# AXIS Camera Station Pro

## Manuale dell'utente

# Informazioni su

AXIS Camera Station Pro è una soluzione di gestione video per il monitoraggio, la registrazione e la gestione dei flussi video provenienti dalle telecamere di rete Axis. Supporta il controllo degli accessi, la gestione multi-sito, l'integrazione con AXIS Audio Manager e l'integrazione di sistemi di terze parti.

È compatibile con tutte le versioni di AXIS OS sottoposte a manutenzione nei percorsi active, Long-Term Support (LTS) e Product Specific Support (PSS)*. Per ulteriori informazioni, consultare le note di rilascio di AXIS Camera Station Pro o il *portale AXIS OS*. Per verificare quali prodotti funzionano con AXIS Camera Station Pro, vedere *Compatible products* (Prodotti compatibili).

*Il nostro obiettivo è garantire la compatibilità con le versioni precedenti del sistema operativo AXIS OS, ove commercialmente fattibile.

## Opzioni di accesso

**server AXIS Camera Station Pro –** gestisce tutte le comunicazioni con le telecamere, i video encoder e i dispositivi ausiliari nel proprio sistema. Per informazioni sui requisiti di sistema e sulla pianificazione della capacità, consultare *Linee guida hardware* nella guida *AXIS Camera Station Pro – Installazione e migrazione*.

**AXIS Camera Station Pro client –** fornisce accesso alle registrazioni, ai video dal vivo, ai registri e alla configurazione. È possibile l'installazione su qualsiasi computer, consentendo la visualizzazione e il controllo remoto da Internet o dalla rete aziendale.

**Client Web per AXIS Camera Station –** mette a disposizione l'accesso a registrazioni e video in diretta di AXIS Camera Station Pro nel browser Web. Vedere *Web client for AXIS Camera Station user manual (manuale per l'utente del client Web per AXIS Camera Station)* per ulteriori informazioni.

**App per dispositivi mobili AXIS Camera Station Pro –** fornisce accesso alle registrazioni, ai video dal vivo su più sistemi. L'app si può installare su dispositivi Android e iOS e abilita la visualizzazione remota da altre posizioni.

## Opzioni di download

Andare alla *pagina di download di AXIS Camera Station Pro* per scaricare, aggiornare o effettuare una prova gratuita per 90 giorni.

- **Free, fully featured 90-day trial (Prova gratuita di 90 giorni con tutte le funzionalità):** provare AXIS Camera Station Pro gratuitamente per 90 giorni. Nessuna licenza richiesta.
- **Aggiorna solo il client – Offline:** aggiorna il client, ovvero la parte di AXIS Camera Station Pro con cui si interagisce direttamente. Utilizzare questa opzione se si deve aggiornare solo il client, non il server.
- **Update your client and server – Offline (Aggiorna il client e il server – Offline):** un pacchetto di aggiornamento compresso sia per il client che per il server. Una volta scaricato il file .ZIP, decomprimerlo per accedere ai file .msi e .cab, quindi eseguire il file .msi per avviare l'aggiornamento.
- **Update your client and server – Online (Aggiorna il client e il server – Online):** scarica, decomprime e effettua l'installazione automatica dell'aggiornamento. Eseguire il file .exe e seguire le istruzioni sullo schermo. Controllare che il computer rimanga connesso a internet per tutta la durata dell'installazione.
- **Mobile app for iOS (App mobile per iOS:** l'app mobile AXIS Camera Station Pro per iPhone e iPad. Disponibile sull'App Store.
- **Mobile app for Android (App mobile per Android):** l'app mobile AXIS Camera Station Pro per smartphone e tablet Android. Disponibile su Google Play.

## Video tutorial

Per ulteriori esempi approfonditi in merito all'uso del sistema, vedere i *tutorial video di AXIS Camera Station Pro*.

## Caratteristiche del sistema

Per ulteriori informazioni sulle funzionalità di sistema, consultare la *Guida alle funzionalità AXIS Camera Station Pro*.

## Novità?

Per le nuove funzionalità in ogni rilascio di AXIS Camera Station Pro, andare a *Novità di AXIS Camera Station Pro*.

## Collegamenti utili per un amministratore


- *Connessione a un server, on page 9*
- *Configurazione dei dispositivi, on page 47*
- *Configurazione dell'archiviazione, on page 75*
- *Configurazione di registrazioni ed eventi, on page 80*
- *Configura servizi connessi, on page 123*
- *Configurare server, on page 126*
- *Configura sicurezza, on page 136*


### Ulteriori manuali

- *Client Web per AXIS Camera Station*
- *Guida di AXIS Camera Station Pro Integrator:*
- *App per dispositivi mobili AXIS Camera Station*
- *Video tutorial di AXIS Camera Station Pro*
- *Guida alla risoluzione di problemi di AXIS Camera Station Pro*
- *Guida alla protezione del sistema AXIS Camera Station Pro*

## Collegamenti utili per un operatore


- *Connessione a un server, on page 9*
- *Configurazione client, on page 118*
- *Visualizzazione in diretta, on page 13*
- *Riproduzione delle registrazioni, on page 26*
- *Esportazione delle registrazioni, on page 29*

# Avvio rapido

Utilizzare questa guida per rendere operativo il proprio sistema.

Prima di iniziare:

- Configura la rete per la propria installazione. Vedere *Configurazione di rete*.
- Se necessario, configurare le porte del server. Vedere *Configurazione della porta del server*.
- Assicurarsi che il proprio sistema sia sicuro. Vedere *Considerazioni sulla protezione*.

Per amministratori:

1. *Avviare il video management system*
2. *Aggiungi dispositivi*
3. *Configura metodo di registrazione, on page 7*

Per gli operatori:

1. *Visualizzazione del video in diretta, on page 7*
2. *Visualizzazioni registrate, on page 7*
3. *Esportazione delle registrazioni, on page 7*
4. *Riproduzione e verifica delle registrazioni in AXIS File Player., on page 7*

## 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.

Quando il client si apre, chiede di dotare il sistema di una licenza. Fare clic su **License now (Conferire licenza ora)** per andare alla pagina **Manage licences (Gestisci licenze)**, che permette la registrazione del server con un'organizzazione. Per ulteriori informazioni, vedere *Gestire servizi connessi, on page 123* e *Gestisci le licenze, on page 135*.
Si deve eseguire la registrazione e connessione del sistema a un'organizzazione per eseguire l'accesso ai servizi connessi, come il client Web VMS, il monitoraggio dell'integrità del sistema e l'ottenimento di licenza online.

È possibile collegarsi a più server AXIS Camera Station Pro in vari modi. Vedere *Connessione a un server*.

## Aggiungi dispositivi

La prima volta che si avvia AXIS Camera Station Pro, si apre la pagina **Add devices (Aggiungi dispositivi)**, che esegue una ricerca nella rete per individuare i dispositivi da aggiungere. Vedere *Aggiungi dispositivi*.

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. Fare clic su **Close (Chiudi)** per saltare la configurazione e proseguire in un secondo momento. Per proseguire con la configurazione a questo punto:
   3.1. Scegliere **Quick configuration** (Configurazione rapida) oppure **Site Designer configuration** (Configurazione Site designer). Per ulteriori informazioni, vedere *Importazione di progetti AXIS Site Designer, on page 51*.
   3.2. Selezionare **Add image overlay for date, time, and text (Aggiungi sovrapposizione di immagine 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 **Retention time (Tempo di archiviazione)** e **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.

Per ulteriori informazioni, vedere *Visualizzazione in diretta, on page 13*.

## Visualizzazioni registrate

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

Per ulteriori informazioni, vedere *Registrazioni, on page 26*.

## 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)**

Per ulteriori informazioni, vedere *Esportazione delle registrazioni, on page 29*.

## 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 dal video firmato. Un video firmato consente di risalire alla telecamera da

cui proviene la registrazione, in modo da poter verificare che non sia stata sottoposta a 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 Pro 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 un firewall separa il client e il server, configurarlo per garantire che la porta HTTP, la porta TCP e la porta di streaming specificate in AXIS Camera Station Pro Service Control possano passare attraverso di esso. Rivolgersi al proprio amministratore della rete per ricevere assistenza.

Per ulteriori informazioni, vedere *Elenco porta per AXIS Camera Station Pro, on page 216*.

## Configurazione della porta del server

Il server AXIS Camera Station Pro utilizza le porte 29202 (TCP) e 29204 (HTTPS) per la comunicazione tra server e client. Se necessario, le porte possono essere cambiate in AXIS Camera Station Pro Service Control.

Nota

Modifica le porte solo se s'intende utilizzare AXIS Camera Station Pro senza Axis Secure Remote Access v2 né altri servizi cloud di Axis

Per ulteriori informazioni vedere *Impostazioni del server generali* oppure *FAQ (Domande frequenti)*.

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

## Connessione a un server

Il client AXIS Camera Station Pro 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 9*.

**Axis Secure Remote Access v2 –** Vedere *Accedere ad AXIS Secure Remote Access v2, on page 9*.

Nota

- La prima volta che ci si connette a un server, il client verifica l'ID del certificato del server. Per assicurarsi di connettersi al server corretto, confrontare l'ID del certificato con quello visualizzato in AXIS Camera Station Pro Service Control. Per ulteriori informazioni, vedere *Impostazioni del server generali, on page 216*.
- Il client e il server devono avere la stessa versione. Se si verifica una discrepanza tra le versioni durante la connessione a un sistema locale o a un sistema con mappatura delle porte, il client può scaricare la versione corretta, compatibile con quella del server, e passare quindi a tale versione.
- Affinché un cliente possa connettersi a più server, è necessario che ogni server disponga della stessa versione. Per impostazione predefinita, il collegamento client utilizza l'ultima versione.

| | |
|---|---|
| **Elenco dei server** | Per connettersi ai server da un elenco di server, selezionarne uno dal menu a discesa **Server list (Elenco server)**. Fare clic su per creare o modificare gli elenchi di server. Vedere *Elenchi dei server*. |
| **Importa lista dei server** | Per importare un file contenente un elenco di server esportati da AXIS Camera Station Pro, fare clic su **Import server list (Importa lista dei server)** e andare a un file .msl. Vedere *Elenchi dei server*. |
| **Elimina password salvate** | Per eliminare i nomi utente e le password per tutti i server collegati, fare clic su **Delete saved passwords (Elimina password salvate)**. |

### 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 presente nell'elenco, 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 29202, 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.

### Accedere ad AXIS Secure Remote Access v2

1. Fare clic sul collegamento **Sign in to AXIS Secure Remote Access v2 (Accedi ad AXIS Secure Remote Access v2)**.

2. Immettere le credenziali dell'account My Axis.
3. Fare clic su **Accedi**.
4. Selezionare un'organizzazione e fare clic su **OK**.
5. Selezionare il server a cui si desidera accedere.
6. Accedere con le credenziali del server.

Nota

Le credenziali del server sono diverse dalle credenziali dell'account My Axis.

La barra di stato nella parte inferiore del client AXIS Camera Station Pro mostra l'utilizzo di Axis Secure Remote Access v2. **Data used this month (Dati utilizzati questo mese)** mostra la quantità totale di dati rinviati utilizzati dall'organizzazione nel corso del mese. Il contatore si azzera il primo giorno di ogni mese a mezzanotte.

### Axis Secure Remote Access v2 su dispositivi mobili

Per accedere al server utilizzando Axis Secure Remote Access v2 su un dispositivo mobile (iOS e Android):

1. Andare a *axis.com/products/axis-camera-station/overview* e scaricare l'app AXIS Camera Station Mobile.
2. Installare e aprire l'app per dispositivi mobili.
3. Accedere ad Axis Secure Remote Access v2 con le credenziali del proprio account My Axis.
4. Selezionare il server a cui si desidera accedere.
5. Accedere con le credenziali del server.

Nota

- Le credenziali del server sono diverse dalle credenziali dell'account My Axis.
- Prima di poter accedere al proprio account My Axis, è necessario ricevere l'invito a iscriversi all'organizzazione come utente.

Nell'app per dispositivi mobili viene visualizzata la quantità totale di dati rinviati utilizzati dall'organizzazione nel corso del mese. Per maggiori informazioni, leggere il *Manuale per l'utente dell'app AXIS Camera Station Mobile*.

## Impostazioni proxy client

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

## AXIS Camera Station Pro client

Schede

| | |
|---|---|
| **Visualizzazione in diretta** | Visualizzare video in diretta dalle telecamere collegate. Vedere *Visualizzazione in diretta*. |
| **Registrazioni** | Trovare, riprodurre ed esportare le registrazioni. Vedere *Registrazioni*. |
| **Ricerca intelligente 1** | Individuare gli eventi in un video registrato usando una ricerca di movimento. Vedere *Ricerca intelligente 1*. |
| **Ricerca dati** | Cercare i dati di un sistema o una sorgente esterna e monitorare cosa è accaduto al momento di ciascun evento. Vedere *Ricerca dati, on page 44*. |
| **Configurazione** | Gestione dei dispositivi connessi e configurazione delle impostazioni dei client e dei server. Vedere *Configurazione*. |
| **Tasti di scelta rapida** | Visualizzare ed effettuare la configurazione dei tasti di scelta rapida. Vedere *Tasti di scelta rapida*. |
| **Registri** | registri di allarmi, di eventi e di controllo. Vedere *Registri*. |
| **Gestione degli accessi** | Configurare e gestire i titolari tessera, i gruppi, le porte, le zone e le regole di accesso al sistema. Vedere *Gestione degli accessi, on page 186*. |
| **Ricerca intelligente 2** | Usare i filtri avanzati per individuare veicoli e persone sulla base delle caratteristiche. Vedere *Ricerca intelligente 2, on page 38*. |
| **Monitoraggio dell'integrità del sistema** | Eseguire il monitoraggio dei dati di integrità da uno o più sistemi AXIS Camera Station Pro. Vedere *Monitoraggio dell'integrità del sistema* BETA*, on page 198*. |
| **Avvisi della visualizzazione in diretta** | Passa automaticamente alle schede di avviso della visualizzazione in diretta della telecamera o della vista quando viene attivata l'azione della visualizzazione in diretta. Vedere *Creazione di azioni della visualizzazione in diretta*. |
| **Avvisi della registrazione** | Nella scheda Allarmi o Registri, selezionare un allarme e fare clic su **Go to recordings (Vai alle registrazioni)** per aprire la scheda degli avvisi Registrazione. Vedere *Allarmi* e *Registri*. |

Menu principale

| | |
|---|---|
| | Aprire il menu principale. |
| Server | Collegarsi a un nuovo server AXIS Camera Station Pro e visualizzare gli elenchi dei server e lo stato della connessione per tutti i server. Vedere *Configurare server*. |

| | |
|---|---|
| **Azioni** | Avviare o interrompere una registrazione manualmente e modificare lo stato delle porte I/O. Vedere *Registrazione manuale* e *Monitoraggio porte I/O*. |
| **Aiuto** | Accedere alle opzioni di assistenza e supporto. Andare a **Help (Guida)** > **About (Informazioni)** per vedere quale versione di client AXIS Camera Station Pro è in uso. |
| **Esci** | Effettuare la disconnessione e disconnettersi dal server. |
| **Esci** | Uscire e chiudere il client AXIS Camera Station Pro. |

### Barra del titolo

| | |
|---|---|
| ? o F1 | Aprire la guida. |
| | Attivare modalità a schermo intero. |
| o ESC | Chiudere la modalità a schermo intero. |

### Barra di stato

- L'icona di avviso indica una discrepanza temporale tra il client e il server. Assicurarsi che i loro orari siano sincronizzati per evitare problemi con la cronologia/ordine cronologico.
- Lo stato della connessione al server mostra il numero di server connessi. Vedere *Stato connessione*.
- Lo stato delle licenze mostra il numero di dispositivi senza licenza. Vedere *Gestisci le licenze*.
- L'utilizzo di Secure Remote Access v2 mostra la quantità di dati consumati nel mese.
- **AXIS Camera Station Pro update available (aggiornamento disponibile)** indica che è disponibile una nuova versione. Visibile solo se è stato effettuato l'accesso come amministratore. Vedere *Aggiorna AXIS Camera Station Pro, on page 129*.

### Allarmi e attività

- Le schede Allarmi e Attività mostrano gli eventi attivati e gli allarmi di sistema. Vedere *Allarmi* e *Attività*.

# Visualizzazione in diretta

La visualizzazione in diretta mostra video in diretta dalle telecamere collegate. Quando ci si connette a più server AXIS Camera Station Pro mostra tutte le viste e le telecamere raggruppate in base al nome del server.

Le viste offrono l'accesso a tutti i dispositivi e le telecamere aggiunti ad AXIS Camera Station Pro. Una vista può essere formata da una o più telecamere, una sequenza di elementi, una mappa o una pagina Web. La visualizzazione in diretta aggiorna in automatico le viste quando si aggiungono o rimuovono dispositivi dal sistema.

Grazie all'integrazione di AXIS Audio Manager Pro, è possibile impostare e aggiungere zone audio con interfacce di paging nella visualizzazione in diretta. Per ulteriori informazioni, consultare *Utilizzare le interfacce di paging nella suddivisione dell'immagine, on page 21*

Tutti gli utenti sono in grado di accedere alle viste. Per ulteriori informazioni sui diritti di accesso dell'utente, vedere *Autorizzazioni utente, on page 136*.

Per effettuare la configurazione della visualizzazione in diretta, vedere *Impostazioni client*.

## Monitor multipli

Per l'apertura di una vista su un altro schermo:

1. Aprire una scheda **Live view (Visualizzazione in diretta)**.
2. Selezionare una o molteplici telecamere, viste o sequenze.
3. Trascinare la selezione sull'altra schermata.

Per aprire una vista su un monitor connesso ad un video decoder Axis:

1. Aprire una scheda **Live view (Visualizzazione in diretta)**.
2. Selezionare una o molteplici telecamere, viste o sequenze.
3. Fare clic con il pulsante destro del mouse e selezionare **Show on AXIS T8705 (Mostra su AXIS T8705)** oppure **Show on AXIS D1110 (Mostra su AXIS D1110)**, in base al decoder video in uso.

Nota

- AXIS T8705 supporta unicamente telecamere Axis.
- AXIS D1110 supporta un massimo di 16 flussi in una suddivisione dell'immagine.

## Gestisci viste nella visualizzazione in diretta

| | |
|---|---|
| + | Aggiungere una nuova suddivisione dell'immagine, una sequenza, una vista della telecamera, una mappa, una pagina Web o una cartella. |
| | Modificare una vista o il nome di una telecamera. Per modificare le impostazioni della telecamera, vedere *Modifica delle impostazioni della telecamera* |
| | Rimuovere una vista. Servono le autorizzazioni per la modifica della vista e di tutte le viste secondarie per rimuoverla. Per rimuovere le telecamere da AXIS Camera Station Pro, consultare *Telecamere, on page 54*. |
| | In qualità di amministratore, è possibile applicare il blocco alla vista per impedire agli operatori di spostarla o effettuare modifiche ad essa. |

## Gestione dell'immagine nella visualizzazione in diretta

| | |
|---|---|
| **Accedi a** | Per andare alla vista della telecamera, fare clic con il pulsante destro del mouse su un'immagine in una suddivisione dell'immagine e selezionare **Navigate (Naviga)**. |
| **Scatta istantanea** | Per acquisire un'istantanea, fare clic su un'immagine e selezionare **Take snapshot (Scatta istantanea)**. Il sistema salva l'istantanea nella cartella delle istantanee specificata in **Configuration > Client > Settings** (Configurazione, Client, Impostazioni).<br>Nota<br>AXIS Camera Station Pro in genere utilizza il flusso video quando si scattano le istantanee, il che significa che si ottiene un'istantanea con la stessa risoluzione del flusso video. Tuttavia, per le telecamere panoramiche e fisheye, che richiedono lo stitching o la distorsione, l'istantanea viene scattata sul lato client, direttamente dallo schermo. Questo può dare luogo a immagini di risoluzione inferiore, soprattutto in viste con più telecamere, in cui ogni immagine appare più piccola sullo schermo. |
| **Add snapshot to export (Aggiungi istantanea da esportare)** | Per aggiungere un'istantanea all'elenco di esportazione fare clic con il pulsante destro del mouse su un'immagine e selezionare **Add snapshot to export (Aggiungi istantanea da esportare)**. |
| **Mostra su** | Per eseguire l'apertura di una vista su un altro schermo, fare clic con il pulsante destro del mouse sull'immagine e selezionare **Show on (Mostra su)**. |
| **Usa PTZ meccanico** | Disponibile per telecamere PTZ e per telecamere in cui è abilitato il PTZ digitale nelle pagine Web della telecamera. Per utilizzare il PTZ meccanico, fare clic con il pulsante destro del mouse sull'immagine e selezionare **Usa PTZ meccanico**. Utilizzare il mouse per eseguire la panoramica, l'inclinazione e lo zoom. |
| **Zoom** | utilizzare la rotellina del mouse per ingrandire e ridurre. In alternativa, premere CTRL + [+] per lo zoom avanti e CTRL + [-] per lo zoom indietro. |
| **Zoom dell'area** | Per l'ingrandimento di un'area, disegnare un rettangolo nell'area che si vuole ingrandire. Per eseguire lo zoom indietro, utilizzare la rotellina del mouse. Per ingrandire un'area in prossimità del centro dell'immagine, utilizzare il pulsante destro del mouse e trascinare il puntatore per disegnare un rettangolo. |
| **Panoramica e inclinazione** | Fare clic sull'immagine dove si vuole puntare la telecamera. Per eseguire in modo continuo la rotazione e l'inclinazione, spostare il cursore al centro dell'immagine per visualizzare la freccia di navigazione. Fare clic e tenere premuto per eseguire una rotazione in direzione della freccia. Per eseguire la rotazione e l'inclinazione a maggiore velocità, fare |

| | |
|---|---|
| | clic e tenere premuto per allungare la freccia di navigazione. |
| **Imposta messa a fuoco** | Per regolare la messa a fuoco per un dispositivo Axis, fare clic con il pulsante destro del mouse sull'immagine e selezionare **Set focus** (Imposta messa a fuoco). Utilizzare le barre **Near** (Vicino) e **Far** (Lontano) per regolare manualmente la messa a fuoco, oppure fare clic su **(AF)** per mettere a fuoco automaticamente.<br><br>Per regolare la messa a fuoco per un dispositivo ONVIF, fare clic con il pulsante destro del mouse sull'immagine e selezionare **Set focus** (Imposta messa a fuoco). Selezionare una **Focus mode** (modalità di messa a fuoco). La finestra di dialogo si aggiorna a seconda della modalità scelta:<br><br>• **Absolute (Assoluta)**: Impostare la messa a fuoco su una posizione specifica inserendo un valore e facendo clic su **Apply (Applica)**.<br>• **Relative (Relativa)**: Regolazione della messa a fuoco in modo incrrementale. Utilizzare **Near** (Vicino) per gli oggetti vicini alla telecamera e **Far** (Lontano) per gli oggetti più lontani.<br>• **Continuous (Continua)**: Spostare la messa a fuoco utilizzando le opzioni **Nearer (Più vicino)** oppure **Further (Più lontano)** e fare clic su **Stop (Arresta)** al termine.<br>• Per mettere a fuoco in modo automatico, fare clic su **AF**. |
| **Zona di richiamo messa a fuoco** | Per aggiungere o rimuovere una zona di richiamo messa a fuoco, fare clic con il pulsante destro del mouse sull'immagine e selezionare **Focus recall zone (Zona di richiamo messa a fuoco)**. |
| **Tracking automatico acceso/spento** | Per attivare o disattivare il tracking automatico per una telecamera PTZ Axis con AXIS PTZ Autotracking configurato, fare clic sull'immagine e selezionare **Autotracking on/off (Tracking automatico on/off)**. |
| **Preset** | Per andare alla posizione preset, fare clic con il pulsante destro del mouse sull'immagine, selezionare **Presets (Preset)**. Per informazioni sulla creazione di preset, vedere *Configurazione PTZ*. |
| **Aggiungi preset** | Per aggiungere un preset, trascinare la vista dell'immagine nella posizione desiderata, fare clic con il pulsante destro del mouse su **Presets > Add preset (Preset, Aggiungi preset)**. |

| | |
|---|---|
| **Movimento PTZ assoluto** | Disponibile per dispositivi ONVIF che supportano il posizionamento PTZ assoluto. Utilizzare questa funzione per spostare la telecamera su coordinate precise ripetibili.<br>Per utilizzare la funzione PTZ assoluto, fare clic con il pulsante destro del mouse sulla telecamera nella visualizzazione in diretta e selezionare **Absolute PTZ Move (Movimento PTZ assoluto)**. Selezionare un sistema di coordinate: **Generic (Generico)** per coordinate standard o **Spherical (Sferico)** per coordinate basate sui gradi. Inserire i valori di posizione per panoramica, inclinazione e zoom, impostare la velocità di movimento e fare clic su **OK** or **Send** (OK, Invia). |
| **Profilo di streaming** | Per impostare il profilo di streaming, fare clic con il pulsante destro del mouse su un'immagine e selezionare **Stream profile (Profilo di streaming)**. Vedere *Profili di flusso*. |

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

*Aggiungi preset digitali*

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

*Comandi PTZ*

Nota

In qualità di amministratore è possibile disattivare il PTZ meccanico per gli utenti. Vedere *Autorizzazioni utente*.

## Registrazione e riproduzione istantanea nella visualizzazione in diretta

| | |
|---|---|
| | Per andare alla scheda Registrazioni, selezionare una telecamera o una suddivisione dell'immagine e fare clic su . |
| | Indica una registrazione in corso nella visualizzazione in diretta. |
| | Indica che è stato rilevato del movimento. |

| | |
|---|---|
| | Per riprodurre una registrazione in corso, passare il cursore sull'immagine e fare clic su **Instant replay (Riproduzione istantanea)**. Viene aperta la scheda Registrazioni e riproduce gli ultimi 5 secondi della registrazione. |
| **REC** | Per registrare manualmente dalla visualizzazione in diretta, passare il cursore sull'immagine e fare clic su **REC**. Il pulsante diventa giallo per mostrare che la registrazione è in corso. Fare di nuovo clic su **REC** per arrestare la registrazione. |

Per configurare le impostazioni della registrazione manuale ad esempio risoluzione, compressione e velocità in fotogrammi, vedere *Metodo di registrazione*. Per ulteriori informazioni sulla registrazione e sulla riproduzione, vedere *Riproduzione delle registrazioni*.

Nota

In qualità di amministratore, è possibile disattivare la funzione di registrazione manuale per gli utenti. Vedere *Autorizzazioni utente*.

## Audio in visualizzazione in diretta

L'audio è disponibile se la telecamera è dotata di funzionalità audio e se l'audio è stato abilitato nel profilo utilizzato per la visualizzazione in diretta.

Andare a **Configuration > Devices > Stream profiles (Configurazione > Dispositivi > Profili di streaming)** e configura l'audio per la telecamera. Vedere *Profili di flusso, on page 55*.

| | |
|---|---|
| **Volume** | Per modificare il volume in una vista, passare il mouse sull'immagine, successivamente sul pulsante dell'altoparlante e usare il cursore per cambiare il volume. Per disattivare o attivare l'audio, fare clic su . |
| **Ascolta solo questa vista** | Per disattivare le altre viste e ascoltare solo questa vista, passare il cursore sull'immagine e fare clic su . |
| **Parla attraverso l'altoparlante** | Per parlare attraverso l'altoparlante configurato in modalità full-duplex, passare il cursore del mouse sull'immagine e fare clic su . |
| **Premi per parlare** | Per parlare attraverso l'altoparlante configurato in modalità simplex e half-duplex, passare il mouse sull'immagine, fare clic e tenere premuto . Per mostrare il pulsante **Push-to-talk (Premi per parlare)** per tutte le modalità duplex, attivare **Use push-to-talk for all duplex modes (Utilizzare Premi per parlare per tutte le modalità duplex)** in **Configuration > Client > Streaming > Audio (Configurazione > Client > Streaming > Audio)**. Vedere *Streaming, on page 121*. |

Nota

Come amministratore si può disattivare l'audio per gli utenti. Vedere *Autorizzazioni utente*.

## Comandi su schermo nella visualizzazione in diretta

Nota

I comandi su schermo richiedono il firmware 7.40 o versione successiva.

| | |
|---|---|
| | Per accedere alle funzioni delle telecamere disponibili nella visualizzazione in diretta, fare clic su . |

## Suddivisione dell'immagine

Una suddivisione dell'immagine mostra più immagini nella stessa finestra. È possibile utilizzare viste delle telecamere, pagine, mappe e altre viste suddivise in una vista suddivisa.

Nota

Quando ci si connette a più server AXIS Camera Station Pro, è possibile aggiungere alla propria vista della mappa qualsiasi vista, telecamera, dispositivo o zona audio di altri server nella suddivisione immagine.

Per aggiungere una vista suddivisa:

1. Nella scheda **Live view** (visualizzazione in diretta), fare clic su .
2. Selezionare **Nuova vista suddivisa**.
3. inserire un nome per l'immagine suddivisa;
4. Seleziona un layout dal menu a discesa **Template (Modello)**.
5. Trascinare e rilasciare le telecamere o le viste dal pannello laterale sulla griglia, oppure fare doppio clic per aggiungerle al primo slot disponibile.
6. Fare clic su **Save view (Salva visualizzazione)**.

Per effettuare una modifica su una telecamera o una vista nella griglia, selezionarla. Nella sezione **Select item to configure (Seleziona un elemento per la configurazione)** è possibile:

- Fare clic su **Remove (Rimuovi)** per eliminarlo dalla griglia.
- Selezionare una **Priority (Priorità)** dal menu a discesa.

Per aggiungere un hotspot:

- Selezionare un fotogramma e fare clic su **Set hotspot (Imposta hotspot)** nella sezione **Hotspot**.

Per visualizzare automaticamente i flussi video attivati nell'hotspot:

- Selezionare **Dynamic hotspot content (Contenuto dinamico hotspot)** e effettuare la configurazione delle impostazioni. Consultare *Hotspot dinamico, on page 18* per ulteriori informazioni.

Per impostare il profilo di streaming di una telecamera:

- Fare clic con il tasto destro del mouse nella vista a griglia e selezionare **Stream profile (Profilo di streaming)**. Vedere *Profili di flusso, on page 55*.

### Hotspot dinamico

Utilizzare gli hotspot dinamici per monitorare più eventi contemporaneamente. Quando vengono attivate le regole di azione, i flussi video vengono visualizzati automaticamente nell'hotspot. Ad esempio, se viene effettuato il rilevamento movimento in tre diversi ingressi, le viste delle tre telecamere vengono visualizzate contemporaneamente.

L'hotspot adatta la propria griglia in base al numero di viste attive. Ogni vista mostra un timer per il conto alla rovescia e scompare al termine del conto alla rovescia.

Nota

Per le telecamere in cui l'attivazione avviene tramite azioni di visualizzazione in diretta con stato, il conto alla rovescia inizia quando l'azione non è più attiva. Per le altre telecamere e le altre viste, il conto alla rovescia inizia immediatamente.

### Creare un hotspot dinamico

Per aggiungere una nuova vista con un hotspot dinamico:

1. Nella scheda **Live view** (visualizzazione in diretta), fare clic su +.
2. Fare clic su **Add hotspot (Aggiungi hotspot)**.
3. Selezionare **Dynamic hotspot content (Contenuto hotspot dinamico)**.
4. Configurare le impostazioni:
   - **Minimum split view cells (Celle minime di suddivisione dell'immagine):** Numero minimo di celle nella griglia, anche quando non sono attive viste. Intervallo: da 1 a 144.
   - **Maximum split view cells (Celle massime di suddivisione dell'immagine):** Il numero massimo di celle a cui la griglia può espandersi man mano che vengono attivate ulteriori viste. Intervallo: da 1 a 144.
   - **Countdown in seconds (Countdown in secondi):** Per quanto tempo rimane visibile ciascuna vista trigger. Impostare il valore su 0 per mantenere visibili le viste fino alla loro rimozione manuale. Intervallo: da 0 a 999.
   - **Seconds remaining before countdown appears in view (Secondi rimanenti prima che il conto alla rovescia compaia nella vista)**: Determina quando il timer per il conto alla rovescia appare sullo schermo. Impostare su 0 per visualizzarlo sempre. Si noti che la visualizzazione del timer comporta l'utilizzo di risorse di sistema. Intervallo: da 0 a 999.
   - **Mute audio on incoming views (Silenzia l'audio sulle viste in arrivo):** I nuovi flussi vengono silenziati. Puoi riattivare l'audio singolarmente.
   - **Allow adding views with click on view (Consenti di aggiungere viste facendo clic sulla vista)**: Aggiungere manualmente le visualizzazioni all'hotspot facendo clic su di esse, insieme alle visualizzazioni trigger.
   - **Allow adding views with hotkey (Consenti di aggiungere viste con il tasto di scelta rapida):** Utilizzare i tasti di scelta rapida per aggiungere viste definite a questo hotspot, insieme alle viste attivate.
5. Fare clic su **Save view (Salva visualizzazione)**.

Per aggiungere un hotspot dinamico a una vista esistente:

1. Nella scheda **Live view (visualizzazione in diretta)**, fare clic su **Edit view (Modifica vista)**.
2. Fare clic su **Add hotspot (Aggiungi hotspot)**.
3. Selezionare **Dynamic hotspot (Hotspot dinamico)**.
4. Configurare le impostazioni come descritto al punto 4 precedente.
5. Fare clic su **Save view (Salva visualizzazione)**.

Nota

È possibile convertire un hotspot esistente in un hotspot dinamico effettuando la modifica nella scheda **Live view (Visualizzazione in diretta)**.

### Controllo e gestione delle viste

Ogni cella di un hotspot dinamico comprende:

- **Countdown indicator (Indicatore del conto alla rovescia)**: Mostra il tempo rimanente prima che la vista scompaia.
- **Pause button (Pulsante di pausa)**: Mette in pausa il conto alla rovescia per mantenere visibile una schermata più a lungo.
- **Close button (Pulsante chiudi)**: Rimuove immediatamente una vista dall'hotspot.
- **Flash indicator (Indicatore lampeggiante)**: Il limite del conto alla rovescia lampeggia quando una vista viene riattivata.

Questi controlli vengono nascosti quando si espande una cella in vista singola o si passa alla modalità di riproduzione. Fare doppio clic su una cella qualsiasi per ingrandirla a schermo intero. Quando è ingrandita, il conto alla rovescia si interrompe in modo automatico. L'hotspot dinamico continua ad aggiornarsi in background e, quando si torna alla visualizzazione a griglia, si vedranno le viste attive.

Nota

Quando si passa alla modalità di riproduzione, i flussi della telecamera diventano fissi e non vengono più aggiornati. Tornare alla visualizzazione in diretta per riprendere il normale funzionamento.

### Dashboard porta in suddivisione dell'immagine

Se è stata configurata una porta, è possibile assistere i titolari della tessera e monitorare lo stato della porta e del blocco e le transazioni recenti in una suddivisione dell'immagine.

1. Aggiunta di una porta. Vedere *Aggiunta di una porta, on page 150*.
2. Aggiungere il dashboard porta a una suddivisione dell'immagine, vedere *Suddivisione dell'immagine, on page 18*.

| | |
|---|---|
| **Dashboard** | Per visualizzare i dettagli della porta e lo stato di blocco, aprire la scheda **Dashboard (Dashboard)**.<br><br>La scheda Dashboard visualizza le seguenti informazioni:<br><br>• Gli eventi di controllo degli accessi con i dettagli del titolare della tessera e le foto, ad esempio, quando un titolare passa una tessera.<br>• Gli allarmi con le informazioni di attivazione degli allarmi, ad esempio, quando una porta è aperta troppo a lungo.<br>• L'ultima transazione. |
| | Per aggiungere un segnalibro a un evento e renderlo disponibile nella scheda **Transactions (Transazioni)** fare clic su . |
| **Accesso** | Per consentire manualmente l'accesso, fare clic su **Access (Accesso)**. In questo modo si apre la porta come se qualcuno avesse esibito le proprie credenziali. La porta effettua nuovamente il blocco automatico dopo un certo tempo. |
| **Blocco** | Per bloccare manualmente la porta, fare clic su **Lock (Blocca)**. |
| **Sblocca** | Per sbloccare manualmente la porta, fare clic su **Unlock (Sblocca)**. La porta rimane sbloccata fino a quando non viene nuovamente bloccata manualmente. |
| **Chiusura totale** | Per impedire l'accesso alla porta, fare clic su **Lockdown (Arresto)**. |
| **Transazioni** | Per visualizzare le transazioni recenti e salvate, aprire la scheda **Transactions (Transazioni)**. |

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

*Monitoraggio e assistenza nel dashboard delle porte*

### Utilizzare le interfacce di paging nella suddivisione dell'immagine

È possibile utilizzare le interfacce di paging per effettuare annunci in diretta, chiamate o riprodurre file audio da dispositivi audio. Ciò richiede l'integrazione di AXIS Audio Manager Pro. Per ulteriori informazioni, consultare *Configurare AXIS Audio Manager Pro, on page 173*.

Per utilizzare le interfacce di paging:

1. Modificare o aggiungere una nuova suddivisione dell'immagine.
2. Trascinare e rilasciare una o più zone audio sulla griglia per trasformarla in un'interfaccia di paging.

Nota

Le zone audio in AXIS Camera Station Pro sono identiche alle zone impostate sul server AXIS Audio Manager Pro.

3. Selezionare **Speak**, **Call**, o **Play a file** (Parla, Chiama, Riproduci un file):
   - Selezionare **Speak** (Parla) per comunicazioni unidirezionali, come annunci in diretta.
   - Selezionare **Call** (Chiama) per la comunicazione bidirezionale, ad esempio quando si desidera parlare con qualcuno tramite un interfono.
   - Selezionare **Play a file (Riproduci un file)** per riprodurre un file dal server AXIS Audio Pro tramite altoparlante.

## Sequenza

Una sequenza passa da una vista all'altra automaticamente.

Nota

Quando ci si connette a più server AXIS Camera Station Pro, è possibile aggiungere alla propria sequenza qualsiasi vista, telecamera o dispositivo di altri server.

Per aggiungere una sequenza:

1. Nella scheda **Live view** (visualizzazione in diretta), fare clic su +.
2. Selezionare **Nuova sequenza**.
3. inserire un nome per la sequenza;
4. Trascinare e rilasciare una o più viste o telecamere nella vista in sequenza.
5. Ordinare le viste nell'ordine in cui si desidera che appaiano.
6. Fare clic su una vista per effettuare la modifica delle impostazioni.
7. Fare clic su **Save view (Salva visualizzazione)**.

| | |
|---|---|
| **Preimpostazione PTZ** | Per le telecamere dotate di funzionalità PTZ, selezionare il preset PTZ verso cui la telecamera deve spostarsi quando questa vista è attiva. |
| **Tempo di interazione** | Il numero di secondi durante i quali viene visualizzata ciascuna vista prima di passare a quella successiva. È possibile impostare questa opzione singolarmente per ogni vista. |

Nota

- Non è possibile aggiungere una vista sequenza all'interno di un'altra vista sequenza.
- Non è possibile aggiungere direttamente le viste dei componenti da un server remoto. Come soluzione alternativa, aggiungere prima la vista del componente a una singola suddivisione dell'immagine, quindi aggiungere tale suddivisione dell'immagine dal server remoto.
- La riproduzione della cronologia/ordine cronologico potrebbe non funzionare come previsto. La riproduzione mostra tutte le telecamere presenti nella sequenza, ma solo una è attiva alla volta.

### Utilizza la barra di sequenza

Durante la visualizzazione di una sequenza, una barra nella parte inferiore della schermata consente di controllare la riproduzione in modo manuale:

- Utilizzare i tasti **[[>]** e **[<]** per passare alla vista successiva o precedente.
- Utilizza i pulsanti **Hold (Pausa)**oppure **Continue (Continua)** per mettere in pausa e riprendere la sequenza.
- Un conto alla rovescia indica quanti secondi mancano al prossimo cambio automatico.
- Fare clic con il tasto destro sulla sequenza per nascondere la barra.
- Quando la sequenza è aperta nella scheda **Recording (Registrazione)**, viene impostata automaticamente su **Hold (Pausa)** ed è possibile scorrere le immagini solo manualmente utilizzando i pulsanti avanti e indietro.

## Immagine telecamera

Un'immagine videocamera mostra il video dal vivo ripreso da una videocamera. Puoi utilizzare le viste delle telecamere in suddivisioni dell'immagine, sequenze e mappe.

Nota

Quando ci si connette a più server AXIS Camera Station Pro nell'elenco vengono visualizzate tutte le telecamere di tutti i server connessi.

Per aggiungere un'immagine videocamera:

1. Nella scheda Visualizzazione in diretta o Registrazioni, fare clic su +.
2. Selezionare **Nuova vista telecamera**.
3. Selezionare la telecamera dal menu a discesa e fare clic su **OK**.

## Mappa

Una mappa è un'immagine importata dove è possibile posizionare immagini delle telecamere, suddivisioni dell'immagine, zone audio, sequenze, pagine web, altre mappe e porte. La mappa fornisce una panoramica visiva e un modo per trovare e accedere a singoli dispositivi. È possibile creare diverse mappe di grandi dimensioni e disporle su una mappa panoramica per grandi installazioni.

Tutti i pulsanti azione sono disponibili anche nella vista mappa. Vedere *Creazione di trigger dei pulsanti di azione*.

Nota

Quando ci si connette a più server AXIS Camera Station Pro, è possibile aggiungere alla propria vista della mappa qualsiasi vista, telecamera o dispositivo di altri server.

Per aggiungere una mappa:

1. Nella scheda **Live view** (visualizzazione in diretta), fare clic su +.
2. Selezionare **Nuova mappa**.
3. inserire un nome per la mappa;
4. Fare clic su **Choose image (Scegli immagine)** e trovare il file della mappa. Il file non deve superare i 20 MB. Formati supportati: BMP, JPG, PNG, e GIF.
5. Trascinare le viste, le telecamere, gli altri dispositivi e le porte sulla mappa.
6. Fare clic su un'icona sulla mappa per modificarne le impostazioni.
7. Fare clic su **Add label (Aggiungi etichetta)**, immettere un nome dell'etichetta e impostare la dimensione, la rotazione, lo stile e il colore dell'etichetta.
8. Fare clic su **Save view (Salva visualizzazione)**.

Nota

- È possibile modificare alcune impostazioni per più icone ed etichette allo stesso tempo.
- Tutti i dispositivi a cui il proprio account utente non ha accesso vengono rimossi dalla mappa quando si effettua una modifica.
- Non è possibile aggiungere direttamente le viste dei componenti da un server remoto. Come soluzione alternativa, aggiungere prima la vista del componente a una singola suddivisione dell'immagine, quindi aggiungere tale suddivisione dell'immagine dal server remoto alla mappa.

## Impostazioni delle icone

Fare clic su un'icona della mappa per aprirne le impostazioni.

| | |
|---|---|
| | Lo stato fisico della porta quando la porta è configurata con un monitor porta. |
| | Lo stato fisico del blocco quando la porta è configurata senza un monitor porta. |
| | Un triangolo rosso di avviso indica un avviso di manomissione presso una porta, un lettore o un door controller. |
| **Icona** | selezionare l'icona che si desidera utilizzare. Questa opzione è disponibile solo per le telecamere e altri dispositivi. |
| **Dimensioni** | Regolare il dispositivo di scorrimento per modificare la dimensione dell'icona. |
| **Colore** | Fare clic su per modificare il colore dell'icona. |
| **Nome** | Attivare questa opzione per visualizzare il nome dell'icona. Selezionare **Bottom (In basso)** o **Top (In alto)** per modificare la posizione del nome dell'icona. |
| **Area di copertura** | Disponibile per i dispositivi compatibili. Attivare questa opzione per visualizzare l'area di copertura del dispositivo sulla mappa. È possibile modificare **Range (Intervallo)**, **Width (Larghezza)**, **Direction (Direzione)** e colore dell'area di copertura. Attivare |

| | |
|---|---|
| | l'opzione **Flash** per far lampeggiare l'area di copertura quando viene avviata una registrazione in seguito al rilevamento movimento o ad altre regole di azione. Per disattivare globalmente le aree di copertura lampeggianti su tutti i dispositivi, consultare *Impostazioni client, on page 118*. |
| **Freccia di direzione** | Mostra le frecce che indicano la direzione del campo visivo di ciascuna telecamera. È possibile visualizzare le frecce con o senza aree di copertura. |
| **Mostra indicatori di registrazione** | Determina quali indicatori di registrazione sono visibili sull'icona. Attivare **Small indicators (Indicatori picolli)** per visualizzare una versione compatta degli indicatori. Utilizzare i singoli pulsanti di attivazione/disattivazione per mostrare/nascondere gli indicatori relativi a **Recording (Registrazione)**, **Motion detected (Rilevamento movimento)**, **Object detected (Rilevamento oggetti)** e **Action rule active (Regola di azione attiva)**. Queste impostazioni vengono salvate sul server, quindi tutti i client condividono la stessa configurazione. |
| **Etichetta** | Un'etichetta è caratterizzata da testo, dimensioni, rotazione e colore. È anche possibile sottolineare e mettere in corsivo il testo dell'etichetta. |
| **Rimuovi** | Fare clic su per rimuovere l'icona dalla mappa. |

### Navigare sulla mappa

**Ingrandire e spostare**

- È possibile ingrandire e spostare la mappa utilizzando il mouse, la tastiera o il joystick. Al momento la funzione touch non è supportata.

**Mouse**

- Scorrere la rotellina del mouse per ingrandire e ridurre.
- Quando la mappa è zoomata, trascinare per spostarsi su di essa.

**Tastiera**

- In alternativa, premere CTRL + (+) per lo ingrandire e CTRL + (-) per rimpicciolire.
- Usa Ctrl + tasti freccia per pan e inclinazione.

**Joystick**

- Ruotare la testina del joystick per ingrandire e rimpicciolire l'immagine.
- Inclinare il joystick per eseguire pan e inclinazione.

**Acquisisci istantanea**

- Fare clic con il tasto destro del mouse sulla mappa per aprire il menu contestuale. È possibile salvare un'istantanea della mappa sul disco oppure aggiungerla alla scheda **Export (Esporta)**. L'istantanea riproduce la mappa esattamente come appare in quel momento, compresi tutti gli stati attuali delle telecamere e degli indicatori.

## Pagina web

L'immagine di una pagina Web visualizza una pagina Internet. È possibile, ad esempio, aggiungere una pagina Web a una suddivisione dell'immagine o a una sequenza.

Per aggiungere una pagina Web:

1. Nella scheda **Live view** (visualizzazione in diretta), fare clic su +.
2. Selezionare **New web page (Nuova pagina web)**.
3. immettere un nome per la pagina web;
4. Inserisci l'URL della pagina web.
5. Fare clic su **OK**.

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

## Cartelle

Utilizzare le cartelle per classificare gli elementi di una navigazione della visualizzazione ad albero. Le cartelle possono contenere suddivisioni dell'immagine, sequenze, viste della telecamera, mappe, pagine web e altre cartelle.

Per aggiungere una cartella:

1. Nella scheda Visualizzazione in diretta o Registrazioni, fare clic su +.
2. Selezionare **Nuova cartella**.
3. Immettere un nome per la cartella e fare clic su **OK**.

# Registrazioni

Dalla scheda **Recordings (Registrazioni)** è possibile cercare, riprodurre ed esportare le registrazioni. La scheda consiste di una vista principale e due pannelli dove si possono trovare viste, immagini, strumenti di riproduzione e telecamere dei server connessi raggruppati per nome del server. Vedere *Visualizzazione in diretta*.

Dalla vista principale si può eseguire la gestione dell'immagine come nella visualizzazione in diretta. Per saperne di più, andare su *Gestione dell'immagine nella visualizzazione in diretta, on page 14*.

Per cambiare il metodo di registrazione e le impostazioni, ad esempio la risoluzione, la compressione e la velocità in fotogrammi, vedere *Metodo di registrazione*.

Nota

Non è possibile eliminare manualmente le registrazioni da AXIS Camera Station Pro. Per eliminare le vecchie registrazioni, modificare il periodo di conservazione in**Configuration > Storage > Selection (Configurazione, Archiviazione, Selezione)**.

## Riproduzione delle registrazioni

Posizionando l'indicatore di riproduzione su molteplici registrazioni nella sequenza temporale, è possibile riprodurre simultaneamente le registrazioni di più telecamere.

Si possono visualizzare in contemporanea video in diretta e registrati quando si usano molteplici monitor.

### Sequenza temporale di riproduzione

Passare il mouse su una registrazione nella sequenza temporale per visualizzare il tipo e l'ora della registrazione. Per avere una vista migliore e individuare le registrazioni, è possibile ingrandire, rimpicciolire e trascinare la sequenza temporale. La riproduzione viene sospesa temporaneamente quando si trascina la sequenza temporale e riprende quando la si rilascia. Scorrere la cronologia per una panoramica dei contenuti e individuare momenti specifici.

- Una linea rossa indica una registrazione attivata dal rilevamento movimento.
- Una linea blu indica una registrazione triggerata da una regola di azione.

### Trovare registrazioni

| | |
|---|---|
| | Fare clic per eseguire la selezione di una data e di un'ora nella sequenza temporale. |
| | Filtrare i tipi di registrazione visualizzati nella cronologia. |
| | Usare per individuare i segnalibri salvati. Vedere *Segnalibri*. |
| | Fare clic per aprire un elenco di registrazioni e segnalibri creati con la telecamera indossabile Axis. Qui si può cercare la data e l'ora, il metodo di attivazione della registrazione e qualsiasi categoria e nota aggiunta dall'utente della telecamera in AXIS Body Worn Assistant. |
| Ricerca intelligente 1 | Cercare le registrazioni utilizzando la Ricerca intelligente 1. Vedere *Ricerca intelligente 1*. |

### Riproduzione delle registrazioni

| | |
|---|---|
| | Riproduci la registrazione. |
| | Mettere in pausa la registrazione. |
| | Saltare all'avvio della registrazione o dell'evento in corso o precedente. Fare clic con il pulsante destro del mouse per andare a registrazioni, eventi o entrambi. |
| | Saltare all'inizio della registrazione o dell'evento successivo. Fare clic con il pulsante destro del mouse per andare a registrazioni, eventi o entrambi. |
| | Andare al fotogramma precedente in una registrazione. Mettere in pausa la registrazione per impiegare questa funzionalità. Fare clic con il tasto destro del mouse per impostare quanti fotogrammi vanno saltati (massimo di 20 fotogrammi). |
| | Andare al fotogramma successivo in una registrazione. Mettere in pausa la registrazione per impiegare questa funzionalità. Fare clic con il tasto destro del mouse per impostare quanti fotogrammi vanno saltati (massimo di 20 fotogrammi). |
| 1x | Modificare la velocità di riproduzione usando i moltiplicatori nel menu a discesa. |
| | Disattivare audio. Solo le registrazioni dotate di audio dispongono di questa funzione. |
| **Cursore audio** | Usarlo per cambiare il volume dell'audio. Solo le registrazioni dotate di audio dispongono di questa funzione. |
| **Mostra tutti i metadati di dispositivi indossabili** | Mostrare i metadati di un sistema indossabile e visualizzare note e categorie da AXIS Body Worn Assistant. |
| **Rotazione, inclinazione e zoom** | Fare clic su un'immagine e scorrere per ingrandire o rimpicciolire. Per ingrandire un'area specifica, posizionare il cursore su di essa prima di scorrere la pagina. |

## Segnalibri

Nota

- Non si può cancellare una registrazione bloccata se non si sblocca in modo manuale.
- Le registrazioni bloccate vengono eliminate quando la telecamera associata viene rimossa dal sistema.

| | |
|---|---|
| | Fare clic per mostrare tutti i segnalibri. Per eseguire il filtraggio dei segnalibri, fare clic sull'icona. |
| | aggiungere un nuovo segnalibro. |
| | Vuol dire che è una registrazione bloccata. La registrazione comprende almeno 2,5 minuti di video prima e dopo il segnalibro. |

| | |
|---|---|
| | Modificare il nome e la descrizione del segnalibro oppure applicare il blocco e sbloccare la registrazione. |
| | Rimuovere un segnalibro. Per rimuovere più segnalibri, selezionali tenendo premuto il tasto Ctrl o Shift, quindi fare clic su **Remove (Rimuovi)**. |
| **Impedisci eliminazione registrazione** | Selezionare questa opzione per applicare il blocco alla registrazione. Premere per sbloccarlo. |

### 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 rendere il segnalibro facile da trovare.
5. Selezionare **Impedisci eliminazione registrazione** per proteggere la registrazione.

Nota

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

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

## Categorie di eventi

Assegnare delle categorie alle registrazioni per facilitare la ricerca di tipi specifici di eventi. Prima di iniziare, accertarsi di disporre delle autorizzazioni degli utenti necessarie. Vedere *Privilegi utente o di gruppo, on page 138*.

**Assegnare le categorie evento**

1. Nella scheda **Recordings (Registrazioni)** individuare la registrazione a cui si vuole assegnare una categoria evento.
2. Fare clic su una registrazione nella cronologia/ordine cronologico e selezionare **Categorize event (Categorizza evento)**.
3. Aggiungere una o più categorie.
4. Fare clic su **OK**.

Quando si classifica un evento, le categorie selezionate appaiono nella miniatura di anteprima della registrazione. Se è stato assegnato un colore alla categoria, l'ordine cronologico visualizza quel colore.

**Rimuovere categorie di evento**

1. Nella scheda **Recordings** (Registrazioni), individuare la registrazione dalla quale desidera rimuovere le categorie.
2. Fare clic su una registrazione nella cronologia/ordine cronologico e selezionare **Categorize event (Categorizza evento)**.
3. Nell'elenco delle categorie assegnate, selezionare la categoria che si desidera rimuovere.
4. Fare clic su **Remove (Rimuovi)**.
5. Ripetere i passaggi 3-4 per ogni categoria che si desidera rimuovere.
6. Fare clic su **OK**.

Nota

È possibile utilizzare il pulsante **Remove (Rimuovi)** solo se si dispone dell'autorizzazione a rimuovere le categorie o se si seleziona una categoria non assegnata dall'elenco.

Per ulteriori informazioni, vedere *Configurazione delle categorie di eventi, on page 90*.

## Esportazione delle registrazioni

Dalla scheda **Export (Esporta)**, si possono esportare le registrazioni a un dispositivo di archiviazione locale o a un percorso di rete. È possibile inoltre individuare informazioni e un'anteprima della registrazione. È possibile esportare più file contemporaneamente nei formati .asf, .mp4 e .mkv.

Per la riproduzione delle registrazioni, usare Windows Media Player (.asf) o AXIS File Player (.asf, .mp4, .mkv). AXIS File Player è un software di riproduzione audio e video gratis che non necessita di installazione.

Nota

Su AXIS File Player, puoi modificare la velocità di riproduzione delle registrazioni in formato .mp4 e .mkv, ma non in formato .asf.

Prima di iniziare, assicurarsi di disporre delle autorizzazioni per l'esportazione. Vedere *Autorizzazione utente per l'esportazione, on page 32*.

Per esportare una registrazione:

1. Nella scheda **Recordings (Registrazioni)**, selezionare una telecamera o una vista.
2. Aggiungere le registrazioni all'elenco di esportazione. Le registrazioni nella sequenza temporale che non sono comprese nell'esportazione hanno un colore a strisce.
   2.1. Fare clic su per mostrare i marcatori di selezione.
   2.2. Spostare gli indicatori per includere le registrazioni che si desidera esportare.
   2.3. Fare clic su per aprire la scheda **Export (Esporta)**.
3. Fare clic su **Export...(Esporta)**
4. Seleziona una cartella in cui esportare le registrazioni.
5. Fare clic su **OK**. L'attività di esportazione del report appare nella scheda **Tasks (Attività)**.

La cartella di esportazione include:

- Le registrazioni nel formato selezionato.
- Un file .txt con appunti, se si seleziona **Include notes (Includere note)**.
- AXIS File Player se è stato selezionato **Include AXIS File Player (Includi AXIS File Player)**.
- Un file di playlist in formato .asx, se si seleziona**Create playlist(.asx) (Crea playlist (.asx))**.

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

*Esportazione delle registrazioni*

| Scheda Recordings (Registrazioni) | |
|---|---|
| | Per la selezione di più registrazioni, fare clic su e spostare gli indicatori di selezione sull'inizio e fine voluti. |
| | Per esportare le registrazioni nei marcatori di sezione, fare clic su . |
| **Aggiungi registrazioni** | Per aggiungere una singola registrazione, fare clic con il pulsante destro del mouse su una registrazione e selezionare **Export > Add recordings (Esporta, Aggiungi registrazioni)**. |
| **Aggiungi registrazioni eventi** | Per eseguire l'aggiunta di tutte le registrazioni avvenute durante un evento, fare clic con il pulsante destro del mouse su una registrazione e selezionare **Export > Add event recordings (Esporta > Aggiungi registrazioni di eventi)**. |
| **Rimuovi registrazioni** | Per rimuovere una singola registrazione dall'elenco di esportazione, fare clic con il pulsante destro del mouse su una registrazione e selezionare **Export > Remove recordings (Esporta, Rimuovi registrazioni)**. |
| **Rimuovi registrazioni** | Per rimuovere molteplici registrazioni comprese nei marcatori di selezione dall'elenco di esportazione, fare clic con il pulsante destro del mouse fuori da una registrazione e selezionare **Export > Remove recordings (Esporta > Rimuovi registrazioni)**. |

| Scheda Export (Esporta) | |
|---|---|
| **Audio** | Per escludere l'audio da una registrazione esportata, deselezionare la casella di controllo nella colonna **Audio**. Per comprendere sempre l'audio nelle registrazioni esportate, andare a **Configuration (Configurazione)** > **Server** > **Settings (Impostazioni)** > **Export (Esporta)** e selezionare **Include audio when adding recordings to export (Includi audio quando aggiungi registrazioni da esportare)**. |
| | Per modificare la registrazione, selezionarla e fare clic su . Vedere *Modifica registrazioni prima dell'esportazione, on page 32*. |
| | Per eseguire la modifica degli appunti per la registrazione, selezionare una registrazione e fare clic su . |
| | Per rimuovere la registrazione dall'elenco di esportazione, selezionare una registrazione e fare clic su . |
| **Switch per l'esportazione** | Se è aperta la scheda **Incident report (Report incidente**, fare clic su **Switch to export (Cambia per l'esportazione** per spostarsi nella scheda **Export (Esporta)**. |

| Scheda Export (Esporta) | |
|---|---|
| **Profilo di streaming preferito** | Selezionare il profilo di streaming nel campo **Preferred stream profile (Profilo di streaming preferito)**. |
| **Anteprima** | Per vedere l'anteprima della registrazione, fare clic su una registrazione nell'elenco esportato per riprodurla. È possibile visualizzare in anteprima più registrazioni solo se provengono dalla stessa telecamera. |
| **Salva** | Per salvare l'elenco di esportazione in un file, fare clic su **Save (Salva)**. |
| **Carica** | Per includer un elenco di esportazione salvato precedentemente, fare clic su **Load (Carica)**. |
| | |
| **Nome dell'esportazione** | Inserire un nome personalizzato per la cartella e i file esportati oppure lasciare il campo vuoto per utilizzare la convenzione di denominazione predefinita in AXIS Camera Station Pro. |
| **Aggiungere il nome della telecamera e il timbro orario** | Selezionare questa opzione per aggiungere il nome della telecamera e il timbro orario al nome della cartella e dei file esportati. |
| **Regolazione del momento di inizio e di fine** | Per adattare il momento di inizio e fine della registrazione, andare alla sequenza temporale nell'anteprima e regolare il momento di inizio e fine. La sequenza temporale mostra fino a trenta minuti di registrazione prima e dopo la registrazione selezionata. |
| **Aggiunta di un'istantanea** | Per aggiungere un'istantanea, trascinare la cronologia nell'anteprima in una ubicazione specifica, fare clic con il tasto destro del mouse sull'anteprima e selezionare **Add snapshot (Aggiungi istantanea)**. |

| Impostaz. avanzate | |
|---|---|
| **Note di inclusione** | Selezionare **Include notes (Includi note)** per includere le note della registrazione come file .txt nella cartella di esportazione e come segnalibro in AXIS File Player. |
| **Include AXIS File Player (Includi AXIS File Player)** | Per includere AXIS File Player con le registrazioni esportate, selezionare **Include AXIS File Player (Includi AXIS File Player)**. |
| **Create playlist(.asx) (Crea playlist (.asx))** | Per creare una playlist in formato .asx utilizzata da Windows Media Player, selezionare **Create playlist(.asx) (Crea playlist (.asx))**. Le registrazioni si riproducono nell'ordine di registrazione. |
| **Aggiungi firma digitale** | Per impedire che l'immagine sia manomessa, selezionare **Add digital signature (Aggiungi firma digitale)**. Questa opzione è disponibile solo per le registrazioni nel formato .asf. Vedere *Riproduzione e verifica delle registrazioni esportate, on page 34*. |

| Impostaz. avanzate | |
|---|---|
| **Esporta in un file Zip** | Per esportare in un file ZIP, selezionare **Export to Zip file (Esporta in file ZIP)** e, se necessario, inserire una password. |
| **Formato di esportazione** | Dal menu a discesa **Export format (Formato di esportazione)** selezionare un formato per esportare le registrazioni. Le registrazioni esportate non includono l'audio nel formato G.711 o G.726 se si seleziona MP4. |
| **Edited video encoding (Codifica video modificata)** | Per video modificati, è possibile impostare il formato di codifica video su `Automatic`, `H.264`, o `M-JPEG` in **Edited video encoding** (Codifica video modificato). Selezionare `Automatic` per usare m-jpeg per formato M-JPEG e H. 264 per tutti gli altri formati. |

## Autorizzazione utente per l'esportazione

Per eseguire l'esportazione di registrazioni o generare rapporti sugli incidenti servono le autorizzazioni appropriate. Si può avere l'autorizzazione per uno o tutti e due. Quando si fa clic su nella scheda **Recordings (Registrazioni)**, la scheda Esporta connessa si apre.

Per configurare le autorizzazioni, andare a *Autorizzazioni utente, on page 136*.

## Modifica registrazioni prima dell'esportazione

### Sfocatura di un oggetto in movimento

1. Nella scheda **Export (Esporta)** o **Incident report (Report dell'incidente)**, selezionare una registrazione e fare clic su .
2. Spostare la sequenza temporale sulla prima occorrenza dell'oggetto in movimento che si vuole coprire.
3. Fare clic su **Bounding boxes > Add (Riquadri delimitatori > Aggiungi)** per aggiungere un nuovo riquadro delimitatore.
4. Andare a **Bounding box options > Size (Opzioni riquadro delimitatore > Dimensioni)** per regolare le dimensioni.
5. Spostare il riquadro delimitatore e posizionarlo sopra l'oggetto.
6. Andare a **Bounding box options > Fill (Opzioni riquadro delimitatore > Riempi)** e impostare **Pixelated (Pixelato)** o **Black (Nero)**.
7. Mentre la registrazione viene riprodotta, fare clic con il pulsante destro del mouse sull'oggetto e selezionare **Add key frame (Aggiungi fotogramma chiave)**.
8. Per aggiungere fotogrammi chiave continui, spostare i riquadri delimitatori del testo fino a coprire l'oggetto durante la riproduzione della registrazione.
9. Spostare la sequenza temporale e assicurarsi che i riquadri delimitatori del testo coprano l'oggetto in tutta la registrazione.
10. Per impostare un punto di fine, fare clic con il pulsante destro del mouse sulla forma a diamante nell'ultimo fotogramma chiave e selezionare **Set end (Imposta la fine)**. Ciò elimina i fotogrammi chiave dopo il punto finale.

Nota

È possibile aggiungere più riquadri delimitatori nel video. Se i riquadri delimitatori del testo si sovrappongono, l'area di sovrapposizione utilizza il riempimento nel seguente ordine: Nero, Pixelato, poi Cancella.

| | |
|---|---|
| **Rimuovi tutto** | Per eseguire la rimozione di tutti i riquadri delimitatori, fare clic su **Bounding boxes > Remove all (Riquadri delimitatori > Rimuovi tutto)**. |
| **Rimuovi fotogramma chiave** | Per rimuovere un fotogramma chiave, fare clic con il pulsante destro del mouse sul fotogramma chiave e selezionare **Remove key frame (Rimuovi fotogramma chiave)**. |

### Visualizzazione di un oggetto in movimento con sfondo sfocato

1. Creare un riquadro delimitatore. Vedere *Sfocatura di un oggetto in movimento, on page 32*.
2. Andare a **Bounding box options > Fill (Opzioni riquadro delimitatore > Compila)** e impostarla su **Clear (Trasparente)**.
3. Andare a **Video background (Sfondo video)** e impostarla su **Pixelated (Pixelato)** o **Black (Nero)**.

| | |
|---|---|
| **Scomponi tutto in pixel tranne questo** | Selezionare più riquadri delimitatori nell'elenco, fare clic con il pulsante destro del mouse e selezionare **Pixelate all but this (Pixelare tutto tranne questo)**. I riquadri delimitatori selezionati diventano **Clear (Trasparenti)** mentre i non selezionati diventano **Pixelated (Pixelati)**. |

### Genera riquadri delimitatori

Per generare riquadri delimitatori del testo dai dati di analisi, assicurarsi che la funzione di analisi della telecamera sia attiva. Vedere *Profili di flusso, on page 55*.

1. Nella scheda **Export (Esportare)** o **Incident report (Report dell'incidente)**, fare clic su .
2. Fare clic su **Generate bounding boxes (Genera riquadri delimitatori)**.
3. Assicurarsi che i riquadri delimitatori del testo coprano l'oggetto in movimento. Se necessario, regolare.
4. Selezionare un riempimento per i riquadri delimitatori o lo sfondo del video.

### Miglioramento dell'editing video con AXIS Video Content Stream

Per migliorare l'editing video, installare l'applicazione AXIS Video Content Stream 1.0 sulle telecamere con firmware da 5.50 a 9.60. AXIS Camera Station Pro avvia automaticamente l'installazione quando si aggiunge una telecamera al sistema. Vedere *Installare le applicazioni per telecamera*.

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

*Modificare le registrazioni prima di esportare*

### Riproduzione e verifica delle registrazioni esportate

Per impedire che le immagini siano manomesse, si può aggiungere una firma digitale alle registrazioni esportate con o senza una password. Usare AXIS File Player per verificare la firma digitale e controllare se la registrazione è stata cambiata.

1. Andare alla cartella con le registrazioni esportate. Nel caso il file Zip esportato sia protetto da password, inserire la password per aprire la cartella.
2. Aprire AXIS File Player. Le registrazioni esportate vengono riprodotte in modo automatico.
3. In AXIS File Player, fare clic su per visualizzare le note relative alla registrazione.
4. Per verificare la firma digitale delle registrazioni esportate con l'opzione **Add digital signature (Aggiungi 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 se è protetto con password.
   4.3. Per vedere i risultati della verifica, fare clic su **Verify (Verificare)**.

## Esporta report dell'incidente

Dalla scheda **Incident report (Report incidente)** è possibile esportare i report degli incidenti in un archivio locale o in un percorso di rete. È possibile includere registrazioni, istantanee e appunti nei report degli incidenti.

Prima di iniziare, assicurarsi di disporre delle autorizzazioni per l'esportazione. Vedere *Autorizzazione utente per l'esportazione, on page 32*.

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

*Report eventi*

**Generate incident reports (Generare i report dell'incidente)**

1. Nella scheda **Recordings (Registrazioni)**, selezionare una telecamera o una vista.
2. Aggiungere le registrazioni all'elenco di esportazione. Vedere *Esportazione delle registrazioni, on page 29*.
3. Fare clic su **Switch to incident report (Passa al report dell'incidente)** per andare alla scheda **Incident report (Report dell'incidente)**.
4. Fare clic su **Create report (Crea report)**.
5. Selezionare una cartella dove salvare il report dell'incidente.
6. Fare clic su **OK**. L'attività di esportazione del report dell'incidente appare nella scheda **Tasks (Attività)**.

La cartella di esportazione include:

- AXIS File Player.
- Le registrazioni nel formato selezionato.
- Un file .txt se si seleziona **Include notes (Includi appunti)**.
- Il report dell'incidente.
- La playlist se si esportano multiple registrazioni.

| | |
|---|---|
| **Audio** | Per escludere l'audio da una registrazione esportata, deselezionare la casella di controllo nella colonna **Audio**. Per comprendere sempre l'audio nelle registrazioni esportate, andare a **Configuration (Configurazione)** > **Server** > **Settings (Impostazioni)** > **Export (Esporta)** e selezionare **Include audio when adding recordings to export (Includi audio quando aggiungi registrazioni da esportare)**. |
| | Per modificare la registrazione, selezionarla e fare clic su . Vedere *Modifica registrazioni prima dell'esportazione, on page 32*. |
| | Per eseguire la modifica degli appunti per la registrazione, selezionare una registrazione e fare clic su . |
| | Per rimuovere una registrazione dall'elenco di esportazione, selezionare una registrazione e fare clic su . |
| **Passare al report dell'incidente** | Se la scheda **Export (Esporta)** è aperta fare clic su **Switch to incident report (Passa la report incidente)** per andare alla schdea **Incident report (Report incidente)**. |
| **Profilo di streaming preferito** | Selezionare il profilo di streaming nel menu a discesa **Preferred stream profile (Profilo di streaming preferito)**. |
| **Anteprima** | Per vedere l'anteprima della registrazione, fare clic su di essa nell'elenco di esportazione per riprodurla. È possibile visualizzare in anteprima più registrazioni solo se provengono dalla stessa telecamera. |
| **Salva** | Per salvare il report dell'incidente in un file, fare clic su **Save (Salva)**. |
| **Carica** | Per caricare un rapporto sull'incidente salvato in precedenza, fare clic su **Load (Carica)**. |
| **Descrizione** | Il campo **Description (Descrizione)** si riempie in automatico con i dati predefiniti dal modello di descrizione. È possibile aggiungere anche le informazioni supplementari da includere nel report dell'incidente. |
| **Categoria** | Selezionare una categoria a cui appartiene il report. |
| **ID di riferimento** | Viene generato automaticamente un **Reference ID (ID di riferimento)**. Se necessario, è possibile effettuare la modifica manualmente. L'ID è univoco e identifica il report dell'incidente. |
| **Note di inclusione** | Selezionare **Include notes (Includi note)** per includere le note della registrazione come file .txt nella cartella di esportazione e come segnalibro in AXIS File Player. |
| **Edited video encoding (Codifica video modificata)** | Per video modificati, è possibile impostare il formato di codifica video su `Automatic`, `H.264`, o `M-` |

| | |
|---|---|
| | `JPEG` in **Edited video encoding** (Codifica video modificato). Selezionare `Automatic` per usare m-jpeg per formato M-JPEG e H. 264 per tutti gli altri formati. |
| **Regolazione del momento di inizio e di fine** | Per adattare il momento di inizio e fine della registrazione, andare alla sequenza temporale nell'anteprima e regolare il momento di inizio e fine. La sequenza temporale mostra fino a trenta minuti di registrazione prima e dopo la registrazione selezionata. |
| **Aggiunta di un'istantanea** | Per aggiungere un'istantanea, spostare la cronologia nell'anteprima in una determinata posizione, fare clic con il tasto destro del mouse sull'anteprima e selezionare **Add snapshot (Aggiungi istantanea)**. |

## Registrazione manuale

Nota

Quando ci si connette a più server AXIS Camera Station Pro, è possibile avviare e interrompere manualmente una registrazione su qualsiasi server connesso. A tal fine, selezionare il server dall'elenco a discesa **Selected server (Server selezionato)** .

Per avviare e interrompere manualmente una registrazione dal menu principale:

1. Andare su ≡ > **Azioni** > **Registra manualmente**.
2. selezionare una o più videocamere;
3. Fare clic su **Start (Avvia)** per avviare la registrazione.
4. fare clic su **Stop** per arrestare la registrazione.

Per avviare e interrompere una registrazione manuale dalla scheda **Live view (Visualizzazione in diretta)**:

1. Andare a **Live view (Visualizzazione in diretta)**.
2. Passa il mouse sul fotogramma della visualizzazione in diretta della telecamera.
3. Fare clic su **REC** per avviare la registrazione. Nel corso della registrazione, un indicatore rosso appare nel riquadro di visualizzazione.
4. Fare clic su **REC** per arrestare la registrazione.

## Ricerca intelligente 1

Utilizza la Ricerca intelligente 1 per individuare le parti di una registrazione in cui si sono verificati movimenti in un'area definita.

Per aumentare la velocità di ricerca, selezionare **Include analytics data (Includi dati di analisi)** nei profili di streaming. Vedere *Profili di flusso*.

Per utilizzare la ricerca intelligente 1:

1. Fare clic su + e aprire una scheda **Smart search 1 (Ricerca intelligente 1)**.
2. Selezionare la telecamera in cui si desidera eseguire la ricerca.
3. Regolare l'area di interesse. È possibile aggiungere fino a 20 punti alla forma. Per rimuovere un punto, fare clic con il pulsante destro del mouse su di esso.
4. Utilizzare **Short-lived objects filter (Filtro per i movimenti di breve durata)** e **Small objects filter (Filtro oggetti piccoli)** per filtrare i risultati indesiderati.
5. Selezionare l'intervallo di date e orari per la ricerca. Utilizzare il tasto Maiusc per selezionare un intervallo di date.
6. fare clic su **Cerca**;

I risultati della ricerca vengono visualizzati nella scheda **Results (Risultati)**. È possibile fare clic con il pulsante destro del mouse su uno o più risultati per esportare le registrazioni.

| | |
|---|---|
| **Short-lived objects filter (Filtro movimenti di breve durata):** | Il tempo minimo per cui un oggetto deve trovarsi nell'area di interesse per essere incluso nei risultati di ricerca. |
| **Small objects filter (Filtro oggetti piccoli)** | Dimensione minima che un oggetto deve includere nei risultati di ricerca. |

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

*Ricerca intelligente 1*

## Ricerca intelligente 2

Impiegare Ricerca intelligente 2 per individuare persone e veicoli in movimento in registrazioni.

Nota

La Ricerca intelligente 2 richiede quanto segue:

- Metadati di analisi dello streaming su RTSP.
- AXIS Video Content Stream sulle telecamere con sistema operativo AXIS precedente a 9.60. Vedere *Installare le applicazioni per telecamera, on page 69*.
- Sincronizzazione dell'ora tra il server AXIS Camera Station Pro e le telecamere.

Quando si attiva la funzione Ricerca intelligente 2 per una telecamera Axis, AXIS Camera Station Pro inizia a effettuare la registrazione dei metadati provenienti da quella telecamera e li utilizza per classificare gli oggetti presenti nella scena. Questo consente di utilizzare i filtri per trovare ciò che interessa.

Nota

- Si consiglia di utilizzare la registrazione continua, poiché il rilevamento movimento può generare segnalazioni senza che vi sia alcuna registrazione video.
- Usare il formato H.264 se si vogliono vedere in anteprima le registrazioni nei risultati della ricerca.
- Controllare che le condizioni di illuminazione siano conformi alle specifiche della telecamera per ottenere una classificazione ottimale dei colori. Se necessario, utilizzare luci supplementari.

### Flusso di lavoro

1. *Configura la ricerca intelligente 2, on page 174*
2. Configurare la sincronizzazione dell'ora tra il server AXIS Camera Station Pro e le telecamere. Vedere *Sincronizzazione dell'ora, on page 74*.
3. Crea un filtro o caricane uno esistente. Vedere *Ricerca con filtri, on page 38*.
4. Gestione dei risultati della ricerca. Vedere *Risultati di Ricerca intelligente, on page 42*.

### Ricerca con filtri

1. Andare a **Configuration > Smart search 2 > Settings (Configurazione > Ricerca intelligente 2 > Impostazioni)** e selezionare le telecamere che si vogliono usare nella Ricerca intelligente 2.
2. Fare clic su + e aprire la scheda **Smart search 2 (Ricerca intelligente 2)**.
3. Definire i criteri di ricerca.
4. fare clic su **Cerca**;

Se la ricerca richiede più tempo del previsto, provare uno o più dei seguenti aspetti per accelerarla:

- Attivare la classificazione del server in background per le telecamere importanti o utilizzate di frequente.
- Applicare filtri in entrata alle telecamere per ridurre i rilevamenti non pertinenti.
- Accorciare il periodo di ricerca.
- Ridurre il numero di telecamere nella ricerca.
- Definire l'area, la direzione dell'oggetto, le dimensioni e la durata per restringere la quantità di dati.

| | |
|---|---|
| **Telecamere** | Per eseguire la limitazione della ricerca in base alla telecamera, fare clic su **Cameras (Telecamere)** e selezionare le telecamere che si vogliono includere nella ricerca. |
| **Intervallo di ricerca** | Per limitare la ricerca in base al tempo, fare clic su **Search interval** (Intervallo di ricerca) e selezionare un |

| | |
|---|---|
| | intervallo di tempo, un intervallo di tempo specifico su più giorni o creare un intervallo personalizzato. |
| **Persona** | Per eseguire il rilevamento di persone, fare clic su **Object characteristics (Caratteristiche dell'oggetto)** > **Pre-classified (Preclassificato)**, selezionare **Person (Persona)** e i colori dei vestiti. È possibile selezionare più colori. |
| **Veicolo** | Per eseguire il rilevamento dei veicoli, fare clic su **Object characteristics (Caratteristiche dell'oggetto)** > **Pre-classified (Preclassificato)** e selezionare i tipi e i colori di veicolo. È possibile selezionare più tipi e colori per i veicoli. |
| **Somiglianza visiva** | Si può usare un risultato di ricerca con una persona presente nell'immagine ai fini della ricerca di persone visivamente simili. Aprire il menu contestuale ⋮ in un elemento dei risultati di ricerca e selezionare **Use as visual similarity reference (Usa come riferimento di somiglianza visiva)**. Quindi fare clic su **Search (Cerca)**.<br>Nota<br>La ricerca per similarità crea rappresentazioni astratte da immagini ritagliate a bassa risoluzione di persone e le confronta con altre rappresentazioni. Quando due rappresentazioni sono simili, si ottiene una risposta alla propria ricerca. La ricerca per similarità non utilizza i dati biometrici per identificare una persona, ma può, ad esempio, riconoscere la forma generale e il colore dei vestiti di una persona. |
| **Ricerca a testo libero** | La ricerca a testo libero consente di descrivere ciò che si sta cercando nelle unità di registrazione utilizzando il parlato naturale (solo inglese). Vedere *Ricerca a testo libero, on page 40*. |
| **Area** | Per filtrare in base all'area, fare clic su **Area**, selezionare una telecamera e attivare l'opzione **Filter by area on this camera (Filtra per area in questa telecamera)**. Regolare l'area di interesse nell'immagine e aggiungere o rimuovere i punti se occorre. |
| **Attraversamento linea** | Per filtrare in base agli attraversamenti linea, fare clic su **Line crossing (Attraversamento linea)**, selezionare una telecamera e attivare **Filter by line crossing on this camera (Filtra per attraversamento linea in questa telecamera)**. Regolare la linea nell'immagine e aggiungere o rimuovere i punti se occorre. |
| **Dimensioni** | Per filtrare per dimensione, fare clic su **Size (Dimensione)**, selezionare la telecamera e attivare **Filter by size on this camera (Filtra per dimensione su questa telecamera)**. Regolare l'altezza e la larghezza minima espressa in percentuale dell'immagine totale. |

| | |
|---|---|
| **Durata** | Per filtrare per durata, fare clic su **Duration (Durata)**, selezionare la telecamera e attivare l'opzione **Filter by duration on this camera (Filtra per durata su questa telecamera)**. Regolare la durata minima in secondi. |
| **Velocità** | Per filtrare per velocità, fare clic su **Speed (Velocità)**, selezionare la telecamera e attivare **Filter by speed on this camera (Filtra per velocità su questa telecamera)**. Specificare l'intervallo di velocità che si desidera includere nel filtro.<br>Nota<br>Il filtro velocità è disponibile per dispositivi come radar e telecamere a fusione che sono in grado di rilevare la velocità. |
| **Rilevamenti oggetti sconosciuti** | Per comprendere i rilevamenti che ricerca intelligente 2 classifica come sconosciuti, selezionare **Object characteristics (Caratteristiche dell'oggetto)** e poi **Unknown object detections (Rilevamenti di oggetti sconosciuti)**. |
| | Per eseguire il salvataggio di un filtro, fare clic su , digitare il nome del filtro e fare clic su **Save (Salva)**.<br>Selezionare **Share with other users (Condividi con altri utenti)** per condividere il filtro con altri utenti.<br>Per la sostituzione di un filtro esistente, fare clic su , selezionare un filtro esistente e fare clic su **Replace (Sostituisci)**. |
| | Per eseguire il caricamento di una ricerca recente, fare clic su > **Recent searches (Ricerche recenti)** e selezionare una ricerca.<br>Per caricare un filtro salvato, fare clic su > **Saved filters (Filtri salvati)** e selezionare un filtro.<br>Per caricare un filtro condiviso da un altro utente, fare clic su > **Shared filters (Filtri condivisi)** e selezionare un filtro. |
| | Per reimpostare un filtro, fare clic su e fare clic su **Reset (Reimposta)**. |

## Ricerca a testo libero

La ricerca a testo libero permette di descrivere ciò che si sta cercando nelle registrazioni utilizzando il linguaggio naturale.

Nota

- La ricerca di testo libero richiede un minimo di 16 GB di RAM.
- La ricerca di testo libero richiede una connessione a Internet.
  - La ricerca a testo libero utilizza la connessione a Internet per scaricare il modello AI da axis.com quando si effettua la prima impostazione e quando Axis aggiorna il modello.

- La ricerca a testo libero si collega una volta alla settimana ai servizi cloud di Axis per verificare se i modelli di intelligenza artificiale richiedono aggiornamenti per conformarsi a normative o requisiti futuri. Se la connessione si interrompe, non sarà possibile utilizzare la ricerca di testo libero finché il sistema non si riconnette.
- La ricerca a testo libero esegue tutte le elaborazioni localmente sul server e **non** utilizza la connessione a Internet per inviare video, immagini o testi richiesti.

Per attivare la ricerca di testo libero:

1. Apri una scheda **Configuration (Configurazione)**.
2. Andare il **Smart search 2 (Ricerca intelligente 2)** > **Settings (Impostazioni)**.
3. Nel campo della ricerca testo libero (Free text search), selezionare **Use free text search (Usa ricerca testo libero)**. Il sistema scarica i file necessari da axis.com.

Per cercare:

1. Aprire una scheda **Smart search 2 (Ricerca intelligente 2)**.
2. Fare clic su **Object characteristics (Caratteristiche dell'oggetto)**.
3. Fare clic su **Free text (Testo libero)**.
4. Fare clic su **Show (Mostra)** per leggere le informazioni sull'uso previsto, le limitazioni e l'uso responsabile.
5. Inserire gli elementi che si vogliono includere ed escludere nella ricerca.
6. fare clic su **Cerca**;

### Linee guida per il prompt

Si consiglia di utilizzare la seguente struttura per le proprie ricerche:

`{person, vehicle or other object} + {specific action or attributes of the person, vehicle, or object}`

**Descrivere l'oggetto con pochi elementi chiave. Ad esempio puoi:**

| Ricerca | Commento |
|---|---|
| Una signora con maglione rosso e cappello nero | Abbastanza corretta |
| Signora in rosso | Un po' troppo vago |
| Una signora alta circa 156 cm, con un cardigan marrone con motivi gialli e un cappello da sole nero di ispirazione fine anni '80 con bordi marrone scuro | Troppi dettagli |

**Descrivere la situazione come se steste parlando con una persona, che non sia un esperto di sorveglianza. Ad esempio puoi:**

| Ricerca | Commento |
|---|---|
| Un furgone giallo parcheggiato vicino a un albero | Abbastanza corretta |
| Un veicolo senza conducente, targa: CHY67F, classe: pickup, colore: giallo, posizione: Adiacente al pioppo grande. | Troppo simile a un rapporto di polizia |

**Descrittori validi che la ricerca a testo libero ha buone possibilità di comprendere:**

| Descrittore | Esempio |
|---|---|
| Classe di oggetti | Persona, Auto, Bicicletta, Animale |
| Colore | Giallo |
| Clima | Sereno |
| Marchi noti (marchi di automobili, loghi) | Furgone UPS |

**Descrittori errati:**

| Descrittore | Esempio |
|---|---|
| Testo | Un'insegna di un negozio con la scritta "Vietato l'ingresso agli orsi danzanti" |
| Dettagli emotivi | Un uomo dall'aria arrabbiata |
| Conteggio | 14 persone che si aggirano in una piazza della città |
| Gergo locale | Un aspirapolvere rosso |

### Moderazione del testo di ricerca

Le ricerche contenenti contenuti offensivi, dannosi o deleteri possono essere bloccate per mantenere un ambiente sicuro e rispettoso. Il nostro sistema utilizza un modello di elaborazione del linguaggio naturale e un elenco personalizzato di categorie e parole di ricerca vietate per valutare ogni query di ricerca.

Se non si è d'accordo riguardo a una parola bloccata o se si vuole suggerirne una nuova, fornire un feedback anonimo attraverso l'interfaccia utente della Ricerca intelligente, che sarà ricevuto dal nostro team per la revisione.

Nota

- La ricerca a testo libero supporta solo l'inglese.
- La ricerca di testo libero comprende le immagini fisse. Può essere difficile ottenere buoni risultati per azioni come cadere, correre o rubare, perché richiedono un contesto più ampio.
- La ricerca a testo libero utilizza immagini ritagliate, quindi potrebbe non includere l'ambiente circostante. È possibile ottenere risultati meno accurati utilizzando descrittori di scena quali città, urbano, parco, giardino, lago e spiaggia.
- Per informazioni più dettagliate sulla funzione di ricerca del testo libero, comprese le limitazioni e le pratiche migliori, consultare il nostro documento tecnico *Free text search in AXIS Camera Station Pro*.

## Risultati di Ricerca intelligente

| | |
|---|---|
| | Si possono raggruppare in intervalli di tempo rilevamenti che sono correlati allo stesso evento.<br>Selezionare un intervallo dal menu a discesa . |
| **Meno recente prima** | Ricerca intelligente 2 mostra i risultati di ricerca in ordine decrescente a partire dagli ultimi rilevamenti.<br>Fare clic su **Oldest first (Più vecchi prima)** perché i rilevamenti più vecchi siano mostrati per primi. |
| **Confidence level (Livello di attendibilità)** | Per filtrare ulteriormente i risultati della ricerca, fare clic su **Confidence level (Livello di attendibilità)** e |

| | |
|---|---|
| | impostare il livello di fiducia. Un livello di confidenza elevato elimina le classificazioni incerte. |
| **Columns (Colonne)** | Per adattare le dimensioni delle thumbnail nel risultato di ricerca, fare clic su **Columns (Colonne)** e cambiare la quantità di colonne. |
| **Detection view (Vista rilevamento)** | Per mostrare come thumbnail una vista ritagliata dell'oggetto rilevato, selezionare **Detection view (Vista rilevamento)**. |

## Limiti

- Ricerca intelligente 2 supporta solo l'area di visione primaria (non ritagliata).
- Ricerca intelligente 2 supporta solo modalità di rilevamento non ritagliate.
- L'utilizzo di Ricerca intelligente 2 con flussi di telecamere speculari e ruotati per dispositivi con ARTPEC-7 o superiore e versione del firmware precedente a 10.6 può causare alcuni problemi.
- Una latenza di rete alta o molto variabile può causare problemi di sincronizzazione dell'ora e influire sulla classificazione dei rilevamenti in base ai metadati basati sull'analisi.
- La classificazione dei tipi di oggetto e la precisione del rilevamento sono influenzate negativamente dalla bassa qualità di immagine a causa di alti livelli di compressione, da condizioni meteo come pioggia forte o neve e telecamere a bassa risoluzione, forte distorsione, ampio campo visivo o vibrazioni eccessive.
- La ricerca intelligente 2 potrebbe non eseguire il rilevamento di oggetti piccoli e distanti.
- La classificazione dei colori non funziona al buio o con illuminazione IR.
- Le Body Cam non sono supportate.
- Il radar può rilevare solo persone e altri veicoli. Non è possibile attivare la classificazione in background del server per il radar.
- Il comportamento di classificazione degli oggetti è imprevedibile per le telecamere termiche.
- Ricerca intelligente 2 non rileva oggetti in movimento quando una posizione preset PTZ cambia e per un breve periodo dopo la modifica della posizione.
- I filtri delle zone e l'attraversamento linea non seguono le modifiche delle posizioni PTZ.

## Ricerca dati

Ricerca dati permette di individuare dati provenienti da una sorgente esterna. Una fonte è un sistema o un dispositivo che genera dati relativi a determinati eventi. Per ulteriori informazioni, vedere *Origini di dati esterne, on page 73*.
Ad esempio puoi:

- Un evento generato da un sistema di controllo degli accessi.
- Una targa catturata da AXIS License Plate Verifier.
- Una velocità catturata da AXIS Speed Monitor.

Per modificare il di tempo di conservazione dei dati esterni, da parte di AXIS Camera Station Pro andare a **Configuration > Server > Settings > External data (Configurazione, Server, Impostazioni. Dati esterni)**.

Per cercare dati:

1. Fare clic su + e selezionare **Data search (Ricerca dati)**.
2. Selezionare un intervallo di ricerca .
3. Selezionare un tipo di sorgente dati dall'elenco a discesa
4. Fare clic su **Search options (Opzioni di ricerca)** e applicare i filtri aggiuntivi. I filtri disponibili variano in base al tipo di origine dati.
5. Inserire una parola chiave qualsiasi nel campo di ricerca. Vedere *Ottimizzazione della tua ricerca, on page 45*.
6. fare clic su **Cerca**;

La ricerca dati aggiunge ai segnalibri i dati generati dalla sorgente se è stata configurata con una vista. Fare clic sui dati nell'elenco per andare alla registrazione associata con l'evento.

| Intervallo di tempo | |
|---|---|
| **Live (In diretta)** | Per eseguire la ricerca di dati in tempo reale, selezionare **Live (Diretta)** come intervallo di tempo. La ricerca dati è in grado di visualizzare fino a 3000 eventi di dati in diretta. La modalità in diretta non supporta gli operatori di ricerca. |
| **Ultima ora – Ultimi 30 giorni** | Per effettuare una ricerca nei dati relativi a un intervallo di tempo preimpostato, selezionare una delle opzioni disponibili: nell'ultima ora, 4 ore, 12 ore, 24 ore, 48 ore, 7 giorni o 30 giorni. |
| **Personalizzato** | Per cercare dati all'interno di un intervallo di tempo specifico, selezionare **Custom** (Personalizzato) e impostare la data e l'ora di inizio e di fine. |

Il risultato della ricerca può essere filtrato in base ai diversi tipi di fonti:

| Tipo di origine dati | |
|---|---|
| **All data (Tutti i dati)** | Questa opzione comprende i dati di sorgenti sia esterne che componenti. |

| | |
|---|---|
| **Controllo accessi** | Utilizzare questa opzione per includere solo i dati provenienti da questo componente. Il controllo degli accessi consente di filtrare porte e zone, titolari di carte e tipi di evento. |
| **Third party (Terze parti)** | Impiegare questa opzione per includere dati di origini di terze parti che non siano i componenti configurati. |

In base alla fonte di dati si possono ottenere elementi diversi nel risultato di ricerca. Ad esempio puoi:

| Risultati della ricerca | |
|---|---|
| **Server** | Il server a cui si inviano i dati dell'evento. Disponibile solo quando ci si collega a più server. |
| **Luogo** | Il nome della porta e il nome del door controller con indirizzo IP. |
| **Velocità di entrata** | La velocità (chilometri all'ora o miglia all'ora) quando l'oggetto entra nella zona Rilevamento movimento radar (RMD). |
| **Classificazione** | Classificazione dell'oggetto. Ad esempio puoi: Veicolo. |

Per esportare i risultati della ricerca in un PDF o un file di testo, fare clic su **Download search result (Scarica i risultati della ricerca)**. È possibile riorganizzare le colonne e regolarne la larghezza per migliorare la struttura della tabella nell'output PDF. Il PDF include fino a 10 colonne.

## Ottimizzazione della tua ricerca

Si possono usare i seguenti operatori di ricerca per avere risultati più precisi:

| | |
|---|---|
| Utilizzare le virgolette `" "` per corrispondenze esatte per parole chiave | • Una ricerca di `"door 1"` restituisce risultati che contengono "porta 1".<br>• Una ricerca di `door 1` restituisce risultati che contengono sia "porta" che "1". |
| Usare `AND` per individuare corrispondenze che contengano tutte le parole chiave. | • Una ricerca di `door AND 1` restituisce risultati che contengono sia "porta" che "1".<br>• Una ricerca di `"door 1" AND "door forced open"` restituisce risultati che contengono sia "porta 1" che "porta forzata aperta". |
| Usare `OR` oppure `\|` per individuare corrispondenze che contengono una qualunque delle parole chiave. | • Una ricerca di `"door 1" OR "door 2"` restituisce risultati che contengono "porta 1" o "porta 2".<br>• Una ricerca di `door 1 OR door 2` restituisce risultati che contengono "porta" o "1" o "2". |
| Utilizzare le parentesi `( )` insieme a `AND` o `OR`. | • La ricerca di `(door 1 OR door 2) AND "Door forced open"` restituisce risultati contenenti uno dei seguenti elementi:<br>– "porta 1" e "porta aperta forzatamente"<br>– "porta 2" e "Apertura forzata della porta" |

| | |
|---|---|
| | • La ricerca di `door 1 AND (door (forced open OR open too long))` restituisce risultati contenenti uno dei seguenti elementi:<br>– "porta 1" e "porta aperta forzatamente"<br>– "porta 1" e "porta aperta troppo a lungo" |
| Usare >, >=, <, or <= per filtrare i numeri in una colonna specifica. | • Una ricerca di `[Max speed] > 28` restituisce risultati che contengono un numero superiore a 28 nella colonna Velocità massima.<br>• Una ricerca di `[Average speed] < = 28` restituisce risultati che contengono un numero inferiore o uguale a 28 nella colonna Velocità media. |
| Utilizzare `CONTAINS` per eseguire una ricerca di testo in una colonna specifica. | • La ricerca di `[Cardholder] CONTAINS Oscar` restituisce dati in cui "Oscar" è nella colonna Titolare di tessera.<br>• La ricerca di `[Door] CONTAINS "door 1"` restituisce dati in cui "porta 1" è nella colonna porta. |
| Usa = per corrispondenze esatte in una colonna specifica. | Una ricerca di `[CardholderId] = ABC123` restituisce le corrispondenze dei risultati per "ABC123" solo nella colonna "Titolare della tessera". |

# Configurazione

Sulla scheda Configurazione si possono gestire i dispositivi collegati e configurare le impostazioni per il client e i server. Fare clic su + e selezionare **Configuration (Configurazione)** per aprire la scheda **Configuration (Configurazione)**.

## Configurazione dei dispositivi

In AXIS Camera Station Pro per dispositivo si intende un dispositivo di rete con un indirizzo IP. Il termine "telecamera" indica una sorgente video, come una telecamera di rete o una porta video (a cui è connessa una telecamera analogica) su un codificatore video multiporta. Ad esempio, un codificatore video a 4 porte è un dispositivo con quattro telecamere.

Nota

- AXIS Camera Station Pro supporta solo dispositivi con indirizzi IPv4.
- alcuni codificatori video hanno un indirizzo IP per ogni porta video. In tal caso, AXIS Camera Station Pro tratta ogni porta video come un dispositivo con una telecamera.

In AXIS Camera Station Pro un dispositivo può essere:

- Una videocamera di rete.
- Un codificatore video con una o più porte video.
- Un dispositivo ausiliario non telecamera, ad esempio un dispositivo audio I/O, un altoparlante di rete o un controller per porte.
- Un interfono.

Da qui è possibile:

- Aggiungere telecamere e dispositivi senza funzionalità video. Vedere *Aggiungi dispositivi*.
- Modificare le preferenze delle telecamere collegate. Vedere *Telecamere*.
- Modificare le preferenze dei dispositivi non telecamera. Vedere *Altri dispositivi*.
- Modificare i profili di streaming per impostare risoluzione, formato e altro ancora. Vedere *Profili di flusso*.
- Apportare modifiche alle impostazioni dell'immagine in tempo reale. Vedere *Configurazione immagine*.
- Aggiungere o rimuovere preset PTZ. Vedere *Configurazione PTZ*.
- Gestire e mantenere i dispositivi connessi. Vedere *Gestione dei dispositivi*.
- Gestisci origini di dati esterne. Vedere *Origini di dati esterne, on page 73*.

### Aggiungi dispositivi

Nota

- Il sistema considera le aree di visione come telecamere singole. È necessario creare aree di visione nella telecamera prima di poterle utilizzare. Vedere *Utilizzo delle aree di visione*.
- Quando si aggiunge un dispositivo, il dispositivo sincronizza l'ora con il server AXIS Camera Station Pro.
- Raccomandiamo di non impiegare caratteri speciali come å, ä e ö nel nome host di un dispositivo.

1. Trovare i dispositivi, i flussi video o i video preregistrati.
   - *Trova i dispositivi, on page 49*
   - *Trova i tuoi flussi video, on page 49*
   - *Trovare video preregistrati, on page 50*
2. *Aggiungere dispositivi, flussi video, o video preregistrati, on page 50*

Vanno risolti eventuali problemi visualizzati nella colonna dello stato del dispositivo prima che si possa eseguire l'aggiunta di un dispositivo.

| | |
|---|---|
| **(vuoto)** | Se non c'è alcuno stato, è possibile aggiungere il dispositivo a AXIS Camera Station Pro. |
| **Communicating (Comunicazione)** | AXIS Camera Station Pro server cerca di accedere al dispositivo. |
| **Certificato dispositivo non attendibile:** | AXIS Camera Station Pro non è in grado di verificare che il certificato HTTPS sul dispositivo sia firmato da un'autorità emittente attendibile. Fare clic sul link per emettere un nuovo certificato HTTPS o indicare AXIS Camera Station Pro per affidarsi a quello esistente. |
| **L'autorità di certificazione è scaduta** | L'autorità di certificazione che ha emesso il certificato del dispositivo non è più valida. Fare clic sul link per emettere un nuovo certificato HTTPS o indicare AXIS Camera Station Pro per affidarsi a quello esistente. |
| **Indirizzo nel certificato del dispositivo non corrispondente** | L'indirizzo del dispositivo non corrisponde a quello del certificato. Fare clic sul link per emettere un nuovo certificato HTTPS o indicare AXIS Camera Station Pro per affidarsi a quello esistente. |
| **Errore di comunicazione** | AXIS Camera Station Pro non riesce a contattare il dispositivo. |
| **inserire la password** | AXIS Camera Station Pro non conosce le credenziali da utilizzare per accedere al dispositivo. Fare clic sul collegamento per immettere un nome utente e una password per un account amministratore del dispositivo. Per impostazione predefinita, AXIS Camera Station Pro utilizzerà il nome utente e la password immessi per tutti i dispositivi su cui è presente l'utente. |
| **Impostazione della password** | L'account e la password root non sono impostati o il dispositivo utilizza ancora la password predefinita. Fare clic sul collegamento per impostare la password utente root.<br>• Inserire la password o fare clic su **Generate (Genera)** per ottenere una password. Si consiglia di salvare una copia della password generata.<br>• Selezionare per utilizzare questa password for tutti i dispositivi con lo stato `Set password`.<br>• Se il dispositivo applica dei criteri password, un indicatore di criteri password mostrerà se la password soddisfa i requisiti. Vedere *Gestione degli utenti, on page 67* per ulteriori informazioni. |
| **Modello non supportato** | AXIS Camera Station Pro non supporta il modello del dispositivo. |
| **Firmware obsoleto** | Il firmware del dispositivo non è aggiornato. Aggiornare prima di aggiungere un dispositivo. |

| | |
|---|---|
| **Dispositivo malfunzionante** | I parametri del dispositivo recuperati da AXIS Camera Station Pro sono corrotti. |
| **Imposta orientamento inclinazione** | Fare clic sul collegamento per selezionare l'orientamento dell'inclinazione: A soffitto, A parete o Su tavolo a seconda della posizione di montaggio della telecamera. In alcuni modelli di telecamera è necessario impostare l'orientamento dell'inclinazione. |
| **Dispositivo ONVIF non supportato** | AXIS Camera Station Pronon supporta questo dispositivo di terze parti. |
| **Dispositivo non supportato** | AXIS Camera Station Pro non supporta questo tipo di dispositivo. |

Nota

I nuovi certificati HTTPS sono emessi da AXIS Camera Station Pro e si rinnovano automaticamente.

**Trova i dispositivi**

Per trovare dispositivi non elencati:

1. Andare a **Configuration > Devices > Add devices** (Configurazione, Dispositivi, Aggiungi dispositivi).
2. Fare clic su **Annulla** per interrompere la ricerca in corso nella rete.
3. Fare clic su **Manual search (Ricerca manuale)**.
4. Per trovare più dispositivi in uno o più intervalli IP:
   4.1. Seleziona **Search one or more IP ranges (Cerca uno o più intervalli IP)**.
   4.2. Digitare l'intervallo di indirizzi IP. Ad esempio puoi: 192.168.10.*, 192.168.20-22.*, 192.168.30.0-50
      – Utilizzare un carattere jolly per tutti gli indirizzi di un gruppo.
      – Utilizzare un trattino per un intervallo di indirizzi.
      – Per separare più intervalli utilizzare una virgola.
   4.1. Per cambiare la porta 80 predefinita, digitare l'intervallo di porta. Ad esempio puoi: 80, 1080-1090
      – Utilizzare un trattino per un intervallo di porte.
      – Per separare più intervalli utilizzare una virgola.
   4.1. fare clic su **Cerca**;
5. Per trovare uno o più dispositivi specifici:
   5.1. Selezionare **Enter one or more hostnames or IP addresses (Immettere uno o più nomi host o indirizzi IP)**.
   5.2. Immettere i nomi host o gli indirizzi IP separati da una virgola.
   5.3. fare clic su **Cerca**;
6. Fare clic su **OK**.

**Trova i tuoi flussi video**

È possibile aggiungere flussi video che supportano quanto segue:

- Protocollo: RTSP, HTTP, HTTPS
- Codifica video: M-JPEG per HTTP e HTTPS, H.264 per RTSP
- Codifica audio: AAC e G.711 per RTSP

Schemi URL flusso video supportati:

- `rtsp://<address>:<port>/<path>`
  Ad esempio: `rtsp://<address>:554/axis-media/media.amp`
- `http://<address>:80/<path>`
  Ad esempio: `http://<address>:80/axis-cgi/mjpg/video.cgi?date=1&clock=1&resolution=1920x1080`
- `https://<address>:443/<path>`
  Ad esempio: `https://<address>:443/axis-cgi/mjpg/video.cgi?date=1&clock=1&resolution=1920x1080`

1. Andare a **Configuration > Devices > Add devices** (Configurazione, Dispositivi, Aggiungi dispositivi).
2. Fare clic su **Enter stream URLs (Inserisci URL flusso)** e immettere uno o più URL di flusso separati da una virgola.
3. Fare clic su **Aggiungi**.

**Trovare video preregistrati**

È possibile aggiungere video preregistrati nel formato .mkv a AXIS Camera Station Pro.

Requisiti:

- Codifica video: M-JPEG, H.264, H.265
- Codifica audio: AAC

1. Creare una cartella **PrerecordedVideos** in `C:\ProgramData\Axis Communications\AXIS Camera Station Server`.
2. Aggiungere un file .mkv alla cartella.
3. Per eliminare la distorsione del video preregistrato, aggiungere un file .dewarp con lo stesso nome del file .mkv alla cartella. Per ulteriori informazioni, vedere *Configurazione immagine, on page 59*.
4. Andare a **Configuration > Devices > Add devices (Configurazione > Dispositivi > Aggiungere dispositivi)** e attivare **Include prerecorded video (Includi video preregistrati)**.
   Puoi individuare i tuoi video preregistrati nonché vari video preregistrati messi a disposizione dal sistema.

**Aggiungere dispositivi, flussi video, o video preregistrati**

1. In un sistema multi-server, selezionare un server dall'elenco a discesa **Selected server (Server selezionato)**.
2. Andare a **Configuration > Devices > Add devices** (Configurazione, Dispositivi, Aggiungi dispositivi).
3. Selezionare i dispositivi, i flussi video o i video preregistrati. Fare clic su **Aggiungi**.
4. Fare clic su **Close (Chiudi)** per saltare la configurazione e proseguire in un secondo momento. Per proseguire con la configurazione:
   4.1. Scegliere **Quick configuration (Configurazione rapida)** per configurare le impostazioni di base. Se si sta importando un progetto di AXIS Site Designer, scegliere **Site Designer configuration (Configurazione Site Designer)**. Per ulteriori informazioni, vedere *Importazione di progetti AXIS Site Designer*.
   4.2. Selezionare **Add image overlay for date, time, and text (Aggiungi sovrapposizione di immagine per data, ora e testo)** per aggiungere sovrapposizioni a alla telecamera Axis che non ne dispone già.
   4.3. Fare clic su **Next (Avanti)**.
   4.4. Selezionare la preferenza del **Recording method** (Metodo di registrazione).
   4.5. Fare clic su **Next (Avanti)**.

4.6. Scegliere **Retention time (Tempo di archiviazione)** e **Recording storage (Archiviazione registrazione)** e fare clic su **Finish (Fine)** per applicare la configurazione.

**Importazione di progetti AXIS Site Designer**

AXIS Site Designer è uno strumento di progettazione online che consente di realizzare un sito con dispositivi e accessori Axis.

Se è stato creato un sito in AXIS Site Designer, si possono importare le impostazioni di progetto in AXIS Camera Station Pro. Si può accedere al progetto usando un codice di accesso o un file di configurazione scaricato.

Per importare un progetto di AXIS Site Designer in AXIS Camera Station Pro:

1. Generare un codice di accesso o scaricare un file di progetto:
   1.1. Accedere alla pagina *http://sitedesigner.axis.com* con l'account My Axis.
   1.2. Selezionare un progetto e andare alla pagina del progetto.
   1.3. Fare clic su **Share (Condividi)**.
   1.4. Fare clic su **Generate code (Genera codice)** se il server AXIS Camera Station Pro dispone di una connessione a internet, oppure fare clic su **Download settings file (Scarica file delle impostazioni)** in caso contrario.
2. Nel client AXIS Camera Station Pro andare a **Configuration > Devices > Add devices (Configurazione > Dispositivi > Aggiungi dispositivi)**.
3. Selezionare i dispositivi e fare clic su **Add** (Aggiungi).
4. Selezionare **Configurazione di Site Designer** e fare clic su **Avanti**.
5. Selezionare **Codice di accesso** e immettere il codice di accesso. Per utilizzare invece il file di impostazione scaricato, selezionare **Chose file (Scegli file)**.
6. Fare clic su **Import (Importa)**. AXIS Camera Station Pro tenta di associare il progetto ai dispositivi selezionati in base all'indirizzo IP o al nome del prodotto. Se la corrispondenza non va a buon fine, selezionare i dispositivi corretti dal menu a discesa.
7. Fare clic su **Next (Avanti)**.
8. Selezionare la preferenza del **Recording method** (Metodo di registrazione). Queste impostazioni si applicano alle telecamere che non corrispondono alla configurazione del progetto.
9. Fare clic su **Next (Avanti)**.
10. Scegliere **Retention time (Tempo di archiviazione)** e **Recording storage (Archiviazione registrazione)** e fare clic su **Finish (Fine)** per applicare la configurazione.

AXIS Camera Station Pro importa le seguenti impostazioni dal progetto di AXIS Site Designer:

| | Codificatori, decodificatori video, door controller, rilevatori radar e altoparlanti | Telecamere, interfoni e serie F/FA |
|---|---|---|
| Pianificazioni con nome e intervalli di tempo | ✓ | ✓ |
| Mappe con nome, colore dell'icona, ubicazione dell'icona e nome dell'elemento | ✓ | ✓ |
| Nome | ✓ | ✓ |
| Descrizione | ✓ | ✓ |
| Registrazione continua: profilo di registrazione e pianificazione inclusi velocità di trasmissione, | | ✓ |

| | Codificatori, decodificatori video, door controller, rilevatori radar e altoparlanti | Telecamere, interfoni e serie F/FA |
|---|---|---|
| risoluzione, codifica video e compressione | | |
| Motion triggered recording (Registrazione attivata da movimento): profilo di registrazione e pianificazione inclusi velocità di trasmissione, risoluzione, codifica video e compressione | | ✓ |
| Intensità Zipstream: | | ✓ |
| Impostazioni audio per la visualizzazione e le registrazioni in diretta | | ✓ |
| Tempo di conservazione per le registrazioni | | ✓ |

Nota

- Se è stato definito unicamente uno dei profili di registrazione o se ci sono due profili di registrazione identici nel progetto di AXIS Site Designer, AXIS Camera Station Pro imposta il profilo come medio.
- Nel caso entrambi i profili di registrazione siano stati definiti nel progetto di AXIS Site Designer, AXIS Camera Station Pro imposta il profilo di registrazione continua come medio e la registrazione attivata dal movimento come alta.
- AXIS Camera Station Pro ottimizza le proporzioni, pertanto la risoluzione potrebbe differire da quella del progetto di AXIS Site Designer.
- AXIS Camera Station Pro può impostare le impostazioni audio se il dispositivo ha un microfono o un altoparlante incorporato. Per utilizzare un dispositivo audio esterno, renderlo attivo dopo l'installazione.
- AXIS Camera Station Pro non applica impostazioni audio ai citofoni, anche se le impostazioni in AXIS Site Designer sono diverse. Sui intercom, l'audio è sempre attivo, ma solo nella visualizzazione in diretta.

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

**Aggiunta di dispositivi di terze parti**

È possibile aggiungere dispositivi di terze parti ad AXIS Camera Station Pro allo stesso modo dei dispositivi Axis. Vedere *Aggiungi dispositivi*.

Nota

È inoltre possibile aggiungere dispositivi di terze parti come flussi video ad AXIS Camera Station Pro. Vedere *Trova i tuoi flussi video, on page 49*.

AXIS Camera Station Pro supporta le seguenti funzioni per i dispositivi di terze parti in base alle norme IEC62676-2-31 e IEC62676-2-32:

- Individuazione della telecamera

- Codifica video: M-JPEG, H.264
- Codifiche audio: G.711 (unidirezionale, dal dispositivo ad AXIS Camera Station Pro)
- Un profilo video per telecamera
- Visualizzazione in diretta
- Registrazioni continue e manuali
- Riproduzione
- Registrazione delle esportazioni
- Trigger evento dispositivo
- PTZ

**Utilizzo delle aree di visione**

Alcuni modelli di telecamera supportano le aree di visione. AXIS Camera Station Pro elenca le aree di visione come telecamere singole nella pagina **Add devices (Aggiungi dispositivi)**. Vedere *Aggiungi dispositivi*.

Nota

- Tutte le aree di visione in una telecamera di rete vengono considerate come singola telecamera nel numero totale di telecamere consentito dalla licenza di AXIS Camera Station Pro.
- Il numero di telecamere che è possibile aggiungere dipende dalla licenza.

Per impiegare le aree di visione in AXIS Camera Station Pro, è necessario prima abilitarle nella telecamera:

1. Andare a **Configurazione > Dispositivi > Telecamere**.
2. Selezionare la telecamera e fare clic sul collegamento nella colonna Indirizzo.
3. Inserire il nome utente e la password per eseguire l'accesso nella pagina di configurazione della telecamera.
4. Fare clic su **Help (Guida)** per ricevere istruzioni su dove trovare le impostazioni. L'ubicazione varia a seconda del modello della telecamera e del firmware.

## Sostituire un dispositivo

Si può eseguire la sostituzione di un dispositivo e mantenere la configurazione e le registrazioni esistenti. Il numero di flussi video configurati nella nuova telecamera deve essere uguale a quello precedente.

Per la sostituzione di un dispositivo:

1. Aggiungere il dispositivo sostitutivo ad AXIS Camera Station Pro.
2. Se il dispositivo da sostituire utilizza l'archiviazione cloud, andare in **Cloud storage (Archiviazione cloud)** in My Systems e disattivare l'archiviazione cloud per il dispositivo.
3. Aprire una scheda **Configuration (Configurazione)** e andare a **Devices (Dispositivi)** > **Management (Gestione)**.
4. Selezionare il dispositivo che si vuole sostituire e fare clic su .
5. Nella finestra di dialogo **Replace device (Sostituzione dispositivo)**, selezionare il dispositivo con cui si vuole sostituire quello precedente.
6. Fare clic su **Finish (Fine)**.
7. Viene visualizzata la finestra di dialogo **Replaced device (Dispositivo sostituito)** per confermare che il dispositivo è stato sostituito con successo. Fare clic su **OK**.
8. Se il dispositivo sostituito utilizzava l'archiviazione cloud, riavviare il servizio sul server AXIS Camera Station Pro. Quindi attivare l'archiviazione su cloud per il dispositivo nella sezione My Systems. Vedere *Attivazione dell'archiviazione su cloud per le singole telecamere*.

9. Verificare la configurazione del nuovo dispositivo per controllare che le impostazioni siano corrette e che funzioni correttamente. Se applicabile:
   9.1. Riconfigurare i preset PTZ sul dispositivo.
   9.2. Aggiungere le porte I/O rimosse e aggiornare le relative regole di azione.
   9.3. Riconfigurare le impostazioni di movimento se la vecchia telecamera utilizzava il rilevamento di oggetti in movimento nel video integrato invece dell'applicazione ACAP per il rilevamento degli oggetti in movimento nel video.
   9.4. Inserire una scheda di memoria o disattivare **Failover recording (Registrazione failover)** nelle impostazioni di selezione dell'archiviazione se la vecchia telecamera utilizzava la registrazione failover.

## Telecamere

Andare a **Configuration > Devices > Cameras (Configurazione, Dispositivi, Telecamere)** per vedere l'elenco di tutte le telecamere aggiunte nel sistema.

Su questa pagina è possibile:

- Fare clic sull'indirizzo di una telecamera per aprirne l'interfaccia web. Ciò richiede che non siano presenti un NAT né un firewall tra il client AXIS Camera Station Pro e il dispositivo.
- Modifica le impostazioni della videocamera. Vedere *Modifica delle impostazioni della telecamera*.
- Rimuovere telecamere. In questo modo vengono eliminate anche tutte le registrazioni associate alle telecamere eliminate, comprese quelle con blocco.

### Modifica delle impostazioni della telecamera

Per modificare le impostazioni della telecamera:

1. Andare a **Configurazione > Dispositivi > Telecamere**.
2. Selezionare una telecamera e fare clic su **Modifica**.

| | |
|---|---|
| **Abilitato** | Per far sì che il flusso video non sia registrato e visualizzato, deselezionare **Enabled (Abilitato)**. Si possono comunque configurare la registrazione e la visualizzazione in diretta. |
| **Canale** | Quando **Channel (Canale)** è disponibile per i video encoder multiporta, selezionare il numero di porta.<br><br>Quando **Channel (Canale)** è disponibile per le aree di visione, selezionare il numero che corrisponde all'area di visione. |

## Altri dispositivi

Andare a **Configuration > Devices > Other devices (Configurazione, Dispositivi, Altri dispositivi)**, per vedere un elenco di dispositivi senza funzionalità video. Questa lista comprende door controller, dispositivi audio e moduli I/O.

Per informazioni sui dispositivi supportati, visitare *www.axis.com*. Vedere *Utilizzo dell'audio da altri dispositivi*.

Su questa pagina è possibile:

- Fare clic sull'indirizzo di un dispositivo per aprirne l'interfaccia web. Ciò richiede che non siano presenti un NAT né un firewall tra il client AXIS Camera Station Pro e il dispositivo.
- Modificare le impostazioni del dispositivo come nome, indirizzo e password del dispositivo.
- Rimozione dei dispositivi.

### Modifica di impostazioni di altri dispositivi

Per cambiare il nome di un dispositivo non telecamera:

1. Andare a **Configurazione > Dispositivi > Altri dispositivi**.
2. Selezionare un dispositivo e fare clic su **Modifica**.
3. immettere il nuovo nome per il dispositivo.

## Profili di flusso

Un profilo di streaming è un gruppo di impostazioni che incidono sul flusso video, quali risoluzione, formato video, velocità in fotogrammi e compressione. Andare a **Configuration > Devices > Stream profiles (Configurazione, Dispositivi, Profili di streaming)** per aprire la pagina **Stream profiles (Profili di streaming)**. La pagina visualizza una lista di tutte le telecamere.

Nella visualizzazione in diretta e nelle impostazioni delle registrazioni sono disponibili i seguenti profili:

**Alta –** Ottimizzato per la massima qualità e risoluzione.

**Medio –** Ottimizzato per bilanciare l'alta qualità con le prestazioni.

**Bassa –** Ottimizzato per le prestazioni.

Nota

Per impostazione predefinita, il profilo di streaming è impostato su **Automatic (Automatico)** sia nella visualizzazione in diretta che nelle registrazioni. Il profilo di streaming cambia automaticamente in **High (Alto)**, **Medium (Medio)**, o **Low (Basso)** in funzione delle dimensioni disponibili per lo streaming video.

### Profili di flusso sulla telecamera

AXIS Camera Station Pro aggiunge automaticamente i profili di streaming alla videocamera per aiutarti nell'impostazione delle regole di registrazione direttamente sulla videocamera stessa. I profili sono visibili nell'interfaccia web della telecamera nella sezione **Stream profiles (Profili di streaming)** e prendono il nome dalla telecamera e dal livello del profilo, ad esempio "Camera 1_ACS_Pro_High".

I profili presenti sulla telecamera vengono aggiunti o aggiornati quando:

- È stata aggiunta una telecamera su AXIS Camera Station Pro.
- I profili dei flussi sono modificati in AXIS Camera Station Pro.
- Si esegue l'aggiornamento notturno.

Quando una telecamera viene rimossa da AXIS Camera Station Pro, i profili di streaming creati da AXIS Camera Station Pro vengono eliminati dalla telecamera.

Nota

I profili di streaming nei formati M-JPEG o MPEG-4 non vengono aggiunti alla telecamera.

### Modifica profili di streaming

1. Andare a **Configuration > Devices > Stream profiles (Configurazione > Dispositivi > Profili di streaming)** e selezionare le telecamere che si vogliono configurare.
2. In **Video profiles (Profili video)**, configurare risoluzione, formato video, velocità in fotogrammi e compressione.
3. In **Audio**, configurare il microfono e l'altoparlante.
4. In **Advanced (Avanzate)**, configurare dati di analisi, streaming FFmpeg, indicatori oggetti tracking automatico PTZ e impostazioni di streaming personalizzate. Queste impostazioni non sono a disposizione per tutti i dispositivi.
5. fare clic su **Applica**;

### Profili video

| | |
|---|---|
| **Codificatore** | • Le opzioni a disposizione dipendono dalle configurazioni del video encoder sul dispositivo. Disponibile solo per dispositivi di terze parti.<br>• Si può usare una sola configurazione di video encoder per un profilo video.<br>• Se il dispositivo ha una sola configurazione del codificatore, è disponibile solo il profilo **Medium (Medio)**. |
| **Risoluzione** | Le opzioni disponibili dipendono dal modello di videocamera. Una risoluzione più elevata fornisce un'immagine con più dettagli, ma richiede una maggiore larghezza di banda e più spazio sul dispositivo. |
| **Formatta** | Le opzioni disponibili dipendono dal modello di videocamera. La maggior parte delle fotocamere supporta i formati **H.264** e **JPEG**. H.264 richiede meno larghezza di banda e spazio di archiviazione rispetto all'M-JPEG. Alcune telecamere supportano anche **lo standard H.265**, che offre una compressione leggermente migliore ma richiede una maggiore potenza di elaborazione. Le nostre telecamere di ultima generazione supportano il formato AV1, che offre una buona compressione e una serie di nuove funzioni, come le sovrapposizioni togglable.<br>Per ulteriori informazioni su AV1, consultare la *pagina del prodotto AV1*.. Per controllare se la telecamera supporta AV1, consultare *compatible cameras page*. (pagina telecamere compatibili). |
| **Frequenza fotogrammi** | L'effettiva frequenza dei fotogrammi dipende dal modello di telecamera, dalle condizioni di rete e dalla configurazione del computer. |
| **Compressione** | Una compressione più bassa migliora la qualità di immagine, tuttavia richiede una maggiore larghezza di banda e più spazio sul dispositivo. |

Nota

- Solo le telecamere con firmware 5 e superiore vengono visualizzate negli elenchi a discesa audio.
- Se più di 5 telecamere utilizzano la stessa sorgente audio, la telecamera sorgente potrebbe sovraccaricarsi e funzionare con minore efficienza.

**Zipstream**

| | | | |
|---|---|---|---|
| **Intensità** | L'intensità di Zipstream stabilisce il livello di riduzione della velocità in bit in un flusso H.264 o H.265 in tempo reale. Questa opzione è disponibile solo per i dispositivi Axis che supportano Zipstream. | **Ripristino dei valori predefiniti di fabbrica** | Utilizzare l'impostazione Zipstream configurata tramite la pagina dell'interfaccia web del dispositivo. |
| | | **Off** | Nessuno |
| | | **Bassa** | Nessun effetto visibile nella maggior parte delle scene. |
| | | **Medio** | Effetto percepibile in alcune scene: minore rumore e livello di dettagli leggermente inferiore nelle regioni di minore interesse. |

| | | | |
|---|---|---|---|
| | | **Alta** | Effetto percepibile in molte scene: minore rumore e livello di dettagli inferiore nelle regioni di minore interesse. |
| | | **Superiore** | Effetto visibile in ancora più scene: minore rumore e livello di dettagli inferiore nelle regioni di minore interesse. |
| | | **Estremo** | Effetto visibile nella maggior parte delle scene: minore rumore e livello di dettagli inferiore nelle regioni di minore interesse. |
| **Ottimizza per archiviazione** | Zipstream esegue l'ottimizzazione del flusso video per l'archiviazione usando il profilo **Optimize for storage (Ottimizza per archiviazione)**. Questo profilo utilizza strumenti di compressione avanzata per ridurre l'uso dello spazio di archiviazione oltre l'impostazione Sipstream predefinita e può ridurre ulteriormente la velocità in bit anche per le scene con molto movimento.<br>• Il formato asf non supporta i B-frame utilizzati da questa funzione.<br>• Questa funzione non influisce sui video registrati su registratori della serie AXIS S30.<br>• Questa funzione richiede AXIS OS 11.7.59 o successivo. | | |

**Audio**

| | |
|---|---|
| **Microfono:** | Per associare un microfono alla telecamera, selezionare **Built-in microphone or line in (Microfono incorporato o ingresso linea)** o un microfono di un altro dispositivo. Vedere *Utilizzo dell'audio da altri dispositivi*. |
| **Speaker (Altoparlante):** | Per associare un altoparlante alla telecamera, selezionare **Built-in speaker or line out (Altoparlante incorporato o uscita linea)** o un altoparlante di un altro dispositivo. Per effettuare annunci, utilizzare un microfono collegato al computer. Vedere *Utilizzo dell'audio da altri dispositivi*. |
| **Usa microfono per:** | Attivare l'audio del microfono per uno o due flussi. Si può attivare l'audio per la visualizzazione dal vivo e le registrazioni, solo per la visualizzazione dal vivo o solo per la registrazione. |

Quando si è connessi ad AXIS Audio Manager Pro, è anche possibile selezionare i dispositivi audio dal server AXIS Audio Manager Pro come dispositivo audio associato a una telecamera. Per ulteriori informazioni, consultare *Configurare AXIS Audio Manager Pro, on page 173*.

**Avanzata**

| | |
|---|---|
| **Includi dati di analisi** | Per consentire di raccogliere dati per la ricerca intelligente durante lo streaming video, selezionare **Include analytics data (Includi dati di analisi)**. Disponibile solo per i dispositivi Axis che supportano i dati di analisi. La raccolta di dati per *Ricerca intelligente 1* può aggiungere latenza nello streaming video. |
| **Utilizza FFmpeg** | Per migliorare la compatibilità con dispositivi di terze parti, selezionare **Use FFmpeg (Utilizza FFmpeg)** per abilitare lo streaming FFmpeg. Disponibile solo per dispositivi di terze parti. |
| **Mostra indicatori oggetti rilevamento automatico PTZ** | Selezionare **Show PTZ autotracking object indicators (Mostra indicatori oggetti rilevamento automatico PTZ)** e impostare il tempo buffer del flusso video fino a 2.000 millisecondi per mostrare gli indicatori oggetti rilevati da una telecamera PTZ nella visualizzazione in diretta. Disponibile solo per le telecamere PTZ Axis dotate della funzione di tracking automatico AXIS PTZ. Vedere AXIS Camera Station ProImposta AXIS PTZ Autotracking *per un flusso di lavoro completo per l'impostazione di AXIS PTZ Autotracking in* . |
| **Personalizzazione del flusso** | Per eseguire la personalizzazione delle impostazioni di streaming per un profilo specifico, inserire le impostazioni separate da `&` per il profilo. Ad esempio, inserire `overlays=off&color=0` per nascondere le sovrapposizioni su quella telecamera.<br><br>Le impostazioni personalizzate sovrascrivono tutte quelle esistenti. Non includere informazioni riservate nelle impostazioni personalizzate. |

Per **personalizzare le impostazioni profilo** relative a risoluzione, velocità in fotogrammi, compressione, formato video e audio, selezionare la telecamera da configurare. Per le videocamere dello stesso modello con funzionalità di configurazione identiche, è possibile configurare più videocamere simultaneamente. Vedere *Impostazioni di configurazione*.

Per **personalizzare le impostazioni dei profili per le registrazioni**, vedere *Metodo di registrazione*.

Si può porre un **limite alla risoluzione e alla velocità in fotogrammi per la visualizzazione in diretta in modo da ridurre il consumo di banda**, ad esempio se la connessione tra il client AXIS Camera Station Pro e il server AXIS Camera Station Pro è lenta. Vedere l'uso della larghezza di banda in *Streaming*.

#### Utilizzo dell'audio da altri dispositivi

È possibile usare l'audio da un altro dispositivo, non telecamera o ausiliario, insieme al video di una telecamera di rete o di video encoder per la visualizzazione in diretta o per la registrazione.

1. Aggiungere il dispositivo non telecamera a AXIS Camera Station Pro. Vedere *Aggiungi dispositivi*.
2. Configurare la telecamera per usare l'audio del dispositivo. Vedere *Profili di flusso*.
3. Abilitare l'audio per visualizzazione in diretta o registrazione. Vedere *Profili di flusso*.

È possibile trovare i seguenti esempi nei *tutorial video di AXIS Camera Station Pro*:

- Configurazione dei dispositivi audio ed esecuzione degli annunci in diretta.
- Creare un pulsante di azione per riprodurre manualmente l'audio quando viene rilevato movimento.
- Riproduzione automatica dell'audio quando viene rilevato movimento.
- Aggiungere una clip audio all'altoparlante e AXIS Camera Station Pro.

### Configurazione immagine

È possibile configurare le impostazioni dell'immagine per le telecamere collegate ad AXIS Camera Station Pro.

Nota

Le modifiche alla configurazione delle immagini hanno effetto immediato.

#### Impostazioni immagini

Per configurare le impostazioni dell'immagine:

1. Andare a **Configuration > Devices > Image configuration (Configurazione, Dispositivi, Configurazione immagine)**. AXIS Camera Station Pro visualizza un elenco di tutte le telecamere aggiunte ad.
2. Selezionare la telecamera per visualizzare in tempo reale il flusso video sotto l'elenco. Utilizzare il campo **Digitare il testo per la ricerca** per trovare una telecamera specifica nell'elenco.
3. Fai clic sulla scheda **Image settings (Impostazioni immagine)** per configurare le impostazioni:

**La luminosità –** consente di regolare la luminosità dell'immagine. Un valore più elevato fornisce un'immagine più luminosa.

**Livello colore –** consente di regolare la saturazione del colore. Diminuendo il valore, viene ridotta la saturazione del colore. Il livello colore 0 fornisce un'immagine in bianco e nero. Il valore massimo darà la saturazione massima.

**Nitidezza –** consente di regolare la quantità di nitidezza applicata all'immagine. L'aumento della nitidezza può aumentare il disturbo dell'immagine, specialmente in caso di scarsa illuminazione. Un valore di nitidezza elevato può anche generare artefatti d'immagine attorno alle aree con contrasto elevato, ad esempio spigoli vivi. Valori di nitidezza inferiori riducono il disturbo dell'immagine, ma la rendono meno nitida.

**Contrasto –** consente di regolare il contrasto dell'immagine.

**Bilanciamento del bianco –** consente di selezionare l'opzione di bilanciamento del bianco nell'elenco a discesa. Il bilanciamento del bianco serve a garantire che i colori dell'immagine appaiano uniformi indipendentemente

dalla temperatura di colore della sorgente luminosa. Quando si seleziona **Automatico** o **Auto**, la telecamera identifica la sorgente luminosa e ne compensa il colore automaticamente. Se il risultato non soddisfa, selezionare un'opzione che corrisponda al tipo di sorgente luminosa. Le opzioni disponibili dipendono dal modello di videocamera.

**Ruota immagine –** consente di impostare i gradi di rotazione dell'immagine.

**Rotazione automatica dell'immagine –** Attivala per la regolazione in automatico della rotazione dell'immagine.

**Mirror image (Immagine speculare): –** abilitare questa impostazione per la specularità dell'immagine.

**Backlight compensation (Compensazione della retroilluminazione): –** Attivare questa opzione se una sorgente luminosa intensa, come una lampadina, fa apparire troppo scure altre aree dell'immagine.

**Dynamic contrast (wide dynamic range) (Contrasto dinamico – ampio intervallo dinamico) –** Attivare per migliorare l'esposizione quando c'è un notevole contrasto tra le aree di luce e di ombra nell'immagine. Utilizzare il cursore per regolare il livello. Disattivare in condizioni di bassa luminosità.

**Custom dewarp settings (Personalizza impostazioni dewarping): –** È possibile importare un file .dewarp contenente i parametri dell'obiettivo, i centri ottici e l'orientamento dell'inclinazione della telecamera. Fare clic su **Reset (Reimposta)** per ripristinare i valori originali dei parametri.

Per configurare le impostazioni personalizzate di correzione della distorsione:

1. Creare un file .dewarp contenente i seguenti parametri:
   - Richiesti: `RadialDistortionX`, `RadialDistortionY`, `RadialDistortionZ` e `TiltOrientation`. I valori possibili per `TiltOrientation` sono `wall`, `desk` e `ceiling`.
   - Opzione: `OpticalCenterX` e `OpticalCenterY`. Se si desidera impostare i centri ottici, è necessario includere entrambi i parametri.
2. Fare clic su **Import (Importa)** e accedere al file .dewarp.

Di seguito viene riportato un esempio di file .dewarp:

```
RadialDistortionX=-43.970703 RadialDistortionY=29.148499 RadialDistortionZ=715.732193
TiltOrientation=Desk OpticalCenterX=1296 OpticalCenterY=972
```

## Configurazione PTZ

Le operazioni Pan, Tilt e Zoom (PTZ) consentono la rotazione (spostamento a destra e sinistra), l'inclinazione (spostamento in alto o in basso) e lo zoom avanti o indietro.

Andare a **Configuration > Devices > PTZ configuration (Configurazione, Dispositivi, Configurazione PTZ)**. AXIS Camera Station Pro visualizza un elenco di telecamere che supportano PTZ. Per visualizzare tutti i preset disponibili per una telecamera, fare clic su di essa. Fare clic su **Refresh (Aggiorna)** per aggiornare l'elenco dei preset.

È possibile utilizzare PTZ con:

- telecamere PTZ, ovvero telecamere che dispongono di funzioni PTZ meccaniche incorporate
- Telecamere fisse con funzione PTZ digitale attiva.
- Telecamere ONVIF che supportano i preset PTZ.

La funzione PTZ digitale può essere attivata dalla pagina di configurazione integrata nella telecamera. Per ulteriori informazioni, consultare il manuale per l'utente della telecamera. Per aprire la pagina di configurazione, accedere alla pagina Gestione dei dispositivi, selezionare la telecamera e fare clic sul collegamento nella colonna **Address (Indirizzo)**.

È possibile eseguire la configurazione dei preset PTZ in AXIS Camera Station Pro e nella pagina di configurazione della telecamera. Si consiglia di configurare i preset PTZ in AXIS Camera Station Pro.

- Si può visualizzare unicamente il flusso all'interno del preset quando un preset è configurato nella pagina di configurazione della telecamera. Nella visualizzazione in diretta non è possibile visualizzare e registrare i movimenti PTZ.

- È possibile visualizzare il flusso completo della telecamera quando un preset PTZ è configurato in AXIS Camera Station Pro. I movimenti PTZ nella visualizzazione in diretta non sono visibili né vengono registrati.

Nota

Non è possibile utilizzare la funzione PTZ mentre la coda di controllo della telecamera è attiva. Per informazioni sulla coda di controllo e su come attivarla e disattivarla, consultare il manuale per l'utente della telecamera.

Per aggiungere una posizione predefinita:

1. Andare a **Configuration > Devices > PTZ (Configurazione > Dispositivi > PTZ)** e selezionare una telecamera nell'elenco.
2. Per le telecamere con PTZ meccanico, utilizzare i comandi PTZ per spostare la vista della telecamera nella posizione desiderata. Per le telecamere con PTZ digitale, utilizzare la rotellina del mouse per ingrandire e trascinare la vista della telecamera nella posizione desiderata.
3. Fare clic su **Aggiungi** e immettere il nome del nuovo preset.
4. Fare clic su **OK**.

- Per rimuovere una regola, selezionare la regola e fare clic su **Remove (Rimuovi)**. Questa operazione eliminerà il preset da AXIS Camera Station Pro e dalla telecamera.

## Gestione dei dispositivi

Gestione dei dispositivi fornisce strumenti per l'amministrazione e la manutenzione di dispositivi connessi ad AXIS Camera Station Pro.

Andare a **Configuration > Devices > Management (Configurazione, Dispositivi, Gestione)** per aprire la pagina **Manage devices (Gestisci dispositivi)**.

Se sono state impostate le verifiche automatiche per le nuove versioni firmware in *Impostazioni di aggiornamento firmware, on page 124*, appare un collegamento quando sono disponibili nuove versioni firmware per i dispositivi. Fare clic sul collegamento per aggiornare le versioni del firmware. Vedere *Aggiornare il firmware*.

Se sono state impostate le verifiche automatiche per le nuove versioni software in *Aggiorna AXIS Camera Station Pro, on page 129*, appare un collegamento quando è disponibile una nuova versione di AXIS Camera Station Pro. Fare clic sul collegamento per installare la nuova versione.

AXIS Camera Station Pro visualizza un elenco di tutti i dispositivi aggiunti. Utilizzare il campo **Digitare il testo per la ricerca** per trovare dispositivi nell'elenco. Per nascondere o visualizzare le colonne, fare clic con il pulsante destro del mouse nella riga dell'intestazione e selezionare quali colonne mostrare. Trascinare la selezione delle intestazioni per visualizzare le colonne con un ordine diverso.

L'elenco dei dispositivi include le seguenti informazioni:

- **Name (Nome):** il nome del dispositivo o un elenco di tutti i nomi delle telecamere associate quando il dispositivo è un video encoder con più telecamere collegate o una telecamera di rete con più aree di visione.
- **MAC address (Indirizzo MAC):** l'indirizzo MAC del dispositivo.
- **Status (Stato):** lo stato del dispositivo.
  - **OK:** Lo stato normale di una connessione a un dispositivo.
  - **Maintenance (Manutenzione):** il dispositivo è in fase di manutenzione e temporaneamente non accessibile.
  - **Not accessible (Non accessibile):** Impossibile stabilire una connessione con il dispositivo.
  - **Not accessible over set hostname (Non accessibile tramite il nome host specificato):** non è possibile stabilire una connessione con il dispositivo tramite il suo nome host.

- **Server not accessible (Server non accessibile):** impossibile stabilire una connessione con il server a cui è connesso il dispositivo.
- **Enter password (Inserisci password):** non è possibile accedere al dispositivo finché non vengono inserite credenziali valide. Fare clic sul collegamento per fornire credenziali utente valide. Se il dispositivo supporta connessioni crittografate, la password viene inviata crittografata per impostazione predefinita.
- **Set password (Imposta password):** l'account e la password root non sono impostati o il dispositivo utilizza ancora la password predefinita. Fare clic sul collegamento per impostare la password utente root.
  - Digitare la password oppure fare clic su **Generate (Genera)** per generare automaticamente una password fino alla lunghezza consentita dal dispositivo. Si consiglia di salvare una copia della password generata.
  - Scegli di utilizzare questa password per tutti i dispositivi con lo stato `Set password`.
  - Selezionare **Enable HTTPS (Abilita HTTPS)** per abilitare HTTPS se il dispositivo lo supporta.
- **Password type: unencrypted (Tipo password non criptata):** non viene stabilita una connessione con il dispositivo poiché il dispositivo è stato precedentemente connesso utilizzando una password crittografata. Per motivi di sicurezza, AXIS Camera Station Pro non consente l'uso di password non crittografate per i dispositivi che hanno utilizzato precedentemente password crittografate. Per i dispositivi che supportano la crittografia, il tipo di connessione viene configurato nella pagina di configurazione del dispositivo.
- **Access blocked (Accesso bloccato):** il dispositivo ha temporaneamente bloccato l'accesso a seguito di un numero eccessivo di tentativi di accesso non riusciti.
- **Certificate error (Errore di certificato):** si è verificato un errore relativo al certificato presente sul dispositivo.
- **Certificate about to expire (Il certificato sta per scadere):** il certificato del dispositivo sta per scadere.
- **Certificate has expired (Certificato scaduto):** il certificato del dispositivo è scaduto.
- **HTTPS certificate not trusted (Certificato HTTPS non attendibile):** il certificato HTTPS presente sul dispositivo non è considerato attendibile da AXIS Camera Station Pro. Fare clic sul collegamento per emettere un nuovo certificato HTTPS.
- **HTTP failed (HTTP non raggiungibile):** Impossibile stabilire una connessione HTTP con il dispositivo.
- **HTTPs failed (HTTPs non raggiungibile):** impossibile stabilire una connessione HTTPS con il dispositivo.
- **Errore HTTP e HTTPS (ping o UDP OK):** impossibile stabilire una connessione HTTP e HTTPS con il dispositivo. Il dispositivo risponde al ping e alla comunicazione UDP (User Datagram Protocol).

- **Address (Indirizzo):** l'indirizzo del dispositivo. Fare clic sul collegamento per accedere alla pagina di configurazione del dispositivo. Mostra l'indirizzo IP o il nome host, a seconda di quale viene utilizzato quando si aggiunge il dispositivo. Vedere *Scheda Configurazione dispositivi, on page 73*.
- **Hostname (Nome host):** il nome host del dispositivo, se disponibile. Fare clic sul collegamento per accedere alla pagina di configurazione del dispositivo. Il nome host visualizzato è il nome completo del dominio. Vedere *Scheda Configurazione dispositivi, on page 73*.
- **Manufacturer (produttore):** la casa produttrice del dispositivo.
- **Model (Modello):** il modello del dispositivo.
- **Firmware:** la versione del firmware attualmente usata dal dispositivo.
- **DHCP:** mostra se il dispositivo è connesso al server mediante DHCP.
- **HTTPS:** lo stato HTTPS del dispositivo. Vedere Stato HTTPS in *Sicurezza, on page 70*.
- **IEEE 802.1X:** lo stato IEEE 802.1X del dispositivo. Vedere Stato IEEE 802.1X in *Sicurezza, on page 70*.

- **Server:** il server AXIS Camera Station Pro al quale è connesso il dispositivo.
- **Tag:** le etichette aggiunte al dispositivo (nascoste per impostazione predefinita).
- **UPnP Friendly Name:** il nome UPnP (nascosto per impostazione predefinita). Si tratta di un nome descrittivo utilizzato per facilitare l'identificazione del dispositivo.

È possibile effettuare le seguenti azioni sui dispositivi:

- assegnazione dell'indirizzo IP ai dispositivi. Vedere *Assegnazione di un indirizzo IP*.
- Imposta password per dispositivi. Vedere *Gestione degli utenti*.
- Aggiornare il firmware per i dispositivi. Vedere *Aggiornare il firmware*.
- Riavvia dispositivi.
- Ripristina dispositivi: ripristina la maggior parte delle impostazioni alle impostazioni predefinite di fabbrica, compresa la password. Le seguenti impostazioni non vengono ripristinate: applicazioni per telecamera caricate, protocollo di boot (DHCP o statico), indirizzo IP statico, router predefinito, subnet mask e ora di sistema.

Nota

- Per impedire accessi non autorizzati, impostare sempre una nuova password dopo aver ripristinato un dispositivo.
- Se il dispositivo da resettare utilizza l'archiviazione cloud, andare in **Cloud storage (Archiviazione cloud)** in My Systems e disattivare l'archiviazione cloud per il dispositivo prima di resettarlo. Una volta ripristinato il dispositivo, riavviare il servizio sul proprio server AXIS Camera Station Pro e attivare l'archiviazione cloud per il dispositivo in My Systems. Vedere *Attivazione dell'archiviazione su cloud per le singole telecamere*.
- Installazione dell'applicazione per telecamera sui dispositivi. Vedere *Installare le applicazioni per telecamera*.
- Aggiornare i dispositivi dopo aver effettuato una modifica delle impostazioni dalla pagina di configurazione del dispositivo.
- Configurazione dei dispositivi. Vedere *Configurazione dei dispositivi*.
- Gestione degli utenti. Vedere *Gestione degli utenti*.
- Gestione certificati. Vedere *Sicurezza, on page 70*.
- Raccolta dei dati dei dispositivi. Vedere *Raccolta dei dati dei dispositivi*.
- Selezionare per utilizzare l'indirizzo IP o il nome host. Vedere *Connessione, on page 72*.
- Etichetta dispositivi. Vedere *Tag*.
- Immissione delle credenziali del dispositivo. Fare clic con il pulsante destro del mouse su un dispositivo e selezionare **Advanced > Enter device credentials (Avanzate, Immettere credenziali dispositivo)** per immettere la password del dispositivo.
- Via alla scheda di configurazione del dispositivo e configura il tuo dispositivo. Vedere *Scheda Configurazione dispositivi, on page 73*.

### Assegnazione di un indirizzo IP

AXIS Camera Station Pro può assegnare un indirizzo IP a più dispositivi. È possibile ottenere automaticamente nuovi indirizzi IP da un server DHCP oppure assegnarli attingendo a un range di indirizzi IP.

#### Assegnazione degli indirizzi IP

1. Andare a **Configurazione > Dispositivi > Gestione** e selezionare i dispositivi da configurare.
2. Fare clic su oppure fare clic con il pulsante destro del mouse e selezionare **Assign IP address (Assegna indirizzo IP)**.

3. Se non è possibile configurare alcuni dei dispositivi selezionati, ad esempio perché è impossibile accedervi, verrà visualizzata la finestra di dialogo Dispositivi non validi. Fare clic su **Continue (Continue)** per saltare i dispositivi che non possono essere configurati.
4. Se si seleziona un dispositivo a cui assegnare un indirizzo IP, fare clic su **Advanced (Avanzate)** per aprire la pagina **Assign IP address (Assegna indirizzo IP)**.
5. Selezionare **Assegnazione automatica dell'indirizzo IP (DHCP)** per ottenere gli indirizzi IP automaticamente dal server DHCP.
6. Selezionare **Assegna il seguente intervallo di indirizzi IP** e specificare l'intervallo di indirizzi IP, la subnet mask e il router predefinito.
   Per specificare il range IP:
   - Utilizzare caratteri jolly. Ad esempio puoi: 192.168.0.* oppure 10.*.1.*
   - Scrivere il primo e l'ultimo indirizzo IP separati da un trattino. Ad esempio puoi: 192.168.0.10-192.168.0.20 (questo intervallo di indirizzi può essere abbreviato come 192.168.0.10-20) o 10.10-30.1.101
   - Combinare caratteri jolly e range. Ad esempio puoi: 10.10-30.1.*
   - Per separare più intervalli utilizzare una virgola. Ad esempio puoi: 192.168.0.*,192.168.1.10-192.168.1.20

Nota

Per assegnare un range di indirizzi IP, i dispositivi devono essere collegati allo stesso server AXIS Camera Station Pro.

7. Fare clic su **Next (Avanti)**.
8. Rivedere gli indirizzi IP correnti e i nuovi indirizzi IP. Per modificare l'indirizzo IP di un dispositivo, selezionare il dispositivo e fare clic su **Modifica IP**.
   - La sezione **Current IP address (Indirizzo IP corrente)** mostra l'indirizzo IP corrente, la subnet mask e il router predefinito.
   - Modificare le opzioni nella sezione **New IP address (Nuovo indirizzo IP)**, e fare clic su **OK**.
9. fare clic su **Fine** quando i nuovi indirizzi IP sono quelli desiderati.

### Configurazione dei dispositivi

È possibile configurare alcune impostazioni su più dispositivi contemporaneamente copiando le impostazioni da un dispositivo all'altro o applicando un file di configurazione.

Nota

Andare alla pagina di configurazione del dispositivo per eseguire la configurazione di tutte le impostazioni su un solo dispositivo. Vedere *Scheda Configurazione dispositivi, on page 73*.

- Per informazioni sulla configurazione dei dispositivi, vedere *Metodi di configurazione*.
- Per informazioni sulla creazione di un file di configurazione, consultare *Crea file di configurazione*.
- Per informazioni su quali impostazioni è possibile copiare, vedere *Impostazioni di configurazione*.

### Metodi di configurazione

Esistono metodi differenti di configurare i dispositivi. AXIS Device Management configura tutti i dispositivi in base alle impostazioni nel metodo. Vedere *Configurazione dei dispositivi*.

#### Usa configurazione del dispositivo selezionato

Nota

Questo metodo è disponibile solo per un singolo dispositivo e riutilizza alcune o tutte le sue impostazioni esistenti.

1. Andare a **Configurazione > Dispositivi > Gestione**.

2. Fare clic con il pulsante destro del mouse su un dispositivo e selezionare **Configure Devices > Configure (Configura dispositivi, Configura)**.
3. Selezionare le impostazioni che si desidera applicare. Vedere *Impostazioni di configurazione, on page 66*.
4. Fare clic su **Avanti** per verificare le impostazioni da applicare.
5. Fare clic su **Fine** per applicare le impostazioni al dispositivo.

**Copia configurazione da altro dispositivo**

1. Andare a **Configurazione > Dispositivi > Gestione**.
2. Fare clic con il pulsante destro del mouse sul dispositivo e selezionare **Configure Devices > Configure (Configura dispositivi, Configura)**. è possibile selezionare dispositivi di modello o firmware diverso;
3. Fare clic su **Dispositivo** per visualizzare i dispositivi con configurazioni riutilizzabili.
4. Selezionare un dispositivo da cui copiare le impostazioni e fare clic su **OK**.
5. Selezionare le impostazioni che si desidera applicare. Vedere *Impostazioni di configurazione, on page 66*.
6. Fare clic su **Avanti** per verificare le impostazioni da applicare.
7. Fare clic su **Fine** per applicare le impostazioni ai dispositivi.

**Utilizzo di un file di configurazione**

Un file di configurazione contiene le impostazioni di un dispositivo. È possibile utilizzarlo per configurare più dispositivi contemporaneamente e riconfigurare un dispositivo, ad esempio se il dispositivo viene ripristinato alle impostazioni predefinite di fabbrica. Un file di configurazione creato da un dispositivo può essere applicato a dispositivi di modello o firmware diversi, anche se alcune impostazioni non esistono su tutti i dispositivi.

Se alcune impostazioni non esistono o non possono essere applicate, lo stato dell'attività mostrerà **Error (Errore)** nella scheda **Tasks (Attività)** nella parte inferiore del client AXIS Camera Station Pro. Fare clic con il tasto destro del mouse sull'attività e selezionare **Show (Mostra)** per visualizzare le informazioni sulle impostazioni non applicabili.

Nota

Questo metodo dovrebbe essere utilizzato solo da utenti esperti.

1. Andare a **Configurazione > Dispositivi > Gestione**.
2. Fare clic con il pulsante destro del mouse sul dispositivo e selezionare **Configure Devices > Configure (Configura dispositivi, Configura)**.
3. Fare clic su **File di configurazione** per accedere al file di configurazione. Per creare un file di configurazione, vedere *Crea file di configurazione, on page 65*.
4. sfogliare i file fino a individuare il file .cfg e fare clic su **Apri**;
5. Fare clic su **Avanti** per verificare le impostazioni da applicare.
6. Fare clic su **Fine** per applicare le impostazioni ai dispositivi.

**Crea file di configurazione**

Un file di configurazione contiene le impostazioni di un dispositivo. È quindi possibile applicare queste impostazioni ad altri dispositivi. Per scoprire su come utilizzare il file di configurazione, vedere *Metodi di configurazione*.

Le impostazioni mostrate sono quelle del dispositivo accessibili tramite AXIS Device Management. Per trovare una particolare impostazione, usare il campo **Digitare il testo per la ricerca**.

Per creare un file di configurazione:

1. Andare a **Configurazione > Dispositivi > Gestione**.
2. Selezionare il dispositivo dal quale creare il file di configurazione.

3. Fare clic con il pulsante destro del mouse e selezionare **Configura dispositivi > Crea file di configurazione**.
4. Selezionare le impostazioni da includere e modificarne i valori se necessario. Vedere *Impostazioni di configurazione*.
5. Fare clic su **Avanti** per verificare le impostazioni.
6. Fare clic su **Fine** per creare il file di configurazione.
7. Fare clic su **Salva** per salvare le impostazioni in un file .cfg.

**Impostazioni di configurazione**

Quando si configurano i dispositivi, è possibile configurare anche i parametri, le regole di azione e le impostazioni aggiuntive dei dispositivi.

**Parametri**

I parametri sono impostazioni interne che regolano il comportamento del dispositivo. Per informazioni generali sui parametri, vedere il manuale dell'utente del prodotto disponibile su *www.axis.com*

Nota

- e devono essere modificati solo da utenti esperti.
- Non tutti i parametri del dispositivo non sono accessibili da AXIS Device Management.

È possibile inserire variabili in alcuni campi di testo. Le variabili vengono sostituite con del testo prima di essere applicate a un dispositivo. Per inserire una variabile, fare clic con il pulsante destro del mouse nel campo di testo e selezionare:

- **Insert device serial number variable (Inserisci variabile numero di serie dispositivo)** verrà sostituita dal numero di serie del dispositivo al quale viene applicato il file di configurazione.
- **Insert device name variable (Inserisci variabile nome dispositivo):** verrà sostituita dal nome del dispositivo utilizzato quando viene applicato il file di configurazione. Il nome del dispositivo si trova nella colonna **Name (Nome)** alla pagina **Device management (Gestione dispositivo)**. Per rinominare un dispositivo, andare alla pagina **Cameras (Telecamere)** oppure **Other devices (Altri dispositivi)**.
- **Insert server name variable (Inserisci variabile nome server):** verrà sostituita dal nome del server utilizzato quando viene applicato il file di configurazione. Il nome del server si trova nella colonna **Server** nella pagina **Device management (Gestione dispositivo)**. Per rinominare un server, andare su AXIS Camera Station Pro Service Control.
- **Insert server time zone variable (Inserisci variabile fuso orario del server):** verrà sostituita dal fuso orario POSIX utilizzato quando viene applicato il file di configurazione. È possibile utilizzarla con il parametro fuso orario POSIX per impostare il corretto fuso orario di tutti i dispositivi in una rete con server che si trovano in fusi orari diversi.

**Regole di azione**

Le regole di azione possono essere copiate da un dispositivo all'altro e devono essere modificate solo da utenti esperti. Per informazioni generali sulle regole di azione, vedere *Regole di azione*.

**Impostazioni supplementari**

- **Stream profiles (Profili di streaming):** un profilo di streaming è un profilo di configurazione della visualizzazione in diretta per le impostazioni audio, dell'immagine e di codifica video. I profili di streaming possono essere copiati da un dispositivo all'altro.
- **Motion detection windows:** le finestre di rilevamento del movimento vengono utilizzate per definire aree specifiche all'interno del campo visivo della telecamera. Normalmente, vengono generati allarmi non appena viene rilevato un movimento (o un arresto) entro aree specificate. La finestra di rilevazione del movimento può essere copiata da un dispositivo all'altro.

### Gestione degli utenti

Andare a **Configuration > Devices > Management (Configurazione, Dispositivi, Gestione)** per gestire gli utenti dei dispositivi.

Quando si imposta la password o si rimuovono gli utenti per più dispositivi, gli utenti che non sono presenti su tutti i dispositivi sono indicati con . Ogni utente compare una sola volta, anche se ricopre ruoli diversi su dispositivi diversi.

Nota

Gli account sono specifici del dispositivo e non sono relativi agli account utente di AXIS Camera Station Pro.

#### Criteri per le password

Alcuni dispositivi richiedono che le password soddisfino determinati criteri. Quando uno o più dispositivi selezionati applicano dei criteri password, l'indicatore di sicurezza della password viene sostituito da un indicatore criteri relativi alle password che mostra se la password soddisfa i requisiti del criterio attivo.

- Se non è richiesto alcun criterio, oppure se il dispositivo è conforme allo standard ONVIF, l'indicatore di sicurezza della password viene visualizzato come di consueto.
- Se sono stati selezionati più dispositivi con criteri diversi, la password deve soddisfare tutti i criteri.
- Se la password non soddisfa i requisiti, viene visualizzato il messaggio **Non-compliant (Non conforme)**. Passare il mouse sull'icona delle informazioni per visualizzare i requisiti specifici:

**Criteri per la lunghezza –** Le password devono comprendere almeno 15 caratteri.

**Criteri sulla complessità –** La password deve contenere almeno 12 caratteri e includere una lettera maiuscola, una lettera minuscola, un numero e un carattere speciale.

**Tutti e due i criteri –** È necessario soddisfare sia i requisiti di lunghezza che quelli di complessità.

#### Impostazione della password

Nota

- I dispositivi con firmware 5.20 o successivo supportano password da 64 caratteri. I dispositivi con versioni precedenti del firmware supportano password da 8 caratteri. Si consiglia l'impostazione di password sui dispositivi con firmware meno recente separatamente.
- Quando si imposta una password su più dispositivi che supportano lunghezze di password diverse, la password deve rispettare la lunghezza supportata più breve.
- Per impedire l'accesso non autorizzato e aumentare la protezione, si consiglia di proteggere con una password tutti i dispositivi aggiunti a AXIS Camera Station Pro.

Nelle password possono essere utilizzati i seguenti caratteri:

- Lettere A-Z, a-z
- Numeri 0-9
- Spazio, virgola (,), punto (.), due punti (:), e punto e virgola (;)
- !, ", #, $, %, &, ', (, +, *, -, ), /, <, >, =, ?, [, \, ^, -, `, {, |, ~, @, ], }

Per impostare una password per gli utenti sui dispositivi:

1. Andare a **Configuration > Devices > Management > Manage devices (Configurazione > Dispositivi > Gestione > Gestisci dispositivi)**.
2. Selezionare i dispositivi e fare clic su . In alternativa, fare clic con il pulsante destro del mouse sui dispositivi e selezionare **User Management > Set password (Gestione degli utenti > Imposta password)**.
3. Selezionare un utente.
4. Digitare la password o fare clic su **Generate (Genera)** per generare una password sicura.
5. Fare clic su **OK**.

Nota

Se si seleziona l'opzione **Use this password for all devices without a factory default password (Usa questa password per tutti i dispositivi privi di impostazione di fabbrica)**, la password verrà applicata a tutti i dispositivi con lo stato **Set password (Imposta password)**. Se la lunghezza della password supera il limite massimo supportato da un dispositivo, si verrà informati prima che si apra la finestra di dialogo e si potrà scegliere di procedere senza quei dispositivi.

**Aggiunta di utenti**

Per aggiungere utenti locali o di Active Directory a AXIS Camera Station Pro:

1. Andare a **Configuration > Devices > Management > Manage devices (Configurazione > Dispositivi > Gestione > Gestisci dispositivi)**.
2. Fare clic con il pulsante destro del mouse sui dispositivi e selezionare **User Management > Add user (Gestione degli utenti > Aggiungi utente)**.
3. Immettere il nome utente e la password e confermare la password. Per un elenco di caratteri validi, vedere la sezione **Set password (Imposta password)** sopra riportata.
4. Selezionare i diritti di accesso dell'utente dall'elenco a discesa **Role (Ruolo)**:
   - **Administrator (Amministratore):** accesso illimitato al dispositivo.
   - **Operator (Operatore):** accesso al flusso video, agli eventi e a tutte le impostazioni eccetto le opzioni di sistema.
   - **Viewer (Visualizzatore):** accesso al flusso video.
5. Selezionare **Enable PTZ control (Attiva comando PTZ)** per consentire all'utente di eseguire panoramica, inclinazione e zoom nella visualizzazione in diretta.
6. Fare clic su **OK**.

**Rimuovi utente**

Per rimuovere gli utenti dai dispositivi:

1. Andare a **Configuration > Devices > Management > Manage devices (Configurazione > Dispositivi > Gestione > Gestisci dispositivi)**.
2. Fare clic con il pulsante destro del mouse sui dispositivi e selezionare **User Management > Remove user (Gestione degli utenti > Rimuovi utente)**.
3. Selezionare l'utente che si desidera rimuovere dall'elenco a discesa **User (Utente)**.
4. Fare clic su **OK**.

**Elenco utenti**

Per elencare tutti gli utenti sui dispositivi e i relativi diritti di accesso:

1. Andare a **Configuration > Devices > Management > Manage devices (Configurazione > Dispositivi > Gestione > Gestisci dispositivi)**.
2. Fare clic con il pulsante destro del mouse sui dispositivi e selezionare **User Management > List users (Gestione degli utenti > Elenco utenti)**.
3. Utilizzare il campo **Type to search (Digita testo ricerca)** per trovare una telecamera specifica nell'elenco.

## Aggiornare il firmware

Il firmware è un software che determina la funzionalità del proprio dispositivo. Mantenere aggiornato il firmware garantisce che il dispositivo disponga delle funzionalità e dei miglioramenti più recenti.

È possibile scaricare il nuovo firmware utilizzando AXIS Camera Station Pro oppure importarlo da un file presente su un disco rigido o su una scheda di memoria. Le versioni del firmware disponibili per il download sono contrassegnate dalla dicitura **Download** dopo il numero di versione. Le versioni del firmware disponibili sul client locale sono visualizzate con il testo **(File)** dopo il numero di versione.

Quando si aggiorna il firmware, è possibile selezionare il tipo di aggiornamento:

- **Standard:** Aggiornare la versione del firmware selezionata e conservare i valori delle impostazioni esistenti.
- **Factory default (Impostazione predefinita di fabbrica):** Aggiornare la versione del firmware selezionata e ripristinare tutte le impostazioni ai valori predefiniti di fabbrica.

Per aggiornare il firmware.

1. Andare a **Configurazione > Dispositivi > Gestione** e selezionare i dispositivi da configurare.
2. Fare clic su oppure fare clic con il pulsante destro del mouse e selezionare **Upgrade firmware (Aggiorna firmware)**.
3. Se non è possibile configurare alcuni dei dispositivi selezionati, ad esempio perché è impossibile accedervi, verrà visualizzata la finestra di dialogo **Invalid devices (Dispositivi non validi)**. Fare clic su **Continue (Continue)** per saltare i dispositivi che non possono essere configurati.
4. Durante l'aggiornamento del firmware non è possibile accedere al dispositivo. fare clic su **Yes (Sì)** per continuare. Se non si desidera visualizzare nuovamente questo messaggio, selezionare **Do not show this dialog again (Non mostrare più questa finestra di dialogo)** e fare clic su **Yes (Sì)**.
5. La finestra di dialogo **Upgrade firmware (Aggiorna firmware)** elenca il modello di dispositivo, il numero dei dispositivi di ciascun modello, la versione del firmware esistente, le versioni firmware disponibili e il tipo di aggiornamento. Per impostazione predefinita, i dispositivi riportati nell'elenco sono preselezionati quando le versioni firmware sono disponibili per il download e la versione firmware più recente p preinstallata per ciascun dispositivo.
   5.1. Per aggiornare l'elenco delle versioni firmware disponibili per il download, fare clic su **Controlla aggiornamenti**. Per accedere a uno o più file di firmware archiviati sul client locale, fare clic su **Sfoglia**.
   5.2. Selezionare i dispositivi, le versioni del firmware che si desidera aggiornare e il tipo di aggiornamento.
   5.3. Fare clic su **OK** per avviare l'aggiornamento dei dispositivi nell'elenco.

Nota

per impostazione predefinita, gli aggiornamenti del firmware vengono eseguiti per tutti i dispositivi selezionati contemporaneamente. L'ordine di aggiornamento può essere modificato. Vedere *Impostazioni di aggiornamento firmware*.

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

### Installare le applicazioni per telecamera

Un'applicazione per videocamera è un software che può essere caricato e installato sui prodotti Axis per il video di rete. Le applicazioni aggiungono funzionalità al dispositivo, ad esempio per il rilevamento, il riconoscimento, il tracking e il conteggio.

Alcune applicazioni possono essere installate direttamente da AXIS Camera Station Pro. Altre applicazioni devono prima essere scaricate da *www.axis.com/global/en/products/analytics-and-other-applications* o dal sito Web del produttore dell'applicazione.

Le applicazioni possono essere installate sui dispositivi che supportano la Piattaforma applicativa per videocamere AXIS. Alcune applicazioni, inoltre, richiedono una versione del firmware o un modello di videocamera specifici.

Se l'applicazione richiede una licenza, è possibile installare il file della chiave di licenza contemporaneamente all'applicazione oppure in un secondo momento tramite la pagina di configurazione del dispositivo.

Per ottenere il file di chiave di licenza, il codice di licenza allegato all'applicazione deve essere registrato su *www.axis.com/se/sv/products/camera-applications/license-key-registration#/registration*

Se non si riesce a installare un'applicazione, visitare il sito web *www.axis.com* e controllare che il modello del dispositivo e la versione del firmware supportino AXIS Camera Application Platform.

Applicazioni per telecamera disponibili:

**AXIS Video Motion Detection 4 –** Un'applicazione che rileva oggetti in movimento all'interno dell'area di interesse. L'applicazione non richiede una licenza e può essere installata su fotocamere con versione firmware 6.50 o successiva. Per verificare se Video Motion Detection 4 è supportato, è possibile inoltre consultare le note di rilascio del firmware del dispositivo.

**AXIS Video Motion Detection 2 –** Un'applicazione che rileva oggetti in movimento all'interno dell'area di interesse. L'applicazione non richiede una licenza e può essere installata su telecamere con versione firmware 5.60 o successiva.

**AXIS Video Content Stream –** Un'applicazione che consente alle telecamere Axis di inviare i dati di rilevamento degli oggetti in movimento a AXIS Camera Station Pro. Può essere installata su telecamere con versione firmware compresa tra 5.50 e 9.59. AXIS Video Content Stream può essere utilizzato solo con AXIS Camera Station Pro.

**Altre applicazioni –** Qualsiasi applicazione si desideri installare. Scaricare l'applicazione nel computer locale prima di avviare l'installazione.

Per installare le applicazioni per telecamera:

1. Andare a **Configurazione > Dispositivi > Gestione**.
2. Selezionare le telecamere in cui si desidera installare le applicazioni. Fare clic su oppure fare clic con il pulsante destro del mouse e selezionare **Install camera application (Installa applicazione per telecamera)**.
3. Selezionare l'applicazione della telecamera che si desidera installare. Se si desidera installare altre applicazioni, fare clic su **Sfoglia** e accedere al file dell'applicazione locale. Fare clic su **Next (Avanti)**.
4. Se l'applicazione è già installata, è possibile selezionare **Consenti la sovrascrittura dell'applicazione** per reinstallare l'applicazione oppure selezionare **Consenti il downgrade dell'applicazione** per installare una versione precedente dell'applicazione.

Nota

Il downgrade o la sovrascrittura dell'applicazione comporta il ripristino delle impostazioni sui dispositivi.

5. Se per l'applicazione è necessaria una licenza, viene visualizzata la finestra di dialogo **Installa licenses (Installa licenze)**.
   5.1. Fare clic su **Sì** per avviare l'installazione di una licenza, quindi fare clic su **Avanti**.
   5.2. Fare clic su **Sfoglia** e accedere al file delle licenze, quindi fare clic su **Avanti**.

Nota

L'installazione di AXIS Video Motion Detection 2, AXIS Video Motion Detection 4 o AXIS Video Content Stream non richiede una licenza.

6. Esaminare nuovamente le informazioni e fare clic su **Fine**. Lo stato della telecamere si modifica da `OK` in `Maintenance`, quindi torna su `OK` al termine dell'installazione.

### Sicurezza

L'autorità di certificazione (CA) AXIS Camera Station Pro firma e distribuisce in automatico i certificati client e server nei dispositivi quando si abilitano HTTPS o IEE 802.1X. L'autorità di certificazione ignora i certificati preinstallati. Per ulteriori informazioni sulla modalità di configurazione dei certificati, vedere *Certificati, on page 140*.

### Gestione dei certificati HTTPS o IEEE 802.1X

Nota

Prima di abilitare IEEE 802.1X, verificare che l'ora sui dispositivi Axis sia sincronizzata con AXIS Camera Station Pro.

1. Andare a **Configurazione > Dispositivi > Gestione**.
2. Fare clic con il pulsante destro del mouse sui dispositivi:
   - Selezionare **Security > HTTPS > Enable/Update (Sicurezza, HTTPS, Abilita/Aggiorna)** per abilitare le impostazioni HTTPS per i dispositivi.
   - Selezionare **Security > IEEE 802.1X > Enable/Update (Sicurezza, IEEE 802.1X, Abilita/Aggiorna)** per abilitare IEEE 802.1X o aggiornare le impostazioni IEEE 802.1X per i dispositivi.
   - Selezionare **Security > HTTPS > Disable (Sicurezza, HTTPS ,Disabilita)** per disattivare HTTPS per i dispositivi.
   - Selezionare **Security > IEEE 802.1X > Disable (Sicurezza, IEEE 802.1X, Disabilita)** per disabilitare IEEE 802.1X per i dispositivi.
   - Selezionare **Certificates... (Certificati...)** per ottenere una panoramica, eliminare certificati o ottenere informazioni dettagliate su un certificato specifico.

Nota

Se lo stesso certificato è installato su più dispositivi viene visualizzato come un elemento. L'eliminazione rimuove il certificato da tutti i dispositivi su cui è installato.

#### Stato di HTTPS e IEEE 802.1X

Lo stato dei certificati HTTPS e IEEE 802.1X viene elencato nella pagina Gestione dispositivi.

| | Stato | Descrizione |
|---|---|---|
| HTTPS | On | AXIS Camera Station Pro usa HTTPS per eseguire la connessione al dispositivo. |
| | Off | AXIS Camera Station Pro usa HTTP per eseguire la connessione al dispositivo. |
| | Sconosciuto | Il dispositivo non è raggiungibile. |
| | Firmware non supportato | HTTPS non è supportato dal momento che il firmware del dispositivo è troppo obsoleto. |
| | Dispositivo non supportato | HTTPS non è supportato su questo modello di dispositivo. |
| IEEE 802.1X | Abilitato | IEEE 802.1X è attivo sul dispositivo. |
| | Disattivato | IEEE 802.1X non è attivo ma pronto per essere attivato sul dispositivo. |
| | Firmware non supportato | IEEE 802.1X non è supportato dal momento che il firmware del dispositivo è troppo obsoleto. |
| | Dispositivo non supportato | IEEE 802.1X non è supportato su questo modello di dispositivo. |

### Raccolta dei dati dei dispositivi

Questa opzione è utilizzata generalmente per la risoluzione di problemi. Genera un file ZIP con un report di raccolta dati per un'ubicazione specifica nei dispositivi.

Per raccogliere i dati dei dispositivi:

1. Andare a **Configurazione > Dispositivi > Gestione**.

2. Fare clic col pulsante destro del mouse e selezionare **Raccogli dati dispositivo**.
3. Nella sezione **Data source on selected devices (Origine dati sui dispositivi selezionati)**:
   – Fare clic su **Preset** e selezionarne uno dei comandi più comunemente usati dall'elenco a discesa.

   Nota

   Alcuni preset non funzionano su tutti i dispositivi. Lo stato PTZ, ad esempio, non funziona sui dispositivi audio.

   – Fare clic su **Personalizza** e specificare il percorso URL dell'origine della raccolta dati sui server selezionati.
4. Nella sezione **Save as (Salva come)** specificare il nome del file e la posizione della cartella per il file .zip della raccolta dati.
5. Selezionare **Apri automaticamente la cartella quando è pronta** per aprire la cartella specificata quando è stata completata la raccolta dati.
6. Fare clic su **OK**.

### Connessione

Per comunicare con i dispositivi tramite indirizzo IP o nome host:

1. Andare a **Configurazione > Dispositivi > Gestione**.
2. Selezionare i dispositivi, fare clic col pulsante destro del mouse e selezionare **Connection (Connessione)**.
   – Per connettersi ai dispositivi utilizzando l'indirizzo IP, selezionare **Use IP (Usa IP)**.
   – Per connettersi ai dispositivi utilizzando il nome host, selezionare **Use hostname (Usa nome host)**.
   – Per modificare le credenziali o le impostazioni dell'indirizzo e della porta, selezionare **Edit (Modifica)**.

### Tag

I tag aiutano a organizzare i dispositivi nella pagina **Device management (Gestione dispositivi)**. Una dispositivo può avere più etichette.

È possibile classificare i dispositivi in base al modello, alla ubicazione o ad altri criteri. Quando i dispositivi sono, ad esempio, etichettati in base al modello della telecamera, è possibile trovare e aggiornare velocemente tutte le telecamere di quel modello.

Per etichettare un dispositivo:

1. Andare a **Configurazione > Dispositivi > Gestione**.
2. Fare clic con il pulsante destro del mouse su un dispositivo e selezionare **Etichetta dispositivi**.
3. Selezionare **Use existing tag (Usa etichetta esistente)** e selezionare un'etichetta, oppure selezionare **Create a new tag (Crea nuova etichetta)** e immettere un nuovo nome per l'etichetta.
4. Fare clic su **OK**.

Per rimuovere un'etichetta da un dispositivo:

1. Andare su **Configuration > Devices > Management (Configurazione > Dispositivi > Gestione)** e fare clic su in alto a destra.
2. Nella cartella **Tags (Etichette)** selezionare un'etichetta. Verranno quindi visualizzati tutti i dispositivi associati a questa etichetta.
3. Selezionare i dispositivi, fare clic col pulsante destro del mouse e selezionare **Untag devicese (Rimuovi etichetta dispositivi)**.
4. Fare clic su **OK**.

Per gestire un'etichetta:

1. Andare su **Configuration > Devices > Management (Configurazione > Dispositivi > Gestione)** e fare clic su in alto a destra.
2. Nella pagina **Device tags (Etichette dispositivo)**:
   - Fare clic con il pulsante destro del mouse su **Etichette** e selezionare **Nuova etichetta** per creare un'etichetta.
   - Fare clic con il pulsante destro del mouse e selezionare **Rinomina etichetta**, quindi immettere un nuovo nome per rinominare un'etichetta.
   - Fare clic con il pulsante destro del mouse, selezionare **Elimina** per eliminare un'etichetta.
   - Fare clip per selezionare la pagina **Device tags (Etichette dispositivo)**.
   - Fare clic su un'etichetta per visualizzare tutti i dispositivi associati ad essa e fare clic su **All devices (Tutti i dispositivi)** per visualizzare tutti i dispositivi collegati a AXIS Camera Station Pro.
   - Fare clic su **Avvisi/Errori** per visualizzare i dispositivi che richiedono attenzione, ad esempio quelli che risultano inaccessibili.

**Scheda Configurazione dispositivi**

Per la configurazione di tutte le impostazioni su un solo dispositivo:

1. Andare a **Configurazione > Dispositivi > Gestione**.
2. Per andare alla scheda di configurazione del dispositivo, fai clic sull'indirizzo o sul nome host del dispositivo.
3. Modifica le impostazioni. Per informazioni sulla configurazione del dispositivo, consultare il manuale per l'utente del dispositivo.
4. Chiudere la scheda. Il dispositivo si riavvia per applicare le modifiche in AXIS Camera Station Pro.

**Limiti**

- Non è supportata l'autenticazione automatica per i dispositivi di terze parti.
- Non siamo in grado di garantire il supporto generale per i dispositivi di terze parti.
- La scheda di configurazione del dispositivo con flussi video attivi comporta un incremento del carico e potrebbe incidere sulle prestazioni del computer server.

## Origini di dati esterne

Un'origine dati esterna è un sistema o un'origine che genera dati che possono essere utilizzati per tenere traccia dell'accaduto al momento di ogni evento. Vedere *Ricerca dati, on page 44*.

Andare a **Configuration > Devices > External data sources (Configurazione, Dispositivi, Origini di dati esterne)** e sarà visualizzato un elenco di tutte le origini dati esterne. Fare clic su un'intestazione di colonna per ordinare in base al contenuto della colonna.

| Elemento | Descrizione |
|---|---|
| Nome | Nome dell'origine dati esterna. |
| Chiave di origine | Identificatore univoco dell'origine dati esterna. |
| Visualizza | Vista a cui è collegata l'origine dati esterna. |
| Server | Il server a cui è connessa l'origine dati. Disponibile solo quando ci si collega a più server. |

Si aggiunge automaticamente un'origine dati esterna quando:

- Viene creata una porta in **Configuration > Access control > Doors and zones (Configurazione > Controllo degli accessi > Porte e zone)**.
  Per un flusso di lavoro completo su come impostare un door controller di rete Axis in AXIS Camera Station Pro, vedere *Impostare un door controller di rete Axis*.
- Viene ricevuto il primo evento dal dispositivo configurato con AXIS License Plate Verifier.
  Per un flusso di lavoro completo per l'impostazione di AXIS License Plate Verifier in AXIS Camera Station Pro, vedere *Imposta AXIS License Plate Verifier*.

Se una sorgente dati esterna è stata configurata con una vista, i dati generati dalla sorgente dati vengono automaticamente contrassegnati con segnalibro nella sequenza temporale della vista nella scheda **Data search (Ricerca dati)**. Per connettere una sorgente dati a una vista:

1. Andare a **Configuration > Devices > External data sources (Configurazione > Dispositivi > Origini di dati esterne)**.
2. Selezionare un'origine dati esterna e fare clic su **Edit (Modifica)**.
3. Selezionare una vista dall'elenco a discesa **View (Vista)**.
4. Fare clic su **OK**.

## Sincronizzazione dell'ora

Andare a **Configuration > Devices > Time synchronization (Configurazione > Dispositivi > Sincronizzazione ora)** per aprire la pagina **Time synchronization (Sincronizzazione ora)**.

AXIS Camera Station Pro visualizza un elenco di tutti i dispositivi aggiunti. Fai clic con il pulsante destro del mouse sulla riga dell'intestazione e seleziona le colonne da mostrare. Trascinare la selezione delle intestazioni per visualizzare le colonne con un ordine diverso.

L'elenco dei dispositivi include le seguenti informazioni:

- **Name (Nome):** il nome del dispositivo o un elenco di tutti i nomi delle telecamere associate quando il dispositivo è un video encoder con più telecamere collegate o una telecamera di rete con più aree di visione.
- **Address (Indirizzo):** l'indirizzo del dispositivo. Fare clic sul collegamento per accedere alla pagina di configurazione del dispositivo. Mostra l'indirizzo IP o il nome host, a seconda di quale viene utilizzato quando si aggiunge il dispositivo. Vedere *Scheda Configurazione dispositivi, on page 73*.
- **MAC address (Indirizzo MAC):** l'indirizzo MAC del dispositivo.
- **Model (Modello):** il modello del dispositivo.
- **Enabled (Abilitata):** indica se la sincronizzazione dell'ora è attiva.
- **NTP Source (Sorgente NTP):** La sorgente NTP configurata per il dispositivo.
  - **Static (Statica):** I server NTP sul dispositivo sono specificati manualmente in **Primary NTP server (Server NTP principale)** e **Secondary NTP server (NTP secondario)**.
  - **DHCP:** Il dispositivo riceve il server NTP dinamicamente dalla rete. **Primary NTP server (Server NTP principale)** e **Secondary NTP server (Server NTP secondario)** non sono disponibili quando **DHCP** è selezionato.
- **Primary NTP server (Server NTP primario):** il server NTP primario configurato per il dispositivo. Disponibile unicamente quando è selezionato **Static (Statico)**.
- **Secondary NTP server (Server NTP secondario):** il server NTP secondario configurato per il dispositivo. Disponibile unicamente per i dispositivi Axis che supportano il protocollo NTP secondario e quando **Static (Statico)** è selezionato.
- **Server time offset (Offset orario server):** la differenza di orario tra dispositivo e server.
- **UTC time (Ora UTC):** l'ora universale coordinata sul dispositivo.
- **Synced (Sincronizzato):** indica se sono state applicate le impostazioni di sincronizzazione dell'ora. Disponibile solo per dispositivi con firmware 9.1 o successive.

- **Time to next sync (Tempo rimanente alla prossima sincronizzazione):** il tempo rimanente fino alla prossima sincronizzazione.

Il servizio Ora di Windows (W32Time) usa il Network Time Protocol (NTP) per la sincronizzazione della data e dell'ora per il server AXIS Camera Station Pro. Sono visualizzate le seguenti informazioni:

- **Server:** Il server AXIS Camera Station Pro su cui viene eseguito il servizio Ora di Windows.
- **Status (Stato):** lo stato del servizio Ora di Windows. `Running` o `Stopped`.
- **NTP server (Server NTP):** Il server NTP configurato per il servizio Ora di Windows.

**Configura sincronizzazione dell'ora**

1. Vai su **Configuration > Devices > Time synchronization (Configurazione > Dispositivi > Sincronizzazione ora)**.
2. Seleziona i tuoi dispositivi e seleziona **Enable time synchronization (Abilita sincronizzazione ora)**.
3. Seleziona la sorgente NTP **Static (Statica)** o **DHCP**.
4. Se è stato selezionato **Static (Statica)**, configurare il server NTP principale e secondario.
5. fare clic su **Applica**;

| | |
|---|---|
| **Send alarm when the time difference between server and device is more than 2 seconds (Invia allarme quando la differenza di ora tra server e dispositivo è maggiore di 2 secondi)** | Selezionare questa opzione per ricevere un allarme se la differenza di ora tra il server e dispositivo è superiore a 2 secondi. |
| **Set the time zone manually through the device interface (Imposta manualmente il fuso orario tramite l'interfaccia del dispositivo)** | Selezionare questa opzione se non si desidera utilizzare il fuso orario del server, ma il fuso orario in base alla posizione del dispositivo. Se si sceglie questa opzione, è necessario impostare manualmente il fuso orario tramite l'interfaccia web del dispositivo. |

## Configurazione dell'archiviazione

Andare a **Configuration > Storage > Management (Configurazione, Archiviazione, Gestione)** per aprire la pagina **Manage storage (Gestisci archiviazione)**. Qui è possibile avere una panoramica delle soluzioni di archiviazione locale e di rete disponibili su AXIS Camera Station Pro.

| Elenco | |
|---|---|
| **Luogo** | Il nome e il percorso dell'archiviazione. |
| **Allocato** | La quantità massima di archiviazione assegnata alle registrazioni. |
| **Utilizzato** | La quantità di spazio di archiviazione attualmente utilizzato per le registrazioni. |

| Elenco | |
|---|---|
| **Stato** | Lo stato dell'archiviazione. I possibili valori sono:<br>• **OK**<br>• **Storage full (Disco pieno):** Il disco è pieno. Il sistema sovrascrive le registrazioni sbloccate più vecchie.<br>• **Unavailable (Non disponibile):** Le informazioni sull'archiviazione non sono attualmente disponibili. Ad esempio, un'archiviazione di rete è stata rimossa o scollegata.<br>• **Intruding data (Dati di intrusioni):** i dati di altre applicazioni impiegano lo spazio di archiviazione allocato per AXIS Camera Station Pro. Oppure, ci sono delle registrazioni prive di connessione al database, le cosiddette registrazioni non indicizzate, nello spazio di archiviazione allocato per AXIS Camera Station Pro.<br>• **No permissions (Senza permessi:** L'utente non ha l'autorizzazione di lettura o scrittura relativamente al dispositivo di archiviazione.<br>• **Low space (Spazio insufficiente):** l'unità ha meno di 15 GB di spazio libero, che AXIS Camera Station Pro considera insufficiente. Per la prevenzione di errori o corruzione, AXIS Camera Station Pro esegue una pulizia forzata, a prescindere dal posizionamento del cursore di archiviazione, per tutelare l'unità. Nel corso della pulizia forzata, AXIS Camera Station Pro impedisce la registrazione finché non diventa disponibile uno spazio di archiviazione superiore a 15 GB.<br>• **Capacità insufficiente**: La dimensione totale del disco è inferiore a 32 GB, una dimensione insufficiente per AXIS Camera Station Pro.<br>Gli AXIS OS Recorder con supporto per RAID possono presentare anche i seguenti stati:<br>• **Online:** il sistema RAID funzinona come dovrebbe. È presente una ridondanza nell'eventualità che si verifichi un guasto in uno dei dischi fisici del sistema RAID.<br>• **Degraded (Degradato):** uno dei dischi fisici nel sistema RAID è guasto. Si possono ancora registrare e riprodurre registrazioni dal dispositivo di archiviazione, ma non la ridondanza non è presente. Se si rompe un altro disco fisico, lo stato RAID passa a **Failure (Guasto)**. Consigliamo di eseguire la sostituzione del disco fisico danneggiato quanto prima. Dopo la sostituzione di un disco rotto, lo stato RAID passa da **Degraded (Degradato)** a **Syncing (In sincronizzazione)**.<br>• **Syncing (Sincronizzazione):** è in corso la sincronizzazione dei dischi RAID. È possibile eseguire la registrazione e riproduzione di registrazioni dal dispositivo di archiviazione, ma non è presente la ridondanza se un disco fisico si rompe. Una volta avvenuta la sincronizzazione dei dischi fisici, si verifica la ridondanza nel sistema RAID e lo stato RAID passa a **Online**.<br>Importante<br>Non eseguire mai la rimozione di un disco RAID nel corso della sincronizzazione. Ciò può condurre a un guasto del disco.<br>• **Failure (Guasto:** molti dischi fisici nel sistema RAID hanno subito guasti. Quando ciò avviene, tutte le registrazioni nel dispositivo di archiviazione vengono perse e la registrazione può avvenire solo in seguito alla sostituzione dei dischi fisici danneggiati. |
| **Server** | Il server in cui si trova l'archiviazione di rete o locale. |

| Panoramica | |
|---|---|
| **Utilizzato** | Spazio di archiviazione attualmente utilizzato dalle registrazioni indicizzate. Se un file si trova nella directory di registrazione ma non è indicizzato nel database, il file appartiene alla categoria **Other data (Altri dati)**. Vedere *Gestione dello spazio di archiviazione, on page 77*. |
| **Gratuito** | Quantità di spazio di archiviazione lasciato nel punto di archiviazione. Si tratta della stessa quantità di "Spazio libero" mostrato nelle proprietà Windows per il punto di archiviazione. |
| **Altri dati** | Quantità di spazio di archiviazione occupata dai file che non sono registrazioni indicizzate e quindi non sono noti a AXIS Camera Station Pro.<br><br>Altri dati = Capacità totale - spazio usato - spazio libero. |
| **Capacità totale** | La quantità totale di spazio su archiviazione. Si tratta della stessa quantità di "Spazio totale" mostrato nelle proprietà Windows per il punto di archiviazione. |
| **Allocato** | La quantità di spazio di archiviazione che AXIS Camera Station Pro può utilizzare per le registrazioni. È possibile regolare il cursore e fare clic su **Apply (Applica)** per regolare lo spazio allocato. |

| Archiviazione di rete | |
|---|---|
| **Percorso** | Il percorso dell'archiviazione di rete. |
| **Nome utente** | Il nome utente utilizzato per collegarsi all'archiviazione di rete. |
| **Password** | La password per il nome utente utilizzata per collegarsi all'archiviazione di rete. |

## Gestione dello spazio di archiviazione

Andare a **Configuration > Storage > Management (Configurazione, Archiviazione, Gestione)** per aprire la pagina **Manage storage (Gestisci archiviazione)**. Qui è possibile specificare la cartella in cui salvare le registrazioni. Per evitare che lo spazio di archiviazione si esaurisca, impostare una percentuale massima della capacità totale che AXIS Camera Station Pro può utilizzare. Si possono aggiungere dispositivi di archiviazione locale e unità di rete supplementari per aumentare la sicurezza e lo spazio disponibile.

Nota

- Quando sussiste la connessione a più server AXIS Camera Station Pro, scegliere il server dal menu a discesa **Selected server (Server selezionato)** per gestire lo spazio di archiviazione.
- Quando il servizio usa l'account di sistema per eseguire l'accesso, non è possibile aggiungere unità di rete che si collegano a cartelle condivise in altri computer. Vedere *Archiviazione di rete non accessibile*.
- Non si può rimuovere il dispositivo di archiviazione locale o l'archiviazione di rete se le telecamere sono impostate per la registrazione o per l'archiviazione delle registrazioni in essi.

### Aggiunta di un dispositivo di archiviazione locale o di un'unità di rete condivisa

1. Andare a **Configurazione > Archiviazione > Gestione**.
2. Fare clic su **Aggiungi**.
3. Per aggiungere un dispositivo di archiviazione locale, selezionare **Local storage (Archiviazione locale)** e selezionare un dispositivo di archiviazione locale dal menu a discesa.
4. Per aggiungere un'unità di rete condivisa, selezionare **Shared network drive (Unità di rete condivisa)** e inserire il percorso. Ad esempio puoi: \\ip_address\share.
5. Fare clic su **OK** e immettere il nome utente e la password per l'unità di rete condivisa.

6. Fare clic su **OK**.

**Rimozione di un dispositivo di archiviazione locale o di un'unità di rete condivisa**

Per rimuovere un'unità di archiviazione locale o un'unità di rete condivisa, selezionarla dall'elenco delle unità di archiviazione e fare clic su **Remove (Rimuovi)**.

**Sposta registrazioni in una nuova cartella**

1. Andare a **Configurazione > Archiviazione > Gestione**.
2. Eseguire la selezione di un dispositivo di archiviazione locale o di un'unità di rete condivisa dall'elenco di archiviazioni.
3. In **Overview (Panoramica)**, inserire un nome per la cartella in **Move recordings to a new folder (Sposta registrazioni in una nuova cartella)** per cambiare la posizione di archiviazione delle registrazioni. In questo modo si spostano nella nuova cartella anche le registrazioni esistenti nella cartella precedente.
4. fare clic su **Applica**;

**Regolazione della capacità di archiviazione**

1. Andare a **Configurazione > Archiviazione > Gestione**.
2. Eseguire la selezione di un dispositivo di archiviazione locale o di un'unità di rete condivisa dall'elenco di archiviazioni.
3. In **Overview (Panoramica)** spostare il cursore per impostare lo spazio massimo che AXIS Camera Station Pro can use. può usare.
4. fare clic su **Applica**;

Nota

- Si raccomanda di lasciare disponibile almeno il 5% dello spazio su disco per prestazioni ottimali.
- I requisiti di spazio di archiviazione minimo di un dispositivo di archiviazione aggiunto ad AXIS Camera Station Pro è 32 GB con almeno 15 GB di spazio libero disponibile.
- Se inferiore a 15 GB, AXIS Camera Station Pro elimina automaticamente le vecchie registrazioni per liberare spazio.

**Raccogli file non indicizzati**

I file non indicizzati possono costituire una parte notevole del segmento **Other data (Altri dati)** sul dispositivo di archiviazione. Un file non indicizzato è costituito dai dati presenti nella cartella di registrazione che non fanno parte del database corrente. Il file può contenere le registrazioni di installazioni precedenti o le perdite di dati che si verificano quando viene utilizzato un punto di ripristino.

Il sistema non elimina i file raccolti, bensì li raccoglie e posiziona nella cartella **Non-indexed files (File non indicizzati)** sul dispositivo di archiviazione registrazioni. Il dispositivo di archiviazione può trovarsi sullo stesso computer del client oppure su un server remoto a seconda della configurazione. Per accedere alla cartella **Non-indexed files (File non indicizzati)** è necessario disporre dei diritti di accesso al server. AXIS Camera Station Pro organizza i dati prima per server e poi per dispositivi collegati a quel server.

È possibile cercare una registrazione o un registro smarrito, oppure eliminare i contenuti per liberare spazio.

Per raccogliere i file non indicizzati per la revisione o la rimozione:

1. Andare a **Configurazione > Archiviazione > Gestione**.
2. Eseguire la selezione di un dispositivo di archiviazione locale o di un'unità di rete condivisa dall'elenco di archiviazioni.
3. In **Collect non-indexed files (Raccogli file non indicizzati)**, fare clic su **Collect (Raccogli)** per avviare l'attività.
4. Quando l'attività è completata, andare a **Alarms and Tasks > Tasks (Allarmi e attività, Attività)** e fare doppio clic sull'attività per visualizzare il risultato.

## Selezione dei dispositivi di archiviazione da collegare

Nota

Le registrazioni sono memorizzate come file .acsm e devono essere convertite prima di poter essere riprodotte. Contattare l'assistenza tecnica Axis per ricevere supporto riguardo la conversione dei file.

Andare a **Configuration > Storage > Selection (Configurazione, Archiviazione, Selezione)** per aprire la pagina **Select storage (Seleziona archiviazione)**. Questa pagina mostra una lista di tutte le telecamere in AXIS Camera Station Pro. Qui è possibile specificare per quanti giorni conservare le registrazioni relative a determinate telecamere. Una volta selezionata questa opzione, è possibile visualizzare le informazioni relative allo spazio di archiviazione nella sezione **Recording Storage (Spazio di archiviazione registrazioni)**. Si possono configurare più telecamere simultaneamente.

| | |
|---|---|
| **Nome** | il nome del dispositivo o un elenco di tutti i nomi delle telecamere associate quando il dispositivo è un video encoder con più telecamere collegate o una telecamera di rete con più aree di visione. |
| **Indirizzo** | l'indirizzo del dispositivo. Fare clic sul collegamento per accedere alla pagina di configurazione del dispositivo. Mostra l'indirizzo IP o il nome host, a seconda di quale è stato utilizzato quando è stato aggiunto il dispositivo. Vedere *Scheda Configurazione dispositivi, on page 73*. |
| **Indirizzo MAC** | l'indirizzo MAC del dispositivo. |
| **Casa produttrice** | la casa produttrice del dispositivo. |
| **Modello** | il modello del dispositivo. |
| **Spazio di archiviazione utilizzato** | La quantità di spazio di archiviazione attualmente utilizzato per le registrazioni. |
| **Luogo** | Il nome e il percorso dell'archiviazione. |
| **Tempo di archiviazione** | Il tempo di conservazione che è stato configurato per la telecamera. |
| **Registrazione più vecchia** | L'ora della registrazione più vecchia della telecamera conservata nell'archiviazione. |
| **Riproduzione da scheda di memoria** | Indica la configurazione della telecamera per riprodurre le registrazioni direttamente dalla propria scheda di memoria in modalità AXIS Camera Station Pro, senza copiarle sul server. |
| **Registrazione di failover** | Indica se la telecamera utilizza la failover recording. |
| **Copia in ACS Pro** | Indica se le registrazioni presenti sulla scheda di memoria vengono copiate su AXIS Camera Station Pro. |
| **Server** | Il server in cui si trova l'archiviazione di rete o locale. |

Le impostazioni di archiviazione per ciascuna telecamera sono state configurate al momento dell'aggiunta delle telecamere a AXIS Camera Station Pro. Per modificare le impostazioni di archiviazione di una telecamera:

1. Andare a **Configurazione > Archiviazione > Selezione**.
2. Selezionare la videocamera per modificare le impostazioni di memorizzazione.
3. In **Recording storage (Archiviazione della registrazione)**, impostare punto di archiviazione e tempo di conservazione.
4. Nella sezione **SD card storage (Archiviazione su scheda di memoria)**, selezionare **Playback of SD card recordings (Riproduzione delle registrazioni su scheda di memoria)**, **Failover recording (Registazione guasto)** e **Copy SD card recordings to ACS Pro server (Copia delle registrazioni dalla scheda di memoria sul server ACS Pro)** seconda delle necessità.
5. fare clic su **Applica**;

| Memorizzazione della registrazione | |
|---|---|
| Nota<br>• Per poter utilizzare lo spazio sula scheda di memoria, il dispositivo deve supportare VAPIX e utilizzare una scheda di memoria Axis.<br>• Le funzionalità della scheda di memoria non sono compatibili con il formato M-JPEG.<br>• Le registrazioni presenti sulla scheda di memoria non vengono eliminate da AXIS Camera Station Pro. La loro conservazione è regolata dal tempo di conservazione impostato sulla scheda di memoria della telecamera. | |
| **Store to (Archivia in)** | Selezionare dal menu a discesa la posizione di per le registrazioni. Le opzioni disponibili sono il dispositivo di archiviazione locale e l'archiviazione di rete create. |
| **Tempo di archiviazione** | • **Unlimited (Illimitato):** Conserva le registrazioni finché lo spazio di archiviazione non è pieno.<br>• **Limited (Limitato):** Impostare il numero massimo di giorni di conservazione delle registrazioni.<br>Nota<br>Se lo spazio di archiviazione destinato ad AXIS Camera Station Pro viene esaurito, il sistema elimina le registrazioni prima della scadenza impostata. |
| **Maximum days to keep recordings (Giorni massimi di conservazione delle registrazioni)** | Specificare il numero di giorni per la conservazione delle registrazioni. |

| Archiviazione scheda di memoria | |
|---|---|
| **Riproduzione delle registrazioni presenti sulla scheda di memoria** | Attivare questa opzione per riprodurre le registrazioni direttamente dalla scheda di memoria della telecamera in AXIS Camera Station Pro, senza copiarle sul server. È possibile esportare anche le registrazioni presenti sulla scheda di memoria visibili nella cronologia. Per questa funzione è necessario disporre di AXIS OS 5.60 o versione successiva. |
| **Registrazione di failover** | Selezionare questa opzione per salvare le registrazioni sulla scheda di memoria della telecamera in caso di interruzione della connessione a AXIS Camera Station Pro. Disponibile solo per le telecamere dotate di scheda di memoria e con versione firmware 5.20 o successiva. |
| **Copia le registrazioni della scheda di memoria sul server ACS** | Selezionare questa opzione per copiare tutte le registrazioni presenti sulla scheda di memoria della telecamera sul server. Utilizzare **Schedule (Pianifica)** per impostare quando copiare le registrazioni. La pianificazione predefinita è **Always (Sempre)**. |

## Configurazione di registrazioni ed eventi

Quando si esegue l'aggiunta di telecamere a AXIS Camera Station Pro, il sistema configura automaticamente la registrazione del movimento o la registrazione continua. In seguito si può modificare il metodo di registrazione secondo le proprie esigenze. Vedere *Metodo di registrazione, on page 86*.

## Registrazione del movimento

È possibile usare il rilevamento movimento con tutte le telecamere di rete e i codificatori video Axis. Rispetto alla registrazione continua, la registrazione nel solo caso di rilevamento del movimento consente di risparmiare più spazio sul dispositivo di archiviazione. Su **Recording method (Metodo di registrazione)**, si può attivare e configurare **Motion detection (Rilevamento movimento)**. Si può, ad esempio, configurare le impostazioni nel caso la telecamera rilevi troppi oggetti o troppo pochi, in movimento o la dimensione dei file registrati sia eccessiva per lo spazio di archiviazione disponibile.

Per configurare la registrazione di movimento:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Metodo di registrazione**.
2. Selezionare una telecamera
3. Selezionare la casella di controllo **Motion detection** (Rilevamento movimento).
4. Fare clic su **Motion settings (Impostazioni di movimento)** per configurare le impostazioni di rilevamento movimento, come il numero di oggetti rilevabili. Le impostazioni disponibili variano a seconda delle telecamere, vedere *Modifica di rilevamento movimento incorporato* e *Modifica di AXIS Video Motion Detection 2 e 4*.
5. Selezionare un **Profile (Profilo)** nel menu a discesa, il profilo **High (Alto)** è quello predefinito.
6. Selezionare una pianificazione o fare clic su **New schedule...(Nuova pianificazione.** per creare una nuova pianificazione personalizzata.
7. Impostare i tempi di pre-buffer e post-buffer e il periodo di trigger.
8. fare clic su **Applica**;

Nota

È possibile usare le regole di azione per configurare la registrazione del movimento. Prima di utilizzare le regole di azione, controllare che l'opzione **Motion detection (Rilevamento movimento)** sia disattivata in **Recording method (Metodo di registrazione)**.

| | |
|---|---|
| **Profilo** | Usare una risoluzione inferiore per diminuire le dimensioni della registrazione. Per modificare le impostazioni del profilo, vedere *Profili di flusso*. |
| **Pianificazione** | La pianificazione delle registrazioni. Per diminuire l'impatto sullo spazio di archiviazione, registrare unicamente in periodi di tempo specifici. |
| **Categoria evento** | Quale categoria di evento a cui si desidera che la registrazione appartenga, se presente. |
| **Pre-buffer** | La quantità di secondi precedenti al movimento rilevato vanno inclusi in una registrazione. |
| **Post-buffer** | La quantità di secondi precedenti dopo il movimento rilevato vanno inclusi in una registrazione. |
| **Trigger period (Periodo di attivazione)** | Impostare il tempo minimo che deve intercorrere tra due trigger per ridurre il numero di registrazioni consecutive. Se si verifica un altro trigger in questo intervallo, la registrazione prosegue e l'intervallo riparte. |
| **Notifiche** | Quando la telecamera effettua il rilevamento movimento, viene inviata una notifica. **L'app mobile** invia una notifica push all'app mobile AXIS Camera Station. **L'allarme del server** attiva un allarme in AXIS Camera Station Pro. |

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

*Configurare il rilevamento di movimento*

## Rilevamento oggetti

La registrazione con rilevamento oggetti acquisisce video quando AXIS Object Analytics rileva e classifica tipi di oggetti quali persone e veicoli. Si consiglia di utilizzarlo insieme al rilevamento movimento o alla registrazione continua per essere certi di non perdere nessun evento. AXIS Object Analytics supporta fino a 10 scenari per telecamera.

Nota

Per poter utilizzare questa funzione, la telecamera deve disporre della versione firmware 12.4.26 o successive, di un sensore singolo e dell'ACAP AXIS Object Analytics installata.

Per utilizzare il rilevamento oggetti:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Metodo di registrazione**.
2. Selezionare una telecamera
3. Selezionare la casella di controllo **Object detection** (Rilevamento oggetti).
4. Effettuare la configurazione delle impostazioni. Per ulteriori informazioni, vedere la tabella che segue.
5. fare clic su **Applica**;

- Gli eventi di rilevamento oggetti sono indicati in rosa sulla cronologia.

| | |
|---|---|
| **Impostazioni di rilevamento oggetti...** | Fare clic per aprire l'interfaccia web AXIS Object Analytics e effettuare la configurazione di quali tipi di oggetti (persone, veicoli) attivano le registrazioni, impostare la dimensione minima degli oggetti, definire le aree di rilevamento e regolare le impostazioni relative al tempo di permanenza nell'area. |
| **Profilo** | Selezionare un **Profile (Profilo)** dal menu a discesa. **High (Alto)** è il profilo predefinito. Usare una risoluzione inferiore per ridurre le dimensioni della registrazione. Per modificare le impostazioni del profilo, vedere *Profili di flusso*. |
| **Pianificazione** | Impostare la pianificazione delle registrazioni. Per diminuire l'impatto sullo spazio di archiviazione, registrare unicamente in periodi di tempo specifici. |
| **Categoria evento** | Selezionare la categoria di evento a cui si desidera che la registrazione appartenga, se presente. Consultare *Categorie di eventi, on page 28* per ulteriori informazioni. |
| **Pre-buffer** | Impostare quanti secondi precedenti al rilevamento oggetto vanno inclusi in una registrazione. |
| **Post-buffer** | Impostare quanti secondi successivi al rilevamento oggetto vanno inclusi in una registrazione. |

| | |
|---|---|
| **Trigger period (Periodo di attivazione)** | Impostare un intervallo di tempo minimo tra i trigger per ridurre le registrazioni consecutive. Se si verifica un altro trigger in questo intervallo, la registrazione prosegue e il periodo di attivazione ricomincia. |
| **Notifiche** | Invia una notifica quando AXIS Object Analytics effettua il rilevamento di un oggetto. **L'app mobile** invia una notifica push all'app mobile AXIS Camera Station. **Server alarm (Allarme server)** genera un avviso in AXIS Camera Station Pro. |

## Registrazione continua e pianificata

La registrazione continua a salvare le immagini senza interruzione e richiede più spazio di archiviazione rispetto alle altre opzioni di registrazione. Per ridurre le dimensioni del file, tenere conto di utilizzare invece la registrazione di rilevamento movimento.

Per utilizzare la registrazione continua:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Metodo di registrazione**.
2. Selezionare una telecamera
3. Selezionare la casella di controllo **Continuous (Continua**.
4. Effettuare la configurazione delle impostazioni. Per ulteriori informazioni, vedere la tabella che segue.
5. fare clic su **Applica**;

| | |
|---|---|
| **Profilo** | Selezionare un **Profile (Profilo)** dal menu a discesa. **High (Alto)** è il profilo predefinito. Usare una risoluzione inferiore per ridurre le dimensioni della registrazione. Per modificare le impostazioni del profilo, vedere *Profili di flusso*. |
| **Pianificazione** | Impostare la pianificazione delle registrazioni. Per diminuire l'impatto sullo spazio di archiviazione, registrare unicamente in periodi di tempo specifici. |
| **Average Bitrate** | Attivare per impostare un limite di archiviazione massimo. Il sistema mostra la velocità in bit media stimata sulla base dello spazio di archiviazione massimo specificato e al periodo di conservazione. La velocità in bit media massima è di 50000 kbit/s. Per ulteriori informazioni, consultare *Configurare la velocità di trasmissione media, on page 86*. |

## Registrazione manuale

Per configurare le impostazioni di registrazione manuale:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Metodo di registrazione**.
2. Selezionare una telecamera
3. Selezionare la casella di controllo **Manual** (Manuale).
4. Effettuare la configurazione delle impostazioni. Per ulteriori informazioni, vedere la tabella che segue.
5. fare clic su **Applica**;

| | |
|---|---|
| **Profilo** | Selezionare un **Profile (Profilo)** dal menu a discesa. **High (Alto)** è il profilo predefinito. Usare una risoluzione inferiore per ridurre le dimensioni della registrazione. Per modificare le impostazioni del profilo, vedere *Profili di flusso*. |
| **Categoria evento** | Selezionare la categoria di evento a cui si desidera che la registrazione appartenga, se presente. |
| **Pre-buffer** | Impostare la quantità di secondi da includere nella registrazione prima di premere il pulsante di registrazione. |
| **Post-buffer** | Impostare la quantità di secondi da includere nella registrazione dopo aver interrotto la registrazione. |
| **Aggiungi segnalibro durante la registrazione** | Aggiunge i dettagli del segnalibro ogni volta che si avvia una registrazione manuale. I segnalibri consentono di individuare e identificare registrazioni specifiche in un secondo momento. Queste impostazioni sono applicabili esclusivamente agli operatori e agli amministratori e sono disattivate per impostazione predefinita. |
| **Durata massima** | Impostare la durata massima di ogni registrazione, esclusi i tempi di pre-buffer e post-buffer. Impostare su 0 per una durata illimitata. |

Per ulteriori informazioni sulla registrazione manuale, vedere *Registrazione manuale*.

## Registrazione attivata da regole

Una registrazione attivata da regole inizia e si ferma in base a una regola creata in Regole di azione. È possibile usare regole, ad esempio ai fini della generazione di registrazioni attivate da segnali provenienti da porte I/O o eventi dispositivo. Una regola può avere diverse attivazioni.

Per creare una registrazione attivata da regole, vedere *Regole di azione*.

Nota

Se si usa una regola per configurare la registrazione del movimento, assicurarsi di aver disattivato la registrazione del movimento per evitare registrazioni duplicate.

## Registrazione di failover

Utilizzare la failover recording per salvare le registrazioni sulla scheda di memoria della telecamera in caso di interruzione della connessione a AXIS Camera Station Pro.

AXIS Camera Station Pro seleziona automaticamente il metodo di failover in base alla versione del firmware della telecamera:

- **Firmware 11.11.42 o successivo:** la failover recording si avvia ogni volta che la telecamera perde il contatto con il server.
- **Firmware precedente:** la failover recording si avvia solo in caso di interruzione imprevista della connessione. I riavvii pianificati del server non attivano la failover recording.

Per configurare la failover recording, consultare la sezione *Selezione dei dispositivi di archiviazione da collegare, on page 79*.

Nota

- Durante l'aggiornamento, se **Failover recording** era stata precedentemente attivata, l'opzione **Copy SD card recordings to ACS Pro server (Copia registrazioni dalla scheda di memoria sul server ACS Pro)** è attivata automaticamente.
- Le registrazioni presenti sulla scheda di memoria non vengono eliminate da AXIS Camera Station Pro. La loro conservazione è regolata dal tempo di conservazione della scheda di memoria impostato sulla telecamera.
- Abilitando failover recording si sovrascrive qualsiasi configurazione failover esistente per quella telecamera su altri server.
- La failover recording può essere attiva solo su un server AXIS Camera Station Pro alla volta per ciascuna vista della telecamera.

Quando la connessione viene ripristinata e l'opzione **Copy SD card recordings to ACS Pro server (Copia registrazioni dalla scheda di memoria sul server ACS Pro)** è attiva, le registrazioni vengono copiate sul server e contrassegnate con un colore grigio scuro nella cronologia. La telecamera utilizza un pre-buffer e un post-buffer di 20 secondi ma possono comunque verificarsi brevi interruzioni di circa 1-4 secondi.

| Metodi di registrazione | |
|---|---|
| **Rilevamento movimento con prebuffer** | Se la connessione viene interrotta per più di 20 secondi, la telecamera continua a registrare sulla scheda di memoria fino a quando la connessione non sarà ripristinata o fino a quando la scheda di memoria non sarà piena. |
| **Rilevamento movimento senza prebuffer** | • Se la connessione viene interrotta per più di 20 secondi senza che sia in corso la registrazione del movimento, la failover recording non si avvia.<br>• Se la connessione viene interrotta per più di 20 secondi mentre la registrazione di movimento è in corso, si avvia la failover recording, che prosegue fino a quando non sarà possibile ripristinare la connessione o fino a quando la scheda di memoria non sarà piena. |
| **Registrazione continua** | Se la connessione viene interrotta per più di 20 secondi, la telecamera continua a registrare sulla scheda di memoria fino a quando la connessione non sarà ripristinata o fino a quando la scheda di memoria non sarà piena. |

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

*Utilizza la scheda di memoria per il failover recording*

## Failover su unità di registrazione Axis

È possibile attivare la failover recording su un dispositivo che usa un registratore AXIS S30 o S40 come archiviazione della registrazione. Una volta attiva, l'unità avvia automaticamente una registrazione continua

quando viene interrotta la connessione tra AXIS Camera Station Pro e l'unità di registrazione. Il dispositivo utilizza il profilo di streaming medio per la failover recording.

Nota

- Questa caratteristica richiede AXIS Camera Station 5.36 o versione successiva, AXIS S30 o AXIS S40 Recorder firmware 10.4 o versione successiva e firmware per dispositivo Axis 5.50 o versione successiva.
- Se una registrazione continua è in corso quando viene avviata la failover recording, verrà avviata una nuova registrazione continua. Il sistema crea duplicati del flusso sul registratore.

Per abilitare il failover recording:

1. Assicurarsi di aver aggiunto il registratore e i dispositivi e di aver selezionato il registratore come archivio di registrazione per il dispositivo. Vedere *Impostazione di AXIS OS Recorders*.
2. Andare a **Configurazione > Archiviazione > Selezione**.
3. Selezionare il dispositivo e selezionare la **Failover recording**.
4. fare clic su **Applica**;

## Metodo di registrazione

AXIS Camera Station Pro configura automaticamente la registrazione del movimento o la registrazione continua quando si aggiungono dispositivi.

Un segno di spunta indica il metodo di registrazione utilizzato da un dispositivo. Per personalizzare le impostazioni dei profili per video e audio, vedere *Profili di flusso*.

Per modificare il metodo di registrazione:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Metodo di registrazione**.
2. Selezionare uno o molteplici dispositivi.
   Per i dispositivi dello stesso modello, si possono configurare più dispositivi simultaneamente.
3. Nella schermata **Recording method (Metodo di registrazione)**, è possibile attivare o disattivare un metodo di registrazione.

Nota

Le aree di visione non supportano il rilevamento movimento.

### Configurare la velocità di trasmissione media

Con la velocità in bit media, la velocità in bit è regolata automaticamente su un lasso di tempo più lungo. Questo consente di soddisfare la velocità in bit di destinazione e fornire una buona qualità video in base all'archiviazione specificata.

Nota

- Questa opzione è disponibile solo per la registrazione continua. Le telecamere devono supportare la velocità in bit medio e disporre del firmware 9.40 o versioni successive.
- Le impostazioni di velocità in bit medie influenzano la qualità del profilo di streaming selezionato.

1. Andare a **Configuration > Storage > Selection (Configurazione, Archiviazione, Selezione)** e assicurarsi di aver impostato un tempo di conservazione limitato per la telecamera.
2. Andare a **Configuration > Devices > Stream profiles (Configurazione > Dispositivi > Profili di streaming)** e assicurarsi di usare il formato H.264 o H.265 per il profilo video impiegato per la registrazione continua.
3. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Metodo di registrazione**.
4. Seleziona la telecamera e attiva **Continuous (Continua)**.
5. In **Video settings (Impostazioni video)**, selezionare il profilo video configurato.
6. Attivare **Average bitrate (Velocità in bit media)** e impostare **Max storage (Spazio di archiviazione massimo)**. Il sistema mostra la velocità in bit media stimata sulla base dello spazio di archiviazione

massimo specificato e al periodo di conservazione. La velocità di trasmissione media massima è 50000 kbit/s.

Nota

**Max storage (Spazio di archiviazione massimo)** indica lo spazio massimo per le registrazioni durante il tempo di conservazione. Assicura unicamente che le registrazioni non superino lo spazio specificato, non che sia presente spazio sufficiente per le registrazioni.

7. fare clic su **Applica**;

### Modificare impostazioni di movimento

Se il dispositivo usa un AXIS Object Analytics, si possono modificare le impostazioni per la registrazione del movimento.

Nota

AXIS Object Analytics in AXIS Camera Station Pro richiede AXIS OS 12.4.

1. Apri una scheda **Configuration (Configurazione)**.
2. Andare a **Recording and events (Registrazione ed eventi)** > **Recording method (Metodo di registrazione)**.
3. Selezionare la telecamera in cui si desidera eseguire la configurazione.
4. Attivare **Motion detection (Rilevazione movimento)**.
5. Fare clic su **Motion settings (Impostazioni movimento)**.

Leggere il *manuale per l'utente AXIS Object Analytics* per sapere come configurare AXIS Object Analytics sul dispositivo.

### Modifica di AXIS Video Motion Detection 2 e 4

AXIS Video Motion Detection 2 e 4 sono applicazioni per telecamere destinate ai prodotti che supportano la piattaforma AXIS Camera Application Platform. Se nella telecamera è installato AXIS Video Motion Detection 2 o 4, il rilevamento del movimento rileva oggetti in movimento all'interno di un'area di interesse. Motion detection 2 richiede firmware 5.60 o successivo mentre AXIS Video Motion Detection 4 richiede firmware 6.50 o successivo. Per verificare se Video Motion Detection 4 è supportato, è possibile inoltre consultare le note di rilascio del firmware del dispositivo.

Se si seleziona la registrazione del movimento quando si aggiungono le telecamere ad AXIS Camera Station Pro, AXIS Video Motion Detection 2 e 4 verranno installati sulle telecamere con il firmware richiesto. Le telecamere senza il firmware richiesto utilizzano il rilevamento del movimento integrato. È possibile installare l'applicazione manualmente dalla pagina di gestione dei dispositivi. Vedere *Installare le applicazioni per telecamera*.

Con AXIS Video Motion Detection 2 e 4, è possibile creare:

- **Area di interesse**: un'area in una registrazione in cui la telecamera rileva oggetti in movimento. La funzionalità ignora gli oggetti al di fuori dell'area di interesse. L'area viene visualizzata sopra l'immagine video sotto forma di poligono. L'area può avere da 3 a 20 punti (angoli).
- **Area da escludere**: un'area all'interno dell'area di interesse che ignora gli oggetti in movimento.
- **Ignora filtri**: crea filtri per ignorare gli oggetti in movimento rilevati dall'applicazione. Utilizzare meno filtri possibile e configurarli con attenzione per assicurarsi che non vengano ignorati oggetti importanti. Utilizzare e configurare un filtro alla volta.
  - **Short-lived objects filter (Filtro movimenti di breve durata)**: questo filtro ignora gli oggetti che vengono visualizzati per un breve periodo di tempo nell'immagine. Ad esempio, i fasci luminosi da un'auto che passa e le ombre che si muovono rapidamente. Impostare il tempo minimo di visualizzazione degli oggetti nell'immagine affinché venga attivato un allarme. Il tempo viene calcolato dal momento in cui l'applicazione rileva l'oggetto. Il filtro ritarda gli allarmi e non li attiva se l'oggetto scompare dall'immagine entro il tempo specificato.
  - **Small objects filter (Filtro oggetti piccoli)**: Questo filtro ignora gli oggetti di piccole dimensioni, come gli animali. Impostare la larghezza e l'altezza espressa in percentuale dell'immagine totale.

Il filtro ignora gli oggetti più piccoli rispetto alla larghezza e all'altezza specificate e non attivano allarmi. L'oggetto deve essere più piccolo dei valori di larghezza e altezza affinché il filtro lo ignori.

– **Swaying objects filter (Filtro oggetti ondulanti)**: Questo filtro ignora gli oggetti che si spostano solo per una breve distanza, ad esempio foglie ondulanti, bandiere e le relative ombre. Impostare la distanza come percentuale dell'immagine totale. Il filtro ignora gli oggetti che si spostano a una distanza più breve rispetto alla distanza dal centro dell'ellissi a una delle punte di freccia. L'ellissi è una misura di movimento e si applica a tutti i movimenti presenti nell'immagine.

Per configurare le impostazioni di movimento:

Nota

Queste impostazioni vengono applicate direttamente alla telecamera.

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Metodo di registrazione**.
2. Selezionare una telecamera con AXIS Video Motion Detection 2 o 4 e fare clic su **Motion Settings (Impostazioni movimento)**.
3. Modifica area di interesse.
4. Modifica area di esclusione.
5. Creare filtri di falso allarme.
6. fare clic su **Applica**;

| | |
|---|---|
| **Aggiungere un nuovo punto** | Per aggiungere un nuovo punto all'area di interesse, fare clic sulla linea tra due punti. |
| **Remove Point (Rimuovi punto)** | Per rimuovere un punto dall'area di interesse, fare clic sul punto, quindi su **Remove Point (Rimuovi punto)**. |
| **Add Exclude Area (Aggiungi area di esclusione)** | Per creare un'area di esclusione, fare clic su **Add Exclude Area (Aggiungi area di esclusione)** e fare clic sulla linea tra due punti. |
| **Remove Exclude Area (Rimuovi area di esclusione)** | Per rimuovere un'area di esclusione, fare clic su **Rimuovi area di esclusione**. |
| **Short lived objects filter (Filtro movimenti di breve durata):** | Per usare un filtro per oggetti di breve durata, selezionare **Short lived objects filter (Filtro oggetti di breve durata)** e usare la barra **Time (Tempo)** per regolare il tempo minimo in cui l'oggetto deve essere visualizzato nell'immagine per attivare un allarme. |
| **Small objects filter (Filtro oggetti piccoli)** | Per usare un filtro per piccoli oggetti, selezionare **Small objects filter (Filtro oggetti piccoli)** e usare i cursori **Width (Larghezza)** e **Height (Altezza)** per regolare le dimensioni degli oggetti ignorati. |
| **Swaying objects filter (Filtro oggetti ondulanti)** | Per usare il filtro per gli oggetti ondulanti, selezionare **Swaying objects filter (Filtro oggetti ondulanti)** e usare il cursore **Distance (Distanza)** per regolare le dimensioni dell'ellissi. |

### Modifica di rilevamento movimento incorporato

Grazie al rilevamento del movimento integrato, la telecamera può rilevare il movimento all'interno di una o più aree incluse e ignora tutti gli altri movimenti. Un'area di inclusione è un'area che rileva il movimento. È possibile utilizzare più aree di inclusione ed esclusione e inserire un'area di esclusione all'interno di un'area di inclusione per ignorare movimenti specifici.

Per aggiungere e modificare un'area di inclusione:

Nota

Queste impostazioni vengono applicate direttamente alla telecamera.

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Metodo di registrazione**.
2. Selezionare una telecamera con rilevamento del movimento integrato e fare clic su **Impostazioni movimento**.
3. Fare clic su **Add (Aggiungi)** nella sezione Finestra.
4. Selezionare **Include (Includi)**.
5. Per visualizzare solo l'area che stai modificando, selezionare **Show selected window (Mostra finestra selezionata)**.
6. Spostare e ridimensionare la forma nell'immagine video. Questa è l'area di inclusione.
7. Regolare **Object size (Dimensioni oggetto)**, **History (Storia)**, e **Sensitivity (Sensibilità)**.
8. Per utilizzare le impostazioni predefinite, selezionare **Low (Basso)**, **Moderate (Moderato)**, **High (Alto)**, o**Very High (Molto alto)**. **Bassa** rileva gli oggetti più grandi con una cronologia più breve. **Molto alta** Rileva gli oggetti più piccoli con una cronologia maggiore.
9. Nella sezione **Activity (Attività)**, esaminare il movimento rilevato nell'area di inclusione. I picchi rossi indicano il movimento. Utilizzare il campo **Activity (Attività)** per impostare **Object size (Dimensioni oggetto)**, **History (Cronologia)** e **Sensitivity (Sensibilità)**.
10. Fare clic su **OK**.

| | |
|---|---|
| **Protezione da** | le dimensioni dell'oggetto relative alle dimensioni della regione. La telecamera rileva solo gli oggetti molto grandi a un livello alto. Impostando un livello basso, può rilevare anche oggetti di dimensioni molto piccole. |
| **Cronologia** | La durata della memoria degli oggetti definisce il tempo per il quale un oggetto deve trovarsi in un'area prima di essere considerato non in movimento. Impostando un livello alto, un oggetto attiva il rilevamento del movimento per un lungo periodo di tempo. Impostando un livello basso, un oggetto attiva il rilevamento di movimento per un breve periodo di tempo. Se nell'area non devono comparire oggetti, è possibile selezionare un livello di cronologia molto alto. Ciò attiva il rilevamento del movimento se l'oggetto è presente nell'area. |
| **Sensibilità** | differenza di luminanza tra lo sfondo e l'oggetto. Con alta sensibilità, la telecamera rileva oggetti con colori ordinari visualizzati su sfondi normali. Con una sensibilità bassa rileva solo oggetti molto luminosi su sfondo scuro. Per rilevare solo una luce lampeggiante, selezionare una bassa sensibilità. In altri casi, si consiglia un alto livello di sensibilità. |

**Per aggiungere e modificare un'area di esclusione:**

1. Nella schermata **Edit Motion Detection (Modifica rilevamento movimento)**, fare clic su **Add (Aggiungi)** nella sezione **Window (Finestra)**.
2. Selezionare **Exclude (Escludi)**.
3. Spostare e ridimensionare la forma ombreggiata nell'immagine video.
4. Fare clic su **OK**.

**Per rimuovere un'area di inclusione o di esclusione:**

1. Nella schermata **Edit Motion Detection (Modifica rilevamento movimento)**, selezionare un'area da rimuovere.
2. Fare clic su **Remove (Rimuovi)**.
3. Fare clic su **OK**.

### Configurazione delle categorie di eventi

Le categorie degli eventi consentono di trovare più facilmente le registrazioni di un determinato tipo. Per creare una categoria di eventi:

1. Andare a **Configuration** > **Recording and events** > **Event categories**.
2. Fare clic su **New..** (Nuovo).
3. Inserire un nome per la categoria di eventi.
4. In alternativa, è possibile impostare un colore per la categoria di eventi e un tempo di conservazione personalizzato per la categoria di eventi.
5. fare clic su **Applica**;

| | |
|---|---|
| **Nome** | Si consiglia di utilizzare per la categoria un nome che rappresenti un tipo di evento, come ad esempio un'aggressione o un blocco del traffico. |
| **Tempo di archiviazione** | È possibile impostare un tempo di archiviazione personalizzato per ciascuna categoria di eventi, che sostituisce il tempo di archiviazione predefinito della telecamera. Il tempo di archiviazione personalizzato della categoria di eventi è applicabile solo se è più lungo di quello predefinito. |

Per ulteriori informazioni, vedere *Categorie di eventi, on page 28*.

### Porte I/O

Molti codificatori video e videocamere dispongono di porte I/O per il collegamento a dispositivi esterni. Alcuni dispositivi ausiliari possono disporre di porte I/O.

Esistono due tipi di porte I/O:

**Porta di input –** Utilizzata per collegare i dispositivi che commutano tra circuito aperto e chiuso. Ad esempio, contatti di porte e finestre, rilevatori di fumo, sensori di rottura del vetro e sensori PIR (rilevatore passivo a infrarossi);

**Porta di uscita –** Utilizzare questa opzione per connettere dispositivi come relè, porte, serrature e allarmi. AXIS Camera Station Pro può controllare i dispositivi collegati alle porte di output.

Nota

- Quando ci si connette a più server AXIS Camera Station Pro, è possibile selezionare qualsiasi server dal menu a discesa **Selected server (Server selezionato)** per aggiungere e gestire le porte I/O.
- Gli amministratori possono disabilitare le porte I/O per gli utenti. Vedere *Autorizzazioni utente*.

Le regole di azione utilizzano le porte I/O come trigger o azioni. I trigger usano i segnali di input, ad esempio, quando AXIS Camera Station Pro riceve un segnale da un dispositivo collegato alla porta di input, vengono eseguite azioni specifiche. Le azioni usano porte di output, ad esempio quando si attiva una regola, AXIS Camera Station Pro può attivare o disattivare un dispositivo collegato a una porta di output. Vedere *Regole di azione*.

Per informazioni sul collegamento dei dispositivi e sulla configurazione delle porte I/O, consultare il manuale per l'utente o la guida all'installazione del prodotto Axis. Alcuni dispositivi dispongono di porte che possono agire come input o output.

È possibile controllare le porte di output manualmente. Vedere *Monitoraggio porte I/O*.

### Aggiunta di porte I/O

Per aggiungere porte I/O:

1. Andare a **Configurazione > Registrazione ed eventi > Porte I/O**.
2. Fare clic su **Add (Aggiungi)** per visualizzare un elenco di porte I/O che è possibile aggiungere.
3. Selezionare la porta e fare clic su **OK**.
4. Controllare le informazioni in **Type (Tipo)** e **Device (Dispositivo)**. Aggiornare se necessario.
5. Inserire un nome in **Port (Porta)**, **Active State (Stato attivo)** e **Inactive State (Stato inattivo)**. I nomi vengono visualizzati anche in Regole di azione, Log e Monitoraggio I/O.
6. Per le porte di output, si può impostare lo stato iniziale quando AXIS Camera Station Pro si connette al dispositivo. Selezionare **On startup set to (All'avvio imposta su)** quindi selezionare lo stato iniziale nel menu a discesa **State (Stato)**.

| | |
|---|---|
| **Edit (Modifica):** | Per modificare una porta, selezionarla e fare clic su **Edit (Modifica)**. Nella finestra di dialogo, aggiornare le informazioni sulla porta e fare clic su **OK**. |
| **Rimuovi** | Per rimuovere una porta, selezionarla e fare clic su **Remove (Rimuovi)**. |
| **Ricarica porte di I/O** | Se si configurano le porte I/O dalla pagina di configurazione del dispositivo, fare clic su **Reload I/O Ports (Ricarica porte di I/O)** per aggiornare l'elenco. |

### Monitoraggio porte I/O

Nota

Quando si è connessi a più server AXIS Camera Station Pro è possibile selezionare qualsiasi server connesso nel menu a discesa **Selected server (Server selezionato)** per monitorare le porte I/O.

Per controllare le porte di output manualmente:

1. Andare a ☰ > **Actions > I/O Monitoring (Azioni > Monitoraggio I/O)**.
2. Selezionare una porta di output.
3. Fare clic su **Change state (Cambia stato)**.

## Regole di azione

Utilizzare le regole di azione per rispondere automaticamente agli eventi. Ad esempio, inviare un'e-mail quando una telecamera rileva un movimento al di fuori dell'orario di ufficio, interagire con i dispositivi collegati alle porte I/O e inviare un avviso agli operatori in merito a eventi importanti.

Ogni regola dispone di trigger (eventi che attivano la regola), azioni (ciò che accade quando viene attivata) e una pianificazione opzionale. Quando i trigger si attivano, la regola esegue tutte le azioni.

Nota

- Quando ci si connette a più server AXIS Camera Station Pro è possibile selezionare qualsiasi server connesso nel menu a discesa **Selected server (Server selezionato)** per creare e gestire regole di azione.
- Per i dispositivi di terze parti, le azioni disponibili possono variare da dispositivo a dispositivo. Alcune di queste azioni richiedono un'ulteriore configurazione del dispositivo.

**Creazione di una nuova regola di azione**

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **Nuova...**.
3. Immettere un nome per la regola nel campo **Nome**.
4. In **Schedule (Pianificazione)**, selezionare **Always (Sempre)**, oppure **Custom schedule (Pianificazione personalizzata)** per scegliere una pianificazione dal menu a discesa. È possibile anche creare una nuova pianificazione o modificarne una esistente.
5. In **Triggers**, fare clic su **Add... (Aggiungi)**, selezionare il tipo di trigger, configurarlo e fare clic su **OK**. Vedere *Aggiunta di trigger* per ulteriori informazioni.
6. In **Actions (Azioni)**, fare clic su **Add... (Aggiungi)**, selezionare il tipo di azione, configurarlo e fare clic su**OK**. Vedere *Aggiunta di azioni* per ulteriori informazioni.
7. fare clic su **Applica**;
   - La regola è attivata automaticamente al momento del salvataggio.

| | |
|---|---|
| **Edit (Modifica):** | Per modificare una regola esistente, selezionare la regola e fare clic su **Edit (Modifica)**. |
| **Copia** | Per copiare una regola esistente, seleziona la regola e fare clic su **Copy... (Copia)**. |
| **Rimuovi** | Per rimuovere una regola, selezionare la regola e fare clic su **Remove (Rimuovi)**. |

**Configurare più regole di azione**

Quando si selezionano più regole, vengono visualizzati solo i trigger e le azioni che sono uguali in tutte le regole selezionate. Qualsiasi modifica apportata verrà applicata a tutte le regole selezionate.

- Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione.**
- Seleziona molteplici regole.
- Apportare le modifiche:
  - Aggiungere trigger o azioni che si applicheranno a tutte le regole selezionate.
  - Rimuovere i trigger o le azioni comuni da tutte le regole selezionate.
  - Modificare la pianificazione per tutte le regole selezionate.
- fare clic su **Applica**;

Nota

Non è possibile effettuare modifiche singole per trigger o azioni quando sono selezionate più regole. Se le modifiche apportate rendono una regola non valida, non è possibile applicarle.

## Aggiunta di trigger

I trigger attivano regole e una regola può avere più trigger. La regola rimane attiva fino a quando uno dei trigger è attivo. Se tutti i trigger devono essere attivi affinché la regola sia attiva, selezionare **All triggers must be active simultaneously to trigger the actions (Tutti i trigger devono essere attivi simultaneamente per attivare le azioni)**. Se si utilizza questa impostazione con i trigger a impulsi, aumentare il periodo di trigger. I trigger a impulsi sono trigger attivi momentaneamente.

Sono disponibili le seguenti attivazioni:

**Rilevamento del movimento –** Il movimento registrato all'interno di un'area definita attiva il trigger di rilevamento movimento. Vedere *Creazione di trigger di rilevamento del movimento, on page 93*.

**sempre attiva –** Questo trigger è sempre attivo. Ad esempio, si può unire questo trigger a una pianificazione sempre attiva e a un'azione di registrazione con un profilo basso per ottenere una seconda registrazione continua idonea per dispositivi con prestazioni limitate.

**Visualizzazione in diretta –** Il trigger della visualizzazione in diretta scatta quando un utente apre il flusso video di una telecamera in particolare. Si può usare, ad esempio, per informare le persone vicine a una telecamera che sono osservate tramite LED. Vedere *Creazione di trigger della visualizzazione in diretta, on page 94*.

**Evento ed errore di sistema –** Un trigger da evento di sistema e da errore si attiva quando si verificano errori di registrazione, un dispositivo di archiviazione raggiunge la capacità massima, la connessione con un'archiviazione di rete non funziona o la connessione con uno o più dispositivi è interrotta. Vedere *Creazione di trigger da evento di sistema e da errore, on page 94*.

**Input/Output –** Il trigger input/output (I/O) si attiva quando la porta I/O di un dispositivo riceve un segnale, ad esempio da una porta connessa, da un rivelatore di fumo o da un interruttore collegati. Vedere *Creazione di trigger di input/output, on page 95*. Si consiglia di utilizzare le attivazioni di eventi del dispositivo invece delle attivazioni di input/output.

**Evento dispositivo –** Questo trigger utilizza gli eventi direttamente dalla telecamera o dal dispositivo ausiliario. Può essere utilizzato se non ci sono trigger idonei disponibili in AXIS Camera Station Pro. Vedere *Creazione di trigger eventi dispositivo, on page 96*.

**Pulsante azione –** Utilizzare i pulsanti di azione per avviare e interrompere le azioni dalla visualizzazione in diretta. Si può usare un pulsante in regole diverse. Vedere *Creazione di trigger dei pulsanti di azione, on page 101*.

**Evento di AXIS Entry Manager –** Questo trigger si attiva quando AXIS Camera Station Pro riceve segnali dalle porte configurate in AXIS Entry Manager. Ad esempio, porte forzate ad aprirsi, aperte troppo a lungo o accesso negato. Vedere *Crea trigger di eventi di AXIS Entry Manager, on page 102*.

**HTTPS esterno –** Il trigger HTTPS esterno consente alle applicazioni esterne di attivare eventi in AXIS Camera Station Pro tramite comunicazione HTTPS. Vedere *Creazione di trigger HTTPS esterni, on page 102*.

**Body Worn Live –** Il trigger Body Worn Live si attiva quando una body cam avvia un flusso dal vivo. Utilizza questo trigger per configurare le azioni automatiche, ad esempio per portare in primo piano la suddivisione dell'immagine, attivare un allarme o popolare un hotspot dinamico con i flussi video in tempo reale delle body cam. Vedere .

**Ricerca intelligente 2 –** Il trigger Ricerca intelligente 2 si attiva quando la Ricerca intelligente 2 rileva un oggetto che corrisponde a un filtro configurato. Vedere *Creazione di trigger con Smart search 2, on page 103*.

### Creazione di trigger di rilevamento del movimento

Il trigger del rilevamento movimento viene attivato quando la telecamera rileva un movimento in un'area definita. Poiché la telecamera elabora il rilevamento, non aggiunge alcun carico di elaborazione ad AXIS Camera Station Pro.

Nota

Non utilizzare i trigger di rilevamento movimento per avviare le registrazioni se la funzione di registrazione al movimento è già attiva nella telecamera. Disattiva la registrazione del movimento prima di utilizzare i trigger di rilevamento del movimento. Per disabilitare la registrazione del movimento, andare a **Configuration > Recording and events > Recording method (Configurazione > Registrazione ed eventi > Metodo di registrazione)**.

Per creare un trigger rilevamento movimento:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. In **Triggers (Trigger)**, fare clic su **Add (Aggiungi)** e selezionare **Motion detection (Rilevamento movimento)**.
4. Fare clic su **OK**.

5. Nella finestra di dialogo:
   5.1. Selezionare la telecamera che dovrebbe rilevare il movimento.
   5.2. Impostare un intervallo di tempo minimo tra i trigger per ridurre le registrazioni consecutive. Se si verifica un altro trigger in questo intervallo, la registrazione prosegue e il periodo di attivazione ricomincia.
   5.3. Fare clic su **Impostazioni movimento** per configurare le impostazioni di rilevamento del movimento. Le impostazioni disponibili variano a seconda del modello di telecamera. Vedere *Modifica di rilevamento movimento incorporato* e *Modifica di AXIS Video Motion Detection 2 e 4*.
6. Fare clic su **OK**.

**Creazione di trigger della visualizzazione in diretta**

Il trigger della visualizzazione in diretta scatta quando un utente apre il flusso video di una telecamera in particolare. Si può usare, ad esempio, per informare le persone vicine a una telecamera che sono osservate tramite LED.

Per creare un trigger della visualizzazione in diretta:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. In **Triggers (Trigger)**, fare clic su **Add... (Aggiungi)** e selezionare **Live view (visualizzazione in diretta)**.
4. Fare clic su **OK**.
5. Selezionare la telecamera trigger.
6. Fare clic su **OK**.

**Creazione di trigger da evento di sistema e da errore**

Selezionare uno o più eventi di sistema e di errore da utilizzare come trigger. Fra gli esempi di eventi di sistema si annoverano gli errori di registrazione, uno spazio di archiviazione pieno, una connessione con l'archiviazione di rete interrotta e uno o più dispositivi che perdono la connessione.

Per creare un trigger da evento di sistema e da errore:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. In **Triggers (Trigger)**, fare clic su **Add...(Aggiungi)** e selezionare **System event and error (Evento ed errore del sistema**.
4. Fare clic su **OK**.
5. Eseguire la selezione di un evento o un errore di sistema per creare il trigger.
6. Fare clic su **OK**.

| | |
|---|---|
| **In caso di errore di registrazione** | Selezionare **In caso di errore di registrazione** per attivare il trigger quando si verificano errori durante la registrazione, ad esempio se la telecamera interrompe lo streaming. |
| **Sul archiviazione completa** | Selezionare **On full storage (Su archiviazione completa)** per attivare il trigger quando un dispositivo di archiviazione per le registrazioni è pieno. |

| | |
|---|---|
| **Se manca la connessione con l'archiviazione di rete** | Selezionare **On no contact with network storage (Se manca la connessione con l'archiviazione di rete)** per attivare il trigger quando si verifica un problema per accedere all'archiviazione di rete. |
| **On lost connection to camera (In caso di disconnessione dalla videocamera)** | Selezionare **On lost connection to camera (In caso di disconnessione dalla telecamera)** per attivare il trigger quando si verifica un problema per contattare le telecamere.<br>• Selezionare **All (Tutto)** per includere tutte le telecamere aggiunte ad AXIS Camera Station Pro.<br>• Selezionare **Selected (Selezionato)** e fare clic su **Cameras (Telecamere)** per mostrare una lista di tutte le telecamere aggiunte ad AXIS Camera Station Pro. Utilizzare **Select all (Seleziona tutto)** o **Deselect all (Deseleziona tutto)** per selezionare o deselezionare tutte le telecamere. |

### Creazione di trigger di input/output

Il trigger input/output (I/O) si verifica quando la porta I/O di un dispositivo riceve un segnale, ad esempio da una porta, da un rivelatore di fumo o da un interruttore collegati.

Nota

- Aggiungere la porta I/O ad AXIS Camera Station Pro prima di utilizzare un trigger I/O. Vedere *Porte I/O*.
- Si consiglia di utilizzare le attivazioni di eventi del dispositivo invece delle attivazioni di input/output. Per ulteriori informazioni, vedere *Creazione di trigger eventi dispositivo, on page 96*.

Per creare un trigger di input/output:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. In **Triggers (Trigger)**, fare clic su **Add... (Aggiungi)** e selezionare **Input/Output**.
4. Fare clic su **OK**.
5. In **Trigger port and state (Porta e stato di attivazione)**, eseguire la configurazione della porta I/O e delle impostazioni di attivazione.
6. Fare clic su **OK**.

| Porta e stato di attivazione | |
|---|---|
| **Porta I/O** | In **I/O port (Porta I/O)**, selezionare la porta di input o output. |
| **Trigger state (Stato attivazione)** | Nel **Trigger state (Stato attivazione)**, selezionare lo stato della porta I/O che dovrebbe attivare il trigger. Gli stati disponibili dipendono dalla configurazione della porta. |
| **Trigger period (Periodo di attivazione)** | Impostare un intervallo minimo tra due trigger consecutivi per ridurre le registrazioni consecutive. Se si verifica un altro trigger in questo intervallo, la registrazione prosegue e il periodo di attivazione ricomincia. |

### Creazione di trigger eventi dispositivo

Questo trigger utilizza gli eventi direttamente dalla telecamera o dal dispositivo ausiliario. Può essere utilizzato se non ci sono trigger disponibili in AXIS Camera Station Pro. Gli eventi differiscono tra telecamere e sono dotati di uno o molteplici filtri da impostare. I filtri sono condizioni che devono essere soddisfatte affinché avvenga l'attivazione dispositivo da evento. Per informazioni sugli eventi e sui filtri dei dispositivi Axis, vedere la documentazione VAPIX® in *axis.com/partners* e *axis.com/vapix*

Per creare un trigger eventi dispositivo:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. In **Triggers (Trigger)**, fare clic su **Add... (Aggiungi...)** e selezionare **Device event (Evento dispositivo)**.
4. Fare clic su **OK**.
5. In **Configure device event trigger (Configura attivazione dispositivo da evento)**, configurare il trigger evento.

Nota

Gli eventi disponibili dipendono dal dispositivo selezionato. Per i dispositivi di terze parti, molti di questi eventi possono richiedere la configurazione aggiuntiva del dispositivo.

6. In **Filters (Filtri)**, selezionare i filtri.
7. In **Activity (Attività)**, rivedere lo stato corrente del trigger eventi del dispositivo in funzione del tempo. Un evento può essere dotato o privo di stato. Una funzione a gradini indica un evento con stato. Una linea retta con impulsi indica un evento senza stato.
8. Fare clic su **OK**.

| Configura l'attivazione di evento sul dispositivo | |
|---|---|
| **Dispositivo** | In **Device (Dispositivo)**, selezionare la telecamera o il dispositivo ausiliario. |
| **Evento** | In **Event (Evento)**, selezionare l'evento da utilizzare come trigger. |
| **Trigger period (Periodo di attivazione)** | Impostare un intervallo minimo tra due trigger consecutivi per ridurre le registrazioni consecutive. Se si verifica un altro trigger in questo intervallo, la registrazione prosegue e il periodo di attivazione ricomincia. |

### Esempi di eventi dispositivo

| Categoria | Evento dispositivo |
|---|---|
| Amplificatore | Sovraccarico amplificatore |
| Comandi audio | Stato del segnale digitale |
| Sorgente audio | Rilevamento audio |
| Autorizzazione | Richiesta di accesso concessa |
| | Richiesta di accesso negata |
| Chiamata | Stato |
| | Modifica stato |
| | Qualità di rete |

| | |
|---|---|
| | Stato account SIP |
| | Video in ingresso |
| Alloggiamento | Alloggiamento aperto |
| Dispositivo | Protezione da sovracorrente con alimentazione ad anello |
| Sensori dispositivo | Sistema pronto |
| | Sensore PIR |
| Stato dispositivi | Sistema pronto |
| Porta | Porta forzata |
| | Rilevata manomissione installazione porta |
| | Porta bloccata (serrata) |
| | Porta aperta troppo a lungo |
| | Posizione della porta |
| | Porta sbloccata |
| Buffer eventi | Inizio |
| Registro eventi | Allarmi eliminati |
| | Eventi eliminati |
| | Allarme |
| Ventola | Stato |
| GlobalSceneChange | Servizio immagini |
| Errore hardware | Errore di archiviazione |
| | Guasto ventola |
| Riscaldatore | Stato |
| Porte di ingresso | Ingresso virtuale |
| | Porta di ingresso digitale |
| | Attivazione manuale |
| | Porta di ingresso supervisionata |
| | Porta di output digitale |
| | Input esterno |
| Luce | Stato |
| LightStatusChanged | Stato |
| Media | Profilo modificato |
| | Configurazione modificata |
| Monitoraggio | Heartbeat |
| MotionRegionDetector | Movimento |
| Rete | Interruzione connessione di rete |

| | |
|---|---|
| | Applicabile solo agli eventi utilizzati dal dispositivo, non applicabile agli eventi utilizzati da AXIS Camera Station Pro. |
| | Indirizzo aggiunto |
| | Indirizzo rimosso |
| Spostamento PTZ | Movimento PTZ sul canale <channel name> |
| Preimpostazioni PTZ | Preset PTZ raggiunto sul canale <channel name> |
| Controller PTZ | Rilevamento automatico |
| | Coda di controllo PTZ |
| | Errore PTZ |
| | PTZ pronta |
| Configurazione registrazione | Creare una registrazione |
| | Eliminare una registrazione |
| | Tracciare una configurazione |
| | Configurazione registrazione |
| | Registrazione configurazione lavoro |
| Telecamera remota | Stato Vapix |
| | Posizione PTZ |
| Pianificazione | Pulse (Impulso): |
| | Intervallo |
| | Evento pianificato |
| Stato | Attivo |
| Magazzino | Interruzione archiviazione |
| | Registrazione in corso |
| Messaggio di sistema | Azione non riuscita |
| Antimanomissione | Inclinazione rilevata |
| | Urto rilevato |
| Sensori di temperatura | Sopra la temperatura di esercizio |
| | Sotto la temperatura di esercizio |
| | All'interno dell'intervallo della temperatura di esercizio |
| | Sopra o sotto la temperatura di esercizio |
| Attivazione | Relè e output |
| | Ingresso digitale |
| Rilevamento di oggetti in movimento nel video | VMD 4: profilo <profile name> |
| | VMD 4: qualsiasi profilo |
| Video Motion Detection 3 | VMD 3 |

| | |
|---|---|
| Sorgente video | Allarme movimento |
| | Accesso al flusso dal vivo |
| | Visualizzazione diurna/notturna |
| | Manomissione telecamera |
| | Degradazione della velocità di trasmissione media |
| | Sorgente video connessa |

**Eventi dispositivo door controller di rete Axis**

| Evento dispositivo | Attivazione della regola di azione |
|---|---|
| **Autorizzazione** | |
| Richiesta di accesso concessa | Il sistema ha permesso a un titolare tessera di accedere quando si è identificato con le proprie credenziali. |
| Coercizione | Qualcuno ha impiegato il proprio PIN di coercizione. Si può usare, ad esempio, per attivare un allarme silenzioso. |
| Richiesta di accesso negata | Il sistema ha rifiutato l'accesso a un titolare tessera quando si è identificato con le proprie credenziali. |
| Doppia passata | Un titolare tessera ha passato la propria tessera due volte. La doppia passata permette al titolare tessera la sovrascrittura dello stato corrente di una porta. Ad esempio, ha la possibilità di usarla per lo sblocco di una porta al di fuori della pianificazione normale. |
| Rilevamento anti-passback | Qualcuno ha impiegato le credenziali di un titolare che è entrato prima in una zona. |
| **Authorization with two-person rule (Autorizzazione con regola per due persone)** | |
| Richiesta di accesso in sospeso | Il primo dei due titolari di carte si è identificato con le proprie credenziali. |
| Richiesta di accesso concessa | Il sistema ha permesso all'ultimo titolare tessera di accedere quando si è identificato con le proprie credenziali. |
| **Alloggiamento** | |
| Alloggiamento aperto | Qualcuno ha aperto o rimosso l'alloggiamento del door controller di rete. Utilizzarla, ad esempio per inviare una notifica all'amministratore se l'alloggiamento è stato aperto a scopo di manutenzione o se qualcuno l'ha manomesso. |
| **Stato dispositivi** | |
| Sistema pronto | Il sistema è pronto all'uso. Ad esempio, il dispositivo Axis rileva lo stato del sistema e invia una notifica all'amministratore quando il sistema è stato avviato. Selezionare **Yes (Sì)** per attivare la regola di azione quando il dispositivo si trova nello stato Pronto. La regola si potrà attivare solo quando tutti i servizi necessari, ad esempio il sistema di eventi, si sono avviati. |
| **Porta** | |
| Porta forzata | La porta è stata forzata. |

| | |
|---|---|
| Rilevata manomissione installazione porta | Quando il sistema rileva quanto segue:<br>• Alloggiamento del dispositivo è aperto o chiuso<br>• Movimento dispositivo.<br>• Rimozione del lettore collegato dalla parete<br>• Manomissione con il monitor porta, lettore o dispositivo REX collegato. Per usare questo trigger, accertarsi di attivare **Supervised input (Input supervisionato)** e ispezionare l'installazione dei resistori terminali sulle relative porte di input del relativo connettore porta. |
| Porta bloccata (serrata) | La serratura è bloccata. |
| Porta aperta troppo a lungo | La porta è aperta troppo a lungo. |
| Posizione della porta | Il monitor porta indica che la porta è aperta o chiusa. |
| Porta sbloccata | La serratura rimane sbloccata. È possibile, ad esempio, utilizzare questo stato quando ai visitatori è consentito aprire una porta senza necessità di presentare le credenziali. |
| **Porte di ingresso** | |
| Ingresso virtuale | Uno degli ingressi virtuali cambia stato. Un client, ad esempio un software di gestione, può usarlo per inizializzare varie azioni. Selezionare la porta di input che deve attivare la regola di azione quando diventa attiva. |
| Porta di ingresso digitale | Una porta digitale di ingresso cambia stato. Utilizzare questo trigger per avviare varie azioni, ad esempio l'invio di una notifica o far lampeggiare il LED di stato. Selezionare la porta di input che deve attivare la regola di azione quando diventa attiva, oppure selezionare **Any (Qualsiasi)** per attivare la regola di azione quando una delle porte di input diventa attiva. |
| Attivazione manuale | Attiva il trigger manuale. Utilizzare questo trigger per avviare o arrestare manualmente la regola di azione tramite l'API VAPIX. |
| Input esterno | L'ingresso di emergenza è attivo o inattivo. |
| **Rete** | |
| Interruzione connessione di rete | La rete perde la connessione.<br><br>Vale solo per gli eventi relativi ai dispositivi, non per quelli utilizzati da AXIS Camera Station Pro. |
| Indirizzo aggiunto | Viene aggiunto un nuovo indirizzo IP. |
| AddressRemoved | L'indirizzo IP viene rimosso. |
| **Pianificazione** | |
| Evento pianificato | Una pianificazione predefinita cambia stato. Utilizzarlo per registrare video in periodi specifici, ad esempio durante l'orario d'ufficio o nei fine settimana. Selezionare una pianificazione nel menu a discesa **Schedule (Pianificazione)**. |
| **Messaggio di sistema** | |
| Azione non riuscita | Una regola di azione ha esito negativo e attiva il messaggio di sistema non riuscito. |

| Attivazione | |
|---|---|
| Ingresso digitale | Una porta di input digitale fisica è attiva o inattiva. |

**Creazione di trigger dei pulsanti di azione**

Usare i pulsanti di azione per avviare e interrompere le operazioni nella visualizzazione in diretta. I pulsanti di azione si trovano in basso nella visualizzazione in diretta o in una mappa. Si può usare un pulsante per molteplici telecamere e mappe e ci possono essere molteplici pulsanti azione per una telecamera o una mappa. È possibile disporre i pulsanti per una telecamera quando si aggiunge o si modifica un pulsante di azione per una telecamera.

Esistono due tipi di pulsanti di azione:

**Pulsanti di comando –** Usato per l'avvio manuale di un'azione. Utilizzare i pulsanti di comando per azioni che non richiedono un pulsante di interruzione. Un pulsante di comando ha un'etichetta e una descrizione del comando. L'etichetta pulsante è il testo mostrato sul pulsante. Passare il puntatore del mouse sul pulsante affinché appaia la descrizione del pulsante.

**Esempio:** Creare un pulsante per l'attivazione di un'output per un periodo predefinito, la generazione di un allarme e l'invio di un'e-mail.

**Pulsanti commutatori –** Utilizzato per l'avvio e l'arresto manuale di un'azione. Il pulsante ha due stati: attiva e disattiva. Fare clic sul pulsante alternare i due stati. Per impostazione predefinita, i pulsanti commutatori avviano l'azione quando si trovano nello stato di attivazione, ma si può anche avviare l'azione nello stato di disattivazione.
Un pulsante commutatore ha un'etichetta "attiva", un'etichetta "disattiva" e una descrizione del comando. I testi visualizzati sui pulsanti negli stati "attiva" e "disattiva" sono le etichette attiva e disattiva. Passare il puntatore del mouse sul pulsante affinché appaia la descrizione del pulsante.

**Esempio:** Creare un pulsante per aprire e chiudere porte, usare l'azione di uscita con impulso impostato su "Finché il trigger è attivo".

Per creare un trigger per il pulsante di azione:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. In **Triggers (Trigger)**, fare clic su **Add... (Aggiungi...)** e selezionare **Action Button (Pulsante azione)**.
4. Fare clic su **OK**.
5. Selezionare **Crea nuovo pulsante** o **Usa pulsante esistente**. Fare clic su **Next (Avanti)**.
6. Se è stata selezionata l'opzione **Create new button (Crea nuovo pulsante)**:
   6.1. Selezionare **Command button (Pulsante comando)** o **Toggle button (Pulsante commutatore)**. Se si desidera utilizzare il pulsante commutatore per avviare l'azione in stato inattivo, selezionare **Attivazione con pulsante in stato inattivo**.
   6.2. Fare clic su **Next (Avanti)**.
   6.3. Aggiungere le etichette e la descrizione del pulsante.

Nota

La lettera o il numero successivo al primo carattere di sottolineatura nell'etichetta di un pulsante di azione diventa la chiave di accesso al pulsante di azione. Premere Alt e la chiave di accesso per attivare il pulsante azione. Ad esempio, quando si nomina un pulsante di azione A_BC, il nome del pulsante viene modificato in ABC nella visualizzazione in diretta. Premere Alt + B per attivare il pulsante azione.

7. Se si seleziona l'opzione **Use existing button (Usa pulsante esistente)**:
   7.1. Cercare il pulsante o fare clic sul pulsante che si vuole utilizzare.
   7.2. Se si sceglie un pulsante commutatore esistente, si deve selezionare **Trigger on toggle (Attivazione a pulsante attivo)** o **Trigger on untoggle (Attivazione con pulsante inattivo)**.

7.3. Fare clic su **Next (Avanti)**.

7.4. Modificare le etichette e la descrizione del pulsante.

8. Selezionare la telecamera o la mappa dal menu a discesa.
9. Per aggiungere il pulsante a più telecamere o mappe, fare clic su **Aggiungi a più telecamere** o **Aggiungi a più mappe**.
10. Se una telecamera ha più pulsanti di azione, fare clic su **Arrange (Disponi)** per modificare l'ordine dei pulsanti. Fare clic su **OK**.
11. Fare clic su **Next (Avanti)**.

### Crea trigger di eventi di AXIS Entry Manager

AXIS Camera Station Pro attiva il trigger quando riceve segnali dalle porte configurate in AXIS Entry Manager. Ad esempio, porte forzate, porte aperte troppo a lungo o accesso negato.

Nota

Il trigger evento di AXIS Entry Manager è disponibile unicamente quando si aggiunge AXIS A1001 Network Door Controller a AXIS Camera Station Pro.

Per creare un trigger dell'evento di AXIS Entry Manager:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. In **Triggers (Trigger)**, fare clic su **Add... (Aggiungi)** e selezionare **AXIS Entry Manager event (Evento AXIS Entry Manager)**.
4. Fare clic su **OK**.
5. Per attivare il trigger, selezionare un evento e una porta.
6. Fare clic su **OK**.

### Creazione di trigger HTTPS esterni

Il trigger HTTPS esterno consente alle applicazioni esterne di attivare eventi in AXIS Camera Station Pro tramite comunicazione HTTPS. Questo trigger supporta solo la comunicazione HTTPS e unl nome utente valido di AXIS Camera Station Pro comprensivo di nome di dominio e password per richieste HTTPS.

Le richieste seguenti sono supportate con il metodo GET* HTTP. È inoltre possibile utilizzare POST con dati JSON indicati nel corpo della richiesta.

Nota

- Le richieste di trigger HTTPS esterne possono essere testate solo in Google Chrome.
- Il trigger HTTPS esterno utilizza le stesse porte dell'app di visualizzazione mobile: vedere porta per la comunicazione mobile e porta per lo streaming mobile in *Impostazioni del server generali*.
- Activate the trigger with ID "trigger1": (Attiva il trigger con ID "trigger1":) `https://[address]:29204/Acs/Api/TriggerFacade/ActivateTrigger?{"triggerName":"trigger1"}`
- Deactivate the trigger with ID "trigger1": (Disattiva il trigger con ID "trigger1":) `https://[address]:29204/Acs/Api/TriggerFacade/DeactivateTrigger?{"triggerName":"trigger1"}`
- Activate the trigger with ID "trigger1" and then automatically deactivate the trigger after 30 seconds: (Attiva il trigger con ID "trigger1", quindi disattivalo automaticamente dopo 30 secondi:) `https://[address]:29204/Acs/Api/TriggerFacade/ActivateDeactivateTrigger?{"triggerName":"trigger1","deactivateAfterSeconds":"30"}`

Nota

Il timer per la disattivazione automatica viene annullato se viene emesso qualsiasi altro comando per lo stesso trigger.

- Pulse the trigger with ID "trigger1" (trigger activation followed by immediate deactivation): (Consenti il trigger con ID "trigger1" (attivazione del trigger seguita da una disattivazione immediata): `https://[address]:29204/Acs/Api/TriggerFacade/PulseTrigger?{"triggerName":"trigger1"}`

Per creare un trigger HTTPS esterno:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. fare clic su **New (Nuovo)**.
3. In **Triggers (Trigger)**, fare clic su **Add... (Aggiungi)** e selezionare **External HTTPS (HTTPS esterno)**.
4. Fare clic su **OK**.
5. Immettere il nome del trigger in **Trigger name (Nome trigger)**.
6. Controllare l'URL di esempio, che utilizza lo stesso indirizzo del server utilizzato dal client per effettuare l'accesso. Gli URL funzionano solo al completamento della regola di azione.
7. Fare clic su **OK**.

**Azioni adatte per trigger HTTPS esterni**

- Le richieste per attivare e disattivare il trigger sono adatte per azioni che consentono l'avvio e l'arresto delle registrazioni.
- Le richieste per consentire il trigger sono adatte per azioni quali **Raise Alarm (Genera allarme)** o **Send Email (Inviare e-mail)**.

### Creazione di trigger con Smart search 2

Il trigger Ricerca intelligente 2 si attiva quando la Ricerca intelligente 2 rileva un oggetto che corrisponde a un filtro configurato. Il trigger si attiva quando l'oggetto esce dalla scena, non quando viene rilevato per la prima volta.

Per creare un trigger di Smart search 2:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. In **Triggers (Trigger)**,fare clic su **Add... (Aggiungi)** e selezionare **Smart search 2 (Ricerca intelligente 2)**.
4. Fare clic su **OK**.
5. Selezionare e configurare il trigger:
   - Per creare un filtro di ricerca intelligente da utilizzare come un trigger, consultare *Attivazioni, on page 175*.
   - Selezionare **High processing delay (Ritardo di elaborazione elevato)** per attivare il trigger ogni volta che Smart search 2 impiega più di un minuto per elaborare i rilevamenti.
6. Fare clic su **OK**.

### Creare trigger AXIS Audio Manager

Per creare un trigger AXIS Audio Manager:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. In **Triggers (Trigger)**, fare clic su **Add... (Aggiungi...)** e selezionare **Audio manager (Gestore audio)**.
4. Fare clic su **OK**.
5. Selezionare e configurare il trigger.
6. Fare clic su **OK**.

| | |
|---|---|
| **Stato dispositivo modificato** | Selezionare **Device status changed (Stato dispositivo modificato)** per attivare il trigger quando lo stato del dispositivo cambia, ad esempio quando si connette o si disconnette. |
| **Stato riproduzione modificato** | Selezionare **Playback status changed** (Stato riproduzione modificato) per attivare il trigger all'avvio o all'arresto della riproduzione. |
| **Target abilitato o disabilitato** | Selezionare **Target enabled or disabled (Target abilitato o disabilitato)** per attivare il trigger quando il target del trigger è abilitato o disabilitato. |
| **Volume del controllo del volume modificato** | Selezionare **Volume controller volume changed** (Volume del controllo del volume modificato) per attivare il trigger quando l'impostazione del controllo del volume cambia. |

## Aggiunta di azioni

Una regola può includere più azioni. Le azioni cominciano nel momento in cui la regola si attiva.

Sono disponibili le seguenti operazioni:

**Registrazione –** Avvia una registrazione dalla telecamera. Vedere *Creazione di azioni di registrazione*.

**Generare allarmi –** Esegue l'invio di un allarme a tutti i client AXIS Camera Station Pro connessi. Vedere *Creazione di azioni di allarme*.

**Impostare uscite –** Imposta lo stato di una porta di output. Usarla per comandare un dispositivo collegato alla porta di output, ad esempio per azionare una luce o bloccare una porta. Vedere *Creazione di azioni di uscita*.

**Invio e-mail –** Inviare un'e-mail a uno o più destinatari. Vedere *Creazione delle azioni di invio e-mail*.

**Visualizzazione in diretta –** Apre la visualizzazione in diretta di una specifica telecamera, vista o posizione preset in tutti i client AXIS Camera Station Pro. È possibile usare anche l'azione Visualizzazione in diretta per ripristinare client aperti dalla barra delle applicazioni o portare i client in primo piano rispetto ad altre applicazioni aperte. Vedere *Creazione di azioni della visualizzazione in diretta*.

**Inviare notifiche HTTP –** Invia una richiesta HTTP a una telecamera, a un door controller o a un server web esterno. Vedere *Creazione di azioni di notifica HTTP*.

**Sirena e luce –** Attiva una sirena e uno schema luminoso su un dispositivo compatibile in base a un profilo preconfigurato. Vedere *Crea azioni sirena e luce, on page 110*.

**I/O virtuale –** Attiva una specifica porta di ingresso virtuale in un dispositivo. Vedere *Crea azioni I/O virtuali, on page 110*

**AXIS Entry Manager –** Consente l'accesso, sblocca o applica il blocco a una porta collegata a un door controller configurato tramite AXIS Entry Manager. Vedere *Crea azioni di AXIS Entry Manager, on page 111*.

**Invia notifica dell'app per dispositivo mobile –** Invia un messaggio personalizzato all'app per dispositivi mobili AXIS Camera Station. Vedere *Creazione di azioni di invio di notifica all'app per dispositivi mobili, on page 111*.

**Attiva o disattiva regole –** Attiva o disattiva altre regole di azione. Vedere *Crea un'azione che attivi o disattivi altre regole di azione, on page 112*.

**Invia al decodificatore video –** Invia una vista a un decodificatore video per la visualizzazione su un monitor per un periodo di tempo specificato. Vedere *Creare un'azione che invii una vista a un decodificatore video, on page 112*

**Controllo accessi –** Include azioni porta e zona in AXIS Camera Station Secure Entry. Vedere *Crea azioni di controllo degli accessi, on page 113*.

### Creazione di azioni di registrazione

L'azione di registrazione avvia una registrazione dalla telecamera. Accedere e riprodurre le registrazioni dalla scheda **Recordings (Registrazioni)**.

Per creare un'azione di registrazione:

1. Specificare dove salvare la registrazione: andare a **Configuration > Storage > Selection (Configurazione, Archiviazione, Selezione)**.
2. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
3. Fare clic su **New..** (Nuovo).
4. Fare clic su **Aggiungi** e creare un trigger. Fare clic su **Next (Avanti)**. Vedere *Aggiunta di trigger*.
5. Fare clic su **Aggiungi** e selezionare **Registra**.
6. Fare clic su **OK**.
7. In **Camera (Telecamera)**, selezionare la telecamera da cui registrare.
8. In **Video setting (Impostazione video)**, configurare profilo, pre-buffer e post-buffer.
9. Nella sezione **Event setting (Impostazione evento)**, selezionare una categoria di evento per la registrazione, se del caso.
10. Fare clic su **OK**.

| Impostazione video | |
|---|---|
| **Profilo** | Selezionare un profilo dal menu a discesa **Profile (Profilo)**. Per modificare le impostazioni del profilo, vedere *Profili di flusso*. |
| **Pre-buffer** | Impostare quanti secondi precedenti al movimento rilevato vanno inclusi in una registrazione. |
| **Post-buffer** | Impostare il numero di secondi da includere nella registrazione quando l'azione non è più in corso. |

### Creazione di azioni di allarme

L'azione Genera allarme invia un allarme a tutti i client AXIS Camera Station Pro connessi. L'allarme viene visualizzato nella scheda **Alarms (Allarmi)** e sotto forma di notifica nella barra delle applicazioni. È possibile allegare un file contenente le procedure relative all'allarme. La procedura di allarme è disponibile dalle schede **Allarmi** e **Registri**.

Per creare un'azione Genera allarme:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. Fare clic su **Add (Aggiungi)** e immettere un nome. Fare clic su **Next (Avanti)**. Vedere *Aggiunta di trigger*.
4. Fare clic su **Aggiungi** e selezionare **Genera allarme**.
5. Fare clic su **OK**.
6. In **Alarm message (Messaggio allarme)**, configurare titolo, descrizione e durata.
7. Aprire **Alarm procedure (Procedura allarme)**.
   - 7.1. Selezionare **On alarm show alarm procedure (Se si attiva allarme, mostra procedura allarme)**.
   - 7.2. Fare clic su **Upload (Carica)** e trovare il file.
   - 7.3. Fare clic su **Preview (Anteprima)** per visualizzare l'anteprima del file.
   - 7.4. Fare clic su **OK**.

| Messaggio allarme | |
|---|---|
| **Titolo (Title)** | Immettere un titolo per l'allarme. Il titolo appare su **Alarms (Allarmi)** nella scheda **Alarms (Allarmi)** e nella notifica della barra delle applicazioni. |
| **Descrizione** | Immettere una descrizione dell'allarme. La descrizione compare in **Alarms > Description (Allarmi > Descrizione)** nella scheda **Alarms (Allarmi)** e nella notifica della barra delle applicazioni. |
| **Duration (s) (Durata (s))** | Impostare una durata tra 1 e 600 secondi per le notifiche. |

### Creazione di azioni di uscita

L'operazione di uscita imposta lo stato di una porta di uscita. Usarla per i comandi del dispositivo collegato alla porta di output, ad esempio per attivvare una luce o bloccare una porta.

Nota

Aggiungere una porta di output ad AXIS Camera Station Pro prima di utilizzare l'azione di output. Vedere *Porte I/O*.

Per creare un'azione di output:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. Fare clic su **Add (Aggiungi)** e immettere un nome. Fare clic su **Next (Avanti)**. Vedere *Aggiunta di trigger*.
4. Fare clic su **Aggiungi** e selezionare **Imposta uscita**.
5. Fare clic su **OK**.
6. In **Output port (Porta di output)**, selezionare la porta di output.
7. In **State on action (Stato sull'azione)** selezionare lo stato su cui impostare la porta. Le opzioni disponibili dipendono dalla configurazione porta.
8. Selezionare **Pulse (Impulso)** per definire la durata del nuovo stato per porta di output.

Nota

Per tenere la porta nel nuovo stato dopo un'azione, deselezionare l'opzione **Impulso**.

9. Fare clic su **OK**.

| | |
|---|---|
| **Fino a quando è abilitata l'attivazione** | Per tenere la porta nel nuovo stato finché sono attivi tutti gli elementi attivatori della regola, selezionare **Fino a quando è abilitata l'attivazione**. |
| **Mantenere lo stato per un periodo fisso** | Per tenere la porta nel nuovo stato per un tempo fissato, selezionare **Keep the state for a fixed time (Mantieni lo stato per un tempo fissato)** e specificare il numero di secondi. |

### Creazione delle azioni di invio e-mail

L'azione e-mail invia una e-mail a uno o più destinatari. È possibile allegare all'e-mail le istantanee scattate con le fotocamere.

Nota

Per inviare e-mail, si deve configurare prima un server SMTP. Vedere *Impostazioni server*.

Per creare un'azione di invio e-mail:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. Fare clic su **Add (Aggiungi)** e immettere un nome. Fare clic su **Next (Avanti)**. Vedere *Aggiunta di trigger*.
4. Fare clic su **Aggiungi** e selezionare **Invia e-mail**.
5. Fare clic su **OK**.
6. Nella sezione **Recipients (Destinatari)**, aggiungere gli indirizzi e-mail:
   6.1. inserire l'indirizzo e-mail in **New Recipient (Nuovo destinatario)** e selezionare **To (A)**, **Cc** o **Bcc (Ccn)**.
   6.2. Fare clic su **Aggiungi**.
7. In **Contents (Contenuto)**, inserire l'oggetto e il messaggio dell'e-mail.
8. In **Advanced (Avanzate)**, configurare allegati, numero di e-mail e intervalli.
9. Fare clic su **OK**.

| Avanzata | |
|---|---|
| **Attach snapshots (Allega istantanee)** | Per allegare istantanee .jpg dalle telecamere come allegati, selezionare **Attach snapshots (Allega istantanee)** e fare clic su **Cameras (Telecamere)**. Appare un elenco di tutte le telecamere aggiunte ad AXIS Camera Station Pro. Usare **Select all (Selezionare tutto)** per selezionare tutte le telecamere o **Deselect all (Deselezionare tutto)** per annullare la selezione. |
| **Send one email for each event (Inviare un'e-mail per ogni evento)** | Per evitare l'invio di più e-mail per lo stesso evento, selezionare **Send one email for each event (Invia un'unica e-mail per ogni evento)**. |
| **Don't send another email for (Non inviare un'altra e-mail per)** | Per evitare di inviare e-mail a intervalli troppo ravvicinati, selezionare **Don't send another email for (Non inviare un'altra e-mail per)** e impostare l'intervallo minimo tra le e-mail dal menu a discesa. |

**Creazione di azioni della visualizzazione in diretta**

L'azione visualizzazione in diretta apre una specifica telecamera, una vista o una posizione preset nella scheda **Live view (Visualizzazione in diretta)** su tutti i client AXIS Camera Station Pro collegati. Se la scheda **Live view (Visualizzazione in diretta)** mostra un'immagine suddivisa con un hotspot, la telecamera selezionata nell'azione della visualizzazione in diretta appare nell'hotspot. Per ulteriori informazioni sugli hotspot, vedere *Suddivisione dell'immagine*.

È possibile usare anche l'azione Visualizzazione in diretta per ripristinare client AXIS Camera Station Pro aperti dalla barra delle applicazioni o portarli in primo piano rispetto ad altre applicazioni aperte.

Per creare un'azione della visualizzazione in diretta:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. Fare clic su **Add (Aggiungi)** e immettere un nome. Fare clic su **Next (Avanti)**. Vedere *Aggiunta di trigger*.
4. Fare clic su **Aggiungi** e selezionare **Visualizzazione in diretta**.
5. Fare clic su **OK**.

6. In **Live view actions (Azioni visualizzazione in diretta)**, configurare cosa mostrare quando l'azione è attiva.
7. In **Shown in (Mostra in)**, eseguire la configurazione del modo di mostrare la vista selezionata.
8. In **Bring to front (Porta in primo piano)**, selezionare **On trigger bring application to front (In caso di attivazione, porta l'applicazione in primo piano)** per ripristinare i client AXIS Camera Station Pro aperti dalla barra delle attività o per portarli in primo piano rispetto alle altre applicazioni aperte quando viene avviata l'azione.
9. Fare clic su **OK**.

| Imposta l'immagine dal vivo | |
|---|---|
| **Visualizza** | Selezionare **View (Vista)**, quindi scegliere una vista dal menu a discesa. |
| **Telecamera** | Selezionare **Camera (Telecamera**, quindi selezionare una telecamera dall'elenco a discesa. Se la telecamera ha un preset PTZ, selezionare **Go to preset (Vai a preset)** e selezionare un'area dal menu a discesa per aprire una posizione preset. |
| **Nessuna operazione** | Selezionare **No action (Nessuna azione)** se non si desidera aprire una vista. |

| Mostrato in | |
|---|---|
| **Scheda Avviso dal vivo** | Seleziona la scheda **Live alert tab (Avviso dal vivo)** per l'apertura della vista selezionata o della vista della telecamera nella scheda **Live alert (Avviso dal vivo)**. |
| **Hotspot in view (Hotspot nella vista)** | Seleziona **Hotspot in view (Hotspot nella vista)** e selezionare una vista dotata di hotspot dal menu a discesa. Se si vede l'hotspot nella visualizzazione in diretta al momento dell'attivazione dell'azione, la vista della telecamera appare nell'hotspot. |

**Esempio:**
In questo esempio vengono utilizzate due azioni di isualizzazione in diretta nella stessa regola di azione.

1. Creare un'azione di visualizzazione in diretta che mostri la vista dell'hotspot nella scheda **Live alert (Avviso dal vivo)**.
   1.1. In **Live view actions (Azioni visualizzazione in diretta)**, selezionare **View (Vista)**.
   1.2. Selezionare **Hotspot view (Vista hotspot)**.
   1.3. In **Show in (Mostra in)**, seleziona la **Live alert tab (Scheda avviso dal vivo)**.
   1.4. Seleziona **On trigger bring application to front (In caso di attivazione, visualizza l'applicazione in primo piano)**.
2. Creare un'altra azione di visualizzazione in diretta che mostri la vista hotspot e la vista della telecamera nell'hotspot.
   2.1. In **Live view actions (Azioni visualizzazione in diretta)**, selezionare **Camera (Telecamera)** e poi una vista della telecamera.
   2.2. In **Show in (Mostra in)**, selezionare **Hotspot in view (Hotspot nella vista)**.
   2.3. Selezionare **Hotspot view (Vista hotspot)**.

### Creazione di azioni di notifica HTTP

L'operazione di notifica HTTP invia una richiesta HTTP a un destinatario. Il destinatario può essere una telecamera, un door controller, un server Web esterno o un qualsiasi server in grado di ricevere richieste HTTP. Ad esempio, è possibile utilizzare le notifiche HTTP per attivare o disattivare una funzione della telecamera, oppure per aprire, chiudere, applicare il blocco o sbloccare una porta collegata a un door controller.

GET e POST, PUT i metodi sono supportati.

Nota

Per mandare notifiche HTTP ai destinatari fuori dalla rete locale, potrebbe essere necessario regolare le impostazioni proxy del server AXIS Camera Station Pro. Contattare il supporto Axis per ulteriori informazioni.

Per creare un'azione di notifica HTTP:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. Fare clic su **Add (Aggiungi)** e immettere un nome. Vedere *Aggiunta di trigger*.
4. Fare clic su **Add (Aggiungi)** e selezionare **Send HTTP notification (Invia notifica HTTP)**.
5. In **URL**, immettere l'indirizzo del destinatario e lo script che gestisce la richiesta. Ad esempio: `https://192.168.254.10/cgi-bin/notify.cgi`
6. Per inviare la notifica ogni volta che si attiva un trigger, selezionare **Send on every trigger (Invia ad ogni trigger)**.
7. Selezionare **Autenticazione richiesta** se il destinatario richiede l'autenticazione. Immettere il nome utente e la password.
8. Selezionare un metodo di autenticazione.
9. Nella scheda **Advanced (Avanzato)**, imposta il metodo, il tipo di contenuto e il corpo della richiesta.
10. Fare clic su **OK**.
11. Fare clic su **Save (Salva)**.

| Metodo di autenticazione | |
|---|---|
| **Digest** | Si consiglia questa opzione in quanto offre la migliore protezione contro le intercettazioni. |
| **Digest con base come fallback** | Utilizzare questa opzione se non si è certi del metodo di autenticazione utilizzato dal dispositivo. |

| Avanzata | |
|---|---|
| **Metodo** | Selezionare un metodo HTTP dal menu a discesa **Method (Metodo)**. |
| **Tipo di contenuto** | Per i metodi POST e PUT, selezionare il tipo di contenuto dal menu a discesa **Content type (Tipo di contenuto)**. |
| **Corpo** | Per i metodi POST e PUT, immettere il corpo richiesta in **Body (Corpo)**. Formattare il corpo in modo che corrisponda al tipo di contenuto selezionato. Ad esempio, un JSON valido se è stata selezionata l'applicazione/json. |
| **Trigger data (Dati trigger)** | si possono anche immettere dati trigger predefiniti dal menu a discesa. |

| Trigger data (Dati trigger) | |
|---|---|
| **Tipo di trigger** | Identifica il tipo di trigger che ha attivato la regola di azione. |
| **ID server** | Identifica il server che ha attivato la regola di azione. |
| **Ora (UTC)** | la data e ora UTC di attivazione della regola di azione. |
| **Time (local) (Ora (locale))** | La data e l'ora del server al momento dell'attivazione della regola di azione. |
| **Source ID (ID sorgente)** | Identifica la fonte che ha triggerato la regola di azione. Spesso si tratta di una telecamera o di un altro tipo di dispositivo. Non tutte le fonti ne hanno uno. |
| **Source Name (Nome sorgente)** | Il nome della fonte che ha triggerato la regola di azione. Spesso si tratta di una telecamera o di un altro tipo di dispositivo. Non tutte le fonti ne hanno uno. |
| **Device ID (ID dispositivo)** | Identifica il dispositivo che ha attivato la regola di azione. Non tutti i trigger ne hanno uno. |
| **ID telecamera** | Identifica la telecamera che ha attivato la regola di azione. Non tutti i trigger ne hanno uno. |
| **Istantanea della telecamera** | Un'istantanea JPEG codificata in Base64 proveniente dalla telecamera che ha attivato la regola di azione. Non tutti i trigger ne hanno uno. |
| **Nome dell'evento** | Il nome dell'evento che ha attivato la regola di azione. Non tutti i trigger ne hanno uno. |
| **Stato dell'evento** | Lo stato dell'evento che ha attivato la regola di azione. Non tutti i trigger ne hanno uno. |

### Crea azioni I/O virtuali

Utilizzare azioni I/O virtuali per attivare una specifica porta di input virtuale in un dispositivo. È possibile utilizzare ogni porta di un dispositivo per un'azione.

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. Fare clic su **Add (Aggiungi)** e immettere un nome. Fare clic su **Next (Avanti)**. Vedere *Aggiunta di trigger*.
4. Fare clic su **Add (Aggiungi)** e selezionare **Virtual I/O (I/O virtuale)**.
5. Fare clic su **OK**.
6. Selezionare il dispositivo e la porta che si vuole attivare.
7. Fare clic su **OK**.

### Crea azioni sirena e luce

L'azione sirena e luce attiva un pattern di sirena e luce su AXIS D4100-E Network Strobe Siren in base ad un profilo configurato.

Nota

Per impiegare tale azione, si deve configurare un profilo dalla pagina di configurazione del dispositivo.

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. Fare clic su **Add (Aggiungi)** e immettere un nome. Fare clic su **Next (Avanti)**. Vedere *Aggiunta di trigger*.
4. Fai clic su **Add (Aggiungi)** e seleziona **Siren and light (Sirena e luce)**.
5. Fare clic su **OK**.
6. Seleziona un dispositivo dal menu a discesa **Device (Dispositivo)**.
7. Selezionare un profilo dal menu a discesa **Profile (Profilo)**.
8. Fare clic su **OK**.

### Crea azioni di AXIS Entry Manager

L'azione AXIS Entry Manager consente l'accesso, apre o chiude una porta collegata ad un door controller configurato da AXIS Entry Manager.

Nota

L'azione AXIS Entry Manager è disponibile unicamente quando AXIS A1001 Network Door Controller è disponibile in AXIS Camera Station Pro.

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. Fare clic su **Add (Aggiungi)** e immettere un nome. Fare clic su **Next (Avanti)**. Vedere *Aggiunta di trigger*.
4. Fare clic su **Add (Aggiungi)** e selezionare **AXIS Entry Manager**.
5. Fare clic su **OK**.
6. Selezionare un'azione e la porta a cui applicarla.
7. Fare clic su **OK**.

### Creazione di azioni di invio di notifica all'app per dispositivi mobili

L'azione di invio di una notifica all'app per dispositivi mobili invia un messaggio personalizzato all'app AXIS Camera Station Mobile. È possibile toccare la notifica ricevuta per passare alla visualizzazione di una specifica telecamera. Vedere il *manuale per l'utente dell'app AXIS Camera Station Mobile*.

Per creare un'azione di invio di notifica all'app per dispositivi mobili:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. Fare clic su **Add (Aggiungi)** e immettere un nome. Fare clic su **Next (Avanti)**. Vedere *Aggiunta di trigger*.
4. Fare clic su **Add (Aggiungi)** e selezionare **Send mobile app notification (Invia notifica al'app per dispositivi mobili)**.
5. Fare clic su **OK**.
6. Nel campo **Message (Messaggio)**, inserire il messaggio da visualizzare nell'app mobile.
7. In **Click notification and go to (Clicca su notifica e vai a)**, configurare cosa deve apparire quando tocca la notifica.
8. Fare clic su **OK**.

| Fare clic su notifica e vai a | |
|---|---|
| **Telecamera** | Selezionare una vista della telecamera da mostrare quando si tocca la notifica. |
| **Ripristino dei valori predefiniti di fabbrica** | Selezionare **Default (Predefinito)** per passare alla pagina iniziale dell'app mobile quando si tocca la notifica. |

### Crea un'azione che attivi o disattivi altre regole di azione

Utilizzare questa azione, ad esempio, per disattivare il rilevamento movimento in un ufficio quando un dipendente striscia la propria tessera di accesso.

Per creare un'azione attiva o disattiva regole:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. Fare clic su **Add (Aggiungi)** e immettere un nome. Fare clic su **Next (Avanti)**. Vedere *Aggiunta di trigger*.
4. Fare clic su **Add (Aggiungi)** e selezionare **Turn rules on or off (Attiva o disattiva regole)**.
5. Fare clic su **OK**.
6. Selezionare una o più regole di azione.
7. Scegliere se si desidera l'attivazione o disattivazione delle regole di azione selezionate.
8. Inserire un ritardo se si vuole aggiungere tempo tra l'attivazione e la modifica dello stato.
9. Selezionare **Return to the previous state when the trigger is no longer active (Torna allo stato precedente quando l'attivazione non è più attiva)** se non si desidera che la regola di azione selezionata resti modificata quando il trigger non è attivo. Nell'esempio precedente, questo vuol dire che il rilevamento movimento si riattiva quando il dipendente rimuove la tessera di accesso dal lettore.
10. Fare clic su **OK**.

### Creare un'azione segnalibro

Un'azione segnalibro aggiunge un segnalibro a una registrazione nel momento in cui si attiva la regola di azione.

Per creare un'azione segnalibro:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. Fare clic su **Add (Aggiungi)** e immettere un nome. Fare clic su **Next (Avanti)**. Vedere *Aggiunta di trigger*.
4. Fare clic su **Add** (Aggiungi) e selezionare **Add bookmark** (Aggiungi segnalibro).
5. Fare clic su **OK**.
6. Configurare il segnalibro inserendo un nome e, se lo si desidera, una descrizione.
7. Fare clic su **OK**.

### Creare un'azione che invii una vista a un decodificatore video

Utilizzare questa azione per inviare una vista a un decodificatore video per la visualizzazione su un monitor per un periodo di tempo specificato.

Per creare azione di invio a decodificatore video:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.

2. Fare clic su **New..** (Nuovo).
3. Fare clic su **Add (Aggiungi)** e immettere un nome. Fare clic su **Next (Avanti)**. Vedere *Aggiunta di trigger*.
4. Fare clic su **Add** e selezionare **Send to video decoder**.
5. Fare clic su **OK**.
6. In **Decoder**, selezionare il decoder video a cui inviare la vista.
7. In **View**, selezionare la telecamera o la vista da inviare.
8. Nel campo **Duration (Durata)**, inserire per quanti secondi deve essere visualizzata la vista.
9. Fare clic su **OK**.

### Crea azioni di controllo degli accessi

L'azione di controllo degli accessi può eseguire le seguenti azioni in AXIS Camera Station Secure Entry:

- **Door actions (Azioni porta):** concedono accesso, blocco, sblocco, ripristino o arresto delle porte selezionate.
- **Zone actions (Azioni zona):** blocco, sblocco, ripristino o arresto di porte selezionate in zone selezionate.
- **Access rule actions (Azioni di regole di accesso):** attivano o disattivano le regole di accesso.

Nota

L'azione di controllo degli accessi è unicamente a disposizione per AXIS Camera Station Secure Entry.

Per creare un'azione di controllo accessi:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. Fare clic su **Add (Aggiungi)** e immettere un nome. Fare clic su **Next (Avanti)**. Vedere *Aggiunta di trigger*.
4. Fare clic su **Add (Aggiungi)** e selezionare **Access control (Controllo degli accessi)**.
5. Fare clic su **OK**.
6. Per eseguire le azioni porta:
   6.1. In **Access control (Controllo degli accessi)**, selezionare **Door actions (Azioni porta)**.
   6.2. Selezionare le porte e l'azione in **Configure action (Configura azione)**.
7. Per eseguire azioni zona:
   7.1. In **Access control (Controllo degli accessi)**, selezionare **Zone actions (Azioni zona)**.
   7.2. Selezionare le zone, i tipi di porta e l'azione in **Configure action (Configura azione)**.
8. Per attivare o disattivare le regole di accesso:
   8.1. In **Access control (Controllo degli accessi)**, selezionare **Action rule actions (Azioni regole di accesso)**.
   8.2. In **Configure action (Configura azione)**, selezionare la regola di accesso da attivare o disattivare.
   8.3. In **Action (Azione)**, selezionare **Enable (Abilita)** o **Disable (Disabilita)**.
9. Fare clic su **OK**.

- Per salvare un report nell'ambito dell'azione, selezionare **Save report (Salva report)** e configurare le impostazioni del report.

### Creare azioni per AXIS Audio Manager

L'azione AXIS Audio Manager controlla la riproduzione audio e le impostazioni del volume sui dispositivi audio collegati.

Per creare un'azione AXIS Audio Manager:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. Fare clic su **Add (Aggiungi)** e immettere un nome. Fare clic su **Next (Avanti)**. Vedere *Aggiunta di trigger*.
4. Fare clic su **Add** (Aggiungi) e selezionare **Audio manager**.
5. Fare clic su **OK**.
6. Selezionare e configurare l'azione che si desidera attivare.
7. Fare clic su **OK**.

| Azioni AXIS Audio Manager | |
|---|---|
| **Riproduci file audio** | Selezionare **Play audio file** (Riproduci file audio) per riprodurre il file audio selezionato. È inoltre possibile effettuare la configurazione dei parametri di riproduzione, quali il numero di ripetizioni, la priorità e il profilo visivo. |
| **Interrompere il file Audio** | Selezionare **Stop audio file (Interrompi file audio)** per interrompere la riproduzione dell'audio. |
| **Abilita o disabilita target** | Selezionare **Enable or disable target (Abilita o disabilita destinazione)** per attivare o disattivare i dispositivi. |
| **Silenzia volume** | Selezionare **Mute volume** (Silenzia volume) per disattivare il controllo del volume. |
| **Imposta volume** | Selezionare **Set volume (Imposta volume)** per regolare il volume di un controller del volume. Il valore può essere positivo o negativo. |
| **Regolazione volume** | Selezionare **Offset volume** per aumentare o diminuire il volume rispetto al livello attuale. Inserire un valore positivo per aumentarlo oppure un valore negativo per diminuirlo. |

## Pianificazioni

La pagina Pianificazioni contiene tutte le pianificazioni che è possibile applicare alle registrazioni, alle regole di azione e a componenti quali AXIS Secure Entry. Alcuni processi di pianificazione vengono creati automaticamente durante l'installazione tramite AXIS Site Designer.

È possibile creare e modificare panificazioni giornaliere e settimanali personalizzate, nonché sovrascrivere gli orari predefiniti. Le pianificazioni sostitutive sono sempre giornaliere, ma è possibile applicarle sia alle pianificazioni giornaliere che a quelle settimanali in date particolari, come nei giorni festivi.

La scheda **Schedules** (Pianificazioni) è la vista principale per la gestione di tutti gli orari giornalieri e settimanali:

- **Nome**: Il nome della pianificazione.
- **Tipo**: Indica se la pianificazione è giornaliera o settimanale.
- **In uso**: Indica se un componente, una regola di registrazione o una regola d'azione sta utilizzando la pianificazione.
- **Sovrascrivi pianificazioni**: Elenca le pianificazioni di intervento applicabili a questa pianificazione.

La scheda **Override schedules (Pianificazioni intervento)** è la vista principale per la gestione delle pianificazioni di intervento, dove è possibile vedere quali pianificazioni giornaliere e settimanali sono state applicate agli interventi.

Nota

Quando sussiste la connessione a molteplici server AXIS Camera Station Pro, si può eseguire l'aggiunta e la gestione di pianificazioni su qualsiasi server connesso. Eseguire la selezione del server dal menu a discesa **Selected server (Server selezionato)** per eseguire la gestione delle pianificazioni.

**Gestire le pianificazioni giornaliere e settimanali**

Per gestire le pianificazioni giornaliere e settimanali, accedere alla scheda **Schedules** (Pianificazioni).

Per creare una nuova pianificazione giornaliera o settimanale, fare clic su **New schedule** (Nuova pianificazione).

Per eliminare una pianificazione, selezionarla dall'elenco e fare clic su **Delete** (Elimina). Prima di eliminarla, assicurarsi che la pianificazione non sia in uso.

Creare o selezionare una pianificazione giornaliera o settimanale per visualizzarne i dettagli.

- Se si tratta di una pianificazione giornaliera, fare clic su **Add dates** (Aggiungi date) per aggiungere un nuovo intervallo di date alla pianificazione. È possibile aggiungere più intervalli di date alla stessa pianificazione giornaliera.
- Per aggiungere una fascia oraria, fare clic su **+** oppure fare doppio clic sulla riga.
- Per modificare un intervallo di date o una fascia oraria, fare clic su di esso con il tasto sinistro del mouse.
- Per aggiungere una pianificazione di intervento, selezionarla dal menu a discesa e fare clic su **Add** (Aggiungi). Per rimuovere una pianificazione di intervento, selezionarla dall'elenco e fare clic su **Remove** (Rimuovi).
- Fare clic su **Apply (Applica)** per salvare le modifiche.

**Gestire le pianificazioni di intervento**

- Per gestire le pianificazioni di intervento, accedere alla scheda **Override schedules** (Pianificazioni di intervento).
- Fare clic su **Add dates (Aggiungi date)** per aggiungere un nuovo intervallo di date alla pianificazione. È possibile aggiungere più intervalli di date alla stessa pianificazione di intervento.
- Per aggiungere una fascia oraria, fare clic su **+** oppure fare doppio clic sulla riga.
- Per modificare un intervallo di date o una fascia oraria, fare clic su di esso con il tasto sinistro del mouse.
- Fare clic su **Apply (Applica)** per salvare le modifiche.

## Esempi di regole di azione.

### Esempio: Apertura forzata porta

**Apertura forzata porta**

Questo esempio mostra come impostare una regola di azione in AXIS Camera Station Pro che attiva una registrazione e un allarme quando qualcuno forza la porta di ingresso.

Prima di iniziare, è necessario:

- Installare un door controller di rete Axis. Vedere *Aggiungi dispositivi, on page 47*.
- Configurare il door controller. Vedere *Aggiunta di una porta, on page 150*.

Creare la regola di azione:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).

3. Aggiungere l'evento porta forzata come trigger:
   3.1. Fare clic su **Aggiungi** e selezionare **Evento dispositivo**.
   3.2. Fare clic su **OK**.
   3.3. In **Configure device event trigger (Configura attivazione dispositivo da evento)**, configurare le impostazioni di attivazione.
   3.4. In **Filters (Filtri)**, eseguire la configurazione delle impostazioni dei filtri.
   3.5. In **Activity (Attività)**, assicurarsi che il trigger mostri attività sulla linea del segnale.
   3.6. Fare clic su **OK**.
4. Fare clic su **Next (Avanti)**.
5. Aggiungere un'operazione di registrazione:
   5.1. Fare clic su **Aggiungi** e selezionare **Registra**.
   5.2. Fare clic su **OK**.
   5.3. Selezionare una telecamera dal menu a discesa **Camera (Telecamera)**.
   5.4. In **Video setting (Impostazione video)**, configurare profilo, pre-buffer e post-buffer.
   5.5. Fare clic su **OK**.
6. Aggiungere un'azione genera allarme:
   6.1. Fare clic su **Aggiungi** e selezionare **Genera allarme**.
   6.2. Fare clic su **OK**.
   6.3. In **Alarm message (Messaggio di allarme)**, inserire un titolo e una descrizione per l'allarme. Ad esempio, "l'ingresso principale è stato forzato".
   6.4. Fare clic su **OK**.
7. Fare clic su **Next (Avanti)** e selezionare **Always (Sempre)** come pianificazione.
8. Fare clic su **Finish (Fine)**.

| Configura l'attivazione di evento sul dispositivo | |
|---|---|
| **Dispositivo** | Selezionare un door controller di rete Axis dal menu a discesa **Device** (Dispositivo). |
| **Evento** | Selezionare **Door > Door forced (Porta > Apertura forzata della porta)** dal menu a discesa **Event (Evento)**. |
| **Trigger period (Periodo di attivazione)** | Impostare 10 secondi come **Trigger period (Periodo di attivazione)**. |

| Filtri | |
|---|---|
| **Nome porta** | Selezionare la porta dal menu a discesa **Door name (Nome porta)**. |
| **Stato porta** | Selezionare **Forced (Forzata)** dal menu a discesa **Door status (Stato porta)**. |

| Impostazioni video | |
|---|---|
| **Profilo** | Selezionare **High (Alto)** dal menu a discesa **Profile (Profilo)**. |
| **Pre-buffer** | Impostare 3 secondi come **Prebuffer (Pre-buffer)**. |
| **Post-buffer** | Impostare 5 secondi come **Postbuffer (Post-buffer)**. |

## Esempio: Quando una persona importante entra

**Quando una persona importante entra**

Questo esempio mostra come creare una regola di azione in AXIS Camera Station Pro che riproduce un messaggio di benvenuto e chiama l'ascensore quando entra una persona importante.

Prima di iniziare, è necessario:

- Installare e configurare door controller di rete Axis e aggiungere titolari di tessere. Vedere *Configurazione del controllo degli accessi, on page 146* e *Gestione degli accessi, on page 186*.
- Installare un dispositivo audio di rete Axis e associarlo a una telecamera. Vedere *Profili di flusso, on page 55*.
- Installare AXIS A9188 Network I/O Relay Module, collegare l'I/O all'ascensore e aggiungere le porte I/O del modulo relè I/O di rete ad AXIS Camera Station Pro. Vedere *Porte I/O, on page 90*.

Creare la regola di azione:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. Aggiungere l'evento del dispositivo come trigger:
   - 3.1. Fare clic su **Aggiungi** e selezionare **Evento dispositivo**.
   - 3.2. Fare clic su **OK**.
   - 3.3. In **Configure device event trigger (Configura attivazione dispositivo da evento)**, configurare le impostazioni evento.
   - 3.4. In **Filters (Filtri)**, eseguire la configurazione delle impostazioni dei filtri.
   - 3.5. In **Activity (Attività)**, assicurarsi che il trigger mostri attività sulla linea del segnale.
   - 3.6. Fare clic su **OK**.
4. Fare clic su **Next (Avanti)**.
5. Aggiungere un'azione di invio di notifica HTTP per riprodurre un messaggio di benvenuto:
   - 5.1. Fare clic su **Add (Aggiungi)** e selezionare **Send HTTP notification (Invia notifica HTTP)**.
   - 5.2. Fare clic su **OK**.
   - 5.3. In **URL**, immettere l'URL della clip audio del messaggio di benvenuto.
   - 5.4. Selezionare **Authentication required (Autenticazione richiesta)** e immettere nome utente e password per il dispositivo audio.
   - 5.5. Fare clic su **OK**.
6. Aggiungere un'azione Imposta output:
   - 6.1. Fare clic su **Aggiungi** e selezionare **Imposta uscita**.
   - 6.2. Fare clic su **OK**.
   - 6.3. Dal menu a discesa **Output port (Porta di output)**, selezionare la porta di output del modulo I/O collegato all'ascensore.
   - 6.4. Dal menu a discesa **State on action (Stato sull'azione)** selezionare lo stato del modulo I/O per chiamare l'ascensore.

6.5. Selezionare **Pulse (Impulso)** e impostare la durata a 60 secondi.

6.6. Fare clic su **OK**.

7. Fare clic su **Next (Avanti)** e selezionare **Always (Sempre)** come pianificazione.
8. Fare clic su **Finish (Fine)**.

| Configura l'attivazione di evento sul dispositivo | |
|---|---|
| **Dispositivo** | Selezionare un door controller di rete Axis dal menu a discesa **Device** (Dispositivo). |
| **Evento** | Selezionare **Authorization > Access request granted (Autorizzazione > Richiesta di accesso concessa)** dal menu a discesa **Event (Evento)**. |
| **Trigger period (Periodo di attivazione)** | Impostare 10 secondi come **Trigger period (Periodo di attivazione)**. |

| Filtri | |
|---|---|
| **Nome porta** | Selezionare la porta dal menu a discesa **Door name (Nome porta)**. |
| **Door side (Lato della porta)** | Selezionare il lato della porta dal menu a discesa **Door side (Lato porta)**. |
| **Numero tessera** | Selezionare" **Card number (Codice carta)** e inserire il codice carta della persona. |

## Configurazione client

Andare a **Configurazione > Client** per:

- Modificare le impostazioni specifiche del client, come tema e lingua. Vedere *Impostazioni client, on page 118*.
- Modificare le impostazioni specifiche dell'utente, come notifiche e opzioni di avvio. Vedere *Impostazioni utente, on page 119*.
- Modificare le impostazioni relative alle prestazioni di streaming specifiche del client come ridimensionamento video e decodifica hardware. Vedere *Streaming, on page 121*.

### Impostazioni client

Queste impostazioni si applicano a tutti gli utenti di AXIS Camera Station Pro sul computer. Andare a **Configuration > Client > Client settings (Configurazione, Client, Impostazioni client)**.

| Tema | |
|---|---|
| **System, Light, Dark (Sistema, chiaro, scuro)** | Selezionare il tema per il client. **System (Sistema)** è l'impostazione predefinita per le nuove installazioni.<br><br>Se si seleziona **System (Sistema)**, il tema seguirà quello del sistema Windows. |

| Generale | |
|---|---|
| **Esegui applicazione all'avvio di Windows** | Attivare questa opzione per eseguire in modo automatico AXIS Camera Station Pro all'avvio di Windows. |

| Visualizzazione in diretta | |
|---|---|
| **Mostra i nomi delle telecamere nelle visualizzazioni in diretta** | Mostra i nomi delle telecamere nella visualizzazione in diretta. |
| | Attivare l'opzione **Show recording indicators in live views and maps (Mostra indicatori di registrazione nelle visualizzazioni in diretta e nelle mappe)** per visualizzare un indicatore relativo alle registrazioni con rilevamento movimento o alle registrazioni avviate da una regola di azione. |
| | Attivare l'opzione **Show event indicators in live views and maps (Mostra indicatori evento nelle visualizzazioni in diretta e nelle mappe)** per visualizzare un indicatore relativo alle registrazioni con rilevamento movimento o alle registrazioni avviate da una regola di azione. |

| Mappe | |
|---|---|
| **Allow flashing coverage areas for all maps (Permetti aree di copertura lampeggianti per tutte le mappe)** | Attivare o disattivare questa impostazione per decidere se le aree di copertura debbano lampeggiare su tutte le mappe. Tale impostazione globale non incide sull'impostazione locale a livello mappa. Vedere *Mappa, on page 22*. |

| Lingua |
|---|
| Modificare la lingua del client AXIS Camera Station Pro. Riavviare il client affinché le modifiche siano implementate. |

| Feedback | |
|---|---|
| **Share anonymous client usage data with Axis Communications to help improve the application and user experience (Condividere dati di utilizzo client anonimi con Axis Communications per aiutare a migliorare l'applicazione e l'esperienza utente)** | Condividere dati anonimi con Axis al fine del miglioramento dell'esperienza utente. Per cambiare questa impostazione per il server, vedere *Impostazioni server, on page 126*. |

## Impostazioni utente

Queste impostazioni si applicano all'utente che ha eseguito l'accesso ad AXIS Camera Station Pro. Andare in **Configuration (Configurazione) > Client > User settings (Impostazioni utente)**.

| Sistema di navigazione | |
|---|---|
| **Sistema di navigazione della visualizzazione ad albero** | Attivato per impostazione predefinita. Mostra le viste, le telecamere o entrambe nel riquadro di navigazione. |
| **Show in navigation (Mostra in navigazione)** | Selezionare cosa visualizzare dal menu a discesa: visualizzazioni, telecamere o entrambe. |
| **Mostra percorso di navigazione durante la navigazione nella vista** | Eseguire l'attivazione di questa opzione per mostrare il percorso di navigazione in alto nella vista quando si naviga nella suddivisione dell'immagine. |

| Notifiche | |
|---|---|
| **Mostra notifica allarmi sulla barra delle applicazioni** | Eseguire l'attivazione di questa opzione per mostrare una notifica nella barra delle applicazioni di Windows quando comincia un allarme. |
| **Mostra notifica attività sulla barra delle applicazioni** | Attivare questa opzione per visualizzare una notifica nella barra delle applicazioni di Windows quando viene aggiunta o completata un'attività. |
| **Mostra notifiche in Gestione dei dispositivi** | Eseguire l'attivazione di questa opzione per mostrare notifiche quando è a disposizione un nuovo firmware da scaricare. |
| **Mostra finestra di notifica interfono** | Eseguire l'attivazione di questa opzione per mostrare una finestra di notifica quando si preme il pulsante di chiamata su un sistema interfono connesso. |

| Istantanea | |
|---|---|
| **Quando viene acquisita un'istantanea mostra un messaggio** | Eseguire l'attivazione di questa opzione per mostrare un messaggio quando viene scattata un'istantanea. |
| **Apri la cartella corrispondente al momento dell'acquisizione dell'istantanea** | Eseguire l'attivazione di questa opzione per aprire la cartella delle istantanee quando viene scattata un'istantanea. |
| **Sfoglia** | Fare clic su **Browse (Sfoglia)** per selezionare la cartella in cui salvare l'istantanea. |

| Avvio | |
|---|---|
| **Avvia in modalità Schermo intero** | Attivare questa opzione per avviare AXIS Camera Station Pro in modalità a schermo intero. |
| **Ricorda ultime schede usate** | Attivare per avviare AXIS Camera Station Pro con le stesse schede, viste e viste di telecamera aperte al momento in cui è stato chiuso per l'ultima volta. |
| **Ricorda ultimi monitor usati** | Attivare per avviare AXIS Camera Station Pro sullo stesso monitor utilizzato l'ultima volta che è stato chiuso. |

Nota

- Il sistema salva le viste e le viste della telecamera per scheda. Il sistema le ricorda solo quando il client si riconnette allo stesso server.
- Il sistema non memorizza mai le viste dinamiche che si trascinano nella visualizzazione in diretta.
- Quando sussiste la connessione a molteplici server con utenti diversi, il sistema non supporta **Remember last used tabs (Ricorda ultime schede usate)**

| Suono in caso di allarme | |
|---|---|
| **Nessun segnale** | Selezionare questa opzione per non riprodurre alcun suono quando l'allarme viene triggerato. |
| **Bip** | Selezionare questa opzione per riprodurre un segnale acustico quando l'allarme viene triggerato. |

| Suono in caso di allarme | |
|---|---|
| **Sound file (File audio)** | Selezionare e fare clic su **Browse (Sfoglia)** per utilizzare un file audio personalizzato quando l'allarme viene triggerato. Supporta qualsiasi formato di file compatibile con Windows Media Player. |
| **Riproduci** | Fare clic per testare il suono. |

| Suono in caso di chiamata in arrivo | |
|---|---|
| **Nessun segnale** | Selezionare questa opzione per non riprodurre alcun suono quando arriva una chiamata. |
| **Bip** | Selezionare questa opzione per riprodurre un segnale acustico quando arriva una chiamata. |
| **Sound file (File audio)** | Selezionare e fare clic su **Browse (Sfoglia)** per utilizzare un file audio personalizzato quando arriva una chiamata. Supporta qualsiasi formato di file compatibile con Windows Media Player. |
| **Riproduci** | Fare clic per testare il suono. |

| Caratteristiche | |
|---|---|
| **Mostra ricerca intelligente 1** | Visualizzato per impostazione predefinita. Disattivare per nascondere la Ricerca intelligente 1. |

| Mostra le finestre di avviso | |
|---|---|
| **Avviso di certificato non valido** | Attivare questa opzione per visualizzare un avviso quando viene effettuato il rilevamento di un certificato non valido. |

## Streaming

Andare a **Configuration > Client > Streaming (Configurazione, Client, Streaming)** per configurare le opzioni di streaming del client.

| Ridimensionamento del video | |
|---|---|
| **Ridimensionamento ottimale** | Selezionare di modo che il video si adatti allo spazio disponibile senza ritagliare o modificare le proporzioni. |
| **Compila l'area video (parti del video potrebbero essere tagliate)** | Selezionare questa opzione per riempire lo spazio disponibile con il video. Se le proporzioni dello spazio disponibile differiscono da quelle del video, il sistema ritaglia il video per adattarlo. |

| Decodifica hardware | |
|---|---|
| **Modalità** | • **Automatic (Automatico):** utilizza la scheda grafica per decodificare i flussi con una risoluzione superiore a 3840 x 2160p@25 fps (anche noti come 4K o UHD).<br>• **On (Attivo):** utilizza la scheda grafica per decodificare i flussi con una risoluzione superiore a 1920 x 1080p@25 fps (anche noti come 1080p o HD).<br>• **Off (Disattivato):** AXIS Camera Station Pro utilizza la CPU per decodificare i video. |
| **Scheda grafica** | selezionare una scheda grafica dal menu a discesa. |

| Schede grafiche supportate | Tecnologia dei decodificatori |
|---|---|
| NVIDIA | PureVideo |
| AMD | Decodificatore video unificato (UVD) |
| Intel | Intel Quick Sync Video (QSV) |

Nota

- La decodifica hardware utilizza la scheda grafica per decodificare i video. Con una scheda grafica ad alte prestazioni, la decodifica hardware può migliorare le prestazioni e ridurre l'utilizzo della CPU, soprattutto quando si riproducono in streaming video con una risoluzione alta. La decodifica hardware supporta esclusivamente flussi H.264 e AV1.
- Le telecamere dotate di una risoluzione al di sotto dei 1080p non possono usare la decodifica hardware, anche se attivata.
- Se la scheda grafica non supporta la decodifica 4K, la decodifica hardware funziona unicamente in flussi 1080p, anche se attivata.
- Per la decodifica hardware viene utilizzata una sola scheda grafica, anche su sistemi dotati di più schede grafiche.

| Uso della larghezza di banda | |
|---|---|
| **Usa sempre il profilo di streaming Basso su questo client** | Attivare per impiegare il profilo di streaming basso per la visualizzazione in diretta. Vedere *Profili di flusso*.<br><br>Questa impostazione incide sui video H.264 e M-JPEG e riduce il consumo di banda. |
| **Sospendi flussi video per schede inattive** | Eseguire l'attivazione per sospendere i flussi video nelle schede inattive. Ciò riduce l'uso della larghezza di banda. |

| PTZ (Pan, Tilt, Zoom) | |
|---|---|
| **Selezionare la vista con il primo clic invece di avviare PTZ** | Attivare in modo che il primo clic nella vista lo selezioni. Fare clic su una PTZ per controllarla. |

| Audio | |
|---|---|
| **Push-to-talk release delay (ms) (Ritardo di rilascio di Premi per parlare (ms))** | Imposta, in millisecondi, la durata della trasmissione audio dal microfono dopo aver rilasciato il pulsante **Push-to-talk**. |
| **Utilizzare Premi per parlare per tutte le modalità duplex** | Attivarlo per usare le modalità push-to-talk, simplex, half-duplex e full-duplex. |
| **Consenti sempre l'audio per gli interfoni** | Attivare questa funzione per ascoltare e parlare tramite gli intercom anche quando non ci sono chiamate in corso. |

| Instant replay | |
|---|---|
| **Playback duration (s) (Durata riproduzione (s))** | Imposta la durata della riproduzione tra 1 e 600 secondi per tornare indietro nella sequenza temporale ed eseguire la riproduzione della registrazione. |

## Configura servizi connessi

### Gestire servizi connessi

I servizi connessi ti consentono di ottenere l'accesso a:

- Client desktop e app mobile AXIS Camera Station
- Web client del cloud di AXIS Camera Station
- Gestione automatica delle licenze
- Monitoraggio dell'integrità del sistema

Per eseguire l'accesso ai servizi connessi, è necessario registrare il proprio sistema e connetterlo a un'organizzazione. Per ulteriori informazioni, vedere *Eseguire la registrazione del sistema con un'organizzazione, on page 124*.

Nota

Affinché il server compaia nella directory dei server di ACS Pro, è necessario che l'opzione **Web client** sia attiva nella pagina **Connected services (Servizi connessi)** > **Management (Gestione)**. Se l'opzione è disattivata, il server viene rimosso dalla directory.

| | |
|---|---|
| **Stato** | La scheda di stato mostra lo stato della connessione tra il server e i servizi collegati, nonché il nome della società presso cui si è registrati. |
| **Gestione delle licenze** | Attivare **License management (Gestione delle licenze)** per sincronizzare in automatico le licenze. Il sistema invia le modifiche relative alle licenze ad AXIS License Manager e recupera lo stato aggiornato delle licenze. Disabilitare **License management (Gestione delle licenze)** per la gestione manuale delle licenze, ad esempio se il sistema non ha una connessione Internet. Per ulteriori informazioni, consultare la sezione Gestione delle licenze. Per ulteriori informazioni, vedere *Gestisci le licenze, on page 135*.<br><br>Importante<br>Per accedere alla directory del server ACS Pro in My Systems, è necessario abilitare l'opzione |

| | |
|---|---|
| | Gestione licenze almeno una volta, in qualsiasi momento dopo l'aggiornamento alla versione 6.19 per ciascuna società da un server 6.19. |
| **Accesso sicuro da remoto** | Attivare il client desktop e l'app mobile o il secure remote access tramite client web. È possibile ottenere l'accesso alla directory del server ACS Pro tramite il link. |
| **Swap region (Modifica regione)** | Fare clic su **Swap region... (Modifica regione)** per effettuare la modifica della regione per i servizi connessi. Selezionare una nuova regione dal menu a tendina e fare clic su **Select (Seleziona)** per effettuare la modifica. |
| **Disconnetti** | Fare clic su **Disconnect... (Disconnetti)** per disconnettere il sistema. Quando si disconnette un server, è possibile che questo continui ad apparire nell'elenco dei server della società. |

**Eseguire la registrazione del sistema con un'organizzazione**

Per eseguire la registrazione del sistema:

1. Andare a **Configuration (Configurazione)** > **Connected services (Servizi connessi)** > **Management (Gestione)**.
2. Fare clic su **Register... (Registra...)**.
3. Nella finestra a comparsa **Register server (Registra server)**, selezionare le funzionalità che si desidera utilizzare quindi fare clic su **Select (Seleziona)** per salvare le scelte.
4. Seguire le istruzioni visualizzate sullo schermo per finire la procedura di registrazione.

Per ulteriori informazioni sulla registrazione del sistema, consultare la *Guida all'installazione e alla migrazione di AXIS Camera Station Pro*.

## Impostazioni di aggiornamento firmware

Nota

Quando ci si connette a più server AXIS Camera Station Pro, è possibile selezionare qualsiasi server dal menu a discesa **Selected server (Server selezionato)** per configurare impostazioni degli aggiornamenti del firmware.

1. Andare a **Configurazione > Servizi connessi > Impostazioni di aggiornamento del firmware**.
2. In **Automatic check for updates (Controllo automatico aggiornamenti)**, eseguire la configurazione della frequenza e della modalità di controllo degli aggiornamenti firmware.
3. In **Upgrade order (Ordine aggiornamento)**, eseguire la configurazione dell'ordine di aggiornamento dei dispositivi.

| Controllo automatico aggiornamenti | |
|---|---|
| **Check for updates (Controlla aggiornamenti)** | Selezionare **Every start-up (Ad ogni avvio)** per verificare la presenza di versioni disponibili del firmware ogni volta che il server si avvia. Per impostazione predefinita, AXIS Camera Station Pro è impostato su **Never (Mai)**. |
| **Check now (Controlla adesso)** | Fare clic per controllare se sul server sono disponibili versioni firmware. |

| Ordine di aggiornamento | |
|---|---|
| **Parallelo** | Selezionare per aggiornare tutti i dispositivi contemporaneamente. Questa opzione è più rapida di **Sequential (Sequenziale)** ma tutti i dispositivi sono offline contemporaneamente. |
| **Sequenziale** | Selezionare per aggiornare i dispositivi uno dopo l'altro. Questa opzione impiega più tempo ma evita che i dispositivi siano tutti offline allo stesso tempo. Eseguire la selezione di **Cancel remaining upgrades if one device fails (Annulla aggiornamenti restanti in caso di errore di un dispositivo)** a fermare l'aggiornamento sequenziale. |

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

*Attiva il controllo firmware automatico*

## Axis Secure Remote Access v2

Axis Secure Remote Access v2 permette di connettersi al proprio server AXIS Camera Station Pro mediante una connessione Internet crittografata.

Nota

Axis Secure Remote Access v2 è disponibile per la versione AXIS Camera Station Pro 6.8 o successiva.

Per abilitare Axis Secure Remote Access v2:

1. Eseguire la registrazione del server con un'organizzazione. Vedere *Eseguire la registrazione del sistema con un'organizzazione, on page 124*.
2. Accedere ad Axis Secure Remote Access v2. Vedere *Accedere ad AXIS Secure Remote Access v2, on page 9*.

Per limitare l'accesso ai soli server AXIS Camera Station Pro:

1. Andare a **Organization (Organizzazioni) > Users (Utenti)** in My Systems.
2. Selezionare l'utente di cui si desidera eseguire la configurazione.
3. Fare clic su **Roles and access (Ruoli e accesso).**
4. Assegnare il ruolo **ACS Pro Secure Remote Access**. Questo ruolo limita l'accesso solo ai server AXIS Camera Station Pro senza consentire l'accesso ad altre funzioni di My Systems di Axis.

Una volta registrati, è possibile gestire le autorizzazioni di accesso assegnando i ruoli utente dell'organizzazione in My Systems di Axis. Per ulteriori informazioni sui diritti di accesso dell'utente AXIS Camera Station Pro, vedere *Autorizzazioni utente, on page 136*.

## Archiviazione cloud

AXIS Camera Station Cloud Storage è un servizio con licenza per archiviare le registrazioni nel cloud. Per ulteriori informazioni, vedere *AXIS Camera Station Cloud Storage - Manuale per l'utente*.

Importante

AXIS Camera Station Cloud Storage funziona solo con AXIS Camera Station Pro versione 6.18 o precedenti. Si consiglia di esportare le registrazioni su un'unità di archiviazione locale prima di procedere all'aggiornamento. Se si esegue l'aggiornamento a una versione successiva alla 6.18, il servizio di archiviazione su cloud smetterà di funzionare e si perderanno tutti i dati attualmente memorizzati nel cloud. Gli aggiornamenti di sicurezza per la versione 6.18 proseguiranno fino a quando il supporto per l'archiviazione su cloud non verrà ripristinato in una versione successiva.

Prima di poter utilizzare il servizio di archiviazione cloud, è necessario registrare il proprio sistema con i servizi connessi. Dopo la registrazione del sistema, è possibile gestire lo spazio di archiviazione cloud per le telecamere in My Systems.

## Configurare server

### Impostazioni server

Andare a **Configuration > Server > Settings (Configurazione , Server, Impostazioni)**.

Nota

Quando si è connessi a più server AXIS Camera Station Pro, scegliere qualsiasi server dal menu a discesa **Selected server (Server selezionato)** per configurare le impostazioni del server.

| Esporta | |
|---|---|
| **Includi audio quando si aggiungono registrazioni da esportare** | Selezionarlo per comprendere l'audio quando si aggiunge una registrazione alla lista esportazione. |

Registri

Specificare il numero di giorni di gestione di allarmi, eventi e log di audit. Impostare un valore tra 7 e 1000 giorni.

Per scrivere continuamente i log in un file in tempo reale, affinché possano essere acquisiti da sistemi di terze parti quali Splunk, Elastic o uno strumento SIEM, selezionare **Write audit logs to file (Scrivi log di controllo su file)**, **Write event logs to file (Scrivi log di eventi su file)**, oppure entrambi.

Il server scrive le voci di log nel file `C:\ProgramData\Axis Communications\AXIS Camera Station\Core\Server\Logs`. I file sono in formato di testo semplice e non vengono inclusi nei report di sistema.

| File | Descrizione |
|---|---|
| `AcsService.exe.audit.log.export` | Voci del log di controllo |
| `AcsService.exe.event.log.export` | Voci del registro eventi |

Dati esterni

Specificare il numero di giorni durante i quali vengono conservati i dati esterni. Impostare un valore tra 1 e 1000 giorni.

#### Server SMTP

Aggiungere server SMTP per l'invio di messaggi e-mail se si verificano allarmi di sistema o si attiva una regola di azione evento.

Per aggiungere un server SMTP:

1. In **SMTP servers (Server SMTP)**, fare clic su **Add (Aggiungi)**.

2. In **Server**, eseguire la configurazione dell'indirizzo del server, della porta, dell'autenticazione e del protocollo TLS.
3. Nel campo **Sender (Mittente)**, inserire l'indirizzo e-mail e il nome da visualizzare come mittente.

| Server | |
|---|---|
| **Indirizzo** | Immettere l'indirizzo del server SMTP. |
| **Porta** | Immettere la porta. 587 è la porta predefinita per le connessioni SMTP TLS. |
| **Utilizza TLS** | Selezionare Utilizza TLS se il server SMTP usa TLS. TLS è il protocollo predefinito. |
| **Utilizza autenticazione** | Selezionare questa opzione se il server richiede un nome utente e una password, quindi inserire le credenziali. |

| | |
|---|---|
| **Edit (Modifica):** | Per modificare un server SMTP, selezionare il server e fare clic su **Modifica**. |
| **Rimuovi** | Per rimuovere un server SMTP, selezionare il server e fare clic su **Rimuovi**. Nella finestra di dialgo, fare clic su **Yes (Sì)** per rimuovere il server. |
| **Test all... (Prova tutto...)** | Per provare un server SMTP, selezionare il server e fare clic su **Test all... (Prova tutto...)**. Nella finestra di dialogo, immettere un indirizzo e-mail in **Recipient (Destinatario)** e fare clic su **OK** per inviare una e-mail di prova. Il server SMTP esegue i test per un elenco di risultati e di eventuali possibili azioni da eseguire. |
| Frecce | Selezionare un server e usare le frecce per le impostazioni dell'ordine. Il sistema contatta i server nell'ordine indicato. |

| Risultati test del server | |
|---|---|
| **OK** | La connessione al server SMTP è stata stabilita correttamente. Accertarsi che i destinatari abbiano ricevuto l'e-mail di prova. |
| **Errore sconosciuto** | Si è verificato un errore imprevisto durante l'invio dell'e-mail. Verificare che il server SMTP funzioni correttamente. |
| **Nessun contatto** | AXIS Camera Station Pro non può accedere al server SMTP. Controllare che il server SMTP funzioni e che i router e i server proxy presenti tra AXIS Camera Station Pro e il server SMTP consentano il traffico. |
| **Errore di configurazione** | È stato richiesto TLS ma il server non supporta StartTLS, non supporta l'autenticazione o non c'è alcun meccanismo di autenticazione compatibile. |
| **Errore di handshake TLS/SSL** | Si è verificato un errore durante la negoziazione TLS/SSL, ad esempio un certificato del server non valido. |
| **Autenticazione richiesta** | Il server necessita dell'autenticazione per l'invio di e-mail. |

| Risultati test del server | |
|---|---|
| **Errore di autenticazione** | Le credenziali sono errate. |
| **Connessione eliminata** | La connessione è stata stabilita, ma poi è stata persa. |

### Allarme sistema

Si verifica un allarme di sistema quando una telecamera perde la connessione, l'accesso all'archiviazione delle registrazioni viene negato, il server si spegne in modo imprevisto o si verificano errori di registrazione. È possibile inviare notifiche via e-mail relative agli allarmi di sistema.

Nota

Per inviare e-mail, è necessario aggiungere prima un server SMTP.

Per inviare un'e-mail al verificarsi di allarmi di sistema:

1. Selezionare **Send email on system alarm to the following recipients (Invia e-mail in caso di allarme di sistema ai seguenti destinatar)i** per attivare l'e-mail in caso di allarme di sistema.
2. In **Recipients (Destinatari)**:
   2.1. Selezionare questa opzione se l'indirizzo deve essere inserito nel campo **To (A)**, **Cc** oppure **Bcc (Ccn)** dell'e-mail.
   2.2. Inserire l'indirizzo e-mail.
   2.3. Fare clic su **Add (Aggiungi)** per salvare l'indirizzo e-mail nella casella **Recipients (Destinatari)**.

| Connessione al dispositivo | |
|---|---|
| **Ove possibile, utilizzare nomi host anziché IP per i dispositivi appena aggiunti** | Se possibile, utilizzare il nome host per connettersi ai dispositivi appena aggiunti. Se un nome host non è disponibile, viene utilizzato invece l'indirizzo IP. |
| **Continua a utilizzare gli hostname anche se diventano irraggiungibili** | Usare il nome host per eseguire la connessione. Per passare automaticamente all'indirizzo IP, invece, deselezionare la casella di controllo. È possibile selezionare manualmente per utilizzare il nome host o l'indirizzo IP per connettersi ai dispositivi. Vedere *Connessione, on page 72*. |

| Lingua | |
|---|---|
| **Modifica la lingua del server** | Consente la modifica della lingua di AXIS Camera Station Pro Service Control e AXIS Camera Station Secure Entry. Ad esempio: gli allarmi di sistema, messaggi registro di controllo e dati esterni nella scheda **Data search (Ricerca dati)**. Riavviare il server affinché le modifiche siano implementate. |

| Body Cam | |
|---|---|
| **Disco**<br>**Cartella** | Selezionare l'unità e la cartella per salvare i contenuti rifiutati dal sistema body cam. Per ulteriori informazioni, vedere *Trasferimento delle registrazioni nell'archiviazione dei contenuti rifiutati nel* manuale per l'utente della soluzione Axis Body Cam. |
| **Numero di giorni per mantenere il contenuto rifiutato dal sistema body cam.** | Imposta il numero di giorni per mantenere il contenuto rifiutato dal sistema body cam. |

| Feedback | |
|---|---|
| **Condividi i dati di utilizzo dei server anonimi con Axis Communications** | Selezionare per condividere dati anonimi con Axis per aiutare a migliorare l'applicazione e l'esperienza utente. Per modificare questa opzione per il client, consultare *Impostazioni client, on page 118*. |

**Impostaz. avanzate**

Effettuare le modifiche a queste impostazioni solo su istruzione del supporto tecnico di Axis. Per modificare un'impostazione avanzata:

1. Inserire l'impostazione e il relativo valore.
2. Fare clic su **Aggiungi**.

Per attivare la registrazione debug per la risoluzione dei problemi, selezionare **Enable server side debug logging (Abilita registrazione debug lato server)**. Queste impostazioni richiedono più spazio su disco. Il file `log4net.config` presente nella directory **ProgramData** lo sovrascrive.

Per ulteriori informazioni, vedere *Impostazione server avanzata nella guida alla risoluzione di problemi di AXIS Camera Station Pro*.

## Componenti

I componenti sono moduli software che conferiscono funzionalità in più al sistema. La pagina **Components (Componenti)** permette la gestione dei componenti e la visualizzazione del loro stato.

Per la visualizzazione della lista dei componenti installati:

1. Andare a **Configuration > Server > Components (Configurazione > Server > Componenti)**.
2. Attivare **Show components (Mostra componenti)**.

Nota

Consideriamo i componenti delle impostazioni avanzate. Visualizzare e gestire i componenti solo dopo aver consultato l'assistenza Axis.

## Aggiorna AXIS Camera Station Pro

Per aggiornare AXIS Camera Station Pro:

1. Andare a **Configuration > Server > Update (Configurazione > Server > Aggiornamento)**.
2. Fare clic su **Download and install... (Scarica e installa...)**.

Nota

- Una volta avviato un aggiornamento, sia esso manuale o con pianificazione, non è possibile annullarlo.
- Gli aggiornamenti pianificati cominciano in automatico.
- In un sistema multi-server, aggiornare sempre il server locale per ultimo.
- Quando si aggiorna il server locale, il client e il controllo del servizio si chiudono temporaneamente. Durante l'aggiornamento non verrà visualizzato alcun indicatore di avanzamento. Mantenere acceso il computer server fino al riavvio del client e del server.

## Report eventi

Se le autorizzazioni relative ai rapporti sugli incidenti sono attive, è possibile generare rapporti sugli incidenti che includono registrazioni, istantanee e note. Vedere *Esporta report dell'incidente, on page 34*.

Per configurare le impostazioni per i report dell'incidente:

1. Andare in **Configuration > Server > Incident report (Configurazione > Server > Report dell'incidente)**.

2. In **Location (Ubicazione)**, selezionare la posizione in cui archiviare i rapporti sull'evento.
3. Dal menu a discesa **Export format (formato di esportazione)** selezionare il formato in cui esportare le registrazioni.
4. In **Categories (Categorie)**, aggiungere o eliminare le categorie per raggruppare i report dell'incidente. Se configurate come variabile nel percorso della directory del server, le categorie diventano nomi di cartelle nella posizione di esportazione.
   4.1. Inserire il nome della categoria nella casella, ad esempio, Incidente o Furto.
   4.2. Fare clic su **Aggiungi**.
   4.3. Per rimuovere una categoria, selezionarla e fare clic su **Remove (Rimuovi)**.
5. In **Description template (Modello descrizione)**, inserire le informazioni da visualizzare in **Description (Descrizione)** quando si generano i report dell'incidente. Ad esempio, "Segnalato da: [nome, e-mail, numero di telefono]."
6. fare clic su **Applica**;

| Luogo | |
|---|---|
| **Server directory path (Percorso del server)** | Inserire il percorso della cartella per salvare report dell'incidente in una cartella del computer. È possibile usare il nome del server, la categoria o il nome utente come variabili. Ad esempio: `C:\Reports\$(Server Name)\$(Category)\$(User Name)\`. |
| **Network directory path (Percorso di rete)** | Selezionare questa opzione per eseguire il salvataggio dei rapporti sugli incidenti in una cartella su un'archiviazione di rete. Inserire il percorso della cartella o usare le credenziali per l'archiviazione di rete. La condivisione deve essere raggiungibile dal server AXIS Camera Station Pro. Vedere *Gestione dello spazio di archiviazione* per le modalità di aggiunta del dispositivo di archiviazione per utilizzare le registrazioni. |

| Formato di esportazione | |
|---|---|
| **ASF** | Selezionare **Add digital signature (Aggiungi firma digitale)** per impedire la manomissione dell'immagine. Vedere la sezione Firma digitale in *Esportazione delle registrazioni*. È inoltre possibile selezionare **Use password (Utilizza password)** per utilizzare un password per la firma digitale. |
| **MP4** | Le registrazioni esportate non comprendono l'audio nel formato G.711 o G.726. |

## Esportazione pianificata

Andare a **Configuration > Server > Scheduled export (Configurazione, Server, Esportazione pianificata)** per creare pianificazioni per esportare le registrazioni.

All'ora pianificata, AXIS Camera Station Pro esporta tutte le registrazioni effettuate dall'ultima esportazione. Se l'esportazione precedente risale a più di una settimana fa, oppure se non è presente alcuna esportazione precedente, vengono incluse solo le registrazioni dell'ultima settimana. Per esportare le registrazioni precedenti, accedere alla scheda **Recordings (Registrazioni)** ed esportarle manualmente. Vedere *Esportazione delle registrazioni*.

Nota

Quando si è connessi a più server AXIS Camera Station Pro, selezionare un server dal menu a discesa **Selected server (Server selezionato)** per gestire le esportazioni programmate.

### Esporta registrazioni pianificate

1. Nella sezione **Scheduled export (Esportazione pianificata)** selezionare **Enable scheduled export (Abilita esportazione pianificata)**.
2. In **Cameras (Telecamere)**, selezionare le telecamere da cui esportare le registrazioni. Il sistema seleziona tutte le telecamere in elenco per impostazione predefinita. Eseguire la deselezione di **Use all cameras (Usa tutte le telecamere)** e selezionare le telecamere specifiche nella lista.
3. In **Export (Esporta)**, configurare dove si deve eseguire il salvataggio delle registrazioni, il formato e la creazione della playlist.
4. In **Weekly schedule (Pianificazione settimanale)**, selezionare l'ora e i giorni in cui esportare le registrazioni.
5. fare clic su **Applica**;

| Esporta | |
|---|---|
| **Server directory path (Percorso del server)** | Selezionare e inserire il percorso della directory per salvare le registrazioni in una cartella sul computer. |
| **Network directory path (Percorso di rete)** | Selezionare questa opzione per eseguire il salvataggio delle registrazioni in una cartella su un'archiviazione di rete. Inserire il percorso della cartella o usare le credenziali per l'archiviazione di rete. La condivisione deve essere raggiungibile dal server AXIS Camera Station Pro. Vedere *Gestione dello spazio di archiviazione* per le modalità di aggiunta del dispositivo di archiviazione per utilizzare le registrazioni. |
| **Crea playlist (.asx)** | Selezionare questa opzione per creare una playlist nel formato .asx utilizzata da Windows Media Player. Le registrazioni si riproducono nell'ordine di registrazione. |
| **Formato di esportazione** | Selezionare un formato per esportare le registrazioni.<br><br>**ASF** – Selezionare **Add digital signature (Aggiungi firma digitale)** per impedire la manomissione delle immagini. Vedere la sezione Firma digitale in *Esportazione delle registrazioni*. È inoltre possibile selezionare **Use password (Utilizza password)** per utilizzare un password per la firma digitale.<br><br>**MP4** – Le registrazioni esportate non comprendono l'audio nel formato G.711 o G.726. |

### Microsoft Windows 2012 Server

Per esportare le registrazioni da un server con sistema operativo Microsoft Windows Server 2012, installare Desktop Experience:

1. Fare clic su **Start > Strumenti di amministrazione > Server Manager** per aprire Gestione server.
2. Selezionare **Gestione > Aggiungi ruoli e funzionalità** per avviare la procedura Aggiunta guidata ruoli e funzionalità.
3. In **Features Summary (Riepilogo funzionalità)**, selezionare **User Interfaces and Infrastructure (Interfacce utente e infrastruttura)**.

4. Selezionare **Desktop Experience**, fare clic su **Next (Avanti)**.
5. fare clic su **Install (Installa)**.

### Impostazioni WebRTC

Il client Web per AXIS Camera Station usa WebRTC per la comunicazione con il server.

| | |
|---|---|
| **Abilita TURN** | Attiva un server TURN locale sul server AXIS Camera Station Pro consentendo alla comunicazione WebRTC di utilizzare una porta singola. Ciò può semplificare la configurazione del firewall. |
| **Prioritize TURN (Dai priorità a TURN):** | Selezionare questa opzione per fare in modo che WebRTC prenda in considerazione solo i candidati per il relay. |

### Nuova connessione

Andare su ☰ > **Servers** > **New connection (Server,Nuova connessione)** per connettersi a un server AXIS Camera Station Pro. Vedere *Connessione a un server*.

### Stato connessione

Andare a ☰ > **Servers** > **Connection status (Stato della connessione)**. per visualizzare lo stato della connessione di tutti i server.

Utilizzare il cursore accanto al nome del server per collegarsi o disconnettersi dal server.

| Codice di stato | Descrizione | Soluzioni possibili |
|---|---|---|
| Collegamento in corso | Il client sta tentando di connettersi al server. | |
| Collegato | Il client usa TCP mentre è connesso a questo server<br><br>. | |
| Connesso (Axis Secure Remote Access v2) | Il client usa Axis Secure Remote Access v2 mentre è connesso a questo server. | |
| Connesso (HTTP) | Il client usa HTTP mentre è connesso a questo server. Questa connessione è meno efficiente rispetto alla connessione TCP ed è più lenta quando durante la connessione a più server. | |
| Disconnessione in corso | Il client si sta disconnettendo dal server<br><br>. | |
| Scollegato | Il client non è connesso al server. | |
| Riconnessione | Il client ha perso la connessione al server e sta tentando di riconnettersi. | |

| | | |
|---|---|---|
| Riconnessione non riuscita | Il server è stato trovato, ma le autorizzazioni o la password dell'utente potrebbero essere cambiate. | • Aggiungere l'utente nella finestra di dialogo delle **User permission (Autorizzazioni utente)**.<br>• Verificare il nome utente e la password. |
| Accesso annullato | L'utente ha annullato dall'accesso. | |
| Nome utente o password non corretta | Fare clic sul collegamento nella colonna **Action (Azione)** e immettere le credenziali corrette. | |
| L'utente non è autorizzato sul server | Il server non dà all'utente l'autorizzazione all'accesso. | Aggiungere l'utente nella finestra di dialogo delle **User permission (Autorizzazioni utente)**. |
| Verifica di sicurezza non riuscita | Un controllo di sicurezza WCF non è riuscito. | Sincronizzare l'ora UTC del computer client e di quello server. |
| Nessun contatto con il computer server | Il server non ha risposto all'indirizzo specificato. | • Verificare che la rete funzioni correttamente.<br>• Verificare che il server sia in funzione. |
| Nessun server in esecuzione | Il computer su cui è in esecuzione il server è accessibile, ma il server non è in esecuzione. | avviare il server. |
| Errore di comunicazione | La connessione al server non è riuscita. | • Assicurarsi che il computer server sia accessibile.<br>• Verificare che la rete funzioni correttamente.<br>• Verificare che il server sia in funzione. |
| Nome host non valido | Il DNS non è in grado di eseguire la conversione del nome host in un indirizzo IP. | • Verificare che il nome host sia scritto correttamente.<br>• Verificare che il DNS sia in grado di risolvere il nome host. |
| Già connesso allo stesso server | Il client è già connesso al server. | Rimuovere il server duplicato. |
| Server non previsto | A questo indirizzo ha risposto un server diverso da quello previsto. | Aggiornare il server con quello corretto. |
| La versione del client (x) non è compatibile con la versione del server (y) | Il client è obsoleto o troppo recente rispetto al server. | Installare la stessa versione di AXIS Camera Station Pro sia sul computer client che su quello server. |
| Server occupato | Il server non ha potuto rispondere a causa di problemi di prestazioni. | Assicurarsi che il computer che funge da server e la rete non siano sovraccarichi. |

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

*Più server*

### Elenchi dei server

È possibile organizzare i server AXIS Camera Station Pro in appositi elenchi. Un server può appartenere a più elenchi dei server. È possibile importare, esportare e usare elenchi server in altri client AXIS Camera Station Pro.

Andare a > **Server > Server lists (Elenchi server)**.

L'elenco **Recent connections (Connessioni recenti)** predefinito mostra i server utilizzati nella sezione precedente. Non si possono rimuovere le **Recent connections (Connessioni recenti)**.

| | |
|---|---|
| | Selezionare l'elenco server e fare clic su per eliminarlo. |
| **New server list (Nuovo elenco di server)** | Fare clic su questo pulsante per aggiungere un nuovo elenco di server e assegnargli un nome. |
| **Aggiungi** | Per aggiungere un server a un elenco server, selezionarne uno e fare clic su **Add (Aggiungi)**. Immettere le informazioni richieste. |
| **Export lists (Esporta elenchi)** | Fare clic per esportare tutti gli elenchi di server in un file .msl. È possibile importare elenchi di server per connettersi ai server. Vedere *Connessione a un server*. |
| **Edit (Modifica):** | Per modificare un server in un elenco di server, selezionare un server e fare clic su **Edit (Modifica)**. È possibile modificare solo un server alla volta. |
| **Rimuovi** | Per rimuovere un server dall'elenco dei server, selezionarlo e fare clic su **Remove (Rimuovi)**. |
| **Rinominare un elenco** | Fare doppio clic sull'elenco e immettere un nuovo nome. |

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

*Organizzare i server in elenchi di server*

## Configura Switch

Se si dispone di un dispositivo della serie AXIS Camera Station S22 Appliance, è possibile configurarlo da AXIS Camera Station Pro. Andare a **Configuration > Switch > Management (Configurazione, Switch, Gestione)** e inserire le credenziali per aprire la pagina di gestione switch .
Per configurare lo switch, consultare il manuale per l'utente AXIS Camera Station S22 Appliance su *axis.com*.

Nota

AXIS Camera Station Pro può connettersi solo a https://192.168.0.1/ che corrisponde all'indirizzo IP predefinito dello switch.

## Gestisci le licenze

La pagina Gestisci licenze illustra lo stato corrente della licenza.

| | |
|---|---|
| **Versione di prova** | Una volta installato AXIS Camera Station Pro, è possibile usufruire di un periodo di prova di 90 giorni. Durante questo periodo, il sistema è pienamente operativo. È possibile effettuare la configurazione e provarne tutte le funzionalità prima di acquistare qualsiasi licenza. |
| **Controllare le licenze** | Se il periodo di licenza del sistema scade senza rinnovo automatico, AXIS License Manager fornisce un ulteriore periodo di prova di 30 giorni. |
| **Con licenza** | Il sistema dispone di licenza completa fino alla prima data di scadenza prevista. |
| **Changes made in the system require a license synchronization (Le modifiche effettuate nel sistema impongono la sincronizzazione della licenza)** | Quando si aggiungono dispositivi a un sistema con licenza, AXIS Camera Station Pro tenta di sincronizzare le modifiche con AXIS License Manager per valutare lo stato della licenza di sistema. Se si usa la concessione automatica delle licenze, è possibile non accorgersene. Se si utilizza la gestione manuale delle licenze e non si esegue la risincronizzazione entro 60 giorni, il sistema perde la licenza. |
| **Software senza licenza** | Il sistema è operativo e pienamente funzionante, ma non sono disponibili nuovi aggiornamenti. Nella barra delle applicazioni viene visualizzato un banner per ricordare all'utente di procurarsi una nuova licenza. |
| **Senza licenza** | Il sistema è operativo ma le sue funzionalità sono limitate. Le regole di registrazione e di azione continuano a funzionare e le registrazioni non andranno perse. Le seguenti caratteristiche non funzioneranno:<br>• Live streams (Flussi dal vivo)<br>• Recordings playback (Riproduzione registrazioni)<br>• Instant playback (Riproduzione istantanea)<br>• Snapshots (Istantanee)<br>• Recordings export (Esportazione di registrazioni) |

Si può ottenere una licenza per il proprio sistema in due modi:

**Concessione automatica delle licenze (sistemi online) –** Il sistema invia in automatico ad AXIS License Manager le modifiche che incidono sul numero di licenze e recupera un nuovo stato di licenza. Per questa opzione serve una connessione Internet. Per ulteriori informazioni, vedere *Ottenimento di una licenza per un sistema online, on page 136*.

**Concessione manuale delle licenze (sistemi offline) –** Con questa opzione, esportare in modo manuale il file di sistema, caricarlo su AXIS License Manager e importare la nuova licenza. Ogni volta che si modifica il sistema in

modo da incidere sul numero di licenze, occorre ripetere il processo. Scegliere questa opzione se si preferisce la gestione manuale delle licenze o se il sistema non ha una connessione Internet. Per ulteriori informazioni, vedere *Ottenimento di una licenza per un sistema offline, on page 136*.

### 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 Pro.
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.

## Configura sicurezza

### Autorizzazioni utente

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

Nota

Agli amministratori del computer su cui viene eseguito il server AXIS Camera Station Pro vengono assegnati determinati privilegi di amministratore in AXIS Camera Station Pro. 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 utente 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 attribuite a lui individualmente e quelle attribuite 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 ha accesso 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 gruppo. I possibili valori sono: Amministratore, Operatore e Visualizzatore. |
| **Dettagli** | Informazioni dettagliate sull'utente come visualizzate sul 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 Pro. Per aggiungere un utente a AXIS Camera Station Pro, 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)**, andare a **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 vengono visualizzati 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 se il numero di utenti o gruppi è troppo elevato. Utilizzare il filtro per restringere i risultati.
5. Selezionare gli utenti o i gruppi e fare clic su **Add (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** | Quando si è connessi a più server AXIS Camera Station Pro, 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 di un utente o un gruppo, vedere *Aggiunta di utenti o gruppi*.

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

**Operator (Operatore): –** Selezionare telecamere, viste e porte I/O per ottenere l'accesso alle immagini dal vivo e al video registrate. Un operatore ha pieno accesso a tutte le funzionalità di AXIS Camera Station Pro ad eccezione della configurazione del sistema.

**Visualizzatore –** 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 con 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 e che hanno **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 Pro. |
| **Edit (Modifica):** | Consente la modifica delle viste in AXIS Camera Station Pro. |

### 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 visualizzati 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, PIN, comunicazione criptata e multiserver. |
| **Gestione degli accessi** | Permette la gestione degli accessi e l'accesso alle impostazioni di Active Directory. |

### AXIS Audio Manager Pro

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

| | |
|---|---|
| **Accedere alle impostazioni del componente AXIS Audio Manager Pro** | Consente la configurazione di AXIS Audio Manager Pro in AXIS Camera Station Pro e l'accesso all'interfaccia server di AXIS Audio Manager Pro. Disponibile esclusivamente per gli operatori. |
| **Accesso all'interfaccia AXIS Audio Manager Pro** | Consente l'accesso all'interfaccia server di AXIS Audio Manager Pro. Disponibile esclusivamente per i visualizzatori. |

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. |

## Certificati

Per la gestione delle impostazioni dei certificati per il server AXIS Camera Station Pro e i dispositivi connessi, andare a **Configuration > Security > Certificates (Configurazione, Sicurezza, Certificati)**.

Per saperne di più su come si attivano, eliminano e visualizzano i certificati HTTPS e IEEE 802.1X, consultare *Sicurezza, on page 70*.

AXIS Camera Station Pro si può usare come:

- **Root certificate authority (CA) (Autorità di certificazione (CA) radice):** AXIS Camera Station Pro utilizza il proprio certificato radice per emettere certificati server, senza il coinvolgimento di altre CA radice.
- **Intermediate certificate authority (Autorità di certificazione intermedia):** importare un Certificato CA e la relativa chiave privata in AXIS Camera Station Pro per firmare ed emettere certificati server per i dispositivi Axis. Questo può essere un certificato radice o un certificato CA intermedio.

Nota

Quando disinstalli AXIS Camera Station Pro, i certificati CA vengono rimossi da Windows Trusted Root Certification Authorities. Non rimuove i certificati CA importati; si devono rimuovere in modo manuale.

### Autorità di certificazione (CA)

Un'autorità di certificazione consente di attivare HTTPS e IEEE 802.1X sui dispositivi senza certificati client/server. Il certificato CA di AXIS Camera Station Pro può creare, firmare e installare automaticamente i certificati client/server sui dispositivi durante l'uso di HTTPS o IEEE 802.1X. È possibile utilizzare AXIS Camera Station Pro come autorità di certificazione root, oppure importare un certificato di autorità di certificazione e lasciare che AXIS Camera Station Pro agisca come autorità di certificazione intermedia. Il sistema genera un CA root al momento dell'installazione del server.

| | |
|---|---|
| **Importa** | Fare clic per eseguire l'importazione di un certificato CA esistente e della relativa chiave privata. AXIS Camera Station Pro archivia la password del certificato. |
| **Genera** | Fare clic per eseguire la generazione di una nuova chiave pubblica e privata e un certificato CA autofirmato che sia valido per 10 anni. Quando viene generata una nuova autorità di certificazione, sostituisce tutti i certificati componenti e riavvia i componenti. |
| **Visualizza** | Fare clic per visualizzare i dettagli del certificato CA. |

| | |
|---|---|
| **Esporta** | Fai clic per esportare il CA in un file. L'esportazione può avvenire in due modi:<br>• **Without the private key (Senza la chiave privata):** Salva il certificato in formato .cer o .crt. Utilizzare questa opzione se è necessaria solo l'installazione del certificato pubblico in altri sistemi che devono considerare attendibili i certificati firmati da AXIS Camera Station Pro.<br>• **With the private key (Con la chiave privata):** salva la CA in formato PKCS#12 (.pfx o .p12). Utilizzare questa opzione se è necessario importare il CA su un altro server AXIS Camera Station Pro.<br>Non è possibile importare nuovamente un certificato .cer o .crt in AXIS Camera Station Pro. |
| **Number of dates the signed client/server certificates will be valid for (Numero di giorni di validità dei certificati client/server firmati)** | Imposta il numero di giorni durante i quali i certificati client/server creati in automatico sono validi. La quantità massima è 1095 giorni (tre anni). La CA non firma certificati che abbiano validità oltre la propria data di scadenza. |

**Generazione di un'autorità di certificazione root**

Quando AXIS Camera Station Pro si avvia, cercare un'autorità di certificazione. Se non viene individuata alcuna CA, ne genera automaticamente una di livello root. Include un certificato root autofirmato e una chiave privata protetta da password. AXIS Camera Station Pro memorizza la password ma non la rende visibile. Un certificato CA generato da AXIS Camera Station Pro è valido per 10 anni.

Per generare manualmente una nuova autorità di certificazione in modo da sostituire quella precedente, vedere *Sostituzione di un'autorità di certificazione, on page 143*.

Se si esegue l'aggiornamento dalla versione 5.45 o precedente con un certificato installato manualmente su un dispositivo, AXIS Camera Station Pro usa automaticamente la CA radice esistente per installare un nuovo certificato quando quello manuale scade.

Nota

Quando generi un certificato CA, è aggiunto ai Windows Trusted Root Certificates.

**Importazione di un'autorità di certificazione**

Quando si esegue l'installazione di un certificato CA da un'altra autorità di certificazione si può usare AXIS Camera Station Pro come una autorità di certificazione intermedia. Importare un'autorità di certificazione esistente, composta da un certificato e da una chiave privata, per consentire a AXIS Camera Station Pro di firmare i certificati per conto dell'autorità di certificazione. Il file deve essere un file PKCS#12, il certificato deve essere dotato di un certificato di base (2.5.29.19) che indica che è un certificato CA e deve essere usato nel periodo di validità. Per importare un'autorità di certificazione in modo da sostituire quella esistente, vedere *Sostituzione di un'autorità di certificazione, on page 143*.

Nota

- Se la CA importata non necessita una password, appare una finestra di dialogo ogni qualvolta che

qualcosa impone una password. Quando si usa, ad esempio, HTTPS o IEEE su un dispositivo o si aggiunge un dispositivo. Fare clic su **OK** per continuare.

- Quando importi un certificato CA, è aggiunto ai Windows Trusted Root Certificates.
- Quando si importa un Certificato CA intermedio, il certificato root deve essere già presente nell'archivio certificati di Windows. Se il certificato radice è mancante, l'importazione non va a buon fine e appare un messaggio di errore. AXIS Camera Station Pro continua a utilizzare il CA precedente.
- Dopo la disinstallazione di AXIS Camera Station Pro, devi rimuovere manualmente i certificati CA importati dalle Windows Trusted Root Certification Authorities.

**Sostituzione di un'autorità di certificazione**

Per eseguire la sostituzione della CA che emette certificati firmati usati su dispositivi con connessione HTTPS:

1. Andare a **Configuration > Security > Certificates > HTTPS (Configurazione > Sicurezza > Certificati > HTTPS)**.
2. Disattivare **Validate device certificate** (Convalida certificato del dispositivo).
3. In **Certificate authority (Autorità di certificazione)**, fare clic su **Generate (Genera)** o **Import (Importa)**.
4. Inserire la password e fare clic su **OK**.
5. Selezionare il numero di giorni di validità dei certificati client/server firmati.
6. Andare a **Configurazione > Dispositivi > Gestione**.
7. Fare clic con il pulsante destro del mouse sui dispositivi e selezionare **Security > HTTPS > Enable/ Update (Sicurezza > HTTPS > Abilita/Aggiorna)**.
8. Andare a **Configuration > Security > Certificates > HTTPS (Configurazione, Sicurezza, Certificati, HTTPS)** e abilitare **Validate certificate device (Convalida certificato dispositivo)**.

**Rilascio di un certificato personalizzato**

Si può creare un certificato personalizzato firmato dall'autorità di certificazione AXIS Camera Station Pro. Ad esempio, si possono usare questi certificati per endpoint HTTPS esterni. Questi certificati si devono rinnovare in modo manuale quando scadono. Per eseguire il rilascio di un certificato personalizzato:

1. Andare a **Configuration (Configurazione)** > **Security (Sicurezza)** > **Certificates (Certificati)**.
2. In **Issue custom certificate (Emettere un certificato personalizzato)**, fare clic su **Issue certificate... (Emettere certificato...)**.
3. Inserire i dettagli del certificato e fare clic su **OK**.

| Emettere certificato | |
|---|---|
| **Nome comune (CN)** | Identifica il titolare del certificato. In genere, CN è il nome dominio completo (FQDN) o l'indirizzo IP dove si installa il certificato. |
| **Private key password (Password chiave privata)** | Password che tutela la chiave privata. |
| **Duration (days) (Durata (giorni))** | Giorni di validità del certificato. |
| **Server authentication (Autenticazione server)** | Selezionare questa opzione se si utilizza il certificato su un server per attestare l'identità del server stesso. Generalmente, i dispositivi o altri endpoint con cui AXIS Camera Station Pro si collega usando HTTPS sono considerati dispositivi server e i rispettivi certificati devono impiegare l'autenticazione del server. |
| **Client authentication (Autenticazione client)** | Selezionare questa opzione se si utilizza il certificato su un client per verificare l'identità del client prima di |

| Emettere certificato | |
|---|---|
| | connettersi a un server. Ad esempio, i dispositivi che vogliono eseguire l'accesso a una rete con accessi controllati IEEE 802.1X devono usare questo certificato prima di entrare. |
| **Società/organizzazione (O)** | L'organizzazione del titolare del certificato. |
| **Country code (C) (Codice paese (C))** | Codice paese del titolare del certificato. |
| **DNS SAN** | Nomi alternativi dell'oggetto del Dynamic Name Server. FQDN alternativi per contattare il titolare del certificato. Quando viene emesso un certificato, il sistema aggiunge in automatico il CN come DNS SAN. Si possono inserire più indirizzi separati da virgole, ad esempio indirizzo-1.com,indirizzo-2.com. |
| **IP SAN** | Nomi alternativi dell'oggetto dell'indirizzo IP. Indirizzi IP alternativi per contattare il titolare del certificato. Il sistema aggiunge in automatico CN in qualità di IP SAN se il CN è un indirizzo IP. Si possono inserire molteplici indirizzi separati da una virgola, ad esempio 192.168.1.1,192.168.1.2. |

**HTTPS**

Per impostazione predefinita, AXIS Camera Station Pro convalida la firma del certificato server HTTPS su ciascun dispositivo connesso e non si connette a un dispositivo senza un certificato valido. Il certificato del server deve essere firmato dall'autorità di certificazione attiva in AXIS Camera Station Pro o convalidato tramite Windows Certificate Store. AXIS Camera Station Pro verifica inoltre se l'indirizzo nel certificato HTTPS del dispositivo corrisponde all'indirizzo utilizzato per comunicare con il dispositivo quando l'opzione **Validate device address (Convalida indirizzo dispositivo)** è attivata.

Le telecamere che dispongono di firmware 7.20 o versione successiva sono dotate di un certificato autofirmato. Questi certificati non sono considerati affidabili. Invece, generare o importare un CA per permettere ad AXIS Camera Station Pro di emettere nuovi certificati per i dispositivi quando si usa HTTPS.

| | |
|---|---|
| **Convalida certificato** | Attivare questa opzione per connettersi solo a dispositivi dotati di un certificato valido. Senza la verifica dei certificati, i dispositivi con certificati non validi possono connettersi. |
| **Convalida indirizzo dispositivo** | Disattivare questa opzione per garantire un funzionamento più stabile sulle reti DHCP che non utilizzano nomi host.<br><br>Attivarla per richiedere che gli indirizzi corrispondano in modo da ottenere sicurezza in più. Si consiglia di attivare questa impostazione solo su reti in cui i dispositivi utilizzano prevalentemente nomi host o dispongono di indirizzi IP statici. |

Nota

- Quando una connessione sicura (HTTPS) non è disponibile, è possibile emettere un nuovo certificato HTTPS. Vedere *Aggiungi dispositivi, on page 47*
- Per utilizzare HTTPS, per i dispositivi video è necessario il firmware 5.70 o versione successiva e il firmware 1.25 o versione successiva per i dispositivi di controllo degli accessi e audio.

**Limiti**

- Le porte non predefinite (diverse dalla porta 443) non sono supportate.
- Tutti i certificati in un gruppo di installazione devono disporre della stessa password.
- Le operazioni relative ai certificati su canali codificati, come **Basic** non sono supportate. Impostare i dispositivi su **Encrypted & unencrypted (Criptati e non criptati)** o **Encrypted only (Solo criptati)** per consentire la comunicazione **Digest**.
- Non si può eseguire l'attivazione di HTTPS sulle serie di swithc di rete AXIS T85 PoE+ Network Switch.

### IEEE 802.1X

Per l'autenticazione IEEE 802.1X di AXIS Camera Station Pro, il supplicant è un dispositivo di rete Axis che si desidera collegare alla rete LAN. L'autenticatore è un dispositivo di rete, come uno switch Ethernet o un access point wireless. Il server di autenticazione è generalmente un host che esegue software che supporta protocolli RADIUS ed EAP.

Si deve eseguire l'importazione di un certificato CA di autenticazione IEEE 802.1X ai fini dell'attivazione di IEEE 802.1X. Il certificato CA di autenticazione IEEE 802.1X e il certificato client IEEE 802.1X si installano quando viene attivato o aggiornato IEEE 802.1X. Un certificato per l'autenticazione può essere ottenuto esternamente, ad esempio dal server di autenticazione IEEE 802.1X oppure generato direttamente in AXIS Camera Station Pro. Questo certificato è installato su ciascun dispositivo Axis per verificare il server di autenticazione.

Nota

Per utilizzare i certificati IEEE 802.1X, i dispositivi video devono disporre di firmware 5.50 o versione successiva e i dispositivi di controllo degli accessi e audio devono disporre di firmware 1.25 o versione successiva.

Per configurare IEEE 802.1X:

1. Andare a **Configuration > Security > Certificates (Configurazione > Sicurezza > Certificati)**.
2. Nel menu a discesa **EAPOL Version (Versione EAPOL)**, selezionare quale versione del protocollo Extensible Authentication Protocol (EAP) si desidera utilizzare.
3. Nel menu a discesa **EAP identity (Identità EAP)**, selezionare questa opzione per utilizzare il MAC address, il nome host del dispositivo o il testo personalizzato.
4. Se è stato selezionato **Custom (Personalizzato)**, inserire il testo da utilizzare come identità EAP.
5. Fare clic su **Import (Importa)** ed eseguire la selezione del file del certificato CA di autenticazione IEEE 802.1X.
6. Nel menu a discesa **Common name (Nome comune)** selezionare l'opzione **Device IP address (Indirizzo IP dispositivo)** o **Device EAP identity (Identità EAP dispositivo)** come nome comune nei singoli certificati che vengono creati per ciascun dispositivo.
7. Andare a **Configurazione > Dispositivi > Gestione**.
8. Fare clic con il pulsante destro del mouse sui dispositivi e selezionare **Security > IEEE 802.1X > Enable/Update (Sicurezza > IEEE 802.1X > Abilita/Aggiorna)**.

#### Limiti

- Per dispositivi con diversi adattatori di rete (ad esempio le telecamere wireless), si può attivare IEEE 802.1X solo per il primo adattatore, generalmente la connessione via cavo.
- I dispositivi che non dispongono del parametro `Network.Interface.I0.dot1x.Enabled` non sono supportati. Ad esempio puoi: AXIS P39 Series, AXIS T85 Series e AXIS T87 Video Decoder
- Le operazioni relative ai certificati su canali codificati, come **Basic** non sono supportate. Impostare i dispositivi su **Encrypted & unencrypted (Criptati e non criptati)** oppure **Encrypted only (Solo criptati)** per consentire la comunicazione **Digest**.

### Avviso di scadenza del certificato

Un avviso appare quando un certificato client o server è scaduto o è sul punto di scadere. L'avviso attiva anche un allarme di sistema per certi certificati. Si applica a tutti i certificati client e server, ai certificati CA del

dispositivo installati da AXIS Camera Station Pro, al certificato CA di AXIS Camera Station Pro e al certificato IEEE 802.1X. L'avviso compare come messaggio in **Status (Stato)** o sulla pagina **Device management (Gestione dispositivi)** e come icona nella lista **Installed certificates (Certificati installati)**.

In **Certificate expiration warning (Avviso di scadenza del certificato)**, specificare con quanti giorni di anticipo rispetto alla data di scadenza si vuole una notifica da AXIS Camera Station Pro.

**Rinnovo dei certificati**

**Rinnovo certificato tra il server e i dispositivi**

I certificati client o server generati da AXIS Camera Station Pro si rinnovano automaticamente 7 giorni prima che appaia l'avviso della scadenza. Questo richiede l'attivazione di HTTPS o IEEE 802.1X sul dispositivo. Per rinnovare o aggiornare manualmente un certificato, vedere *Sicurezza, on page 70*.

**Rinnovo certificato tra il server e il client**

È possibile generare un nuovo certificato del server nella scheda **Certificates (Certificati)** del service control di AXIS Camera Station Pro. Per le istruzioni, vedere *Certificati, on page 229*.

**Reset della password**

1. Andare a **Configuration > Security > Certificates (Configurazione > Sicurezza > Certificati)**.
2. Disattivare l'opzione **Validate device certificate (Verifica validità certificato dispositivo)** in modo che i dispositivi che utilizzano certificati CA rimangano accessibili.
3. In **Certificate authority (Autorità di certificazione)**, fare clic su **Generate (Genera)** e immettere la propria password.
4. In **Certificate authority (Autorità di certificazione)**, fare clic su **Export (Esporta)** per eseguire il salvataggio locale del certificato CA.
5. Andare a **Configuration > Devices > Management (Configurazione > Dispositivi > Gestione)** e attivare HTTPS sui dispositivi selezionati.
6. Attivare **Validate device certificate** (Convalida certificato del dispositivo).

## Configurazione del controllo degli accessi

Se si aggiunge un network door controller Axis al sistema, è possibile configurare l'hardware di controllo degli accessi in AXIS Camera Station versione 6.x o successiva.

Per un flusso di lavoro completo per l'impostazione di un network door controller Axis in AXIS Camera Station Pro, vedere *Imposta un network door controller Axis*.

Nota

Prima di iniziare, fare quanto segue:

- Aggiornare la versione del sistema operativo AXIS OS del controller in **Configuration > Devices > Management (Configurazione, Dispositivi, Gestione)**.
- Impostare data e ora per il dispositivo di controllo in **Configuration > Devices > Management (Configurazione > Dispositivi > Gestione)**.
- Attivare HTTPS sul dispositivo di controllo in **Configuration > Devices > Management (Configurazione > Dispositivi > Gestione)**.

**Workflow to configure access control (Flusso di lavoro per configurare il controllo degli accessi)**

1. Per modificare i profili di identificazione predefiniti o crearne di nuovi, vedere *Profili di identificazione, on page 165*.
2. Per utilizzare un'impostazione personalizzata per i formati della tessera e la lunghezza del PIN, vedere *Formati tessera e PIN, on page 167*.
3. Aggiungere una porta e applicare un profilo di identificazione alla porta. Vedere *Aggiunta di una porta, on page 150*.

4. Configurare la porta:
   - *Aggiungere un sensore di posizione della porta, on page 156*
   - *Aggiungere un sensore di emergenza, on page 158*
   - *Aggiungere un formato di un lettore tessera, on page 159*
   - *Aggiungi un dispositivo REX, on page 162*
5. Aggiungere una zona e aggiungere porte alla zona. Vedere *Aggiunta di una zona, on page 163*.

## Compatibilità del software del dispositivo per i door controller

Importante

Quando si esegue l'aggiornamento di AXIS OS sul door controller, tenere presente quanto segue:

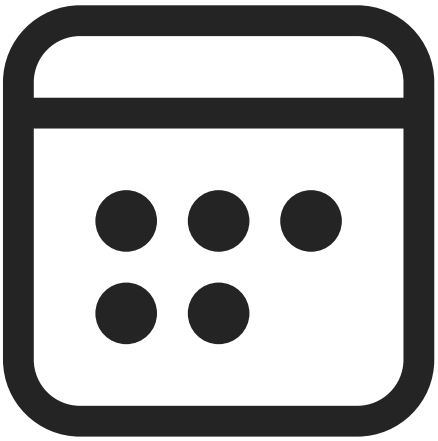
- **Supported AXIS OS versions (Versioni AXIS OS supportate):** Le versioni del sistema operativo AXIS OS supportate elencate in precedenza sono valide solo in caso di aggiornamento dalla rispettiva versione AXIS Camera Station Pro originale consigliata e quando il sistema è dotato di porta. Se il sistema non soddisfa queste condizioni, è necessario eseguire l'aggiornamento alla versione di AXIS OS consigliata per la versione AXIS Camera Station Pro specifica.
- **Versione AXIS OS minima supportata:** La versione di AXIS OS più vecchia installata nel sistema determina la versione minima supportata di AXIS OS, con un limite di due versioni precedenti. Supponiamo che si stia utilizzando la versione 6.5 di AXIS Camera Station Pro e che si effettui l'aggiornamento di tutti i dispositivi alla versione 12.0.86.2 di AXIS OS, come raccomandato. D'ora in poi, la versione 12.0.86.2 di AXIS OS sarà la versione minima supportata per il sistema.
- **Upgrading beyond recommended AXIS OS version (Aggiornamento a una versione di AXIS OS superiore a quella consigliata):** supponiamo che si esegua l'aggiornamento a una versione di AXIS OS superiore a quella consigliata per una determinata versione di AXIS Camera Station Pro. In tal caso, è sempre possibile eseguire il downgrade alla versione AXIS OS consigliata senza alcun problema, purché rientri nei limiti di supporto fissati per la versione di AXIS Camera Station Pro.
- **Future AXIS OS recommendations (Suggerimenti di ACIS OS futuri):** Seguire sempre la versione AXIS OS consigliata per la rispettiva versione di AXIS Camera Station Pro per garantire la stabilità del sistema e la piena compatibilità.
- **Track change (Modifica track):** La modifica del firmware tra la versione 10.12.xx e 11.0.xx o superiore richiede un ripristino delle impostazioni di fabbrica.

La tabella seguente mostra la versione minima e consigliata di AXIS OS per ciascuna versione di AXIS Camera Station Pro:

| Versione AXIS Camera Station | Versione minima AXIS OS | Versione AXIS OS consigliata |
|---|---|---|
| Pro 6.17 | 12.6.102.1 | 12.9.65.3 |
| Pro 6.16 | 12.6.102.1 | 12.9.65.3 |
| Pro 6.15 | 12.5.68.1 | 12.8.55.1 |

## Porte e zone

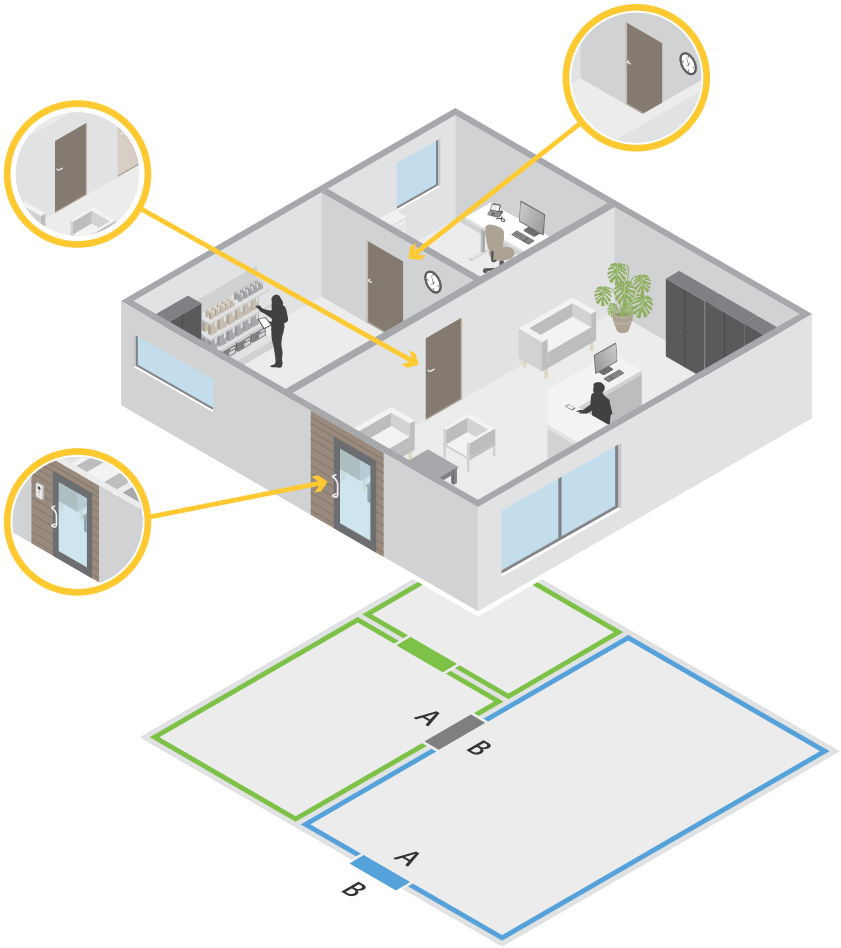
Andare a **Configuration > Access control > Doors and zones (Configurazione > Controllo degli accessi > Porte e zone)** per ottenere una panoramica ed eseguire la configurazione di porte e zone.

| | |
|---|---|
| <br>**Azioni manuali** | Impostare manualmente lo stato di una porta. Selezionare dalle seguenti opzioni: **Reset (Ripristinare)** (seguire le regole del sistema), **Grant access (Concedere l'accesso)** (sbloccare la porta per 7 secondi), **Unlock (Sbloccare)** (mantenere la porta sbloccata), **Lock (Bloccare)** (mantenere la porta bloccata) oppure **Lockdown (Attivare la chiusura)** (nessuno può entrare o uscire). |
|  <br>**Sblocca pianificazioni** | Impostate la pianificazione per sbloccare automaticamente le porte a orari prestabiliti. In tutti gli altri casi le porte rimangono bloccate. Per richiedere che la prima persona sblocchi manualmente la porta prima che la pianificazione si attivi, attivare l'opzione **Prima persona inserita**. |
| **Profilo di identificazione** | Cambiare il profilo di identificazione delle porte. |
| **Schema dei PIN** | Visualizzare lo schema dei pin del controller associato a una porta. Per stampare lo schema pin, fare clic su **Print (Stampa)**. |
| **Canale sicuro** | Disattivare o attivare OSDP Secure Channel per uno specifico lettore. |

| **Porte** | |
|---|---|
| Nome | Il nome della porta. |
| Type (Tipo): | Il tipo di configurazione della porta. |
| Dispositivo | Il dispositivo collegato alla porta. |

| | |
|---|---|
| Indirizzo IP | L'indirizzo IP del door controller connesso alla porta. |
| Lato A | La zona in cui si trova il lato A della porta. |
| Lato B | La zona in cui si trova il lato B della porta. |
| Profilo di identificazione | Il profilo di identificazione applicato alla porta. |
| Batteria | Lo stato della batteria del door controller. |
| Stato | Lo stato della porta.<br>• **Online:** la porta è online e funziona correttamente.<br>• **Reader offline (Lettore offline):** il lettore nella configurazione della porta è offline.<br>• **Reader error (Errore lettore):** il lettore non supporta il canale sicuro oppure questa funzione è disattivata per il lettore.<br>• **Old firmware (Firmware obsoleto):** il dispositivo utilizza una versione di firmware obsoleta. Aggiornare il firmware per garantire prestazioni e sicurezza ottimali. |
| **Zone** | |
| Nome | Il nome della zona. |
| Numero di porte | Numero di porte incluse nella zona. |
| Livello di sicurezza | Il livello di sicurezza applicato alla zona. |

### Esempio di porte e zone




- Esistono due zone: zona verde e zona blu.
- Sono disponibili tre porte: porta verde, porta blu e porta marrone.
- La porta verde è una porta interna alla zona verde.
- La porta blu è una porta perimetrale solo per la zona blu.
- La porta a chiave è una porta perimetrale sia per la zona verde che per quella blu.

### Aggiunta di una porta

Nota

- Si può configurare un door controller con una porta con due serrature o due porte con una serratura ciascuna. I sistemi multi-controllo supportano ulteriori configurazioni di blocco.
- Se un door controller non ha porte e si sta utilizzando una nuova versione di AXIS Camera Station Pro con firmware precedente sul door controller, il sistema impedirà di aggiungere una porta. Ciononostante, se c'è già una porta disponibile, il sistema consente nuove porte sui controller di sistema con firmware precedente.

Per aggiungere una porta:

1. Andare a **Configuration > Access control > Doors and zones (Configurazione, Controllo degli accessi Porte e zone)**.
2. Fare clic su + **Add (Aggiungi)** e selezionare il tipo di porta dall'elenco a discesa.

| Tipi di porta | |
|---|---|
| **Porta** | Una porta standard dotata di un monitor che supporta blocchi e lettori. Richiede un door controller. |
| **Piano** | Un tipo di porta per il controllo degli ascensori che effettua l'autenticazione dell'accesso ai piani dell'ascensore tramite lettori di tessere. Per ulteriori informazioni, vedere *Aggiungere una planimetria BETA, on page 158*. |
| **Porta di monitoraggio** | Una porta in grado di segnalare se è aperta o chiusa. Per ulteriori informazioni, vedere *Aggiungere una porta di monitoraggio, on page 157*. |
| **Porta wireless** | Una porta che è possibile configurare con blocchi wireless e hub di comunicazione ASSA ABLOY Aperio®. Per ulteriori informazioni, vedere *Aggiungere un blocco wireless, on page 155*. |
| **Porta predisposta** | Una porta provvisoria che è possibile aggiungere al sistema senza selezionare l'hardware. |

3. Inserire un nome per la porta e selezionare un door controller nel menu a discesa **Device** (Dispositivo) da associare alla porta. Il controller appare in grigio quando non è possibile aggiungere un'altra porta, quando è offline o quando HTTPS non è attivo.
4. Fare clic su **Next (Avanti)** per passare alla pagina di configurazione della porta.
5. Selezionare una porta relè dal menu a discesa **Primary lock (Blocco principale)**.
6. Per configurare due blocchi sulla porta, selezionare una porta relè dal menu a discesa **Secondary lock (Blocco secondario)**.
7. Selezionare un profilo di identificazione. Vedere *Profili di identificazione, on page 165*.
8. Configurare la porta aggiungendo sensori o lettori in **Sensors (Sensori)**, **Side A (Lato A)**, e **Side B (Lato B)**.
9. Configurare le impostazioni specifiche della porta. Vedere *Impostazioni della porta, on page 152*.
10. Configurare il livello di sicurezza. Vedere *Livello di sicurezza porta, on page 153*.
11. Fare clic su **Save (Salva)**.

Copia una configurazione porta:

1. Andare a **Configuration > Access control > Doors and zones (Configurazione, Controllo degli accessi Porte e zone)**.
2. Fare clic su + **Add (Aggiungi)**.
3. Inserire un nome per la porta e selezionare un door controller nel menu a discesa **Device** (Dispositivo) da associare alla porta.
4. Fare clic su **Next (Avanti)**.
5. Nel menu a discesa **Copy configuration (Copia configurazione)** selezionare una configurazione di porta esistente. Mostra le porte connesse mentre il controller risulta disattivato (grigio) se è stato configurato con due porte o una porta con due serrature.
6. Modificare le impostazioni se si desidera.
7. Fare clic su **Save (Salva)**.

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

*Aggiungere e configurare porte e zone*

**Impostazioni della porta**

Per modificare una porta:

1. Andare a **Configuration > Access control > Door and Zones (Configurazione > Controllo degli accessi > Porte e zone)**.
2. Selezionare la porta che si desidera modificare.
3. Fare clic su **Edit (Modifica)**.
4. Nella sezione **Door settings (Impostazioni porta)**, modificare le impostazioni desiderate e fare clic su **Save (Salva)**.

| | |
|---|---|
| **Tempo di accesso (sec)** | Impostare per quanti secondi la porta rimane sbloccata dopo che è stato concesso l'accesso. La porta si blocca di nuovo quando si chiude, anche se c'è ancora tempo. |
| **Open-too-long time (sec) (Tempo di apertura eccessivo (sec))** | Valido solo se è stato configurato un monitor porta. Impostare per quanti secondi la porta può rimanere aperta. Se la porta è ancora aperta allo scadere del tempo, scatta l'allarme per apertura porta prolungata. Impostare una regola di azione per scegliere cosa deve succedere quando scatta questo evento. |
| **Tempo di accesso lungo (sec)** | Con queste impostazioni, è possibile definire per quanti secondi la porta rimane sbloccata dopo che è stato concesso l'accesso ai titolari di tessera per i quali è abilitata questa funzione. Questo sovrascrive il tempo di accesso standard. |
| **Long open-too-long time (sec) (Tempo di apertura eccessivo lungo (sec))** | Valido solo se è stato configurato un monitor porta. Impostare per quanti secondi la porta può rimanere aperta per i titolari di tessera con l'opzione **Long access time (Tempo di accesso prolungato)** abilitato. Sovrascrive il tempo di apertura standard eccessivo. |
| **Ritardo ripetizione blocco (ms)** | Impostare per quanti millisecondi la porta rimane sbloccata dopo essere stata aperta o chiusa. |
| **Ripetizione blocco** | • **After opening (dopo apertura):** valido solo se è stato aggiunto un monitor porta.<br>• **After closing (dopo chiusura):** valido solo se è stato aggiunto un monitor porta. |

| | |
|---|---|
| **Porta forzata** | Selezionare se si desidera che il sistema attivi un sistema allarme quando si forza la porta a restare aperta. È necessario un sensore di posizione della porta (DPS). |
| **Porta aperta troppo a lungo** | Selezionare se si desidera che il sistema attivi un sistema allarme quando la porta è tenuta aperta troppo a lungo. |

Per rimuovere una porta:

1. Andare a **Configuration > Access control > Doors and zones > Doors (Configurazione > Controllo degli accessi > Porta e zone > Porte)**.
2. Selezionare una porta dall'elenco.
3. Fare clic su **Remove (Rimuovi)** e conferma.

**Azioni manuali**

È possibile eseguire le seguenti azioni manuali su porte e zone:

**Riprendi pianificazione –** Ritorna alle regole di sistema configurate.

**Consenti accesso –** Sblocca una porta o una zona per 7 secondi e poi la blocca di nuovo.

**Sblocca –** Mantiene la porta aperta fino al reset.

**Blocco –** Mantiene chiusa la porta finché il sistema non concede l'accesso a un titolare di tessera.

**Chiusura totale –** Nessuno può entrare o uscire finché non si resetta o si sblocca.

Per eseguire un'azione manuale:

1. Andare a **Configuration (Configurazione)** > **Access control (Controllo degli accessi)** > **Doors and zones (Porte e zone)**.
2. Selezionare la porta o la zona.
3. Fare clic su una qualsiasi delle azioni manuali.

**Livello di sicurezza porta**

È possibile aggiungere le seguenti funzionalità di sicurezza alla porta:

**Regola due persone –** La regola per due persone richiede a due persone di utilizzare una credenziale valida per ottenere l'accesso.

**Doppia passata –** La doppia passata consente al titolare tessera di sovrascrivere lo stato corrente di una porta. Ad esempio, può usarla per il blocco o lo sblocco di una porta fuori della pianificazione normale, il che è più comodo che sbloccare la porta tramite sistema. La doppia passata non influisce su una pianificazione esistente. Ad esempio, se è pianificato il blocco di una porta all'ora di chiusura e un dipendente esce per la pausa pranzo, la porta si blocca comunque in base alla pianificazione.

È possibile configurare il livello di sicurezza quando si aggiunge una nuova porta o lo si applica a una porta esistente.

Per aggiungere una **regola due persone** a una porta esistente:

1. Andare a **Configuration (Configurazione)** > **Access control (Controllo degli accessi)** > **Doors and zones (Porte e zone)**.
2. Selezionare la porta per la quale si desidera configurare un livello di sicurezza.
3. Fare clic su **Edit (Modifica)**.

4. Fare clic su **Security level (Livello di sicurezza)**.
5. Attiva una **regola due persone**.
6. fare clic su **Applica**;

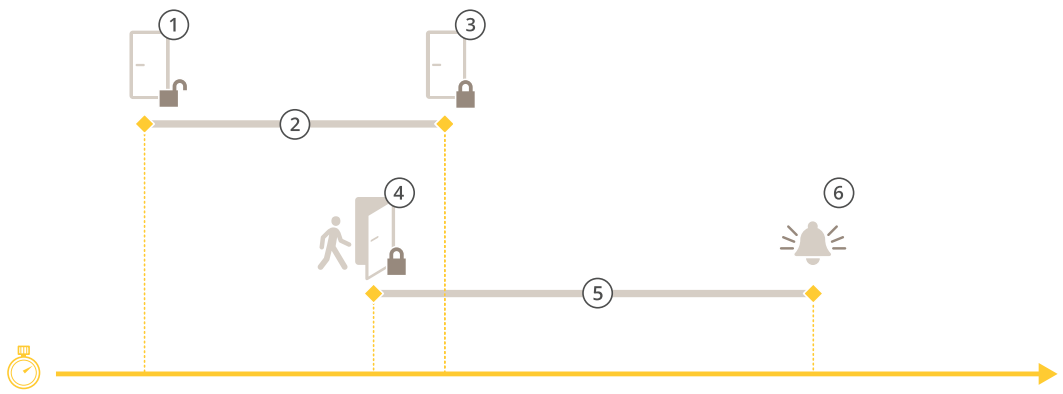
| Regola due persone | |
|---|---|
| **Side A (Lato A)** e **Side B (Lato B)** | Selezionare i lati della porta su cui usare la regola. |
| **Pianificazioni** | Selezionare quando è attiva la regola. |
| **Timeout (secondi)** | Timeout è il tempo massimo consentito tra i passaggi di tessera o altri tipi di credenziali valide. |

Per aggiungere una **Doppia passata** a una porta esistente:

1. Andare a **Configuration (Configurazione)** > **Access control (Controllo degli accessi)** > **Doors and zones (Porte e zone)**.
2. Selezionare la porta per la quale si desidera configurare un livello di sicurezza.
3. Fare clic su **Edit (Modifica)**.
4. Fare clic su **Security level (Livello di sicurezza)**.
5. Attivare la **Doppia passata**.
6. fare clic su **Applica**;
7. Applicare la **Double-swipe (Doppia passata)** a un titolare della tessera.
   7.1. Aprire una scheda **Access Management (Gestione degli accessi)**.
   7.2. Fare clic su ⋮ sul titolare della tessera che si desidera modificare e fare clic su **Edit (Modifica)**.
   7.3. Fare clic su **More (Altro)**.
   7.4. Selezionare **Allow double-swipe (Consenti doppia passata)**.
   7.5. fare clic su **Applica**;

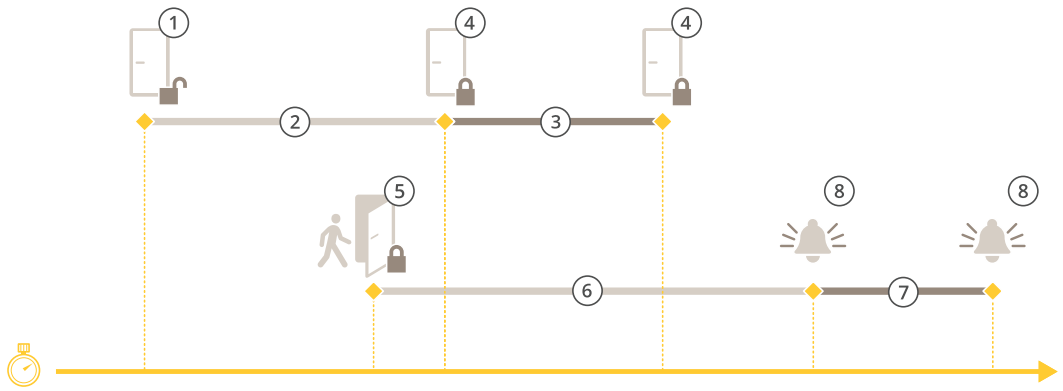
| Doppia passata | |
|---|---|
| **Timeout (secondi)** | Timeout è il tempo massimo consentito tra i passaggi di tessera o altri tipi di credenziali valide. |

### Opzioni relative all'orario




*1 Accesso consentito: la serratura si sblocca*
*2 Tempo di accesso*

*3 Nessuna azione intrapresa - il blocco rimane chiuso*
*4 Azione compiuta (porta aperta): la serratura si blocca o rimane sbloccata finché non si chiude la porta*
*5 Tempo di apertura eccessivo*
*6 Scatta l'allarme tempo di apertura eccessivo*




*1 Accesso consentito: la serratura si sblocca*
*2 Tempo di accesso*
*3 2+3: Tempo di accesso lungo*
*4 Nessuna azione intrapresa - il blocco rimane chiuso*
*5 Azione compiuta (porta aperta): la serratura si blocca o rimane sbloccata finché non si chiude la porta*
*6 Tempo di apertura eccessivo*
*7 6+7: Tempo di apertura eccessivo lungo:*
*8 Scatta l'allarme tempo di apertura eccessivo*

### Aggiungere un blocco wireless

AXIS Camera Station Pro supporta i blocchi wireless e gli hub di comunicazione ASSA ABLOY Aperio®. Il blocco wireless si collega al sistema attraverso un hub di comunicazione Aperio connesso al connettore RS485 del door controller. Si può connettere un massimo di 16 blocchi wireless a un door controller.

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

Nota

- L'impostazione richiede che il door controller Axis disponga della versione 11.6.16.1 o successiva di AXIS OS.
- L'impostazione richiede una licenza di AXIS Door Controller Extension valida.
- L'ora sul door controller di Axis e sul server AXIS Camera Station Pro deve essere sincronizzata.
- Prima di cominciare, usare l'applicazione Aperio che ASSA ABLOY supporta per associare i blocchi Aperio all'hub Aperio
- È possibile collegare un solo hub di comunicazione Aperio per ogni connettore RS485. La modalità multi-drop non è supportata.
- I blocchi wireless non seguono le pianificazioni di sblocco quando si è offline.

1. Accedere al door controller.
   1.1. Andare a **Configurazione > Dispositivi > Altri dispositivi**.

1.2. Aprire l'interfaccia Web del door controller connesso all'hub di comunicazione Aperio.

2. Attivare AXIS Door Controller Extension.
   2.1. Nell'interfaccia Web del door controller, andare a **Apps (App)**.
   2.2. Aprire il menu contestuale AXIS Door Controller Extension .
   2.3. Fare clic su **Activate license with a key (Attiva licenza con una chiave)** e selezionare la licenza.
   2.4. Attivare **AXIS Door Controller Extension**.
3. Connettere il blocco wireless al door controller attraverso l'hub di comunicazione.
   3.1. Nell'interfaccia web del door controller, andare ad **Access control > Wireless locks (Controllo degli accessi > Blocchi wireless)**.
   3.2. Fare clic su **Connect communication hub (Connetti hub comunicazioni)**.
   3.3. Immettere un nome per l'hub e fare clic su **Connect (Connetti)**.
   3.4. Fare clic su **Connect wireless lock (Collega blocco wireless)**.
   3.5. Selezionare l'indirizzo e le funzionalità di blocco per il blocco che si vuole aggiungere e fare clic su **Save (Salva)**.
4. Aggiungere e configurare la porta con il blocco wireless.
   4.1. In AXIS Camera Station Pro, andare a **Configuration > Access control > Doors and zones (Configurazione > Controllo degli accessi > Porte e zone)**.
   4.2. In **Doors (Porte)**, fare clic su **Add (Aggiungi)**.
   4.3. Selezionare **Wireless door (Porta wireless)** come **Door type (Tipo di porta)** e il door controller collegato all'hub di comunicazione Aperio.
   4.4. Fare clic su **Next (Avanti)**.
   4.5. Selezionare un **Wireless lock (Blocco wireless)**.
   4.6. Definire i lati porta A e B e aggiungere sensori. Per maggiori informazioni, vedere *Porte e zone, on page 147*.
   4.7. Fare clic su **Save (Salva)**.

Una volta connesso il blocco wireless, se ne può visualizzare il livello e lo stato della batteria nella panoramica delle porte.

| Livello batteria | Azione |
|---|---|
| Buono | Nessuno |
| Bassa | Il blocco funziona come previsto, ma è bene sostituirne la batteria prima che il livello diventi critico. |
| Critico | Sostituisci la batteria. Il blocco potrebbe non funzionare come previsto. |

| Stato serratura | Azione |
|---|---|
| Online | Nessuno |
| Blocco inceppato | Risoluzione di eventuali problemi meccanici del blocco. |

### Aggiungere un sensore di posizione della porta

Un sensore di posizione della porta è un interruttore che rileva lo stato fisico di una porta. È possibile aggiungere un sensore di posizione della porta e configurarne la modalità per connetterlo.

1. Andare alla pagina di configurazione della porta. Vedere *Aggiunta di una porta, on page 150*.
2. In **Sensors (Sensori)**, fare clic su **Add (Aggiungi)**.
3. Selezionare **Door position sensor (Sensore posizione porta)**.
4. Selezionare la porta I/O a cui si desidera collegare il monitor porta.
5. In **Door open if (Porta aperta se)**, selezionare la modalità di collegamento dei circuiti del monitor della porta.
6. Per ignorare le modifiche di stato dell'input digitale prima che entri in un nuovo stato stabile, imposta un **Debounce time (Tempo debounce)**.
7. Per attivare un evento quando la connessione tra il door controller e il monitor porta si interrompe, attivare il **Supervised input (Input supervisionato)**. Vedere *Ingressi con supervisione, on page 164*.

| **Porta aperta se** | |
|---|---|
| **Circuito aperto** | Il circuito del monitor porta è normalmente chiuso. Quando il circuito è aperto, il monitor porta invia un segnale di porta aperta. Quando il circuito è chiuso, il monitor porte invia un segnale di porta chiusa. |
| **Circuito chiuso** | Il circuito del monitor porta è normalmente aperto. Quando il circuito è chiuso, il monitor porta invia un segnale di porta aperta. Quando il circuito è aperto, il monitor porta invia un segnale di porta chiusa. |

### Aggiungere una porta di monitoraggio

Una porta di monitoraggio è un tipo di porta che può mostrare se è aperta o chiusa. Ad esempio, è possibile utilizzarla per una porta antincendio che non richiede una serratura, ma è necessario sapere se è aperta.

Una porta di monitoraggio è diversa da una porta normale dotata di monitor. Una porta normale con monitor supporta serrature e lettori, ma richiede un door controller. Una porta di monitoraggio supporta un sensore di posizione delle porte ma richiede solo un modulo relè I/O di rete collegato a un door controller. È possibile collegare fino a cinque sensori di posizione delle porte a un modulo relè I/O di rete.

Nota

Una porta di monitoraggio richiede un AXIS A9210 Network I/O Relay Module con il firmware più recente, inclusa l'applicazione AXIS Monitoring Door ACAP.

Per impostare una porta di monitoraggio:

1. Installare AXIS A9210 ed eseguire l'aggiornamento con l'ultima versione di AXIS OS.
2. Installare i sensori di posizione delle porte.
3. In AXIS Camera Station Pro, andare a **Configuration (Configurazione)** > **Access control (Controllo degli accessi)** > **Doors and zones (Porte e zone)**.
4. Fare clic su **Add door (Aggiungi porta)**.
5. Inserire un nome.
6. In **Type (Tipo)**, selezionare **Monitoring door (Porta di monitoraggio)**.
7. In **Device (Dispositivo)**, selezionare il modulo relè I/O di rete.
8. Fare clic su **Next (Avanti)**.
9. In **Sensors (Sensori)**, fare clic su + **Add (Aggiungi)** e selezionare **Door position sensor (Sensore di posizione delle porte)**.
10. Selezionare la porta I/O connessa al sensore di posizione delle porte.
11. Fare clic su **Aggiungi**.

### Aggiungere una planimetria BETA

Un piano è un tipo di porta che si utilizza per controllare l'accesso ai piani dell'ascensore. Quando si aggiunge un piano, si crea una risorsa ascensore che raggruppa tutti i piani per quell'ascensore. Ogni piano utilizza un lettore di tessere all'interno della cabina dell'ascensore per l'autenticazione degli utenti prima di consentire l'accesso al piano.

Prima di iniziare, è necessario:

- Un door controller di rete supportato aggiunto al sistema, come *AXIS A1610*, *AXIS A1710-B* o *AXIS A1810-B*.
- Un modulo di espansione I/O per utleriori relè. Consigliamo *AXIS A9920*.

Nota

Questa funzione è in versione Beta e attualmente supporta fino a 64 piani e solo lettori di schede.

Per impostare un piano:

1. Andare a **Configuration > Access control > Doors and zones (Configurazione, Controllo degli accessi Porte e zone)**.
2. Fare clic su + **Add (Aggiungi)** e selezionare **Piano** BETA.
3. Immettere un nome per il piano.
4. Selezionare il controller.
5. In **Elevator** (Ascensore), selezionare un ascensore esistente o fare clic su **Create new elevator** (Crea nuovo ascensore) per aggiungerne uno nuovo, quindi inserire un nome.
6. In **Side A (Lato A)**, selezionare **Card reader (Lettore tessere)** e configurare il lettore. **Side B** (Lato B) non può essere configurato per motivi di sicurezza.
7. Fare clic su **Save and add new** (Salva e aggiungi nuovo) per aggiungere più piani allo stesso ascensore. I campi di configurazione dell'ascensore e del lettore restano compilati per il piano successivo. Questa opzione è disponibile solo se il controller dispone di relè.
8. Fai clic su **Save** (Salva) dopo aver aggiunto il piano. I piani vengono denominato con "Nome ascensore - Nome piano": "Lato ovest - Piano 1"

Nota

- I lettori utilizzati su più piani possono essere sottoposti a modifica solo nel primo piano in cui sono stati aggiunti.
- Gli ascensori vengono eliminati in modo automatico quando sono eliminati tutti i piani correlati.

### Aggiungere un sensore di emergenza

Si può eseguire l'aggiunta e la configurazione di un input di emergenza per avviare un'azione che blocca o sblocca la porta. Si può anche configurare la modalità di collegamento del circuito.

1. Andare alla pagina di configurazione della porta. Vedere *Aggiunta di una porta, on page 150*.
2. In **Sensors (Sensori)**, fare clic su + **Add (Aggiungi)**.
3. Selezionare **Emergency input (Input di emergenza)**.
4. In **Emergency state (Stato di emergenza)**, selezionare la connessione di circuito.
5. Per ignorare le modifiche allo stato dell'ingresso digitale prima che entri in un nuovo stato stabile, configurare l'opzione **Debounce time (ms) (Tempo debounce (ms))**.
6. Selezionare l'elemento che deve essere attivato da **Emergency action (Azione di emergenza)** quando la porta riceve un segnale di stato di emergenza.

| Stato di emergenza | |
|---|---|
| **Circuito aperto** | Il circuito di ingresso di emergenza è normalmente chiuso. Quando il circuito è aperto, l'ingresso di emergenza invia un segnale di stato di emergenza. |
| **Circuito chiuso** | Il circuito di ingresso di emergenza è normalmente aperto. Quando il circuito è chiuso, l'input di emergenza invia un segnale di stato di emergenza. |

| Azione di emergenza | |
|---|---|
| **Sblocca porta** | La porta si sblocca nel momento in cui riceve il segnale di stato di emergenza. |
| **Blocca porta** | La porta si sblocca nel momento in cui riceve il segnale di stato di emergenza. |

### Aggiungere un lettore IP

È possibile utilizzare come lettore un intercom di rete Axis o un altro dispositivo abilitato all'IP. Prima di poterlo assegnare a una porta, si deve aggiungere il dispositivo ad AXIS Camera Station Pro.

Nota

Prima di iniziare, assicurarsi che il lettore IP sia acceso e connesso alla stessa rete di AXIS Camera Station Pro.

1. Andare a **Configuration > Devices > Add devices (Configurazione, Dispositivi, Aggiungi dispositivi)**.
2. Selezionare il lettore IP dall'elenco dei dispositivi rilevati e fare clic su **Add (Aggiungi)**.
3. Inserire le credenziali del dispositivo quando richiesto.

Una volta aggiunto il dispositivo, è possibile assegnarlo a una porta. Vedi *Aggiungere un formato di un lettore tessera, on page 159*.

### Aggiungere un formato di un lettore tessera

Si può configurare un door controller per supportare più lettori cablati. Scegliere di aggiungere un lettore su un lato o su entrambi i lati di una porta.

Se si applica un'impostazione personalizzata dei formati tessera o della lunghezza del PIN a un lettore, apparirà in **Card formats (Formati tessera)** in **Configuration > Access control > Doors and zones (Configurazione > Controllo degli accessi > Porte e zone)**. Vedere *Porte e zone, on page 147*.

Nota

- È inoltre possibile aggiungere fino a 16 lettori Bluetooth a un door controller. Per ulteriori informazioni, vedere *Aggiungi un lettore Bluetooth, on page 161*.
- Se si usa un interfono di rete Axis come un lettore IP, il sistema impiega la configurazione PIN impostata nella pagina Web del dispositivo.

1. Andare alla pagina di configurazione della porta. Vedere *Aggiunta di una porta, on page 150*.
2. Su un lato della porta, fare clic + **Add (Aggiungi)**.
3. Selezionare **Card reader (Lettore di schede)**.
4. Selezionare **Reader type (Tipo di lettore)**.
5. Per usare una lunghezzaa PIN personalizzata per questo lettore:
   5.1. fare clic su **Avanzate**;
   5.2. Attivare **Custom PIN length (Lunghezza PIN personalizzata)**.

5.3. Imposta la **Min PIN length (Lunghezza PIN minima)**, **Max PIN length (Lunghezza PIN massima)** e **End of PIN character (Fine del carattere PIN)**.

6. Per usare un formato tessera personalizzato per questo lettore:
   6.1. fare clic su **Avanzate**;
   6.2. Attivare i **Custom card formats (Formati tessera personalizzati)**.
   6.3. Selezionare i formati tessera che si desidera utilizzare per il lettore. Se è già in uso un formato tessera con la stessa lunghezza in bit, è necessario disattivarlo prima. Un'icona di avviso compare nel client quando la configurazione del formato scheda differisce dall'impostazione del sistema configurata.
7. Fare clic su **Aggiungi**.
8. Per l'aggiunta di un lettore all'altro lato della porta, ripetere la procedura.

Per informazioni su come installare un lettore AXIS Barcode Reader vedere *Installa AXIS Barcode Reader, on page 170*.

| **Tipo di lettore** | |
|---|---|
| **OSDP** | Per i lettori che supportano le credenziali crittografate Axis, selezionare **OSDP**, una porta del lettore e un indirizzo del lettore. |
| **SSCP** | Per i lettori che supportano il protocollo SSCP in modalità trasparente, selezionare **SSCP**, la porta del lettore e un indirizzo del lettore. Questa modalità supporta le credenziali crittografate sulle tessere MIFARE DESFire. |
| **Wiegand** | Per i lettori che usano i protocolli Wiegand, selezionare **Wiegand** e una porta per il lettore. |
| **Lettore IP** | Selezionare **IP reader (Lettore IP)** e scegliere un dispositivo dal menu a discesa. È possibile utilizzare gli intercom di rete Axis come lettori IP. |

| **Wiegand** | |
|---|---|
| **Comando LED** | Selezionare **Single wire (Cavo singolo)** o **Dual wire (R/G) (Cavo doppio (R/G))**. I lettori con controllo LED doppio utilizzano cavi diversi per i LED rossi e verdi. |
| **Avviso manomissione** | Selezionare lo stato del circuito che attiva l'input di manomissione del lettore.<br>• **Open circuit (Circuito aperto)**: Il lettore invia il segnale di manomissione alla porta quando il circuito è aperto.<br>• **Closed circuit (Circuito chiuso)**: Il lettore invia il segnale di manomissione alla porta quando il circuito è chiuso. |

| | |
|---|---|
| **Tamper debounce time (Tempo debounce manomissione)** | Per ignorare le variazioni di stato dell'input manomissione del lettore prima che entri in un nuovo stato stabile, impostare un **Tamper debounce time (Tempo debounce manomissione)**. |
| **Input supervisionato** | Attivare per il trigger di un evento quando c'è un'interruzione della connessione tra il door controller e il lettore. Vedere *Ingressi con supervisione, on page 164*. |

### Aggiungi un lettore Bluetooth

È possibile utilizzare il lettore Bluetooth® di rete AXIS A4612 Network Bluetooth® Reader per estendere i limiti delle porte cablate dei door controller di Axis. È possibile assegnare un massimo di 16 lettori per ogni door controller. Ogni lettore può gestire la serratura della porta, la richiesta di uscita (REX) e l'interruttore di posizione della porta (DPS).

L'aggiunta e l'utilizzo di questi lettori non richiede alcuna licenza aggiuntiva.

Per aggiungere un lettore AXIS A4612 Network Bluetooth Reader a una porta:

1. Assicurarsi di aver associato AXIS A4612 con il door controller. Vedere *Utilizzare l'app AXIS Mobile Credential come credenziali Bluetooth, on page 161*.
2. Andare alla pagina di configurazione della porta. Vedere *Aggiunta di una porta, on page 150*.
3. Su un lato della porta, fare clic su + **Add (Aggiungi)**, quindi su **Card reader (Lettore scheda)**.
4. Selezionare **IP reader** (lettore IP) e scegliere l'AXIS A4612 associato dal menu a discesa. Se il lettore è utilizzato per l'associazione delle credenziali, contrassegnarlo per l'associazione. Fare clic su **Aggiungi**.
5. Nella scheda **Overview** (Panoramica), modificare il profilo di identificazione. È possibile utilizzare i profili **Tap in app** (Tocca in app) o **Touch reader** (Lettore touch) se l'AXIS A4612 è collegato solo a un lato della porta e si utilizza un REX sull'altro.

### Utilizzare l'app AXIS Mobile Credential come credenziali Bluetooth

Questo esempio mostra come aggiungere un lettore Bluetooth AXIS A4612 al sistema per consentire ai titolari della tessera di sbloccare le porte tramite l'app AXIS Mobile Credential.

1. Installare il lettore Bluetooth e collegarlo al controller della porta.
2. Aggiungere il lettore Bluetooth nell'interfaccia web del controller della porta.
   2.1. Accedere al controller della porta e passare a **Peripherals (Periferiche)** > **Readers (Lettori)**.
   2.2. Fare clic su **Add reader (Aggiungi lettore)**.
   2.3. Inserire le informazioni richieste nella finestra di dialogo **Add Bluetooth reader (Aggiungi lettore Bluetooth)**.
   2.4. Fare clic su **Aggiungi**.
3. Aggiungere il lettore Bluetooth a una porta su AXIS Camera Station Pro.
   3.1. Andare a **Configuration (Configurazione)** > **Access control (Controllo degli accessi)** > **Doors and zones (Porte e zone)**.
   3.2. Selezionare la porta a cui aggiungere il lettore Bluetooth e fare clic su **Edit (Modifica)**.
   3.3. Fare clic su + **Add (Aggiungi)** sul lato della porta dove si trova il lettore Bluetooth.
   3.4. Selezionare **Card reader (Lettore di schede)**.
   3.5. In **Add IP reader (Aggiungi lettore IP)**, selezionare **IP reader (Lettore IP)**.
   3.6. In **Select IP reader (Seleziona lettore IP)**, selezionare il lettore Bluetooth.

3.7. Fare clic su **Aggiungi**.

4. Selezionare un lettore Bluetooth per l'associazione. Questa operazione deve essere eseguita per almeno un lettore Bluetooth presente nel sistema.
   4.1. Selezionare il lettore Bluetooth appena aggiunto.
   4.2. Fare clic su **Edit (Modifica)**.
   4.3. IN **Edit bluetooth reader (Modifica lettore Bluetooth)**, selezionare **Use this reader for pairing (Usa questo lettore per l'associazione)**.
   4.4. fare clic su **Applica**;
5. Scegliere il profilo di identificazione **Tap in app (Tocco nell'app)** o **Touch reader (Tocco sul lettore)**. Per ulteriori informazioni, vedere *Profili di identificazione, on page 165*.
6. Aggiungere le credenziali mobili al titolare della tessera. Vedere *Aggiungi credenziali, on page 188*.
7. Associare le credenziali mobili al lettore di associazione:
   7.1. Avvicinare il telefono cellulare del titolare della tessera al lettore Bluetooth abilitato.
   7.2. Seguire le istruzioni fornite nell'e-mail inviata al titolare della tessera.

### Aggiungi un dispositivo REX

È possibile aggiungere una richiesta per uscire da un dispositivo (REX) su un lato o su entrambi i lati della porta. Un dispositivo REX può essere un sensore PIR, un pulsante REX o un maniglione.

1. Andare alla pagina di configurazione della porta. Vedere *Aggiunta di una porta, on page 150*.
2. Sotto un lato della porta, fare clic su **Add (Aggiungi)**.
3. Selezionare **REX device (Dispositivo REX)**.
4. Selezionare la porta I/O a cui si desidera connettere il dispositivo REX. Se è disponibile una sola porta, questa viene selezionata automaticamente.
5. Selezionare quale **Action (Azione)** attivare quando la porta riceve il segnale REX.
6. Selezionare la connessione circuiti del monitor della porta in **REX active (REX attivo)**.
7. Per ignorare le modifiche allo stato dell'ingresso digitale prima che entri in un nuovo stato stabile, configurare l'opzione **Debounce time (ms) (Tempo debounce (ms))**.
8. Per attivare un evento quando la connessione tra il door controller e il dispositivo REX s'interrompe, attivare **Supervised input (Input supervisionato)**. Vedere *Ingressi con supervisione, on page 164*.

| Azione | |
|---|---|
| **Sblocca porta** | Sceglierlo per sbloccare la porta nel momento in cui riceve il segnale REX. |
| **Nessuno** | Selezionare questa opzione per non eseguire alcuna azione quando la porta riceve il segnale REX. |

| REX attivo | |
|---|---|
| **Circuito aperto** | Selezionare questa opzione se il circuito REX è normalmente chiuso. Il dispositivo REX invia il segnale quando il circuito è aperto. |
| **Circuito chiuso** | Selezionare questa opzione se il circuito REX è normalmente aperto. Il dispositivo REX invia il segnale quando il circuito è chiuso. |

### Aggiunta di una zona

Una zona è un'area fisica specifica con un gruppo di porte. È possibile creare zone e aggiungere porte alle zone. Esistono due tipi di porte:

- **Perimeter door (Porta perimetrale:** I titolari della tessera entrano nella zona o la abbandonano attraverso questa porta.
- **Internal door (Porta interna):** Una porta interna all'interno della zona.

Nota

Una porta perimetrale può appartenere a due zone. Una porta interna può appartenere a una sola zona. Per una panoramica, consultare *Esempio di porte e zone, on page 150*.

1. Andare a **Configuration > Access control > Doors and zones > Zones (Configurazione > Controllo degli accessi > Porte e zone > Zone)**.
2. Fare clic su **Add zone (Aggiungi zona)**.
3. Immettere il nome di una zona.
4. Fare clic su **Add door (Aggiungi porta)**.
5. Selezionare le porte che si vuole aggiungere alla zona e fare clic su **Add (Aggiungi)**.
6. La porta è impostata come porta perimetrale per impostazione predefinita. Per modificarla, selezionare **Internal door (Porta interna)** dal menu a discesa.
7. Per impostazione predefinita, una porta perimetrake impiega il lato A della porta come lato di ingresso per la zona. Per modificare questa impostazione, selezionare **Leave (Abbandona)** dal menu a discesa.
8. Per rimuovere una porta dalla zona, selezionarla e fare clic su **Remove (Rimuovi)**.
9. Fare clic su **Save (Salva)**.

Per modificare una zona:

1. Andare a **Configuration > Access control > Doors and zones > Zones (Configurazione > Controllo degli accessi > Porte e zone > Zone)**.
2. Selezionare una zona dall'elenco.
3. Fare clic su **Edit (Modifica)**.
4. Modificare le impostazioni e fare clic su **Save (Salva)**.

Per rimuovere una zona:

1. Andare a **Configuration > Access control > Doors and zones > Zones (Configurazione > Controllo degli accessi > Porte e zone > Zone)**.
2. Selezionare una zona dall'elenco.
3. Fare clic su **Remove (Rimuovi)**.
4. Fare clic su **Sì**.

### Livello di sicurezza zona

Si può aggiungere la funzionalità di sicurezza che segue ad una zona:

**Anti-passback –** Fa sì che le persone non possano impiegare le stesse credenziali di qualcuno entrato in un'area prima di loro. Per poter utilizzare nuovamente le proprie credenziali, è necessario uscire dall'area.

Nota

- Con l'anti-passback, tutte le porte nella zona devono avere sensori di posizione della porta in modo che il sistema possa registrare che un utente ha aperto la porta dopo aver passato la carta.
- Se un door controller passa offline, l'anti-passback funziona finché tutte le porte nella zona appartengono allo stesso door controller. Tuttavia, se le porte nella zona appartengono a diversi door controller che passano offline, l'anti-passback smette di funzionare.

Si può eseguire la configurazione del livello di sicurezza quando si aggiunge una nuova zona o la si applica a una zona esistente. Per eseguire l'aggiunta di un livello di sicurezza a una zona esistente:

1. Andare a **Configuration (Configurazione)** > **Access control (Controllo degli accessi)** > **Doors and zones (Porte e zone)**.
2. Eseguire la selezione della zona per la quale si desidera configurare un livello di sicurezza.
3. Fare clic su **Edit (Modifica)**.
4. Fare clic su **Security level (Livello di sicurezza)**.
5. Eseguire l'attivazione delle funzioni di sicurezza che si vogliono aggiungere alla zona.
6. fare clic su **Applica**;

| **Anti-passback** | |
|---|---|
| **Log violation only (Soft) (Solo log violazione (tollerante))** | Selezionare questa opzione per consentire a una seconda persona di inserire le stesse credenziali della prima persona. Questa opzione risulta unicamente in un allarme di sistema. |
| **Deny access (Hard) (Nega accesso (rigido))** | Selezionare questa opzione per impedire che una seconda persona inserisca le stesse credenziali della prima. Anche questa opzione risulta in un allarme di sistema. |
| **Timeout (secondi)** | Il tempo che deve trascorrere prima che il sistema consenta all'utente di entrare di nuovo. Inserire 0 per disattivare il timeout; in questo modo, la funzione anti-passback rimarrà attiva fino a quando l'utente non uscirà dalla zona. Usare unicamente il timeout 0 con **Deny access (Hard) (Nega accesso (rigido))** se tutte le porte nella zona hanno lettori su entrambi i lati. |

**Ingressi con supervisione**

Gli ingressi supervisionati sono in grado di attivare un evento in caso di interruzione della connessione a un door controller.

- Collegamento tra Door controller e Door monitor. Vedere *Aggiungere un sensore di posizione della porta, on page 156*.
- Collegamento tra Door controller e lettore basato su protocolli Wiegand. Vedere *Aggiungere un formato di un lettore tessera, on page 159*.
- Collegamento tra Door controller e dispositivo REX. Vedere *Aggiungi un dispositivo REX, on page 162*.

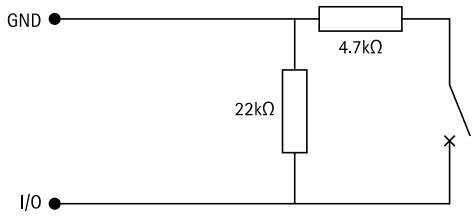
Per utilizzare gli input supervisionati:

1. Installare resistori terminali il più vicino possibile al dispositivo periferico secondo lo schema delle connessioni.
2. Andare alla pagina di configurazione di un lettore, di un monitor porta o di un dispositivo REX, attivare **Supervised input (Input supervisionato)**.

3. Se è stato seguito lo schema di prima connessione parallela, selezionare **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Prima connessione parallela con un resistore parallelo da 22 KΩ e un resistore seriale da 4,7 KΩ)**.
4. Se è stato seguito lo schema di prima connessione in serie, selezionare **Serial first connection (Prima connessione in serie)** e selezionare un valore dei resistori dal menu a discesa **Resistor values (Valori resistore)**.

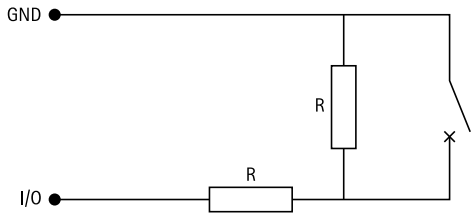
**Prima connessione parallela**

I valori dei resistori devono essere 4,7 kΩ e 22 kΩ.




**Prima connessione in serie**

I valori dei resistori devono essere uguali nell'intervallo compreso tra 1 e 10 kΩ.




## Profili di identificazione

Un profilo di identificazione è una combinazione di tipi di identificazione e pianificazioni. Si può applicare un profilo di identificazione a una o molteplici porte per impostare come e quando un titolare tessera è in grado di accedere a una porta.

Nota

Si devono usare QR e PIN dinamici insieme.

Andare a **Configuration > Access control > Identification profiles (Configurazione > Controllo degli accessi > Profili di identificazione)** per creare, modificare o rimuovere profili di identificazione.

I profili di identificazione disponibili:

**Badge –** I titolari della tessera devono strisciare la tessera per accedere alla porta.

**Tessera e PIN –** I titolari della tessera devono strisciare la tessera e inserire il PIN per accedere alla porta.

**PIN –** I titolari della tessera devono inserire il PIN per accedere alla porta.

**Tessera o PIN –** I titolari della tessera devono strisciare la tessera o inserire il PIN per accedere alla porta.

**QR –** I titolari della tessera devono mostrare il QR Code® alla telecamera per ottenere l'accesso alla porta. Si può usare il profilo di identificazione QR sia per QR statico sia per QR dinamico.

**Targa –** I titolari della tessera devono dirigersi verso la telecamera a bordo di un veicolo con targa omologata.

**Tocco nell'app –** I titolari della tessera devono inserire le credenziali nell'app AXIS Camera Station Mobile mentre si trovano nel raggio d'azione del lettore Bluetooth.

**Tocco sul lettore –** I titolari della tessera devono toccare il lettore Bluetooth quando usano un telefono cellulare con credenziali mobili.

*QR Code è un marchio registrato di Denso Wave Incorporated in Giappone e in altri paesi.

### Creare un profilo di identificazione

1. Andare a **Configuration > Access control > Identification profiles (Configurazione > Controllo degli accessi > Profili di identificazione)**.
2. Fare clic su + **Create identification profile (Crea profilo di identificazione)**.
3. Inserire un nome per il profilo di identificazione.
4. Selezionare **Include facility code for card validation (Includi codice struttura per convalida tessera)** per utilizzare il codice struttura come uno dei campi di convalida delle credenziali. Questo campo è disponibile solo se si attiva **Facility code (Codice struttura)** in **Access management > Settings (Gestione degli accessi > Impostazioni)**.
5. Per il Lato A, fare clic su + **Add (Aggiungi)**, selezionare un tipo di identificazione e una pianificazione.
   - Per richiedere ai titolari di tessere di utilizzare più di un tipo di identificazione, selezioni più tipi nella stessa riga.
   - Per consentire ai titolari di tessere di utilizzare entrambi i tipi, fare clic nuovamente su + **Add (Aggiungi)** e aggiungere un'altra riga.
6. Per il Lato B, fare clic su + **Add (Aggiungi)**, selezionare un tipo di identificazione e una pianificazione.
7. Fare clic su **OK**.

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

*Impostare profili di identificazione*

### Modificare un profilo di identificazione

1. Andare a **Configuration > Access control > Identification profiles (Configurazione > Controllo degli accessi > Profili di identificazione)**.
2. Selezionare un profilo di identificazione e fare clic su ✎.
3. Per cambiare il nome del profilo di identificazione, inserire un nuovo nome.
4. Eseguire le modifiche per il lato della porta.
5. Per modificare il profilo di identificazione dall'altro lato della porta, ripetere i passaggi precedenti.
6. Fare clic su **OK**.

| Modifica profilo di identificazione | |
|---|---|
| × | Per rimuovere un tipo di identificazione e la pianificazione correlata. |
| **Tipo di identificazione** | Per modificare un tipo di identificazione, selezionare uno o più tipi dal menu a discesa **Identification type (Tipo di identificazione)**. |

| | |
|---|---|
| **Pianificazione** | Per modificare una pianificazione, selezionare una o più pianificazioni dal menu a discesa **Schedule (Pianificazione)**. |
| + **Aggiungi** | Aggiungere un tipo di identificazione e la pianificazione correlata, fare clic su **Add (Aggiungi)** e impostare i tipi di identificazione e le pianificazioni. |

**Rimuovere un profilo di identificazione**

1. Andare a **Configuration > Access control > Identification profiles (Configurazione > Controllo degli accessi > Profili di identificazione)**.
2. Selezionare un profilo di identificazione e fare clic su 🗑.
3. Se il profilo di identificazione è usato su una porta, selezionare un altro profilo di identificazione per la porta.
4. Fare clic su **OK**.

**Ripristinare un formato tessera predefinito:**

1. Andare a **Configuration > Access Control > Card formats and PIN (Configurazione > Controllo degli accessi > Formati tessera e PIN)**.
2. Fare clic su ↺ per ripristinare un formato tessera alla mappa dei campi predefinita.

## Formati tessera e PIN

Un formato di scheda definisce il modo in cui un lettore di schede interpreta i dati provenienti da una scheda. Sono disponibili formati di scheda predefiniti che è possibile utilizzare o modificare; inoltre, è possibile creare formati di scheda personalizzati

Andare a **Configuration > Access Control > Card formats and PIN (Configurazione > Controllo degli accessi > Formati tessera e PIN)**. La pagina presenta due schede:

**Configurazione PIN –** Impostare la lunghezza del PIN e il carattere di fine del PIN.

**Formati tessera –** Visualizzare, creare, modificare, eliminare e attivare i formati scheda.

**PIN**

Impostare la lunghezza minima e massima del PIN. Se si effettuano impostazioni diverse per il minimo e il massimo, definire un carattere di fine PIN per segnalare che l'inserimento del PIN è terminato.

1. Andare a **Configuration > Access Control > Card formats and PIN (Configurazione, Controllo degli accessi, Formati tessera e PIN, Configurazione PIN)**.
2. Inserire **Min PIN length (Lunghezza minima del PIN)** e **Max PIN length (Lunghezza massima del PIN)**.
3. Se necessario, inserire **End of PIN character (Carattere di fine PIN)**.
4. Fare clic su **OK**.

**Aggiungere un formato di una tessera**

1. Andare a **Configuration > Access Control > Card formats and PIN (Configurazione, Controllo degli accessi, Formati tessera e PIN)**.
2. Fare clic su + **Add** (Aggiungi).
3. Inserire un nome e una lunghezza in bit compresa tra 1 e 256.

4. Selezionare **Invert bit order (Inverti ordine dei bit)** se si desidera invertire l'ordine dei bit dei dati ricevuti dal lettore di tessere.
5. Selezionare **Invert byte order (Inverti ordine dei byte)** se si desidera invertire l'ordine dei byte dei dati ricevuti dal lettore di tessere. Questa opzione è disponibile solo quando si specifica una lunghezza in bit che si può dividere per otto.
6. Attivare **Card Number (Codice tessera)**, **Facility code (Codice struttura)** o entrambi. Almeno uno di essi deve essere attivo nel formato delle schede.
7. Impostare l'intervallo bit dei dati per il campo dati. L'intervallo deve essere compreso tra i valori specificati per bit length (Lunghezza in bit).
8. Selezionare il formato di output dei dati per il campo dati.
   - Decimale: Il sistema numerico a base 10. Utilizza i numeri 0-9.
   - Hexadecimal (Esadecimale): Il sistema numerico a base 16. Utilizza 16 simboli: i numeri 0-9 e le lettere a-f.
9. Selezionare l'ordine dei bit.
   - Little-endian: Il primo bit è il più piccolo o il meno significativo.
   - Big-endian: Il primo bit è il più grande (più significativo.
10. Fare clic su **OK**.

Nota

- Non è possibile che due formati scheda con la stessa lunghezza in bit possano essere attivi contemporaneamente. Per esempio, se sono stati definiti due formati di tessera a 32 bit, solo uno può essere attivo. Eseguire la disattivazione del formato tessera per attivare l'altro.
- È possibile attivare e disattivare i formati scheda solo se il door controller è stato configurato con almeno un lettore.
- È possibile effettuare la modifica dei formati tessera predefiniti, ma non è possibile eliminarli. Per annullare eventuali modifiche apportate a un formato predefinito, selezionare sull'icona di ripristino per ripristinarlo alle impostazioni predefinite. È possibile eliminare i formati di tessera che sono stati creati.

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

*Impostazione dei formati tessera*

**Modificare il formato di una tessera:**

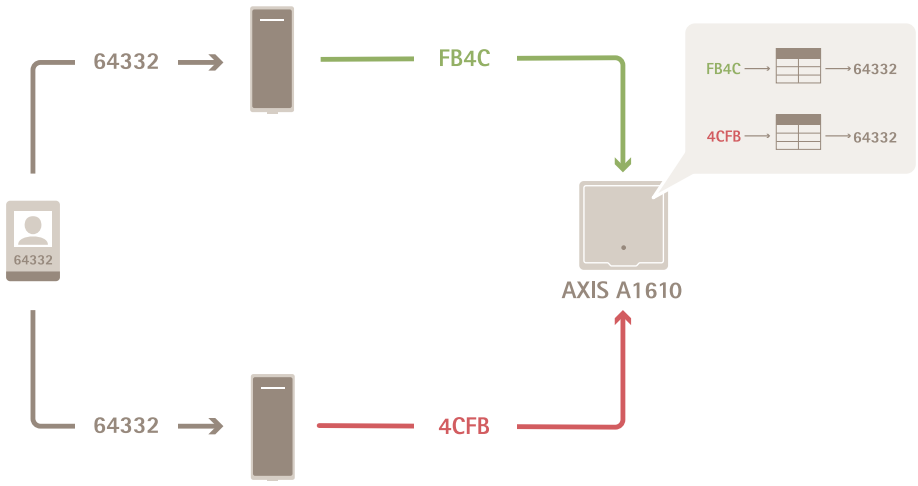
1. Andare a **Configuration > Access Control > Card formats and PIN (Configurazione > Controllo degli accessi > Formati tessera e PIN)**.
2. Selezionare un formato tessera e fare clic su .
3. Se cambia un formato tessera predefinito, si può modificare solo **Invert bit order (Inverti ordine dei bit)** e **Invert byte order (Inverti ordine dei byte)**.
4. Fare clic su **OK**.

È possibile rimuovere solo i formati tessera personalizzati. Per rimuovere un formato tessera personalizzato:

1. Andare a **Configuration > Access Control > Card formats and PIN (Configurazione > Controllo degli accessi > Formati tessera e PIN)**.
2. Selezionare un formato tessera personalizzato, fare clic su e **Yes (Sì)**.

## Impostazioni formato tessera

### Panoramica




- Il codice carta in decimale è `64332`.
- Un lettore trasferisce il codice carta al numero esadecimale `FB4C`. L'altro lettore la trasferisce al numero esadecimale `4CFB`.
- AXIS A1610 Network Door Controller riceve `FB4C` e lo trasferisce al numero decimale `64332` in base alle impostazioni del formato tessera nel lettore.
- AXIS A1610 Network Door Controller riceve `4CFB` e lo cambia in `FB4C` invertendo l'ordine dei byte e lo trasferisce al numero decimale `64332` in base alle impostazioni del formato tessera nel lettore.

### Inverti ordine bit

Dopo aver capovolto l'ordine dei bit, i dati della scheda ricevuti dal lettore vengono letti da destra a sinistra bit per bit.

### Inverti ordine byte

Un gruppo di otto bit è un byte. Dopo aver capovolto l'ordine dei byte, i dati della scheda ricevuti dal lettore vengono letti da destra a sinistra byte per byte.

### Formato tessera Wiegand standard a 26 bit

P FFFFFFFF NNNNNNNNNNNNNNNN P

① ② ③ ④

1 *Parità principale*
2 *Codice struttura*
3 *Numero tessera*
4 *Parità finale*

## Comunicazione crittografata

### Canale sicuro OSDP

AXIS Camera Station Secure Entry supporta il canale sicuro OSDP (Open Supervised Device Protocol) per l'attivazione della crittografia della linea tra il dispositivo di controllo e i lettori Axis.

Per attivare il canale sicuro OSDP per un intero sistema:

1. Andare a **Configuration > Access control > Encrypted communication (Configurazione > Controllo degli accessi > Comunicazione crittografata)**.
2. Inserire la chiave di crittografia principale e fare clic su **OK**.
3. Attivare **OSDP Secure Channel (Canale sicuro OSDP)**. Solo dopo l'inserimento della chiave di crittografia principale questa opzione diventa disponibile.
4. Per impostazione predefinita, la chiave di crittografia principale genera una chiave del canale sicuro OSDP. Per impostare in modo manuale la chiave del canale sicuro OSDP:
   4.1. In **OSDP Secure Channel (Canale sicuro OSDP)** fare clic su .
   4.2. Deselezionare **Use main encryption key to generate OSDP Secure Channel key (Utilizzare la chiave di crittografia principale per generare la chiave del canale sicuro OSDP)**.
   4.3. Inserire la chiave del canale sicuro OSDP e fare clic su **OK**.

Per l'attivazione o la disattivazione del canale sicuro OSDP per un lettore specifico, vedere *Porte e zone*.

### AXIS Barcode Reader

AXIS Barcode Reader è un'applicazione che si può installare sulle telecamere Axis. Il door controller Axis utilizza la chiave di autenticazione periferica esterna per concedere l'accesso e autenticare il lettore di codici a barre AXIS Barcode Reader e AXIS License Plate Verifier. Per un flusso di lavoro completo per l'impostazione di AXIS License Plate Verifier in AXIS Camera Station Pro, vedere .

### Installa AXIS Barcode Reader

1. Scaricare il file di installazione dell'applicazione da *axis.com*.
2. Vai alla pagina Web del tuo interfono o della tua telecamera Axis.
3. Installa l'applicazione.
4. Attivare la licenza.
5. Avvia l'applicazione.
6. Consigliamo la modifica delle seguenti impostazioni della telecamera per maggiore precisione del QR.
   6.1. Vai alle impostazioni della telecamera.
   6.2. In **Image > Exposure (Immagine > Esposizione)**, sposta il cursore **Blur-noise trade-off (Compromessi disturbo-sfocatura)** al centro.

### Configura AXIS Barcode Reader

1. Per modificare il profilo di identificazione QR, andare in **Configuration (Configurazione) > Access control (Controllo degli accessi) > Identification profiles (Profili di identificazione)** e fare clic su . Vedi *Profili di identificazione*.
2. Aggiunta di una porta. Vedere *Aggiunta di una porta*.
3. Seleziona **QR** come profilo di identificazione per questa porta. Vedere *Impostazioni porta*.
4. Aggiungi un lettore di codice a barre. Vedi *Aggiungi un lettore*.
   4.1. Sotto un lato della porta, fare clic su **Add reader (Aggiungi lettore)**.
   4.2. Seleziona **AXIS Barcode Reader** da **Reader type (Tipo di lettore)** dall'elenco a discesa. Immetti un nome e fai clic su **OK**.

### Crea una connessione con il door controller

1. In AXIS Camera Station Pro:
   1.1. Andare a **Configuration > Access control > Encrypted communication (Configurazione > Controllo degli accessi > Comunicazione crittografata)**.
   1.2. In **External Peripheral Authentication Key (Chiave di autenticazione dispositivo periferico esterno)**, fare clic su **Show authentication key (Mostra chiave di autenticazione)** e **Copy key (Copia chiave)**.
2. Nell'interfaccia Web del dispositivo dove si esegue AXIS Barcode Reader:
   2.1. Aprire l'applicazione AXIS Barcode Reader.
   2.2. Se il certificato del server non è stato configurato in AXIS Camera Station Pro, attivare **Ignore server certificate validation (Ignora convalida certificato server)**. Per ulteriori informazioni, vedi *Certificati*.
   2.3. Se il certificato del server non è stato configurato in AXIS Camera Station Pro, attivare **Ignore server certificate validation (Ignora convalida certificato server)**. Per ulteriori informazioni, vedi *Certificati*.
   2.4. Attiva **AXIS Camera Station Secure Entry**.
   2.5. Fai clic su **Add (Aggiungi)** e immetti l'indirizzo IP del door controller e incolla la chiave di autenticazione.
   2.6. Selezionare il lettore che legge codici a barre dal menu a discesa della porta.

## Multi-server BETA

I server secondari collegati possono, con multi server, usare i titolari di tessera e i gruppi di titolari di tessera globali dal server principale.

Nota

- Un sistema è un grado di supportare un massimo di 64 server secondari.
- Richiede AXIS Camera Station 5.47 o successivo.
- Il server principale e i server secondari devono essere sulla stessa rete.
- Sui server principali e sui server secondari, assicurati di configurare Windows Firewall per permettere le connessioni TCP in entrata sulla porta Secure Entry. La porta predefinita è 55767. Per una configurazione personalizzata delle porte, consultare la sezione *Impostazioni generali del server*.
- Il collegamento di un server secondario a un server principale comporta la sostituzione della chiave del suo lettore, rendendo non valide tutte le credenziali Bluetooth esistenti. Per evitare ciò, creare le credenziali Bluetooth sul server principale anziché sul server secondario.

### Flusso di lavoro

1. Configura un server come server secondario e genera il file di configurazione. Vedere *Genera il file di configurazione dal server secondario, on page 172*.
2. Configura un server come server principale e importa il file di configurazione dei server secondari. Vedere *Importa il file di configurazione sul server principale, on page 172*.
3. Configura i titolari di tessera e i gruppi di titolari di tessera globali nel server principale. Vedere *Aggiungi un titolare tessera, on page 186* e *Aggiungi un gruppo, on page 191*.
4. Visualizza e monitora i titolari di tessera e i gruppi di titolari di tessera globali dal server secondario. Vedere *Gestione degli accessi, on page 186*.

### Genera il file di configurazione dal server secondario

1. Dal server secondario, vai su **Configuration > Access control > Multi server (Configurazione > Controllo degli accessi > Multiserver)**.
2. Fai clic su **Sub server (Server secondario)**.
3. Fare clic su **Generate (Genera)**. Viene generato un file di configurazione in formato .json.
4. Fai clic su **Download** e scegli una posizione per salvare il file.

### Importa il file di configurazione sul server principale

1. Dal server principale, vai su **Configuration > Access control > Multi server (Configurazione > Controllo degli accessi > Multiserver)**.
2. Fai clic su **Main server (Server principale)**.
3. Fare clic su + **Add (Aggiungi)** e andare al file di configurazione generato dal server secondario.
4. Inserisci il nome del server, l'indirizzo IP e il numero di porta del server secondario.
5. Fare clic su **Import (Importa)** per eseguire l'aggiunta del server secondario.
6. Lo stato del server secondario indicato è `Connected`.

### Revoca un server secondario

Si può revocare un server secondario solo prima di importarne il file di configurazione su un server principale.

1. Dal server principale, vai su **Configuration > Access control > Multi server (Configurazione > Controllo degli accessi > Multiserver)**.
2. Fai clic su **Sub server (Server secondario)** e fai clic su **Revoke server (Revoca server)**.
   Ora puoi configurare questo server come server principale o secondario.

### Rimuovi un server secondario

Dopo l'importazione del file di configurazione di un server secondario, connette il server secondario al server principale.

Per rimuovere un server secondario:

1. Dal server principale:
   1.1. Andare a **Access management > Dashboard (Gestione degli accessi > Dashboard)**.
   1.2. Trasformare i titolari di tessera e i gruppi globali in titolari di tessera e gruppi locali.
   1.3. Andare a **Configuration > Access control > Multi server (Configurazione > Controllo degli accessi > Multiserver)**.
   1.4. Fare clic su **Main server (Server principale)** per mostrare l'elenco dei server secondari.
   1.5. Seleziona il server secondario e fai clic su **Delete (Elimina)**.

2. Dal server secondario:
   - Andare a **Configuration > Access control > Multi server (Configurazione > Controllo degli accessi > Multiserver)**.
   - Fare clic su **Sub server (Server secondario)** e su **Revoke server (Revoca server)**.

### Impostazioni di Active Directory[BETA]

Nota

Gli account utente in Microsoft Windows e gli utenti e i gruppi di Active Directory possono accedere ad AXIS Camera Station Pro. Il modo in cui si aggiungono gli utenti in Windows varia a seconda della versione. Per saperne di più, andare a *support.microsoft.com*. Vedere l'amministratore di rete se si usa una rete di dominio di Active Directory.

La prima volta che viene aperta la pagina delle impostazioni Active Directory, hai la possibilità di importare gli utenti di Microsoft Active Directory nei titolari di tessera in AXIS Camera Station Pro. Vedere *Importare gli utenti Active Directory, on page 173*.

Dopo la configurazione iniziale, appaiono le seguenti opzioni nella pagina impostazioni di Active directory.

- Creare e gestire gruppi di titolari di tessera a seconda dei gruppi in Active Directory.
- Impostare la sincronizzazione pianificata tra Active Directory e il sistema di gestione degli accessi.
- Sincronizzare in modo manuale per eseguire l'aggiornamento di tutti i titolari di tessera importati da Active Directory.
- Gestire la mappatura dei dati tra i dati utente di Active Directory e le proprietà dei titolari di tessera.

#### Importare gli utenti Active Directory

Per eseguire l'importazione degli utenti Active Directory ai titolari di tessera in AXIS Camera Station Pro:

1. Andare su **Configuration (Configurazione)** > **Access control (Controllo degli accessi)** > **Active directory settings (Impostazioni di Active Directory)**[BETA].
2. Fare clic su **Set up import (Configura importazione)**.
3. Seguire le istruzioni sullo schermo per completare queste tre fasi principali:
   - 3.1. Selezionare un utente da Active Directory da impiegare in qualità di modello per la mappatura dati.
   - 3.2. Mappare dati utente dal database Active Directory alle proprietà dei titolari di tessera.
   - 3.3. Creare un nuovo gruppo di titolari di tessera nel sistema di gestione degli accessi e selezionare quali gruppi Active Directory vanno importati.

Non è possibile modificare i dati utente importati, ma è possibile aggiungere le credenziali a un titolare di una tessera importata, vedere *Aggiungi credenziali, on page 188*.

Importante

Se si disattiva un utente in Active Directory, AXIS Camera Station Pro elimina definitivamente il titolare della tessera e tutti i dati correlati, compresa la cronologia. Questa non può essere annullata. Per bloccare l'accesso di un titolare di tessera senza perdere i suoi dati, sospenderli in AXIS Camera Station Pro anziché disattivarli in Active Directory.

## Configurare AXIS Audio Manager Pro

È possibile connettersi a un server AXIS Audio Manager Pro e utilizzare i dispositivi audio collegati in AXIS Camera Station Pro.

Questa impostazione richiede AXIS Camera Station Pro 6.12 o versioni successive e AXIS Audio Manager Pro 5.0 o versioni successive. Entrambi i server devono essere impostati sia sullo stesso server che su computer diversi all'interno della stessa rete.

Importante

Se AXIS Camera Station Pro e AXIS Audio Manager Pro sono entrambi in esecuzione sullo stesso server, entrambi utilizzano la porta 443 come da impostazione predefinita. Per evitare problemi di connessione, configurare uno dei due dispositivi per l'utilizzo di una porta diversa.

È possibile modificare la configurazione della porta in AXIS Camera Station Pro tramite *Impostazioni del server generali, on page 216*. Per informazioni su come modificare la configurazione della porta in AXIS Audio Manager Pro, consultare *AXIS Audio Manager Pro — Manuale per l'utente*.

Per iniziare a utilizzare AXIS Audio Manager Pro in AXIS Camera Station Pro:

1. In AXIS Audio Manager Pro:
   1.1. Andare a **System settings** > **API access** (Impostazioni di sistema, Accesso API).
   1.2. Abilitare l'API e inserire nome utente e password.
2. In AXIS Camera Station Pro:
   2.1. Andare a **Configuration** > **AXIS Audio Manager Pro** (Configurazione, AXIS Audio Manager PRO) e fare clic su **Connect** (Connetti) per configurare una connessione al server AXIS Audio Manager Pro.
   2.2. Nella finestra di dialogo popup, inserire **Server URL** (l'URL del server), **API username** (Nome utente API) e **API password** (Password API) del server AXIS Audio Manager Pro, quindi fare clic su **Connect** (Connetti).

Quando la connessione è stabilita, è possibile:

- Visualizzare **Server status** (Stato del server) di AXIS Audio Manager Pro e **Device status** (Stato dispositivo) dei dispositivi collegati a tale server.
- Aprire una nuova scheda AXIS Audio Manager Pro per accedere all'interfaccia web del server.
- Utilizzare le nuove funzionalità relative all'audio disponibili in AXIS Camera Station Pro.

Per ulteriori informazioni, consultare *AXIS Audio Manager Pro, on page 207*.

Nota

Per evitare problemi relativi ai certificati, si consiglia di creare o ottenere un certificato da un'autorità di certificazione (CA) attendibile, caricarlo su AXIS Audio Manager Pro e aggiungerlo all'elenco dei certificati attendibili del server AXIS Camera Station Pro. Per ulteriori informazioni, consultare *AXIS Audio Manager Pro - Manuale per l'utente*.

## Configura la ricerca intelligente 2

Con Ricerca intelligente 2, è possibile impostare i filtri per trovare persone e veicoli di interesse nelle registrazioni generate dalle telecamere Axis.

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

Per i requisiti, i limiti e l'utilizzo di ricerca intelligente 2, vedere *Ricerca intelligente 2, on page 38*.

1. Andare su **Configuration > Smart search 2 (Configurazione > Ricerca intelligente 2) > Settings (Impostazioni)**.
2. In **Cameras (Telecamere)**:
   2.1. Selezionare le telecamere che devono inviare i metadati a Ricerca intelligente 2.
   2.2. Per permettere la classificazione server in background per una telecamera, selezionare **Allow (Consenti)** in **Background server classification (Classificazione server in background)**.

Questa operazione aumenta il carico del server, ma migliora l'esperienza utente.

2.3. Per limitare la quantità di rilevamenti salvati sul server, in **Filter (Filtro)**, fare clic su ⚙ e creare filtri per **Area (Area)**, **Size and duration (Dimensione e durata)**, e **Swaying objects (Oggetti ondulanti)**.
È possibile utilizzare questi filtri per escludere aree, oggetti piccoli o che appaiono soltanto per un periodo di tempo molto breve, oppure oggetti ondulanti come il fogliame.
I filtri di Ricerca intelligente usano qualsiasi filtro delle impostazioni di movimento esistente come punto di partenza.

3. In **Storage (Archiviazione)**:
   - Seleziona l'unità e la cartella dove archiviare i rilevamenti e fai clic su **Apply (Applica)**.
   - Imposta il limite per le dimensioni di archiviazione e fai clic su **Apply (Applica)**. Quando l'archiviazione raggiunge il limite, rimuove i rilevamenti più vecchi.
4. Selezionare **Include periods with missing metadata (Includi periodi con metadati mancanti)** per visualizzare i risultati per i quali non sono stati registrati metadati.
5. Selezionare **Let the server classify detections when you start a search** (Consentire al server di classificare i rilevamenti quando i avvia una ricerca) per ottenere risultati di ricerca più dettagliati, inclusi i rilevamenti che la telecamera non ha classificato. Per ottenere risultati di ricerca più rapidi, si consiglia di disattivare questa opzione.

| Classificazione server in background | |
|---|---|
| | Stato della classificazione del server dell'ultima ora quando la classificazione del server è lenta. Appare quando viene classificato meno del 95% dei rilevamenti. |
| | Stato della classificazione del server dell'ultima ora quando la classificazione del server è lenta. Appare quando viene classificato meno del 50% dei rilevamenti. |

## Attivazioni

È possibile configurare filtri di ricerca intelligente come trigger nelle regole di azione. Per creare un trigger di ricerca intelligente:

1. Andare a **Configuration** > **Smart search 2** > **Triggers** (Configurazione, Ricerca intelligente, Trigger).
2. Fare clic su **Create (Crea)**.
3. Impostare il filtro. Per ulteriori informazioni sui filtri di ricerca intelligente, consultare *Ricerca con filtri, on page 38*.
4. Fare clic su **Next (Avanti)**.
5. Regolare il livello di **Confidence** (Confidenza) dei rilevamenti. Un livello di confidenza più elevato elimina le classificazioni incerte, riducendo il numero di rilevamenti.
6. Fare clic su **Next (Avanti)**.
7. Inserire un nome per il trigger e fare clic su **Save** (Salva).

Nota

- Smart search 2 richiede solitamente alcuni secondi dopo che un oggetto è uscito dal campo visivo della telecamera per analizzare il filmato e verificare il rilevamento. Ad esempio, se è stata impostata una

regola di azione che si attiva al rilevamento di un'auto rossa, l'azione si attiva solo pochi secondi dopo che l'oggetto è uscito dal campo visivo della telecamera.

- **Visual similarity** (Somiglianza visiva) non è disponibile come opzione per i trigger di Smart search 2.
- La creazione di un trigger per una telecamera consente al server di elaborare i rilevamenti di oggetti anche se l'opzione **Enable background processing** (Abilita elaborazione in background) è disattivata per quella telecamera.
- **Delayed detection periods (Periodi di rilevamento ritardati)** sono periodi con un elevato ritardo di elaborazione con conseguente attivazione ritardata delle regole di azione. Se ciò si verifica di frequente, è possibile riconfigurare il filtro trigger per includere un numero inferiore di telecamere e utilizzare filtri quali attraversamento linea, area, dimensione e durata per ridurre i ritardi di elaborazione.

Per utilizzare trigger di Smart search 2 in una regola di azione, consultare *Creazione di trigger con Smart search 2, on page 103*.

## Configura Monitoraggio dell'integrità del sistema BETA

Nota

- Quando si è connessi a più server AXIS Camera Station Pro, è possibile configurare il Monitoraggio dell'integrità del sistema su qualsiasi server connesso. A tal fine, selezionare il server dal menu a discesa **Selected server (Server selezionato)**.
- Se si gestiscono sistemi che si trovano su reti diverse, il monitoraggio server in My Systems mette a disposizione la stessa funzionalità, ma tramite cloud.

### Impostazioni

| | |
|---|---|
| **Connessione a cloud** | Se il server è stato registrato con un'organizzazione, è possibile visualizzare ovunque i dati relativi all'integrità del sistema. Se non si è ancora connessi, fare clic su **Manage (Gestisci)** e seguire le istruzioni sullo schermo. |
| **Data retrieval frequency (Frequenza recupero dati)** | Selezionare una frequenza di aggiornamento dei dati inferiore per risolvere gli avvisi relativi a dati obsoleti o a problemi generali di prestazioni. In una configurazione multisistema, raccomandiamo di utilizzare per un sottosistema un'impostazione uguale o superiore a quella del sistema sovraordinato.<br>• **Low (Basso)**: per sistemi con oltre 100 dispositivi.<br>• **Medium (Medio)**: per sistemi con 25-100 dispositivi.<br>• **High (Alto)**: per sistemi con meno di 25 dispositivi. |

### Notifiche

Per inviare notifiche e-mail:

1. Configura un server SMTP e un indirizzo e-mail per l'invio delle notifiche. Vedere *Impostazioni server, on page 126*
2. Configura gli indirizzi e-mail per la ricezione delle notifiche. Vedere *Configurazione di destinatari e-mail, on page 177*.
3. Configura le regole di notifica. Vedere *Configura regole di notifica, on page 177*.

### Configurazione di destinatari e-mail

1. Andare a **Configuration > System Health Monitoring > Notifications (Configurazione > Monitoraggio dell'integrità del sistema > Notifiche)**.
2. In **Email recipients (Destinatari e-mail)**, immettere un indirizzo e-mail e fare clic su **Save (Salva)**. Ripeti l'operazione per eseguire l'aggiunta di più destinatari e-mail.
3. Per testare il server SMTP, fai clic su **Send test email (Invia e-mail di prova)**. Un messaggio conferma l'invio di un'e-mail di prova.

### Configura regole di notifica

Sono presenti due regole di notifica attivate per impostazione predefinita.

**Sistema fuori uso –** Manda una notifica quando il sistema in una singola impostazione di sistema o qualsiasi sistema in un'impostazione multisistema è fuori uso per più tempo del previsto.

**Dispositivo fuori uso –** Inviare una notifica quando un dispositivo elencato in Monitoraggio dell'integrità del sistema è fuori uso per più tempo del previsto.

1. Andare a **Configuration > System Health Monitoring > Notifications (Configurazione > Monitoraggio dell'integrità del sistema > Notifiche)**.
2. In **Notification rules (Regole di notifica)**, è possibile attivare o disattivare le regole di notifica.
3. In **Applied rules (Regole applicate)** è possibile visualizzare un elenco di sistemi e dispositivi e le regole di notifica applicate.

## Multisystem

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

Con System Health Monitoring, puoi eseguire da un sistema principale il monitoraggio dei dati relativi all'integrità di vari sistemi secondari.

1. In un sistema secondario, eseguire la generazione della configurazione di sistema. Vedere *Genera configurazione di sistema, on page 177*.
2. Nel sistema principale, caricare la configurazione di sistema. Vedere *Recupero di dati da altri sistemi, on page 178*.
3. Ripeti i passaggi precedenti in altri sistemi secondari.
4. Esegui il monitoraggio dei dati relativi all'integrità di molteplici sistemi dal sistema principale. Vedere *Monitoraggio dell'integrità del sistema BETA, on page 198*.

### Genera configurazione di sistema

1. Andare a **Configuration > System Health Monitoring > Multisystem (Configurazione > Monitoraggio dell'integrità del sistema > Multisistema)**.
2. Fare clic su **Generate (Genera)**.
3. Fare clic su **Copy (Copia)** per copiarlo e caricarlo nel sistema principale.
4. Per vedere i dettagli della configurazione di sistema, fai clic su **Show details (Mostra dettagli)**.
5. Per la rigenerazione della configurazione di sistema, fare clic su **Delete (Elimina)** per eliminare prima quella esistente.

Dopo aver caricato la configurazione del sistema nel sistema principale, le informazioni del sistema principale appaiono in **Systems with access (Sistemi con accesso)**.

**Recupero di dati da altri sistemi**

Dopo aver generato e copiato la configurazione di un sistema secondario è possibile caricarla nel sistema principale.

1. Nel sistema principale, andare a **Configuration > System Health Monitoring > Multisystem (Configurazione > Monitoraggio dell'integrità del sistema > Multisistema)**.
2. Fare clic su **Paste (Incolla)** per aggiungere le informazioni copiate dal sistema secondario.
3. Controllare l'indirizzo IP dell'host e fai clic su **Add (Aggiungi)**.
   Il sistema secondario appare in **Available systems (Sistemi disponibili)**.

## Configurazione dell'analisi

### AXIS Data Insights Dashboard

AXIS Data Insights Dashboard presenta i dati di analisi dai dispositivi in grafici e tabelle. La pagina di configurazione di AXIS Data Insights Dashboard mostra tutte le applicazioni supportate e gli scenari configurati sui dispositivi del sistema.

Andare in **Analytics (Analisi)** > **Data Insights Dashboard (Cruscotto dati)** per:

- Creare e gestire dashboard
- Includere o escludere scenari
- Vedere lo stato degli scenari
- Configurare gli scenari nel contesto
- Utilizzare i tag negli scenari per filtrare i dati
- Visualizzare un elenco di dispositivi e fonti di dati che eseguono le applicazioni supportate
- Visualizzare un elenco delle applicazioni e degli scenari supportati per ogni dispositivo o fonte di dati
  Sono supportate le seguenti applicazioni e scenari:
  - AXIS Object Analytics: Conteggio attraversamenti e presenza in un'area
  - AXIS Audio Analytics
  - AXIS Image Health Analytics
  - AXIS People Counter
  - AXIS P8815-2 3D Counter
  - AXIS Air Quality Sensors

La pagina di configurazione di Axis Data Insights Dashboard presenta tre schede: Dashboard, Devices e Tags.

- **Dashboard:** creare, modificare o rimuovere dashboard. Una volta aggiunti i dispositivi, la cartella Dashboard diventa automaticamente visibile nella visualizzazione in diretta.
- **Devices (Dispositivi):** consente di accedere alle interfacce dei dispositivi per effettuare l'impostazione delle fonti dei dati di input per la propria dashboard. L'elenco dei dispositivi viene filtrato automaticamente per mostrare solo i dispositivi compatibili con i modelli selezionati.
- **Tag:** Creare, modificare o rimuovere tag. Etichettare gli scenari per filtrare i dati nella dashboard, ad esempio per il raggruppamento dei dispositivi nella stessa posizione.

Per aggiungere un nuovo scenario di dashboard:

1. Aprire la scheda **Dashboards**.
2. Fare clic su **New... (Nuovo)** per aprire la pagina di configurazione.
3. Inserire un nome per la dashboard.

4. Selezionare un modello della dashboard, *Modelli di scenario disponibili per la dashboard, on page 179*.
5. Fare clic su **Add (Aggiungi)** per visualizzare le telecamere disponibili.
6. Nella finestra **Select devices (Seleziona dispositivi)**, selezionare una telecamera e fare clic su **OK**. Fare clic su **Cancel (Annulla)** se non si desidera salvare le modifiche.
7. Fare clic su **Configure (Configura)** per aprire la finestra **Configure devices (Configura dispositivi)** e abilitare o disabilitare gli scenari.
8. Fare clic sul dispositivo per espandere lo scenario.
9. Abilitare lo scenario selezionando la casella di controllo corrispondente.
10. In alternativa, aggiungere tag nella scheda **Tags**.
11. Fare clic su **OK** per salvare le modifiche e chiudere la finestra a comparsa.
12. Fare clic su **Add (Aggiungi)** per completare la nuova dashboard.

Nota

La stima dell'occupazione richiede di assegnare le direzioni, mentre il monitoraggio del traffico no.

Per aggiungere una nuova etichetta:

1. Aprire la scheda **Tags (Etichette)**.
2. Inserire un nome per il tag nella scheda **Create (Crea)**.
3. Fare clic su una freccia per salvare il tag.

Nota

- AXIS Data Insights Dashboard richiede la versione 1.2 o superiore di TLS per le connessioni crittografate sul server Windows.
- AXIS Data Insights Dashboard sovrascrive qualsiasi impostazione MQTT esistente in un dispositivo se:
  - Il dispositivo non ha un client MQTT configurato.
  - È stato abilitato in modo manuale un dispositivo per una telecamera connessa a un altro server AXIS Camera Station Pro.
- Mentre è collegato ad AXIS Data Insights Dashboard, il client MQTT sul dispositivo è dedicato alla dashboard Data Insights.
- I dispositivi e il server AXIS Camera Station Pro devono essere sulla stessa rete.

### Modelli di scenario disponibili per la dashboard

#### Stima dell'occupazione

Utilizzare questa dashboard per stimare il numero di persone o oggetti attualmente presenti all'interno di un'area, sulla base degli ingressi e delle uscite.

- Mostra server:
  - Stima attuale del numero di persone, ingressi e uscite
  - Flusso in entrata e in uscita nel tempo
  - Andamento dei livelli di presenza, picchi di presenza, utilizzo degli ingressi e mappa termica basata sul tempo
- Fonti dei dati:
  - Scenari di conteggio trasversale di AXIS Object Analytics (AOA)
  - Sono supportate anche le fonti di Conteggio persone e di Conteggio persone stereo
- Configurazione:
  1. Creare uno scenario di conteggio attraversamento linea presso ogni ingresso o uscita e selezionare le classi di oggetti da conteggiare.
  2. Aggiungere i dispositivi pertinenti alla dashboard.

3. In Configura dispositivi, includere ogni scenario di origine.
4. Per le fonti AOA, assegnare a ciascuno scenario lo stato In (in entrata) oppure Out (in uscita).

Nota

La stima si calcola sottraendo i conteggi in uscita a quelli in entrata. Assegnare indicazioni direzionali coerenti per tutti gli ingressi selezionati.

Il risultato è una stima e dipende dall'accuratezza degli scenari di conteggio configurati.

**Monitoraggio del traffico**

Utilizzare questa dashboard per analizzare il volume e la composizione del traffico che transita su una o più linee virtuali.

- Mostra server:
  - Totale odierno, media oraria e ora di punta
  - Conteggi nel tempo e mappe termiche delle attività
  - Tendenze medie orarie e nei giorni feriali
  - Totali per categoria di oggetto
- Fonti dei dati:
  - Scenari di conteggio di attraversamento linea AOA
- Configurazione:
  1. Crea uno o più scenari di conteggio di attraversamento linea in AOA.
  2. Posizionare ciascuna linea virtuale nel punto di misurazione desiderato e selezionare le classi di oggetti pertinenti.
  3. Aggiungere i dispositivi pertinenti alla dashboard.
  4. In Configure devices (Configura dispositivi), includere gli scenari richiesti.

Nota

La dashboard riepiloga i conteggi di attraversamento linea selezionati e li raggruppa per ora e per categoria di oggetto. Non richiede l'assegnazione "In" o "Out" nella dashboard di Axis Data Insights.

AOA stessa richiede una direzione di trigger per ciascuna linea virtuale. Creare scenari distinti nei casi in cui sia necessario conteggiare il traffico in entrambe le direzioni fisiche.

**Analitiche zona**

Utilizzare questa dashboard per monitorare il numero stimato di oggetti attualmente presenti nelle aree definite.

- Mostra server:
  - Presenza attuale per zona e ora dell'ultimo aggiornamento
  - Presenza media nel tempo
  - Presenza zona combinata, orari di punta e mappa termica basata sul tempo
- Fonti dei dati:
  - Scenari di occupazione nell'area AOA
- Configurazione:
  1. Creare uno scenario di occupazione dell'area per ciascuna zona.
  2. Definire l'area di interesse e selezionare le classi di oggetti da includere.
  3. Aggiungere i dispositivi pertinenti alla dashboard.
  4. In Configure devices (Configura dispositivi), includere gli scenari richiesti.

Nota

Ogni scenario diventa una zona nella dashboard. Il valore di occupazione rappresenta la stima di AOA relativa agli oggetti attualmente presenti in quella zona, compresi quelli fissi. Non è richiesta alcuna assegnazione In oppure Out.

### Analitiche audio

Utilizzare questa dashboard per analizzare gli eventi audio rilevati e i livelli sonori sui dispositivi selezionati.

- Mostra server:
  - Eventi audio rilevati per tipo, fonte, ora e giorno della settimana
  - Misure del livello di pressione sonora nel tempo
- Fonti dei dati:
  - Funzionalità AXIS Audio Analytics abilitate sui dispositivi compatibili
- Configurazione:
  1. Abilitare e configurare le funzionalità audio analitiche richieste su ciascun dispositivo.
  2. Aggiungere i dispositivi pertinenti alla dashboard.
  3. In Configure devices (Configura dispositivi), includere le sorgenti audio richieste.
  4. In alternativa, assegnare dei tag per filtrare la dashboard.

### Condizione dell'immagine

Utilizzare questa dashboard per monitorare i problemi relativi alla qualità di immagine delle telecamere e individuare i dispositivi che richiedono un intervento.

- Mostra server:
  - Stato di integrità del dispositivo: Normale, Avviso o Critico
  - Attività degli allarmi per ora e durata
  - Totali degli allarmi per tipo di problema
  - Dispositivi con gli allarmi più recenti
- Fonti dei dati:
  - Funzionalità di AXIS Image Health Analytics abilitate sui dispositivi compatibili
- Configurazione:
  1. Abilitare le funzionalità di Image Health Analytics richieste su ciascun dispositivo.
  2. Aggiungere i dispositivi pertinenti alla dashboard.
  3. In Configure devices (Configura dispositivi), includere le fonti attive relative all'integrità delle immagini.
  4. In alternativa, assegnare dei tag per filtrare la dashboard.

Nota

Lo stato di un dispositivo è Healthy (integro) quando non vengono segnalati allarmi.

Quando sono presenti degli allarmi, viene visualizzato un messaggio di avviso.

Si verifica una situazione critica quando in un giorno vengono segnalati più di tre allarmi o quando la durata complessiva degli allarmi supera i 30 minuti.

### Monitoraggio della qualità dell'aria

Utilizzare questa dashboard per avere una panoramica della qualità dell'aria interna rilevata dai dispositivi selezionati.

- Mostra server:
  - Indice di qualità dell'aria (AQI) e AQI medio
  - Valori medi per dispositivo
  - $CO_2$, VOC, NOx, particolato, temperatura, umidità, indice di calore e Humidex
  - Valori massimi per ora
  - Eventi di rilevamento fumo di sigaretta elettronica/normale, ove previsti

- Fonti dei dati:
  - Dispositivi di monitoraggio della qualità dell'aria AXIS compatibili (ad esempio AXIS D6310, D6210)
- Configurazione:
  1. Aggiungere alla dashboard i dispositivi di monitoraggio della qualità dell'aria pertinenti.
  2. Selezionare Celsius o Fahrenheit per la temperatura.
  3. In alternativa, assegnare dei tag per filtrare la dashboard.

Nota

Utilizzare questo scenario per confrontare le condizioni di qualità dell'aria in diverse ubicazioni o su diversi dispositivi.

**Monitoraggio qualità dell'aria dettagliato**

Utilizzare questa dashboard per analizzare i dati dettagliati sulla qualità dell'aria e gli allarmi relativi ai dispositivi selezionati.

- Mostra server:
  - AQI e misurazioni dettagliate relative a $CO_2$, VOC, NOx, particolato, temperatura, umidità, indice di calore e Humidex
  - Allarmi relativi alla qualità dell'aria
  - Eventi di rilevamento fumo di sigaretta elettronica/normale, ove previsti
- Fonti dei dati:
  - Dispositivi di monitoraggio della qualità dell'aria AXIS compatibili (ad esempio AXIS D6310, D6210)
- Configurazione:
  1. Aggiungere alla dashboard i dispositivi di monitoraggio della qualità dell'aria pertinenti.
  2. Selezionare Celsius o Fahrenheit per la temperatura.
  3. In alternativa, assegnare dei tag per filtrare la dashboard.

Nota

Utilizzare questo scenario quando sono necessari valori dettagliati e informazioni sugli allarmi relativi a un dispositivo specifico o a un numero limitato di dispositivi.

Importante

- Per prestazioni ottimali, consigliamo l'uso di un server con un minimo di 16 GB di RAM per eseguire AXIS Data Insights Dashboard in AXIS Camera Station Pro.
- È possibile archiviare un massimo di 200 MB di dati, pertanto il tempo di archiviazione sarà limitato. Ad esempio puoi:
  - Le analitiche di zona in un parcheggio dotato di quattro telecamere, ciascuna configurata per rilevare cinque sottoclassi di veicoli come auto e biciclette 24 ore su 24, 7 giorni su 7, ha come risultato un periodo di conservazione di 1700 giorni.
  - Il monitoraggio del traffico con una telecamera in grado di contare sei categorie di veicoli, in funzione ininterrottamente 24 ore su 24, 7 giorni su 7, ha come risultato un periodo di conservazione dei dati di circa 7000 giorni.
  - La stima dell'occupazione in un ambiente di vendita al dettaglio dotato di otto telecamere, in cui il flusso di persone è continuo per 12 ore, ha come risultato un periodo di conservazione di circa 6200 giorni.
  - Un sensore di qualità dell'aria con monitoraggio di tutti i 12 tipi di dati ha come risultato un periodo di conservazione di circa 3400 giorni.

### License Plate Verifier

Nella pagina AXIS License Plate Verifier è possibile visualizzare lo stato del verificatore targhe AXIS sulle proprie telecamere e raggruppare le telecamere per facilitare la gestione dell'elenco.

La scheda **Cameras** (telecamere) contiene un elenco di tutti i dispositivi collegati con AXIS License Plate Verifier installato:

- **Telecamera**: Il nome della telecamera.
- **Version (Versione)**: Quale versione di AXIS License Plate Verifier è installata sulla telecamera.
- **Status (Stato)**: Lo stato attuale di AXIS License Plate Verifier.
- **Latest event (Ultimo evento)**: L'ora dell'ultimo evento registrato dalla telecamera.
- **Allowed (Autorizzato)**: Il numero di targhe incluse nell'elenco degli "Autorizzati" della telecamera.
- **Blocked (Bloccati)**: Il numero di targhe incluse nell'elenco "Bloccati" della telecamera.
- **Personalizzato**: Il numero di targhe incluse nell'elenco "Personalizzato" della telecamera.
- **Gruppo**: A quale gruppo appartiene la telecamera.

La scheda **Groups (Gruppi)** elenca tutti i gruppi di telecamere e le telecamere presenti in ciascun gruppo. In questa scheda è possibile:

- Fare clic su **New... (Nuovo...)** per aggiungere un nuovo gruppo.
- Fare clic su **Delete (Elimina)** per eliminare un gruppo esistente.
- Rinominare un gruppo selezionato nel campo **Group Name (Nome gruppo)**
- Fare clic su **Add... (Aggiungi...)** per aggiungere la telecamera al gruppo selezionato.
- Fare clic su **Remove (Rimuovi)** per rimuovere una telecamera da un gruppo.

È possibile creare elenchi condivisi per telecamere raggruppate. Per ulteriori informazioni, consultare *Gestione delle targhe, on page 206*.

## Configurare la body cam

### Collegare un sistema body cam

Collegare il sistema body cam ad AXIS Camera Station Pro per trasferire le registrazioni e i metadati dalle telecamere body cam.

1. Andare a **Configuration > Body worn > Connect a body worn system** (Configurazione, Body cam, Collegare un sistema Body cam).
2. In **Connection method** (Metodo di connessione), selezionare la modalità di connessione desiderata:
   - **Connect directly** (Connessione diretta): Inserire l'indirizzo IP e le credenziali del Body cam manager.
   - **Generate connection file** (Genera file di connessione): Creare un file di configurazione da caricare su Body Worn Manager.

Nota

Prima di creare il file di connessione, è necessario rinnovare il certificato server se l'indirizzo IP del server è cambiato o se AXIS Camera Station è stato aggiornato da una versione precedente alla 5.33. Per informazioni su come rinnovare il certificato, vedere *Certificati, on page 140*.

Se è stata selezionata **Connect directly (Connessione diretta)**

3. In **Configure direct connection** (Configura connessione diretta), immettere **IP address** (Indirizzo IP), **User name** (Nome utente), e **Password** (Password) per Body Worn Manager.

1. In alternativa, modificare il **nome di sistema di AXIS Camera Station**. Questo nome indica la destinazione delle registrazioni copiate e trasferite.

2. Se desidera chiudere tutte le connessioni attive, selezionare **End existing connections** (Termina connessioni attive). Caricare il nuovo file di connessione su ciascun controller del sistema AXIS Body Cam.
3. Fare clic su **Connetti**.

Se è stato selezionato **Generate connection file** (Genera file di connessione):

4. In **Generate connection file** (Genera file di connessione), modificare in alternativa **il nome del sistema di AXIS Camera Station**. Questo consente di identificare dove vengono copiate o trasferite le registrazioni.
   4.1. Se desidera chiudere tutte le connessioni attive, selezionare **End existing connections** (Termina connessioni attive). Caricare il nuovo file di connessione su ciascun controller del sistema AXIS Body Cam.
   4.2. Fare clic su **Export** (Esporta) e salvare il file di connessione.
   4.3. Caricare il file di connessione sul Body Worn Manager.

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

*Impostazione di un sistema indossabile Axis*

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

*Riproduzione ed esportazione delle registrazioni della telecamera indossabile AXIS Body Worn Camera*

## Istantanee

Esportare automaticamente le istantanee dai segnalibri delle body cam in una cartella al momento del trasferimento delle registrazioni su AXIS Camera Station Pro.

1. Andare a **Configuration > Body worn > Snapshots** (Configurazione, Body cam, Istantanee).
2. In **Storage location (Posizione di archiviazione)**, inserire il percorso della cartella in cui si desidera salvare le istantanee.
3. fare clic su **Applica**;
4. Attivare **Snapshot export** (Esporta istantanee).

## Integrazione CAD

Integrare il Sistema di dispacciamento assistito da computer (CAD) per classificare automaticamente le registrazioni delle body cam in base ai dati di invio.

Per impostare l'integrazione:

1. Andare a **Configuration > Body worn > CAD integration** (Configurazione, Body cam, Integrazione CAD).
2. Fare clic su **Set up integration (Configura integrazione)**.
3. Selezionare il formato del file (CSV o XML) e fare clic su **Next** (Avanti).
4. Attivare l'opzione **Shared network drive** (Disco di rete condiviso) se il file CAD si trova su un disco di rete condiviso.

5. Inserire il percorso della cartella in cui si trova il file CAD, il nome del file (solo per CSV) e il separatore di colonna.
6. Fare clic su **Next (Avanti)**.
7. Mappare ciascun campo all'identificatore così come appare nel file CAD:
   - **Officer name (Nome agente)**: deve corrispondere ai nomi delle telecamere virtuali in AXIS Camera Station Pro. Se il nome non corrisponde, aggiornarlo in Body Worn Manager, non in AXIS Camera Station Pro.
   - **Event ID (ID evento)**: identificatore univoco della spedizione.
   - **Call category (Categoria chiamata)**: categoria di registrazione. Se non esiste, verrà creata.
   - **Dispatch time (Ora di invio)**: ora di inizio in formato RFC 3339, ad esempio "2025-11-25T09:49:17+01:00".
   - **Clearance time (Tempo di ripristino)**: orario di fine nel formato RFC 3339.
   - **Case number (Numero di pratica)**: l'ID della pratica associata alla spedizione. La colonna deve essere presente nel file, ma il valore può essere lasciato vuoto.
8. Fare clic su **Finish** (Fine) poi su **Apply** (Applica).
9. Per rivedere le registrazioni, fare clic su + e selezionare **CAD recordings** (Registrazioni CAD) per visualizzare tutte le registrazioni classificate in modo automatico. È possibile filtrare i risultati in base all'ora o al nome dell'agente.

Nota

Se le nuove categorie vengono create automaticamente, si deve impostare manualmente i relativi periodi di conservazione.

**Limiti**

Le informazioni potrebbero andare perse se:

- AXIS Camera Station Pro o il componente non è in esecuzione.
- I file di esportazione superano 1 GB.
- È necessario aggiornare le credenziali di rete.

## Impostazioni dispositivi indossabili

Configurare le posizioni di archiviazione per le registrazioni effettuate con la body cam.

**Memorizzazione della registrazione**

Selezionare un punto di archiviazione predefinito per le registrazioni effettuate con le Body Cam per i nuovi utenti del sistema:

1. Andare a **Configuration > Body worn > Body worn settings** (Configurazione, Body cam, Impostazioni body cam).
2. In **Recording storage (Archiviazione registrazioni)** selezionare un disco dall'elenco a discesa **Disk (Disco)**.
3. Fare clic su **Save (Salva)**.

**Archiviazione delle registrazioni rifiutata**

Selezionare il punto per archiviare i contenuti rifiutati dalla body cam:

1. In **Rejected recordings storage (Archiviazione registrazioni rifiutate)**, selezionare un disco dall'elenco a discesa **Disk (Disco)** e digitare un nome della **Folder (Cartella)**.
2. Impostare il numero di giorni in cui conservare i contenuti rifiutati in **Number of days to keep rejected content from the body worn system** (Numero di giorni in cui conservare i contenuti rifiutati dal sistema body cam).
3. Fare clic su **Save (Salva)**.

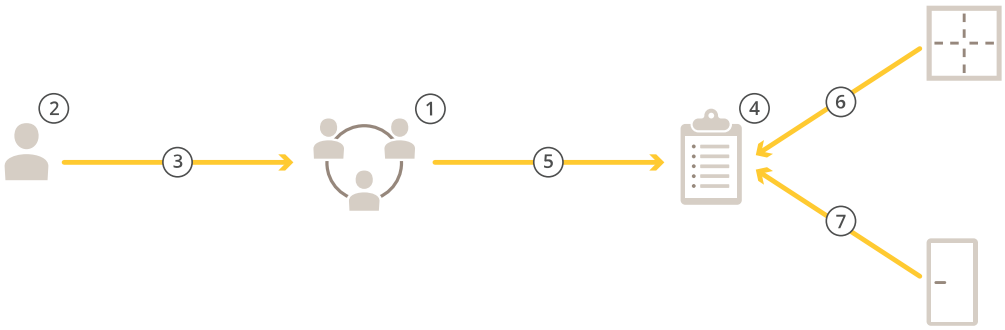
# Gestione degli accessi

Utilizzare la scheda **Access management (Gestione degli accessi)** per configurare e gestire i titolari di tessere, i gruppi e le regole di accesso del sistema.

Per un flusso di lavoro completo per l'impostazione di un network door controller Axis in AXIS Camera Station Pro, vedere *Imposta un network door controller Axis*.

## Flusso di lavoro di gestione degli accessi

La struttura di gestione degli accessi è flessibile per cui è possibile sviluppare un flusso di lavoro più adatto alle proprie esigenze. Esempio di flusso di lavoro:




1. *Aggiungi un gruppo, on page 191.*
2. *Aggiungi un titolare tessera, on page 186.*
3. Aggiunta di titolari di tessera ai gruppi.
4. *Aggiungi una regola di accesso, on page 191.*
5. Applicazione di gruppi alle regole di accesso.
6. Applicare le zone alle regole di accesso.
7. Applicare le porte alle regole di accesso.

## Aggiungi un titolare tessera

Il titolare della tessera è una persona con un ID univoco registrato nel sistema. Configurare un titolare di tessera con le credenziali che identificano la persona e definire quando e come può avere accesso alle porte.

È possibile anche mappare gli utenti in un database di Active Directory come titolari di tessera. Vedere *Impostazioni di Active Directory*[BETA], *on page 173.*

1. Aprire una scheda di gestione degli accessi .
2. Andare a **Cardholder management (Gestione titolari tessere)** > **Cardholders (Titolari di tessere)** e fare clic su **Add (Aggiungi)**.
3. Inserire il nome e il cognome del titolare di tessera. Facoltativamente, è possibile aggiungere ulteriori dettagli al titolare della tessera:
   - In **Email**, inserire l'indirizzo e-mail del titolare della tessera.
   - In **Groups (Gruppi)**, selezionare i gruppi a cui si desidera aggiungere il titolare della tessera.
   - In **Access rules (Regole di accesso)**, selezionare le regole di accesso che si desidera applicare al titolare della tessera.
4. Per aggiungere una foto, cliccare su **Cardholder picture (Foto del titolare della tessera)** e selezionare:
   - **Upload (Caricare)** per aggiungere un'immagine dal proprio dispositivo.

– **Capture (Acquisire)** per scattare una foto direttamente con la fotocamera.

Nota

L'immagine deve essere un file JPG, PNG o GIF. Le immagini vengono ridimensionate automaticamente a un massimo di 700x700 pixel e convertite in formato JPG.

5. Cliccare su **Advanced (Avanzate)** per configurare le opzioni supplementari.
6. Aggiungere una credenziale al titolare di tessere. Vedere *Aggiungi credenziali, on page 188*.
7. Fare clic su **Save (Salva)**.
8. Per stampare i badge, selezionare uno o più titolari di tessera e fare clic su **Stampa badge**BETA. Per ulteriori informazioni vedere *Print badge (Stampa badge) BETA, on page 197*.

Utilizzare il campo di ricerca per trovare un titolare di tessera in base al nome o al cognome. Per filtrare in base alle fonti, fare clic su **Filter (Filtra)** e selezionare **Local (Locale)**, **Global (Globale)**, **AD** o **Center (Centro)**.

| **Avanzata** | |
|---|---|
| **Tempo di accesso lungo** | Selezionare per attribuire al titolare della tessera un tempo di accesso lungo e un tempo di apertura troppo a lungo quando c'è un monitor porta installato. |
| **Sospendi titolare tessera** | Selezionare per eseguire la sospensione del titolare tessera. Questo rimuove temporaneamente tutti gli accessi dal titolare di tessera. |
| **Allow double-swipe (Consenti doppia passata)** | Selezionare per consentire a un titolare di tessere di ignorare lo stato corrente di una porta. Ad esempio, il titolare della tessera ha la possibilità di usarla per lo sblocco di una porta al di fuori della pianificazione normale. |
| **Esente da blocco** | Selezionare questa opzione per consentire al titolare della tessera l'accesso durante la chiusura totale. |
| **Exempt from anti-passback (Esente da anti-passback)** | Selezionare per dare al titolare della carta un'esenzione dalla regola anti-passback. L'anti-passback fa sì che le persone non possano impiegare le stesse credenziali di qualcuno entrato in un'area prima di loro. La prima persona deve uscire dall'area prima che le sue credenziali possano essere riutilizzate. |
| **Titolare di tessera globale** | Selezionare questa opzione per consentire la visualizzazione e il monitoraggio del titolare della tessera sui server secondari. Questa opzione è a disposizione solo per i titolari di tessere creati sul server principale. Vedere *Multi-server BETA, on page 171*. |

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

*Aggiunta di titolari di tessera e gruppi*

## Aggiungi credenziali

È possibile aggiungere i seguenti tipi di credenziali al titolare della tessera:

- *Credenziali con codici QR, on page 188*
- *Credenziali PIN, on page 188*
- *Credenziali su dispositivi mobili, on page 189*
- *Credenziali tessera, on page 189*
- *Credenziali targa, on page 190*

| Data di scadenza | |
|---|---|
| **Valido da** | Impostare una data e un'ora il cui le credenziali diventano valide. |
| **Valido fino a** | Selezionare un'opzione dal menu a discesa. |

| Valido fino a | |
|---|---|
| **Nessuna data di fine** | Le credenziali non hanno scadenza. |
| **Data** | Impostare una data e un'ora di scadenza delle credenziali. |
| **Dal primo utilizzo** | Selezionare l'intervallo di scadenza delle credenziali, a partire dal primo utilizzo. Selezionare giorni, mesi, anni o numero di volte dopo il primo utilizzo. |
| **Dall'ultimo utilizzo** | Selezionare il periodo di validità prima della scadenza delle credenziali, a partire dall'ultimo utilizzo. Selezionare giorni, mesi o anni dopo l'ultimo utilizzo. |

### Credenziali con codici QR

Nota

L'impiego di codici QR come credenziali richiede la sincronizzazione tra l'orario sul controller di sistema e la telecamera con AXIS Barcode Reader. Si consiglia di utilizzare la stessa fonte di sincronizzazione per entrambi i dispositivi, in modo da mantenere l'ora sincronizzata.

Per aggiungere un codice QR come credenziale di un titolare di tessere:

1. In **Credentials (Credenziali)**, + fare clic su **Add (Aggiungi)** e selezionare **QR-code (Codice QR)**.
2. Inserire un nome per le credenziali.
3. Dynamic QR è attivo per impostazione predefinita. È necessario utilizzarlo con credenziali PIN.
4. Impostare la data di inizio e di fine delle credenziali.
5. Per inviare per e-mail in automatico il codice QR dopo aver salvato il titolare di tessera, seleziona **Send QR code to cardholder when credential is saved** (Invia codice QR al titolare di tessera quando le credenziali vengono salvate).
6. Fare clic su **Aggiungi**.

### Credenziali PIN

Per aggiungere un PIN come credenziale di un titolare di tessere:

1. In **Credentials (Credenziali)**, fare clic su + **+Add (+ Aggiungi)** e selezionare **Card (Badge)**.
2. Immettere un PIN.

3. In alternativa, per attivare un allarme silenzioso con un PIN separato, attivare l'opzione **Duress PIN** (PIN di emergenza) e inserire un PIN di emergenza.
4. Impostare le date **Valid from** (Valido da) e **Valid to** (Valido fino al) per le credenziali.
5. Fare clic su **Aggiungi**.

**Credenziali su dispositivi mobili**

Nota

Il titolare tessera deve disporre di un indirizzo e-mail per ricevere le credenziali mobili.

Per aggiungere un telefono cellulare come credenziali di un titolare di tessere:

1. In **Credentials (Credenziali)**, fare clic su + **+Add (+ Aggiungi)** e selezionare **Mobile credential (Credenziali telefono cellulare)**.
2. Inserire un nome per le credenziali.
3. Impostare la data di inizio e di fine delle credenziali.
4. Selezionare **Send the mobile credential to the cardholder after saving (Invia le credenziali mobili al titolare della tessera dopo il salvataggio)**. Il titolare della tessera riceve un messaggio e-mail con le istruzioni per eseguire l'associazione.
5. Fare clic su **Aggiungi**.

Per un esempio, vedere *Utilizzare l'app AXIS Mobile Credential come credenziali Bluetooth, on page 161*.

**Credenziali tessera**

Per aggiungere un badge come credenziale di un titolare di tessere:

1. In **Credentials (Credenziali)**, fare clic su + **+Add (+ Aggiungi)** e selezionare **Card (Badge)**.
2. Immettere il nome credenziale.
3. Selezionare il tipo di tessera:
   - **Card (Tessera):** utilizzare per le tessere standard, non crittografate.
   - **Encrypted card (Tessera crittografata):** utilizzare per le tessere che utilizzano una comunicazione crittografata. Questa opzione richiede un lettore SSCP con configurazione per supportare le tessere crittografate.
4. Se è stato selezionato **Cart (Tessera)**, inserire il codice della tessera e la lunghezza in bit, oppure recupera automaticamente i dati della tessera:
   4.1. Selezionare una porta dall'elenco **Select reader (Seleziona lettore)**.
   4.2. Passare la tessera sul lettore connesso a tale porta.
   4.3. Fare clic su **Get last swiped card data from the door's readers (Acquisisci i dati dell'ultima tessera strisciata dai lettori della porta)**.

Nota

- La lunghezza dei bit è configurabile solo quando si crea un formato tessera con una specifica lunghezza di bit non ancora definita nel sistema.
- Per acquisire i dati della tessera, hai la possibilità di usare un lettore di tessere USB desktop 2N. Se necessiti di maggiori informazioni, consulta *Configurazione del lettore di tessere USB desktop 2N*.

5. Se è stato selezionato **Encrypted Card (Tessera crittografata)**, crittografare la tessera utilizzando un lettore USB:
   5.1. Selezionare il lettore USB dall'elenco **USB reader (Lettore USB)**.
   5.2. Appoggiare la tessera sul lettore. Il pannello mostra **Card identified. Hold still for encryption (Tessera identificata. Tenerla ferma per la crittografia).**
   5.3. Selezionare **Encrypt card (Crittografa tessera)**. Non rimuovere la tessera mentre sul pannello è visualizzato il messaggio **Writing card data (Scrittura dati tessera)**.

5.4. Quando il pannello visualizza il messaggio " **Card encrypted successfully (Tessera crittografata con successo)**, il numero crittografato e l'UID della tessera verranno compilati automaticamente.

6. Inserire un codice struttura. Questo campo è disponibile solo se il **Facility code (Codice struttura)** è stato abilitato in **Access management > Settings (Gestione degli accessi, Impostazioni)**.
7. Impostare la data di inizio e di fine delle credenziali.
8. Fare clic su **Aggiungi**.

**Credenziali targa**

Per aggiungere una targa come credenziale di un titolare di tessere:

1. In **Credentials (Credenziali)**, fare clic su **+Add (+ Aggiungi)** e selezionare **License plate (Targa)**.
2. Inserire un nome credenziali che descriva il veicolo.
3. Inserisci il numero targa del veicolo.
4. Impostare la data di inizio e di fine delle credenziali.
5. Fare clic su **Aggiungi**.

**Usare il numero di targa come credenziale**

Questo esempio illustra il modo di impiegare un door controller, una telecamera dotata di AXIS License Plate Verifier e il numero targa di un veicolo come credenziali per concedere l'accesso.

1. Aggiungere il door controller e la telecamera a AXIS Camera Station Pro. Vedere *Aggiunta di dispositivi*.
2. Aggiorna il firmware sui nuovi dispositivi alla versione più recente a disposizione. Vedere *Aggiornamento del firmware*.
3. Aggiungi una nuova porta connessa al tuo door controller. Vedere *Aggiunta di una porta, on page 150*.
   3.1. Aggiungi un lettore su **Side A (Lato A)**. Vedere *Aggiungere un formato di un lettore tessera, on page 159*.
   3.2. In **Door settings (Impostazioni porta)**, seleziona **AXIS License Plate Verifier** come **Reader type (Tipo lettore)** e inserisci un nome per il lettore.
   3.3. In via facoltativa, aggiungi un lettore o un dispositivo REX su **Side B (Lato B)**.
   3.4. Fare clic su **OK**.
4. Installare e attivare AXIS License Plate Verifier sulla tua telecamera. Vedi il manuale per l'utente *AXIS License Plate Verifier*.
5. Avvia AXIS License Plate Verifier.
6. Configura AXIS License Plate Verifier.
   6.1. Andare a **Configuration > Access control > Encrypted communication (Configurazione > Controllo degli accessi > Comunicazione crittografata)**.
   6.2. In **External Peripheral Authentication Key (Chiave di autenticazione dispositivo periferico esterno)**, fare clic su **Show authentication key (Mostra chiave di autenticazione)** e **Copy key (Copia chiave)**.
   6.3. Apri AXIS License Plate Verifier dall'interfaccia Web della telecamera.
   6.4. Salta la procedura guidata di impostazione.
   6.5. Andare a **Settings (Impostazioni)**.
   6.6. In **Access control (Controllo degli accessi)**, seleziona **Secure Entry** come **Type (Tipo)**.
   6.7. In **IP address (Indirizzo IP)**, immetti l'indirizzo IP e le credenziali per il door controller.
   6.8. In **Authentication key (Chiave di autenticazione)**, incollare la chiave di autenticazione copiata in precedenza.
   6.9. Fare clic su **Connetti**.

6.10. In **Door controller name (Nome door controller)**, seleziona il door controller.

6.11. In **Reader name (Nome lettore)**, seleziona il lettore che hai aggiunto in precedenza.

6.12. Attiva l'integrazione.

7. Aggiungere il titolare della carta a cui si desidera concedere l'accesso. Vedere *Aggiungi un titolare tessera, on page 186*
8. Eseguire l'aggiunta di credenziali targa al nuovo titolare tessera. Vedere *Aggiungi credenziali, on page 188*
9. Aggiungi una regola di accesso. Vedere *Aggiungi una regola di accesso, on page 191*.

   9.1. Aggiungere una pianificazione.

   9.2. Aggiungere il titolare tessera a cui vuoi concedere l'accesso tramite targa.

   9.3. Aggiungi la porta con il lettore AXIS License Plate Verifier.

## Aggiungi un gruppo

I gruppi consentono di effettuare la gestione aggregata dei titolari di tessere e delle relative regole di accesso.

1. Aprire una scheda di gestione degli accessi .
2. Andare a **Cardholder management (Gestione titolari tessere)** > **Groups (Gruppi)** e fare clic su **Add (Aggiungi)**.
3. Inserire un nome e, facoltativamente, le iniziali del gruppo.
4. Selezionare **Global group (Gruppo globale)** per visualizzare e monitorare i titolari delle carte sui server secondari. Questa opzione è a disposizione solo per i titolari di tessere creati sul server principale. Vedere *Multi-server BETA, on page 171*.
5. Aggiungere i titolari di tessere al gruppo:

   5.1. Fare clic su **Add** (Aggiungi).

   5.2. Selezionare i titolari di tessere che si desidera aggiungere e fare clic su **Add (Aggiungi)**.
6. Fare clic su **Save (Salva)**.
7. Per stampare i badge di tutti i titolari di tessera di un gruppo, seleziona il gruppo e fai clic su **Print Badge (Stampa badge)**BETA. Per ulteriori informazioni, consultare *Print badge (Stampa badge) BETA, on page 197*.

## Aggiungi una regola di accesso

Una regola di accesso definisce le condizioni che devono essere soddisfatte per consentire l'accesso.

Una regola di accesso è composta da:

**Titolari tessera e gruppi titolari tessere –** a chi concedere l'accesso.

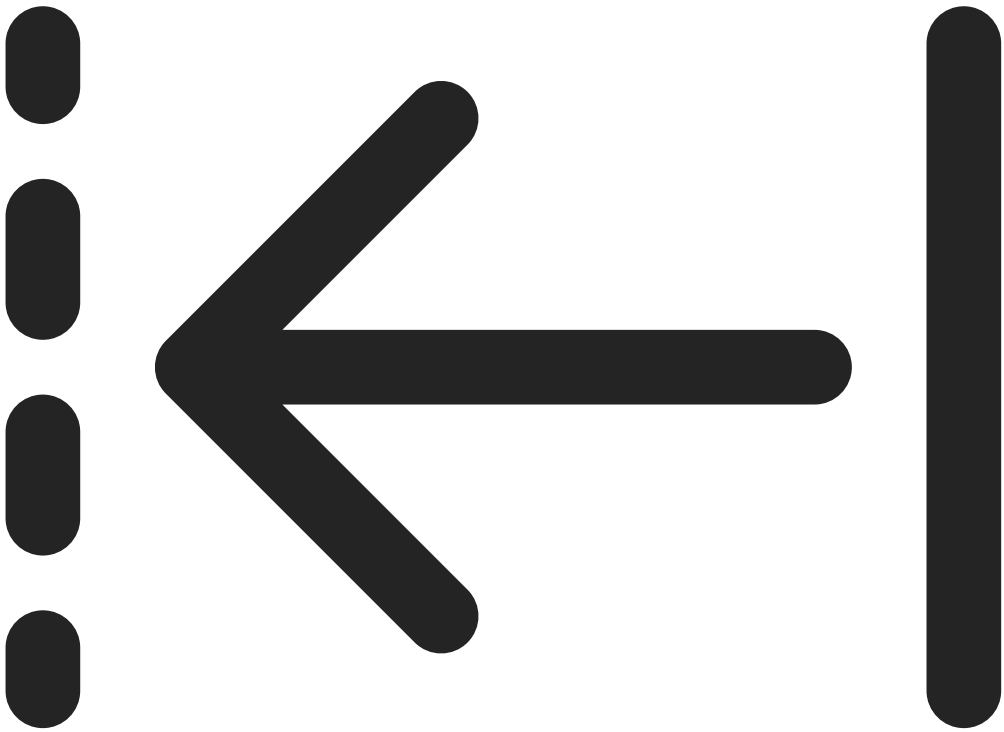
**Porte e zone –** dove si applica l'accesso.

**Pianificazioni –** quando concedere l'accesso.

Per aggiungere una regola di accesso:

1. Aprire una scheda di gestione degli accessi .
2. Andare in **Cardholder management (Gestione titolari tessere)**.

3. In **Access rules (Regole di accesso)**



, fare clic su + **Add (Aggiungi)**.

4. Immettere un nome per la regola di accesso e fare clic su **Next (Avanti)**.
5. Configurazione dei titolari e dei gruppi:
   5.1. In **Cardholders (Titolari di tessera)** o **Groups (Gruppi)**, fare clic su + **Add (Aggiungi)**.
   5.2. Selezionare i titolari di tessera o i gruppi e fare clic su **Add (Aggiungi)**.
   5.3. È inoltre possibile trascinare e rilasciare un titolare di tessera o un gruppo direttamente su una regola di accesso per applicarla. Durante il trascinamento, vengono evidenziate le regole di accesso su cui è possibile rilasciare gli elementi. Se si trascinano più titolari di tessera o gruppi contemporaneamente, un conteggio indica quanti se ne stanno spostando.
6. Configurazione di porte e zone:
   6.1. In **Doors (Porte)** o **Zones (Zone)**, fare clic su + **Add (Aggiungi)**.
   6.2. Selezionare le porte o le zone e fare clic su **Add (Aggiungi)**.
7. Configurazione delle pianificazioni:
   7.1. In **Schedules (Pianificazioni)**, fare clic su + **Add (Aggiungi)**.

7.2. Selezionare uno o più programmi e fare clic su **Add (Aggiungi)**.

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

Una regola di accesso priva di uno o più dei componenti descritti sopra è incompleta. È possibile visualizzare tutte le regole di accesso incomplete nella scheda **Incomplete**.

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

## Esportazione dei report sulla configurazione del sistema

È possibile esportare report contenenti diversi tipi di informazioni sul sistema. AXIS Camera Station Pro esporta i report come file CSV (comma-separated value) e lo salva nella cartella di download predefinita. Per esportare un report:

1. Aprire una scheda di gestione degli accessi .
2. Andare in **Reports** > **System configuration (Configurazione del sistema)**.
3. Selezionare i rapporti da esportare e fare clic su **Download**.

| | |
|---|---|
| **Report di dettagli titolari tessera** | Include informazioni sui titolari di tessera, sulle credenziali, sulla convalida della tessera e sull'ultima transazione. |
| **Report di accesso titolari tessera** | Include le informazioni relative al titolare di tessera e le informazioni su gruppi titolari di tessera, regole di accesso, porte e zone correlate al titolare di tessera. |
| **Report di accesso gruppo titolari di tessera** | Include il nome del gruppo titolare di tessera e le informazioni su titolari di tessera, regole di accesso, porte e zone correlate al gruppo titolare di tessera. |
| **Report di regola di accesso** | comprende il nome della regola di accesso e informazioni su titolari di tessera, gruppi titolari di tessera, porte e zone correlate alla regola di accesso. |
| **Report di accesso porta** | comprende il nome della porta e informazioni su titolari di tessera, gruppi titolari di tessera, regole di accesso e zone correlate alla porta. |
| **Report di accesso zone** | comprende il nome della zona e informazioni su titolari di tessera, gruppi titolari di tessera, regole di accesso e porte correlate alla zona. |

## Crea report sull'attività dei titolari di tessere

Un report appelli elenca i titolari di tessere all'interno di una zona specifica, aiutando a identificare chi è presente in un determinato momento.

Un rapporto raduno elenca i titolari di carta all'interno di una zona specifica, aiutando a identificare chi è al sicuro e chi manca durante le emergenze. Aiuta i responsabili della gestione degli edifici a determinare l'ubicazione del personale e dei visitatori dopo le evacuazioni. Un punto di raccolta è un luogo prestabilito dove il personale deve presentarsi in caso di emergenza. Il sistema genera un report delle persone presenti e assenti dal sito. Il sistema segnala i titolari di tessera come dispersi finché non si presentano a un punto di raccolta o finché qualcuno non li segnala manualmente come al sicuro.

Sia i rapporti di appello che quelli di raduno richiedono che le zone tengano traccia dei titolari di tessera.

Per creare ed eseguire un report appello o raduno:

1. Aprire una scheda di gestione degli accessi .
2. Andare in **Reports** > **Cardholder activity (Attività titolari tessera)**.
3. Fare clic su **Add (Aggiungi)** e selezionare **Roll call / Mustering (Appello presenti)**.
4. Immettere un nome per il report.
5. Selezionare le zone da includere nel report.
6. Selezionare i gruppi che si desidera includere nel report.
7. Se si desidera un report di raduno, selezionare **Mustering point (Punto di raduno)** e un lettore.
8. Selezionare un intervallo temporale per il report.
9. Fare clic su **Save (Salva)**.
10. Selezionare il report e fare clic su **Run (Esegui)**.

| Stato del report appello | Descrizione |
|---|---|
| **Presente** | Il titolare della tessera è entrato nella zona specificata e non è uscito prima della compilazione del report. |
| **Non presente** | Il titolare della tessera è uscita dalla zona specificata e non è rientrato prima della compilazione del report. |

| Stato del report raduno | Descrizione |
|---|---|
| **Al sicuro** | Il titolare ha strisciato il proprio badge presso il punto di raduno. |
| **Mancante** | Il titolare non ha strisciato il proprio badge presso il punto di raduno. |

## Importa ed esporta

### Importa titolari della tessera

Questa opzione importa i titolari di tessera, i gruppi, le credenziali e le foto da un file CSV. Per importare le foto dei titolari della tessera, assicurarsi che il server abbia accesso alle foto.

Quando importi i titolari tessera, il sistema di gestione degli accessi salva in automatico la configurazione del sistema, inclusa tutta la configurazione hardware, ed elimina qualsiasi configurazione salvata in precedenza.

È possibile anche mappare gli utenti in un database di Active Directory come titolari di tessera. Vedere *Impostazioni di Active Directory*[BETA], *on page 173*.

| Opzione di importazione | |
|---|---|
| **Nuovo** | Rimuove i titolari di tessere esistenti e aggiunge nuovi titolari. |
| **Aggiorna** | Aggiorna i titolari di tessere esistenti e aggiunge nuovi titolari di tessere. |
| **Aggiungi** | Mantiene i titolari di tessere esistenti e aggiunge nuovi titolari. I codici carta e gli ID titolare tessera sono univoci e si possono usare una sola volta. |

1. Nella scheda **Access management (Gestione accessi)**, fare clic su **Import and export (Importazione ed esportazione)**.
2. Fare clic su **Import cardholders (Importa titolari di tessera)**.
3. Selezionare **New (Nuovo)**, **Update (Aggiorna)** o **Add (Aggiungi)**.
4. Fare clic su **Next (Avanti)**.
5. Fare clic su **Choose a file (Scegli un file)**, individuare la posizione del file CSV e fare clic su **Open (Apri)**.
6. Immettere un delimitatore di colonna e selezionare un identificatore univoco e fare clic su **Next (Avanti)**.
7. Assegnare un'intestazione a ogni colonna.
8. Fare clic su **Import (Importa)**.

| Impostazioni importazione | |
|---|---|
| **Prima riga è intestazione** | Specificare se il file CSV contiene un'intestazione colonna. |
| **Delimitatore colonna** | Inserire una formattazione delimitatore di colonna per il file CSV. |
| **Identificatore univoco** | Il sistema usa **Cardholder ID (ID titolare tessera)** per riconoscere il titolare tessera per impostazione predefinita. Puoi anche usare il nome e il cognome o l'indirizzo e-mail. Utilizzare questa opzione per evitare l'importazione di record del personale duplicati. |
| **Formato numero di tessera** | **Allow both hexadecimal and number (Consenti sia valori esadecimali che numeri)** è selezionata per impostazione predefinita. |

## Esporta titolari di tessera

Questa opzione esporta i dati di titolari di tessera nel sistema in un file CSV.

1. Nella scheda **Access management (Gestione accessi)**, fare clic su **Import and export (Importazione ed esportazione)**.
2. Fare clic su **Export cardholders (Esporta i titolari di tessera)**.
3. Scegliere una posizione per il download e fare clic su **Save (Salva)**.

AXIS Camera Station Pro aggiorna le foto dei titolari di tessera in `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos` ogni volta che si modifica la configurazione.

### Undo import (Annulla importazione)

Il sistema salva in automatico la configurazione quando importi i titolari tessera. L'opzione **Undo import (Annulla importazione)** reimposta i dati dei titolari di tessera e tutte le configurazioni hardware allo stato precedente all'ultima importazione.

1. Nella scheda **Access management (Gestione accessi)**, fare clic su **Import and export (Importazione ed esportazione)**.
2. Fare clic su **Undo import (Annulla importazione)**.
3. Fare clic su **Sì**.

## Impostazioni di gestione degli accessi

Per personalizzare i campi del titolare della tessera utilizzati nel dashboard di gestione degli accessi:

1. Nella scheda **Access management (Gestione accessi)**, fare clic su **Settings (Impostazioni)** > **Custom cardholder fields (Campi personalizzati titolari tessere)**.
2. Fare clic su + **Add (Aggiungi)** e digitare un nome. Si possono aggiungere fino a 6 campi personalizzati.
3. Fare clic su **Aggiungi**.

Per usare il codice struttura per verificare il sistema di controllo degli accessi:

1. Nella scheda **Access management (Gestione accessi)**, fare clic su **Settings (Impostazioni)** > **Facility code (Codice struttura)**.
2. Selezionare **Facility code on (Codice struttura attivo)**.

Nota

È anche necessario selezionare **Include facility code for card validation (Includi codice struttura per convalida tessera)** quando si configurano i profili di identificazione. Vedere *Profili di identificazione, on page 165*.

Per modificare un modello di e-mail per l'invio di credenziali QR o mobili:

1. Nella scheda **Access management (Gestione accessi)**, fare clic su **Settings (Impostazioni)** > **Email templates (Modelli email)**.
2. Modificare il proprio modello e fare clic su **Update (Aggiorna)**.

### Modelli di badge BETA

È possibile personalizzare i modelli di badge con le informazioni del titolare della tessera, foto, loghi e marchi personalizzati. Per creare un nuovo modello:

1. Andare ad **Access management > Settings > Badge templates** BETA (Gestione degli accessi, Impostazioni, Modelli badge, BETA).
2. Fare clic su **Create new template (Crea nuovo modello)**.
3. Immettere un nome nel campo **Template name (Nome modello)**.
4. Selezionare **Use as default template for printing (Utilizza come modello predefinito per la stampa)** se si desidera impostare il modello come predefinito.
5. Personalizzare il design del badge:
   - Selezionare fino a cinque campi di testo da visualizzare sul lato anteriore, compresi eventuali campi personalizzati che sono stati creati. Durante la stampa, sul badge compaiono solo i campi compilati.
   - Scegliere il carattere e il colore del testo.
   - Aggiungere un colore o un'immagine di sfondo.
   - Caricare un logo della propria organizzazione.

- Sul retro, aggiungere un colore di sfondo o un'immagine.

6. Fare clic su **Save (Salva)** per salvare le modifiche, oppure su **Save as (Salva come)** per salvare come un nuovo modello.

Nota

Una volta creato, il modello non può subire modifiche, può essere solo rinominato.

**Print badge (Stampa badge)** BETA

È possibile stampare badge di identificazione per i titolari di tessere utilizzando i modelli di badge configurati. Al momento il codificatore schede non è supportato. Prima di iniziare:

- Verificare che il titolare della tessera disponga di almeno una credenziale della tessera. Non è possibile stampare badge per i titolari di tessere senza credenziali.
- È necessaria una stampante che supporti il formato CR80 e materiali di stampa compatibili, come del cartoncino spesso.
- Configurare le impostazioni di stampa del browser:
  1. Configurare le impostazioni pagina su CR80 o su un formato personalizzato che corrisponda alla dimensione della tessera.
  2. Impostare l'orientamento su verticale.
  3. Disattivare i margini o impostarli al minimo.

Importante

Secure Entry funziona con le stampanti dotate di driver Windows. È stato verificato che le stampanti della serie HID Fargo funzionino correttamente. Se è necessario un driver per la stampante, contattare il fornitore della stampante.

Per stampare i badge:

1. Andare a **Access management > Cardholder management > Cardholders** (Gestione degli accessi, Gestione titolari tessera, Titolari tessera).
2. Selezionare uno o più titolari tessera;
3. Fare clic su **Print badge** (Stampa badge) BETA.
4. Fare clic su **Select template (Seleziona modello)** e dall'elenco a discesa **Template (Modello)** selezionare il modello di badge che si desidera utilizzare.
5. Se il titolare tessera dispone di più credenziali, selezionarne una dall'elenco a discesa **Card (Tessera)**.
6. Fare clic su **Print (Stampa)**.

Nota

Se la stampante non supporta la stampa fronte/retro, stampare prima tutti i lati anteriori, quindi capovolgere la pila di cartoncini e reinserirli nel vassoio per stampare i lati posteriori.

## Monitoraggio dell'integrità del sistema BETA

Utilizza la scheda Monitoraggio dello stato del sistema per monitorare i dati relativi allo stato di uno o più AXIS Camera Station Pro sistemi presenti sulla stessa rete.

Se si gestiscono sistemi che si trovano su reti diverse, il monitoraggio server in My Systems mette a disposizione la stessa funzionalità, ma tramite cloud.

| | |
|---|---|
| | mostra un riepilogo dei dispositivi e dei sistemi ai quali puoi accedere. Vedere *Magazzino, on page 198*. |
| | Mostra un riepilogo dell'archiviazione e i dettagli di registrazione di ogni telecamera dai sistemi monitorati. Vedere *Magazzino, on page 199*. |
| | mostra i registri di System Health Monitoring dei sistemi monitorati. Vedere *Notifiche, on page 200*. |

### Limiti

- Non è possibile monitorare lo spazio di archiviazione per le registrazioni sulle serie di unità di registrazione AXIS S30 e S40.
- Le impostazioni di notifica influiscono unicamente sul server di System Health Monitoring locale.
- Il sistema contrassegna le registrazioni il cui tipo è **None (Nessuno)** ad eccezione delle registrazioni continue e di quelle attivate da movimento.

### Flusso di lavoro

1. *Configura Monitoraggio dell'integrità del sistema BETA, on page 176*
   1.1. Configurazione delle notifiche. Vedere *Notifiche, on page 176*.
   1.2. Configura multisistema. Vedere *Multisystem, on page 177*.
2. Eseguire il monitoraggio dei dati relativi all'integrità dai sistemi AXIS Camera Station Pro.
   2.1. *Magazzino, on page 198*
   2.2. *Magazzino, on page 199*
   2.3. *Notifiche, on page 200*

### Magazzino

La pagina Magazzino illustra un riepilogo dei dispositivi e dei sistemi ai quali è possibile accedere.

1. Nella scheda **System Health Monitoring (Monitoraggio dell'integrità del sistema)** BETA, fare clic su .
2. Per visualizzare un riepilogo di un sistema, fare clic su **AXIS Camera Station**.
   Il pannello di destra mostra dettagli del sistema e del server.
3. Per visualizzare il riepilogo di un dispositivo in un sistema, fare clic sul dispositivo nell'elenco.
   Il pannello di destra mostra le informazioni relative al dispositivo e allo spazio di archiviazione, qualora il dispositivo contenga una sorgente video.
4. Per scaricare il report di sistema, selezionare **AXIS Camera Station system report (Report di sistema AXIS Camera Station)** dal menu a discesa **Create report (Crea report)**. Vedere *Report del sistema, on page 211*.
5. Per scaricare il report del monitoraggio dell'integrità del sistema:
   5.1. Dal menu a discesa **Create report (Crea report)**, selezionare **System Health Monitoring report (Report monitoraggio stato di salute del sistema)**.

5.2. Per includere il database nel report, selezionare **Include all databases (Includi tutti i database)** e fare clic su **Download**.

5.3. Quando il report è pronto, fai clic per salvarlo.

## Magazzino

La pagina di archiviazione illustra il riepilogo dell'archiviazione e i dettagli di registrazione di ogni telecamera dai sistemi monitorati. Fare clic sull'intestazione di una colonna per ordinare i dati in base a quella colonna.

1. Nella scheda **System Health Monitoring (Monitoraggio dell'integrità del sistema)** BETA, fare clic su .
2. Durante il monitoraggio dei dati relativi all'integrità multisistema, selezionare un sistema dal menu a discesa.

| **Sommario** | |
|---|---|
| Stato | Lo stato dell'archiviazione. Vedere *Configurazione dell'archiviazione, on page 75*. |
| Luogo | Il nome e il percorso dell'archiviazione. |
| Totale | La quantità totale di spazio su archiviazione. Corrisponde alla "Dimensione totale" visualizzata nelle proprietà di Windows relative al punto di archiviazione. |
| Allocato | La quantità massima di spazio di archiviazione assegnata alle registrazioni. |
| Utilizzato | Lo spazio di archiviazione attualmente utilizzato per le registrazioni. |
| Ultimo aggiornamento | Ora dell'ultimo aggiornamento delle informazioni. |

| **Telecamera** | |
|---|---|
| Stato | (vuoto): Stato normale.<br><br>Icona di avviso: Il requisito di conservazione non è soddisfatto.<br><br>Icona informativa: Il periodo di conservazione non è soddisfatta in quanto le registrazioni della telecamera sono troppo brevi. |
| Nome | Il nome della telecamera. |
| Tipo di registrazione | I tipi di registrazione applicati alla telecamera. |
| Imposta conservazione | Il tempo di conservazione configurato per la telecamera in **Configuration > Storage > Selection (Configurazione > Archiviazione > Selezione)**. |
| Conservazione corrente | Il numero di giorni in cui le registrazioni sono in archivio. |
| Registrazione più vecchia | L'ora della registrazione più vecchia della telecamera nell'archiviazione. |
| Ultima registrazione | L'ora della registrazione più recente della telecamera nell'archiviazione. |
| Luogo | Il punto di archiviazione usato dalla telecamera. |
| Spazio di archiviazione utilizzato | Quantità di spazio di archiviazione usata da questa telecamera per le registrazioni. |
| Ultimo aggiornamento | Ora dell'ultimo aggiornamento delle informazioni. |

## Notifiche

La pagina delle notifiche mostra i registri di System Health Monitoring dei sistemi monitorati. Fare clic sull'intestazione di una colonna per ordinare i dati in base a quella colonna.

Nella scheda **System Health Monitoring (Monitoraggio dell'integrità del sistema)** BETA, fare clic su .

| **Cronologia** | |
|---|---|
| Notifica inviata | Ora in cui è stata inviata la notifica. |
| Elemento | Mostra il nome del dispositivo per le notifiche attivate da `device down` o `system` per le notifiche attivate da `system down`. |
| Sistema | Il nome del sistema in cui si è verificato l'evento. |
| Regola | La regola che ha attivato la notifica. `System down` o `Device down` |
| Rilevato | L'ora in cui il problema è stato rilevato. |
| Risolto | L'ora in cui il problema è stato risolto. |

## Tasti di scelta rapida

Nella scheda Tasti di scelta rapida sono mostrati i tasti di scelta rapida disponibili. Il tipo di tasto di scelta rapida dipende dallo strumento con cui si controlla AXIS Camera Station Pro.

- Una combinazione di tasti della tastiera
- Una combinazione di tasti della tastierina
- Un tasto del joystick
- Un tasto del jog dial

Quando una telecamera o una vista viene rimossa da un server collegato, vengono rimossi anche i relativi tasti di scelta rapida.

Il sistema suddivide i tasti di scelta rapida nelle categorie che seguono:

- Telecamera
- Gestione dei dispositivi
- Passa alla telecamera
- Passa alla vista
- Navigazione
- Preimpostazioni PTZ
- Registrazioni
- Sequenze
- Suddivisione dell'immagine
- Tab
- Altro

È necessario eseguire l'assegnazione manuale alle azioni nelle categorie Passa alle telecamere e Passa alle viste.

Nota

- Quando si aggiunge o si modifica un tasto di scelta rapida e il tasto di scelta rapida assegnato è già in uso per un'altra azione, viene visualizzata un'icona di avviso. Muovere il puntatore del mouse sull'icona di avviso per visualizzare l'azione di conflitto. Premere ESC per annullare. Premere ENTER per impiegare il tasto di scelta rapida e rimuovere in automatico il tasto di scelta rapida in conflitto.
- Quando ci si collega a più server, le categorie Passa alle telecamere e Passa alle viste elencano anche le telecamere e le viste sui server connessi.

| | |
|---|---|
| **Assegnare un tasto di scelta rapida** | Se il valore della tastiera di un'azione è vuoto, fare clic sul campo vuoto per aggiungere un tasto di scelta rapida.<br>• Per aggiungere un tasto di scelta rapida con la tastiera, premere Ctrl e almeno un altro tasto o un tasto funzione F2-F12.<br>• Per aggiungere un tasto di scelta rapida con una tastiera, premere una combinazione di testi numerici o premere uno dei tasti funzione (F1-F5).<br>• Per aggiungere un tasto di scelta rapida con un joystick o jog dial, premere il tasto del joystick o jog dial per assegnarlo. |
| **Modifica tasto di scelta rapida** | Fare clic su un valore della tastiera di un'azione per effettuare una modifica. |

| | |
|---|---|
| **Rimuovi un tasto di scelta rapida** | Fare clic sul valore della tastiera di un'azione per rimuoverla. |
| | Fare clic su per stampare la tabella dei tasti di scelta rapida. |
| | Fare clic su per ripristinare tutti i tasti di scelta rapida alle impostazioni originali. |

## Tasti pannello di controllo sorveglianza video

| Mappatura tasti scelta rapida - Joystick | Azione predefinita | AXIS TU9002 | AXIS T8311 |
|---|---|---|---|
| Tasto 1 | Andare a preset 1 | J1 | J1 |
| Tasto 2 | Andare a preset 2 | J2 | J2 |
| Tasto 3 | Andare a preset 3 | J3 | J3 |
| Tasto 4 | Andare a preset 4 | J4 | J4 |
| Tasto 5 | Simulare pulsante sinistro del mouse | J5 | L |
| Tasto 6 | Simulare il pulsante sinistro destro | J6 | R |
| Tasto 7 | Seleziona la cella precedente nella vista suddivisa | In alto a sinistra | - |
| Tasto 8 | Seleziona la cella successiva nella vista suddivisa | In alto a destra | - |
| Tasto 9 | Salta alla registrazione precedente | | - |
| Tasto 10 | Riproduci/Pausa | | - |
| Tasto 11 | Salta alla registrazione successiva | | - |
| Tasto 12 | Aggiunta di un segnalibro | | - |
| Tasto 13 | Alterna zoom digitale e velocità di riproduzione nella funzione ghiera dello zoom | M1 | - |
| Tasto 14 | Passaggio dalle immagini dal vivo alle registrazioni | M2 | - |
| Tasto 15 | Passaggio a fotogramma precedente | In alto a sinistra attivato/disattivato | - |
| Tasto 16 | Passaggio al fotogramma successivo | In alto a destra attivato/disattivato | - |

| Mappatura tasti scelta rapida - tastierino | Azione predefinita | AXIS TU9003 | AXIS T8312 |
|---|---|---|---|
| A | Apri viste | | |
| B | Passare alla telecamera o vista successiva | | |
| ALT+B | Passare alla telecamera o vista precedente | Alt+ | - |
| TABULAZIONE | Passa alla scheda successiva | | - |
| ALT+TAB | Passa alla scheda precedente | Alt+ | - |
| C | - | - | |
| D | - | - | |
| E | - | - | |
| PIÙ | Messa a fuoco più distante | + | - |
| MENO | Messa a fuoco più vicina | - | - |
| F2 | Apri tasti di scelta rapida | F2 | F2 |
| F4 | Apertura dei registri | F4 | F4 |
| F5 | Apri configurazione | F5 | F5 |
| F10 | Messa a fuoco automatica | F10 | - |

| Mappatura tasti scelta rapida: Jog | Azione predefinita | AXIS T8313 |
|---|---|---|
| Jog 1 | Mostrare o nascondere indicatore esportazione. | L |
| Jog 2 | Aggiunta di un segnalibro | |
| Jog 3 | Salta alla registrazione precedente | |
| Jog 4 | Riproduci/Pausa | |
| Jog 5 | Salta alla registrazione successiva | |
| Jog 6 | Passaggio dalle immagini dal vivo alle registrazioni | R |

Nota

AXIS T8311 Video Surveillance Joystick non supporta i pulsanti da 7 a 10 del joystick.

## Registri

Per impostazione predefinita, la scheda **Logs (Registri)** mostra gli eventi e gli allarmi in tempo reale e i registri di controllo. È anche possibile cercare i registri precedenti. È possibile configurare il numero di giorni per la conservazione dei log in **Configuration > Server > settings (Configurazione > Server > Impostazioni)**.

| | |
|---|---|
| **Time (Orario)** | Data e ora dell'azione. |
| **Type (Tipo):** | Il tipo di azione: allarme, evento o controllo. |
| **Categoria** | La categoria dell'azione. |
| **Messaggio** | Breve descrizione dell'azione. |
| **Utente** | L'utente AXIS Camera Station Pro che esegue l'azione. |
| **Computer** | Il computer (nome dominio di Windows) sul quale è installato AXIS Camera Station Pro. Questo valore viene fornito dal cliente e non può essere verificato in modo indipendente dal server. |
| **Utente Windows** | L'utente Windows che amministra AXIS Camera Station Pro. Questo valore viene fornito dal cliente e non può essere verificato in modo indipendente dal server. La colonna Utente mostra l'utente che ha effettuato l'autenticazione. |
| **Server** | Disponibile solo quando ci si collega a più server.<br><br>Il server sul quale si verifica l'azione. |
| **Componente** | Il componente da cui viene generato il registro. |

### Ricerca dei registri

1. Nella scheda **Logs (Registri)** fare clic su **Search (Cerca)** in **Log search (Ricerca nel registro)**.
2. Nella casella del filtro digitare le parole chiave. AXIS Camera Station Pro esegue la ricerca nell'elenco dei log escludendo **Time (Ora)**, e mostra i risultati che contengono tutte le parole chiave. Per operatori di ricerca supportati, vedere *Ottimizzazione della tua ricerca, on page 45*.
3. Scegliere **Alarms (Allarmi)**, **Audits (Controlli)** o **Events (Eventi)** in **Filter (Filtro)**.
4. Selezionare una data o un intervallo di date dal calendario.
5. Selezionare **Start time (Ora inizio)** e **End time (Ora fine)** dai menu a discesa.
6. fare clic su **Cerca**;

### Registro degli allarmi

Il Registro degli **Alarms (Allarmi)** mostra gli allarmi di sistema e quelli generati da regole e rilevamento movimento. L'elenco include la data, l'ora e la categoria dell'allarme e un messaggio di allarme. Vedere *Allarmi*.

| | |
|---|---|
| | Fare clic su un allarme e su per aprire la scheda **Records (Registrazioni)** e avviare la riproduzione quando un allarme contiene una registrazione. |
| | Fare clic su un allarme e su per aprire l'eventuale procedura eventualmente inclusa nell'allarme. |

| | |
|---|---|
| ✔ | Fare clic su un allarme e su ✔ per notificare agli altri client che gli allarmi sono stati gestiti. |
| 💾 | Fare clic su un allarme e su 💾 per eseguire l'esportazione del log in un file di testo. |

### Registro degli eventi

Il Registro **Events (Eventi)** visualizza eventi della telecamera e del server, ad esempio registrazioni, attivazioni, allarmi, errori e messaggi di sistema, in un elenco. L'elenco include la data e l'ora dell'evento, la categoria dell'evento e un messaggio dell'evento. Selezionare gli eventi e fare clic su 💾 nella barra degli strumenti per esportare gli eventi in un file in formato testo.

### Registro di controllo

Nel Registro **Audit (Controllo)** si possono visualizzare tutte le azioni dell'utente, come le registrazioni manuali, i flussi video avviati o arrestati, le regole di azione, le porte create e i titolari di tessera creati. Selezionare i controlli e fare clic su 💾 nella barra degli strumenti per esportarli in un file in formato testo.

## Gestione delle targhe

Per gestire gli elenchi delle targhe in AXIS Camera Station Pro, aprire la scheda **Gestione targhe**.

In questa scheda è possibile modificare tre elenchi di targhe per singole telecamere o gruppi di telecamere:

1. Seleziona un gruppo o una telecamera dagli elenchi **Groups (Gruppi)** e **Cameras (Telecamere)**.
2. Selezionare quale elenco modificare. Per impostazione predefinita, i tre elenchi che possono essere modificati sono denominati **Allow list (Elenco autorizzati)**, **Block List (Elenco bloccati)** o **Custom List (Elenco personalizzato)**.
3. Apportare modifiche all'elenco:
   - Per modificare il nome dell'elenco, fare clic su **Edit list name (Modifica nome elenco)**.
   - Per aggiungere una nuova targa, inserire il numero di targa nella colonna Targa e, se lo si desidera, una descrizione nella colonna Descrizione. Fare clic su **Aggiungi**.
   - Per modificare o rimuovere una targa esistente, selezionarla e fare clic su **Edit (Modifica)** o **Remove (Rimuovi)**.
   - Per importare un elenco di targhe da un file CSV, fare clic su **Import (Importa)** e selezionare il file. Questa operazione sovrascriverà l'elenco attuale, quindi esportarlo prima se si desidera conservarne una copia.
   - Per esportare un elenco di targhe in un file CSV, fare clic su **Export (Esporta)**.
4. Fare clic su **Apply (Applica)** per salvare le modifiche.

Nota

Una volta applicate le modifiche, AXIS Camera Station Pro si occuperà della gestione degli elenchi delle targhe per quel gruppo o quella telecamera. Ogni notte, aggiorniamo la telecamera in base agli elenchi salvati in AXIS Camera Station Pro, il che comporta la sovrascrittura di eventuali targhe memorizzate direttamente sulla telecamera.

## AXIS Audio Manager Pro

Utilizzare la scheda **AXIS Audio Manager Pro** per accedere all'interfaccia del server AXIS Audio Manager Pro direttamente dall'indirizzo AXIS Camera Station Pro. Per ulteriori informazioni sull'interfaccia server, consultare *AXIS Audio Manager Pro - Manuale per l'utente.*

La scheda viene visualizzata solo dopo essersi connessi a un server AXIS Audio Manager Pro in AXIS Camera Station Pro. Per ulteriori informazioni, consultare *Configurare AXIS Audio Manager Pro, on page 173*.

Importante

Non è possibile accedere all'interfaccia server di AXIS Audio Manager Pro con Secure Remote Access v2.

L'integrazione permette inoltre di:

- *Creare trigger AXIS Audio Manager, on page 103*.
- *Creare azioni per AXIS Audio Manager, on page 113*.
- Aggiungere zone audio alle mappe. Vedere *Mappa, on page 22*.
- *Utilizzare le interfacce di paging nella suddivisione dell'immagine, on page 21*.
- Impostare i privilegi utente relativi ad AXIS Audio Manager Pro in AXIS Camera Station Pro. Vedere *Privilegi utente o di gruppo, on page 138*.
- Selezionare i dispositivi Audio dal server AXIS Audio Manager Pro come dispositivi Audio associati a una telecamera. Vedere *Modifica profili di streaming, on page 55*.

## Allarmi

La scheda Allarmi è disponibile nella parte inferiore del client AXIS Camera Station Pro e mostra gli eventi attivati e gli allarmi di sistema. Per informazioni su come creare allarmi, vedere *Regole di azione*. Per informazioni sull'allarme "È necessaria la manutenzione del database", vedere *Manutenzione database, on page 228*.

| | |
|---|---|
| **Time (Orario)** | l'ora alla quale si è verificato l'allarme. |
| **Categoria** | La categoria dell'allarme attivato. |
| **Descrizione** | Una breve descrizione dell'allarme. |
| **Server** | Disponibile quando ci si connette a più server. Il server AXIS Camera Station Pro che invia l'allarme. |
| **Componente** | il componente che attiva l'allarme. |
| | Illustra una procedura di allarme. Disponibile solo quando l'allarme contiene una procedura di allarme. |
| | Andare alle registrazioni. Disponibile solo quando l'allarme contiene una registrazione. |
| | Confermare l'allarme selezionato |
| | Rimuovere l'allarme. L'allarme viene rimosso solo temporaneamente se non lo si conferma prima. |

Per risolvere un allarme specifico.

1. Fare clic su **Alarms and Tasks (Allarmi e attività)** in fondo al client AXIS Camera Station Pro e aprire la scheda **Tasks (Attività)**.
2. Per allarmi che contengono una registrazione, selezionare l'allarme e fare clic su per andare alla registrazione nella scheda **Recording alerts (Avvisi della registrazione)**.
3. Per allarmi senza registrazione, aprire una scheda con visualizzazione in diretta e fare doppio clic sull'allarme per mostrare la registrazione dell'ora dell'allarme nella scheda **Recording alerts (Avvisi della registrazione)**.
4. Per allarmi che contengono una procedura di allarme, selezionare l'allarme e fare clic su per aprire la procedura di allarme.
5. Per notificare agli altri client che gli allarmi sono stati confermati, selezionare gli allarmi e fare clic su .
6. Per la rimozione degli allarmi dall'elenco, selezionare gli allarmi e fare clic su .

## Attività

La scheda Attività è disponibile nella parte inferiore del client AXIS Camera Station Pro.

Le seguenti attività sono personali e sono visibili soltanto agli amministratori e agli utenti che le hanno avviate:

- Report del sistema
- Crea report dell'incidente
- Esportazione delle registrazioni

Se si è un amministratore, è possibile visualizzare e gestire tutte le attività avviate da qualsiasi utente, comprese le attività personali.

Se si è un operatore o un visualizzatore, è possibile:

- Visualizzare tutte le attività avviate personalmente e le attività non personali avviate da altri utenti.
- Annullare o riprovare le attività avviate. È possibile ritentare solo le attività di report dell'incidente e di esportazione di registrazioni.
- Visualizzare il risultato di tutte le attività nell'elenco.
- Rimuovere tutte le attività finite presenti nell'elenco. Ciò influisce solo sul client locale.

| | |
|---|---|
| **Nome** | Il nome dell'attività. |
| **Avvia** | Indica l'ora in cui l'attività è stata avviata. |
| **Messaggio** | Mostra lo stato o le informazioni relative all'attività.<br><br>Gli stati possibili:<br>• **Canceling (Annullamento in corso)**: Pulizia prima della cancellazione dell'attività.<br>• **Canceled (Annullato)**: La pulizia è completa e l'attività viene annullata.<br>• **Error (Errore)**: L'attività non è andata a buon fine su uno o più dispositivi.<br>• **Finished (Finito)**: Attività completata.<br>• **Finished during lost connection (Terminata durante la perdita di connessione)**: l'attività è stata completata mentre la connessione al server era inattiva. Impossibile determinare lo stato dell'attività.<br>• **Lost Connection (Connessione interrotta)**: il client ha perso la connessione al server mentre l'attività era in esecuzione. Impossibile determinare lo stato dell'attività.<br>• **Running (In esecuzione)**: Attività in esecuzione.<br>• **Pending (In attesa)**: In attesa del completamento di un'altra attività. |
| **Proprietario** | L'utente che ha avviato l'attività. |
| **Avanzamento** | Mostra il progresso dell'attività. |
| **Server** | Disponibile quando ci si connette a più server. Mostra il server AXIS Camera Station Pro che esegue l'attività. |

Per eseguire una o più attività:

1. Fare clic su **Alarms and Tasks (Allarmi e attività)** in fondo al client AXIS Camera Station Pro e fare clic sulla scheda **Tasks (Attività)**.
2. Selezionare le attività e fare clic su una azione

| | |
|---|---|
| | Fare clic per visualizzare la finestra di dialogo dei risultati Attività. |
| | Fare clic per annullare l'attività. |
| | Fare clic per eliminare le attività dall'elenco. |
| | Se l'attività non viene eseguita quando si esportano registrazioni o si creano report dell'incidente, fare clic per ritentare. |

**Risultato attività**

Se un'attività è stata eseguita su più dispositivi, la finestra di dialogo visualizza i risultati per ogni dispositivo. Verificare e effettuare la configurazione manuale di tutte le operazioni non andate a buon fine.

Per la maggior parte delle attività, vengono elencati i seguenti dettagli. Per attività quali **Export recordings (Registrazioni di esportazione)** e **System report (Report di sistema)**, fare doppio clic sull'attività per aprire la cartella con i file salvati.

| | |
|---|---|
| **Indirizzo MAC** | L'indirizzo MAC del dispositivo aggiornato. |
| **Indirizzo** | L'indirizzo IP del dispositivo aggiornato. |
| **Messaggio** | Informazioni sul modo in cui l'attività è stata eseguita:<br>• **Finished (Finita)**: L'attività è stata completata con successo.<br>• **Error (Errore)**: Non è stato possibile completare l'attività sul dispositivo.<br>• **Canceled (Annullata)**: L'attività è stata annullata prima del completamento. |
| **Descrizione** | Informazioni sull'attività. |

A seconda del tipo di attività eseguita, vengono elencati i seguenti dettagli:

| | |
|---|---|
| **Nuovo indirizzo** | Nuovo indirizzo IP assegnato al dispositivo. |
| **Regole di azione** | Versione firmware e nome del dispositivo. |
| **Dettagli** | Numero di serie e indirizzo IP di un dispositivo sostituito e numero di serie e indirizzo IP del nuovo dispositivo. |
| **ID di riferimento** | L'ID di riferimento del report dell'incidente. |

# Genera report

## Foglio di configurazione client

Il foglio di configurazione client serve per la risoluzione di problemi e per contattare l'assistenza.

Per visualizzare una panoramica in formato HTML della configurazione del sistema client:

1. Andare in **Configuration (Configurazione)** > **Server** > **Diagnostics (Diagnostica)**.
2. Fare clic su **View client configuration sheet (Visualizza foglio di configurazione client)**.

## Foglio di configurazione server

Il foglio di configurazione del server include le informazioni sulla configurazione generale, le impostazioni della telecamera incluse le regole di azione, le pianificazioni, l'archiviazione per le registrazioni, i dispositivi ausiliari e le licenze. È utile per la risoluzione dei problemi e per contattare l'assistenza.

Per visualizzare una panoramica in formato HTML della configurazione del sistema del server:

1. Andare in **Configuration (Configurazione)** > **Server** > **Diagnostics (Diagnostica)**.
2. Fare clic su **View server configuration sheet (Visualizza foglio di configurazione server)**.

## Report del sistema

Il report del server è un file .zip che contiene parametri e file di registro che aiutano il supporto tecnico Axis ad analizzare il sistema.

Includere sempre un report di sistema quando si contatta l'assistenza clienti.

Per generare il report di sistema:

1. Andare a ☰ > **Help** > **System report (Guida, Report di sistema)**.
2. Modificare il nome del file se si desidera modificarlo in modo da sostituirlo con uno diverso da quello automatico.
3. Fare clic su **Browse... (Sfoglia)** per selezionare la posizione in cui salvare il report di sistema.
4. Scegli le impostazioni preferite:
   - **Automatically open folder when report is ready (Apri automaticamente cartella quando il report è pronto)** per visualizzarlo subito.
   - **Include all database** (Includi tutti i database) per aggiungere informazioni dettagliate sulle unità di registrazione e sui dati di sistema.
   - **Include screenshots of all monitors (Allega screenshot di tutti i monitor)** per facilitare l'analisi del rapporto di sistema.
5. Fare clic su **OK**.

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

*Generare un report di sistema*

Nota

- Se il server non si avvia, è possibile generare un rapporto di sistema semplificato dalla scheda **Tools (Strumenti)** di AXIS Camera Station Service Control.
- Se il cliente non riesce ad accedere a un server, l'assistenza clienti di Axis potrebbe richiedere i log del client. Sono disponibili in una cartella specifica per la versione del client: `C:\ProgramData\Axis Communications\AXIS Camera Station\Core\Client 6.xx`.
- A seconda del problema, potrebbe essere necessario raccogliere anche i registri degli eventi di Windows. Per farlo, aprire il Visualizzatore eventi, andare a **Windows Logs (Registri di Windows)**, quindi fare clic con il pulsante destro del mouse su **Application (Applicazione)** e selezionare **Save all events as (Salva tutti gli eventi come)**. Procedere allo stesso modo per **System (Sistema)**.

In questi casi, l'assistenza clienti di Axis avrà bisogno anche dei log di sistema standard del server per poter svolgere le indagini.

## AXIS Installation Verifier

AXIS Installation Verifier avvia un test delle prestazioni dopo l'installazione per verificare che tutti i dispositivi nel sistema siano completamente operativi. L'esecuzione del test richiede circa 20 minuti.

| Test | |
|---|---|
| **Normal conditions (Condizioni normali)** | Verificare lo streaming di dati e l'archiviazione di dati con le impostazioni di sistema correnti in AXIS Camera Station Pro. I risultati vengono indicati come superato o non superato. |
| **Condizioni di scarsa illuminazione** | Test del flusso e dell'archiviazione dei dati con impostazioni ottimizzate per le tipiche condizioni di bassa luminosità. I risultati vengono indicati come superato o non superato. |
| **Stress test** | Test che aumentano progressivamente il flusso di dati e lo spazio di archiviazione fino a quando il sistema non raggiunge il proprio limite massimo. I risultati mostrano le prestazioni massime del sistema. |

Nota

- Si possono testare solo dispositivi che supportano AXIS Camera Application Platform 2 (ACAP 2) e versione successiva.
- Durante il test, AXIS Camera Station Pro va in modalità manutenzione e ogni attività di sorveglianza è temporaneamente non disponibile.

Per dare inizio al test:

1. Andare in **Configuration (Configurazione)** > **Server** > **Diagnostics (Diagnostica)**.
2. Fare clic su **(Open AXIS installation verifier...) AXIS Installation Verifier...**
3. Fare clic su **Avvia**.
4. Una volta finito il test, fare clic su **View report (Visualizza report)** per aprire il report oppure su **Save report (Salva report)** per salvarlo.

## Elenco di risorse

È possibile esportare un elenco di risorse per il Video Management System. L'elenco di risorse include il nome, il tipo, il modello, lo stato e il numero di serie di:

- Tutti i server collegati
- Tutti i dispositivi collegati

- Il terminal client da cui si esporta l'elenco di risorse quando ci si connette a più terminali

Per esportare un elenco di risorse:

1. Andare su ☰ > **Other** > **Asset list (> Altro > Elenco di risorse)**.
2. fare clic su **Esporta**.
3. Selezionare la posizione del file e fare clic su **Salva**.
4. In **Latest export (Ultima esportazione)**, appare un link al file o aggiornamenti.
5. Fare clic sul collegamento per andare alla posizione del file.

## Stato dei servizi Axis

Per visualizzare lo stato dei servizi online Axis:

1. Andare in **Configuration (Configurazione)** > **Server** > **Diagnostics (Diagnostica)**.
2. Fare clic su **View status of Axis services (Visualizza stato dei servizi Axis)**.

## Aprire il AXIS Camera Station Pro service control

Il server utilizza il AXIS Camera Station Pro service control per avviare,arrestare e modificare le relative impostazioni. Verrà avviato automaticamente un volta completata l'installazione. Se il computer del server viene riavviato, il controllo del servizio si riavvierà automaticamente entro circa 2 minuti. Un'icona nell'area di notifica di Windows mostra lo stato del servizio.

Fare clic con il pulsante destro del mouse sull'icona e selezionare **Open AXIS Camera Station Service Control (Apri Controllo del servizio AXIS Camera Station)**, **Start Service (Avvia servizio)**, **Stop Service (Arresta servizio)**, **Restart Service (Riavvia servizio)** oppure **Exit (Esci)**.

Per eseguire l'apertura del controllo del servizio dal menu start:

Andare al menu **Start (Avvio)** e selezionare **All Programs > Tools > Service Control (Tutti i programmi > Strumenti > Controllo del servizio)**.

| | |
|---|---|
| | Running (In esecuzione): |
| | Avvio |
| | Arrestato |

| | |
|---|---|
| **Modify Settings (Modifica impostazioni)** | Selezionare per modificare le impostazioni del server. |
| **Ripristina le impostazioni** | Fare clic per ripristinare tutte le impostazioni predefinite originali. |

Server:

| | |
|---|---|
| **Avvia** | Fare clic per avviare il server. |
| **Arresta** | Fare clic su per arrestare il server. |
| **Rinizia** | Fare clic su per riavviare il server. |

Database:

| | |
|---|---|
| **Avvia** | Fare clic per avviare il database. |
| **Arresta** | Fare clic su Arresta per arrestare il database. |
| **Rinizia** | Fare clic su per riavviare il database. |

Nota

Utilizzare i pulsanti **Start (Avvia)**, **Stop (Arresta)** e **Restart (Rinizia)** del database esclusivamente per la risoluzione di problemi e solo quando richiesto dal supporto di Axis.

## Impostazioni del server generali

Nel controllo del servizio AXIS Camera Station Pro selezionare **Modify settings (Modifica impostazioni)** e fare clic su **General (Caratteristiche generali)** per modificare le impostazioni generali del server.

| | |
|---|---|
| **Nome del server** | Il nome del server. Il nome server appare nel client software. Il nome predefinito del server è il nome del computer. Il nome non cambia se si cambia il nome del computer. |
| **Web client port (Porta del client Web)** | Il client Web per AXIS Camera Station usa questa porta. |
| **Ports range (Intervallo porte)** | Specificare l'intervallo di porte. Il resto delle porte cambia automaticamente. |
| **Allow AXIS Camera Station Pro to add exceptions to the Windows Firewall (Consenti a di aggiungere eccezioni a Windows Firewall)** | Selezionare per consentire a AXIS Camera Station Pro di aggiungere automaticamente eccezioni a Windows Firewall quando un utente modifica l'intervallo di porte. |

Nota

- Se è presente un NAT, un firewall o un dispositivo simile tra il server e il client, configurare il NAT o il firewall in modo da consentire il passaggio per queste porte.
- I numeri di porta devono essere compresi nell'intervallo 1024-65534.

### Elenco porta per AXIS Camera Station Pro

Le tabelle che seguono mostrano le porte e i protocolli usati da AXIS Camera Station Pro. Potrebbe essere necessario consentirli nel proprio firewall per prestazioni e usabilità ottimali. I numeri di porta vengono calcolati in base alla porta principale HTTP 29200. In alcune sezioni sono elencate sia le porte obbligatorie che quelle

facoltative. Affinché AXIS Camera Station Pro funzioni correttamente, le porte richieste devono essere sempre aperte. Se le porte opzionali non sono consentite, le relative funzionalità non funzioneranno.

**Da server ai dispositivi**

| Obbligatorio | | | | |
|---|---|---|---|---|
| **Porta** | **Numero** | **Protocollo** | **Direzione** | **Descrizione** |
| Porte HTTP e HTTPS principali | 443 | HTTPS | In uscita | Utilizzata per attivare la licenza, scaricare il firmware e, i servizi connessi. |
| **Facoltativo** | | | | |
| Porta WS-Discovery predefinita | 3702 | UDP | In entrata e in uscita | Servizi web WS-Discovery utilizzati per individuare i dispositivi ONVIF. Multicast 239.255.255.250. |
| Porta bonjour predefinita | 5353 | UDP | In entrata e in uscita | Utilizzato per il rilevamento dei dispositivi tramite mDNS (Bonjour). Multicast 224.0.0.251.<br><br>Se la porta predefinita non è disponibile, è possibile che un'altra applicazione la stia utilizzando e non la condivida. In tal caso si usa invece, una porta casuale. Si noti che i dispositivi con indirizzi di collegamento locale non sono rilevabili tramite Bonjour quando si utilizza una porta casuale. |

**Da client a server**

| Sono richieste tutte le porte | | | | | |
|---|---|---|---|---|---|
| **Porta** | **Numero** | **Protocollo** | **Direzione** | **Comunicazione tra** | **Descrizione** |
| Porta HTTP principale e porta di streaming HTTP | 29200 | HTTP | In entrata | Server e client ACS | Utilizzata per video, audio e flusso di metadati |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | (crittografia AES). |
| Porta TCP principale | 29202 | TCP | In entrata | Server e client ACS | Utilizzato esclusivamente per interruttore client a partire dalla versione 6.17. In precedenza, questa era la porta TCP principale. |
| Porta del server Web API ACS | 29204 | HTTPS | In entrata | Server ACS e app per dispositivi mobili | Utilizzato per i dati delle applicazioni e lo streaming video MP4 tramite HTTPS. |
| Porta HTTP proxy locale | 29206 | TCP | In entrata | All'interno del server ACS | Le app mobili effettuano chiamate al modulo SRA, che riceve HTTPS, la converte in HTTP e la invia nuovamente alla porta HTTP del proxy locale. |
| Porta endpoint proxy Web | 29207 | TCP | In entrata | Server ACS e componenti | Utilizzato per una comunicazione sicura tra componente e dispositivi. |

## Domini e porte per Secure Remote Access v2

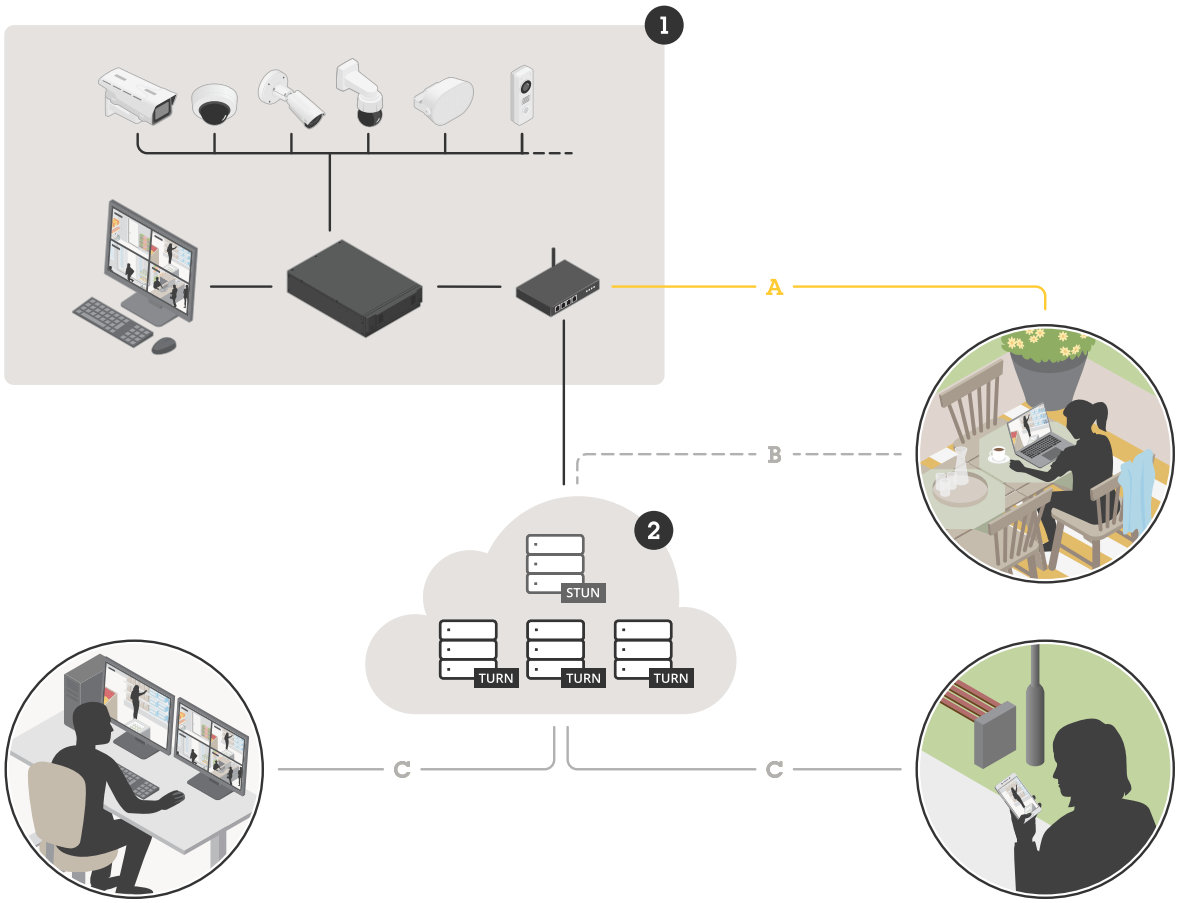



*Immagine: Panoramica della soluzione Axis Secure Remote Access v2 in AXIS Camera Station Pro*

1. Sito monitorato su rete locale con client di visualizzazione locale
   - A – Connessione remota (peer-to-peer)
   - B – Connessione STUN/TURN temporanea ai servizi connessi ad Axis Cloud

| Nome o tipo | Indirizzo | Numero porta | Protocollo | Direzione |
|---|---|---|---|---|
| SRA v2 - Accesso a My Axis | eu.login.connect.axis.com | 443 | TCP | In entrata e in uscita |
| SRA v2 - Comunicazione del servizio cloud | eu.cs.connect.axis.com | 443 | TCP | In entrata e in uscita |
| SRA v2 - Comunicazione API del servizio cloud | api.vms.axis.cloud | 443 | TCP | In entrata e in uscita |
| Componente di uplink | acspro.mysystems.axis.com | 443 | - | In entrata e in uscita |
| Componente EdgeHost | 75.2.119.140 | 443, 8443 | - | In entrata e in uscita |
| Componente EdgeHost | 99.83.133.42 | 443, 8443 | - | In entrata e in uscita |
| Componente EdgeHost | cep.connect.axis.com | 443, 8443 | - | In entrata e in uscita |

2. Servizi connessi ad Axis Cloud
   - C – Connessione TURN da remoto ai servizi connessi ad Axis Cloud

| Nome o tipo | Indirizzo | Numero porta | Protocollo | Direzione |
|---|---|---|---|---|
| Comunicazione proxy P2P e componente WebRTC | wss://signaling.prod.webrtc.connect.axis.com | 443 | TCP | In entrata e in uscita |
| Comunicazione proxy P2P e componente WebRTC | https://*.turn.prod.webrtc.connect.axis.com | 443, 3478, 5349, 49152-65535 | TCP | In entrata e in uscita |

**Riservato per componenti**

| Obbligatorio | | | | | | |
|---|---|---|---|---|---|---|
| **Componente** | **Ascolta l'interfaccia** | **Numero** | **Protocollo** | **Direzione** | **Comunicazione tra** | **Descrizione** |
| Server di segnalazione WebRTC locale | localhost | 29227 | WSS | In entrata | Client incorporabile, WebClient e WebRTC Streamer verso il server di segnalazione | Parte del componente WebRTC on-premises. |
| Configurazione WebRTC locale | localhost | 29229 | HTTPS | In entrata | Client ACS (pagina web) | Usato per l'hosting della pagina web di configurazione WebRTC e il back-end. Parte del componente WebRTC on-premises. |
| Server TURN locale | Tutti (0.0.0.0/INADDR_ANY) | 29230 | UDP | In entrata e in uscita | Server Client/WebClient in TURN incorporabile | Usato per "WebRTC a porta singola" su ACS sul posto. |
| IAM locale (IDP) | 0.0.0.0 | 29232 | HTTPS | In entrata | Proxy inverso e local-iam, client ACS per Windows e local-iam | Porta pubblica IDP_OIDC. |
| IAM locale (IDP) | 0.0.0.0 | 29233 | HTTPS | In entrata | Servizi di terze parti | Porta amministratore mTLS. |

| | | | | | | |
|---|---|---|---|---|---|---|
| IAM locale (IDP) | 127.0.0.1 | 29234 | HTTPS | In entrata | Servizi di terze parti | Porta tokenizer. |
| WebRTC | localhost | 29235 | HTTPS | In entrata | Componente cloud | Viene utilizzato durante la fase di onboarding per effettuare la configurazione della connessione WebRTC al cloud. Parte del componente WebRTC. |
| API di servizio | 127.0.0.1 | 29244 | NATS | In entrata | Tra ACS e componenti, e tra i componenti stessi, tramite NATS. | NATS Broker. |
| **Facoltativo** | | | | | | |
| Secure Entry (CA-MSM) | 127.0.0.1 | 29214 | HTTPS (WS) | In entrata | Client ACS (pagina Web) e componente | Configurabile tramite la porta base ACS. Installazioni precedenti usavano la porta 8081. |
| Secure Entry (CA-MSM) | Tutti (0.0.0.0/ INADDR_ ANY) | 29215 | HTTPS (WS) | In entrata | Componenti di Secure Entry in diversi siti | Configurabile tramite la porta base ACS. |
| Monitoraggio dell'integrità del sistema | Tutti (0.0.0.0/ INADDR_ ANY) | 29216 | HTTPS | In entrata | ACS (pagina Web), backend SHM (componente) | Utilizzato per ospitare le pagine web di Monitoraggio dell'integrità del sistema e per condividere i dati in configurazione multi-sistema. |
| Servizio cloud di monitoraggio dello stato di salute del | localhost | 29217 | HTTPS | In entrata | ACS (pagina Web) e backend del servizio cloud | Utilizzato per i servizi cloud. |

| | | | | | | |
|---|---|---|---|---|---|---|
| sistema / Servizio cloud | | | | | (componente) | |
| Ricerca intelligente 2 | localhost | 29218 | HTTPS | In entrata | Client ACS (scheda "Ricerca intelligente" della pagina Web) e backend di Ricerca intelligente (componente) | Utilizzato per ospitare l'API di ricerca smart e pubblicare la pagina web del client. |
| API VMS | 127.0.0.1, ::1 | 29219 | GraphQL | In entrata | API VMS e client GraphQL | Usato per esporre ACS come API GraphQL a un client. |
| Client web | localhost | 29223 | HTTPS | In entrata | Da WebClient a API/client incorporabile VMS | Il backend agisce come un proxy davanti all'API VMS. |
| Client incorporabile | localhost | 29224 | HTTPS | In entrata | Da client incorporabile ad API VMS, WebRTC Streamer e segnalazione server | Il backend funge da proxy davanti all'API del VMS. |
| Configurazione web client | localhost | 29225 | HTTPS | In entrata | Client ACS (pagina web) | Usato per l'hosting della pagina di configurazione Web Client incorporabile e il back-end. |
| Configurazione client incorporabile | localhost | 29226 | HTTPS | In entrata | Client ACS (pagina web) | Usato per l'hosting della pagina web di configurazione del Client incorporabile e il back-end. |
| Opentelemetry | 127.0.0.1 | 29236 | gRPC | In entrata | Servizi di terze parti (ACS e altri componenti) | Porta gRPC. |
| Opentelemetry | 127.0.0.1 | 29237 | HTTPS | In entrata | Servizi di terze parti | Porta HTTP. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | (ACS e altri componenti) | |
| Gestore audio | | 29238 | HTTPS | In entrata | Servizi e componenti di integrazione di terze parti | Porta del server Web. |
| Data Insights Dashboard | localhost | 29241 | HTTPS | In entrata | | Porta del server Web ricevitore. |
| Data Insights Dashboard | 0.0.0.0 | 29242 | MQTTS | In entrata e in uscita | Ricevitore di messaggi di eventi della telecamera | Broker Mosquitto. |
| Openteleme-try | 127.0.0.1 | 29245 | HTTP | In entrata | Endpoint di monitoraggio per il recupero di metriche dal collettore OpenTeleme-try | Porta HTTP. |
| Ricerca intelligente 2 | localhost | 29247 | gRPC | In entrata | Nucleo dell'API VMS e resolver Ricerca intelligente | Resolver di ricerca intelligente. |
| Gateway API | 0.0.0.0 | 29248 | HTTPS | In entrata | Host Edge e API Gateway | Porta di fallback del gateway API utilizzata dall'host edge. |
| Gateway API | 0.0.0.0 | 29250 | HTTPS | In entrata | Client ACS e gateway API | Porta di riserva per il traffico HTTP e HTTPS sulle porte 80 e 443. Si differenzia da +48 perché +48 utilizza certificati di componente, mentre questo utilizza certificati di server. |
| Monitoraggio dell'integrità del sistema | 127.0.0.1 | 29251 | gRPC | In entrata | Il server ACS ed eventual-mente altri componenti | Utilizzato dai produttori di dati sullo stato di salute del |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | verso il collettore SHM | sistema per trasferire i dati al collettore SHM. |
| Monitoraggio dell'integrità del sistema | 127.0.0.1 | 29252 | HTTPS | In entrata | Il server ACS ed eventual-mente altri componenti verso il collettore SHM | Utilizzato dai produttori di dati sullo stato di salute del sistema per trasferire i dati al collettore SHM. |
| Ricevitore AXIS Body Worn Live | 127.0.0.1 | 29254 | TCP | In entrata | Server di flusso dal vivo che accetta richieste HTTPS dal server ACS | Server di flusso dal vivo. |

**Altre porte**

**Obbligatorio**

| Porta | Numero | Protocollo | Direzione | Comunicazione tra | Descrizione |
|---|---|---|---|---|---|
| Porta HTTP | 80 | HTTP | In uscita | Server ACS e dispositivi, nonché client ACS e server ACS connessi all'internet | Utilizzato per l'attivazione delle licenze, il download del firmware e i servizi connessi. |
| Porta HTTP | 80 | HTTP | In entrata | Client ACS e server ACS | Utilizzato per flussi video e dati del dispositivo. |
| HTTPS port (Porta HTTPS) | 443 | TCP | In entrata | Client ACS e server ACS | Utilizzato per flussi video e dati del dispositivo. |
| Porta UDP stato di aggiornamento | 15156 | UDP | In entrata e in uscita | Controllo del server ACS e del servizio ACS | ACS service Control è in ascolto sulla porta e ACS server trasmette lo stato di un aggiornamento in corso. |
| PostgreSQL | 29210 | TCP | In entrata e in uscita | PostgreSQL e qualsiasi utente | Tra le utenze attuali figurano Data Insights Dashboard, il componente AXIS |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Audio Manager Pro e il componente AXIS Body Worn. |
| **Facoltativo** | | | | | |
| Servizi a bordo dei veicoli | 29253 | UDP | In entrata | Ricevitore GNSS per il componente dei servizi di bordo | |
| Porta HTTP | 80 | HTTP | In uscita | Server ACS e dispositivi, client ACS e server ACS connessi a internet | Utilizzata per attivare la licenza, scaricare il firmware, i servizi connessi, ecc. |
| Porta HTTP | 80 | HTTP | In entrata | Client ACS e server ACS | Utilizzato per flussi video e dati del dispositivo. |

## Database

### File del database

#### File del database di base

AXIS Camera Station Pro memorizza i file del core database in `C:\ProgramData\AXIS Communications\AXIS Camera Station Server`.

Per le versioni di AXIS Camera Station precedenti alla 5.13, è presente il solo file di database: **ACS.FDB**.

Per la versione 5.13 o successive di AXIS Camera Station, sono presenti tre file di database:

- **ACS.FDB**: questo file di database principale contiene la configurazione del sistema sotto forma di informazioni su dispositivi, viste, autorizzazioni, eventi e profili di streaming.
- **ACS_LOGS.FDB**: Questo file di database registri contiene i riferimenti ai registri.
- **ACS_RECORDINGS.FDB**: Questo file di database delle registrazioni contiene i metadati e i riferimenti alle registrazioni memorizzate nella posizione specificata in **Configuration > Storage (Configurazione > Archiviazione)**. AXIS Camera Station Pro richiede che questo file visualizzi le registrazioni nella sequenza temporale durante la riproduzione.

#### File del database componenti

**SecureEntry.db –** Il file di database di AXIS Secure Entry contiene tutti i dati di controllo degli accessi ad eccezione delle foto dei titolari di tessera. È salvato in `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\INTERNAL\main_db`.

**smartSearch.sqlite3 –** Il file di database di Ricerca intelligente contiene la configurazione della telecamera e i filtri di ricerca salvati. È salvato in `C:\ProgramData\Axis Communications\AXIS Smart Search\data`.

### Impostazioni del database

Il sistema esegue il backup del database ogni notte e prima di ogni aggiornamento. Nel controllo del servizio di AXIS Camera Station Pro, selezionare **Modify settings (Modifica impostazioni)** e fare clic su **Database** per cambiare le impostazioni di backup.

| | |
|---|---|
| **Backup folder (Cartella di backup)** | Fare clic su **Browse (Sfoglia)** e selezionare la posizione in cui salvare i backup. Riavviare il server AXIS Camera Station Pro per applicare la modifica.<br><br>Se il percorso della cartella di backup non è corretto o AXIS Camera Station Pro non ha accesso alla condivisione di rete, il backup viene salvato in`C:\ProgramData\Axis Communications\AXIS Camera Station Server\backup`. |
| **Days to keep backups (Numero di giorni di conservazione dei backup):** | Specificare il numero di giorni di conservazione dei backup. È possibile impostare qualsiasi numero compreso tra 1 e 30. Il numero di giorni predefinito è 14. |
| **Avanzamento dell'aggiornamento** | Fare clic su **Visualizza dettagli** per visualizzare i dettagli sull'ultimo aggiornamento del database. Comprende gli eventi accaduti a partire dall'ultimo riavvio del controllo del servizio AXIS Camera Station Pro. |

## Backup del database

Il database contiene informazioni relative alle registrazioni e ad altri metadati necessari al corretto funzionamento del sistema.

Importante

- Il database non memorizza le registrazioni. Specificare un punto di archiviazione in **Configuration > Storage (Configurazione > Archiviazione)** ed eseguire il backup delle registrazioni separatamente.
- Le impostazioni del server e del database nel controllo del servizio AXIS Camera Station Pro non vengono salvate.

### Backup del sistema

Il sistema salva in automatico il backup del sistema nella cartella specificata nella scheda **Database**. Vedere *Impostazioni del database, on page 225*. Un backup del sistema comprende sia i file del database di base sia i file del database dei componenti. Vedere *File del database, on page 225*.

| File di backup | |
|---|---|
| `System_YYYY-MM-DD-HH-mm-SSSS.zip` | Un backup attivato di notte. |
| `PreUpgrade_YYYY-MM-DD-HH-mm-SSSS.zip` | Un backup attivato prima di un aggiornamento del database. |
| `User_YYYY-MM-DD-HH-mm-SSSS.zip` | Un backup attivato prima della rimozione di un dispositivo di archiviazione. |

Nel file .zip puoi trovare i seguenti file:

| | |
|---|---|
| **ACS** | Questa cartella include i file del core database `ACS.FDB`, `ACS_LOGS.FDB` e `ACS_RECORDINGS.FDB`. |
| **Componenti** | Questa cartella è disponibile solo se si utilizza un componente, ad esempio AXIS Camera Station Secure Entry o la Ricerca intelligente.<br><br>• **webrtc**: questa cartella contiene i file di configurazione WebRTC. |

| | |
|---|---|
| | • **ACMSM**: Questa cartella comprende il file del database di AXIS Camera Station Secure Entry `SecureEntry.db` e le foto del titolare della tessera.<br>• **ricerca intelligente**: Questa cartella include il file del database della ricerca intelligente `smartSearch-backup-yyyyMMddHHmmssfff.sqlite3`. |
| `backup_summary.json` | Questo file comprende informazioni più dettagliate che riguardano il backup. |
| `_cluster_yyyyMMddHHmmssfff.dbcbackup` | Questo file contiene un backup logico del cluster di database PostgreSQL, che include dati relativi all'intero cluster, come ruoli e tablespace. |

**Backup di manutenzione**

Specificare in quale cartella di backup archiviare i backup di manutenzione nella scheda **Database**. Vedere *Impostazioni del database, on page 225*. Un backup di manutenzione include i file del core database con ogni file del database in una cartella separata `PreMaintenance_YYYY-MM-DD-HH-mm-SSSS`.

Si può attivare in vari modi:

- In automatico quando si aggiorna AXIS Camera Station Pro.
- Quando si esegue manualmente la **manutenzione del database** dal service control di AXIS Camera Station Pro. Vedere *Manutenzione database, on page 228*.
- In automatico, da parte dell'attività di manutenzione pianificata del database configurata in Utilità di pianificazione Windows. Vedere *Strumenti, on page 230*.

**Backup manuale**

Nota

Un backup manuale può comprendere solo i file del database di base. Non esegue il backup dei file del database dei componenti, ad esempio il file del database di ricerca intelligente.

Esistono due modi per eseguire un backup manuale:

- **Opzione 1:** Andare a `C:\ProgramData\AXIS Communications\AXIS Camera Station Server` e copiare i file del database. Successivamente, eseguire il backup del cluster del database PostgreSQL:
  1. Aprire un terminale come amministratore nella directory in cui si desidera salvare il backup.
  2. Eseguire `"C:\Program Files\Axis Communications\AXIS Camera Station \Core\DbConsole\DbConsole.exe" backup -cluster`
  3. Il backup viene salvato in una cartella denominata **yyyyMMddHHmmssfff** nella directory in cui è stato aperto il terminale.
- **Opzione 2:** geneare un report di sistema e selezionare **Include all databases (Includi tutti i database)** per includere i file di backup dei database. Vedere *Report del sistema, on page 211*.

## Ripristino del database

Se si perdono dati del database in seguito a un errore hardware o ad altri problemi, è possibile ripristinare il database da uno dei backup salvati. Per impostazione predefinita, il sistema conserva i file di backup per 14 giorni. Per ulteriori informazioni sul backup del database, vedere *Backup del database, on page 226*.

Nota

Il database non memorizza le registrazioni. Specificare un punto di archiviazione in **Configuration > Storage (Configurazione > Archiviazione)** ed eseguire il backup delle registrazioni separatamente.

Per ripristinare il database:

1. Andare al controllo del servizio AXIS Camera Station Pro e fare clic su **Stop (Arresta)** per arrestare il servizio.
2. Andare ai file di backup del database. Vedere *Backup del database, on page 226*.
3. Eseguire l'estrazione dei file.
4. Ripristinare il cluster del database PostgreSQL:
   4.1. Aprire un terminale come amministratore nella cartella estratta.
   4.2. Eseguire `"C:\Program Files\Axis Communications\AXIS Camera Station\Core\DbConsole\DbConsole.exe" restore -backup-file _cluster_yyyyMMddHHmmssfff.dbcbackup`
   4.3. Fare clic su **y** quando richiesto per confermare che si ritiene attendibile la fonte del file di backup.
5. Nella cartella estratta, copiare i seguenti file del database in **ACS** su `C:\ProgramData\AXIS Communications\AXIS Camera Station Server\`.
   - **ACS.FDB** - È necessario copiare questo file per ripristinare il database.
   - **ACS_LOGS.FDB** - Copiare questo file se si desidera ripristinare i registri.
   - **ACS_RECORDINGS.FDB** - Copiare questo file se si desidera ripristinare le registrazioni.
6. Se si utilizza AXIS Camera Station Secure Entry, seguire le istruzioni riportate in `RESTORE_INSTRUCTIONS.txt` all'indirizzo `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry 2\INTERNAL\main_db`.
7. Se si usa la Ricerca intelligente, copiare **smartSearch-backup-yyyyMMddHHmmssfff.sqlite3** da `smartsearch` a `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Smart Search\data` e rinominarlo in **smartSearch.sqlite3**.
8. Se si utilizza il client Web VMS, copiare tutti i file da `webrtc` a `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\WebRTC`.
9. Tornare al controllo del servizio AXIS Camera Station Pro e fare clic su **Start (Avvia)** per avviare il servizio.

## Manutenzione database

Eseguire la manutenzione del database se viene visualizzato l'allarme `Database maintenance is required` o in caso di arresto anomalo del sistema, ad esempio per interruzione di corrente.

Per avviare la manutenzione del database, vedere *Strumenti, on page 230*.

Nota

AXIS Camera Station Secure Entry utilizza DB Janitor per monitorare e comprimere i file del database, se necessario. Il sistema di controllo degli accessi diventa temporaneamente non disponibile quando si verifica una contrazione forzata.

## Miglior prassi per database

Per evitare problemi, tenere presente i punti elencati di seguito.

**Controllo di errori del disco –** gli errori del disco possono danneggiare il database. Utilizzare uno strumento come chkdsk (Controllo disco detto anche Controllo errori) per cercare i settori danneggiati sul disco rigido usato per il database. Eseguire chkdsk regolarmente.

**Software antivirus e backup esterni –** Non eseguire scansioni con l'antivirus sul database perché alcuni software antivirus possono danneggiarlo. Se si utilizza un sistema di backup esterno, non eseguire il backup del database attivo. Creare invece un backup dai file nella cartella di backup.

**Interruzione di corrente –** un arresto imprevisto, dovuto ad esempio a un'interruzione di corrente, può danneggiare il database. Utilizzare un UPS (gruppo di continuità) per le installazioni critiche.

**Spazio esaurito –** il database si può danneggiare se si esaurisce lo spazio sul disco rigido. Per evitarlo, installare il server AXIS Camera Station Pro su un computer con memoria sufficiente. Per informazioni sui requisiti hardware, vedere *axis.com/products/axis-camera-station/hardware-guidelines*.

**Memoria RAM danneggiata –** Esegui regolarmente lo strumento di diagnostica della memoria di Windows per verificare la presenza di errori nella RAM.

## Certificati

Utilizzare la scheda **Certificates (Certificati)** per gestire i certificati del server per AXIS Camera Station Pro. È possibile visualizzare le informazioni sul certificato server corrente, vedere quando scade, generare e importare nuovi certificati server o esportare quello corrente. I certificati del server sono memorizzati in C:\ProgramData\Axis Communications\AXIS Camera Station Server\certs.

### Certificato del server

| | |
|---|---|
| **Genera** | Creazione di un nuovo certificato del server autofirmato. Questo sostituisce il certificato precedente utilizzato dal server e richiede un riavvio del server perché abbia effetto. |
| **Importa...** | Importare un certificato del server da un file. I formati file supportati sono PEM e PFX/PKCS12. Sono supportate solo chiavi RSA con almeno 2048 bit. |

Nota

Quando si importa un certificato con certificati intermedi nel formato PEM, tutti i certificati intermedi devono essere presenti nel file .cer. Se si stanno creando i propri certificati, vedere *Preparare i certificati intermedi per l'importazione, on page 229*.

### Certificato corrente

Mostra le informazioni relative al certificato del server corrente. Utilizzare questa opzione per verificare in modo manuale che il client si sia connesso al server corretto.

| | |
|---|---|
| **Visualizza** | Visualizzare ulteriori dettagli sul certificato del server. |
| **Esporta...** | Esportare il certificato del server come file PFX. |

### Generare un nuovo certificato server

- Premere il tasto Windows + S per cercare e aprire il controllo del servizio AXIS Camera Station Pro.
- Nella scheda **Certificates (Certificati)**, fare clic su **Generate (Genera)** per generare un nuovo certificato del server.
- Riavviare il server per applicare il nuovo certificato del server.

### Preparare i certificati intermedi per l'importazione

Per importare un certificato con certificati intermedi in AXIS Camera Station Pro, combinare il certificato del server e il certificato intermedio in un unico file:

1. Aprire uno dei certificati del server e il certificato intermedio in Blocco note. I contenuti saranno strutturati come segue:

```
cert.cer
-----BEGIN CERTIFICATE-----
MIIFTDCCB....
-----END CERTIFICATE-----
```

2. Copiare e incollare il contenuto di un certificato nell'altro e modificare la prima riga in combined_cert.cer:

```
combined_cert.cer
-----BEGIN CERTIFICATE-----
MIIFTDCCB....
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIE+zCCA+OgA.....
-----END CERTIFICATE-----
```

3. Salvare il file.

## Strumenti

Nel service control di AXIS Camera Station Pro selezionare **Modify Settings (Modifica impostazioni)**, quindi fare clic su **Tools (Strumenti)** per eseguire la manutenzione del database, creare un report parziale del sistema, abilitare la registrazione di rete o reimpostare l'autorità di certificazione.

### Manutenzione database

Per eseguire la manutenzione database:

1. Aprire il AXIS Camera Station Pro Service Control.
2. Fare clic su **Tools (Strumenti)**.
3. In **Database maintainer (Manutenzione database)**, fare clic su **Run (Esegui)**.
4. Appare il tempo di inattività stimato. fare clic su **Yes (Sì)** per continuare. Una volta avviata, la procedura non può essere annullata.

Nota

- AXIS Camera Station Pro server e tutte le registrazioni in corso si fermano nel corso della manutenzione. Dopo la manutenzione, il server si riavvia automaticamente.
- Non spegnere il computer durante la manutenzione.
- La manutenzione del database richiede i diritti di amministratore nel computer Windows.
- Se la manutenzione del database non è in grado di recuperare il database, contattare l'assistenza tecnica Axis.

Assicurarsi di eseguire la manutenzione del database se viene visualizzato l'allarme "È necessaria la manutenzione del database" o in caso di arresto anomalo del sistema, ad esempio per interruzione di corrente.

L'esecuzione automatica della manutenzione del database può essere programmata attivando " AXIS Camera Station Pro Database Maintenance Task" nell'Utilità di pianificazione Windows. Si può modificare il trigger per personalizzare quando e con quale frequenza deve essere eseguita la manutenzione database.

### Registrazione rete

Per avviare la registrazione di rete:

1. Aprire il AXIS Camera Station Pro Service Control.
2. Fare clic su **Tools (Strumenti)**.
3. In **Network logging (collegamento di rete**, fare clic sul collegamento per scaricare un'applicazione per l'analisi del protocollo di rete.
4. Una volta installata, fare clic su **Start... (Avvia)** per avviare l'applicazione.

## Report di sistema parziale

Il report di sistema parziale è un file .zip che contiene parametri e file di registro che aiutano l'assistenza clienti Axis ad analizzare il sistema. Includere sempre un report di sistema quando si contatta l'assistenza clienti.

Per generare un report di sistema completo, consultare la sezione *Report del sistema, on page 211*.

Per generare un report di sistema parziale:

1. Aprire controllo del servizio AXIS Camera Station Pro.
2. Fare clic su **Tools (Strumenti)**.
3. Nella sezione **Partial system report (Report parziale sistema)**, fare clic su " **Run...** (Esegui).
4. Selezionare e inserire le informazioni necessarie nella finestra di dialogo.
5. Fare clic su **Genera report**.

## Ripristinare l'autorità di certificazione

Quando AXIS Camera Station Pro si avvia, controlla lo stato di integrità dell'autorità di certificazione (CA):

- Se AXIS Camera Station Pro ha creato la CA e il controllo non riesce, il sistema rigenera automaticamente la CA radice. Non è richiesta alcuna azione da parte dell'utente.
- Se la CA è stata importata e la verifica non va a buon fine, AXIS Camera Station Pro arresta il server e mostra un errore relativo all'autorità di certificazione, ad esempio: "Impossibile decrittografare la chiave privata".

Per risolvere un errore relativo all'autorità di certificazione:

1. Aprire il service control di AXIS Camera Station Pro.
2. Fare clic su **Tools (Strumenti)**.
3. In **Reset certificate authority (Ripristino autorità di certificazione)**, fare clic su **Reset (Ripristino)**.
4. Una volta che il servizio si riavvia, aprire il client AXIS Camera Station Pro e andare a **Configuration > Security > Certificates (Configurazione, Sicurezza, Certificati)**.
5. Reimportare l'autorità di certificazione.

# Risoluzione dei problemi

## Informazioni su questa guida

Questa guida raccoglie problemi relativi ad AXIS Camera Station Pro e illustra la relativa risoluzione. Gli argomenti sono raggruppati per tema per facilitarne la ricerca. Un argomento può essere, ad esempio, l'audio o la visualizzazione in diretta. Ogni numero include una soluzione suggerita.

Per ulteriori risorse, tra cui i requisiti di hardware, gli aggiornamenti di software e i tutorial, visitare *axis.com/support*.

Se si verificano problemi di carattere generale, provare a effettuare il riavvio del servizio server AXIS Camera Station Pro prima di procedere con ulteriori operazioni di risoluzione di problemi:

1. Andare in **Configuration (Configurazione)** > **Server** > **Diagnostics (Diagnostica)**.
2. Fare clic su **Restart AXIS Camera Station server service... (Riavvia il servizio server di AXIS Camera Station...)**.

Nota

Il riavvio del servizio server può richiedere un po' di tempo e non è possibile annullarlo. Il server non è disponibile e tutti i dispositivi connessi perdono la connessione durante il riavvio.

## Il servizio AXIS Camera Station Pro

### Il servizio si riavvia spesso

È possibile che il server sia sovraccarico, 1uesto causa una lunga coda di attività e può anche danneggiare i database.

- Verificare se AXIS Camera Station Pro o qualsiasi altra applicazione sta utilizzando un numero elevato di risorse.
- Eseguire l'applicazione di manutenzione database. Vedere *Manutenzione database, on page 228*.

Se nessuna delle soluzioni di cui sopra risolve il problema, contattare l'assistenza Axis. Andare a *Processo di escalation, on page 248* .

## Dispositivi nel Video Management System

### Problemi comuni

| | |
|---|---|
| Le telecamere elencate non sono state aggiunte perché il VMS non riesce a connettersi alla telecamera | 1. Controllare che la telecamera sia dotata di una connessione di rete, che ci sia alimentazione e che la telecamera sia in funzione.<br>2. Andare a **Configuration > Add devices (Configurazione > Aggiungi dispositivi)** e riprovare ad aggiungere la telecamera. |
| Le telecamere elencate non sono state aggiunte perché l'utente ha annullato l'installazione | Per aggiungere le telecamere, andare a **Configurazione > Aggiungi dispositivi**. |
| Impossibile impostare la password per le telecamere elencate | 1. Per l'impostazione manuale della password, vai a **Configuration > Devices > Management (Configurazione > Dispositivi > Gestione)**.<br>2. Fare clic con il pulsante destro del mouse sulla telecamera e selezionare **User Management > Set password (Gestione degli utenti > Imposta password)**. |

### Impossibile aggiungere il dispositivo

| | |
|---|---|
| Il dispositivo era stato utilizzato in un altro sistema prima di essere aggiunto a AXIS Camera Station Pro | • Eseguire il ripristino delle impostazioni di fabbrica sul dispositivo.<br>• Provare ad aggiungere il dispositivo ad AXIS Device Manager per la gestione. |
| Viene aggiunto un modello di dispositivo diverso da quello desiderato | Potrebbe trattarsi di un problema di compatibilità. Utilizzare sempre la versione AXIS Camera Station Pro più recente. |
| Non è possibile aggiungere un altro modello di dispositivo | Risoluzione di problemi della telecamera, andare su *axis.com/support/troubleshooting*. |

### Non è possibile aggiornare il firmware del dispositivo attraverso AXIS Camera Station Pro

| | |
|---|---|
| Non è possibile aggiornare ul firmware della telecamera tramite l'interfaccia web | Risoluzione di problemi della telecamera, andare su *axis.com/support/troubleshooting*. |
| Non è possibile aggiornare il firmware su tutti i dispositivi | • Controllare che ci sia un collegamento di rete.<br>• Se il problema non è il collegamento di rete, contattare l'assistenza Axis. Andare a *Processo di escalation, on page 248* . |
| Impossibile aggiornare il firmware per modelli specifici | Potrebbe trattarsi di un problema di compatibilità. Contatta l'assistenza Axis. Andare a *Processo di escalation, on page 248* . |

### Nessun dispositivo rilevato

Il Video Management System cerca automaticamente nella rete le telecamere e i video encoder connessi senza trovarli.

- Verificare che la telecamera abbia una connessione di rete e che sia presente l'alimentazione.
- Se il client, il server o le telecamere si trovano in reti diverse, configurare le impostazioni proxy e del firewall.
  - Modificare le impostazioni del proxy client se il server proxy separa il client e il server.
  - Modificare il NAT o il sistema di sicurezza se un NAT o un sistema di sicurezza separa il client e il server. Autorizzare che la porta HTTP, TCP (Transmission Control Protocol) e la porta di streaming specificate nel controllo servizio AXIS Camera Station passino attraverso il sistema di sicurezza o NAT. Per visualizzare l'elenco completo delle porte, consultare *Elenco porta per AXIS Camera Station Pro, on page 216*.
- Aggiungere le telecamere in modo manuale. Andare a *Aggiungi dispositivi, on page 6*.

### Messaggio ripetuto "Riconnessione alla videocamera tra 15 secondi"

**Problemi possibili:**

- Una rete sovraccarica.
- La telecamera non è accessibile. Verificare che la telecamera disponga di un Collegamento di rete.
- Vi sono problemi con la scheda grafica.

**Possibili soluzioni per i problemi della scheda grafica:**

- Installare i driver della scheda grafica più recenti.

- passare a una scheda grafica con più memoria video e con maggiori prestazioni;
- Utilizzare la CPU per il rendering video. Selezionarla nella in **Graphics card (Scheda grafica)** in **Decodifica hardware (Hardware decoding)**. È possibile trovare queste impostazioni in **Configuration > Client > Streaming (Configurazione > Client > Streaming)**.
- Regolare le impostazioni video e audio. Ad esempio, ottimizzare le impostazioni del profilo per una larghezza di banda ridotta.

## Registrazioni

### Problemi comuni

| | |
|---|---|
| La registrazione continua non è attiva | 1. Per l'attivazione della registrazione continua, andare a **Configuration > Recording and events > Recording method (Configurazione > Registrazione ed eventi > Metodo di registrazione)**.<br>2. Seleziona la telecamera e attiva **Continuous (Continua)**. |
| Impossibile registrare sull'unità specificata | 1. Per utilizzare un dispositivo di archiviazione locale, andare a **Configuration > Storage > management (Configurazione > Archiviazione > Gestione)**.<br>2. Eseguire l'aggiunta del dispositivo di archiviazione e configurare le impostazioni di archiviazione per le telecamere. |
| Non è pssibile installare l'applicazione AXIS Video Content Stream | 1. Per l'installazione manuale dell'applicazione, andare a **Configuration > Devices > Management (Configurazione > Dispositivi > Gestione)**.<br>2. Selezionare una telecamera e fare clic su . |

### La registrazione non si avvia

Se le registrazioni non partono o si interrompono dopo pochi secondi, significa che il disco è pieno o che ci sono troppi dati indesiderati.

- Nel foglio di configurazione server, in **Recording Storage (Memorizzazione della registrazione)** controllare che sia disponibile spazio libero e non vi siano dati di intrusione.
- Incrementare il limite di archiviazione per il Video Management System.
- Assegnare più spazio di archiviazione al pool di archiviazione. Vedere *Configurazione dell'archiviazione, on page 75*.

### Spazi vuoti di registrazione durante la registrazione continua

Le lacune fanno scattare allarmi denominati **Recording errors (Errori di registrazione)**. Gli spazi vuoti si verificano per diversi motivi, ad esempio:

- Sovraccarico del server
- Problema di connessione di rete
- Sovraccarico telecamera
- Sovraccarico del disco

Verificare se le interruzioni nella registrazione si verificano su tutte le telecamere. Se non si verificano su tutte le telecamere, ciò potrebbe indicare un sovraccarico delle telecamere. Utilizzare queste domande come aiuto per individuare la causa:

- Con quale frequenza si verificano le lacune, ogni ora o ogni giorno?
- Quanto dura la lacuna, secondi o ore?
- A che ora si verifica lo spazio vuoto?

**Soluzioni possibili:**

- Nel gestore delle attività del server, verificare se qualche risorsa hardware viene utilizzata più del normale. Se il disco presenta segni di utilizzo eccessivo, aggiungere altri dischi e spostare qualche telecamere perché registri sui nuovi dischi.
- Ridurre la quantità di dati scritti sul disco (impostazioni video, Zipstream, velocità in fotogrammi, risoluzione). Considerare il throughput stimato da AXIS Site Designer, vedere *axis.com/support/tools/axis-site-designer*.

Per maggiori informazioni, vedere *Performance visualizzazione in diretta e riproduzione, on page 236*.

## Impossibile eseguire la riproduzione delle registrazioni esportate

Se Windows Media Player non esegue la riproduzione delle tue registrazioni esportate, controlla il formato del file. Per la riproduzione delle registrazioni esportate, usare Windows Media Player (.asf) o AXIS File Player (.asf, .mp4, .mkv).

Per saperne di più, vedere *Riproduzione e verifica delle registrazioni in AXIS File Player., on page 7*.

Nota

AXIS File Player apre in automatico tutte le registrazioni nella stessa cartella del lettore.

## Le registrazioni scompaiono

Il sistema salva registrazioni solo per un certo numero di giorni. Per cambiare il numero di giorni, andare a **Configuration (Configurazione) > Storage (Archiviazione) > Selection (Selezione)**.

Se lo spazio di archiviazione è pieno, il sistema potrebbe eliminare le registrazioni prima della scadenza del periodo di conservazione. Per evitare che lo spazio di archiviazione si esaurisca, provare le seguenti operazioni:

- Aggiungere più spazio di archiviazione. Andare a **Configurazione > Archiviazione > Gestione**.
- Modificare la quantità di spazio di archiviazione assegnato a AXIS Camera Station Pro. Andare a **Configurazione > Archiviazione > Gestione**.
- Ridurre le dimensioni dei file registrati modificando, ad esempio, la risoluzione o la velocità in fotogrammi. Andare a **Configuration > Devices > Stream profiles (Configurazione > Dispositivi > Profili di streaming)**.
  - Utilizzare il formato video H.264 per la registrazione. Il formato M-JPEG richiede molto più spazio di archiviazione.
  - Usare Zipstream per ridurre ulteriormente le dimensioni delle registrazioni.

### Problemi di failover recording

| | |
|---|---|
| La larghezza di banda tra la telecamera e il server non è sufficiente per il trasferimento della registrazione | Aumentare la larghezza di banda. |
| La telecamera non ha registrato sulla scheda di memoria durante la disconnessione | • Controllare il report del server della telecamera. Vedi *axis.com/support/troubleshooting*.<br>• Controllare che la scheda di memoria funzioni e che vi siano registrazioni. |
| L'orario della telecamera è cambiato/si è spostato dopo la disconnessione | • Accertarsi di configurare NTP per le registrazioni future.<br>• Sincronizzare l'orario della telecamera con il server o usare lo stesso server NTP sulla telecamera e sul server. |

Nota

La failover recording non funziona durante gli spegnimenti controllati del server o in caso di interruzioni della connessione di durata inferiore a 10 secondi.

## Visualizzazione in diretta

### Performance visualizzazione in diretta e riproduzione

Questa sezione descrive le possibili soluzioni in caso di perdita di fotogrammi o problemi grafici nel client AXIS Camera Station Pro.

| Hardware del client | |
|---|---|
| Verificare che il driver della scheda grafica o dell'adattatore di rete sia aggiornato | 1. Aprire DirectX Diagnostic Tool (cerca dxdiag sul computer).<br>2. Andare al sito Web del produttore per verificare se il driver è il più recente per questo OS.<br>3. Verificare che il client e il server siano in esecuzione sullo stesso computer.<br>4. Provare a eseguire il client su un computer dedicato. |
| Verificare il numero di monitor | Si sconsiglia di utilizzare più di due monitor per scheda grafica.<br>Nota<br>L'esecuzione del client su una macchina virtuale non è supportata. |
| La scheda grafica non supporta il formato di codifica configurato in **Configuration > Devices > Stream Profiles (Configurazione, Dispositivi, Profili di streaming)** | • Controllare che la scheda grafica supporti il formato di codifica dei flussi.<br>• Provare a utilizzare diversi formati di codifica.<br>• Se un formato di codifica supportato non funziona come previsto su più telecamere, controllare che i driver della scheda grafica siano aggiornati. |

| Dispositivi connessi | |
|---|---|
| Molti client connessi contemporaneamente | Basandosi sul tipico caso d'uso, verificare che il sistema soddisfi i requisiti e rispettare le linee guida hardware. Vedere i *Requisiti del server nella guida di installazione e migrazione di AXIS Camera Station Pro*. |
| La telecamera è collegata a un Video Management System diverso da quello di AXIS Camera Station Pro | Disconnettere la telecamera dall'altro client e impostarla come predefinita prima di connetterla a AXIS Camera Station Pro. |
| Una telecamera impiega molti flussi diversi, specialmente la risoluzione elevata | Questo potrebbe rappresentare un problema, soprattutto per alcune telecamere della serie M-Line o per le telecamere multisensore.<br>• Far passare il flusso verso lo stesso profilo di streaming o una risoluzione inferiore. Vedere *Profili di flusso, on page 55*. |

| Sovraccarico del server | |
|---|---|
| Utilizzo CPU o RAM insolito corrispondente allo stesso orario del problema | Controllare che non ci siano altre applicazioni in esecuzione che consumino risorse della CPU o della RAM. |

| Problema di connessione di rete | |
|---|---|
| Utilizzo larghezza di banda inusuale corrispondente allo stesso orario del problema | Controllare che non ci siano altre applicazioni che consumano molta larghezza di banda in esecuzione contemporaneamente. |
| Larghezza di banda sufficiente, rete remota o locale | • Esaminare la propria topologia di rete.<br>• Eseguire un controllo di integrità su qualsiasi dispositivo di rete come switch, router, adattatore di rete e cavo in uso tra le telecamere, il server e il client. |

## Nessun video nella visualizzazione in diretta

La visualizzazione in diretta non mostra video di una telecamera nota.

- Disattiva la decodifica hardware. Per impostazione predefinita, la decodifica hardware è impostata su **Auto**. Vedere Decodifica hardware nella sezione *Streaming, on page 121*.
- Se è stato installato un software antivirus, questo potrebbe bloccare i flussi dal vivo o le cartelle e i processi di AXIS Camera Station Pro. Consultare le *domande frequenti.*

**Altre soluzioni possibili:**

- Se non si può vedere la visualizzazione in diretta attraverso l'interfaccia web o se l'interfaccia web non funziona, eseguire la risoluzione dei problemi della telecamera. Andare a *axis.com/support/troubleshooting*.
- Creare un report del server delle telecamere. Andare a *axis.com/support/troubleshooting*.
- Assicurarsi che il firewall non blocchi le connessioni su determinate porte; consultare la sezione *Impostazioni del server generali, on page 216*.
- Verificare di aver installato Desktop Experience per le versioni del sistema operativo del server Windows supportate. Vedere *Esportazione pianificata, on page 130*.
- Verificare che il flusso a risoluzione inferiore funzioni correttamente.

Se nessuna delle opzioni precedenti è di aiuto, andare a *Processo di escalation, on page 248*.

### Prestazioni di decodifica hardware

Utilizzare questa guida alla risoluzione di problemi se riscontri rallentamenti, immagini a scatti o interruzioni nel video, un elevato utilizzo della CPU durante la visualizzazione in diretta o frequenti messaggi del tipo Riconnessione alla telecamera.

1. Aggiornare i driver della scheda grafica. I driver obsoleti sono la causa più comune dei problemi di accelerazione dell'hardware. Andare sul sito web del produttore (NVIDIA, AMD o Intel) e scarica il driver più recente per il tuo modello di GPU.
2. Regolare la modalità di decodifica hardware. Andare a **Configuration > Client > Streaming (Configurazione, Client, Streaming)**:
   - Se la modalità è impostata su **Automatic (Automatico)** o **On** e si riscontrano dei problemi, impostarla su **Off**. Se le prestazioni migliorano, è possibile che la GPU non disponga di capacità sufficiente per il carico del flusso attuale. Vedere il punto 6.
   - Se la modalità è **Off** e l'utilizzo della CPU è elevato, prova a impostare la modalità su **Automatic (Automatico)** oppure **On**, a condizione che disponga di una GPU adeguata.
3. Monitorare le risorse di sistema. Aprire Gestione attività di Windows (Ctrl + Maiusc + Esc) e andare alla scheda **Prestazioni**:
   - Un utilizzo della CPU costantemente superiore all'80% circa, in assenza di decodifica hardware, suggerisce che il sistema potrebbe non essere sufficientemente potente per il numero o la risoluzione dei flussi.
   - Il fatto che la memoria dedicata della GPU sia quasi al limite della sua capacità con la decodifica hardware attivata indica un collo di bottiglia della GPU.
4. Ridurre il numero di telecamere visualizzate contemporaneamente oppure imposta le telecamere su profili di streaming a risoluzione inferiore per ridurre il carico sul sistema.
5. Assicurarsi che il flusso delle telecamere sia in formato H.264 o AV1. Altri codec non utilizzano la decodifica hardware.
6. Valutare le prestazioni della GPU. Anche una GPU che supporta la decodifica hardware può presentare dei limiti in termini di risoluzione o velocità in fotogrammi. Per le impostazioni con numerosi flussi ad alta risoluzione, verificare *i requisiti del client AXIS Camera Station Pro* e valutare l'aggiornamento a una GPU con maggiore VRAM e una maggiore capacità di decodifica.
7. Se nessuna delle soluzioni sopra indicate dovesse funzionare, contatta *l'assistenza Axis* tenendo a portata di mano le seguenti informazioni:
   - Hardware di sistema (CPU, GPU, RAM).
   - Versione del sistema operativo.
   - Versione del driver grafico.
   - versione AXIS Camera Station Pro.
   - Sintomi specifici e fasi di riproduzione.

## Magazzino

### Archiviazione di rete non accessibile

Se si utilizza l'account di sistema locale per accedere al controllo del servizio AXIS Camera Station Pro, è possibile aggiungere l'archiviazione di rete collegata a cartelle condivise su altri computer.

Per modificare l'account di accesso al servizio:

1. Aprire il **Pannello di controllo di Windows**.
2. Cercare "Servizi".
3. Fare clic su **View local services (Visualizza servizi locali)**.

4. Fare clic con il pulsante destro del mouse su AXIS Camera Station Pro e selezionare **Properties (Proprietà)**.
5. Andare alla scheda **Log on (Accesso)**.
6. Modificare la selezione da **Account di sistema locale** ad **Account**.
7. selezionare un utente con accesso a Windows Active Directory.

### Archiviazione di rete non disponibile

Verificare che il computer e il server dove viene eseguito il software per la gestione video facciano parte dello stesso dominio del dispositivo di archiviazione di rete.

### Impossibile riconnettersi a un dispositivo di archiviazione di rete con un nuovo nome utente e password

Se un dispositivo di archiviazione di rete richiede l'autenticazione, è importante scollegare il dispositivo di archiviazione di rete da tutte le connessioni in esecuzione prima di cambiare il nome utente e la password.

Per modificare il nome utente e la password per un dispositivo di archiviazione di rete e riconnettersi:

1. Disconnettere il dispositivo di archiviazione di rete da tutte le connessioni in esecuzione.
2. cambiare il nome utente e la password.
3. Andare a **Configuration > Storage > Management (Configurazione > Archiviazione > Gestione)** e riconnettere il dispositivo di archiviazione di rete con il nuovo nome utente e la password.

## Rilevamento del movimento

### Problemi comuni

| | |
|---|---|
| Non è possibile installare l'applicazione AXIS Video Motion Detection | Per l'installazione manuale dell'applicazione, andare a *Installare le applicazioni per telecamera, on page 69*. |
| Impossibile recuperare i dati relativi al rilevamento movimento in corso | Ripristina le impostazioni di fabbrica della telecamera:<br>1. Andare a **Configurazione > Dispositivi > Gestione**.<br>2. Fare clic con il pulsante destro del mouse sulla telecamera che presenta il problema e seleziona **Restore the camera to factory settings (Ripristina le impostazioni di fabbrica della telecamera)**.<br>Durante il ripristino, la telecamera non è disponibile. Le impostazioni IP e HTTPS non subiscono alcuna modifica. Una volta finito il ripristino, la colonna Stato mostra la dicitura **Set password (Imposta password)**. Fare clic su **Set password (Imposta password)** per ricollegare la telecamera al server. |

| | |
|---|---|
| Rilevamento movimento non configurato | 1. Per configurare manualmente il rilevamento del movimento, andare a **Configuration (Configurazione) > Registrazione ed eventi > Metodo di registrazione**.<br>2. Selezionare la telecamera e fare clic su **Motion settings (Impostazioni movimento)** per configurare il rilevamento movimento. |
| Il rilevamento movimento non è attivato | 1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Metodo di registrazione**.<br>2. Selezionare la telecamera e attivare **Motion detection (Rilevamento movimento)** per attivare la registrazione del rilevamento movimento. |

### Il rilevamento movimento rileva troppi oggetti in movimento o troppo pochi

Questa sezione illustra possibili soluzioni se si dispone di un numero maggiore o inferiore di rilevamenti nelle registrazioni correlate al video motion detection.

#### Regolazione delle impostazioni di movimento

Si possono selezionare le impostazioni di movimento per la regolazione dell'area che rileva gli oggetti in movimento.

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Metodo di registrazione**.
2. Selezionare la telecamera e fare clic su **Motion Settings (Impostazioni movimento)**.
3. Scegliere le impostazioni a seconda del firmware della telecamera.

| | |
|---|---|
| AXIS Video Motion Detection 2 e 4 | Si può configurare l'area di interesse. Vedere *Modifica di AXIS Video Motion Detection 2 e 4, on page 87*. |
| Funzione di rilevazione movimento incorporata | Si possono configurare i riquadri di inclusione e di esclusione. Vedere *Modifica di rilevamento movimento incorporato, on page 88*. |

#### Regolazione del periodo di attivazione

Il periodo di trigger è l'intervallo di tempo tra due trigger successivi. Usare questa impostazione per ridurre il numero di registrazioni consecutive. Se avviene un altro trigger nell'intervallo, la registrazione prosegue e il periodo di attivazione ricomincia.

Per cambiare il periodo di attivazione:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Metodo di registrazione**.
2. Selezionare la telecamera.
3. In **Advanced (Avanzate)**, regolare **Trigger period (Periodo di attivazione)** in secondi.

## Regole di azione

### Eventi di trigger I/O inattesi

Se si verificano eventi di input/output inaspettati intorno alle ore 1:15 di notte, sostituire i propri trigger I/O esistenti con trigger di eventi del dispositivo.

# Audio

## Niente audio nella visualizzazione in diretta

Se non è presente l'audio nella visualizzazione in diretta, controllare quanto segue:

- Verificare che la telecamera disponga di funzionalità audio.
- Verificare che il computer disponga di una scheda audio e che sia in uso.
- Verificare che il profilo in uso sia stato configurato per l'audio.
- Verificare che l'utente disponga dei diritti di accesso alle funzionalità audio.

### Configura i profili per l'audio

1. Andare a **Configuration > Devices > Stream profiles (Configurazione > Dispositivi > Profili di streaming)**.
2. Selezionare la telecamera.
3. Selezionare **MPEG-4** o **H.264** in **Format (Formato)** nelle impostazioni del profilo video.
4. In **Audio**, selezionare un microfono nel menu a discesa **Microphone (Microfono)**.
5. Selezionare quando usare l'audio nel menu a discesa **Use microphone for (Usa microfono per)**.
6. Se applicabile, selezionare un altoparlante nel menu a discesa **Speaker (Altoparlante)**.
7. Fare clic su **OK**.

### Verifica e modifica i diritti di accesso degli utenti

Nota

Per eseguire questa procedura, è necessario disporre dei diritti di amministratore per AXIS Camera Station Pro.

1. Andare in **Configuration (Configurazione) > Security (Sicurezza) > User permissions (Autorizzazioni utente)**.
2. Selezionare utente o gruppo.
3. Selezionare **Audio listen (Ascolta con audio)** o **Audio speak (Parla con audio)** per un dispositivo specifico.
4. fare clic su **Applica**;

## Audio assente nelle sequenze

Si può eseguire l'attivazione o la disattivazione dell'audio nei profili di streaming. Per ulteriori informazioni, consultare *Profili di flusso, on page 55*.

## Audio assente in riproduzione

Durante la riproduzione, l'audio è disponibile se è stato attivato nel profilo utilizzato per la registrazione.

Nota

Non si può usare l'audio con i video M-JPEG. Selezionare un altro formato video.

Per usare l'audio nelle registrazioni:

1. Andare a **Configuration > Devices > Stream profiles (Configurazione > Dispositivi > Profili di streaming)** per impostare il formato video per il profilo video che si vuole usare.
2. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Metodo di registrazione**.
3. Selezionare la telecamera.
4. Selezionare il profilo che è stato configurato dal menu a discesa **Profile (Profilo)**.

5. fare clic su **Applica**;

**Registrazioni attivate da regole**

Per abilitare l'audio in una regola esistente:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. selezionare la regola e fare clic su **Modifica**;
3. Fare clic su **Next (Avanti)** per andare ad **Actions (Azioni)**.
4. Selezionare l'azione **Record (Registra)** e fare clic su **Edit (Modifica)**.
5. Selezionare un profilo che usi l'audio.
6. fare clic su **Fine** per salvare.

## Accedi

### Impossibile effettuare l'accesso o connettersi al server

Questa sezione descrive i problemi di accesso e di connessione a un singolo server. Se è stato effettuato l'accesso a più server, il client si avvia e mostra lo stato della connessione sulla barra di stato. Per ulteriori informazioni sullo stato di connessione, vedere *Stato connessione, on page 132*.

| | |
|---|---|
| Nome utente o password non corretta | • Rivedere l'ortografia o utilizzare un altro account.<br>• Verificare che l'utente disponga dei diritti di accesso al server AXIS Camera Station Pro.<br>• Gli orologi del server e del client AXIS Camera Station Pro devono essere sincronizzati. Per gli utenti del dominio, l'orologio del server del dominio deve essere sincronizzato con il server e il client.<br>• Un utente che non è stato aggiunto al server ma è un membro del gruppo degli amministratori locali deve eseguire il client come amministratore.<br>• Per ulteriori informazioni sui diritti di accesso dell'utente, vedere *Autorizzazioni utente, on page 136*. |
| Un utente non è autorizzato ad accedere al server | Aggiungere l'utente nella finestra di dialogo **User permissions (Autorizzazioni utente)**. |
| Impossibile verificare la sicurezza del messaggio | L'ora UTC del server e del client devono essere ragionevolmente sincronizzate. Regolare l'ora del client e del server in modo che la differenza massima fra entrambe sia di 3 ore. |
| Nessun contatto con il server | • Assicurarsi che il computer server possa essere collegato in rete.<br>• Assicurarsi che il computer server sia in esecuzione.<br>• Assicurarsi che il firewall sia configurato correttamente.<br>• Controllare l'ortografia dell'indirizzo del server.<br>• Controllare le impostazioni proxy del client. |
| Nessuna risposta dal server | Assicurarsi di connettersi al computer corretto e che il server AXIS Camera Station Pro sia in esecuzione. |
| Il client non può collegarsi al server | Verificare che la rete sia configurata correttamente:<br>• Verificare che il SO sia supportato. Per un elenco completa dei sistemi operativi supportati, andare alle *note sul rilascio*. |

| | |
|---|---|
| | • Dal Service Control, verificare che il server AXIS Camera Station Pro sia in esecuzione o avviarlo, se necessario.<br>• Verificare che il client e il server siano collegati alla stessa rete. In caso contrario, il client dovrebbe utilizzare l'indirizzo IP esterno del server.<br>• Sul computer server, effettuare la configurazione delle impostazioni del proxy del server in Opzioni Internet di Windows.<br>• Configurare l'impostazione proxy del client nella pagina di accesso, selezionare **Change proxy settings (Modifica impostazioni proxy)**.<br>• Sul computer client, effettuare la configurazione delle impostazioni del proxy client nelle Opzioni internet di Windows. |
| Impossibile connettersi al server | • Assicurarsi che l'indirizzo e la porta del server AXIS Camera Station Pro siano corretti. Verificare che l'intervallo di porte sia impostato correttamente in Service Control.<br>• Assicurarsi che NAT, firewall o software antivirus non blocchino la connessione al server. Per ulteriori informazioni, consultare *Domini e porte per Secure Remote Access v2, on page 219*.<br>• Usare il controllo del servizio AXIS Camera Station Pro per verificare che il server sia in esecuzione.<br>– Aprire Service control AXIS Camera Station Pro vedere *Aprire il AXIS Camera Station Pro service control, on page 214*.<br>– Visualizzare lo stato del server nella scheda **General (Generale)**. Se lo stato è **Stopped (Arrestato)**, fare clic su **Start (Avvia)** per avviare il server. |
| Impossibile trovare il server | • Assicurarsi che il computer server possa essere collegato alla rete.<br>• Assicurarsi che l'indirizzo e la porta del server AXIS Camera Station Pro siano corretti.<br>• Assicurarsi che NAT, firewall o software antivirus non blocchino la connessione al server.<br>• Verificare che le impostazioni DNS del tuo client siano corrette.<br>• Verificare che il Sever DNS contenga una voce relativa al nome host e all'indirizzo IP del server. |
| Impossibile connettersi al server | Verificare che computer server e rete non siano sovraccarichi. |
| La versione del client e del server differiscono | Aggiornare il server in modo che esegua la stessa versione del client. |
| Il server AXIS Camera Station Pro locale non viene eseguito | Utilizzare il Service Control per avviare AXIS Camera Station Pro, o selezionare un server remoto a cui accedere. |
| Su questo computer non è installato il server AXIS Camera Station Pro | Installare il server AXIS Camera Station Pro o scegliere un altro server. |
| L'elenco dei server selezionato è vuoto | Per aggiungere server all'elenco, fare clic su **Edit (Modifica)** accanto alla selezione dell'elenco dei server. |

## Licenze

### Problemi di registrazione licenza

Se la registrazione automatica non va a buon fine, provare le seguenti operazioni:

- Verificare che il sistema sia registrato in un'organizzazione.
- Andare a **Configuration (Configurazione)** e assicurarsi che l'opzione **Automatic licensing (Licenza automatica)** sia attiva. Vedere *Gestisci le licenze, on page 135*.
- Verificare che l'ora del server sia aggiornata.

Per ulteriori informazioni, vedere *AXIS Camera Station Pro - Guida all'installazione e alla migrazione*.

## Utenti

### Impossibile trovare gli utenti del dominio

Se la ricerca degli utenti del dominio non ha esito positivo, cambiare l'account di accesso al servizio:

1. Aprire il **Pannello di controllo di Windows**.
2. Cercare "Servizi".
3. Fare clic su **View local services (Visualizza servizi locali)**.
4. Fare clic con il pulsante destro del mouse su AXIS Camera Station Pro e selezionare **Properties (Proprietà)**.
5. Fare clic sulla scheda **Log on (Accesso)**.
6. Modificare la selezione da **Account di sistema locale** ad **Account**.
7. selezionare un utente con accesso a Windows Active Directory.

## Errori di certificato

Risolvere gli errori del certificato non appena si verificano. Gli errori del certificato del dispositivo impediscono ad AXIS Camera Station Pro di comunicare con il dispositivo. Un errore dell'autorità di certificazione impedisce l'avvio del server.

| Possibili errori | |
|---|---|
| Certificato non trovato | Se si conosce la ragione, fare clic su **Repair (Ripara)**. Se si sospetta un accesso non autorizzato, approfondire il problema prima di ripristinare il certificato. Fare clic su **Advanced (Avanzate)** per visualizzare dettagli sul certificato. Ragioni possibili per rimuovere il certificato:<br>• il dispositivo è stato reimpostato ai valori predefiniti di fabbrica;<br>• la comunicazione sicura HTTPS è stata disabilitata.<br>• il dispositivo ha subito modifiche a seguito di accesso non autorizzato. |
| Certificato non attendibile | Se si conosce la ragione, fare clic su **Trust This Device (Considera attendibile questo dispositivo)**. In caso contrario, approfondire il problema prima di considerare attendibile il certificato. Fare clic su **Advanced (Avanzate)** per visualizzare dettagli sul certificato. |
| Errore dell'autorità di certificazione | AXIS Camera Station Pro non è possibile utilizzare l'autorità di certificazione per emettere nuovi certificati, ad esempio perché non è in grado di decriptare la chiave privata. Se AXIS Camera Station Pro ha creato l'autorità di certificazione ne genera automaticamente una nuova. Se l'autorità di certificazione è stata importata, andare a **Service Control > Tools (Controllo servizi, Strumenti)** e fre clic su **Reset (Ripristina)** nella sezione **Reset certificate authority (Ripristina autorità di certificazione)**. |

### Password mancante per autorità di certificazione

Se si dispone di un'autorità di certificazione in AXIS Camera Station Pro senza una password memorizzata, appare il seguente allarme:

| |
|---|
| **È necessario indicare una password per il certificato della Autorità di certificazione. Read the user manual for more information. (Devi fornire una passphrase per il certificato dell'autorità di certificazione. Per ulteriori informazioni, vedere il manuale per l'utente.)** |

È possibile risolvere questo problema in tre modi:

- Attivare HTTPS su un dispositivo
- Importa un'autorità di certificazione esistente
- Generare una nuova autorità di certificazione

Per attivare HTTPS su un dispositivo:

1. Andare a **Configurazione > Dispositivi > Gestione**.
2. Nella lista, fare clic con il pulsante destro del mouse su un dispositivo e selezionare **Security > HTTPS > Enable/Update (Sicurezza, HTTPS, Abilita/aggiorna)**.
3. Fare clic su **Sì** per confermare.
4. Inserire la password dell'autorità di certificazione.

5. Fare clic su **OK**.

Per importare un'autorità di certificazione esistente:

1. Andare a **Configuration > Security > Certificates > Devices** (Configurazione, Sicurezza, Certificati, dispositivi).
2. In HTTPS, disattivare **Validate device certificate** (Convalida certificato del dispositivo).
3. In **Certificate authority (Autorità di certificazione)**, fare clic su **Import (Importa)**.
4. Inserire la password e fare clic su **OK**.
5. Selezionare il numero di giorni di validità dei certificati client/server firmati.
6. Andare a **Configurazione > Dispositivi > Gestione**.
7. Fare clic con il pulsante destro del mouse sui dispositivi e selezionare **Security > HTTPS > Enable/ Update (Sicurezza > HTTPS > Abilita/Aggiorna)**.
8. Andare a **Configuration > Security > Certificates > Devices (Configurazione, Sicurezza, Certificati, Dispositivi)** e abilitare **Validate certificate device (Convalida certificato dispositivo)**.

Nota

AXIS Camera Station Pro perde la sua connessione ai dispositivi e alcuni componenti di sistema si riavviano.

Per consentire a AXIS Camera Station Pro di generare una nuova autorità di certificazione:

1. Andare a **Configuration > Security > Certificates > Devices** (Configurazione, Sicurezza, Certificati, dispositivi).
2. In HTTPS, disattivare **Validate device certificate** (Convalida certificato del dispositivo).
3. In **Certificate authority (Autorità di certificazione)**, fare clic su **Generate (Genera)**.
4. Inserire la password e fare clic su **OK**.
5. Selezionare il numero di giorni di validità dei certificati client/server firmati.
6. Andare a **Configurazione > Dispositivi > Gestione**.
7. Fare clic con il pulsante destro del mouse sui dispositivi e selezionare **Security > HTTPS > Enable/ Update (Sicurezza > HTTPS > Abilita/Aggiorna)**.
8. Andare a **Configuration > Security > Certificates > Devices (Configurazione, Sicurezza, Certificati, Dispositivi)** e abilitare **Validate certificate device (Convalida certificato dispositivo)**.

Nota

AXIS Camera Station Pro perde la sua connessione ai dispositivi e alcuni componenti di sistema si riavviano.

## Sincronizzazione dell'ora

### Il servizio Ora di Windows non è in esecuzione

Il servizio Ora di Windows e il server NTP non sono sincronizzati. Ciò può essere dovuto al fatto che il servizio Ora di Windows non riesce a connettersi al server NTP.

- Verificare che il server NTP sia online.
- Controllare che le impostazioni del firewall siano esatte.
- Controllare che il dispositivo sia su una rete in grado di raggiungere il server NTP.

Per ottenere supporto, contatta l'amministratore di sistema.

### Differenza oraria rilevata su un dispositivo

Il dispositivo non è sincronizzato con l'ora del server. L'indicazione di data e ora della registrazione mostra l'ora in cui il server l'ha ricevuta anziché l'ora di registrazione da parte del dispositivo.

1. Andare a **Configuration > Devices > Time synchronization (Configurazione > Dispositivi > Sincronizzazione ora)** e verificare l'offset dell'ora server del dispositivo.
2. Se l'offset dell'ora del server è maggiore di 2 secondi:
   2.1. Selezionare **Enable time synchronization (Abilita sincronizzazione ora)**.
   2.2. Controllare che il dispositivo sia in grado di raggiungere il server NTP specificato.
   2.3. Ricarica il dispositivo in **Configuration > Devices > Management (Configurazione > Dispositivi > Gestione)**.
3. Se l'offset dell'ora server è inferiore a 2 secondi, è possibile che il dispositivo non invii dati sufficienti per sincronizzare l'ora.
   3.1. Deselezionare **Send alarm when the time difference between server and device is larger than 2 seconds (Invia allarme quando la differenza di orario tra server e dispositivo è superiore a 2 secondi)** per disattivare gli allarmi.

Per ricevere aiuto, contatta l'assistenza Axis.

## Secure Remote Access v2

### Impossibile connettersi ai servizi cloud localmente

Per risolvere i problemi di connettività con i servizi cloud:

1. Aprire AXIS Camera Station Pro e andare a **Configuration (Configurazione)** > **Connected services (Servizi connessi)** > **Management (Gestione)**.
2. Verificare che **Status (Stato)** sia in verde. In caso contrario, controllare la connessione a Internet.
3. Se il problema persiste, contattare il supporto di Axis per assistenza.

### Impossibile connettersi ai servizi cloud da remoto

In AXIS Camera Station Pro:

1. Andare a **Menu (Menu)** > **Help (Guida)** e fare clic su **Status of Axis services (Stato dei servizi Axis)**. Si aprirà la pagina di stato di *https://status.axis.com*, in cui è possibile controllare le notifiche di manutenzione o i tempi di inattività programmati.
2. Nella sezione Axis Camera Station Pro, espandere l'elenco a discesa per verificare se i servizi cloud sono accessibili.
3. Verificare che l'invito per l'account My Axis sia ricevuto dall'organizzazione corretta.

In AXIS Camera Station Pro Mobile App:

1. Andare a **More (Altro)** > **Help section (Sezione guida)** e fare clic su **Status of Axis services (Stato dei servizi Axis)**. Si aprirà la pagina di stato di *https://status.axis.com*, in cui è possibile controllare le notifiche di manutenzione o i tempi di inattività programmati.
2. Controllare che la connessione a Internet sia stabile. Provare a eseguire il test con un dispositivo mobile diverso per identificare la causa del problema.
3. Verificare che l'invito per l'account My Axis sia ricevuto dall'organizzazione corretta.

Se il problema persiste, contattare il supporto di Axis per assistenza.

### Problemi generali di perdita di pacchetti, latenza o instradamento errato

1. Assicurarsi di poter accedere a Internet. Le principali porte utilizzate sono 80 e 443 e devono essere aperte anche per il traffico in uscita.
2. A seconda del router, potrebbe essere necessario aprire i seguenti domini extra con le porte:
   - https://eu.login.connect.axis.com con porta 433
   - https://eu.cs.connect.axis.com con porta 433

- https://api.vms.axis.cloud con porta 433
- wss://signaling.prod.webrtc.connect.axis.com con porta 433
- https://*.turn.prod.webrtc.connect.axis.com con porte 443, 3478, 5349 e 49152-65535

Nota

L'asterisco " * " è dinamico e consiste in una combinazione di ID regione e ID server non statici).

Per ulteriore assistenza, contattare l'assistenza Axis.

## Assistenza tecnica

L'assistenza tecnica è disponibile per i clienti che possiedono una versione con licenza di AXIS Camera Station Pro. Per contattare l'assistenza tecnica, andare su > **Help > Online Support (Guida > Supporto online)** o *axis.com/support*.

Si consiglia di allegare il report di sistema e alcune schermate alla richiesta di supporto.

Andare a > **Help > System report (Guida > Report di sistema)** per creare un report di sistema.

### Processo di escalation

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

- Una descrizione chiara su come riprodurre il problema o delle circostanze nelle quali si verifica.
- L'ora in cui si è verificato il problema e, in caso, il nome o l'indirizzo IP della telecamera interessata.
- report di sistema AXIS Camera Station Pro generato direttamente dopo che si è verificato il problema. Il report di sistema deve essere generato dal client o dal server in cui è stato riprodotto tale problema. Se il problema si ripresenta in modo prevedibile, abilitare la registrazione di debug sia per il server che per il client, in modo da acquisire informazioni più complete sul problema. Ricordarsi di disattivare la registrazione dei messaggi di debug quando è arrivata la fine.

Per alcune questioni, il team di assistenza potrebbe richiedere ulteriori informazioni.

Nota

Se il file supera 1 GB, come ad esempio un'analisi di rete o i file di database, usare un servizio di condivisione file sicuro che si considera attendibile per inviare il file.

| Informazioni aggiuntive | |
|---|---|
| Log a livello di debug | I log a livello di debug sono disabilitati per impostazione predefinita, poiché la dimensione del file di log è limitata. Se si abilita la registrazione a livello di debug, ricordarsi di disabilitarla una volta generato il rapporto di sistema.<br><br>Server: **Configuration > Server > Settings > Enable debug logging (Configurazione, Server, Impostazioni, Abilita registrazione di debug**<br>Client: **Configuration > Client > Settings > Enable debug logging (Configurazione, Client, Impostazioni, Abilita registrazione di debug)** |
| Sovrapposizione di debug per la visualizzazione in diretta e la riproduzione | Quando si verifica un problema con la visualizzazione in diretta o la riproduzione, è utile disporre di una registrazione dello schermo che mostri la sovrapposizione testo di debug. Questa registrazione dovrebbe acquisire l'intero schermo, compreso |

| Informazioni aggiuntive | |
|---|---|
| | l'orologio di sistema, in modo da poter risalire al problema nei log.<br>• Premere una volta Ctrl + I per mostrare le informazioni in sovrapposizione nella visualizzazione in diretta.<br>• Premere due volte Ctrl + I per aggiungere informazioni di debug.<br>• Premere tre volte Ctrl + I per nascondere la sovrapposizione testo. |
| File del database | Utilizzarlo , nei casi in cui è necessario esaminare o riparare manualmente il database. Selezionare **Include database in the report (Includi database nel report)** prima di generare il report di sistema. Inserire questa riga ogni volta che si verifica un problema con l'avvio del servizio AXIS Camera Station. |
| Schermate | Quando si aggiungo degli screenshot, acquisire l'intera schermata per fornire un contesto più completo. Se si ritiene che lo screenshot a schermo intero sia ambiguo, indicare l'area di messa a fuoco con delle frecce. |
| Screen recordings (Registrazioni schermo) | Utilizzare le registrazioni dello schermo quando il problema è difficile da descrivere a parole, ad esempio quando la riproduzione del problema comporta numerose interazioni nell'interfaccia utente. |
| File di registrazione | Il servizio di assistenza potrebbe chiederti di fornire alcuni esempi dei file .acsm e .acsi che AXIS Camera Station utilizza per archiviare le registrazioni. Ciò vale in caso di problemi con la riproduzione o l'esportazione delle registrazioni, oppure in caso di problemi con AXIS File Player. È possibile trovare questi file nel punto di archiviazione che è stato selezionato per ciascuna telecamera. |

T10196821_it

2026-09 (M35.4)

© 2023 – 2026 Axis Communications AB