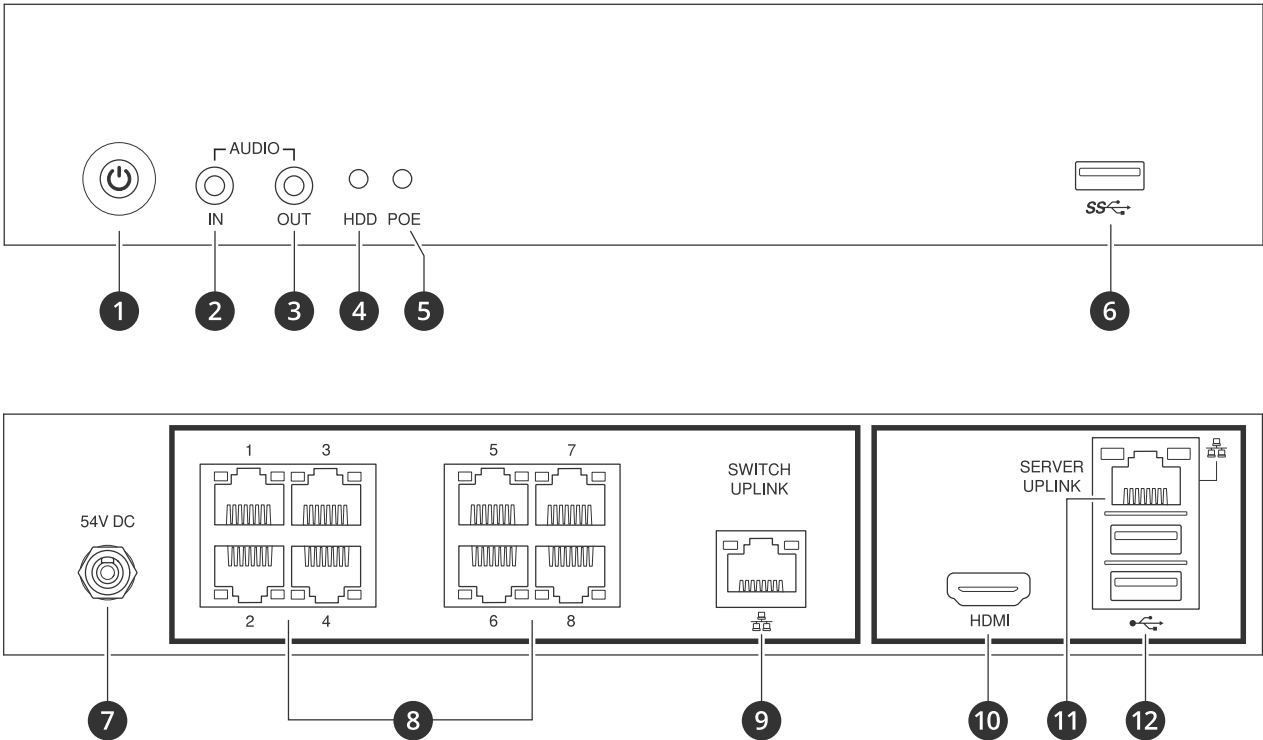
- 1 dispositivo di classe PoE 3 necessita di alimentazione da 15,4 W.
- 8 dispositivi di classe PoE 3 richiedono $(8 \times 15,4) =$ alimentazione da 123,2 W. Rientra nel limite di 125 W permesso dal controller PoE.
- 1 dispositivo di classe PoE 3 consuma di solito un'alimentazione fra 10 e 12 W.
- 8 dispositivi di classe PoE 3 consumano di solito un'alimentazione fra 80 e 96 W. Rientra nel limite di 105 W del power budget totale.

▲ AVVISO

- Quando i dispositivi connessi richiedono un'alimentazione oltre 125 W:
 - L'ultimo dispositivo collegato non si avvia.
 - Il LED di sovraccarico PoE si accende di rosso fisso fino al momento in cui non scollegherai l'ultimo dispositivo connesso o non si libererà un budget PoE sufficiente con la rimozione di altri dispositivi.
- Quando i dispositivi connessi consumano effettivamente un'alimentazione superiore a 105 W:
 - L'ultimo dispositivo acceso si arresterà e tenterà di riavviarsi.
 - Il LED di sovraccarico PoE non si accenderà.

Panoramica dei prodotti

Parte anteriore e posteriore



- 1 *Tasto di accensione/LED di accensione*
- 2 *Ingresso audio*
- 3 *Uscita audio*
- 4 *LED attività disco rigido*
- 5 *LED di stato delle porte PoE*
- 6 *Porta USB 3.0*
- 7 *Connettore di alimentazione*
- 8 *Porte PoE*
- 9 *Porta uplink switch RJ45*
- 10 *Porta HDMI*
- 11 *Porta uplink server RJ45*
- 12 *Porte USB 2.0*

Dati tecnici

LED anteriori

Indicatore LED	Colore	Significato
Alimentazione	Verde	Server attivo
Disco rigido	Lampeggia in giallo	Attività del disco rigido
	Lampeggia in rosso	Possibile guasto del disco rigido
Sovraccarico PoE	Rosso	Oltre il budget PoE
	Off	OK

LED posteriori

Velocità e attività della rete	Colore	Significato
LED destro	Giallo	10/100 Mbit/s
	Verde ¹	1000 Mbit/s
LED sinistro	Lampeggia in verde	Attività di rete

1. Valido solo per uplink switch e uplink server.

Risoluzione dei problemi

Eseguire un ripristino del sistema

Se si è verificato un guasto totale del sistema, è necessario utilizzare un'immagine di ripristino per ricreare il sistema Windows®. Per scaricare il kit di ripristino del registratore video di rete AXIS Network Video Recorder Recovery Kit, contattare il supporto tecnico Axis e fornire il numero di serie del dispositivo.

Nota

Il kit di ripristino per registratori video di rete AXIS è disponibile in due versioni:

- **sb11**: per i dispositivi che utilizzano ancora il certificato del 2011.
- **sb23**: per i dispositivi che sono passati al certificato del 2023.

Controllare lo stato del certificato prima di scaricare il Kit di ripristino e selezionare la variante corrispondente. Se si seleziona la variante errata, l'installazione non produrrà un risultato in grado di essere avviato e si dovrà ricominciare con l'immagine corretta. Questo non arrecherà danno al dispositivo.

Se sul dispositivo è già installato il certificato del 2023, la variante sb11 può ancora essere utilizzata in tutta sicurezza, a condizione che il certificato del 2011 non sia stato revocato in modo manuale. Una volta revocato, funzionerà solo sb23.

Per ricreare il sistema:

1. Scaricare il kit di ripristino del registratore video di rete AXIS Network Video Recorder Recovery Kit e lo strumento di ripristino AXIS Network Video Recorder Recovery: ISO su USB.
2. Inserire un'unità USB nel computer.
 - Utilizzare un'unità USB di minimo 16 GB.
 - L'unità USB verrà formattata e tutti i dati esistenti verranno cancellati.
3. Eseguire lo strumento AXIS Network Video Recorder Recovery: da ISO a USB e seguire le istruzioni visualizzate sullo schermo.
La scrittura dei dati sull'unità USB richiede da 10 a 15 minuti. Non rimuovere l'unità USB finché il processo non è completo.
4. Una volta eseguito lo strumento AXIS Network Video Recorder Recovery: da ISO a USB, prendere l'unità USB e collegarla al dispositivo.
5. Avviare il dispositivo.
6. Quando viene visualizzata la schermata iniziale di Axis, premere F12.
7. Fare clic su **UEFI: USB Drive (UEFI: supporto USB)**.
8. Accedere all'unità USB e premere enter (invio). Il sistema si avvia nel kit di ripristino del registratore di rete AXIS Network Video Recorder Recovery Kit.
9. Fare clic su **Reinstall Operating System (Reinstalla sistema operativo)**.
Il recupero richiede dai 10 ai 15 minuti. Sono disponibili istruzioni dettagliate nel download per il kit di recupero.

Risoluzione dei problemi di AXIS Camera Station

Per informazioni su come risolvere i problemi di AXIS Camera Station, andare al *manuale utente di AXIS Camera Station*.

Bisogno di assistenza?

Link utili

- *Guida per l'utente di AXIS Camera Station*
- *Accedi ad AXIS Secure Remote Access*
- *Elementi da includere nella lista consentiti di un antivirus per AXIS Camera Station*

Contattare l'assistenza

Se serve ulteriore assistenza, andare su axis.com/support.

T10181903_it

2026-07 (M7.2)

© 2022 – 2026 Axis Communications AB