

AXIS Camera Station S2208 Mk II Appliance

Impostazioni preliminari

Il flusso di lavoro standard per configurare un server di registrazione AXIS Camera Station Pro 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 7*.
4. Configurare Windows®. Si consiglia di:
 - Aggiornare Windows® alla versione più recente. Vedere *Aggiornare Windows®, on page 21*.
 - Creare un account utente standard. Vedere *Creare un account utente, on page 13*.
5. Aggiornare AXIS Camera Station Pro alla versione più recente.
 - Se il sistema è online: aprire l'applicazione AXIS Recorder Toolbox e fare clic su **Update AXIS Camera Station Pro (Aggiorna AXIS Camera Station Pro)**.
 - Se il sistema è offline: andare in *axis.com* e scaricare l'ultima versione.
6. Avviare il client AXIS Camera Station Pro.
7. *Connessione al server AXIS Camera Station Pro.*
8. *Configurazione di AXIS Camera Station Pro, on page 8.*

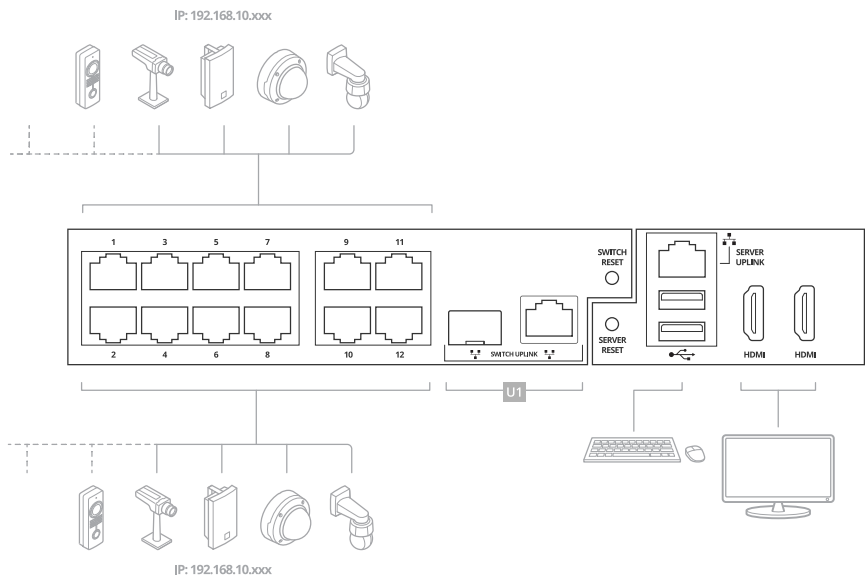
Installare il dispositivo

Per istruzioni relative all'installazione del prodotto, consulta la guida all'installazione inclusa nella confezione o nella pagina di supporto del prodotto su *axis.com*.

Esempi di setup

Configurazione in una rete di sorveglianza indipendente

È possibile creare una rete di sorveglianza indipendente che non abbia interconnettività con un'altra rete esterna. Questa configurazione è un'installazione plug and play di base. Il server DHCP dello switch incorporato è abilitato per impostazione predefinita. Non appena si collegano le telecamere alle porte PoE, le prime si accendono, ottengono un indirizzo IP e diventano accessibili tramite AXIS Camera Station Pro.



Livello di difficoltà	Base
Vantaggi	Rete di sorveglianza dedicata senza interconnettività verso un'altra rete esterna Installazione plug-and-play
Limiti	Larghezza di banda Budget PoE Nessun accesso remoto
Azioni necessarie	Modificare la password predefinita per lo switch integrato Registrare la licenza di AXIS Camera Station Pro

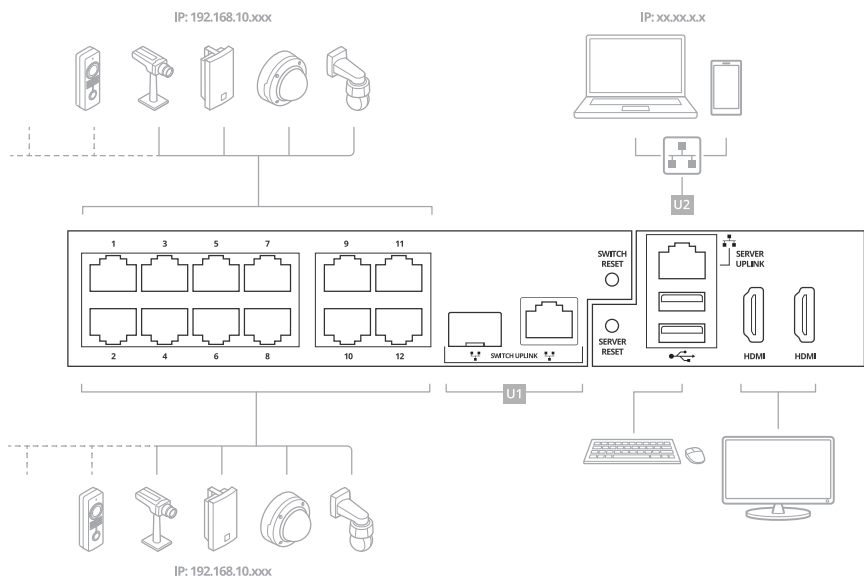
Connettori utilizzati	Porte Ethernet PoE Porte USB 2.0 (per tastiera e mouse) Displayport™ o connettore HDMI
Connettori NON utilizzati	Porta uplink switch Porta uplink server Porta USB 3.2 (lato anteriore) Presa audio universale (lato anteriore)

Configurazione in una rete esistente

È possibile creare una rete di sorveglianza all'interno di una rete esistente. Ciò significa che la rete di sorveglianza è separata dalla rete esistente.

Nota

L'apparecchio non dirige i dati di rete dalla rete di sorveglianza alla rete server per la registrazione quando si utilizza un registratore supplementare, ad esempio i modelli AXIS S30 Recorders. Assicurarsi che gli AXIS S30 Recorders e le telecamere siano collegati alla stessa rete.

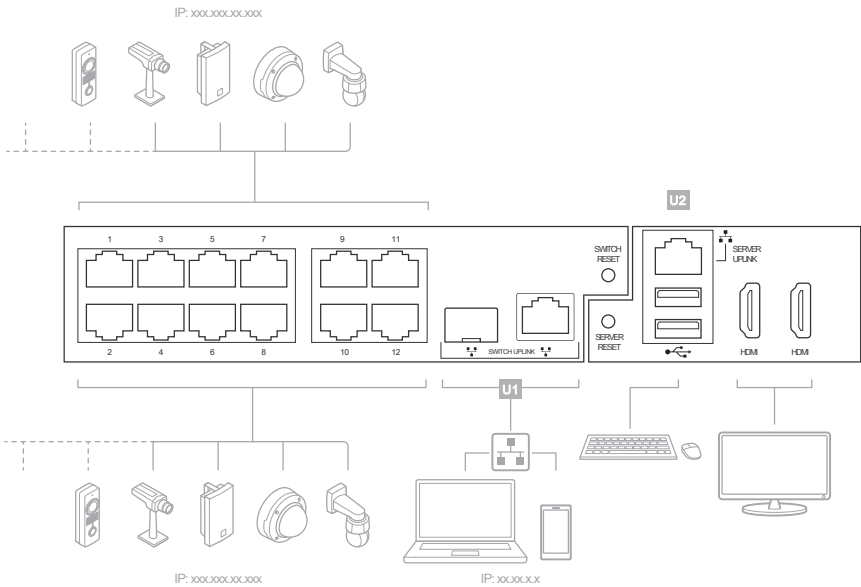


Livello di difficoltà	Avanzata
Vantaggi	Possibilità di utilizzare un client AXIS Camera Station Pro per connettersi alla serie S22 in rete. Separazione della rete
Limiti	Potrebbe richiedere l'ottemperanza con le politiche della rete aziendale
Azioni necessarie	Modificare la password predefinita per lo switch integrato Registrare la licenza di AXIS Camera Station Pro

Connettori utilizzati	Porte Ethernet PoE Porta Ethernet – Uplink del server per il collegamento di rete (Facoltativo) porte USB 2.0 (per tastiera e mouse) (Facoltativo) Connettore Displayport™ o HDMI
Connettori NON utilizzati	Porta uplink switch Porta USB 3.2 (lato anteriore) Presa audio universale (lato anteriore)

Collegare lo switch direttamente alla rete aziendale

Questa impostazione integra il sistema direttamente nella rete aziendale esistente, consentendo l'accesso e il monitoraggio delle telecamere da qualsiasi punto della rete.



Livello di difficoltà	Avanzata
Vantaggi	Le telecamere sono accessibili dalla rete aziendale e possono essere monitorate con un server SNMP.
Limiti	Potrebbe richiedere l'ottemperanza con le politiche della rete aziendale
Azioni necessarie	Disattivare DHCP sullo switch Modificare l'indirizzo IP dello switch con uno statico della rete aziendale. Impostare il NIC interno del PC su DHCP o su un IP statico sulla rete aziendale Modificare la password predefinita dello switch. Configurazione e registrazione di AXIS Camera Station Pro

Connettori utilizzati	Porte Ethernet PoE Porta uplink switch (U1) (Facoltativo) porte USB 2.0 (per tastiera e mouse) (Facoltativo) Connettore Displayport™ o HDMI
Connettori NON utilizzati	Porta uplink PC (U2) Porta USB 3.2 (lato anteriore) Presa audio universale (lato anteriore)

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.

Nota

Le impostazioni sono per il server. Per modificare le impostazioni dello switch, andare alla pagina di gestione dello switch. Vedere *Impostazioni*, on page 28.

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.

Connessione a un server

Il client AXIS Camera Station S2208 Mk II Appliance consente di connettersi a un singolo server o a più server in diversi modi:

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 8.

Nota

- La prima volta che si effettua la connessione a un server, il client verifica l'ID del certificato del server. Per essere sicuri di connettersi al server corretto, confrontare l'ID del certificato con quello visualizzato nel controllo di servizio di AXIS Camera Station S2208 Mk II Appliance.

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 per tutti i server collegati, fare clic su Delete saved passwords (Elimina password salvate) .
Cambia le impostazioni proxy del client	Se non si riesce a connettersi a un server, potrebbe essere necessario aggiornare le impostazioni del proxy del client. 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 S2208 Mk II 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 S2208 Mk II Appliance**, è necessario configurare le impostazioni proxy in Windows sul server **AXIS Camera Station S2208 Mk II 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 Pro

Operazioni preliminari:

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

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

1. *Avviare il video management system*
2. *Aggiunta di dispositivi*
3. *Configura metodo di registrazione, on page 9*
4. *Visualizzazione del video in diretta, on page 10*
5. *Visualizzazioni registrate, on page 10*
6. *Aggiunta di segnalibri, on page 10*
7. *Esportazione delle registrazioni, on page 10*
8. *Riproduzione e verifica delle registrazioni in AXIS File Player., on page 10*

Avviare il video management system

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

È possibile collegarsi a più server di AXIS Camera Station Pro in modi diversi.

Aggiunta di dispositivi

Al primo avvio di AXIS Camera Station S2208 Mk II Appliance, si apre la pagina **Add devices (Aggiungi dispositivi)**, che esegue la ricerca nella rete per individuare i dispositivi da aggiungere.

1. Selezionare i dispositivi che si desidera aggiungere dall'elenco. Se non si riesce a trovare un dispositivo, fare clic su **Manual search** (Ricerca manuale) oppure digitare il filtro.
2. Fare clic su **Aggiungi**.
3. Fai clic su **Close (Chiudi)** per saltare la configurazione e proseguire in un secondo momento. Adesso, per proseguire con la configurazione:
 - 3.1. Scegliere **Quick configuration** (Configurazione rapida) oppure **Site Designer configuration** (Configurazione Site designer). Per ulteriori informazioni, vedere .
 - 3.2. Selezionare **Add image overlay for date, time, and text** (Aggiungi una sovrapposizione di immagini per data, ora e testo) per aggiungere sovrapposizioni a qualsiasi telecamera Axis che non ne dispone già.
 - 3.3. Fare clic su **Next (Avanti)**.
 - 3.4. Selezionare la preferenza del **Recording method** (Metodo di registrazione).
 - 3.5. Fare clic su **Next (Avanti)**.
 - 3.6. Scegliere il **Retention time** (Tempo di archiviazione), il **Recording storage** (Archiviazione registrazione) e fare clic su **Finish (Fine)** per applicare la configurazione.

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 del proxy o del firewall prima di utilizzare AXIS Camera Station S2208 Mk II Appliance se il client, il server e i dispositivi di rete collegati si trovano su reti diverse.

Impostazioni proxy client

Se un server proxy si trova tra il client e il server, configurare le impostazioni proxy in Windows sul computer client. Contattare il supporto Axis per ulteriori informazioni.

Impostazioni proxy del server

Se il server proxy si trova tra il dispositivo di rete e il server, è necessario configurare le impostazioni proxy in Windows sul server. Contattare il supporto Axis per ulteriori informazioni.

NAT and Firewall (NAT e Firewall)

Quando un NAT o firewall separa il client e il server, configurarli per garantire che la porta HTTP, la porta TCP e la porta di streaming specificate in AXIS Camera Station S2208 Mk II Appliance Service Control possano passare attraverso. Contattare il proprio amministratore di rete per ricevere assistenza.

Configurazione della porta del server

Il server AXIS Camera Station S2208 Mk II Appliance 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 S2208 Mk II Appliance su una rete protetta separata da una rete d'ufficio. È possibile installare il client AXIS Camera Station S2208 Mk II 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

Per utilizzare la licenza automatica, è necessario registrare il proprio sistema e connetterlo a un'organizzazione.

1. Andare a **Configuration (Configurazione) > Licenses (Licenze) > Management (Gestione)**.
2. Verificare che l'opzione **Automatic licensing (Licenza automatica)** sia attiva.
3. Fare clic su **Register... (Registra...)**.
4. Eseguire l'accesso usando il proprio account My Axis e seguire le istruzioni sullo schermo.
5. Fare clic su **Go to AXIS License Manager (Vai ad AXIS License Manager)** per la gestione delle licenze. Per saperne di più, leggere il *manuale per l'utente My Systems su help.axis.com*.

Ottenimento di una licenza per un sistema offline

Per l'ottenimento manuale di una licenza per il sistema:

1. Andare a **Configuration (Configurazione) > Licenses (Licenze) > Management (Gestione)**.
2. Disattivare **Automatic licensing (Concessione automatica delle licenze)**.
3. Fare clic su **Export system file... (Esporta file di sistema...)** e salvare il file sul computer.

Nota

Per eseguire l'accesso ad AXIS License Manager è necessaria una connessione Internet. Se il computer client non ha Internet, copiare il file di sistema su un computer che lo ha.

4. Aprire *AXIS License Manager*.
5. In *AXIS License Manager*:
 - 5.1. Selezionare l'organizzazione giusta o crearne una se necessario. Per saperne di più, leggere il *manuale per l'utente My Systems su help.axis.com*.
 - 5.2. Andare a **System setup (Configurazione del sistema)**.
 - 5.3. Fare clic su **Upload system file (Carica file di sistema)**.
 - 5.4. Fare clic su **Upload system file (Carica file di sistema)** e selezionare il proprio file di sistema.
 - 5.5. Fare clic su **Upload system file (Carica file di sistema)**.
 - 5.6. Fare clic su **Download license file (Scarica il file di licenza)**.
6. Tornare al client *AXIS Camera Station S2208 Mk II Appliance*.
7. Fare clic su **Import license file... (Importa file di licenza...)** e selezionare il proprio file di licenza.
8. Fare clic su **Go to AXIS License Manager (Vai ad AXIS License Manager)** per la gestione delle licenze.

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 (Impostazioni) > Accounts (Account) > Other users (Altri Utenti) > Add other user (Aggiungi altro utente)** e fare clic su **Add account (Aggiungi account)**.
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 Pro

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 S2208 Mk II Appliance.

Nota

Agli amministratori del computer su cui viene eseguito il server AXIS Camera Station S2208 Mk II Appliance vengono garantiti determinati privilegi di amministratore in AXIS Camera Station S2208 Mk II 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 S2208 Mk II Appliance. Per aggiungere un utente a AXIS Camera Station S2208 Mk II 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 S2208 Mk II 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 S2208 Mk II 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 S2208 Mk II Appliance.
Modifica	Consente la modifica delle viste in AXIS Camera Station S2208 Mk II 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.

Aggiunta di ulteriore archiviazione

Lo spazio di archiviazione necessario può variare. Il tempo di conservazione dei dati memorizzati o l'archiviazione di registrazioni ad alta risoluzione richiedono spesso l'installazione di una maggiore quantità di memoria. Questa sezione spiega come installare un disco rigido aggiuntivo nel prodotto della serie AXIS S22.

Nota

Seguire le istruzioni riportate di seguito per aggiungere archiviazione ai prodotti AXIS S22 applicabili. Queste istruzioni vanno intese così come sono e Axis Communications AB non si assume alcuna responsabilità per la perdita di dati o la configurazione errata durante questi passaggi. Rispettare le precauzioni standard quando si esegue il backup di dati critici per l'azienda. La seguente procedura di espansione dell'archiviazione non sarà supportata dall'assistenza tecnica Axis.

Nota

Per evitare scariche elettrostatiche, si consiglia di utilizzare sempre un tappetino statico e una cinghia statica durante gli interventi sui componenti interni del sistema.

Garanzia

Informazioni dettagliate sulla garanzia sono disponibili all'indirizzo: www.axis.com/support/warranty.



Per guardare questo video, andare alla versione web di questo documento.

Rimozione della mascherina

1. Allentare le due viti a testa zigrinata poste su ciascun lato della mascherina.
2. Rimozione della mascherina.

Installazione del disco rigido

⚠ ATTENZIONE

- Utilizza solo dischi rigidi che sono stati testati e approvati per l'uso con la serie AXIS S22.
 - Quando si installa un disco rigido, accertarsi che il supporto del disco rigido sia premuto fino in fondo. Si sente un clic su quando si blocca il supporto per disco rigido.
 - Prima dell'installazione di un disco rigido, assicurati che il cavo di alimentazione sia scollegato.
1. Arresta il sistema e verifica che l'apparecchio sia spento.
 2. Scollega il cavo dell'alimentazione.
 3. Premere il pulsante di rilascio nella parte anteriore del supporto per disco rigido e aprire la maniglia di tale supporto.
 4. Estrarre il supporto del disco rigido utilizzando la maniglia.
 5. Inserire un disco rigido nel supporto per disco rigido.

6. Fissare il disco rigido al supporto del disco rigido con quattro viti.
7. Inserire il supporto per disco rigido nello slot del disco rigido fino a quando il supporto non si collega con il backplane.
8. Chiudere la maniglia del supporto per disco rigido per bloccare il disco.
9. Rimontare la mascherina anteriore.
10. Avvia il sistema.

Aggiungere una nuova archiviazione per la registrazione

1. Creare e formattare una nuova partizione del disco rigido in Windows:
 - 1.1. Fai clic con il pulsante destro del mouse su **Start menu (Menu Avvio)** e seleziona **Disk Management (Gestione disco)**.
 - 1.2. Fare clic su **OK** se appare il messaggio pop-up **Initialize Disk (Inizializza disco)**. Se così non fosse, fare clic con il tasto destro del mouse sul nuovo disco rigido e selezionare **Initialize Disk (Inizializza disco)**.
 - 1.3. Fare clic con il tasto destro del mouse su una regione non allocata del disco appena inizializzato e selezionare **New Simple Volume (Nuovo volume semplice)**.
 - 1.4. Seguire la procedura guidata per impostare le dimensioni del volume, assegnare una lettera all'unità e formattare la partizione.
 - 1.5. Completate la procedura guidata per creare il nuovo volume semplice.
2. Aggiungere un nuovo archivio di registrazione in AXIS Camera Station Pro:
 - 2.1. Aprire AXIS Camera Station Pro.
 - 2.2. Andare a **Storage (Archiviazione) > Management (Gestione)**.
 - 2.3. Fare clic su **Aggiungi...**
 - 2.4. Selezionare il disco aggiunto di recente e fare clic su **OK**.
 - 2.5. Andare a **Storage (Archiviazione) > Selection (Selezione)**.
 - 2.6. Selezionare i dispositivi su cui trasferire i dati di registrazione sulla nuova unità.
 - 2.7. Nell'elenco a discesa **Store to (Archivia in)**, selezionare la nuova unità e fare clic su **Apply (Applica)**.

Per ulteriori informazioni sulla gestione dell'archiviazione, vedere *AXIS Camera Station Pro - User manual*.

Gestire lo switch integrato

Informazioni sullo switch integrato

AXIS Camera Station S22 Mk II Appliance Series è dotata di uno switch Power over Ethernet (PoE) integrato. È possibile configurare e gestire lo switch incorporato.

Lo scopo dello switch è quello di separare il traffico sulla rete in modo che le telecamere di sicurezza e il traffico correlato gestito dallo switch (porte PoE e uplink switch) non siano condivisi con altre reti.

La gestione di potenza dello switch segue queste regole:

- Ogni porta può riservare alimentazione in base alla classe PoE del dispositivo alimentato collegato. È anche possibile assegnare manualmente la potenza a una porta.
- Se il consumo energetico effettivo per una determinata porta supera l'alimentazione riservata per tale porta, essa si arresterà.
- Le porte si disattivano quando il consumo energetico effettivo per tutte le porte supera la quantità totale di energia che l'alimentatore è in grado di fornire. Le porte vengono quindi disattivate in base alla priorità, un numero di porta inferiore indica una priorità più alta.

Accedere alla pagina di gestione dello switch

1. Andare alla barra dei menu.
 - Immettere l'indirizzo IP dello switch nel browser web. Predefinito: 192.168.10.1
 - Da AXIS Recorder Toolbox, andare a **Switch > Open the switch configuration (Switch > Aprire la configurazione dello switch)**.
2. Accedere con nome utente password.
 - Il nome utente è `admin`
 - La password è riportata sull'adesivo posto sull'unità, dietro il coperchio anteriore e inclusa nel contenuto della confezione come etichetta autoadesiva.

Log out (Uscire) dalla barra dei menu per uscire dalla pagina di gestione dello switch.

Configurazione in esecuzione

La configurazione in esecuzione è l'insieme delle impostazioni attualmente attive e operanti sul dispositivo di rete. Riflette lo stato attuale del dispositivo e il suo funzionamento in tempo reale. Tuttavia, sono modifiche che non vengono salvate quando si riavvia il dispositivo.

Invece, la configurazione di avvio è l'insieme delle impostazioni salvate nella memoria non volatile del dispositivo. Questa configurazione viene caricata e applicata all'avvio o al riavvio del dispositivo.

Quando si apportano modifiche nell'interfaccia web e si fa clic su **Save (Salva)**, tali modifiche vengono applicate alla configurazione in esecuzione.

Per salvare le impostazioni nella configurazione di avvio, utilizzare l'icona Save (Salva) nell'angolo superiore destro dell'interfaccia web.

Se ci sono modifiche non salvate nella configurazione in esecuzione, l'icona lampeggia in giallo.

Panoramica

Nella barra dei menu, fare clic su **Overview (Panoramica)**.

Informazioni generali

Categoria	Elemento	Descrizione
Riepilogo delle porte	Porte attive	Il numero di porte in uso.

	Porte che utilizzano PoE	Il numero di porte PoE abilitate, in uso.
	Porte bloccate	Il numero di porte bloccate.
Consumo elettrico	Utilizzo PoE corrente	La potenza PoE in watt consumata dai dispositivi e la percentuale di potenza PoE consumata rispetto alla potenza totale PoE dedicata.
	Alimentazione necessaria	l'energia totale in watt e la percentuale allocata ai dispositivi.
Stato delle porte	Attivo	La porta è in uso.
	Inattivo	La porta è pronta per l'uso.
	Bloccato	La porta è bloccata.

Nota

È possibile fare clic su una porta per visualizzare ulteriori informazioni su di essa.

Gestione alimentazione

Nella barra dei menu, fare clic su **Power management (Gestione potenza)**.

Elenco delle porte

Elemento	Descrizione
Porta	il numero della porta a cui è collegato il dispositivo.
PoE	Lo stato PoE. È possibile fare clic sull'icona per attivare o disattivare PoE sulla porta.
Classe PoE	Classe PoE del dispositivo connesso.
Priorità	La priorità dell'allocazione dell'alimentazione al dispositivo connesso. Per impostazione predefinita, la priorità è il numero di porta.
Consumo energetico (W)	L'energia in watt consumata dal dispositivo collegato alla porta.
Alimentazione necessaria (W)	L'energia in watt richiesta dal dispositivo collegato alla porta.
Alimentazione allocata (W)	Regolare manualmente l'alimentazione allocata alla porta. Disponibile solo quando si seleziona Manual (Manuale) come metodo di allocazione dell'alimentazione.

Allocazione dell'alimentazione

L'alimentazione PoE può essere allocata ai dispositivi collegati nei seguenti modi:

- **Classe PoE:** lo switch alloca l'alimentazione PoE in base alla classe PoE del dispositivo collegato.
- **Manual (Manuale):** è possibile regolare manualmente l'alimentazione PoE allocata al dispositivo collegato.
- **LLDP-MED:** lo switch comunica con il dispositivo collegato e alloca dinamicamente la potenza PoE in base alle esigenze.

Nota

Il metodo di allocazione potenza di LLDP-MED funziona solo per le telecamere con AXIS OS 9.20 o versione successiva.

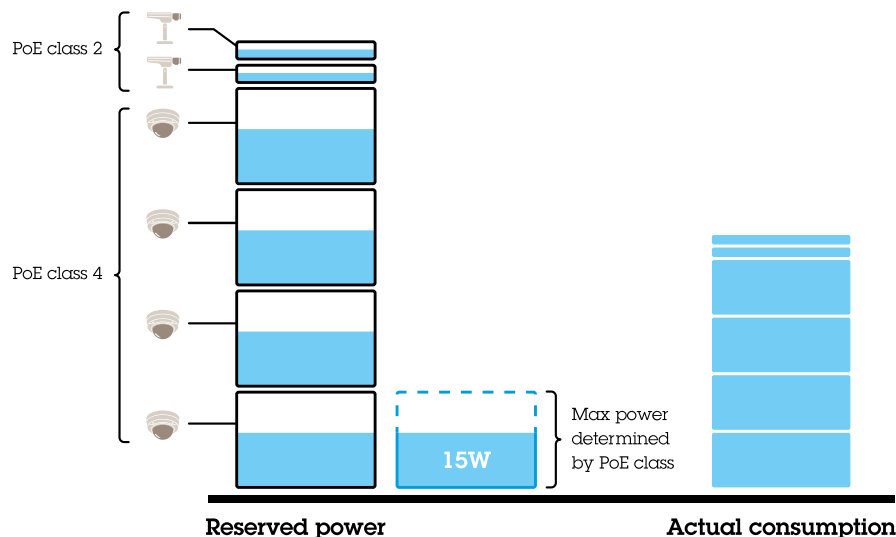
Per modificare il metodo di allocazione dell'alimentazione:

1. nella pagina di gestione dell'alimentazione dello switch, andare a **Power management (Gestione alimentazione)**.
2. Selezionare **PoE Class (Classe PoE)**, **Manual (Manuale)** o **LLDP-MED in Allocate power (Alloca alimentazione)**
3. Se si è selezionato **Manual (Manuale)**, è possibile modificare la potenza assegnata al dispositivo collegato nella colonna **Power allocated (Potenza assegnata)**.
4. Se si desidera modificare la priorità del dispositivo connesso, selezionare una priorità per tale dispositivo. La priorità degli altri dispositivi cambierà automaticamente.

Esempio:

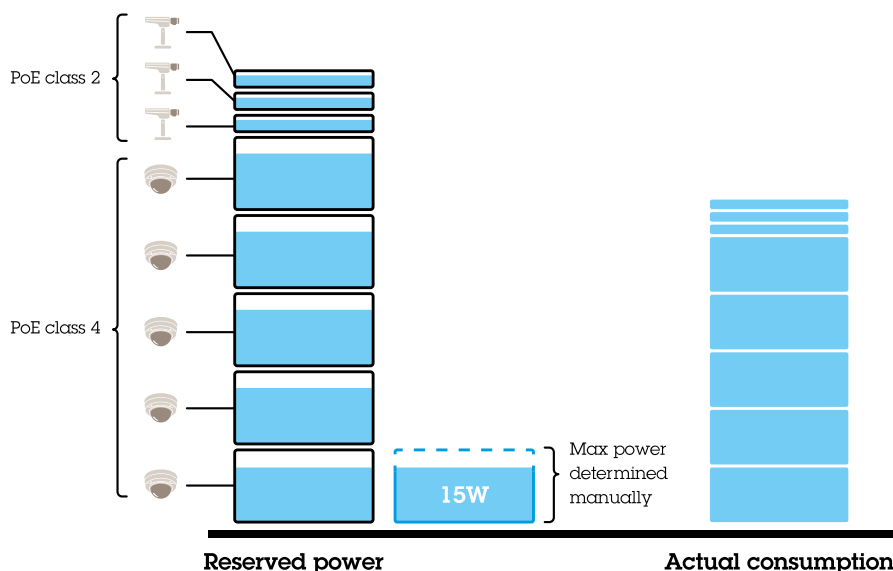
In questo esempio, lo switch ha un fabbisogno di potenza totale di 135 W. Un dispositivo di classe PoE 4 richiede 30 W di potenza ma consuma solo 15 W. Un dispositivo di classe PoE 2 richiede 7 W di potenza ma consuma solo 5 W di potenza.

Allocate power by PoE class (Allocaire l'alimentazione in base alla classe PoE)



L'alimentazione richiesta da ogni dispositivo è determinata dalla classe PoE. Lo switch può alimentare 4 dispositivi PoE di classe 4 e 2 dispositivi PoE di classe 2. L'alimentazione totale richiesta è $(4 \times 30) + (2 \times 7) = 134$ W. La potenza effettiva consumata è $(4 \times 15) + (2 \times 5) = 70$ W. In questo modo, è garantita l'alimentazione sufficiente a tutti i dispositivi collegati e la priorità è meno importante.

Allocate power manually (Allocaire l'alimentazione manualmente)



L'alimentazione richiesta viene regolata manualmente a 20 W per i dispositivi PoE di classe 4. Lo switch può alimentare 5 dispositivi PoE di classe 4 e 3 dispositivi PoE di classe 2. L'alimentazione totale richiesta è $(5 \times 20) + (3 \times 7) = 121$ W. La potenza effettiva consumata è $(5 \times 15) + (3 \times 5) = 90$ W. In questo modo, è garantita l'alimentazione sufficiente a tutti i dispositivi collegati e la priorità è meno importante.

Attivare e disattivare PoE

Attivare PoE su una porta

1. Nella barra dei menu, fare clic su **Overview (Panoramica)**.
2. Nella colonna PoE, fare clic per attivare  PoE sulla porta specifica.

Turn off PoE on a port (Disattivare PoE su una porta)

1. Nella barra dei menu, fare clic su **Overview (Panoramica)**.
2. Nella colonna PoE, fare clic su  per disattivare PoE sulla porta specifica.

Attivare e disattivare PoE su tutte le porte

1. Nella barra dei menu, fare clic su **Power management (Gestione potenza)**.
2. Per disattivare PoE su tutte le porte, andare al menu a discesa **PoE port state (Stato porta PoE)** e selezionare **Turn off all (Disattiva tutto)**.
3. Per attivare PoE su tutte le porte, andare al menu a discesa **PoE port state (Stato porta PoE)** e selezionare **Turn off all (Attiva tutto)**.

Panoramica di rete

La panoramica di rete fornisce informazioni dettagliate sullo stato del traffico di rete di ciascuna porta.

Porte PoE

Elemento	Descrizione
Porta	il numero della porta a cui è collegato il dispositivo.
Dispositivo	Il nome del dispositivo collegato alla porta.
Indirizzo IP	L'indirizzo IP del dispositivo collegato alla porta.
Indirizzo MAC	Il MAC address del dispositivo collegato alla porta.
Receive (Ricezione)	La velocità corrente dei dati in megabit al secondo per i dati in entrata sulla porta.

Transmit (Trasmissione)	La velocità corrente dei dati in megabit al secondo per i dati in uscita sulla porta.
Packet sent (Pacchetto inviato)	Il numero di pacchetti di dati che lo switch ha trasmesso alla rete.
Packet received (Pacchetto ricevuto)	Il numero di pacchetti di dati che lo switch ha ricevuto dalla rete.
Packet lost (Pacchetto perso)	Il numero e la percentuale di pacchetti di dati che non hanno raggiunto la propria destinazione a causa di problemi di rete.
Serratura	Indica se la porta è bloccata. È possibile fare clic sull'icona per bloccare o sbloccare la porta.

Bloccare e sbloccare le porte

È possibile legare un MAC address a una porta in modo che passi solo il traffico proveniente da esso. Ciò migliora la sicurezza e impedisce agli utenti non autorizzati di connettere un computer portatile o altri dispositivi alla rete di sicurezza.

Bloccare un MAC address a una porta

1. Nella barra dei menu, fare clic su **Network overview (Panoramica della rete)**.
2. Nella colonna **Lock (Blocca)**, fare clic su  per bloccare la porta specifica.

Sbloccare un MAC address da una porta

1. Nella barra dei menu, fare clic su **Network overview (Panoramica della rete)**.
2. Nella colonna **Lock (Blocca)**, fare clic su  per sbloccare la porta specifica.

Bloccare o sbloccare tutte le porte

1. Nella barra dei menu, fare clic su **Network overview (Panoramica della rete)**.
2. Per bloccare tutte le porte, andare al menu a discesa **Lock ports (Blocca porte)** e selezionare **Lock all (Blocca tutto)**.
3. Per sbloccare tutte le porte, andare al menu a discesa **Lock ports (Blocca porte)** e selezionare **Unlock all (Sblocca tutto)**.

Impostazioni

Configurare le impostazioni di rete

È possibile modificare l'indirizzo IP dello switch. Tuttavia, per la maggior parte delle installazioni della telecamera, si consiglia di utilizzare le impostazioni predefinite. Il motivo è che una rete di sorveglianza normalmente è isolata dalle altre reti, ad esempio da una LAN aziendale. In questo caso, la rete di sorveglianza verrebbe utilizzata solo per gestire e raccogliere i dispositivi di sorveglianza e i dati dal software per la gestione video installato sul server.

1. Nella barra dei menu, andare a **Settings (Impostazioni) > Network settings (Impostazioni di rete)**.
2. Immettere il tipo di connessione, l'indirizzo IP, la subnet mask, il gateway, il DNS primario, il DNS secondario e il nome host.

Nota

Le impostazioni predefinite di fabbrica sono: una connessione IP statica con l'indirizzo 192.168.10.1 e una subnet mask con l'indirizzo 255.255.255.0.

3. Fare clic su **Save (Salva)**.

Configurare la data e l'ora

1. Nella barra dei menu, andare a **Settings (Impostazioni) > Date and time (Data e ora)**.
2. Selezionare il paese e il fuso orario.
3. Per impostare l'ora manualmente, selezionare **Manual (Manuale)** e regolare manualmente l'ora.
4. Per impostare un server NTP, selezionare **NTP server (Server NTP)** e immettere l'indirizzo del server NTP.

Nota

NTP funziona solo quando lo switch è connesso a una rete e configurato con accesso a Internet.

5. Fare clic su **Save (Salva)**.

Configurare server DHCP

È possibile configurare lo switch perché utilizzi il proprio server DHCP interno per assegnare indirizzi IP ai dispositivi connessi. Quando si utilizza la connessione switch uplink per consentire ai dispositivi di accedere o consentire l'accesso ad essi da parte di applicazioni esterne, è necessario specificare il gateway e gli indirizzi DNS.

1. Nella barra dei menu, andare a **Settings (Impostazioni) > DHCP server (Server DHCP)**.
2. Selezionare **Enable DHCP server (Abilita il server DHCP)**.
3. Immettere l'indirizzo IP iniziale, l'indirizzo IP finale, la subnet mask, il gateway, il DNS primario, il DNS secondario, la durata del lease e il nome di dominio.
4. Fare clic su **Save (Salva)**.

Configurare SNMP

1. Nella barra dei menu, andare a **Settings (Impostazioni) > SNMP**.
2. Immettere il nome del server, il contatto e l'ubicazione utilizzati per la connessione SNMP.
3. Se si desidera utilizzare SNMPV1 o SNMPV2c, selezionare **SNMPV1 / SNMPV2c** e accedere alla comunità con privilegi in lettura.
4. Se si desidera utilizzare SNMPV3, selezionare **SNMPV3 (MD5)** e immettere il nome utente e la password.

Nota

Attualmente è supportata solo l'autenticazione MD5 utilizzata per SNMP.

5. Fare clic su **Save (Salva)**.

Manutenzione

Aggiornamento firmware

1. Nella barra dei menu, andare a **Maintenance (Manutenzione) > Update firmware (Aggiorna firmware)**.
2. Trascinare e rilasciare il file del firmware o fare clic su **Browse (Sfoglia)** e accedere al file del firmware.
3. Fare clic su **Upload (Carica)**.
4. Una volta aggiornato il firmware, riavviare lo switch.

Riavviare lo switch

Importante

Durante il riavvio dello switch, tutti i dispositivi collegati perderanno temporaneamente la connessione con esso, incluso PoE.

1. Nella barra dei menu, andare a **Maintenance (Manutenzione) > Reboot switch (Riavvia switch)**.

2. Fare clic su **Reboot (Riavvia)** e **Yes (Sì)**.
3. Quando lo switch si riavvia dopo alcuni minuti, immettere il nome utente e la password per accedere.

Eseguire il backup delle impostazioni dello switch

Nota

Il nome utente e la password sono inclusi nel file di backup.

1. Nella barra dei menu, andare a **(Maintenance) Manutenzione > Backup and restore (Backup e ripristino)**.
2. Fare clic su **Create a backup file (Crea un file di backup)**. Questa operazione crea un file di backup in formato .bin e lo salva nella cartella **Downloads (Download)**.

Ripristinare le impostazioni dello switch

Nota

Per ripristinare le impostazioni dello switch, è necessario aver creato in precedenza un file di backup.

1. Nella barra dei menu, andare a **(Maintenance) Manutenzione > Backup and restore (Backup e ripristino)**.
2. Trascinare e rilasciare il file di backup o fare clic su **Browse (Sfoglia)** e accedere al file di backup.
3. Fare clic su **Upload (Carica)**.

Possono volerci alcuni minuti per ripristinare lo switch dal file di backup. Dopo il ripristino delle impostazioni, lo switch si riavvierà automaticamente e si dovrà accedere di nuovo.

Gestione certificati

1. Nella barra dei menu, andare a **Maintenance (Manutenzione) > Manage certificates (Gestione certificati)**.
2. Fare clic su  e accedere al file della chiave privata.
3. Fare clic su  e accedere al file del certificato.
4. Fare clic su  e accedere al file CA bundle.
5. Fare clic su **Save (Salva)**.
6. Riavviare lo switch.

Modifica della password

È possibile modificare la password predefinita dello switch e impostare una password scelta dall'utente.

Importante

Assicurarsi di selezionare una password facile da ricordare. Se si dimentica la password, vedere *Ripristino delle impostazioni predefinite di fabbrica, on page 31* per ripristinare la password predefinita in fabbrica.

1. Nella barra dei menu, andare a **Maintenance (Manutenzione) > Change password (Modifica password)**.
2. Immettere la password corrente e la nuova password come richiesto.
3. Fare clic su **Save (Salva)**.

Configurazione delle impostazioni web

1. Nella barra dei menu, andare a **Maintenance (Manutenzione) > Web settings (Impostazioni Web)**.
2. Immettere il numero di porta.

Nota

- Se si decide di modificare il numero porta, assicurarsi di annotare il nuovo numero porta. Se si dimentica il nuovo numero porta, vedere *Ripristino delle impostazioni predefinite di fabbrica, on page 31* per ripristinare il numero porta predefinito in fabbrica.
- Si raccomanda di mantenere abilitato HTTPS.

Ripristino delle impostazioni predefinite di fabbrica

Tenere premuto il pulsante di reset per cinque secondi per ripristinare le impostazioni predefinite di fabbrica dello switch.

È possibile resettare lo switch tramite interfaccia web:

1. Nella barra dei menu, andare a **Maintenance (Manutenzione) > Reset to factory default settings (Ripristino delle impostazioni predefinite di fabbrica)**.
2. Fare clic su **Reset (Reimposta)** e **Yes (Sì)**.

Al termine del ripristino, lo switch si riavvierà automaticamente.

Registri

Nella barra dei menu, fare clic su **Logs (Registri)** per accedere a un elenco di log. Fare clic sul titolo della colonna per ordinare le voci in ordine alfabetico.

Elemento	Descrizione
Ora	La data e l'ora in cui si è verificato l'evento del registro.
Livello	Il livello di gravità visualizzato come icone di avviso.
Utente	L'utente che avvia l'evento del registro.
Indirizzo IP	L'indirizzo IP dell'utente che avvia l'evento del registro.
Servizio	Il servizio a cui è correlato l'evento del registro. I possibili valori sono desktop, rete, rete, sistema, ntpd, archiviazione, dhcp, ecc.
Evento	Descrizione dell'evento di registro.

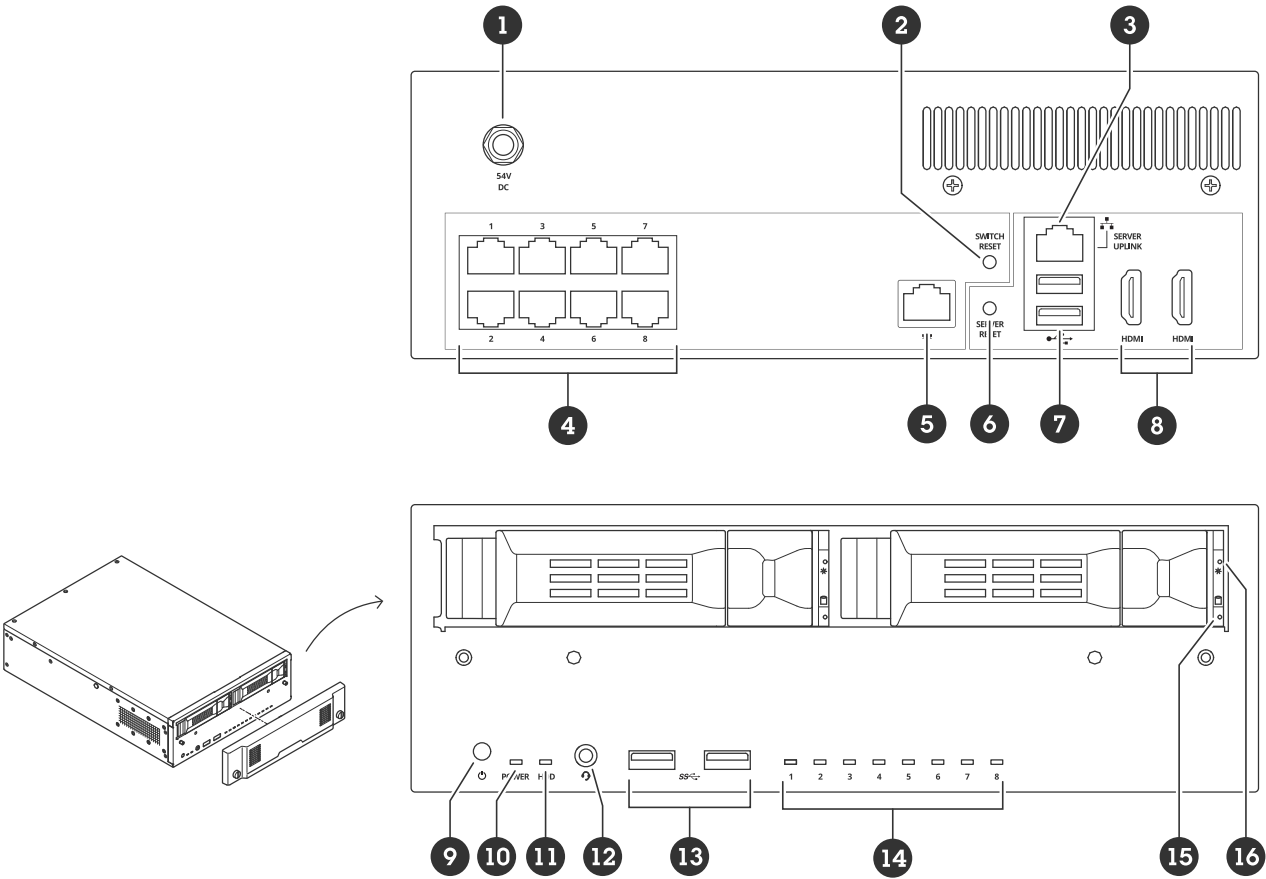
Creare report dello switch

Nella pagina di registro, fare clic su **Export (Esporta)** per creare un file di testo con le informazioni sullo switch, comprese le voci di registro della pagina di registro.

Dati tecnici

Panoramica dei prodotti

Anteriore e posteriore



- 1 Connettore di alimentazione
- 2 Pulsante di ripristino dello switch
- 3 1 porta Ethernet GbE – Uplink del server
- 4 1 porta Ethernet PoE GbE
- 5 1 porta Ethernet GbE – Switch uplink (RJ45)
- 6 Pulsante di ripristino del server
- 7 Porte USB 2.0
- 8 Porte HDMI
- 9 Tasto di accensione
- 10 LED di alimentazione
- 11 LED attività disco rigido
- 12 Jack audio universale
- 13 Porte USB 3.2
- 14 LED stato delle porte Ethernet PoE
- 15 LED attività disco rigido
- 16 LED di stato del disco rigido

Indicatori LED

LED anteriori

Tasto di accensione	LED di alimentazione	Significato
Non premuto	Off	Il PC e lo switch sono spenti

	Giallo	Il PC è acceso e lo switch è spento
	Lampeggia in giallo	Il PC è acceso e lo switch esegue il processo di avvio
	Verde	Il PC è acceso e lo switch ha concluso il processo di avvio.
Premuto	Fino a 0 secondi	Attiva sia lo switch che il PC se sono spenti.
	Finché non lampeggia con colore giallo (3 secondi)	Lo switch avvia lo spegnimento graduale
	Finché non lampeggia con colore rosso (6 secondi)	Il PC e lo switch avviano lo spegnimento graduale
	Finché non diventa rosso fisso (9 secondi)	Il PC avvia lo spegnimento non graduale, lo switch avvia lo spegnimento graduale

Indicatore LED	Colore	Significato
Disco rigido (HDD)	Lampeggia in verde	Attività del disco rigido
	Rosso	Possibile guasto del disco rigido
Stato porta Ethernet PoE	Verde	Stato del collegamento
	Giallo	Dispositivo alimentato, nessuno stato di collegamento
	Rosso	Potenza PoE superata
Stato del disco rigido	Verde	Disco rigido presente
	Rosso	Possibile guasto del disco rigido

LED posteriori

Velocità e attività della rete	Colore	Significato
LED destro	Giallo	10/100 Mbit/s
	Verde	1000 Mbit/s
LED sinistro	Verde	Connessione PoE OK
	Rosso	Potenza PoE superata

Risoluzione dei problemi

Reimpostare il server

È possibile utilizzare il pulsante di reimpostazione del server per reimpostare il server. Ci vorrà più di un'ora per reimpostare il server.

1. Spegnere il dispositivo.
2. Tenere premuto il pulsante di ripristino del server per circa 5 secondi. Windows® RE sarà avviato.
3. Selezionare **Troubleshoot (Risoluzione dei problemi)**.
4. Selezionare **Reset your PC (Reimposta PC)**.
5. Selezionare **Keep my files (Conserva i miei file)** o **Remove everything (Rimuovi tutto)**. Se si seleziona **Keep my files (Conserva i miei file)**, è necessario fornire le credenziali di amministratore.
6. Seguire le istruzioni visualizzate sullo schermo.
7. Il server si riavvia e comincia la procedura per ripristinare le impostazioni predefinite di fabbrica di Windows®.



Ripristinare le impostazioni predefinite di fabbrica del server

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 di problemi per AXIS Camera Station Pro

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

Bisogno di assistenza?

Link utili

- *Manuale per l'utente di AXIS Camera Station Pro*
- *Accedi ad AXIS Secure Remote Access*
- *Accedere ad AXIS Secure Remote Access v2*
- *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.

T10199908_it

2026-07 (M4.4)

© 2024 – 2026 Axis Communications AB