AXIS Camera Station 5

Manuale dell'utente

Informazioni su AXIS Camera Station 5

AXIS Camera Station 5 è un sistema di monitoraggio e registrazione completo per installazioni di piccole e medie dimensioni.

È compatibile con tutte le versioni di AXIS OS attualmente supportate nei percorsi attivi, di Supporto a lungo termine (LTS) e di Supporto specifico per il prodotto (PSS)*. Per ulteriori informazioni, consultare le note di rilascio di AXIS Camera Station 5 o il portale *AXIS OS Portal*. Per verificare quali prodotti funzionano con AXIS Camera Station 5, vedere *Compatible products* (Prodotti compatibili).

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

Opzioni di accesso

AXIS Camera Station 5 Audio Manager – gestisce tutte le comunicazioni con le telecamere, i video encoder e i dispositivi ausiliari nel sistema. La larghezza di banda totale disponibile limita il numero di telecamere ed encoder con cui può comunicare ciascun server.

AXIS Camera Station 5 client – fornisce accesso alle registrazioni, ai video dal vivo, ai registri e alla configurazione. Il client si può installare su qualsiasi computer, consentendo la visualizzazione e il controllo remoto da Internet o dalla rete aziendale.

App di visualizzazione per dispositivi mobili AXIS – 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. Usa HTTPS per comunicare con il server AXIS Camera Station 5. Configurare le porte per la comunicazione mobile e per lo streaming mobile come descritto nella sezione Impostazioni server in *Generale*. Consulta il *manuale per l'utente di AXIS Camera Station Mobile App* per maggiori informazioni.

Video tutorial

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

Caratteristiche del sistema

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

Novità

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

Collegamenti utili per un amministratore

Ecco alcuni argomenti che potrebbero risultare interessanti per l'utente:

- *Connessione a un server, on page 8*
- *Configurazione dei dispositivi, on page 41*
- *Configurazione dell'archiviazione, on page 70*
- *Configurazione di registrazioni ed eventi, on page 75*
- *Configura servizi connessi, on page 113*
- *Configurare server, on page 116*
- *Configurazione delle licenze, on page 124*
- *Configura sicurezza, on page 127*

Ulteriori manuali

- *Guida AXIS Camera Station Integrator:*
- *Novità di AXIS Camera Station*
- *Guida all'installazione e alla migrazione AXIS Camera Station*
- *App per dispositivi mobili AXIS Camera Station*
- *Guida alle funzionalità di AXIS Camera Station*
- *Video tutorial AXIS Camera Station*
- *Guida alla risoluzione di problemi di AXIS Camera Station*
- *Guida alla protezione del sistema AXIS Camera Station*

Collegamenti utili per un operatore

Ecco alcuni argomenti che potrebbero risultare interessanti per l'utente:

- *Guida introduttiva per AXIS Camera Station per operatori*
- *Connessione a un server, on page 8*
- *Configurazione client, on page 108*
- *Visualizzazione in diretta, on page 12*
- *Riproduzione delle registrazioni, on page 22*
- *Esportazione delle registrazioni, on page 24*
- *Vademecum AXIS Camera Station - revisione ed esportazione*

Avvio rapido

Questo tutorial spiegherà i passaggi per rendere operativo il sistema.

Operazioni preliminari:

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

Per amministratori:

1. *Avviare il video management system*
2. *Aggiunta di dispositivi*
3. *Configura metodo di registrazione, on page 5*

Per gli operatori:

1. *Visualizzazione del video in diretta, on page 5*
2. *Visualizzazioni registrate, on page 6*
3. *Esportazione delle registrazioni, on page 6*
4. *Riproduzione e verifica delle registrazioni in AXIS File Player., on page 6*

Avviare il video management system

Fare doppio clic sull'icona del client AXIS Camera Station 5 per avviare il client. Quando viene avviato per la prima volta, il client tenta di accedere al server AXIS Camera Station 5 installato nello stesso computer del client.

È possibile collegarsi a più server AXIS Camera Station 5 in vari modi. Vedere *Connessione a un server*.

Aggiunta di dispositivi

La pagina **Add devices (Aggiunta di dispositivi)** si apre al primo avvio di AXIS Camera Station 5. AXIS Camera Station 5 cerca i dispositivi connessi nella rete e mostra l'elenco dei dispositivi trovati. Vedere *Aggiunta di dispositivi*.

1. Selezionare le telecamere che si desidera aggiungere dall'elenco. Se non è possibile trovare la telecamera, fare clic su **Manual search (Ricerca manuale)**.
2. Fare clic su **Aggiungi**.
3. Selezionare **Configurazione rapida** o **Configurazione di Site Designer**. Fare clic su **Next (Avanti)**. Vedere *Importazione di progetti Site Designer, on page 44*.
4. Utilizzare le impostazioni predefinite e verificare che il metodo di registrazione sia impostato su **None (Nessuno)**. fare clic su **Install (Installa)**.

Configura metodo di registrazione

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

Visualizzazione del video in diretta

1. Aprire una scheda **Live view (Visualizzazione in diretta)**.

2. Selezionare una telecamera per visualizzarne il video in diretta.

Per ulteriori informazioni, vedere *Visualizzazione in diretta, on page 12*.

Visualizzazioni registrate

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

Per ulteriori informazioni, vedere *Registrazioni, on page 22*.

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 24*.

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)**. Viene visualizzata la pagina dei risultati della verifica.

Nota

- La firma digitale differisce da Video firmato. Il video firmato consente di tracciare il video sulla telecamera da cui proviene, rendendo possibile verificare che la registrazione non sia stata manomessa. 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 5 se il client AXIS Camera Station 5, il server AXIS Camera Station 5 e i dispositivi di rete collegati si trovano su reti diverse.

Impostazioni proxy client

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

1. Aprire il client AXIS Camera Station 5.
2. Fare clic su **Change client proxy settings (Cambia le impostazioni proxy del client)**.
3. Cambia le impostazioni proxy del client. Vedere *Impostazioni proxy client*.
4. Fare clic su **OK**.

Impostazioni proxy del server

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

1. Aprire il AXIS Camera Station 5 Service Control.
2. Selezionare **Modify settings (Modifica impostazioni)**.
3. Nella sezione Impostazioni proxy, utilizzare l'**System account internet option (Opzione Internet account di sistema)** predefinita oppure selezionare **Use manual proxy settings (Utilizza impostazioni proxy manuali)**. Vedere *Generale*.
4. Fare clic su **Save (Salva)**.

NAT and Firewall (NAT e Firewall)

Quando un NAT, un firewall o un dispositivo simile separa il client e il server, configurare il NAT o il firewall per garantire che la porta HTTP, la porta TCP e la porta di streaming specificate in AXIS Camera Station 5 Service Control possano passare attraverso il firewall o il NAT. Contattare l'amministratore di rete per istruzioni su come configurare il NAT o il firewall.

Per ulteriori informazioni, vedere *Elenco porta per AXIS Camera Station 5, on page 186*.

Configurazione della porta del server

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

Per ulteriori informazioni, vedere *Generale* oppure *FAQ*.

Considerazioni sulla protezione

Per evitare accessi non autorizzati alle telecamere e alle registrazioni, tenere presente quanto segue:

- Usare password complesse per tutti i dispositivi di rete (telecamere, video encoder e dispositivi ausiliari).
- Installare il server, le telecamere, i video encoder e i dispositivi ausiliari di AXIS Camera Station 5 su una rete protetta separata da una rete d'ufficio. È possibile installare il client AXIS Camera Station 5 su un computer in un'altra rete, ad esempio una rete con accesso a Internet.
- Assicurarsi che tutti gli utenti dispongano di password complesse. Windows® Active Directory offre un livello elevato di protezione.

Connessione a un server

Utilizzando il client AXIS Camera Station 5 è possibile connettersi a più server o a un singolo server installato sul computer locale oppure in un'altra posizione nella rete. È possibile collegarsi ai server AXIS Camera Station 5 in vari modi:

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

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

Server remoto – Vedere *Connessione a un server remoto, on page 8*.

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

Nota

Quando si tenta di connettersi a un server per la prima volta, il client controlla l'ID del certificato del server. Per assicurarsi che ci si stia connettendo al server corretto, verificare manualmente l'ID del certificato con quello visualizzato in AXIS Camera Station 5 Service Control. Vedere *Generale, on page 185*.

Elenco dei server	Per connettersi ai server da un elenco di server, selezionarne uno dal menu a discesa **Server list (Elenco dei server)**. Fare clic su per creare o modificare gli elenchi di server. Vedere *Elenchi dei server*.
Importa lista dei server	Per importare un file contenente un elenco di server esportati da AXIS Camera Station 5, 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 salvati su tutti i server collegati, fare clic su **Delete saved passwords (Elimina password salvate)**.
Cambia le impostazioni proxy del client	Potrebbe essere necessario modificare le impostazioni proxy del client per connettersi a un server, fare clic su **Change client proxy settings (Cambia le impostazioni proxy del client)**. Vedere *Impostazioni proxy client*.

Connessione a un server remoto

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

Accedi ad AXIS Secure Remote Access

Importante

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

Cosa significa tutto ciò per il vostro sistema AXIS Camera Station 5?

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

Nota

- Il server non può aggiornare il client automaticamente durante un tentativo di connessione a un server attraverso Axis Secure Remote Access.
- Se il server proxy si trova tra il dispositivo di rete e il server AXIS Camera Station 5, è necessario configurare le impostazioni proxy in Windows sul server AXIS Camera Station 5 per accedere al server utilizzando AXIS Secure Remote Access.

1. Fare clic sul collegamento **Accedi ad AXIS Secure Remote Access**.
2. Immettere le credenziali dell'account My Axis. Vedere *Axis Secure Remote Access*.
3. Fai clic su **Accedi**.
4. Fare clic su **Grant (Concedi)**.

Impostazioni proxy client

Queste impostazioni si applicano a un server proxy che si trova tra il client AXIS Camera Station 5 e il server AXIS Camera Station 5.

Nota

Utilizzare AXIS Camera Station 5 Service Control per configurare le impostazioni proxy di un server proxy presente tra un server AXIS Camera Station 5 e le telecamere di rete. Vedere *AXIS Camera Station 5 controllo servizio*.

Selezionare l'opzione appropriata per la configurazione.

- **Direct connection (Connessione diretta)**: Selezionare questa opzione se non sono presenti server proxy tra il client AXIS Camera Station 5 e il server AXIS Camera Station 5.
- **Use Internet Options settings (Usa le impostazioni Opzioni Internet)** (impostazione predefinita): selezionare questa opzione per utilizzare le impostazioni Windows.
- **Use manual proxy settings (Utilizza impostazioni proxy manuali)**: selezionare questa opzione per configurare le impostazioni proxy manualmente. Fornire le informazioni necessarie nella sezione Impostazioni manuali.
  - **Indirizzo**: immettere l'indirizzo o il nome host del server proxy.
  - **Porta**: immettere il numero di porta del server proxy.
  - **Do not use proxy server for addresses beginning with (Non utilizzare il server proxy per gli indirizzi che iniziano con)**: immettere i server a cui il proxy non deve accedere. Utilizzare il punto e virgola per separare le voci. È possibile utilizzare caratteri jolly per gli indirizzi o i nomi host, ad esempio: "192.168.*" o "*.ilmiodominio.com".
  - **Always bypass proxy server for local addresses (Escludi sempre il server proxy per gli indirizzi locali)**: selezionare questa opzione per escludere il proxy quando si esegue la connessione a un server sul computer locale. Gli indirizzi locali non hanno un'estensione per il nome di dominio, ad esempio http://webserver/, http://localhost, http://loopback, o http://127.0.0.1.

AXIS Camera Station 5 client

Quando si utilizza AXIS Camera Station 5 per la prima volta, si apre la pagina Aggiungi dispositivi nella scheda Configurazione. Vedere *Aggiunta di dispositivi*.

Schede

Visualizzazione in diretta	Visualizzare video in diretta dalle telecamere collegate. Vedere *Visualizzazione in diretta*.
Registrazioni	trova, riproduce ed esporta le registrazioni. Vedere *Registrazioni*.
Ricerca intelligente 1	Individuare con rapidità eventi importanti 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 38*.
Configurazione	amministrazione e manutenzione di dispositivi collegati, nonché impostazioni per il client e i server. Vedere *Configurazione*.
Tasti di scelta rapida	un elenco dei tasti di scelta rapida per le azioni. 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 del sistema. Vedere *Gestione degli accessi, on page 160*.
Ricerca intelligente 2	Usare i filtri avanzati per individuare veicoli e persone sulla base delle caratteristiche. Vedere *Ricerca intelligente 2, on page 34*.
Monitoraggio dell'integrità del sistema	Eseguire il monitoraggio dei dati di integrità da uno o più sistemi AXIS Camera Station 5. Vedere *Monitoraggio dell'integrità del sistema BETA, on page 169*.
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 5 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	Aprire le opzioni relative alla Guida. Andare a **Help (Guida)** > **About (Informazioni)** per vedere quale versione di client AXIS Camera Station 5 è in uso.
Esci	Disconnettersi dal server e uscire dal client AXIS Camera Station 5.
Esci	Uscire e chiudere il client AXIS Camera Station 5.

Barra del titolo

? o F1	Aprire la Guida.
	Attivare la modalità a schermo intero.
 o ESC	Uscire dalla modalità schermo intero.

Barra di stato

La barra di stato può includere quanto segue:

- viene visualizzata un'icona di avviso quando l'orario del client e del server non corrisponde. Assicurarsi che l'orario nel client sia sincronizzato con l'orario del server per evitare problemi di sequenza temporale.
- 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 .
- L'utilizzo dell'accesso remoto protetto mostra la quantità di dati rimasti o la quantità di copertura utilizzata questo mese per la quantità inclusa nel livello di servizio. Vedere *Axis Secure Remote Access*.
- **AXIS Camera Station 5 update available (Aggiornamento disponibile)** appare quando c'è una nuova versione se sei connesso come amministratore. Vedere *Aggiorna AXIS Camera Station 5, on page 119*.

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 le viste, le telecamere e i video in diretta dalle telecamere collegate e mostra tutte le viste e le telecamere dei server connessi, raggruppate in base al nome del server quando ci si connette a più server AXIS Camera Station 5.

Le viste offrono l'accesso a tutti i dispositivi e le telecamere aggiunti ad AXIS Camera Station 5. 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.

Tutti gli utenti sono in grado di accedere alle viste. Per informazioni sui diritti di accesso dell'utente, vedere *Autorizzazioni utente, on page 127*.

Per saperne di più su come si configura la 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 su telecamere, visualizzazioni o sequenze 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 9 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 informazioni su come 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 sapere come si rimuovono le telecamere da AXIS Camera Station 5, vedere *Telecamere, on page 47*.
🔒	In qualità di amministratore, è possibile bloccare la vista e impedire agli operatori o alle viste di spostarsi o modificare la vista.

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).
Add snapshot to export (Aggiungi istantanea da esportare)	Per eseguire l'aggiunta di un'istantanea all'elenco di esportazione nella scheda Esporta, 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 le telecamere PTZ e per le 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 dell'immagine, 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 nell'immagine dal vivo, spostare il cursore al centro dell'immagine per visualizzare la freccia di navigazione. Quindi, fare clic e tenere premuto per eseguire una rotazione in direzione della freccia di navigazione. Per eseguire la rotazione e l'inclinazione nell'immagine a maggiore velocità, fare clic e tenere premuto per allungare la freccia di navigazione.
Imposta messa a fuoco	Per regolare la messa a fuoco della telecamera, fare clic con il pulsante destro del mouse sull'immagine e selezionare **Set focus (Imposta messa a fuoco)**. Fare clic su **AF** per mettere a fuoco la videocamera automaticamente. Per regolare la messa a fuoco manualmente, selezionare i lati delle barre **Vicino** e **Lontano**. Utilizzare **Vicino** per mettere a fuoco gli

	oggetti vicini alla telecamera. Utilizzare **Lontano** per mettere a fuoco oggetti lontani.
Zona di richiamo messa a fuoco	Per aggiungere o rimuovere la zona di richiamo messa a fuoco, fare clic con il pulsante destro del mouse sull'immagine, 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 con il pulsante destro, selezionare **Autotracking 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 *Preimpostazioni 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 per un posizionamento ripetibile. 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*.



Aggiungi preset digitali



Comandi PTZ

Nota

Gli amministratori possono 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 la riproduzione di 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

Gli amministratori sono in grado di 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 48*.

 **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 111*.

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 web, mappe e altre viste suddivise nella vista suddivisa.

Nota

Quando ci si connette a più server AXIS Camera Station 5, 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 Visualizzazione in diretta, fare clic su .
2. Selezionare **Nuova vista suddivisa**.
3. inserire un nome per l'immagine suddivisa;
4. Selezionare un modello che si desidera utilizzare dal menu a discesa **Template (Modello)**.
5. Trascinare e rilasciare una o più viste, zone audio, o telecamere nella griglia.
6. Fare clic su **Save view (Salva vista)** per salvare l'suddivisione sul server corrente.

Configura hotspot	Per definire un riquadro dell'hotspot, fare clic con il pulsante destro del mouse e selezionare **Set hotspot (Imposta hotspot)**. Quando si fa clic su un altro riquadro, questo si apre nell'hotspot. Gli hotspot sono comodi per suddivisioni dell'immagine asimmetriche composte da un grande fotogramma e diversi fotogrammi più piccoli. Il fotogramma più ampio viene definito generalmente hotspot.
Profilo di streaming	Per impostare il profilo di streaming per la telecamera, fare clic con il pulsante destro del mouse nella vista a griglia e selezionare **Stream profile (Profilo di streaming)**. Vedere *Profili di flusso*.



Aggiunta di un'immagine suddivisa

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 le transazioni recenti in una suddivisione dell'immagine.

1. Aggiunta di una porta. Vedere *Aggiunta di una porta, on page 137*.
2. Aggiungere il dashboard porta a una suddivisione dell'immagine, vedere *Suddivisione dell'immagine, on page 16*.

Dashboard	Per visualizzare i dettagli della porta, lo stato della porta e lo stato di blocco, aprire la scheda **Dashboard (Dashboard)**. La scheda Dashboard visualizza le seguenti informazioni: • Gli eventi di controllo degli accessi con i dettagli del titolare della tessera, inclusa la foto, ad esempio, quando un titolare passa una tessera. • Gli allarmi con le informazioni di attivazione degli allarmi, ad esempio, quando una porta è aperta troppo a lungo. • 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, la porta viene sbloccata nello stesso modo che farebbe se qualcuno presentasse le proprie credenziali, il che significa che

	la porta si blocca automaticamente dopo un tempo impostato.
Serratura	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)**.



Monitoraggio e assistenza nel dashboard delle porte

Sequenza

Una sequenza passa da una vista all'altra.

Nota

Quando ci si connette a più server AXIS Camera Station 5, è possibile aggiungere alla propria sequenza qualsiasi vista, telecamera o dispositivo di altri server.

Per aggiungere una sequenza:

1. Nella scheda 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. Disporre le immagini nell'ordine desiderato per la sequenza.
6. Facoltativamente, impostare i singoli tempi di attesa per ogni vista.
7. Per le telecamere con funzionalità PTZ, selezionare un preset PTZ dall'elenco a discesa **Preset PTZ**. Vedere *Preimpostazioni PTZ*.
8. Fare clic su **Save view (Salva vista)** per salvare la sequenza sul server corrente.

Tempo di interazione	Il tempo di attesa è il numero di secondi per cui una vista viene mostrata prima di passare a quella successiva. È possibile impostare questa opzione singolarmente per ogni vista.



Aggiunta di una sequenza

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 5 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, 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 della mappa. Vedere *Creazione di trigger dei pulsanti di azione*.

Nota

Quando ci si connette a più server AXIS Camera Station 5, è possibile aggiungere alla propria vista della mappa qualsiasi vista, telecamera o dispositivo di altri server.

Per aggiungere una mappa:

1. Nella scheda 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. Le dimensioni massime del file sono di 20 MB e sono supportati i formati BMP, JPG, PNG, GIF.
5. Trascinare le viste, le telecamere, gli altri dispositivi e le porte sulla mappa.
6. Fare clic su un'icona sulla mappa per modificare 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.

Nota

È possibile modificare alcune impostazioni per più icone ed etichette allo stesso tempo.

8. Fare clic su **Save view (Salva vista)** per salvare la mappa sul server corrente.

	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.
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.
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.
Area di copertura	Questa opzione è disponibile solo per le telecamere e altri dispositivi. 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 **Flash (Lampeggio)** se si vuole che l'area di copertura lampeggi quando la telecamera registra come conseguenza dell'attivazione da rilevamento movimento o da altre regole di azione. Nella pagina delle impostazioni del client, si può eseguire la disattivazione delle aree di copertura lampeggianti globalmente per tutti i dispositivi, vedere *Impostazioni client, on page 108*.
Rimuovi	Fare clic su per rimuovere l'icona dalla mappa.

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

Aggiunta di una mappa

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

Attivazione dell'audio da una mappa

Pagina Web

Una vista pagina Web mostra una pagina Internet. È possibile aggiungere una pagina Web, ad esempio, a una suddivisione dell'immagine o a una sequenza.

Per aggiungere una pagina web:

1. Nella scheda Visualizzazione in diretta, fare clic su +.
2. Selezionare **New webpage (Nuova pagina web)**.
3. Immettere un nome per la pagina Web.
4. Immettere l'URL completo della pagina Web.
5. Fare clic su **OK**.



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 Registrazioni si possono gestire le ricerche, la riproduzione e l'esportazione delle registrazioni. La scheda consiste di una vista della registrazione e due pannelli dove si possono trovare viste, immagini, strumenti di riproduzione e telecamere dei server collegati raggruppati per nome del server, vedere *Visualizzazione in diretta*.

Dalla vista principale della registrazione si può eseguire la gestione dell'immagine come nella visualizzazione in diretta. Per saperne di più, andare a *Gestione dell'immagine nella visualizzazione in diretta, on page 13*.

Per cambiare metodo e impostazioni delle registrazioni, 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 5. Si deve modificare il tempo di conservazione in **Configuration > Storage > Selection (Configurazione > Archiviazione > Selezione)** per eliminare le registrazioni precedenti.

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

Usare la sequenza temporale per navigare nella riproduzione e scoprire quando è accaduta una registrazione. Una linea rossa nella sequenza temporale simbolizza una registrazione con rilevamento movimento. Una linea blu nella sequenza temporale simbolizza una registrazione attivata da una regola di azione. 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. In una registrazione, spostare la sequenza temporale (ripulitura) per avere una panoramica del contenuto e individuare occorrenze specifiche.

Trovare registrazioni

	Fare clic per eseguire la selezione di una data e di un'ora nella sequenza temporale.
	Usare il filtro per eseguire la configurazione del tipo di registrazioni da mostrare nella sequenza temporale.
	Usare per individuare i segnalibri salvati, vedere *Segnalibri*.
 **Ricerca intelligente 1**	Impiega la ricerca intelligente per cercare le registrazioni, consulta *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).
	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 sull'immagine e scorrere in alto o in basso per eseguire ingrandimenti e rimpicciolimenti dell'immagine e spostare la vista per visualizzare parti diverse dell'immagine. Per ingrandire un'area, posizionare il cursore sull'area desiderata e scorrere per eseguire lo zoom.

Segnalibri

Nota

- Non si può cancellare una registrazione bloccata se non si sblocca in modo manuale.
- Il sistema elimina le registrazioni bloccate quando si rimuove la telecamera da AXIS Camera Station 5.

	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.
	Cambiare il nome del segnalibro, la descrizione ed eseguire lo sbloccaggio o il bloccaggio della registrazione.

	Rimuovere un segnalibro. Per rimuovere dei segnalibri multipli, selezionare più segnalibri e tenere premuto CTRL o MAIUSC per la rimozione di più segnalibri.
Impedisci eliminazione registrazione	Selezionare o deselezionare per eseguire il bloccaggio o lo sbloccaggio della registrazione.

Aggiunta di segnalibri

1. Andare alla registrazione.
2. Nella sequenza temporale delle telecamere, 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 parole chiave nella descrizione per trovare e riconoscere il segnalibro più facilmente.
5. Selezionare **Impedisci eliminazione registrazione** per proteggere la registrazione.

Nota

Non si può cancellare una registrazione bloccata. Per rimuovere la protezione della registrazione, deselezionare l'opzione o eliminare il segnalibro.

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

Esportazione delle registrazioni

Dalla scheda **Export (Esporta)**, si possono esportare le registrazioni a un archivio locale o a un percorso di rete. Qui si possono inoltre individuare informazioni e un'anteprima della registrazione. Si possono esportare molteplici file in contemporanea e si può scegliere di esportarli in formato .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 27*.

Esportazione delle registrazioni

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 delle registrazioni 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 .asx con una playlist se si seleziona **Create playlist(.asx) (Crea playlist (.asx))**.



Esportazione delle registrazioni

Scheda **Recordings (Registrazioni)**	
	Per la selezione di molteplici registrazioni, fare clic su  e spostare gli indicatori di selezione sull'inizio e fine voluti.
	Per eseguire l'esportazione delle registrazioni nei marcatori di sezione, fare clic su .
Aggiungi registrazioni	Per eseguire l'esportazione di 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 eseguire la rimozione di una 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	Al fine dell'esclusione dell'audio nella 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 delle registrazioni (redazione) prima dell'esportazione, on page 28*.
	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	Per passare alla scheda **Export (Esporta)** se la scheda **Incident report (Report dell'incidente)** è aperta, fare clic su **Switch to export (Switch per l'esportazione)**.
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 un'anteprima di più registrazioni solo se provengono dalla stessa telecamera.
Salva	Se si desidera salvare l'elenco di esportazione in un file, fare clic su **Save (Salva)**.
Carica	Se si vuole comprendere un elenco di esportazione salvato precedentemente, fare clic su **Load (Carica)**.
Note di inclusione	Per includere note nelle registrazioni, selezionare **Includi note**. Le note sono disponibili sotto forma di file .txt nella cartella esportata e come segnalibro alla registrazione in AXIS File Player.

Scheda **Export (Esporta)**	
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 eseguire l'aggiunta di istantanee, trascinare la sequenza temporale nell'anteprima in una posizione specifica. Fare clic con il pulsante destro del mouse sull'anteprima e selezionare **Add snapshot (Aggiungi istantanea)**.

Impostaz. avanzate	
Include AXIS File Player (Includi AXIS File Player)	Per includere AXIS File Player con le registrazioni esportate, selezionare **Includi AXIS File Player**.
Create playlist(.asx) (Crea playlist (.asx))	Per creare una playlist in formato .asx utilizzata da Windows Media Player, selezionare **Crea playlist (. asx)**. Le registrazioni vengono riprodotte 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 29*.
Esporta in un file Zip	Per esportare un file in formato zip, selezionare **Export to Zip file (Esporta in un file zip)** e scegliere di immettere una password per il file zip esportato.
Formato di esportazione	Selezionare un formato nel quale esportare le registrazioni dal menu a discesa **Export format (Formato di esportazione)**. Nelle registrazioni esportate non è incluso 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). Scegliere `Automatic` per usare m-jpeg per formato M-JPEG e H. 264 per altri formati.

Autorizzazione utente per l'esportazione

Per eseguire l'esportazione di registrazioni o generare rapporti sugli incidenti serve l'autorizzazione. Si può avere l'autorizzazione per uno o entrambi. 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 127*.

Modifica delle registrazioni (redazione) 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 una 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 si sovrappongono, la parte sovrapposta si riempie di colore, nell'ordine: nero, pixelato e trasparente.

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 28*.
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)** e i non selezionati diventano **Pixelated (Pixelati)**.

Genera riquadri delimitatori

Per eseguire la generazione di riquadri delimitatori sulla base di dati analitici, attivare i dati analitici della telecamera. Vedere *Profili di flusso, on page 48*.

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. Verificare che i riquadri delimitatori coprano l'oggetto in movimento, regolandoli se serve.
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 5 avvia automaticamente l'installazione quando si aggiunge una telecamera al sistema. Vedere *Installazione dell'applicazione per telecamera*.



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 password. Usare AXIS File Player per eseguire la verifica della 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 propria password per aprire la cartella.
2. Aprire AXIS File Player, le registrazioni esportate sono riprodotte in automatico.
3. In AXIS File Player, fare clic su per visualizzare le note nelle registrazioni.
4. In AXIS File Player, verificare la firma digitale per le registrazioni con **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 Report dell'incidente si possono esportare i report degli incidenti in un archivio locale o in un percorso di rete. Qui si possono 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 27*.



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 24*.
3. Fare clic su **Switch to incident report (Passa al report dell'incidente)** per andare alla scheda del 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	Al fine dell'esclusione dell'audio nella 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 delle registrazioni (redazione) prima dell'esportazione, on page 28*.
	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 .
Passare al report dell'incidente	Per passare alla scheda **Incident report (Report dell'incidente)** se la scheda **Export (Esporta)** è aperta, fare clic su **Switch to incident report (Passare al report dell'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 una registrazione nell'elenco esportato e comincerà a riprodurla. È possibile visualizzare un'anteprima di più registrazioni solo se provengono dalla stessa telecamera.
Salva	Se si desidera salvare il report dell'incidente in un file, fare clic su **Save (Salva)**.
Carica	Se si vuole includere un report dell'incidente salvato prima, fare clic su **Load (Carica)**.
Descrizione	Il campo **Description (Descrizione)** si riempie in automatico con i dati predefiniti dal modello 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	Un **Reference ID (ID di riferimento)** è generato in automatico e si può modificare in modo manuale se serve. L'id di riferimento è univoco e identifica il report dell'incidente.
Note di inclusione	Per includere note nelle registrazioni e nelle istantanee, selezionare **Include notes (Includi note)**. Le note sono disponibili sotto forma di file .txt nella cartella esportata e come segnalibro alla registrazione 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). Scegliere `Automatic` per usare m-jpeg per formato M-JPEG e H. 264 per 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 eseguire l'aggiunta di istantanee, spostare la sequenza temporale nell'anteprima in una posizione specifica. Fare clic con il pulsante destro del mouse sull'anteprima e selezionare **Add snapshot (Aggiungi istantanea)**.

Registrazione manuale

Nota

Quando ci si connette a più server AXIS Camera Station 5, 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. spostare il puntatore del mouse sul fotogramma dell'immagine dal vivo della videocamera;
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

Utilizzare la ricerca intelligente 1 per trovare le parti di una registrazione che hanno movimento in un'area dell'immagine 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. Regola 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'ora di inizio e di fine e la data 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)**. Qui 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.



Ricerca intelligente 1

Ricerca intelligente 2

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

Quando si attiva la Ricerca intelligente 2 per una telecamera Axis, AXIS Camera Station 5 comincia a registrare metadati da tale telecamera. Ricerca intelligente 2 usa i metadati per la classificazione degli oggetti nella scena e consente di usare i filtri per trovare oggetti di interesse.

Nota

La Ricerca intelligente 2 richiede quanto segue:

- Metadati di analisi dello streaming su RTSP.
- AXIS Video Content Stream sulle telecamere con AXIS OS precedente a 9.60. Vedere *Installazione dell'applicazione per telecamera, on page 65*.
- Sincronizzazione dell'ora tra il server AXIS Camera Station 5 e le telecamere.

Nota

Raccomandazioni generali:

- Consigliamo di usare la registrazione continua. Usare il rilevamento movimento può comportare rilevamenti senza video.
- Raccomandiamo l'uso del formato H.264 se si vogliono vedere in anteprima le registrazioni nei risultati della ricerca.
- Accertarsi che le condizioni di illuminazione rientrino nelle specifiche della telecamera per classificare i colori in modo ottimale. Se necessario, utilizzare luci supplementari.

Flusso di lavoro

1. *Configura la ricerca intelligente 2, on page 156*
2. Configurare la sincronizzazione dell'ora tra il server AXIS Camera Station 5 e le telecamere. Vedere *Sincronizzazione dell'ora, on page 69*.
3. Crea un filtro o caricane uno esistente. Vedere *Ricerca con filtri, on page 34*.
4. Gestione dei risultati della ricerca. Vedere *Risultati di Ricerca intelligente, on page 36*.

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 metodi per accelerarla:

- Attivare l'elaborazione 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 ridurre 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)**. Nota 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 in un determinato momento.
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 secondo necessità.
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)**. Adattare la linea nell'immagine e aggiungere o rimuovere i punti che servono.
Dimensioni e durata	Per filtrare per dimensioni e durata, fare clic su **Size and duration (Dimensioni e durata)**, selezionare la telecamera e attivare **Filter by size and duration on this camera (Filtra per dimensioni e durata in questa telecamera)**. Regolare la larghezza e l'altezza minima

	espressa in percentuale dell'immagine totale. Regolare la durata minima in secondi.
Velocità	Per filtrare per velocità, fare clic su **Speed (Velocità)**, selezionare la telecamera e attivare l'opzione **Filter by speed on this camera (Filtra per velocità su questa telecamera)**. Specificare l'intervallo di velocità che si desidera includere nel filtro. Nota 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 di un filtro e fare clic su **Save (Salva)**. 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. Per caricare un filtro salvato, fare clic su > **Saved filter settings (Impostazioni filtro salvate)** e selezionare un filtro.
	Per reimpostare un filtro, fare clic su e fare clic su **Reset (Reimposta)**.

Risultati di Ricerca intelligente

	Si possono raggruppare in intervalli di tempo rilevamenti che probabilmente sono correlati allo stesso evento. Selezionare un intervallo dal menu a discesa .
Meno recente prima	La Ricerca intelligente 2 mostra i risultati di ricerca in ordine decrescente a partire dagli ultimi rilevamenti. 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'elevata fiducia ignora 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 telecamere indossabili non sono supportate.
- Il radar può rilevare solo persone e altro veicolo. Non si può abilitare la classificazione server in background per il radar.
- La classificazione degli oggetti ha un comportamento sconosciuto per le telecamere termiche.
- Ricerca intelligente 2 non rileva oggetti in movimento quando una posizione preset PTZ cambia e per un breve periodo di ricalibrazione 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 sorgente rappresenta un sistema o un dispositivo che genera dati usabili per saperne di più sull'accaduto in un evento. Per ulteriori informazioni, vedere *Origini di dati esterne, on page 68*. Ecco qualche esempio:

- 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 l'intervallo di tempo di conservazione dei dati esterni, da parte di AXIS Camera Station 5, 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 sulle opzioni di ricerca e applicare qualsiasi filtro in più. I filtri possono variare in base al tipo di origine dati.
5. Inserire una parola chiave qualsiasi nel campo di ricerca. Vedere *Ottimizzazione della tua ricerca, on page 39*.
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	
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 cercare i dati relativi a un intervallo di tempo preset, selezionare una delle opzioni disponibili: 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	Controllo degli accessi è un esempio di componente che produce dati. Utilizzare questa opzione se si desidera includere soli i dati di questo componente specifico. Il controllo degli accessi consente di filtrare porte e zone, titolari di carte e tipi di evento.
Third party (Terze parti)	Impiegare questa opzione se si desidera includere dati di origini di terze parti che non siano i componenti configurati.

In base alla sorgente dati si possono ottenere elementi diversi nel risultato di ricerca. Ecco qualche esempio:

Risultati della ricerca	
Server	Il server a cui vengono inviati i dati dell'evento. Disponibile solo quando ci si collega a più server.
Location	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: Veicoli.

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)**. Questa funzione si limita ad esportare le informazioni sugli eventi, non le registrazioni o le immagini.

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". • 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". • 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". • 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: – "porta 1" e "Apertura forzata della porta"

	– "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: – "porta 1" e "porta aperta forzatamente" – "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. • 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. • La ricerca di `[Door] CONTAINS "door 1"` restituisce dati in cui "porta 1" è nella colonna porta.

Configurazione

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

Configurazione dei dispositivi

In AXIS Camera Station 5 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 5 supporta solo dispositivi con indirizzi IPv4.
- alcuni codificatori video hanno un indirizzo IP per ogni porta video. In tal caso, AXIS Camera Station 5 tratta ogni porta video come un dispositivo con una telecamera.

In AXIS Camera Station 5 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

È possibile effettuare le seguenti azioni per i dispositivi:

- Aggiungere telecamere e dispositivi senza funzionalità video. Vedere *Aggiunta di dispositivi*.
- Modificare le preferenze delle telecamere collegate. Vedere *Telecamere*.
- Modificare le preferenze dei dispositivi non telecamera. Vedere *Altri dispositivi*.
- Modificare la risoluzione, il formato e altri elementi dei profili di streaming. Vedere *Profili di flusso*.
- Apportare modifiche alle impostazioni dell'immagine in tempo reale. Vedere *Configurazione immagine*.
- Aggiungere o rimuovere preset PTZ. Vedere *Preimpostazioni PTZ*.
- Gestire e mantenere i dispositivi connessi. Vedere *Gestione dei dispositivi*.
- Gestisci origini di dati esterne. Vedere *Origini di dati esterne, on page 68*.

Aggiunta di 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 5.
- Raccomandiamo di non impiegare caratteri speciali come å, ä e ö nel nome host di un dispositivo.

1. Trova i tuoi dispositivi, flussi video o video preregistrati.
   - *Trova i dispositivi, on page 43*
   - *Trova i tuoi flussi video, on page 43*
   - *Trovare video preregistrati, on page 44*
2. *Aggiungere dispositivi, flussi video o video preregistrati, on page 44*

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

(nessuna)	Se non c'è alcuno stato, è possibile aggiungere il dispositivo a AXIS Camera Station 5.
Communicating (Comunicazione)	AXIS Camera Station 5 server cerca di accedere al dispositivo.
Certificato dispositivo non attendibile:	AXIS Camera Station 5 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 5 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 5 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 5 per affidarsi a quello esistente.
Errore di comunicazione	AXIS Camera Station 5 non riesce a contattare il dispositivo.
Inserisci password	AXIS Camera Station 5 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 5 utilizzerà il nome utente e la password immessi per tutti i dispositivi su cui è presente l'utente.
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. • Immettere la propria password o fare clic su **Generate (Crea)** per ottenere una password. Si consiglia di visualizzare la password generata e crearne una copia. • Scegli di utilizzare questa password per tutti i dispositivi con lo stato `Set password`.
Modello non supportato	AXIS Camera Station 5 non supporta il modello del dispositivo.
Firmware obsoleto	Il firmware del dispositivo è vecchio e si deve aggiornare prima di poter aggiungere il dispositivo.
Dispositivo malfunzionante	I parametri del dispositivo recuperati da AXIS Camera Station 5 sono corrotti.
Imposta orientamento inclinazione	Fare clic sul link per selezionare l'orientamento dell'inclinazione tra A soffitto, A parete o Su tavolo a seconda della posizione di montaggio della telecamera. L'orientamento dell'inclinazione è un'impostazione necessaria per alcuni modelli di videocamera.

Dispositivo ONVIF non supportato	AXIS Camera Station 5 non supporta tale dispositivo di terze parti.
Dispositivo non supportato	AXIS Camera Station 5 non supporta questo tipo di dispositivo.

Nota

I nuovi certificati HTTPS sono emessi da AXIS Camera Station 5 e si rinnovano automaticamente.

Trova i dispositivi

Per trovare dispositivi non elencati:

1. andare a **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 predefinita 80, 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 i flussi video che supportano quanto segue:

- Protocol (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 **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 **Add**.

Trovare video preregistrati

È possibile aggiungere video preregistrati in formato .mkv ad AXIS Camera Station 5.

Requisiti file .mkv:

- 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 54*.
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 **Configurazione > Dispositivi > Aggiungi dispositivi**.
3. Se si desidera modificare il nome del dispositivo, fare clic sul nome nell'elenco e immettere un nuovo nome.
4. Selezionare i dispositivi, i flussi video o i video preregistrati. Fare clic su **Add**.
5. Scegliere se utilizzare nomi host anziché indirizzi IP quando possibile per i dispositivi.
6. Scegliere **Quick configuration (Configurazione rapida)** se si vogliono configurare unicamente le impostazioni di base.
   Se si importa un progetto Site Designer, vedere *Importazione di progetti Site Designer*.
7. Scegliere le preferenze **Retention time (Tempo di conservazione)**, **Recording storage (Archivio registrazione)** e **Recording method (Metodo di registrazione)**.

Nota

Se si sceglie l'opzione di archiviazione della registrazione **Automatic (Automatico)**, a ogni telecamera verrà assegnata un'archiviazione con una capacità di almeno 32 GB su un'unità non OS, quando possibile. Il sistema seleziona automaticamente gli archivi con almeno 15 GB di spazio disponibile, seguiti da archivi con un minor numero di telecamere configurate per registrarli e da eventuali archivi già installati in AXIS Camera Station 5.

8. Fare clic su **Install (Installa)**. AXIS Camera Station 5 abilita automaticamente HTTPS nei dispositivi che lo supportano.

Importazione di progetti 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 5. Si può accedere al progetto usando un codice di accesso o un file di configurazione di Site Designer scaricato.

Per importare un progetto di Site Designer in AXIS Camera Station 5:

1. generare un codice di accesso per il progetto Site designer o scaricare un file di progetto.
   1.1. Accedere alla pagina *http://sitedesigner.axis.com* con l'account MyAxis.
   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 5 ha una connessione a Internet. Oppure fare clic su **Download settings file (Download file delle impostazioni)** se il server non ha una connessione a Internet.
2. Nel client AXIS Camera Station 5 andare a **Configuration > Devices > Add devices (Configurazione > Dispositivi > Aggiungi dispositivi)**.
3. Selezionare le telecamere e fare clic su **Aggiungi**.
4. Selezionare **Configurazione di Site Designer** e fare clic su **Avanti**.
5. Selezionare **Codice di accesso** e immettere il codice di accesso. In alternativa, selezionare **Choose file (Scegli file)** e trovare il file di configurazione di Site Designer scaricato.
6. Fare clic su **Importa**. In fase di importazione, AXIS Camera Station 5 tentare di associare il progetto Site Designer alle telecamere selezionate in base all'indirizzo IP o al nome del prodotto. Si potrà selezionare la telecamera corretta dal menu a discesa se l'associazione non riesce.
7. Fare clic su **Installa**.

AXIS Camera Station 5 esegue l'importazione delle seguenti impostazioni dal progetto 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 attivata da movimento: profilo di registrazione e pianificazione inclusi velocità di trasmissione, risoluzione, codifica video e compressione		✓
Registrazione continua: profilo di registrazione e pianificazione inclusi velocità di trasmissione, risoluzione, codifica video e compressione		✓
Intensità Zipstream:		✓

	Codificatori, decodificatori video, door controller, rilevatori radar e altoparlanti	Telecamere, interfoni e serie F/FA
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 Site Designer, AXIS Camera Station 5 imposta il profilo come medio.
- Nel caso entrambi i profili di registrazione siano stati definiti nel progetto Site Designer, AXIS Camera Station 5 imposta il profilo di registrazione continua come medio e la registrazione attivata dal movimento come alta.
- AXIS Camera Station 5 esegue l'ottimizzazione delle proporzioni, il che vuol dire che la risoluzione può differire tra il progetto importato e quello di Site Designer.
- AXIS Camera Station 5 può impostare le impostazioni audio se il dispositivo ha un microfono o un altoparlante incorporato. Per utilizzare un dispositivo audio esterno, si deve abilitare manualmente dopo la sua installazione.
- AXIS Camera Station 5 non applica impostazioni audio ai citofoni, anche se le impostazioni in Site Designer sono diverse. Sui citofoni, l'audio è sempre attivo unicamente nella visualizzazione in diretta.



Aggiunta di dispositivi di terze parti

È possibile aggiungere dispositivi di terze parti ad AXIS Camera Station 5 allo stesso modo dei dispositivi Axis. Vedere *Aggiunta di dispositivi*.

Nota

È inoltre possibile aggiungere dispositivi di terze parti come flussi video ad AXIS Camera Station 5. Vedere *Trova i tuoi flussi video, on page 43*.

Per informazioni sul supporto per dispositivi di terze parti, vedere il *documento tecnico più recente*.

Nota

È possibile scaricare ed eseguire lo strumento di compatibilità dei dispositivi AXIS Camera Station per verificare se i dispositivi con tecnologia video di rete sono compatibili con AXIS Camera Station 5 o versioni successive. Lo strumento verifica se il sistema può ricevere flussi video dai dispositivi video di rete. Vedere *Strumento di compatibilità dei dispositivi AXIS Camera Station*.

AXIS Camera Station 5 non è conforme a ONVIF, ma richiede che i dispositivi di terze parti siano conformi al profilo S di ONVIF e siano verificati tramite AXIS Camera Station Device Compatibility Tool.

AXIS Camera Station 5 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 5)
- Un profilo video per telecamera
- Visualizzazione in diretta
- Registrazioni continue e manuali
- Riproduzione
- Esportazione delle registrazioni
- Trigger evento dispositivo
- PTZ

Utilizzo delle aree di visione

Alcuni modelli di telecamera supportano le aree di visione. AXIS Camera Station 5 elenca le aree di visione come telecamere singole nella pagina **Add devices (Aggiungi dispositivi)**. Vedere *Aggiunta di dispositivi*.

Nota

- Tutte le aree di visione in una telecamera di rete sono considerate come singola telecamera nel numero totale di telecamere consentito dalla licenza di AXIS Camera Station 5.
- Il numero di telecamere aggiungibili dipende dalla licenza.
- Ogni licenza di AXIS Camera Station 5 consente un determinato numero di telecamere.

Per impiegare le aree di visione in AXIS Camera Station 5, è necessario che siano prima abilitate 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 sulla **Help (Guida)** per le istruzioni su dove trovare l'impostazione che differisce a seconda del modello della telecamera e del firmware.

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 5 e il dispositivo.
- Modifica le impostazioni della videocamera. Vedere *Modifica delle impostazioni della telecamera*.
- Rimuovere telecamere. In questo modo AXIS Camera Station 5 elimina tutte le registrazioni, incluse quelle bloccate, associate alle telecamere eliminate.

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**.

Attivato	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. Quando **Channel (Canale)** è disponibile per le aree di visione, selezionare il numero che corrisponde all'area di visione.
Nome utente	Nome utente per un account di amministratore associato alla telecamera.
Password	Password per un account amministratore della telecamera. AXIS Camera Station 5 utilizza la password per comunicare con la telecamera.

Altri dispositivi

Andare a **Configuration > Devices > Other devices (Configurazione > Dispositivi > Altri dispositivi)**, per vedere un elenco di dispositivi non dotati di 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 5 e il dispositivo.
- Modificare le impostazioni del dispositivo come nome, indirizzo e password del dispositivo.
- Rimuovere dispositivi.

Modifica di impostazioni di altri dispositivi

Per modificare le impostazioni di un dispositivo non telecamera:

1. Andare a **Configurazione > Dispositivi > Altri dispositivi**.
2. Selezionare un dispositivo e fare clic su **Modifica**.

Nome utente	Nome utente per un account di amministratore associato al dispositivo.
Password	Password per un account amministratore del dispositivo. AXIS Camera Station 5 utilizza la password per comunicare con 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 Profili di streaming. La pagina mostra una lista di tutte le telecamere.

Nella visualizzazione in diretta e nelle impostazioni per le 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

Il profilo di streaming è impostato per impostazione predefinita su **Automatic (Automatico)** nella visualizzazione in diretta e nelle registrazioni, il che vuol dire che il profilo di streaming passa in automatico a **High (Alto)**, **Medium (Medio)**, o **Low (Basso)** in base alla dimensione disponibile per il flusso video.

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. Questa opzione è disponibile solo per i dispositivi di terze parti. • Si può usare una sola configurazione di video encoder per un profilo video. • 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 telecamere supporta **H.264** e **M-JPEG**. H.264 richiede larghezza di banda e spazio di archiviazione minori rispetto a M-JPEG. Alcune telecamere supportano anche **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 attivabili.
Velocità in fotogrammi	L'effettiva frequenza dei fotogrammi dipende dal modello di videocamera, 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 in modo meno efficiente.

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	Effetti visibili in alcune scene: meno disturbi e livello leggermente inferiore di dettagli nelle aree di minore interesse
		Alta	Effetti visibili in molte scene: meno disturbi e livello inferiore di dettagli nelle aree di minore interesse
		Superiore	Effetti visibili in un numero ancora maggiore di scene: meno disturbi e livello inferiore di dettagli nelle aree di minore interesse
		Estremo	Effetti visibili nella maggior parte delle scene: meno disturbi e livello inferiore di dettagli nelle aree 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)**. Ottimizza per archiviazione usa strumenti di compressione più avanzati per un maggiore risparmio di spazio di archiviazione rispetto all'impostazione Zipstream predefinita. Questo profilo è in grado di ridurre ulteriormente la velocità in bit anche per scene con molto movimento. • Il formato asf non offre supporto per i B-frame usati da questa funzione. • Questa funzione non incide sui video registrati sugli AXIS S30 Series Recorder. • Per questa funzione è necessario disporre di AXIS OS 11.7.59 o versione successiva.		

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*.
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:	abilitare l'audio del microfono per uno o due flussi. Si può abilitare l'audio per la visualizzazione dal vivo e le registrazioni, solo per la visualizzazione dal vivo o solo per la registrazione.

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)**. Questa opzione è 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. Questa opzione è disponibile solo per i 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. Ci si può avvalere di questa opzione solo per una telecamera PTZ Axis dotata di AXIS PTZ Autotracking. Vedere AXIS Camera Station 5Imposta 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. Le impostazioni personalizzate sovrascrivono tutte quelle esistenti. Non includere informazioni riservate nelle impostazioni personalizzate.

Per **personalizzare le impostazioni del 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 5 e il server AXIS Camera Station 5 è lenta. Vedere Uso della larghezza di banda in *Streaming*.

Utilizzo dell'audio da altri dispositivi

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

1. Aggiungere il dispositivo non telecamera a AXIS Camera Station 5. Vedere *Aggiunta di dispositivi*.
2. Configurare la telecamera per usare l'audio del dispositivo. Vedere *Profili di flusso*.
3. Abilita audio per Visualizzazione in diretta o Registrazione. Vedere *Profili di flusso*.

Si possono trovare i seguenti esempi nei *tutorial video AXIS Camera Station*:

- 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 5

Configurazione immagine

È possibile configurare le impostazioni dell'immagine per le telecamere collegate ad AXIS Camera Station 5.

Nota

Le modifiche alla configurazione dell'immagine vengono applicate immediatamente.

Per configurare le impostazioni dell'immagine:

1. Andare a **Configuration > Devices > Image configuration (Configurazione > Dispositivi > Configurazione immagine)** per visualizzare un elenco di tutte le telecamere aggiunte ad AXIS Camera Station 5.
2. Selezionare la telecamera e il feed video verrà mostrato sotto l'elenco in tempo reale. Utilizzare il campo **Digitare il testo per la ricerca** per trovare una telecamera specifica nell'elenco.
3. Configurare le impostazioni dell'immagine.

Impostazioni immagini

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. L'opzione Bilanciamento del bianco viene utilizzata per rendere i colori dell'immagine simili ai colori reali, indipendentemente dalla temperature del 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

è soddisfacente, selezionare un'opzione che corrisponda al tipo di sorgente luminosa. Le opzioni disponibili dipendono dai modelli di telecamera.

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): abilitare questa impostazione nel caso in cui un punto luminoso, ad esempio una lampadina, renda troppo buie altre aree dell'immagine.

Dynamic contrast (wide dynamic range) (Contrasto dinamico (ampio intervallo dinamico)): abilitare questa impostazione per utilizzare l'ampio intervallo dinamico per migliorare l'esposizione quando c'è un notevole contrasto tra le aree di luce e di ombra nell'immagine. Servirsi del cursore per regolare il contrasto dinamico. Abilitare il contrasto dinamico in caso di forte controluce. Disattivare il contrasto dinamico in caso di scarsa illuminazione.

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.

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
```

Preimpostazioni PTZ

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

Andare a **Configurazione > Dispositivi > Preset PTZ**, viene visualizzato un elenco di telecamere che possono essere utilizzate con la funzione 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 sulle quali sono abilitate le operazioni PTZ digitali
- Telecamere ONVIF che supportano i preset PTZ.

Le operazioni PTZ digitali vengono abilitate dalla pagina di configurazione integrata della 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 Indirizzo.

È possibile eseguire la configurazione dei preset PTZ in AXIS Camera Station 5 e nella pagina di configurazione della telecamera. Consigliamo di configurare i preset PTZ in AXIS Camera Station 5.

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

- È possibile visualizzare il flusso completo della telecamera quando un preset PTZ è configurato in AXIS Camera Station 5. Non si possono visualizzare e non vengono registrati i movimenti PTZ nella visualizzazione in diretta.

Nota

Le operazioni PTZ non possono essere utilizzate se è abilitata la coda di controllo della telecamera. Per informazioni sulla coda di controllo e su come abilitarla o disabilitarla, vedere il Manuale per l'utente della videocamera.

Per aggiungere una posizione predefinita:

1. Andare a **Configurazione > Dispositivi > Preset PTZ** e selezionare una telecamera dall'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 posizione predefinita, selezionare la posizione predefinita e fare clic su **Rimuovi**. Questa operazione eliminerà il preset da AXIS Camera Station 5 e dalla telecamera.

Gestione dei dispositivi

Gestione dei dispositivi fornisce strumenti per l'amministrazione e la manutenzione di dispositivi connessi ad AXIS Camera Station 5.

Andare a **Configurazione > Dispositivi > Gestione** per aprire la pagina Gestisci dispositivi.

Se è stata configurata la verifica automatica per le nuove versioni firmware in *Impostazioni di aggiornamento firmware, on page 113*, viene visualizzato 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*.



Aggiornamento delle versioni del firmware

Se è stata configurata la verifica automatica per le nuove versioni software in *Aggiorna AXIS Camera Station 5, on page 119*, viene visualizzato un collegamento quando è disponibile una nuova versione di AXIS Camera Station 5. Fare clic sul collegamento per installare una nuova versione di AXIS Camera Station 5.



Installare una nuova versione di AXIS Camera Station 5

Viene visualizzato un elenco di dispositivi aggiunti ad AXIS Camera Station 5. 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 in ordine diverso.

L'elenco dei dispositivi include le seguenti informazioni:

- **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 MAC:** l'indirizzo MAC del dispositivo.
- **Stato:** lo stato del dispositivo.
  - **OK:** Lo stato normale di una connessione a un dispositivo.
  - **Manutenzione:** il dispositivo è in manutenzione e temporaneamente non accessibile.
  - **Non accessibile:** Impossibile stabilire una connessione con il dispositivo.
  - **Non è accessibile sul nome host impostato:** non è possibile stabilire una connessione con il dispositivo tramite il relativo nome host.
  - **Server non accessibile:** Impossibile stabilire una connessione con il server a cui è connesso il dispositivo.
  - **Inserisci password:** La connessione a un dispositivo viene stabilita solo quando vengono immesse 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.
  - **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.
    - Digita la password oppure fai clic su **Generate (Genera)** per generare automaticamente una password fino alla lunghezza consentita dal dispositivo. Si consiglia di visualizzare la password generata automaticamente e crearne una copia.
    - Scegli di utilizzare questa password per tutti i dispositivi con lo stato `Set password`.
    - Seleziona **Enable HTTPS (Abilita HTTPS)** per abilitare HTTPS se il dispositivo lo supporta.
  - **Tipo di password: non crittografata:** 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 5 non consente l'uso di password non crittografate per 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.
  - **Errore di certificato:** si è verificato un errore con il certificato sul dispositivo.
  - **Il certificato sta per scadere:** il certificato sul dispositivo sta per scadere.
  - **Certificato scaduto:** il certificato sul dispositivo è scaduto.
  - **Certificato HTTPS non attendibile:** il certificato HTTPS associato al dispositivo non è considerato attendibile da AXIS Camera Station 5. Fare clic sul collegamento per emettere un nuovo certificato HTTPS.
  - **Errore HTTP:** Impossibile stabilire una connessione HTTP con il dispositivo.
  - **Errore HTTPS:** 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).
- **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 68*.
- **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 68*.
- **Casa produttrice:** la casa produttrice del dispositivo.
- **Modello:** il modello del dispositivo.
- **Firmware:** La versione del firmware attualmente usata dal dispositivo.

- **DHCP:** indica se il dispositivo è connesso al server mediante DHCP.
- **HTTPS:** lo stato HTTPS del dispositivo. Vedere Stato HTTPS in *Sicurezza, on page 66*.
- **IEEE 802.1X:** lo stato IEEE 802.1X del dispositivo. Vedere Stato IEEE 802.1X in *Sicurezza, on page 66*.
- **Server:** il server AXIS Camera Station 5 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*.
- Imposta data e ora sui dispositivi. Vedere *Impostazione di data e ora*.
- Riavvia dispositivi.
- La maggior parte delle impostazioni, inclusa la password, verrà ripristinata alle impostazioni predefinite di fabbrica. Le seguenti impostazioni non vengono riportate ai valori originali: applicazioni per videocamera caricate, protocollo di boot (DHCP o statico), indirizzo IP statico, router predefinito, subnet mask e ora di sistema.

Nota

- Per evitare l'accesso non autorizzato, si consiglia vivamente di impostare la password dopo il ripristino del 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 AXIS Camera Station 5server 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 *Installazione dell'applicazione per telecamera*.
- Ricaricare i dispositivi quando le impostazioni sono state modificate dalla pagina di configurazione dei dispositivi.
- Configura dispositivi. Vedere *Configurazione dei dispositivi*.
- Gestione degli utenti. Vedere *Gestione degli utenti*.
- Gestione certificati. Vedere *Sicurezza, on page 66*.
- Raccolta dei dati del dispositivo. Vedere *Raccolta dei dati dei dispositivi*.
- Selezionare per utilizzare l'indirizzo IP o il nome host. Vedere *Connessione, on page 67*.
- Etichetta dispositivi. Vedere *Tag*.
- Immissione delle credenziali del dispositivo. Fare clic con il pulsante destro del mouse su un dispositivo e selezionare **Avanzate > Immetti 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 68*.

Assegnazione di un indirizzo IP

AXIS Camera Station 5 può assegnare un indirizzo IP a più dispositivi. I nuovi indirizzi IP possono essere ottenuti automaticamente da un server DHCP o assegnati tramite 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 **Avanzate** per aprire la pagina 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.* o 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 5.

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**.
   - L'indirizzo IP, la subnet mask e il router predefinito correnti vengono visualizzati nella sezione Indirizzo IP attuale.
   - Modificare le opzioni nella sezione 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 68*.

- Per informazioni su come configurare dispositivi, vedere *Metodi di configurazione*.
- Per informazioni su come creare un file di configurazione, vedere *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 tenterà di configurare 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 la configurazione di un singolo dispositivo attraverso il riutilizzo di alcune o tutte le impostazioni esistenti.

1. Andare a **Configurazione > Dispositivi > Gestione**.
2. Fare clic con il pulsante destro del mouse su un dispositivo, selezionare **Configura dispositivi > Configura**.
3. Selezionare le impostazioni da applicare. Vedere *Impostazioni di configurazione, on page 61*.
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, selezionare **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 da applicare. Vedere *Impostazioni di configurazione, on page 61*.
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 Errore nella scheda Attività nella parte inferiore del client AXIS Camera Station 5. Fare clic con il tasto destro del mouse sull'attività e selezionare 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, selezionare **Configura dispositivi > Configura**.
3. Fare clic su **File di configurazione** per accedere al file di configurazione. Per la creazione di un file di configurazione, vedere *Crea file di configurazione, on page 60*.
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. Queste impostazioni potranno poi essere applicate ad altri dispositivi. Per informazioni su come utilizzare il file di configurazione, vedere *Metodi di configurazione*.

Le impostazioni visualizzate sono le impostazioni del dispositivo accessibili utilizzando 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 interni sono utilizzati per controllare il funzionamento dei dispositivi 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.
- tutti i parametri dei dispositivi non sono accessibili da AXIS Device Management.

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

- **Inserire la variabile del numero di serie del dispositivo:** Questa variabile verrà sostituita dal numero di serie del dispositivo al quale viene applicato il file di configurazione.
- **Inserisci variabile nome dispositivo:** Questa variabile verrà sostituita dal nome del dispositivo utilizzato quando viene applicato il file di configurazione. Il nome del dispositivo si trova nella colonna Nome nella pagina Gestione dei dispositivi. Per rinominare un dispositivo, andare alla pagina Telecamere o Altri dispositivi.
- **Inserire la variabile del nome del server:** Questa variabile 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 Gestione dei dispositivi. Per rinominare un server, andare ad AXIS Camera Station 5 Service Control.
- **Inserire la variabile del fuso orario del server:** Questa variabile verrà sostituita dal fuso orario POSIX utilizzato quando viene applicato il file di configurazione. Questa variabile può essere utilizzata 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

- **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.
- **Finestre di rilevamento del movimento:** 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 **Configurazione > Dispositivi > Gestione**, viene visualizzata la pagina Gestisci dispositivi per consentire la gestione degli utenti dei dispositivi.

Quando si imposta la password o si rimuovono gli utenti per più dispositivi, gli utenti non presenti su tutti i dispositivi sono indicati con . Ciascun utente viene visualizzato una sola volta anche quando è presente in più dispositivi con ruoli diversi.

Nota

Gli account sono specifici del dispositivo e non sono correlati agli account utente di AXIS Camera Station 5.

Imposta 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 di impostare le 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 5.

Nelle password possono essere utilizzati i seguenti caratteri:

- lettere maiuscole e minuscole da A a Z
- tutti i numeri interi 0-9
- spazio, virgola (,), punto (.), due punti (:), e punto e virgola (;)
- !, ", #, $, %, &, ', (, +, *, -,), /, <, >, =, ?, [, \, ^, -, `, {, |, ~, @,], }

Per impostare la 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 complessa.
5. Fare clic su **OK**.

Aggiunta di utenti

Per aggiungere utenti locali o di Active Directory a AXIS Camera Station 5:

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 Impostazione della password sopra riportata.
4. Selezionare i diritti di accesso degli utenti dal menu a discesa del campo **Ruolo**:
   - **Amministratore:** accesso illimitato al dispositivo.
   - **Operatore:** accesso al flusso video, agli eventi e a tutte le impostazioni eccetto le opzioni di sistema.
   - **Utente:** accesso al flusso video.
5. Selezionare **Attiva comandi 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 da rimuovere dall'elenco a discesa del campo **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 **Digitare il testo per la ricerca** per trovare un utente specifico nell'elenco.

Aggiornare il firmware



Il firmware è un software che determina la funzionalità del prodotto Axis. L'utilizzo del firmware più recente assicura al dispositivo le funzionalità e i perfezionamenti più recenti.

Il nuovo firmware può essere scaricato utilizzando AXIS Camera Station 5 o importato da un file su un disco rigido o una scheda di memoria. Le versioni del firmware disponibili da scaricare sono visualizzate con il testo **(Scarica)** 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:** Eseguire l'aggiornamento alla versione del firmware selezionata e conservare i valori delle impostazioni esistenti.
- **Factory default (Valori predefiniti di fabbrica):** Eseguire l'aggiornamento alla 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 Dispositivi non validi. Fare clic su **Continue (Continue)** per saltare i dispositivi che non possono essere configurati.
4. Il dispositivo non è accessibile durante il processo di aggiornamento del firmware, fare clic su **Sì** per continuare. Se è stato già confermato e non si desidera che venga visualizzato nuovamente, selezionare **Non mostrare più questa finestra di dialogo** e fare clic su **Sì**.

5. La finestra di dialogo 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*.

Impostazione di data e ora

Le impostazioni di data e ora dei dispositivi Axis possono essere sincronizzate con l'ora del computer server, con un server NTP oppure impostate manualmente.

Per impostare data e ora sui dispositivi:

1. Andare a **Configurazione > Dispositivi > Gestione**.
2. Selezionare il dispositivo e fare clic su oppure fare clic con il pulsante destro del mouse e selezionare **Imposta data e ora**.
3. **Ora dispositivo** elenca la data e l'ora correnti del dispositivo Axis. Quando si selezionano più dispositivi, **Ora dispositivo** non è disponibile.
4. Selezionare il fuso orario.
   – Selezionare il fuso orario che si desidera utilizzare per il dispositivo Axis dall'elenco a discesa **Fuso orario**.
   – Selezionare **Passa automaticamente all'ora legale** se il dispositivo si trova in un'area in cui è in vigore l'ora legale.

Nota

Il fuso orario può essere impostato quando si seleziona la modalità **Sincronizza con server NTP** o **Imposta manualmente**.

5. Nella sezione modalità tempo:
   – Selezionare **Synchronize with server computer time (Sincronizza con l'ora del computer server)** per sincronizzare la data e l'ora del dispositivo in uso con l'orologio del computer server, cioè il computer in cui è installato il server AXIS Camera Station 5.
   – Selezionare **Sincronizza con server NTP** per sincronizzare la data e l'ora del dispositivo in uso con quelle di un server NTP. Immettere l'indirizzo IP, il DNS o il nome host del server NTP nel campo fornito.
   – Selezionare **Imposta manualmente** per impostare manualmente la data e l'ora.
6. Fare clic su **OK**.



Impostazione di data e ora

Installazione dell'applicazione 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 la rilevazione, il riconoscimento, il tracking e il conteggio.

Alcune applicazioni possono essere installate direttamente da AXIS Camera Station 5. 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, il file della chiave di licenza può essere installato contemporaneamente all'applicazione o in un momento successivo mediante la pagina di configurazione dei dispositivi.

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 licenze e può essere installata su videocamere 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 licenze e può essere installata su videocamere con versione firmware 5.60 o successiva.

AXIS Video Content Stream – Applicazione che consente alle telecamere Axis di inviare i dati di rilevamento degli oggetti in movimento a AXIS Camera Station 5. Può essere installata su telecamere con versione firmware compresa tra 5.50 e 9.59. L'uso di AXIS Video Content Stream è consentito solo in combinazione con AXIS Camera Station 5.

Altre applicazioni – Qualsiasi applicazione che si desidera 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 per telecamera che si desidera installare sulle telecamere. 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 consente di ripristinare le impostazioni dell'applicazione sui dispositivi.

5. Se per l'applicazione è necessaria una licenza, viene visualizzata la finestra di dialogo 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 5 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 131*.

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 5.

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 solo elemento. L'eliminazione del certificato lo rimuoverà da tutti i dispositivi sui quali 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 5 usa HTTPS per eseguire la connessione al dispositivo.
	Off	AXIS Camera Station 5 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	Attivato	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 scopi di risoluzione di problemi. Consente di generare 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 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 Salva con nome, 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 utilizzando l'indirizzo IP o il 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)**.

Tag

Le etichette vengono utilizzate per organizzare i dispositivi nella pagina Gestione dei dispositivi. Una dispositivo può avere più etichette.

Per esempio, è possibile etichettare i dispositivi in base al modello o all'ubicazione. Quando i dispositivi sono, ad esempio, etichettati secondo il 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 **Usa etichetta esistente** e selezionare un'etichetta, oppure selezionare **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 Etichette, selezionare un'etichetta. Verranno quindi visualizzati tutti i dispositivi associati a questa etichetta.
3. selezionare i dispositivi; Fare clic con il pulsante destro del mouse e selezionare **Elimina 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 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 clic su per aggiungere la pagina Etichette dispositivo.
   - Fare clic su un'etichetta per visualizzare tutti i dispositivi associati all'etichetta e fare clic su Tutti i dispositivi per visualizzare tutti i dispositivi collegati ad AXIS Camera Station 5.
   - 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. Vedere il manuale per l'utente del dispositivo per ottenere informazioni su come eseguire la configurazione del dispositivo.
4. Chiudere la scheda e il dispositivo sarà ricaricato affinché le modifiche siano implementate in AXIS Camera Station 5.

Limiti

- Non è supportata l'autenticazione automatica per i dispositivi di terze parti.
- Non può essere assicurato il supporto generale per 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 38*.

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 5, 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 5, 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 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

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

Viene visualizzato un elenco di dispositivi aggiunti ad AXIS Camera Station 5. 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 in ordine diverso.

L'elenco dei dispositivi include le seguenti informazioni:

- **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 viene utilizzato quando si aggiunge il dispositivo. Vedere *Scheda Configurazione dispositivi, on page 68*.
- **Indirizzo MAC:** l'indirizzo MAC del dispositivo.
- **Modello:** il modello del dispositivo.
- **Abilitato:** Mostra se la sincronizzazione ora è abilitata.
- **Sorgente NTP:** La sorgente NTP configurata per il dispositivo.
  - **Statico:** 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.
- **Server NTP primario:** Il server NTP principale configurato per il dispositivo. Disponibile unicamente quando è selezionato **Static (Statico)**.
- **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.
- **Offset ora server:** la differenza di orario tra dispositivo e server.
- **Ora UTC:** l'ora universale coordinata sul dispositivo.
- **Sincronizzato:** mostra se le impostazioni di sincronizzazione dell'orario sono davvero applicate. Questa opzione è disponibile solo per i dispositivi con firmware 9.1 o versione successiva.
- **Tempo fino alla sincronizzazione seguente:** Il tempo che rimane fino alla sincronizzazione successiva.

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 5. Sono visualizzate le seguenti informazioni:

- **Server:** Il server AXIS Camera Station 5 su cui viene eseguito il servizio Ora di Windows.
- **Stato:** Stato del servizio Ora di Windows. `Running` o `Stopped`.
- **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 hai selezionato **Static (Statica)**, configura il server NTP principale e secondario.
5. fare clic su **Applica**;

Send alarm when the time difference between server and device is larger 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 server e dispositivo è superiore a 2 secondi.

Configurazione dell'archiviazione

Andare a **Configurazione > Archiviazione > Gestione** per aprire la pagina Gestisci archiviazione. La pagina Gestione dello spazio di archiviazione mette a disposizione una panoramica dell'archiviazione locale e dell'archiviazione di rete che esiste in AXIS Camera Station 5.

Elenco	
Location	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: • **OK** • **Archiviazione completa:** Il dispositivo di archiviazione è pieno. Il sistema sovrascrive le registrazioni sbloccate più vecchie. • **Non disponibile:** Le informazioni sull'archiviazione non sono attualmente disponibili. Ad esempio, un'archiviazione di rete è stata rimossa o scollegata. • **Intrusione dati:** i dati di altre applicazioni impiegano lo spazio di archiviazione allocato per AXIS Camera Station 5. Oppure, ci sono delle registrazioni prive di connessione al database, le cosiddette registrazioni non indicizzate, nello spazio di archiviazione allocato per AXIS Camera Station 5. • **Nessuna autorizzazione:** L'utente non ha l'autorizzazione di lettura o scrittura relativamente al dispositivo di archiviazione. • **Spazio insufficiente:** l'unità ha meno di 15 GB di spazio libero, che AXIS Camera Station 5 considera insufficiente. Per la prevenzione di errori o corruzione, AXIS Camera Station 5 esegue una pulizia forzata, a prescindere dal posizionamento del cursore di archiviazione, per tutelare l'unità. Nel corso della pulizia forzata, AXIS Camera Station 5 impedisce la registrazione finché non diventa disponibile uno spazio di archiviazione superiore a 15 GB. • **Capacità insufficiente**: La dimensione totale del disco è inferiore a 32 GB, una dimensione insufficiente per AXIS Camera Station 5. Gli AXIS OS Recorder con supporto per RAID possono presentare anche i seguenti stati: • **Online:** Il sistema RAID funziona regolarmente. C'è una ridondanza nell'eventualità che si verifichi un guasto in uno dei dischi fisici del sistema RAID. • **Degradato:** uno dei dischi fisici nel sistema RAID è guasto. Si possono ancora registrare e riprodurre registrazioni dal dispositivo di archiviazione, ma non c'è ridondanza. 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)**. • **In sincronizzazione:** I dischi RAID si sincronizzano. Puoi eseguire la registrazione e riproduzione di registrazioni dal dispositivo di archiviazione, ma non c'è 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**. Importante Non eseguire mai la rimozione di un disco RAID nel corso della sincronizzazione. Ciò può condurre a un guasto del disco. • **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 Raccolta dei file non indicizzati in *Gestione dello spazio di archiviazione, on page 72*.
Gratuita	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 preso dai file che non sono registrazioni indicizzate e quindi non sono noti a AXIS Camera Station 5. 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 5 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 **Configurazione > Archiviazione > Gestione** per aprire la pagina Gestisci archiviazione. In questa pagina è possibile specificare la cartella in cui archiviare le registrazioni. Per impedire il riempimento dello spazio di archiviazione, impostare una percentuale massima di capacità totale utilizzabile da AXIS Camera Station 5. 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 5, 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 collegate 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 dal menu a discesa.
4. Per aggiungere un'unità di rete condivisa, selezionare **Unità di rete condivisa** e inserire un percorso a un'unità di rete condivisa. 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 dispositivo di archiviazione locale o un'unità di rete condivisa, selezionare un dispositivo di archiviazione locale o un'unità di rete condivisa dall'elenco delle archiviazioni 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 5 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.
- Il requisito dello spazio minimo di un dispositivo di archiviazione aggiunto ad AXIS Camera Station 5 è 32 GB con almeno 15 GB di spazio libero disponibile.
- Se lo spazio libero è inferiore a 15 GB, AXIS Camera Station 5 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 per le 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 accedere al server. AXIS Camera Station 5 posiziona i dati nelle cartelle nell'ordine in cui sono stati trovati, prima dal server e quindi dai dispositivi connessi allo specifico server.

È possibile cercare una determinata registrazione o un log perso o eliminare semplicemente 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 iniziare un'attività.

4. Quando l'attività viene 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 **Configurazione > Archiviazione > Selezione** per aprire la pagina Seleziona archiviazione. In questa pagina è presente un elenco di tutte le telecamere in AXIS Camera Station 5 ed è possibile specificare il numero di giorni di conservazione delle registrazioni per telecamere specifiche. Se selezionata, le informazioni sull'archiviazione sono disponibili in Memorizzazione della registrazione. 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 68*.
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.
Location	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.
Registrazione di failover	Mostra se la telecamera impiega il failover recording.
Registrazione fallback	Mostra se la telecamera impiega la registrazione di fallback.
Server	Il server in cui si trova l'archiviazione di rete o locale.

La soluzione di archiviazione di ogni telecamera è stata configurata all'aggiunta di telecamere ad AXIS Camera Station 5. 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. fare clic su **Applica**;

Memorizzazione della registrazione	
Store to (Archivia in)	Selezionare dal menu a discesa il dispositivo di archiviazione dove eseguire il salvataggio delle registrazioni. Le opzioni disponibili sono il dispositivo di archiviazione locale e l'archiviazione di rete create.
Registrazione di failover	Selezionare questa opzione per archiviare le registrazioni sulla scheda di memoria della fotocamera quando AXIS Camera Station 5 e la telecamera perdono la connessione. Una volta rispristinata la connessione, i failover recording vengono trasferiti ad AXIS Camera Station 5. Nota Questa funzione è disponibile solo per le telecamere dotate di scheda di memoria e con versione firmware 5.20 o successiva.
Illimitato	Selezionare tempo di conservazione per mantenere le registrazioni fino ad esaurimento dello spazio sul dispositivo di archiviazione.
Limitato	Selezionare per impostare il numero massimo di giorni di conservazione delle registrazioni. Nota Se lo spazio di archiviazione destinato ad AXIS Camera Station 5 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.

Configurazione di registrazioni ed eventi

Quando si esegue l'aggiunta di telecamere a AXIS Camera Station 5, questo configura automaticamente la registrazione del movimento o la registrazione continua. In seguito si può modificare il metodo di registrazione secondo le proprie esigenze, andare a *Metodo di registrazione, on page 80*.

Registrazione del movimento

Si può usare il rilevamento movimento con tutte le telecamere di rete e i codificatori video Axis. Registrare nel solo caso di rilevamento movimento da parte di una telecamera consente un notevole risparmio dello spazio di archiviazione rispetto alla registrazione continua. 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 o pochi oggetti 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 eseguire la configurazione delle impostazioni di rilevamento movimento, come il numero di oggetti rilevabili. 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*.
5. Selezionare un **Profile (Profilo)** nel menu a discesa, il profilo **High (Alto)** è predefinito.

6. Selezionare una pianificazione o fare clic su **New schedule...** (Nuova pianificazione...) per creare una nuova pianificazione personalizzata.
7. Impostare le impostazioni temporali per il pre-buffer e il post-buffer, nonché per il periodo di trigger.
8. Fare clic su **Applica**.

Nota

È possibile usare le regole di azione per configurare la registrazione del movimento. Assicurarsi di disattivare **Motion detection (Rilevamento movimento)** in **Recording method (Metodo di registrazione)** prima di usare le regole di azione.

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 da eseguire. Per diminuire l'impatto sullo spazio di archiviazione, registrare unicamente in periodi di tempo specifici.
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 l'intervallo di tempo tra due trigger consecutivi per ridurre il numero di registrazioni consecutive. Se avviene un altro trigger in questo intervallo, la registrazione prosegue e il periodo di attivazione ricomincia.
Generare allarmi	Attiva un allarme quando la telecamera effettua il rilevamento movimento.



Configurare il rilevamento di movimento

Registrazione continua e pianificata

La registrazione continua salva le immagini in modo continuo e richiede più spazio di archiviazione rispetto alle altre opzioni di registrazione. Per la riduzione delle dimensioni del file, tenere conto della 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) per utilizzare la registrazione 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)** nel menu a discesa, il profilo **High (Alto)** è 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 da eseguire. Per diminuire l'impatto sullo spazio di archiviazione, registrare unicamente in periodi di tempo specifici.
Average Bitrate	Attivare e impostare l'archiviazione massima. 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 80*.

Registrazione manuale

Per ulteriori informazioni su come registrare manualmente, vedere *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)** nel menu a discesa, il profilo **High (Alto)** è predefinito. Usare una risoluzione inferiore per ridurre le dimensioni della registrazione. Per modificare le impostazioni del profilo, vedere *Profili di flusso*.
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	Selezionare per aggiungere 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 per impostazione predefinita sono disattivate.
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.

Registrazione attivata da regole

Una registrazione attivata da regole inizia e si ferma in base a una regola creata in Regole di azione. Si possono usare regole, ad esempio, per generare registrazioni attivate da segnali provenienti dalle porte I/O, tentativi di manomissione o AXIS Cross Line Detection. Una regola può avere diverse attivazioni.

Per eseguire la creazione di 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 garantire che le registrazioni vengano salvate in caso di interruzione della connessione a AXIS Camera Station 5. Quando la failover recording è abilitata, la telecamera salva le registrazioni sulla scheda di memoria in caso di interruzione della connessione per più di 20 secondi. È necessario che la telecamera disponga di una scheda di memoria installata e che la funzione sia abilitata. Il failover recording vengono interessa solo per le registrazioni in formato H.264.

Per abilitare il failover recording:

1. Andare a **Configurazione > Archiviazione > Selezione**.
2. Selezionare una telecamera che supporta il failover recording.
3. Selezionare **Failover recording**.
4. Fare clic su **Applica**.

Nota

- Riavviando il server AXIS Camera Station 5 non si attiverà la failover recording. Ad esempio, quando si esegue Gestione database, riavviare AXIS Camera Station 5 Service Control o riavviare il computer in cui è installato il server.
- L'abilitazione della failover recording sovrascrive qualsiasi configurazione failover esistente per quella telecamera su altri server.
- La failover recording può essere attiva solo per un server AXIS Camera Station 5 alla volta per ciascuna vista della telecamera.

Quando la connessione è ripristinata, AXIS Camera Station 5 importa in modo automatico le failover recording e le contrassegna con un colore grigio scuro nella cronologia.

La telecamera utilizza un pre-buffer e un post-buffer di 20 secondi per ridurre al minimo le interruzioni nella registrazione, ma possono comunque verificarsi brevi interruzioni di circa 1-4 secondi. Il profilo di streaming elevato viene sempre utilizzato per le failover recording. Audio è incluso se è abilitato sulla telecamera e fa parte del flusso prima di attivare failover.

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. • 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.

Nota

I dispositivi che utilizzano una versione di AXIS OS precedente alla 11.11.42 impiegano un metodo di failover recording legacy. Le principali differenze sono:

- La telecamera avvia la failover recording dopo 10 secondi di interruzione della connessione.
- La fotocamera utilizza un buffer di memoria interna di 10 secondi invece di un pre-buffer e un post-buffer di 20 secondi.



Utilizza la scheda di memoria per il failover recording

Registrazione fallback

È possibile attivare la registrazione di fallback su un dispositivo che usa AXIS S3008 Recorder come memoria di registrazione. Una volta attivata la registrazione di fallback, il dispositivo avvia automaticamente una registrazione continua quando si perde la connessione tra AXIS Camera Station 5 e il registratore. Il dispositivo impiega il profilo di streaming medio ai fini della registrazione fallback.

Nota

- Richiede AXIS Camera Station 5.36 o versione successiva, AXIS S3008 Recorder firmware 10.4 o versione successiva, firmware del dispositivo Axis 5.50 o versione successiva.
- Se c'è una registrazione continua in corso quando viene avviata la registrazione di fallback, verrà avviata una nuova registrazione continua. Il sistema crea duplicati del flusso sul registratore.

Per eseguire l'attivazione della registrazione di fallback:

1. Assicurarsi di aver eseguito l'aggiunta di AXIS S3008 Recorder e dei dispositivi e di selezionare 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 **registrazione di fallback**.
4. fare clic su **Applica**;

Metodo di registrazione

AXIS Camera Station 5 configura automaticamente la registrazione del movimento o la registrazione continua quando si aggiungono dispositivi.

Un segno di spunta nella lista mostra quale metodo di registrazione usa 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)**, eseguire l'attivazione o disattivazione di 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. In questo modo è possibile 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 e le telecamere devono supportare la velocità di trasmissione media ed essere dotate di firmware 9.40 o successivo.
- 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 disponibile spazio a sufficienza per le registrazioni.

7. fare clic su **Applica**;

Modifica di AXIS Video Motion Detection 2 e 4

AXIS Video Motion Detection 2 e 4 sono applicazioni per telecamere installabili su dispositivi che supportano 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 a AXIS Camera Station 5, 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 *Installazione dell'applicazione 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 (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 di 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 (Oggetti piccoli)**: Questo filtro ignora gli oggetti piccoli, ad esempio gli animali piccoli. 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 (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

Le impostazioni selezionate qui modificano le impostazioni nella 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 **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 i movimenti di breve durata, selezionare **Short lived objects filter (Filtro movimenti 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 rileva 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 posizionare un'area di esclusione all'interno di un'area di inclusione per ignorare il movimento. È possibile utilizzare più aree di inclusione e di esclusione.

Per aggiungere e modificare un'area di inclusione:

Nota

Le impostazioni selezionate qui modificheranno le impostazioni nella 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 vedere solo l'area modificata, seleziona **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 (Cronologia)** e **Sensitivity manually (Sensibilità)** manualmente.
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 del 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 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**.

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 5 può controllare i dispositivi collegati alle porte di output.

Nota

- Quando ci si connette a più server AXIS Camera Station 5, 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 5 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 5 può attivare o disattivare un dispositivo collegato a una porta di output. Vedere *Regole di azione*.

Per informazioni relative a come collegare dispositivi e come configurare le porte I/O, vedere la Guida all'installazione o il manuale per l'utente del dispositivo 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)**. Se serve, modificare le informazioni.
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, è possibile impostare lo stato iniziale quando AXIS Camera Station 5 si connette al dispositivo. Selezionare **On startup set to (All'avvio imposta su)** e selezionare lo stato iniziale nel menu a discesa **State (Stato)**.

Modifica	Per modificare una porta, selezionarla e fare clic su **Modifica**. Nella finestra a comparsa, aggiornare le informazioni sulla porta e fare clic su **OK**.
Rimuovi	Per rimuovere una porta, selezionarla e fare clic su **Rimuovi**.
Ricarica porte di I/O	Se configuri 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 ci si connette a più server AXIS Camera Station 5, è possibile selezionare qualsiasi server connesso dal 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 5 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. Molte di queste azioni possono richiedere la configurazione aggiuntiva del dispositivo.

Aggiunta di trigger

I trigger attivano le 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)**. Aumentare il periodo di attivazione se si usa questa impostazione con trigger a impulsi. 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 86*.

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.

Allarme anti-manomissione attivo – Il trigger anti-manomissione si attiva quando si riposiziona il dispositivo, qualcosa copre l'obiettivo o l'obiettivo è notevolmente sfocato. Vedere *Creazione di trigger di allarmi antimanomissione attivi, on page 86*.

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 .

AXIS Cross Line Detection – AXIS Cross Line Detection è un'applicazione per telecamere e video encoder. L'applicazione rileva oggetti in movimento che attraversano una linea virtuale e può essere utilizzata, ad esempio, per monitorare punti di entrata e di uscita. Vedere *Creazione di trigger AXIS Cross Line Detection, on page 87*.

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, un'archiviazione di rete non può essere raggiunta o viene interrotta la connessione con uno o più dispositivi. Vedere *Creazione di trigger da evento di sistema e da errore, on page 87*.

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. Vedere *Creazione di trigger di input/output, on page 88*. Raccomandiamo, ove possibile, 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 5. Vedere *Creazione di trigger eventi dispositivo, on page 89*.

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 94*.

Evento di AXIS Entry Manager – Questo trigger si attiva quando AXIS Camera Station 5 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 95*.

HTTPS esterno – Il trigger HTTPS esterno consente alle applicazioni esterne di attivare eventi in AXIS Camera Station 5 tramite la comunicazione HTTPS. Vedere *Creazione di trigger HTTPS esterni, on page 95*.

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 elabora il rilevamento, la telecamera non aggiunge alcun carico di elaborazione ad AXIS Camera Station 5.

Nota

Evitare di utilizzare i trigger di attivazione del rilevamento del movimento per avviare registrazioni, se nella telecamera è abilitata la registrazione del movimento. 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. Fare clic su **Aggiungi** e selezionare **Rilevamento movimento**.
4. Fare clic su **OK**.
5. Nella schermata a comparsa:
   5.1. Selezionare la telecamera che dovrebbe rilevare il movimento.
   5.2. Impostare un intervallo di tempo tra due trigger consecutivi per ridurre il numero di registrazioni consecutive. Se avviene 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 di allarmi antimanomissione attivi

L'allarme di active tampering si attiva quando si riposiziona la telecamera, qualcosa copre l'obiettivo o l'obiettivo è notevolmente sfocato. Poiché il dispositivo elabora il rilevamento di manomissioni, non aggiunge alcun carico di elaborazione al server AXIS Camera Station 5.

L'allarme di active tampering è disponibile per le telecamere con supporto per manomissione telecamera e con firmware 5.11 o versione successiva.

Per creare un trigger di allarme antimanomissione attivo:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. Fare clic su **Aggiungi** e selezionare **Attiva allarme antimanomissione**.
4. Fare clic su **OK**.
5. In **Trigger on (Attivazione)**, selezionare la telecamera da usare.
6. Fare clic su **OK**.

Creazione di trigger AXIS Cross Line Detection

AXIS Cross Line Detection è un'applicazione per telecamere e video encoder. L'applicazione rileva oggetti in movimento che attraversano una linea virtuale e attiva il trigger. Si può anche usare, ad esempio, per il monitoraggio dei punti di entrata e uscita. Poiché la telecamera elabora il rilevamento, non aggiunge alcun carico di elaborazione al server AXIS Camera Station 5.

Si può installare l'applicazione solo sui dispositivi che supportano la AXIS Camera Application Platform. Per utilizzare AXIS Cross Line Detection come trigger, è necessario scaricare l'applicazione da *axis.com* e installarla sui dispositivi. Vedere *Installazione dell'applicazione per telecamera*.

Per creare un trigger AXIS Cross Line Detection:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. Fare clic su **Aggiungi** e selezionare **AXIS Cross Line Detection**.
4. Fare clic su **OK**.
5. Fare clic su **Aggiorna** per aggiornare l'elenco.
6. Selezionare la telecamera da utilizzare dal menu a discesa **Trigger on (Attivazione)**.
   Si possono selezionare solo le telecamere in cui è stato installata AXIS Cross Line Detection.
7. Impostare un intervallo di tempo tra due trigger consecutivi in **Trigger period (Periodo di attivazione)** per ridurre il numero di registrazioni consecutive.
   Se avviene un altro trigger in questo intervallo, la registrazione prosegue e il periodo di attivazione ricomincia.
8. Fare clic su **AXIS Cross Line Detection settings (Impostazioni di AXIS Cross Line Detection)** per aprire la pagina **Applications (Applicazioni)** della telecamera in un browser Web. Per informazioni sulle impostazioni disponibili, vedere la documentazione fornita con AXIS Cross Line Detection.

Nota

per configurare AXIS Cross Line Detection, usare Internet Explorer e impostare il browser in modo da consentire i controlli ActiveX. Se richiesto, fare clic su **Yes (Sì)** per installare AXIS Media Control.

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, il contatto non riuscito con un'archiviazione di rete 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. Fare clic su **Aggiungi** e selezionare **Errore e allarme 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 di accesso 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 nel contattare le telecamere. • Selezionare **All (Tutto)** per includere tutte le telecamere aggiunte ad AXIS Camera Station 5. • Selezionare **Selected (Selezionato)** e fare clic su **Cameras (Telecamere)** per mostrare una lista di tutte le telecamere aggiunte ad AXIS Camera Station 5. Usare **Select all (Selezionare tutto)** per selezionare tutte le telecamere o **Deselect all (Deselezionare tutto)** per la deselezione di 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 5 prima di utilizzare un trigger I/O. Vedere *Porte I/O*.
- Se possibile, utilizzare le attivazioni di eventi del dispositivo invece delle attivazioni di input/output. Le attivazioni degli eventi del dispositivo offrono una migliore esperienza utente complessiva. Per ulteriori informazioni, vedere *Creazione di trigger eventi dispositivo, on page 89*.

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. Fare clic su **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 di tempo tra due trigger consecutivi in **Trigger period (Periodo di attivazione)** per ridurre il numero di registrazioni consecutive. Se avviene 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 sono presenti trigger adatti in AXIS Camera Station 5. Gli eventi differiscono tra una telecamera e l'altra e sono dotati di uno o molteplici filtri da impostare. I filtri sono condizioni che devono verificarsi 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. Fare clic su **Aggiungi** e selezionare **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 dispositivo in funzione del tempo. Un evento può essere dotato o privo di stato. Una funzione a gradino rappresenta l'attività di un evento dotato di stato. Una linea retta con impulsi dal momento dell'attivazione dell'evento rappresenta l'attività di un evento privo di 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 di tempo tra due trigger consecutivi in **Trigger period (Periodo di attivazione)** per ridurre il numero di registrazioni consecutive. Se avviene 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	Heatbeat
MotionRegionDetector	Movimento
Rete	Interruzione connessione di rete Applicabile solo agli eventi utilizzati dal dispositivo, non applicabile agli eventi utilizzati da AXIS Camera Station 5.
	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	Impulso
	Intervallo
	Evento pianificato
Stato	Attivo
Archiviazione	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 <nome profilo>
	VMD 4: qualunque 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.

Rilevamento anti-passback	Qualcuno ha impiegato le credenziali di un titolare che è entrato prima in una zona.
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 nello stato pronto. Ad esempio, il dispositivo Axis rileva lo stato del sistema e invia una notifica all'amministratore quando il sistema è stato avviato. Selezionare **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 un sistema di eventi, sono stati avviati.
Porta	
Porta forzata	La porta è stata forzata.
Rilevata manomissione installazione porta	Quando il sistema rileva quanto segue: • Alloggiamento del dispositivo aperto o chiuso • Movimento dispositivo • Rimozione del lettore connesso dal muro • Manomissione con dispositivo REX, lettore o monitor porta connesso. Per usare questo trigger, accertarsi di attivare Input supervisionati e ispezionare l'installazione dei resistori terminali sulle relative porte di input del 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 il requisito 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 notifiche 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. Applicabile solo agli eventi utilizzati dal dispositivo, non applicabile agli eventi utilizzati da AXIS Camera Station 5.
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, nei fine settimana, ecc. 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 **Live view (Visualizzazione in diretta)**. Si possono trovare i pulsanti di azione 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.

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 – Usarlo 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 fanno iniziare l'azione quando si trovano nello stato "attivo", ma si può anche avviare l'azione nello stato "disattiva".

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. Fare clic su **Aggiungi** e selezionare **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 e il pulsante azione si attiva.

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 usare.
   7.2. Se si sceglie di utilizzare un pulsante commutatore esistente, si deve selezionare **Trigger on toggle (Attivazione a pulsante)** o **Trigger on untoggle (Attivazione con pulsante in stato 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 5 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 5.

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. 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 5 tramite la comunicazione HTTPS. Questo trigger supporta solo la comunicazione HTTPS e richiede che venga fornito il nome utente valido di AXIS Camera Station 5 comprensivo di nome di dominio e password nelle 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 *Generale*.
- Activate the trigger with ID "trigger1": (Attiva il trigger con ID "trigger1":) `https://[address]:55756/Acs/Api/TriggerFacade/ActivateTrigger?{"triggerName":"trigger1"}`
- Deactivate the trigger with ID "trigger1": (Disattiva il trigger con ID "trigger1":) `https://[address]:55756/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]:55756/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]:55756/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. Fare clic su **Aggiungi** e selezionare **HTTPS esterno**.
4. Fare clic su **OK**.
5. Immettere il nome del trigger in **Trigger name (Nome trigger)**.
6. Rivedere l'URL campione che utilizza lo stesso indirizzo server utilizzato dal client al momento dell'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)**.

Aggiunta di azioni

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

Sono disponibili le seguenti operazioni:

Registrazione – questa azione avvia una registrazione dalla telecamera. Vedere *Creazione di azioni di registrazione*.

Generare allarmi – Questa azione esegue l'invio di un allarme a tutti i client AXIS Camera Station 5 connessi. Vedere *Creazione di azioni di allarme*.

Impostare uscite – Questa azione imposta lo stato di una porta di output. Usarla per i comandi del dispositivo collegato alla porta di output, ad esempio per accendere una luce o bloccare una porta. Vedere *Creazione di azioni di uscita*.

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

Inviare notifiche HTTP – questa azione 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 – Questa azione ha come funzione l'innesco di una sirena e di uno schema luminoso su un dispositivo compatibile in base a un profilo preconfigurato. Vedere *Crea azioni sirena e luce, on page 102*.

AXIS Entry Manager – questa azione può essere utilizzata per concedere l'accesso, aprire o chiudere una porta collegata ad un door controller configurato da AXIS Entry Manager. Vedere *Crea azioni di AXIS Entry Manager, on page 102*.

Invia notifica dell'app per dispositivo mobile – L'azione 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 103*.

Attiva o disattiva regole – Utilizzare questa azione per attivare o disattivare altre regole di azione. Vedere *Crea un'azione che attivi o disattivi altre regole di azione, on page 103*.

Invia al 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. Vedere

Controllo accessi – questa azione include azioni porta e azioni zona in AXIS Camera Station Secure Entry. Vedere *Crea azioni di controllo degli accessi, on page 104*.

Creazione di azioni di registrazione

L'azione di registrazione comincia a registrare dalla telecamera. Accedere e riprodurre la registrazione dalla scheda **Recordings (Registrazioni)**.

Per creare un'azione di registrazione:

1. Specificare una posizione 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. 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	Selezionare 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 5 connessi. L'allarme viene visualizzato nella scheda **Alarms (Allarmi)** e come notifica nella barra delle applicazioni. Si possono includere nell'allarme istruzioni sotto forma di file con procedure d'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 **Aggiungi** e creare un trigger. 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 di allarme)**, configurare titolo, descrizione e durata.
7. In **Alarm procedure (Procedura di allarme)**.
   7.1. Selezionare **Se si attiva allarme, mostra procedura allarme**;
   7.2. fare clic su **Upload (Carica)** e trovare il file desiderato.
   7.3. fare clic su **Anteprima** per aprire il file caricato in una finestra di anteprima;
   7.4. Fare clic su **OK**.

Messaggio allarme	
Titolo	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 tra 1 e 600 secondi di durata per gli allarmi pop-up.

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 accendere una luce o bloccare una porta.

Nota

Aggiungere una porta di output ad AXIS Camera Station 5 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 **Aggiungi** e creare un trigger. 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 della porta.

8. Selezionare **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 fisso, selezionare la seconda opzione e specificare il numero di secondi.

Creazione delle azioni di invio e-mail

L'azione e-mail invia un messaggio e-mail a uno o più destinatari. Si possono allegare istantanee provenienti dalle telecamere attraverso l'e-mail.

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 **Aggiungi** e creare un trigger. 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. Aggiungere i destinatari su **Recipients (Destinatari)**:
   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 **Add (Aggiungi)** per aggiungere l'indirizzo e-mail a **Recipients (Destinatari)**.
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 nella notifica e-mail 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 5. Si può usare **Select all (Selezionare tutto)** per selezionare tutte le telecamere o **Deselect all (Deselezionare tutto)** per la deselezione di tutte le telecamere.
Send one email for each event (Inviare un'e-mail per ogni evento)	Per prevenire l'invio di più e-mail per lo stesso evento, selezionare **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 mail troppo ravvicinate. Selezionare **Don't send another email for (Non inviare altre e-mail per)** e impostare il tempo minimo tra le e-mail dal menu a discesa.

Creazione di azioni della visualizzazione in diretta

L'azione **Live view (Visualizzazione in diretta)** apre la scheda Visualizzazione in diretta con telecamere, viste o posizioni preset specifiche. La scheda **Live view (Visualizzazione in diretta)** si apre in tutti i client AXIS Camera Station 5 connessi. Se la scheda **Live view (Visualizzazione in diretta)** mostra un'immagine suddivisa con un hotspot, la telecamera selezionata nell'azione della visualizzazione in diretta si caricherà 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 5 aperti dalla barra delle applicazioni o portare i client 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 **Aggiungi** e creare un trigger. 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 va mostrato 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 (Apparizione in primo piano)**, selezionare **On trigger bring application to front (In caso di attivazione, visualizza l'applicazione in primo piano)** per ripristinare i client AXIS Camera Station 5 aperti dalla barra delle attività o per portare i client in primo piano rispetto alle altre applicazioni aperte quando viene avviata l'azione Visualizzazione in diretta.
9. Fare clic su **OK**.

Imposta l'immagine dal vivo	
Visualizza	Per aprire una vista, selezionare **View (Vista)** e selezionare la vista dal menu a discesa.
Telecamera	Per aprire una vista telecamera, selezionare **Camera (Telecamera)** e selezionare la telecamera dal menu a discesa. Se la telecamera ha 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)** per non aprire nessuna 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, mostrerà la vista della telecamera nell'hotspot.

Esempio:

Per aprire una scheda **Live view (Visualizzazione in diretta)**, andare alla vista dell'hotspot e visualizzare una vista della telecamera nell'hotspot, configurare due azioni di visualizzazione 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 vada alla vista hotspot e mostri la vista della telecamera nell'hotspot.
   2.1. In **Live view actions (Azioni visualizzazione in diretta)**, seleziona **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. Le notifiche HTTP, ad esempio, possono essere utilizzate per attivare o disattivare una funzione della telecamera o per aprire, chiudere, bloccare 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, può essere necessario regolare le impostazioni proxy del server AXIS Camera Station 5. Vedere *Generale*.

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 **Aggiungi** e creare un trigger. Fare clic su **Next (Avanti)**. Vedere *Aggiunta di trigger*.
4. Fare clic su **Aggiungi** e selezionare **Invia notifica HTTP**.
5. Fare clic su **OK**.
6. 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`
7. Selezionare **Autenticazione richiesta** se il destinatario richiede l'autenticazione. Immettere il nome utente e la password.
8. Fare clic su **Avanzate** per visualizzare le impostazioni avanzate.
9. Fare clic su **OK**.

Avanzata	
Metodo	Selezionare il 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)**.

Avanzata	
Corpo	Per i metodi POST e PUT, immettere il corpo della richiesta in **Body (Corpo)**.
Trigger data (Dati trigger)	si possono anche immettere dati trigger predefiniti dal menu a discesa. per ulteriori informazioni, vedere di seguito;

Trigger data (Dati trigger)	
Tipo	Il trigger che ha eseguito l'attivazione di questa regola di azione.
Source ID (ID sorgente)	L'ID sorgente è l'ID della sorgente che ha attivato la regola di azione e frequentemente rappresenta una telecamera o un tipo di dispositivo diverso. Non tutte le sorgenti sono dotate di un ID sorgente.
Source Name (Nome sorgente)	Il nome sorgente è il nome della sorgente che ha attivato la regola di azione e frequentemente rappresenta una telecamera o un tipo di dispositivo diverso. Non tutte le sorgenti sono dotate di un nome sorgente.
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.

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 **Aggiungi** e creare un trigger. 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 può essere utilizzata per concedere l'accesso, aprire o chiudere 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 5.

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

2. Fare clic su **New..** (Nuovo).
3. Fare clic su **Aggiungi** e creare un trigger. 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. Per eseguire un'azione, selezionare un'azione e una porta.
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 fare clic sulla 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 **Aggiungi** e creare un trigger. 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. In **Message (Messaggio)**, inserire il messaggio che l'app per dispositivi mobili dovrebbe mostrare.
7. In **Click notification and go to (Clicca su notifica e vai a)**, configurare cosa deve essere mostrato quando si fa clic sulla notifica.
8. Fare clic su **OK**.

Fare clic su notifica e vai a	
Telecamera	Selezionare una vista della telecamera dal menu a discesa **Camera (Telecamera)** che dovrebbe apparire facendo clic sulla notifica nell'app per dispositivi mobili.
Ripristino dei valori predefiniti di fabbrica	Selezionare **Default (Predefinito)** per passare alla pagina iniziale dell'app per dispositivi mobile quando si fa clic sulla notifica sull'app per dispositivi mobili.

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

Usare l'azione Attiva o disattiva regole, ad esempio, se si vuole disattivare il rilevamento movimento in un ufficio quando un dipendente fa passare la 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 **Aggiungi** e creare un trigger. 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. Seleziona una o molteplici regole di azione.
7. Scegli se vuoi l'attivazione o disattivazione delle regole di azione selezionate.
8. Inserire un ritardo se si vuole che passi tempo tra l'attivazione e la modifica dello stato.

9. Seleziona **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 vuoi che la regola di azione selezionata resti modificata quando il trigger non è attivo. Nell'esempio di cui sopra, questo vuol dire che il rilevamento movimento si riattiva quando il dipendente rimuove la tessera di accesso dal lettore.
10. Fare clic su **OK**.

Crea azioni di controllo degli accessi

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

- **Azioni porta:** concessione dell'accesso, blocco, sblocco o arresto delle porte selezionate.
- **Azioni zona:** blocco, sblocco o arresto delle porte selezionate nelle zone selezionate.

Nota

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

Per creare un'azione di controllo degli accessi:

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Regole di azione**.
2. Fare clic su **New..** (Nuovo).
3. Fare clic su **Aggiungi** e creare un trigger. 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. Fare clic su **OK**.

Pianificazioni

La pagina Pianificazioni contiene tutte le pianificazioni che è possibile applicare alla registrazione, alle regole di azione e a componenti come AXIS Secure Entry. AXIS Site Designer crea alcune pianificazioni durante l'installazione.

Le pianificazioni consentono di creare e modificare panificazioni giornaliere e settimanali personalizzate, nonché di 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**: Mostra 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 di intervento) è la vista principale per la gestione delle pianificazioni di intervento, dove è possibile vedere quali pianificazioni giornaliere e settimanali sono state applicate.

Nota

Quando sussiste la connessione a molteplici server AXIS Camera Station 5, 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). Assicurarsi che la pianificazione non sia in uso prima di tentare di eliminarla.

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 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 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

Un esempio che mostra come impostare una regola di azione in AXIS Camera Station 5 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 *Aggiunta di dispositivi, on page 41*.
- Configurare il door controller. Vedere *Aggiunta di una porta, on page 137*

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'attivazione dell'evento Apertura forzata della porta.
   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 aperto forzatamente.

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 il 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)**.

Impostazione 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

Un esempio di come creare una regola di azione in AXIS Camera Station 5 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 i titolari di tessere. Vedere *Configurazione del controllo degli accessi, on page 135* e *Gestione degli accessi, on page 160*.
- Installare un dispositivo audio di rete Axis e associare il dispositivo audio a una telecamera. Vedere *Profili di flusso, on page 48*.
- 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 5. Vedere *Porte I/O, on page 83*.

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'attivazione dispositivo da evento.
   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 uscita.
   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 60 secondi per mantenere la porta nello stato.
   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 importante.

Configurazione client

Andare a **Configurazione > Client** per:

- Modificare le impostazioni specifiche del client, come il tema e la lingua. Vedere *Impostazioni client, on page 108*.
- Modificare le impostazioni specifiche dell'utente, come le notifiche e le opzioni di avvio. Vedere *Impostazioni utente, on page 109*.
- Modificare le impostazioni relative alle prestazioni di streaming specifiche del client come il ridimensionamento video e la decodifica hardware. Vedere *Streaming, on page 111*.

Impostazioni client

Queste impostazioni si applicano a tutti gli utenti di AXIS Camera Station 5 sul computer. Andare a **Configuration > Client > Client settings (Configurazione > Client > Impostazioni client)** per configurare le impostazioni del client AXIS Camera Station 5.

Tema	
System, Light, Dark (Sistema, chiaro, scuro)	Selezionare il tema per il client. Per le nuove installazioni, **System** (Sistema) è il tema predefinito. Selezionando **System** (Sistema), il sistema utilizza il tema chiaro o scuro a seconda del tema del sistema di Windows.

Generale	
Esegui applicazione all'avvio di Windows	Da attivare se si vuole che AXIS Camera Station 5 venga eseguito in automatico a ogni avvio di Windows.

Visualizzazione in diretta	
Mostra i nomi delle telecamere nelle visualizzazioni in diretta	Mostrare nome telecamera nella visualizzazione in diretta.
	Abilitare l'opzione **Show recording indicators in live views and maps (Mostra indicatori di registrazione nelle visualizzazioni in diretta e nelle mappe)** per indicare qualsiasi tipo di registrazione.
	Per indicare la registrazione del rilevamento movimento o le registrazioni avviate da una regola di azione, abilitare l'opzione **Show event indicators in live views and maps (Mostra indicatori di eventi nelle visualizzazioni in diretta e nelle mappe)**.

Mappe	
Allow flashing coverage areas for all maps (Permetti aree di copertura lampeggianti per tutte le mappe)	Usarlo per impedire o permettere il lampeggiamento di tutte le aree di copertura impiegando **Flash (Lampeggiamento)**. Tale impostazione globale non incide sull'impostazione locale a livello della mappa. Vedere *Mappa, on page 19*.

Lingua
Cambiare la lingua del client AXIS Camera Station 5. Le modifiche avranno effetto in seguito al riavvio del client.

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 l'opzione per il server, vedere *Impostazioni server, on page 116*.

Impostazioni utente

Queste impostazioni si applicano all'utente che ha eseguito l'accesso ad AXIS Camera Station 5. Andare a **Configuration > Client > User settings (Configurazione > Client > Impostazioni utente)** per configurare le impostazioni utente del client AXIS Camera Station 5.

Sistema di navigazione	
Sistema di navigazione della visualizzazione ad albero	Si attiva per impostazione predefinita per eseguire l'abilitazione del pannello di navigazione della visualizzazione ad albero con le viste e le telecamere.
Show in navigation (Mostra in navigazione)	Selezionare questa opzione al fine della visualizzazione di viste o telecamere o entrambe nel menu a discesa.
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	Eseguire l'attivazione di questa opzione per mostrare una notifica sulla barra delle applicazioni di Windows quando viene aggiunta o terminata 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 viene premuto 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 sul pulsante **Browse (Sfoglia)** per selezionare la cartella in cui salvare le istantanee.

Avvio	
Avvia in modalità Schermo intero	Attivare questa opzione per avviare AXIS Camera Station 5 in modalità a schermo intero.
Ricorda ultime schede usate	Attivare questa opzione per avviare AXIS Camera Station 5 con le stesse schede, viste e viste di telecamera aperte al momento in cui AXIS Camera Station 5 è stato chiuso per l'ultima volta.
Ricorda ultimi monitor usati	Attivare per avviare AXIS Camera Station 5 sullo stesso monitor utilizzato l'ultima volta che AXIS Camera Station 5 è stato chiuso.

Nota

- Il sistema salva le viste e le viste della telecamera per scheda. Il sistema ricorda solo quando il client si riconnette allo stesso server.
- Memorizzare le schede in modo da memorizzare monitor, viste e viste della telecamera.
- 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 se non si desidera nessun segnale di allarme.
Bip	Selezionare se si desidera un segnale acustico standard per l'allarme.

Suono in caso di allarme	
Sound file (File audio)	Selezionare e fare clic su **Browse (Sfoglia)** per trovare un file audio se si desidera un segnale di allarme personalizzato. Impiegare qualsiasi formato di file supportato da Windows Media Player.
Riproduci	Fare clic per testare il suono.

Suono in caso di chiamata in arrivo	
Nessun segnale	Selezionare se non si desidera nessun suono con una chiamata in entrata.
Bip	Selezionare se si desidera un segnale acustico standard per la chiamata in entrata.
Sound file (File audio)	Selezionare e fare clic su **Browse (Sfoglia)** per trovare un file audio se si desidera un segnale di chiamata in entrata personalizzato. Impiegare qualsiasi formato di file supportato da Windows Media Player.
Riproduci	Fare clic per testare il suono.

Caratteristiche	
Mostra ricerca intelligente 1	Per impostazione predefinita appare la ricerca intelligente 1. Eseguire la disattivazione per nascondere questa funzione.

Mostra le finestre di avviso	
Avviso di certificato non valido	Attivare per mostrare questo avviso, se applicabile.

Streaming

Andare a **Configuration > Client > Streaming (Configurazione > Client > Streaming)** per configurare le opzioni di streaming del client AXIS Camera Station 5.

Ridimensionamento del video	
Ridimensionamento ottimale	Selezionare l'opzione per mostrare il video in tutto lo spazio a disposizione, senza perdita delle proporzioni o taglio dell'immagine.
Compila l'area video (parti del video potrebbero essere tagliate)	Selezionare perché il video si adatti allo spazio a disposizione e conservi le proporzioni. Se lo spazio disponibile ha una proporzione diversa rispetto al video, il sistema taglia il video.

Decodifica hardware	
Modalità	• **Automatic (Automatico)** Usare la scheda grafica (se supportata) per decodificare i flussi con una risoluzione superiore a 3840 x 2160p a 25 fps (anche noti come 4K o UHD). • **On (Attivo)** Usare la scheda grafica (se supportata) per decodificare i flussi con una risoluzione superiore a 1920 x 1080p a 25 fps (anche noti come 1080p o HD). • **Off (Inattivo)** La decodifica hardware è disattivata e AXIS Camera Station 5 utilizza la CPU per decodificare il video.
Scheda grafica	selezionare una scheda grafica dal menu a discesa.

Nota

- La decodifica hardware utilizza la scheda grafica per decodificare il video. Se si dispone di una scheda grafica ad alte prestazioni, la decodifica hardware è ideale per migliorare le prestazioni e ridurre l'uso della CPU, soprattutto per lo streaming di video ad alta risoluzione. La decodifica hardware supporta M-JPEG e H.264.
- Le telecamere dotate di una risoluzione al di sotto dei 1080p non si può usare la decodifica hardware, anche se la decodifica hardware è impostata su **On (Attiva)**.
- Se la scheda grafica non offre il supporto per la decodifica 4K, la decodifica hardware funziona unicamente in flussi 1080p, anche se la decodifica hardware è **On (Attiva)**.

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*. Questa impostazione incide sui video H.264 e M-JPEG e abbassa il consumo di banda.
Sospendi flussi video per schede inattive	Eseguire l'attivazione per sospendere i flussi video nelle schede inattive. Ciò abbassa il consumo di banda.

PTZ (Pan, Tilt, Zoom)	
Selezionare la vista con il primo clic invece di avviare PTZ	Attivalo per eseguire l'attivazione della selezione della vista al primo clic nella vista. Tutti i clic successivi nella vista controllano PTZ.

Audio	
Push-to-talk release delay (ms) (Ritardo di rilascio di Premi per parlare (ms))	Regolare la quantità di millisecondi per i quali si desidera conservare l'audio trasmesso dal microfono dopo il rilascio del pulsante **Push-to-talk (Premi per parlare)**.
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 opzione per avere la possibilità di ascoltare e parlare agli interfono anche in assenza di chiamate in corso da essi.

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

Impostazioni di aggiornamento firmware

Nota

Quando ci si connette a più server AXIS Camera Station 5, 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 (A ogni avvio)** dal menu a discesa per controllare le versioni firmware disponibili sul server ad ogni avvio. L'impostazione predefinita di AXIS Camera Station 5 è **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

Importante

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

Cosa significa tutto ciò per il vostro sistema AXIS Camera Station 5?

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

Axis Secure Remote Access consente di connettersi al proprio server AXIS Camera Station 5 mediante una connessione Internet protetta e crittografata. Axis Secure Remote Access non utilizza il port forwarding del router per l'accesso alla telecamera.

Nota

- Axis Secure Remote Access è disponibile solo per AXIS Camera Station 5.12 o versione successiva.
- Quando sussiste la connessione a più server AXIS Camera Station 5, scegliere qualsiasi server dal menu a discesa **Selected server (Server selezionato)** per la configurazione di Axis Secure Remote Access.

Abilitazione di Axis Secure Remote Access

Axis Secure Remote Access è disponibile se si esegue l'accesso al proprio account My Axis. Axis Secure Remote Access deve essere attivato manualmente. Questa funzione permette l'accesso al server remotamente, consultare *Connessione a un server*.

1. Andare a **Configurazione > Servizi connessi > Axis Secure Remote Access**.
2. Nell'account My Axis, inserire le proprie credenziali per l'account My Axis.
3. fare clic su **Applica**;
4. Nella sezione Axis Secure Remote Access, fare clic su **Enable (Abilita)** per attivare l'accesso remoto.

Axis Secure Remote Access su dispositivi mobili

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

1. Utilizzando il dispositivo mobile, 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. Eseguire l'accesso ad Axis Secure Remote Access con lo stesso account My Axis impiegato per l'attivazione dell'accesso remoto.
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.

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

Utilizzo di Axis Secure Remote Access

L'uso di Axis Secure Remote Access appare sulla barra di stato nella parte inferiore del client AXIS Camera Station 5. Fare clic sul collegamento per ottenere una panoramica di come usare la connessione remota sicura.

Livello servizio	mostra il livello di servizio della sottoscrizione ad Axis Secure Remote Access.
Dati utilizzati in questo mese	Mostra i dati utilizzati nel mese corrente. Il contatore si azzera il primo giorno di ogni mese a mezzanotte.
Eccedenza	Mostra i dati utilizzati nel mese corrente che hanno superato la quantità inclusa nel proprio livello di servizio. Questa opzione è disponibile solo se si ha Eccedenza nell'abbonamento.
Connessioni	Mostra i server che sono connessi attraverso Secure Remote Access.

Imposta il servizio cloud di Monitoraggio dell'integrità del sistema di AXIS

Il Servizio cloud di monitoraggio dell'integrità di sistema di AXIS permette il monitoraggio dei dati relativi all'integrità dei sistemi ubicati su reti diverse. Per ulteriori informazioni, vedere *Società/organizzazioni, on page 115*.

Si deve creare un account My Axis prima di eseguire l'impostazione del Servizio cloud di monitoraggio dell'integrità di sistema di AXIS. Vedere *my.axis.com*.

1. Andare a **Configuration System Health Monitoring > Settings (Configurazione Monitoraggio dell'integrità del sistema > Impostazioni)**.
2. Fare clic su **Manage (Gestisci)**.
3. Eseguire l'accesso con il proprio account My Axis e seguire le istruzioni sullo schermo.

Società/organizzazioni

L'organizzazione è al centro dei tuoi servizi cloud.

- Connette il sistema AXIS Camera Station 5 agli utenti dei diversi servizi cloud.
- Attivare il Monitoraggio dell'integrità del sistema con base su cloud. Per ulteriori informazioni, vedere *Imposta il servizio cloud di Monitoraggio dell'integrità del sistema di AXIS, on page 115*.
- Definisce i diversi ruoli utente, ad es. l'amministratore del servizio e l'operatore.
- Si può strutturare un'organizzazione in cartelle che, ad esempio, rappresentano sistemi ubicati in siti diversi. Per la creazione di un'organizzazione, ti serve un account My Axis. Vedere *my.axis.com*.

Disconnetti un sistema da un'organizzazione

In determinati casi, si potrebbe dover disconnettere un sistema dalla sua organizzazione corrente. Ad esempio, quando si sposta un sistema da un'organizzazione a un'altra.

1. Andare a **Configuration > Connected services > AXIS System Health Monitoring Cloud Service (Configurazione > Servizi connessi > Servizio cloud di monitoraggio dell'integrità di sistema di AXIS)**.
2. Fai clic su **Disconnect (Disconnetti)**.

Invita un utente ad un'organizzazione

1. Andare a **Configuration > System Health Monitoring > Settings (Configurazione > Monitoraggio dell'integrità del sistema > Impostazioni)**.
2. Fare clic su **Open AXIS System Health Monitoring Cloud Service (Apri Servizio cloud di monitoraggio dell'integrità di sistema di AXIS)**.
3. Selezionare l'organizzazione a cui si desidera invitare l'utente.
4. Aprire le impostazioni dell'utente e fare clic su **Manage organizations (Gestisci organizzazioni)**.

5. Apri la scheda **Users (Utenti)**.
6. Fare clic su **Generate (Genera)**.
7. Copia il codice d'invito e invialo all'utente che vuoi invitare.

Nota

Quando si condivide il codice d'invito con l'utente, includere il nome dell'organizzazione nell'invito.

Aderisci ad un'organizzazione

Si riceve un codice di invito quando qualcuno vuole che l'utente aderisca ad un'organizzazione. Per aderire all'organizzazione:

1. Copiare il codice invito.
2. Andare a **Configuration > System Health Monitoring > Settings (Configurazione > Monitoraggio dell'integrità del sistema > Impostazioni)**.
3. Fare clic su **Open AXIS System Health Monitoring Cloud Service (Apri Servizio cloud di monitoraggio dell'integrità di sistema di AXIS)**.
4. Selezionare l'organizzazione a cui si desidera invitare l'utente.
5. Aprire le impostazioni dell'utente e fare clic su **Manage organizations (Gestisci organizzazioni)**.
6. Apri la scheda **Users (Utenti)**.
7. Incolla il codice invito.
8. Fai clic su **Join (Aderisci)**.

Configurare server

Impostazioni server

Andare a **Configuration > Server > Settings (Configurazione > Server > Impostazioni)** per configurare le impostazioni del server AXIS Camera Station 5.

Nota

Quando sussiste la connessione a più server AXIS Camera Station 5, scegliere qualsiasi server dal menu a discesa **Selected server (Server selezionato)** per la configurazione delle 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 controlli. Impostare un valore tra 7 e 1000 giorni.

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 configurazione 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. In **Sender (Mittente)**, immettere l'indirizzo e-mail e il nome che si vuole sia visualizzato nell'e-mail del 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 se sono necessari un nome utente e una password per il server. Immettere il nome utente e la password per accedere al server.

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 a comparsa, fare clic su **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 a comparsa, 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 utilizzare le frecce per cambiare l'ordine dei server nell'elenco. Il sistema usa i server nello stesso ordine in cui sono elencati.

Risultati test del server	
OK	la connessione al server SMTP è stata stabilita correttamente. Verificare 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 5 non può accedere al server SMTP. Verificare che il server SMTP funzioni correttamente e che tutti i router e i server proxy presenti tra AXIS Camera Station 5 e il server SMTP consentano il traffico.
Errore di configurazione	È stato richiesto TLS ma il server non supporta StartTLS, il server non supporta l'autenticazione o non c'è alcun meccanismo di autenticazione compatibile.

Risultati test del server	
Errore di handshake TLS/SSL	Errore nel corso dell'autenticazione TLS/SSL, come certificato server non valido.
Autenticazione richiesta	Il server necessita dell'autenticazione per l'invio di e-mail.
Errore di autenticazione	Le credenziali sono errate.
Connessione eliminata	La connessione è stata stabilita, ma poi è stata persa.

Allarme sistema

Un allarme di sistema viene generato se una telecamera perde la connessione, quando viene negato l'accesso all'archiviazione di registrazione, se si verifica un arresto imprevisto del server o in caso di errori di registrazione. Si possono mandare notifiche e-mail su 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 **Invia e-mail in caso di allarme sistema ai seguenti destinatari** 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 **Aggiungi** per aggiungere l'indirizzo e-mail nella casella **Destinatari**.

Connessione al dispositivo	
Continua a utilizzare gli hostname anche se diventano irraggiungibili	Usare il nome host per eseguire la connessione. Per passare automaticamente all'utilizzo dell'indirizzo IP per connettersi, 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 67*.

Lingua	
Modifica la lingua del server	Consente la modifica del nome di AXIS Camera Station 5 Service Control e AXIS Camera Station Secure Entry. Ad esempio: allarmi di sistema, messaggi registro di controllo e dati esterni nella scheda **Data search (Ricerca dati)**. Le modifiche avranno effetto in seguito al riavvio.

Body Cam	
Disco **Cartella**	Selezionare l'unità e la cartella in cui si desidera ricevere 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.	Questo è il tempo di conservazione del contenuto rifiutato.

Feedback	
Condividi i dati di utilizzo dei server anonimi con Axis Communications	Selezionare questa opzione per contribuire al miglioramento dell'applicazione e dell'esperienza utente. Per eseguire la modifica delle opzioni per il client, consultare *Impostazioni client, on page 108*.

Impostaz. avanzate

È necessario modificare le impostazioni solo quando richiesto dal supporto 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 scopi di risoluzione dei problemi, selezionare **Enable server side debug logging (Abilita registrazione debug lato server)**. Questa impostazione utilizza maggiore spazio sul disco e il file `log4net.config` nella cartella **ProgramData** la sovrascrive.

Aggiorna AXIS Camera Station 5

Per avere la versione più recente di AXIS Camera Station 5:

1. Andare a **Configuration > Server > Update (Configurazione > Server > Aggiornamento)**.
2. Fare clic su **Download and install... (Scarica e installa...)**.

Nota

- Dopo l'inizio di un aggiornamento, che sia manuale o pianificato, non si può annullare.
- Gli aggiornamenti pianificati cominciano in automatico.
- Il sistema non esegue l'aggiornamento dei client connessi attraverso secure remote access.
- 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 viene visualizzata l'interfaccia utente o l'indicatore di avanzamento. Mantenere acceso il computer server fino al riavvio del client e del server.
- Questa funzione usa il programma di installazione di Windows (msi) a prescindere dal tipo che si usa correntemente.

Report eventi

Se si attiva l'autorizzazione per i report degli incidenti, è possibile generare report dell'incidente che comprendano registrazioni, istantanee e note relative agli incidenti. Vedere *Esporta report dell'incidente, on page 29*.

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. Selezionare un formato nel quale si desidera esportare le registrazioni dal menu a discesa **Export format (Formato di esportazione)**.
4. In **Categories (Categorie)**, aggiungere o eliminare le categorie per raggruppare i report dell'incidente. Le categorie possono essere il nome della cartella nella posizione di esportazione se si configura la categoria come una variabile nel percorso del server.
   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 puoi: Riportato da: <Inserire nome, e-mail e numero di telefono>.
6. fare clic su **Applica**;

Location	
Server directory path (Percorso del server)	Selezionare ed inserire il percorso della cartella per salvare i 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 5. Vedere *Gestione dello spazio di archiviazione* per le modalità di aggiunta del dispositivo di archiviazione per utilizzare le registrazioni.

Formato di esportazione	
ASF	Se viene selezionato, si può scegliere **Add digital signature (Aggiungi la firma digitale)** per impiegare una 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 eseguire la creazione di pianificazioni per esportare le registrazioni.

All'ora selezionata, comincerà l'esportazione di tutte le registrazioni effettuate dopo l'esportazione precedente. Se l'esportazione precedente risale a più di una settimana prima o se non c'è alcuna esportazione precedente, l'esportazione conterrà solo registrazioni avvenute da meno di una settimana. Per esportare le registrazioni

precedenti, accedere alla scheda **Recordings (Registrazioni)** ed esportarle manualmente. Vedere *Esportazione delle registrazioni*.

Nota

Quando ci si connette a più server AXIS Camera Station 5, selezionare qualsiasi server dal menu a discesa **Selected server (Server selezionato)** per attivare e gestire le esportazioni pianificate.

Esporta registrazioni pianificate

1. In **Scheduled export (Esportazione pianificata)**, selezionare **Enable scheduled export (Abilita esportazione pianificata)** per usare l'esportazione pianificata.
2. In **Cameras (Telecamere)**, selezionare le telecamere da cui esportare le registrazioni. Il sistema seleziona ogni telecamera elencata come 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 5. 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	Scegliere un formato in cui eseguire l'esportazione delle registrazioni. **ASF** – scegliere **Add digital signature (Aggiungi firma digitale)** per usare una firma digitale al fine di rendere impossibile 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.

Microsoft Windows 2008 Server

Per poter esportare le registrazioni da un server su cui è installato Microsoft Windows 2008 Server, si deve installare Desktop Experience:

1. Fare clic su **Start > Strumenti di amministrazione > Server Manager** per aprire Gestione server.

2. In **Features Summary (Riepilogo funzionalità)**, fare clic su **Add features (Aggiungi funzionalità)**.
3. Selezionare **Desktop Experience**, fare clic su **Next (Avanti)**.
4. fare clic su **Install (Installa)**.

Microsoft Windows 2012 Server

Per poter esportare le registrazioni da un server su cui è installato Microsoft Windows 2012 Server, si deve 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)**.

Nuova connessione

Andare su ☰ **> Servers > New connection (> Server > Nuova connessione)** per connettersi a un server AXIS Camera Station 5. Vedere *Connessione a un server*.

Stato connessione

Andare a ☰ **> Servers > Connection status (Server > Stato connessione)**, viene per visualizzare un elenco dello stato delle connessioni.

Usare il cursore di fronte al nome del server per eseguire la connessione o disconnessione dal server.

Codici di stato	Descrizione	Soluzioni possibili
Collegamento in corso	Il client tenta di connettersi a questo server.	
Collegato	Il client usa TCP mentre è connesso a questo server.	
Connessione stabilita (mediante Secure Remote Access)	Il client usa Secure Remote Access mentre è connesso a questo server.	
Collegato (tramite 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 disconnette dal server.	
Scollegato	Non esiste alcuna connessione fra il client e questo server.	
Riconnessione	Il client ha perso la connessione al server e tenta di riconnettersi.	
Riconnessione non riuscita	Il client non riesce a riconnettersi al server. Trova il server ma le autorizzazioni o la password	• aggiungere l'utente nella finestra di dialogo delle autorizzazioni utente;

	dell'utente possono essere cambiate.	• 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 autorizzazioni utente;
Verifica di sicurezza non riuscita	Un controllo di sicurezza WCF non riesce. Accertarsi di eseguire la sincronizzazione dell'ora UTC di client e computer server.	
Nessun contatto con il computer server	Assenza di risposta dal computer server all'indirizzo utilizzato.	• Verificare che la rete funzioni correttamente. • Controllare che il server sia in esecuzione.
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.	• Verificare che la rete funzioni correttamente. • Controllare che il server sia in esecuzione.
Nome host non valido	Il DNS non è in grado di eseguire la conversione del nome host in un indirizzo IP.	• Verificare che l'ortografia del nome host sia corretta. • verificare che il DNS disponga delle informazioni necessarie.
Già connesso allo stesso server	Il client è già connesso al server.	Rimuovere il server duplicato.
Server non previsto	A questo indirizzo risponde un server diverso rispetto a quello previsto.	aggiornare l'elenco dei server per connettersi al server.
La versione del client (x) non è compatibile con la versione del server (y)	Il client è obsoleto o troppo recente rispetto al server.	Verificare che sul client e sul computer server sia installata la stessa versione di AXIS Camera Station 5.
Server occupato	Il server non ha potuto rispondere a causa di problemi di prestazioni.	Verificare che il computer server e la rete non subiscano un sovraccarico.

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

Più server

Elenchi dei server

È possibile organizzare i server AXIS Camera Station 5 in appositi elenchi. Un server può appartenere a più elenchi dei server. Si possono importare, esportare e usare elenchi server in altri client AXIS Camera Station 5.

Andare a > **Servers > Server lists (> Server > Elenchi dei server)** per aprire la finestra di dialogo degli elenchi dei server.

L'elenco **Recent connections (Connessioni recenti)** predefinito mostra e contiene i server utilizzati nella sezione precedente. Non si possono rimuovere le **Recent connections (Connessioni recenti)**.

	Selezionare l'elenco dei server e fare clic su .
+ New server list (+ Nuovo elenco di server)	fare clic per aggiungere un nuovo elenco di server e immettere il nome dell'elenco.
Aggiungi	Per eseguire l'aggiunta di un server a un elenco server, selezionarne uno e fare clic su 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 l'elenco di server per accedere ai server. Vedere *Connessione a un server*.
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 i server in un elenco di server, selezionare i server e fare clic su **Remove (Rimuovi)**.
Rinominare un server	Fare doppio clic sull'elenco e immettere un nuovo nome per l'elenco.

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

Organizzare i server in elenchi di server

Configura Switch

Se si ha un dispositivo di serie AXIS Camera Station S22 Appliance, si può eseguire la relativa configurazione da AXIS Camera Station 5. Andare a **Configuration > Switch > Management (Configurazione > Switch > Gestione)** e inserire le credenziali per aprire la pagina di gestione switch nel client AXIS Camera Station 5. Per sapere in che modo si configura lo switch, consultare il manuale per l'utente AXIS Camera Station S22 Appliance su *axis.com*.

Nota

AXIS Camera Station 5 può connettersi solo a https://192.168.0.1/ che corrisponde all'indirizzo IP predefinito dello switch.

Configurazione delle licenze

Sulla pagina Licenza, è possibile visualizzare le chiavi di licenza, lo stato delle licenze e gestire le licenze dei dispositivi connessi.

Nota

- Quando sussiste la connessione a molteplici server AXIS Camera Station, scegliere qualsiasi server dal menu a discesa **Selected server (Server selezionato)** per gestire le licenze.
- Si consiglia di annotare le chiave di licenza o di salvarle in formato digitale su un'unità USB per utilizzarle come riferimento in futuro. Non si possono recuperare le chiavi di licenza perse.
- Quando si registra il registratore video di rete Axis in AXIS License Portal, si riceve una licenza Core NVR. Le licenze NVR core sono bloccate sull'hardware del dispositivo e non possono essere spostate. È possibile aggiornare NVR Core a Universal allo stesso modo delle licenze Core. Le licenze aggiornate si possono spostare e utilizzare per qualsiasi sistema.

Gestione delle licenze

Andare a **Configurazione > Licenze > Gestione** per una panoramica del numero di dispositivi senza licenza collegati al server. Si possono gestire le licenze online e offline. Ricordare di aggiungere le licenze per tutti i dispositivi prima della fine del periodo di prova di 30 giorni. Vedere *Come acquistare le licenze*. È anche possibile fare clic sul collegamento relativo allo stato delle licenze nella barra di stato per vedere la panoramica delle licenze del dispositivo.

Come amministratore della licenza, si possono aggiungere molteplici account My Axis al sistema AXIS Camera Station.

Aggiungere un account My Axis a un sistema online

1. andare a **Configuration (Configurazione) > Licenze > Management (Gestione)**.
2. Assicurarsi che **Manage licenses online (Gestisci licenze online)** sia attivo.
3. Fai clic su **Go to AXIS License Portal (Vai ad AXIS License Portal)**.
4. In AXIS License Portal, accedere con il nuovo account My Axis che si desidera aggiungere.
5. Passare a **Edit license admins (Modifica informazioni sulla licenza)** e verificare che l'account sia stato aggiunto come amministratore della licenza.

Aggiungere un account My Axis a un sistema offline

1. andare a **Configuration (Configurazione) > Licenze > Management (Gestione)**.
2. Disattivare **Manage licenses online (Gestisci licenze online)**.
3. Fare clic su **Esporta file di sistema**.
4. Salvare il file di sistema su un'unità flash USB.
5. Andare al portale della licenza AXIS, *license-portal.lp.axis.com*.
6. Eseguire l'accesso con l'account My Axis nuovo che si vuole aggiungere.
7. Caricare il proprio file di sistema.
8. Passare a **Edit license admins (Modifica informazioni sulla licenza)** e verificare che l'account sia stato aggiunto come amministratore della licenza.

Le licenze per il sistema possono essere ottenute in modi diversi a seconda della connessione a Internet.

- *Ottenimento di una licenza per un sistema online*
- *Ottenimento di una licenza per un sistema offline*
- *Spostamento delle licenze tra i sistemi, on page 126*

Stato dispositivi

Andare a **Configuration > Licenses > Device status (Configurazione > Licenze > Stato dispositivo)** per visualizzare un elenco di tutti i dispositivi connessi e lo stato delle licenze.

Tasti

Andare a **Configurazione > Licenze > Chiavi** per visualizzare un elenco delle chiavi necessarie per ciascuna licenza per tutti i dispositivi connessi.

Ottenimento di una licenza per un sistema online

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

1. andare a **Configuration (Configurazione) > Licenze > Management (Gestione)**.
2. Assicurarsi che **Manage licenses online (Gestisci licenze online)** sia attivo.
3. Accedi con l'account MyAxis.
4. In **Add license key (Aggiungi chiave di licenza)**, immettere la chiave di licenza.
5. Fare clic su **Aggiungi**.
6. Nel client AXIS Camera Station assicurarsi che le chiavi di licenza appaiano in **Configuration > Licenses > Keys (Configurazione > Licenze > Chiavi)**.

Ottenimento di una licenza per un sistema offline

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

Spostamento delle licenze tra i sistemi

Nota

Non si possono spostare le licenze NVR Core perché sono bloccate sull'hardware del dispositivo.

Per spostare le licenze da un sistema a un altro sistema con lo stesso account My Axis:

1. Andare al portale della licenza AXIS, *license-portal.lp.axis.com*.
2. In **My systems** (I miei sistemi), fare clic sul nome del sistema da cui si desidera spostare una licenza.
3. In **License keys (Chiavi di licenza)**, trovare la chiave di licenza che si desidera spostare.
4. Fare clic su ⋮ e su **Move (Sposta)**.

5. Nel menu a discesa **To system (Sistema di destinazione)**, selezionare un sistema verso cui si desidera spostare la licenza.
6. Fare clic su **Move license key (Sposta chiave di licenza)** e fare clic su **Close (Chiudi)**. Puoi trovare i dettagli dell'azione in **History (Cronologia)**.
7. Andare a **My systems** (I miei sistemi) e accertarsi che le licenze compaiano nel sistema corretto.



Sposta licenze in un altro sistema

Per rilasciare le licenze da un sistema e aggiungerle a un altro con un account My Axis diverso:

1. Andare al portale della licenza AXIS, *license-portal.lp.axis.com*.
2. In **My systems** (I miei sistemi), fare clic sul nome del sistema da cui si desidera spostare una licenza.
3. In **License keys (Chiavi di licenza)**, trovare la chiave di licenza che si desidera spostare.
4. Effettuare prima una copia della chiave di licenza.
5. Fare clic su ⋮ e **Release (Rilasciare)**.
6. Disconnessione e accesso con un altro account My Axis.
7. In **My systems** (I miei sistemi), fare clic sul sistema a cui si desidera concedere una licenza.
8. In **Add license key (Aggiungi chiave di licenza)**, inserire la chiave di licenza rilasciata.
9. Fare clic su **Aggiungi**. Puoi trovare i dettagli dell'azione in **History (Cronologia)**.
10. Andare a **My systems** (I miei sistemi) e accertarsi che le licenze compaiano nel sistema corretto.

Configura sicurezza

Autorizzazioni utente

Andare a **Configuration > Security > User permissions (Configurazione > Sicurezza > Autorizzazioni utente)** per visualizzare gli utenti e i gruppi che esistono in AXIS Camera Station 5.

Nota

Agli amministratori del computer su cui viene eseguito il server AXIS Camera Station 5 vengono assegnati determinati privilegi di amministratore di AXIS Camera Station 5. Non è possibile cambiare o rimuovere i privilegi del gruppo degli Amministratori.

Prima di poter aggiungere un utente o gruppo, registrare l'utente o gruppo nel computer locale o assicurarsi che abbiano un account utente in Windows® Active Directory. Per aggiungere utenti o gruppi, vedere *Aggiunta di utenti o gruppi*.

Quando un utente fa parte di un gruppo, l'utente dispone delle autorizzazioni di ruolo più elevate assegnate al singolo utente o al gruppo. All'utente viene anche concesso l'accesso come utente singolo e riceve i diritti come parte del gruppo. Ad esempio, un utente ha l'accesso alla telecamera X come singolo. L'utente è inoltre un membro di un gruppo che dispone dell'accesso alle telecamere Y e Z. L'utente perciò dispone di accesso alle telecamere X, Y e Z.

person	Indica se la voce si riferisce a un utente singolo.
group	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 dato all'utente o gruppo. I possibili valori sono: Amministratore, Operatore e Visualizzatore.
Dettagli	Informazioni dettagliate sull'utente come visualizzate nel 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 5. Per aggiungere un utente a AXIS Camera Station 5, è necessario aggiungere utenti o un gruppo a Windows®.

Per aggiungere un utente in Windows® 10 e 11:

- Premere il tasto Windows + X e selezionare **Computer Management (Gestione computer)**.
- Nella finestra **Computer Management (Gestione computer)**, spostarsi su **Local Users and Groups (Utenti e gruppi locali)** > **Users (Utenti)**.
- Fare clic con il tasto destro del mouse su **Users (Utenti)** e selezionare **New user (Nuovo utente)**.
- Nella finestra di dialogo a scomparsa, inserire i dettagli del nuovo utente e deselezionare **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**.
   È possibile vedere gli utenti e i gruppi disponibili nella lista.
3. In **Scope (Ambito)**, scegliere dove si devono cercare utenti e gruppi.
4. In **Show (Mostra)**, selezionare per mostrare utenti o gruppi.
   Il risultato della ricerca non viene visualizzato se esistono troppi utenti o gruppi. Usa la funzione filtro.
5. Selezionare gli utenti o i gruppi e fare clic su **Aggiungi**.

Ambito	
Server	Selezionare per cercare utenti o gruppi sul computer locale.
Dominio	Selezionare per eseguire la ricerca di utenti o gruppi Active Directory.
Server selezionato	Quando si è connessi a più server AXIS Camera Station 5, selezionare un server dal menu a discesa **Selected server (Server selezionato)**.

Configurare un utente od un gruppo

1. Selezionare un utente o un gruppo nell'elenco.
2. In **Role (Ruolo)**, selezionare **Administrator (Amministratore)**, **Operator (Operatore)** o **Viewer (Visualizzatore)**.

3. Se si è selezionato **Operator (Operatore)** o **Viewer (Visualizzatore)**, è possibile configurare i privilegi utente o gruppo. Vedere *Privilegi utente o di gruppo*.
4. Fare clic su **Save** (Salva).

Rimuovere un utente od un gruppo

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

Privilegi utente o di gruppo

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

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

Operatore – Selezionare telecamere, viste e porte I/O per ottenere l'accesso alle immagini dal vivo e registrate. Un operatore ha pieno accesso a tutte le funzionalità di AXIS Camera Station 5 ad eccezione della configurazione del sistema.

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

Telecamere

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

Accesso	consente l'accesso alla telecamera e a tutte le relative funzioni.
Video	consente l'accesso al video dal vivo dalla telecamera.
Ascolta con audio	consente l'accesso per ascoltare l'audio dalla telecamera.
Parla con audio	consente l'accesso per parlare alla telecamera.
Registrazione manuale	consente di avviare e interrompere le registrazioni manualmente.
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 se **Mechanical PTZ (PTZ meccanico)** è 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 5.
Modifica	Consentire la modifica delle viste in AXIS Camera Station 5.

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 l'	consente di visualizzare lo stato della porta I/O. L'utente non è in grado di modificare lo stato della porta.
Scrittura	consente di modificare lo stato della porta I/O.

Sistema

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

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

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

Controllo accessi

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

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

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

Monitoraggio dell'integrità del sistema

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

Configurazione di Monitoraggio dell'integrità del sistema	Permette di configurare il sistema di monitoraggio dell'integrità del sistema.
Accesso a monitoraggio dell'integrità del sistema	Consentire l'accesso al sistema di monitoraggio dell'integrità del sistema.

Certificati

Per la gestione delle impostazioni per i certificati tra il server AXIS Camera Station 5 e i dispositivi, 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 66*.

AXIS Camera Station 5 si può usare come:

- **Autorità di certificazione (CA) radice:** Se si utilizza AXIS Camera Station 5 come autorità di certificazione root significa che AXIS Camera Station 5 utilizza il proprio certificato root per rilasciare certificati server e non verrà coinvolta nessuna autorità di certificazione root nel processo.
- **Autorità di certificazione intermedia:** In questo scenario è necessario importare un certificato CA e la relativa chiave privata in AXIS Camera Station 5 per firmare e rilasciare certificati server per i dispositivi Axis. Tale certificato CA può consistere in un certificato root o un certificato CA intermedio.

Nota

Quando disinstalli AXIS Camera Station 5, 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 5 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 5 come autorità di certificazione root, oppure importare un certificato di autorità di certificazione e lasciare che AXIS Camera Station 5 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 5 archivia la password.
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 tutti 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: • **Senza 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 5. • **Con chiave privata:** Salva il CA in formato PKCS#12 (.pfx o .p12). Utilizzare questa opzione se è necessario importare il CA su un altro server AXIS Camera Station 5.
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). Tenere conto che 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 5 si avvia, cercare un'autorità di certificazione. Se manca, genera una root di autorità di certificazione in automatico. Include un certificato root autofirmato e una chiave privata protetta da password. AXIS Camera Station 5 memorizza la password ma non la rende visibile. Un certificato CA generato da AXIS Camera Station 5 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 133*.

Se si esegue l'aggiornamento dalla versione 5.45 o precedente che utilizza un certificato installato manualmente su un dispositivo, AXIS Camera Station 5 usa automaticamente la CA root esistente per installare un nuovo certificato quando il certificato installato manualmente 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 di un'autorità di certificazione da un'altra autorità di certificazione si può usare AXIS Camera Station 5 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 5 di firmare i certificati per conto di tale 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 si deve usare 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 133*.

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. È necessario fare clic su **OK** per continuare.
- Quando importi un certificato CA, è aggiunto ai Windows Trusted Root Certificates.
- Dopo la disinstallazione di AXIS Camera Station 5, 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 il 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 device certificate (Convalida certificato dispositivo)**.

HTTPS

Per impostazione predefinita, AXIS Camera Station 5 convalida la firma del certificato server HTTPS attivo su ciascun dispositivo connesso e non si connette a un dispositivo senza un certificato convalidato. Il certificato del server deve essere firmato dall'autorità di certificazione attiva in AXIS Camera Station 5 o convalidato tramite Windows Certificate Store. AXIS Camera Station 5 verifica inoltre se l'indirizzo nel certificato HTTPS del dispositivo corrisponde all'indirizzo utilizzato per comunicare con il dispositivo se 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. Tali certificati non sono attendibili. Invece, generare o importare un CA per permettere ad AXIS Camera Station 5 di emettere nuovi certificati per i dispositivi quando si usa HTTPS.

Ignora temporaneamente convalida certificato	Attivare per consentire a AXIS Camera Station 5 di accettare qualsiasi certificato HTTPS e permettere di configurare dispositivi non sicuri. Disattivare in modo che AXIS Camera Station 5 convalidi i certificati del dispositivo. Nel caso non sia attendibile, appare un messaggio di avviso **Status (Stato)** in **Device management (Gestione dispositivi)** e il dispositivo non è accessibile.
Convalida indirizzo dispositivo	Disattivare per ottenere un comportamento stabile su reti DHCP senza impiegare i nomi host. Attivarla per richiedere che gli indirizzi corrispondano in modo da ottenere sicurezza in più. Consigliamo l'attivazione di questa impostazione solo su reti in cui i dispositivi usano principalmente il nome host per comunicare o i dispositivi hanno un indirizzo IP statico.

Nota

- Quando una connessione sicura (HTTPS) non è disponibile, è possibile emettere un nuovo certificato HTTPS. Vedere *Aggiunta di dispositivi, on page 41*
- Per utilizzare HTTPS, per i dispositivi video serve il firmware 5.70 o versione successiva e per i dispositivi di controllo degli accessi e audio il firmware 1.25 o versione successiva.

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 "Crittografata e non crittografata" oppure "Solo crittografata" per consentire la comunicazione "Digest".
- Non si può eseguire l'attivazione di HTTPS su AXIS T85 PoE+ Network Switch Series.

IEEE 802.1X

Per l'autenticazione IEEE 802.1X di AXIS Camera Station 5, il supplicant è un dispositivo di rete Axis che desidera collegarsi 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 originato esternamente, ad esempio dal server di autenticazione IEEE 802.1X oppure direttamente da AXIS Camera Station 5. Questo certificato si installa su ciascun dispositivo Axis e verifica il server di autenticazione.

Nota

Per utilizzare i certificati IEEE 802.1X, serve il firmware 5.50 o versione successiva per i dispositivi video e il firmware 1.25 o versione successiva per i dispositivi di controllo degli accessi e audio.

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 EAP (Extensible Authentication Protocol) si desidera utilizzare.
3. Nel menu a discesa **EAP identity (Identità EAP)**, selezionare questa opzione per utilizzare il testo personalizzato, il MAC address o il nome host del dispositivo.
4. Se è stata selezionata l'opzione **Custom (Personalizzato)**, immettere qualsiasi testo che funga da identità EAP nel campo **Custom (Personalizzato)**.
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 quando AXIS Camera Station 5 funge da autorità di certificazione.
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 mancano di 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 "Crittografata e non crittografata" oppure "Solo crittografata" 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 5, al certificato CA di AXIS Camera Station 5 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 5.

Rinnovo dei certificati

Rinnovo certificato tra il server e i dispositivi

I certificati client o server del dispositivo generati da AXIS Camera Station 5 si rinnovano automaticamente 7 giorni prima che appaia l'avviso della scadenza. Affinché ciò sia possibile, HTTPS o IEEE 802.1X deve essere attivo sul dispositivo. Per eseguire il rinnovo o l'aggiornamento manuale di un certificato, vedere *Sicurezza, on page 66*.

Rinnovo certificato tra il server e il client

1. Andare a **Configuration (Configurazione)** > **Security (Sicurezza)** > **Certificates (Certificati)**.
2. In **Certificate renewal (Rinnovo del certificato)**, fai clic su **Renew (Rinnova)**.
3. Riavvia il server per applicare il certificato rinnovato.

Reset della password

1. Andare a **Configuration > Security > Certificates (Configurazione > Sicurezza > Certificati)**.
2. Disattivare **Validate device certificate** (Convalida certificato dispositivo) per far sì che i dispositivi che usano certificati CA siano 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 il 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 5, vedere *Imposta un network door controller Axis*.

Nota

Prima di iniziare, fare quanto segue:

- Effettuare un aggiornamento della 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 creare un nuovo profilo di identificazione, vedere *Profili di identificazione, on page 149*.
2. Per utilizzare un'impostazione personalizzata per i formati della tessera e la lunghezza del PIN, vedere *Formati tessera e PIN, on page 150*.
3. Aggiungere una porta e applicare un profilo di identificazione alla porta. Vedere *Aggiunta di una porta, on page 137*.
4. Configurare la porta.
   - *Aggiungi un monitor porta, on page 142*
   - *Aggiungi ingresso di emergenza, on page 143*
   - *Aggiungi un lettore, on page 144*
   - *Aggiungi un dispositivo REX, on page 146*
5. Aggiungere una zona e aggiungere porte alla zona. Vedere *Aggiunta di una zona, on page 146*.

Compatibilità del software del dispositivo per i door controller

La tabella seguente mostra la versione minima e consigliata di AXIS OS per ciascuna versione di AXIS Camera Station 5:

Versione AXIS Camera Station	Versione AXIS OS consigliata
5.59	12.4.68.1
5.58	12.4.68.1
5.57	11.8.20.2

Porte e zone

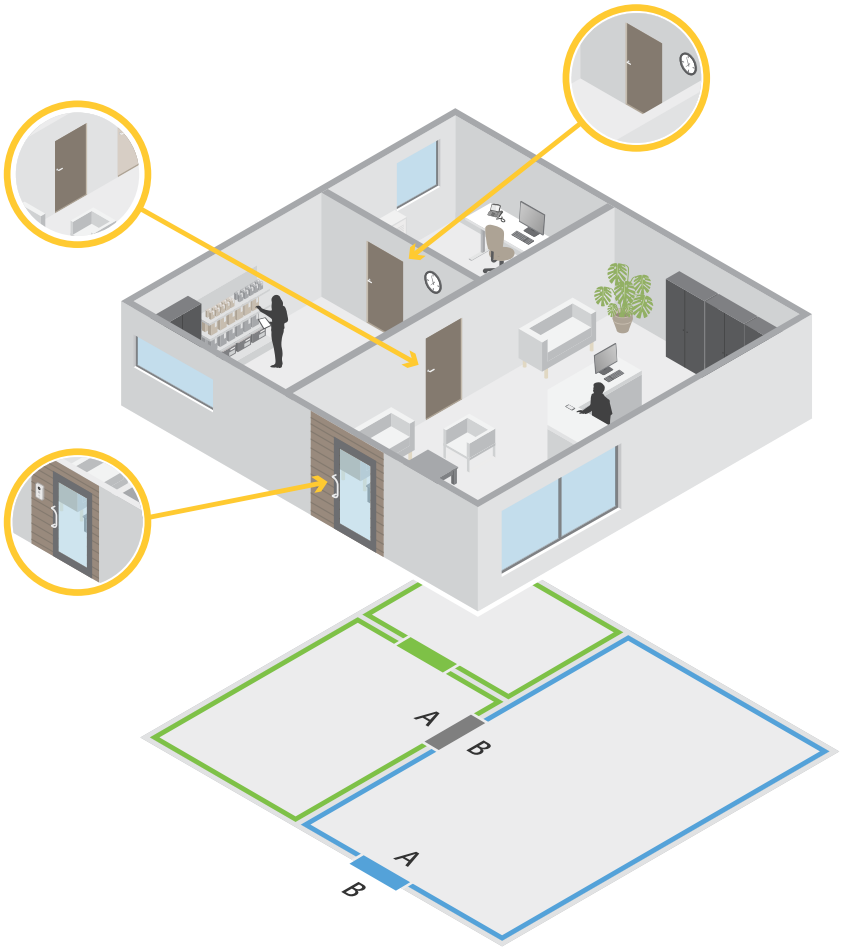
Andare a **Configuration > Access control > Doors and zones (Configurazione > Controllo degli accessi > Porte e zone)** per ottenere una panoramica ed eseguire la configurazione di porte e zone.

Schema dei PIN	Visualizzare lo schema dei pin del controller associato a una porta. Per stampare lo schema dei pin, fare clic su **Print (Stampa)**.
Profilo di identificazione	Cambiare il profilo di identificazione delle porte.
Canale sicuro	Disattivare o attivare OSDP Secure Channel per uno specifico lettore.

Porte	
Nome	Il nome della porta.
Door controller	Il 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.
Formati tessera e PIN	Mostra il tipo di formato tessera o la lunghezza del PIN.
Stato	lo stato della porta. • **Online:** la porta è online e funziona correttamente.

	• **Lettore offline:** il lettore nella configurazione della porta è offline. • **Errore lettore:** il lettore nella configurazione della porta non supporta il canale sicuro oppure il canale sicuro non è attivato per il lettore.
Zone	
Nome	Il nome della zona.
Numero di porte	Numero di porte incluse nella zona.

Esempio di porte e zone



- Esistono due zone: la zona verde e la zona blu.
- Esistono 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.

Creare una nuova configurazione porta 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 door** (Aggiungi porta) e seleziona 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.
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 141*.
Porta di monitoraggio	Una porta in grado di segnalare se è aperta o chiusa. Per ulteriori informazioni, vedere .
Porta predisposta	Una porta che è possibile aggiungere come segnaposto nel sistema senza la necessità di selezionare il relativo hardware.
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, consultare .

3. Inserire un nome per la porta e selezionare un door controller nel menu a discesa **Device** (Dispositivo) da associare alla porta. Il controller è disattivato (grigio) quando non si può aggiungere un'altra porta, quando è offline o 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 149*.
8. Configurare le impostazioni della porta. Vedere *Impostazioni della porta, on page 139*.
9. *Aggiungi un monitor porta, on page 142*
10. *Aggiungi ingresso di emergenza, on page 143*
11. *Aggiungi un lettore, on page 144*
12. *Aggiungi un dispositivo REX, on page 146*
13. Fare clic su **Save (Salva)**.

Copiare una configurazione di porta esistente 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 door (Aggiungi porta)**.
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 modificare 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 **Edit (Modifica)**.
4. Modificare le impostazioni e fare clic su **Save (Salva)**.

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)**.
4. Fare clic su **Sì**.



Aggiungere e configurare porte e zone

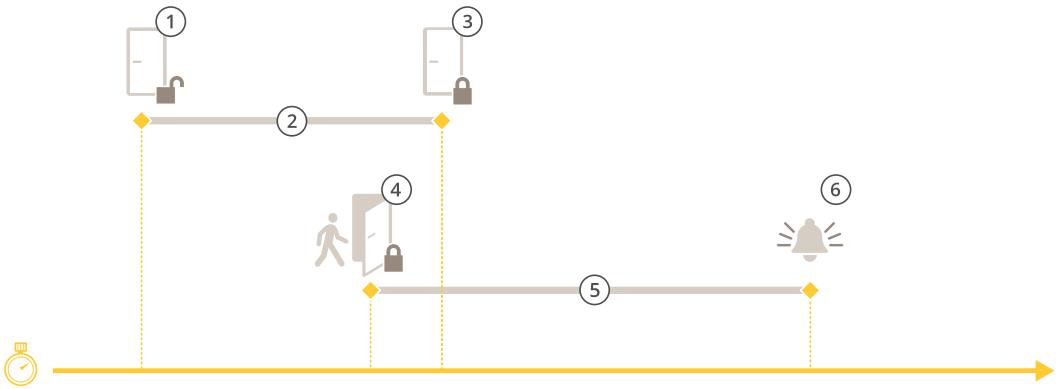
Impostazioni della porta

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)**.

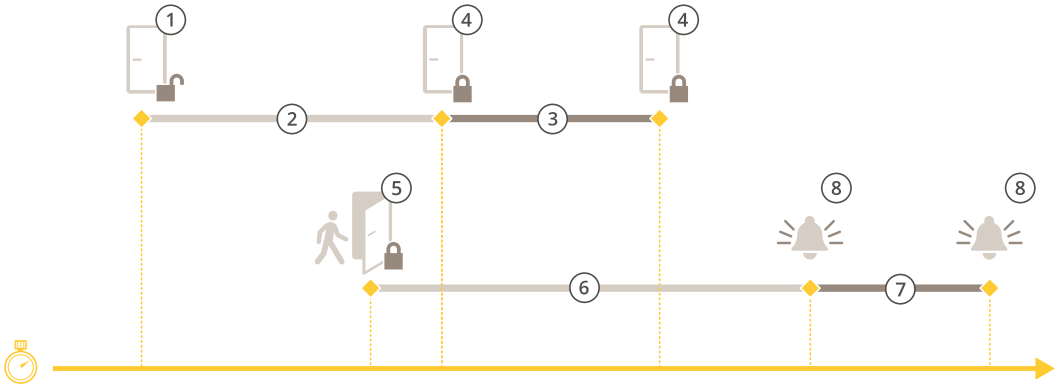
Tempo di accesso (sec)	Impostare il numero di secondi per cui la porta rimane sbloccata dopo aver consentito l'accesso. La porta rimane sbloccata fino all'apertura della porta o alla fine del tempo impostato. La porta si blocca quando si chiude anche se rimane del tempo di accesso a disposizione.
Open-too-long time (sec) (Tempo di apertura eccessivo (sec))	Valido solo se si è configurato un monitor porta. Impostare il numero di secondi durante i quali la porta resta aperta. Se la porta è aperta al termine del tempo impostato, si attiva l'allarme tempo di apertura eccessivo. Impostare una regola di azione per configurare l'azione che verrà attivata dall'evento porta aperta troppo a lungo.

Tempo di accesso lungo (sec)	Impostare il numero di secondi per cui la porta rimane sbloccata dopo aver consentito l'accesso. Il tempo di accesso lungo sovrascrive il tempo di accesso per i titolari della tessera che ha questa impostazione attivata.
Long open-too-long time (sec) (Tempo di apertura eccessivo lungo (sec))	Valido solo se si è configurato un monitor porta. Impostare il numero di secondi durante i quali la porta resta aperta. Se la porta è aperta al termine del tempo impostato, si attiva l'evento tempo di apertura eccessivo. Il tempo di apertura eccessivo lungo sovrascrive il tempo di apertura eccessivo già impostato per i titolari della tessera se si attiva l'impostazione **Long access time (Tempo di accesso lungo)**.
Ritardo ripetizione blocco (ms)	Impostare il tempo di sblocco della porta in millisecondi dopo l'apertura o la chiusura.
Ripetizione blocco	• **After opening (Dopo l'apertura):** valido solo se è stato aggiunto un monitor porta. • **After closing (Dopo la chiusura):** valido solo se è stato aggiunto un monitor porta.
Porta forzata	Selezionare se si desidera che il sistema attivi un allarme quando viene forzata l'apertura di una porta.
Porta aperta troppo a lungo	Selezionare se si desidera che il sistema attivi un allarme quando l'apertura di una porta si prolunga eccessivamente.

Opzioni relative all'orario



1 Accesso consentito: la serratura si sblocca
2 Tempo di accesso
3 Nessuna azione compiuta: la serratura si blocca
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 compiuta: la serratura si blocca*
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 5 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 Axis e sul server AXIS Camera Station 5 deve essere sincronizzata.
- Prima di cominciare, usare l'applicazione Aperio che ASSA ABLOY supporta per associare i blocchi Aperio all'hub Aperio
- I blocchi wireless non seguiranno 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 5, andare a **Configuration > Access control > Doors and zones (Configurazione > Controllo degli accessi > Porte e zone)**.
   4.2. Fare clic su + **Add door (Aggiungi porta)**.
   4.3. Selezionare il door controller collegato all'hub di comunicazione Aperio, selezionare **Wireless door (Porta wireless)** come **Door type (Tipo di porta)**.
   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 ulteriori informazioni, vedere *Porte e zone, on page 136*.
   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 porte.

Livello batteria	Operazione
Buono	Nessuno
Bassa	Il blocco funziona come previsto, ma è bene sostituirne la batteria prima che il livello diventi critico.
Critico	Sostituire la batteria. Il blocco potrebbe non funzionare come previsto.

Stato serratura	Operazione
Online	Nessuno
Blocco inceppato	Risoluzione di eventuali problemi meccanici del blocco.

Aggiungi un monitor porta

Un monitor porta è uno switch di posizione della porta che controlla lo stato fisico di una porta. È possibile aggiungere un monitor porta alla porta e configurare la modalità di collegamento del monitor porta.

1. Andare alla pagina di configurazione della porta. Vedere *Aggiunta di una porta, on page 137*.
2. In **Sensors (Sensori)**, fare clic su **Add (Aggiungi)**.
3. Selezionare **Door monitor sensor (Sensore monitor 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 avviene un'interruzione della connessione tra il door controller e il monitor porta, attivare il **Supervised input (Input supervisionato)**. Vedere *Ingressi con supervisione, on page 148*.

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.

Aggiungi ingresso 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 137*.
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.

Aggiungi un lettore

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, sarà visibile 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 136*.

Nota

- È inoltre possibile aggiungere fino a 16 lettori Bluetooth a un door controller. Per ulteriori informazioni, vedere *Aggiungi un lettore Bluetooth, on page 145*.
- Se si usa un interfono di rete Axis come 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 137*.
2. Sotto un lato della porta, fare clic su **Add (Aggiungi)**.
3. Selezionare **Card reader (Lettore di schede)**.
4. Selezionare **Reader type (Tipo di lettore)**.
5. Per usare una configurazione personalizzata della lunghezza del PIN 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 appare 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 questa procedura.

Per informazioni su come installare un lettore di codici a barre AXIS, consultare il sito .

Tipo di lettore	
OSDP RS485 half-duplex	Per i lettori RS485, selezionare **OSDP RS485 half-duplex** e una porta per il lettore.
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. Vedere *Lettore IP, on page 145* per conoscere i requisiti e i dispositivi supportati.

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 quando l'input manomissione del lettore è attivo. • **Open circuit (Circuito aperto)**: Il lettore invia il segnale di manomissione alla porta quando il circuito è aperto. • **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 148*.

Aggiungi un lettore Bluetooth

È possibile utilizzare il lettore AXIS A4612 Network Bluetooth Reader per espandere i limiti delle porte cablate dei door controller di Axis, che consentono di assegnare fino a 16 di questi lettori alla propria porta. 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 .
2. Andare alla pagina di configurazione della porta. Vedere *Aggiunta di una porta, on page 137*
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 verrà 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.

Lettore IP

È possibile usare i citofoni di rete Axis come lettore IP in AXIS Camera Station Secure Entry.

Nota

- Richiede AXIS Camera Station 5.38 o versione successiva, e un door controller Axis con firmware 10.6.0.2 o successivo.
- Non serve nessuna configurazione speciale per usare il citofono come lettore IP.

Dispositivi supportati:

- AXIS A8207-VE Network Video Door Station con firmware 10.5.1 o successivo
- AXIS A8207-VE Mk II Network Video Door Station con firmware 10.5.1 o successivo
- AXIS I8116-E Network Video Intercom

Aggiungi un dispositivo REX

È possibile scegliere di 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 137*.
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 collegare il dispositivo REX. Se è disponibile una sola porta, verrà 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 avviene un'interruzione della connessione tra il door controller e il dispositivo REX, attivare **Supervised input (Input supervisionato)**. Vedere *Ingressi con supervisione, on page 148*.

Operazione	
Sblocca porta	Sceglierlo per sbloccare la porta nel momento in cui riceve il segnale REX.
Nessuno	Selezionare questa opzione se non si desidera attivare 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):** Cardholders enter or leave the zone through this door (I titolari della tessera entrano nella zona o la abbandonano attraverso questa porta).
- **Internal door (Porta interna):** An internal door within the zone (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.

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 del perimetro impiega il lato della porta A come 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. Impone l'uscita dall'area prima che si possano usare di nuovo le proprie credenziali.

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 area o si può fare in 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 porta.
6. fare clic su **Applica**;

Anti-passback	
Log violation only (Soft) (Solo log violazione (tollerante))	Usare se si vuole permettere a una seconda persona di entrare dalla porta usando le stesse credenziali

	della prima persona. Questa opzione risulta unicamente in un allarme di sistema.
Deny access (Hard) (Nega accesso (rigido))	Da usare se si vuole evitare che il secondo utente entri dalla porta nel caso usi le stesse credenziali della prima persona. 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. Immettere 0 se non si vuole un timeout, il che significa che la zona ha l'anti-passback finché l'utente non lascia la 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 se si verifica un'interruzione della connessione a un door controller.

- Collegamento tra Door controller e Door monitor. Vedere *Aggiungi un monitor porta, on page 142*.
- Collegamento tra Door controller e lettore basato su protocolli Wiegand. Vedere *Aggiungi un lettore, on page 144*.
- Collegamento tra Door controller e dispositivo REX. Vedere *Aggiungi un dispositivo REX, on page 146*.

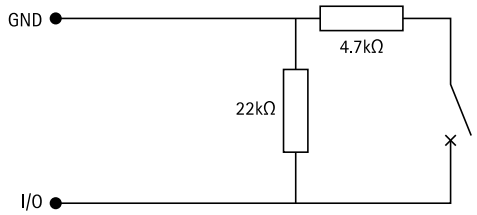
Per utilizzare gli input supervisionati:

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)**.

Schemi delle connessioni

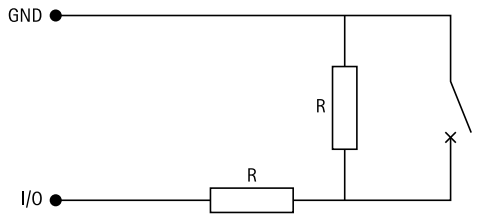
Prima connessione parallela

I valori dei resistori devono essere 4,7 kΩ e 22 kΩ.



Connessione prima 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.

I tipi di identificazione sono vettori di credenziali necessarie per l'accesso a una porta. I tipi di identificazione più diffusi sono i token, i numeri di identificazione personale (PIN), le impronte digitali, le mappe facciali e i dispositivi REX. È possibile che un tipo di identificazione contenga uno o molteplici tipi di informazioni.

Tipi di identificazione supportati: tessera, PIN, REX, QR statico e QR dinamico.

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.

Sono disponibili cinque profili di identificazione predefiniti da utilizzare così come sono o modificare secondo necessità.

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.

QR Code è un marchio registrato di Denso Wave Incorporated in Giappone e in altri paesi.

Per creare 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 (Creare 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. Eseguire la configurazione del profilo di identificazione per un lato della porta.
6. Sull'altro lato della porta, ripetere i passaggi precedenti.
7. Fare clic su **OK**.

Per 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**.

Per rimuovere 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**.

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.



Impostare profili di identificazione

Formati tessera e PIN

Un formato tessera definisce la modalità in cui una tessera memorizza i dati. Si tratta di una tabella di conversione tra i dati in ingresso e i dati convalidati nel sistema. Ciascun formato di tessera dispone di un set di regole diverso riguardante il modo di organizzare le informazioni memorizzate. Definendo un formato tessera si indica al sistema come interpretare le informazioni che il dispositivo di controllo ottiene dal lettore di tessere.

Esistono formati di tessera comunemente usati predefiniti che è possibile utilizzare così come sono o modificare in base alle necessità. È possibile inoltre creare formati tessera personalizzati.

Andare a **Configuration > Access Control > Card formats and PIN (Configurazione > Controllo degli accessi > Formati tessera e PIN)** per la creazione, la modifica o l'attivazione dei formati tessera. È inoltre possibile configurare il PIN.

I formati della tessera personalizzati possono contenere i seguenti campi dati utilizzati per la convalida delle credenziali.

Numero tessera – Un sottoinsieme dei dati binari delle credenziali codificati come numeri decimali o esadecimali. Usare il codice carta per identificare un titolare o una tessera specifica.

Codice struttura – Un sottoinsieme dei dati binari delle credenziali codificati come numeri decimali o esadecimali. Usare il codice struttura per identificare un sito o un cliente finale specifico.

Per creare un formato tessera:

1. Andare a **Configuration > Access Control > Card formats and PIN (Configurazione > Controllo degli accessi > Formati tessera e PIN)**.
2. Fare clic su **Add card format (Aggiungi formato scheda)**.
3. Inserire un nome per il formato tessera.
4. Digitare una lunghezza in bit tra 1 e 256 nel campo **Bit length (Lunghezza in bit)**.
5. Selezionare **Invert bit order (Inverti ordine dei bit)** se si desidera invertire l'ordine dei bit dei dati ricevuti dal lettore di tessere.
6. 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.
7. Selezionare e configurare i campi dati in modo che siano attivi nel formato tessera. Il **Card number (Codice carta)** o il **Facility code (Codice struttura)**.
8. Fare clic su **OK**.
9. Per attivare il formato della tessera, selezionare la casella di controllo davanti al nome del formato della tessera.

Nota

- Non è possibile che due formati scheda con la stessa lunghezza in bit possano essere attivi contemporaneamente. Ad 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.

ⓘ	Fare clic su ⓘ per vedere un esempio di output dopo l'inversione dell'ordine dei bit.
Intervallo	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)**.
Formato di output	Selezionare il formato di output dei dati per il campo dati. **Decimal (Decimale)**: noto anche come sistema numerico posizionale in base 10, è composto dai numeri compresi tra 0 e 9. **Hexadecimal (esadecimale)**: noto anche come sistema numerico posizionale in base 16, è composto da 16 simboli unici: i numeri 0-9 e le lettere a-f.
Ordine bit di subrange	Selezionare l'ordine dei bit. **Little endian**: il primo bit è il più piccolo (meno significativo). **Big endian**: il primo bit è il più grande (più significativo).

Per 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)**.

Per il reset di 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.

Per configurare la lunghezza PIN:

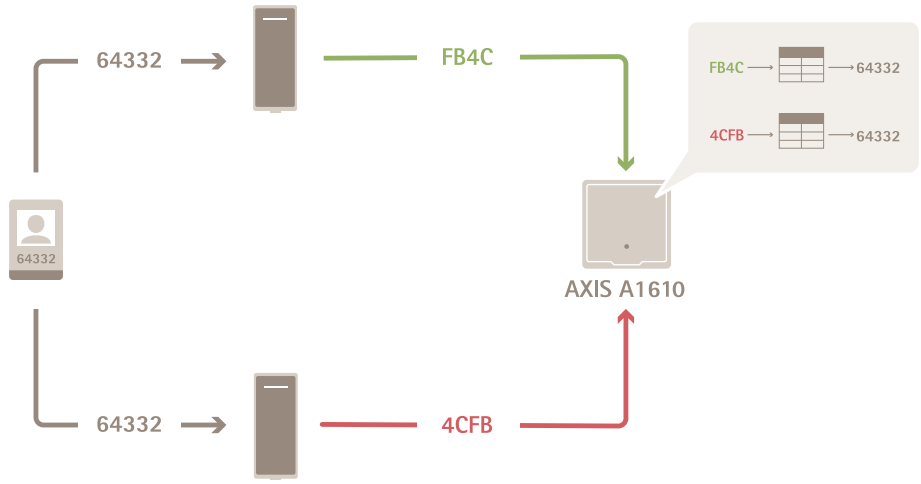
1. Andare a **Configuration > Access Control > Card formats and PIN (Configurazione > Controllo degli accessi > Formati tessera e PIN)**.
2. In **PIN configuration (Configurazione PIN)** fare clic su .
3. Specificare **Min PIN length (Lunghezza PIN minima)**, **Max PIN length (Lunghezza PIN massima)** e **End of PIN character (Fine del carattere PIN)**.
4. Fare clic su **OK**.



Impostazione dei formati tessera

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



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.

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 la configurazione personalizzata della porta, consulta *Generale, on page 185*.
- 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 155*.
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 155*.
3. Configura i titolari di tessera e i gruppi di titolari di tessera globali nel server principale. Vedere *Aggiungi un titolare tessera, on page 160* e *Aggiungi un gruppo, on page 164*.

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 160*.

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 5. 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 5. Vedere *Importare gli utenti Active Directory, on page 156*.

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 5:

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 161*.

Configura la ricerca intelligente 2

Con Ricerca intelligente 2, è possibile impostare diversi filtri per trovare facilmente persone e veicoli di interesse dalle registrazioni generate dalle telecamere Axis.



Per i requisiti, i limiti e l'utilizzo di ricerca intelligente 2, vedere *Ricerca intelligente 2, on page 34*.

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 crea 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 solo per un periodo di tempo molto breve, oppure oggetti ondulanti come il fogliame.

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 mostrare i risultati che indicano la mancata registrazione di metadati nel corso di un periodo specificato.
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.

Configura Monitoraggio dell'integrità del sistema BETA

Nota

- Quando si è connessi a più server AXIS Camera Station 5, 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, AXIS System Health Monitoring Cloud Service fornisce la stessa funzionalità, ma attraverso il cloud. Per ulteriori informazioni, vedere *Imposta il servizio cloud di Monitoraggio dell'integrità del sistema di AXIS, on page 115*.

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 116*
2. Configura gli indirizzi e-mail per la ricezione delle notifiche. Vedere *Configurazione di destinatari e-mail, on page 158*.
3. Configura le regole di notifica. Vedere *Configura regole di notifica, on page 158*.

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 mostra l'invio di un'e-mail di prova.

Configura regole di notifica

Ci sono 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 5 minuti.

Dispositivo fuori uso – Inviare una notifica quando un dispositivo elencato in Monitoraggio dell'integrità del sistema è fuori uso per 5 minuti.

1. Andare a **Configuration > System Health Monitoring > Notifications (Configurazione > Monitoraggio dell'integrità del sistema > Notifiche)**.
2. In **Notification rules (Regole di notifica)**, attivare o disattivare le regole di notifica.
3. In **Applied rules (Regole applicate)** si può visualizzare un elenco di sistemi e dispositivi, compresa la regola di notifica applicata.

Multisystem



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 158*.
2. Nel sistema principale, caricare la configurazione di sistema. Vedere *Recupero di dati da altri sistemi, on page 159*.
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 169*.

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. Fai clic su **Copy (Copia)** per eseguire il caricamento sul 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, fai clic su **Delete (Elimina)** per eliminare prima quella esistente.

Dopo aver eseguito il caricamento della 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

Puoi caricare la configurazione di un sistema secondario nel sistema principale dopo averla generata e copiata.

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 l'inserimento delle 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)**.

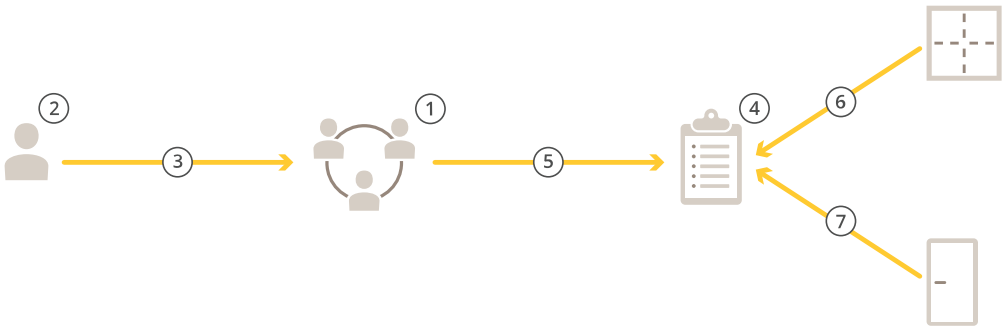
Gestione degli accessi

La scheda Access management (Gestione degli accessi) consente di configurare e gestire gli utenti, 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 5, vedere *Imposta un network door controller Axis*.

Flusso di lavoro di gestione degli accessi

La struttura di gestione degli accessi è flessibile. Questo consente all'utente di sviluppare un flusso di lavoro più adatto alle proprie esigenze. Di seguito è riportato un esempio di flusso di lavoro:



1. Aggiungi gruppi. Vedere *Aggiungi un gruppo, on page 164*.
2. Aggiungi titolari tessera. Vedere *Aggiungi un titolare tessera, on page 160*.
3. Aggiunta di titolari di tessera ai gruppi.
4. Aggiungi regole di accesso. Vedere *Aggiungi una regola di accesso, on page 164*.
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. Eseguire la configurazione di un titolare della tessera con le credenziali che identificano la persona e il modo e il momento in cui lasciarla passare dalle porte.

Puoi anche scegliere di mappare gli utenti in un database di Active Directory come titolari tessera, vedi *Impostazioni di Active Directory*^{BETA}*, on page 156*.

1. Aprire una scheda di gestione degli accessi .
2. Andare in **Cardholder management (Gestione titolari tessere)** > **Cardholders (Titolari di tessere)** e fare clic su **+Add (+Aggiungi)**.
3. Immettere il nome e il cognome del titolare di tessere e fare clic su **Next (Avanti)**.
4. Oppure, fare clic su **Advanced (Avenzate)** e selezionare le opzioni.
5. Aggiungere una credenziale al titolare di tessere. Vedere *Aggiungi credenziali, on page 161*
6. Fare clic su **Save (Salva)**.
7. Aggiunge il titolare di tessere a un gruppo.
   7.1. In **Groups (Gruppi)**, selezionare il gruppo a cui si vuole aggiungere il titolare di tessere e fare clic su **Edit (Modifica)**.

7.2. Fare clic su **+Add (+Aggiungi)** e selezionare il titolare di tessere che si desidera aggiungere al gruppo. È possibile selezionare più titolari di tessere.

7.3. Fare clic su **Aggiungi**.

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

Avanzata	
Tempo di accesso lungo	Selezionare per consentire al titolare della tessera un tempo di accesso lungo e un tempo di apertura eccessivo lungo quando c'è un monitor porta installato.
Sospendi titolare tessera	Selezionare per eseguire la sospensione del titolare 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, ha la possibilità di usarla per lo sblocco di una porta al di fuori della pianificazione normale.
Esente da blocco	Selezionare per permettere al titolare della tessera l'accesso durante il blocco.
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 154*.



Aggiunta di titolari di tessera e gruppi

Aggiungi credenziali

È possibile aggiungere i seguenti tipi di credenziali al titolare della tessera:

- codice QR
- PIN
- Badge
- Targa

Per aggiungere un QR come credenziale di un titolare di tessere:

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. Per una sincronizzazione dell'ora perfetta, consigliamo l'uso della stessa origine ora per entrambi i dispositivi.

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 (QR dinamico)** è attivo per impostazione predefinita. È necessario usare la funzione QR dinamica 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**.

Per aggiungere un PIN come credenziale di un titolare di tessere:

1. In **Credentials (Credenziali)**, fare clic su **+Add (+ Aggiungi)** e selezionare **PIN**.
2. Immettere un PIN.
3. Per utilizzare un PIN di coercizione per attivare un allarme silenzioso, attivare **Duress PIN (PIN di coercizione)** e inserire un PIN di coercizione.
4. Impostare le date **Valid from** (Valido da) e **Valid to** (Valido fino al) per le credenziali.
5. Fare clic su **Aggiungi**.

È inoltre possibile configurare un PIN di coercizione che apre la porta e attiva un allarme silenzioso nel sistema.

Nota

Il titolare tessera deve disporre di un indirizzo e-mail per ricevere le credenziali mobili.

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. Per immettere manualmente i dati della tessera: inserire il nome della tessera, il numero della tessera e la lunghezza dei bit.

Nota

La lunghezza dei bit è configurabile solo quando si crea un formato tessera con una specifica lunghezza di bit non presente nel sistema.

3. Per ottenere automaticamente i dati della tessera dell'ultima tessera letta:
   3.1. Selezionare una porta dal menu a discesa **Select reader (Seleziona lettore)**.
   3.2. Passare la tessera sul lettore connesso a tale porta.
   3.3. Fare clic su **Get last swiped card data from the door's reader(s) (Acquisisci i dati dell'ultima tessera strisciata dal lettore/dai lettori della porta)**.

Nota

Per acquisire i dati della tessera, hai la possibilità di usare il lettore di tessere USB desktop 2N. Se necessiti di maggiori informazioni, consulta *Configurazione del lettore di tessere USB desktop 2N*.

4. 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)**.
5. Impostare la data di inizio e di fine delle credenziali.
6. Fare clic su **Aggiungi**.

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**.

Vedere l'esempio in *Usare il numero di targa come credenziale, on page 163*.

Data di scadenza	
Valido da	Impostare una data e un'ora di validità delle credenziali.
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 delle credenziali, a partire dall'ultimo utilizzo. Selezionare giorni, mesi o anni dopo l'ultimo utilizzo.

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 5. Vedere *Aggiunta di dispositivi, on page 5*
2. Impostare la data e l'ora per i nuovi dispositivi con **Synchronize with server computer time (Sincronizza con l'ora del computer server)**. Vedere *Impostazione di data e ora, on page 64*.
3. Aggiorna il firmware sui nuovi dispositivi alla versione più recente a disposizione. Vedere *Aggiornare il firmware, on page 63*.
4. Aggiungi una nuova porta connessa al tuo door controller. Vedere *Aggiunta di una porta, on page 137*.
   4.1. Aggiungi un lettore su **Side A (Lato A)**. Vedere *Aggiungi un lettore, on page 144*.
   4.2. In **Door settings (Impostazioni porta)**, seleziona **AXIS License Plate Verifier** come **Reader type (Tipo lettore)** e inserisci un nome per il lettore.
   4.3. In via facoltativa, aggiungi un lettore o un dispositivo REX su **Side B (Lato B)**.
   4.4. Fare clic su **OK**.
5. Installare e attivare AXIS License Plate Verifier sulla tua telecamera. Vedi il manuale per l'utente *AXIS License Plate Verifier*.
6. Avvia AXIS License Plate Verifier.
7. Configura AXIS License Plate Verifier.
   7.1. Andare a **Configuration > Access control > Encrypted communication (Configurazione > Controllo degli accessi > Comunicazione crittografata)**.

7.2. 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)**.

7.3. Apri AXIS License Plate Verifier dall'interfaccia Web della telecamera.

7.4. Non effettuare l'impostazione.

7.5. Andare a **Settings (Impostazioni)**.

7.6. In **Access control (Controllo degli accessi)**, seleziona **Secure Entry** come **Type (Tipo)**.

7.7. In **IP address (Indirizzo IP)**, immetti l'indirizzo IP e le credenziali per il door controller.

7.8. In **Authentication key (Chiave di autenticazione)**, incolla la chiave di autenticazione che hai copiato in precedenza.

7.9. Fare clic su **Connetti**.

7.10. In **Door controller name (Nome door controller)**, seleziona il door controller.

7.11. In **Reader name (Nome lettore)**, seleziona il lettore che hai aggiunto in precedenza.

7.12. Attiva l'integrazione.

8. Aggiungi il titolare tessera a cui vuoi concedere l'accesso. Vedere *Aggiungi un titolare tessera, on page 160*
9. Eseguire l'aggiunta di credenziali targa al nuovo titolare tessera. Vedere *Aggiungi credenziali, on page 161*
10. Aggiungi una regola di accesso. Vedere *Aggiungi una regola di accesso, on page 164*.
    10.1. Aggiungere una pianificazione.
    10.2. Aggiungi il titolare tessera a cui vuoi concedere l'accesso tramite targa.
    10.3. Aggiungi la porta con il lettore AXIS License Plate Verifier.

Aggiungi un gruppo

I gruppi consentono di gestire i titolari di tessera e le rispettive regole di accesso collettivamente e in modo efficiente.

1. Aprire una scheda di gestione degli accessi .
2. Andare in **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 rendere possibile visualizzare e monitorare il 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 154*.
5. Aggiungere i titolari di tessere al gruppo:
    5.1. Fare clic su **+ Aggiungi**.
    5.2. Selezionare i titolari di tessere che si desidera aggiungere e fare clic su **Add (Aggiungi)**.
6. Fare clic su **Save (Salva)**.

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)**.
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 (Programmi)**, 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**.



Porte

Per informazioni sulle azioni manuali, come lo sblocco manuale di una porta, vedere .

Zone

Per informazioni sulle azioni manuali, come lo sblocco manuale di una zona, vedere .

Esportazione dei report sulla configurazione del sistema

È possibile esportare report contenenti diversi tipi di informazioni sul sistema. AXIS Camera Station 5 esporta il 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.

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 immettere 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 149*.

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)**.

Importa ed esporta

Importa titolari della tessera

Questa opzione importa i titolari di tessera, i gruppi di titolari, le credenziali e le foto dei titolari della tessera 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.

Puoi anche scegliere di mappare gli utenti in un database di Active Directory come titolari tessera, vedi *Impostazioni di Active Directory[BETA], on page 156*.

Opzione di importazione	
Nuovo	questa opzione rimuove i titolari di tessere esistenti e aggiunge nuovi titolari.
Aggiorna	questa opzione aggiorna i titolari di tessere esistenti e aggiunge nuovi titolari di tessere.
Aggiungi	questa opzione 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. Seleziona **New (Nuovo)**, **Update (Aggiorna)** o **Add (Aggiungi)**.
4. Fare clic su **Next (Avanti)**.
5. Fare clic su **Choose a file (Scegli un file)** e andare al file CSV. Fare clic su **Open (Apri)**.
6. Immettere un delimitatore di colonna e selezionare un identificatore univoco, quindi fare clic su **Next (Avanti)**.
7. Assegnare un'intestazione a ogni colonna.
8. Fare clic su **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. L'identificativo univoco impedisce l'importazione di registri 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 5 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 di tutte le configurazioni hardware allo stato precedente all'ultima importazione dei titolari tessera.

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**.

Monitoraggio dell'integrità del sistema BETA

La scheda Monitoraggio dell'integrità del sistema permette il monitoraggio dei dati relativi all'integrità da un singolo sistema o da più sistemi AXIS Camera Station 5 sulla stessa rete.

Se si gestiscono sistemi che si trovano su reti diverse, AXIS System Health Monitoring Cloud Service fornisce la stessa funzionalità, ma attraverso il cloud. Per ulteriori informazioni, vedere *Imposta il servizio cloud di Monitoraggio dell'integrità del sistema di AXIS, on page 115*.

	mostra un riepilogo dei dispositivi e dei sistemi ai quali puoi accedere. Vedere *Magazzino, on page 169*.
	Mostra un riepilogo dell'archiviazione e i dettagli di registrazione di ogni telecamera dai sistemi monitorati. Vedere *Archiviazione, on page 170*.
	mostra i registri di System Health Monitoring dei sistemi monitorati. Vedere *Notifiche, on page 171*.

Limiti

- Non si può eseguire il monitoraggio dello spazio di archiviazione per registrazioni in AXIS S3008 Recorder.
- Le impostazioni di notifica influiscono unicamente sul server di System Health Monitoring locale.
- Il sistema contrassegna registrazioni, eccetto quelle continue e attivate da movimento, con **None (Nessuno)** come tipo di registrazione.

Flusso di lavoro

1. *Configura Monitoraggio dell'integrità del sistema BETA, on page 157*
   1.1. Configura notifiche. Vedere *Notifiche, on page 157*.
   1.2. Configura multisistema. Vedere *Multisystem, on page 158*.
2. Eseguire il monitoraggio dei dati relativi all'integrità dai sistemi AXIS Camera Station 5.
   2.1. *Magazzino, on page 169*
   2.2. *Archiviazione, on page 170*
   2.3. *Notifiche, on page 171*

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 informazioni, inclusi i 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 informazioni che includono i dettagli del dispositivo e le informazioni di archiviazione se contiene 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 180*.
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 dell'integrità 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.

Archiviazione

La pagina di archiviazione illustra il riepilogo dell'archiviazione e i dettagli di registrazione di ogni telecamera dai sistemi monitorati. Fare clic su un'intestazione di colonna per ordinare in base al contenuto della 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 70*.
Location	Il nome e il percorso dell'archiviazione.
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 massima di spazio di archiviazione assegnata alle registrazioni.
Utilizzato	La quantità di spazio su archiviazione attualmente utilizzato per le registrazioni.
Ultimo aggiornamento	Ora dell'ultimo aggiornamento delle informazioni.

Telecamera	
Stato	(vuoto): stato normale. Icona di avviso: il periodo di conservazione non è stato rispettato. Icona informazioni: 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	Numero di giorni durante i quali le registrazioni della telecamera sono state in archiviazione.
Registrazione più vecchia	L'ora della registrazione più vecchia della telecamera conservata nell'archiviazione.
Ultima registrazione	L'ora della registrazione più recente della telecamera conservata nell'archiviazione.
Location	Il punto di archiviazione usato dalla telecamera.

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 su un'intestazione di colonna per ordinare in base al contenuto della 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 avviene 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 5.

- 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
- Tabulazione
- Altro

Si deve 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'operazione 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 valore vuoto per aggiungere il tasto di scelta rapida per questa azione. • Per aggiungere un tasto di scelta rapida con la tastiera, premere Ctrl e almeno un altro tasto o un tasto funzione F2 - F12. • Per aggiungere un tasto di scelta rapida con una tastiera, premere una combinazione di testi numerici o premere uno dei tasti funzione (F1-F5). • Per aggiungere un tasto di scelta rapida con un joystick o jog dial, premere il tasto del joystick o jog dial per assegnarlo all'azione.
Modifica tasto di scelta rapida	Fare clic sul valore della tastiera di un'azione e modificare il valore.

Rimuovi un tasto di scelta rapida	Fare clic sul valore della tastiera di un'azione e rimuovere il valore.
	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 Registri mostra i registri in tempo reale, inclusi i registri di controllo, gli eventi e gli allarmi in tempo reale. 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)**.

Ora	Data e ora dell'azione.
Tipo	Il tipo di azione: allarme, evento o controllo.
Categoria	La categoria dell'azione.
Messaggio	Breve descrizione dell'azione.
Utente	AXIS Camera Station 5 utente che esegue l'azione.
Computer	Il computer (nome dominio di Windows) sul quale è installato AXIS Camera Station 5.
Utente Windows	L'utente Windows che amministra AXIS Camera Station 5.
Server	Disponibile solo quando ci si collega a più server. Il server sul quale si verifica l'azione.
Componente	Il componente da cui viene generato il registro.

Ricerca dei registri

1. Nella scheda Registri, fare clic su **Search (Cerca)** in **Log search (Ricerca nel registro)**.
2. Nella casella del filtro digitare le parole chiave. AXIS Camera Station 5 esegue la ricerca nell'elenco dei log tranne che in **Time (Ora)** e mostra i risultati che contengono tutte le parole chiave. Per operatori di ricerca supportati, consulta *Ottimizzazione della tua ricerca, on page 39*.
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 allarmi mostra gli allarmi di sistema e gli allarmi generati da regole e rilevamento movimento in un elenco. 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 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 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 di 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 esportare i controlli in un file in formato testo.

Allarmi

La scheda Allarmi è disponibile nella parte inferiore del client AXIS Camera Station 5 e visualizza 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 197*.

Ora	l'ora alla quale si è verificato l'allarme.
Categoria	La categoria dell'allarme attivato.
Descrizione	Una breve descrizione dell'allarme.
Server	Disponibile quando si è connessi a più server. Il server AXIS Camera Station 5 che invia l'allarme.
Componente	il componente che attiva l'allarme.
	Mostra una procedura di allarme, disponibile solo quando l'allarme contiene una procedura di allarme.
	Andare alle registrazioni, disponibili unicamente quando l'allarme contiene una registrazione.
	Confermare l'allarme selezionato
	Rimuovere l'allarme. Se non viene confermato prima della rimozione, l'allarme viene rimosso solo in modo temporaneo.

Per risolvere un allarme specifico.

1. Fare clic su **Alarms and Tasks (Allarmi e attività)** in fondo al client AXIS Camera Station 5 e aprire la scheda **Alarms (Allarmi)**.
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 già stati gestiti, 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 5.

Le seguenti attività sono personali e sono visibili solo per gli amministratori e gli utenti che le hanno avviate.

- Report del sistema
- Crea report dell'incidente
- Esportazione delle registrazioni

Se si è amministratori, 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 ritentare le attività avviate personalmente. 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.
Inizio	Indica l'ora in cui l'attività è stata avviata.
Messaggio	Mostra lo stato o le informazioni relative all'attività. Stati possibili: • **Canceling (Annullamento)**: pulizia prima della cancellazione dell'attività. • **Canceled (Annullato)**: la pulizia è completa e l'attività viene cancellata. • **Error (Errore)**: attività completata con errori, ossia l'attività non è andata a buon fine su uno o più dispositivi. • **Finished (Finito)**: attività completata. • **Finished during lost connection (Terminato durante la perdita della connessione)**: visualizzato se l'attività è stata completata mentre la connessione al server era inattiva. Non è stato possibile determinare lo stato dell'attività. • **Lost connection (Connessione persa)**: visualizzato se viene persa la connessione al server mentre l'attività era in esecuzione. Non è stato possibile determinare lo stato dell'attività. • **Running (In esecuzione)**: attività in esecuzione. • **Pending (In sospeso)**: 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 5 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 5 e fare clic sulla scheda **Tasks (Attività)**.
2. Selezionare le attività e fare clic su una delle azioni

	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. Tutte le operazioni non riuscite devono essere riviste e configurate manualmente.

Per la maggior parte delle attività, vengono elencati i seguenti dettagli. Per attività quali le registrazioni di esportazione e il 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 sullo stato di esecuzione dell'attività: • **Finished (Finito)**: L'attività è stata completata con successo. • **Error (Errore)**: Non è stato possibile completare l'attività sul dispositivo. • **Canceled (Annullato)**: 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 un report in formato HTML con la configurazione generale di sistema del 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 delle telecamere 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 un report in formato HTML con la configurazione generale di 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 al menu nell'angolo in alto a destra
2. Fare clic su **Help** > **System report** (Guida, Report di sistema).
3. Cambiare il nome del file se si vuole modificare il nome del file generato in automatico.
4. Fare clic su **Sfoglia** per selezionare la posizione in cui salvare il report di sistema.
5. 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 screenshot of all monitors** (Includi gli screenshot di tutti i monitor) per semplificare l'analisi dei report di sistema.
6. Fare clic su **OK**.



Generare un report di sistema

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)	Verifica dello streaming di dati e dell'archiviazione di dati con le impostazioni di sistema correnti in AXIS Camera Station 5. Documentazione prodotta: operazione riuscita o non riuscita.
Condizioni di scarsa illuminazione	test dello streaming di dati e dell'archiviazione di dati con impostazioni ottimizzate per tipiche condizioni di bassa luminosità, ad esempio le impostazioni di guadagno. Documentazione prodotta: operazione riuscita o non riuscita.
Stress test	test che aumenta gradualmente lo streaming di dati e l'archiviazione di dati, finché non viene raggiunto il limite massimo del sistema. Documentazione prodotta: informazioni sulle prestazioni di sistema massime.

Nota

- Si possono testare solo dispositivi che supportano AXIS Camera Application Platform 2 (ACAP 2) e versione successiva.
- Durante il test, AXIS Camera Station 5 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 visualizzare il report oppure su **Save report (Salva report)** per salvarlo.

Feedback

Si può decidere di condividere in automatico i dati di uso del client anonimi quando si esegue la configurazione del client e inviare in modo manuale il feedback per aiutarci a migliorare AXIS Camera Station 5 e l'esperienza dell'utente. Vedere *Configurazione client, on page 108*.

Nota

Non usare il modulo di feedback per richieste di assistenza.

1. Andare a ☰ > **Help > Feedback (Guida > Feedback)**.
2. Scegliere una reazione e inserire il feedback.
3. Fare clic su **Send (Invia)**.

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.

Impostazioni dispositivi indossabili

Per connettersi a un sistema indossabile, è necessario creare un file di connessione. Vedere *Impostazione di un sistema indossabile Axis.*

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 131*.

Per creare un file di connessione:

1. Andare a ☰ > **Other (Altro) > Body worn settings (Impostazioni Body Cam)**.
2. Per cambiare il nome predefinito del sito mostrato nel sistema indossabile, inserire un nuovo nome.
3. fare clic su **Esporta**.
4. In **Latest export (Ultima esportazione)**, appare un link al file o aggiornamenti.
5. Fare clic sul collegamento per andare alla posizione del file.



Impostazione di un sistema indossabile Axis



Riproduzione ed esportazione delle registrazioni della telecamera indossabile AXIS Body Worn Camera

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)**.

AXIS Camera Station 5 controllo servizio

Il server utilizza il controllo del servizio AXIS Camera Station 5 per avviare e arrestare e per 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** e selezionare **All Programs > Tools > Service Control (Tutti i programmi > Strumenti > Controllo del servizio)**.

	In esecuzione
	Avvio
	Arrestato

Modify Settings (Modifica impostazioni)	Selezionare questa opzione per essere in grado di modificare le impostazioni del server.
Ripristina le impostazioni	Fare clic per ripristinare tutte le impostazioni predefinite originali.
Inizio	Fare clic per cambiare lo stato del server.
Arresta	
Rinizia	Fare clic su per riavviare il server.

Generale

Nel controllo del servizio AXIS Camera Station 5 selezionare **Modify settings (Modifica impostazioni)** e fare clic su **General (Caratteristiche generali)** per modificare le impostazioni generali del server.

Impostazioni server	
Nome del server	Il nome del server. Il nome server è visualizzato nel client software. Il nome predefinito del server è il nome del computer. Il nome non cambia se si cambia il nome del computer.
Ports range (Intervallo porte)	Specificare l'intervallo di porte. Il resto delle porte cambia in automatico.
Server HTTP port (Porta HTTP del server)	Il numero di porta HTTP che il server usa per comunicare con il client. La porta predefinita è 55752.
Server TCP port (Porta TCP del server)	Il numero di porta TCP che il server usa per comunicare con il client. La porta predefinita è 55754. Il numero di porta viene calcolato aggiungendo 2 al numero di porta del server.
Mobile communication port (Porta comunicazione mobile)	Il numero di porta mobile che il server usa per comunicare con il client. La porta predefinita è 55756. Il numero di porta viene calcolato aggiungendo 4 al numero di porta del server.
Mobile streaming port (Porta streaming mobile)	Il numero di porta mobile che il server usa per lo streaming video. La porta predefinita è 55757. Il numero di porta viene calcolato aggiungendo 5 al numero di porta del server.
Component communication port (Porta di comunicazione componente)	Il numero di porta utilizzato dal componente per comunicare con i dispositivi di rete tramite il server. La porta predefinita è 55759. Il numero di porta viene calcolato aggiungendo 7 al numero di porta del server.
Porte utilizzate dai componenti di AXIS Camera Station 5	Dopo aver specificato l'intervallo delle porte, nell'elenco vengono mostrate le porte utilizzabili per i componenti. L'intervallo di porte predefinito per i componenti di AXIS Camera Station 5 è 55760–55764.
Allow AXIS Camera Station 5 to add exceptions to the Windows Firewall (Consenti a di aggiungere eccezioni a Windows Firewall)	Selezionare questa opzione se si desidera consentire a AXIS Camera Station 5 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.

Impostazioni proxy	
Connessione diretta	Selezionare questa opzione se non è presente alcun server proxy tra il server AXIS Camera Station 5 e le telecamere del sistema.
System account Internet options / automatic (Opzione Internet account di sistema/automatico)	Impostazioni proxy predefinite. Questa opzione usa le impostazioni del proxy correnti in Opzioni Internet per l'account di sistema.
Utilizza impostazioni proxy manuali	Selezionare questa opzione se un server proxy separa il server AXIS Camera Station 5 e tutte le telecamere nel sistema. Immettere l'indirizzo e il numero di porta del server proxy. Normalmente corrispondono all'indirizzo e al numero di porta immessi in Opzioni Internet nel Pannello di controllo di Windows. • Specificare di non usare il server proxy con indirizzi che iniziano con determinati caratteri. • Selezionare **Always bypass proxy server for local addresses (Escludi sempre il server proxy per gli indirizzi locali)** e inserire gli indirizzi locali o i nomi host delle telecamere locali se la comunicazione non passa attraverso il proxy. È possibile utilizzare caratteri jolly per l'indirizzo o i nomi host, ad esempio: "192." o ".ilmiodominio.com".

Elenco porta per AXIS Camera Station 5

Le tabelle che seguono mostrano le porte e i protocolli usati da AXIS Camera Station 5. Può essere necessario consentirli nel proprio firewall per prestazioni e usabilità ottimali. I numeri di porta vengono calcolati in base alla porta principale HTTP predefinita 55752.

AXIS Camera Station 5 server invia i dati ai dispositivi sulle seguenti porte:

Porta	Numero	Protocollo	Ingresso/Uscita	Descrizione
Porte HTTP e HTTPS principali	80 & 443	TCP	In uscita	Utilizzato per flussi video e dati del dispositivo.
Porta bonjour predefinita	5353	UDP	Multicast (In entrata + In uscita)	Utilizzato per individuare i dispositivi con mDNS Discovery (Bonjour). Multicast 224.0.0.251. L'impossibilità di eseguire il bind alla porta predefinita potrebbe essere

				dovuta al fatto che un'altra applicazione la sta utilizzando e rifiuta di condividerla. In tal caso si usa una porta casuale. Bonjour non rileva dispositivi con indirizzo di collegamento locale quando si usa una porta casuale.
Porta SSDP predefinita	1900	UDP	Multicast (In entrata + In uscita)	Utilizzato per individuare i dispositivi con SSDP (UPNP). Multicast 239.255.255.250.
Porta WS-Discovery predefinita	3702	UDP	Multicast (In entrata + In uscita)	WS-Discovery webservices discovery utilizzati per individuare i dispositivi Onvif. Multicast 239.255.255.250.

AXIS Camera Station 5 server riceve dati dai client sulle seguenti porte:

Porta	Numero	Protocollo	Ingresso/Uscita	Comunicazione tra	Descrizione
Porta SSDP predefinita	1900	UDP	Multicast (In entrata + In uscita)	Server e client	Utilizzato per individuare i server AXIS Camera Station 5 con SSDP (UPNP). Multicast 239.255.255.2-50.
Porta HTTP principale e porta di streaming HTTP	55752	TCP	In entrata	Server e client	Utilizzata per video, audio e flusso di metadati (crittografia AES).
Porta TCP principale	55754	TCP	In entrata	Server e client	Offset +2 dalla porta HTTP principale. Utilizzata per i dati

					dell'applicazione (crittografia TLS 1.2). Per 5.15.007 o inferiore, viene utilizzata la codifica TLS 1.1.
Porta del server Web SSDP	55755	TCP	In entrata	Server e client	Offset +3 dalla porta HTTP principale. Utilizzato per l'individuazione del server AXIS Camera Station 5 con SSDP/ UPNP.
Porta del server Web API	55756	TCP	In entrata	Server e app per dispositivi mobili	Offset +4 dalla porta HTTP principale. Utilizzata per dati dell'applicazione crittografati e flusso video MP4 su HTTPS.
Porta multimediale API	55757	TCP	In entrata	Server e app per dispositivi mobili	Offset +5 dalla porta HTTP principale. Utilizzata per il flusso video RTSP su HTTP.

Porta HTTP proxy locale	55758	TCP	In entrata	Comunicazione interna nel server	Offset +6 dalla porta HTTP principale. Offset +2 dalla porta del server Web API. Accessibile solo internamente sul computer server AXIS Camera Station 5. Porta inevasa per problema sconosciuto. 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 e alla porta multimediale API.
Porta endpoint proxy Web	55759	TCP	In entrata	Server e componenti	Offset +7 dalla porta HTTP principale. Utilizzato per una comunicazione sicura tra componente e dispositivi.

Porte riservate per i componenti

Componente	Ascolta l'interfaccia	Porta	Numero	Protocollo	Ingresso/Uscita	Comunicazione tra	Descrizione
Secure Entry	Localhost (127.0.0.1)	Porta del server Web	55766	HTTPS	In entrata	Client (scheda Gestione degli accessi) e componente	Offset +14 dalla porta HTTP principale. Installazioni precedenti usavano la porta 8081.
Secure Entry	Tutti (0.0.0.0/ INADDR_ ANY)	Porta del server Web	55767	HTTPS	In entrata	Server principale e server secondari	Offset +15 dalla porta HTTP principale. Usato per la comunicazione tra server principale e server secondari nell'impostazione multiserver.
System Health Monitoring	Tutti (0.0.0.0/ INADDR_ ANY)	Porta del server Web	55768	HTTPS	In entrata	Client (scheda Monitoraggio dell'integrità del sistema) e componente	Offset +16 dalla porta HTTP principale. Utilizzato per ospitare pagine web di Monitoraggio dell'integrità del sistema e per condividere i dati in configurazione multisistema.
Servizio cloud di Monitoraggio dell'integrità del sistema	localhost	Porta del server Web	55769	HTTPS	In entrata	AXIS Camera Station 5 (pagina web) e backend	Offset +17 dalla porta HTTP principale. Usato per il servizio

Componente	Ascolta l'interfaccia	Porta	Numero	Protocollo	Ingresso/Uscita	Comunicazione tra	Descrizione
						CloudService (plugin)	cloud Monitoraggio dell'integrità del sistema per consentire il monitoraggio dell'integrità del sistema.
Ricerca intelligente 2	localhost	Porta del server Web	55770	HTTPS	In entrata	Client (scheda Ricerca intelligente) e componente	Offset +18 dalla porta HTTP principale. Utilizzato per ospitare l'API di ricerca intelligente e pubblicare la pagina web del client.
			55771				Riservato per uso futuro.
			55772				Riservato per uso futuro.
			55773				Riservato per uso futuro.
			55774				Riservato per uso futuro.
			55775				Riservato per uso futuro.
			55776				Riservato per uso futuro.
			55777				Riservato per uso futuro.

Componente	Ascolta l'interfaccia	Porta	Numero	Protocollo	Ingresso/Uscita	Comunicazione tra	Descrizione
			55778				Riservato per uso futuro.
			55779				Riservato per uso futuro.
			55780				Riservato per uso futuro-
			55781				Riservato per uso futuro.
			55782				Riservato per uso futuro.
			55783				Riservato per uso futuro.
IAM locale (IDP)	0.0.0.0	IDP_OIDC (pubblico)	55784	HTTPS	In entrata	Proxy inverso e iam locale	Offset +32 dalla porta HTTP principale. Porta pubblica.
IAM locale (IDP)	0.0.0.0	MTLS (Admin)	55785	HTTPS	In entrata	Servizi di terze parti	Offset +33 dalla porta HTTP principale. Porta amministratore.
IAM locale (IDP)	127.0.0.1	TOKENIZER	55786	HTTPS	In entrata	Servizi di terze parti	Offset +34 dalla porta HTTP principale. Porta tokenizer.
			55787				Riservato per uso futuro.
Opentelemetry	127.0.0.1	Porta gRPC	55788	gRPC	In entrata	Servizi di terze parti	Offset +36 dalla porta HTTP principale.
Opentelemetry	127.0.0.1	Porta HTTP	55789	HTTPS	In entrata	Servizi di terze parti	Offset +37 dalla porta

Componente	Ascolta l'interfaccia	Porta	Numero	Protocollo	Ingresso/Uscita	Comunicazione tra	Descrizione
							HTTP principale.
		Porta del server Web	55790	HTTPS	In entrata	Servizi di integrazione di terze parti e componenti	
			55791				Riservato per uso futuro.
			55792				Riservato per uso futuro.
			55793				Riservato per uso futuro.
			55794				Riservato per uso futuro.
			55795				Riservato per uso futuro.
NATS Broker	127.0.0.1	NATS	55796	NATS	In entrata	Tra AXIS Camera Station 5 e i componenti, e tra i componenti stessi	Offset +44 dalla porta HTTP principale.
Opentelemetry	127.0.0.1	Porta HTTP	55797	HTTP	In entrata	Endpoint di monitoraggio per il recupero di metriche dal collettore telemetria aperto	Offset +45 dalla porta HTTP principale.

Altre porte

Porta	Numero	Protocollo	Ingresso/Uscita	Comunicazione tra	Descrizione
Internet HTTPS	80 & 443	TCP	In uscita	Client e server verso Internet	Utilizzata per attivare la licenza, scaricare il

					firmware, i servizi connessi, ecc.
Porta di streaming TCP del server	55750	TCP	In entrata	Server e dispositivo	Offset -2 dalla porta HTTP principale.
Porta UDP stato di aggiornamento	15156	UDP	In ingresso + In uscita	Controllo server e servizio	AXIS Camera Station 5 Service Control è in ascolto sulla porta e il server trasmette lo stato di un aggiornamento in corso.

Database

File del database

File del database di base

AXIS Camera Station 5 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 5 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`.

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 database crea un backup ogni notte e prima di ogni aggiornamento di sistema. Nel controllo del servizio di AXIS Camera Station 5, 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 5 per applicare la modifica. Se il percorso della cartella di backup non è corretto o AXIS Camera Station 5 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 utilizzabile qualsiasi numero da 1 a 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 5.

Backup del database

Il database contiene informazioni relative alle registrazioni e ad altri metadati necessari al corretto funzionamento del sistema.

Importante

- Il database non conserva le registrazioni, bensì specifica una posizione in **Configuration > Storage (Configurazione > Archiviazione)** per archiviarle. Eseguire il backup delle registrazioni separatamente.
- Le impostazioni del server, del proxy e del database nel controllo del servizio AXIS Camera Station 5 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 194*. 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 194*.

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 usi un componente. Ad esempio, AXIS Camera Station Secure Entry o Ricerca intelligente. • **ACMSM**: Questa cartella comprende il file di database di AXIS Camera Station Secure

	Entry `SecureEntry.db` e le foto del titolare della tessera. • **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 sul backup.

Backup di manutenzione

Specificare in quale cartella di backup archiviare i backup di manutenzione nella scheda **Database**, vedere *Impostazioni del database, on page 194*. 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 5.
- Quando si esegue manualmente la manutenzione del database dal controllo del servizio AXIS Camera Station 5. Vedere *Manutenzione database, on page 197*.
- In automatico, da parte dell'attività di manutenzione pianificata del database configurata in Utilità di pianificazione Windows. Vedere *Strumenti, on page 197*.

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.

Ci sono due modi per condurre un backup manuale:

- Andare a `C:\ProgramData\AXIS Communications\AXIS Camera Station Server` e copiare i file del database.
- Eseguire la generazione di un report di sistema con tutti i database compresi e copiare i file di backup del database. Accertarsi di selezionare **Include all databases (Includi tutti i database)**. Vedere *Report del sistema, on page 180*.

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 195*.

Nota

Il database non conserva le registrazioni, bensì specifica una posizione in **Configuration > Storage (Configurazione > Archiviazione)** per archiviarle. Eseguire il backup delle registrazioni separatamente.

Per ripristinare il database:

1. Andare al controllo del servizio AXIS Camera Station 5 e fare clic su **Stop (Arresta)** per arrestare il servizio.
2. Andare ai file di backup del database. Vedere *Backup del database, on page 195*.
3. Eseguire l'estrazione dei file.
4. 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.

5. Se si utilizza AXIS Camera Station Secure Entry, copiare **SecureEntry.db** da `Components > ACMSM` a `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry 2\INTERNAL\main_db`.
6. 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**.
7. Tornare al controllo del servizio AXIS Camera Station 5 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 197*.

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 nei rari casi di compressione 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 danneggiare il database. Se si utilizza un sistema di backup esterno, non eseguire il backup del database corrente e 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 5 su un computer con memoria sufficiente. Per informazioni sui requisiti hardware, vedere *axis.com/products/axis-camera-station/hardware-guidelines*.

Memoria RAM danneggiata – Eseguire regolarmente lo Strumento di diagnostica memoria Windows per cercare eventuali errori nella memoria RAM.

Strumenti

Nel controllo del servizio AXIS Camera Station 5, selezionare **Modify settings (Modifica impostazioni)** e fare clic su **Tools (Strumenti)** per avviare la manutenzione del database e creare report di sistema parziali.

Manutenzione database

- Aprire il controllo del servizio AXIS Camera Station 5.
- Fare clic su **Tools (Strumenti)**.
- In **Database maintainer (Manutenzione database)**, fare clic su **Run (Esegui)**.
- Viene mostrato 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 5 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 5 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.

Report del sistema

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, andare su  **> Help > System report (Guida > Report di sistema)** nel client AXIS Camera Station 5.

Per generare un report di sistema parziale:

1. fare clic su **Esegui**;
2. Selezionare e inserire le informazioni necessarie nella finestra di dialogo.
3. Fare clic su **Genera report**.

Strumento Rapporto di sistema	
Nome file	Inserire un nome file per il rapporto di sistema.
Cartella	Impostare dove salvare il report del server.
Apre automaticamente la cartella al completamento del report.	Selezionare per l'apertura automatica della cartella una volta pronto il report di sistema.
Includi file del database nel report	Selezionare questa opzione per includere il database nel report di sistema. Il database AXIS Camera Station 5 contiene informazioni sulle registrazioni e sui dati necessari al corretto funzionamento del sistema.

Registrazione rete

- Fare clic sul collegamento per scaricare un'applicazione per l'analisi del protocollo di rete.
- Una volta installata, fare clic su **Start (Avvia)** per avviare l'applicazione.

Ripristinare l'autorità di certificazione

- Fare clic su **Reset** (Ripristino) per generare una nuova autorità di certificazione e riavviare il servizio.
- Una volta effettuato il riavvio del servizio, si potrà effettuare l'accesso e importare un'autorità di certificazione personalizzata, se necessario.

Risoluzione dei problemi

Informazioni su questa guida

Questa guida raccoglie problemi relativi ad AXIS Camera Station 5 e illustra la relativa risoluzione. Abbiamo inserito i problemi in un argomento correlato per semplificare la ricerca di ciò che si desidera. Un argomento può essere ad esempio l'audio o la visualizzazione in diretta. Per ogni problema viene descritta una soluzione.

Per saperne di più

Visita *axis.com/support* per

- domande frequenti;
- requisiti hardware;
- aggiornamenti software;
- esercitazioni, materiali didattici e altre informazioni utili.

Il servizio AXIS Camera Station 5

Il servizio si riavvia spesso

È possibile che il server sia sovraccarico. Questo causa una lunga coda di attività e può anche danneggiare i database.

- Nella gestione delle risorse del sistema, verificare se AXIS Camera Station 5 o qualsiasi altra applicazione utilizza un numero elevato di risorse.
- Eseguire la manutenzione del database, andare a *Manutenzione database* nel manuale per l'utente di AXIS Camera Station 5.

Se nessuna delle soluzioni di cui sopra aiuta, contattare l'assistenza Axis. Andare in *Processo di escalation, on page 214*.

Dispositivi nel Video Management System

Problemi comuni

Impossibile contattare la telecamera	
Il VMS non può contattare la telecamera. Le telecamere in elenco non sono state aggiunte.	1. Verificare che la telecamera sia dotata di una connessione di rete, che ci sia alimentazione e che la telecamera sia operativa. 2. Andare a **Configuration > Add devices (Configurazione > Aggiungi dispositivi)** e riprovare ad aggiungere la telecamera.

L'installazione è stata annullata	
L'utente ha annullato l'installazione. Le telecamere in elenco non sono state aggiunte.	Per aggiungere le telecamere, andare a **Configurazione > Aggiungi dispositivi**.

Impossibile impostare la password nella telecamera	
Impossibile impostare la password per le telecamere elencate.	1. Per l'impostazione manuale della password, vai a **Configuration > Devices > Management (Configurazione > Dispositivi > Gestione)**. 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

Se il dispositivo è stato usato in un sistema diverso prima di essere aggiunto a AXIS Camera Station 5:

- Ripristinare le impostazioni predefinite di fabbrica del dispositivo.

Se non è ancora possibile aggiungere il dispositivo al Video Management System, provare ad aggiungerlo ad AXIS Device Manager.

Si può eseguire l'aggiunta di un modello di dispositivo diverso da quello che si desidera aggiungere:

- Se il dispositivo è un nuovo prodotto o ha un firmware appena rilasciato, può trattarsi di un problema di compatibilità. Assicurarsi di utilizzare l'ultima versione del software AXIS Camera Station 5.

Se non è possibile aggiungere un altro modello di dispositivo:

- Procedi alla risoluzione di problemi della telecamera, andare su *axis.com/support/troubleshooting*.

Non è possibile eseguire l'aggiornamento del firmware del dispositivo attraverso AXIS Camera Station 5

Non è possibile aggiornare la telecamera dall'interfaccia web:

- Procedi alla risoluzione di problemi della telecamera, andare su *axis.com/support/troubleshooting*.

Impossibile aggiornare il firmware per tutti i dispositivi:

- Verificare la presenza di una connessione di rete.
- Se non si tratta di un problema di rete, contattare l'assistenza Axis. Andare in *Processo di escalation, on page 214*.

Impossibile aggiornare il firmware per modelli specifici:

- Può trattarsi di un problema di compatibilità, contattare l'assistenza Axis. Andare in *Processo di escalation, on page 214*.

Nessun dispositivo rilevato

Il Video Management System cerca automaticamente nella rete le telecamere e i video encoder connessi ma non è in grado di individuare alcuna telecamera.

- Verificare che la telecamera abbia una connessione di rete e 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. Andare a *Impostazioni proxy client* nel manuale per l'utente di AXIS Camera Station 5.
  - Modificare il NAT o il sistema di sicurezza se un NAT o un sistema di sicurezza separa il client e il server. Assicurarsi di autorizzare il passaggio della porta HTTP, della porta TCP (Transmission Control Protocol) e della porta di streaming specificate nel controllo del servizio AXIS Camera

Station attraverso il sistema di sicurezza o NAT. Per la visualizzazione dell'elenco completo delle porte, vedere *Elenco delle porte per AXIS Camera Station 5*.

– Modificare le impostazioni del proxy server se un server proxy separa il server e i dispositivi. Andare alla sezione Impostazioni proxy in *Impostazioni generali controllo servizio* nel manuale per l'utente di AXIS Camera Station 5.

- Aggiungere le telecamere manualmente, andare ad *Aggiungi dispositivi* nel manuale per l'utente di AXIS Camera Station 5.

Messaggio ripetuto "Riconnessione alla videocamera tra 15 secondi"

Problemi possibili:

- Una rete sovraccarica.
- La telecamera non è accessibile. Verificare che la telecamera abbia una connessione di rete e l'alimentazione.
- 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.
- Modificare le impostazioni video e audio, ad esempio ottimizzando le impostazioni del profilo per una bassa larghezza di banda.

Registrazioni

Vedere *Visualizzazione in diretta, on page 203* per ulteriori informazioni su eventuali problemi di prestazioni che incidono sulle registrazioni e la riproduzione.

Problemi comuni

La registrazione continua non è abilitata	
La registrazione continua non è attivata nelle telecamere nella lista.	1. Per l'attivazione della registrazione continua, andare a **Configuration > Recording and events > Recording method (Configurazione > Registrazione ed eventi > Metodo di registrazione)**. 2. Seleziona la telecamera e attiva **Continuous (Continua)**.

Impossibile registrare sull'unità specificata	
Il sistema non è in grado di eseguire la configurazione dell'archiviazione delle registrazioni.	1. Per utilizzare un dispositivo di archiviazione locale, andare a **Configuration > Storage > management (Configurazione > Archiviazione > Gestione)**. 2. Eseguire l'aggiunta del dispositivo di archiviazione e configurare le impostazioni di archiviazione per le telecamere.

Impossibile installare l'applicazione AXIS Video Content Stream	
Questo messaggio di errore appare se non è stato possibile installare l'applicazione su una telecamera che supporta AXIS Video Content Stream.	1. Per l'installazione manuale dell'applicazione, andare a **Configuration > Devices > Management (Configurazione > Dispositivi > Gestione)**. 2. Selezionare una telecamera e fare clic su .

La registrazione non si avvia

Se le registrazioni non iniziano o si fermano dopo pochi secondi, vuol dire che il disco è pieno o che sono presenti troppi dati di intrusione.

- Verificare che nel foglio di configurazione server, in **Recording Storage (Memorizzazione della registrazione)**, 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. Andare a *Configurazione dei dispositivi di archiviazione* nel manuale per l'utente di AXIS Camera Station 5.

Spazi vuoti di registrazione durante la registrazione continua

Insieme a spazi vuoti, allarmi con l'etichetta **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

Controllare se gli spazi vuoti di registrazione avvengono su tutte le telecamere. Se non avvengono su tutte le telecamere, è possibile che si tratti di un sovraccarico della telecamera. Porsi queste domande per individuare la causa:

- Con quale frequenza si verificano gli spazi vuoti, ogni ora o ogni giorno?
- Quanto dura lo spazio vuoto, secondi o ore?
- A che ora si verifica lo spazio vuoto?

Soluzioni possibili:

- Nella gestione attività del server, controllare se il sistema usa una delle risorse hardware più del normale. Se il disco presenta segni di utilizzo eccessivo, aggiungere altri dischi e spostare più telecamere perché registrino sui nuovi dischi.
- Ridurre la quantità di dati scritti sul disco (Impostazioni video, flussi ZIP, FPS, risoluzione). Tenere presente il throughput stimato da AXIS Site Designer, vedere *axis.com/support/tools/axis-site-designer*.

Per ulteriori informazioni, vedere *Performance visualizzazione in diretta e riproduzione, on page 203*.

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 esportate* nel manuale per l'utente di AXIS Camera Station 5.

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 numero di giorni specificato. Per cambiare il numero di giorni, andare a **Configuration (Configurazione) > Storage (Archiviazione) > Selection (Selezione)**.

Se lo spazio sul dispositivo di archiviazione si esaurisce, il sistema elimina le registrazioni prima di arrivare al numero di giorni designato.
Per evitare che lo spazio di archiviazione si esaurisca, prova 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 5. 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)**.
  - Usa il formato video H.264 per la registrazione, il formato M-JPEG necessita di molto più spazio di archiviazione.
  - Usa Zipstream per ridurre ulteriormente le dimensioni delle registrazioni.

Problemi di failover recording

Il failover recording non registra sul server dopo il ripristino della connessione.

Causa	Soluzione
La larghezza di banda tra la telecamera e il server non è sufficiente per il trasferimento della registrazione.	Miglioramento della 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*. • 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 sincronizzare il NTP per le registrazioni future. • Sincronizzare l'orario della telecamera con il server o impostare lo stesso server NTP sulla telecamera e sul server.

Il failover recording in AXIS Camera Station 5 non funziona nei seguenti scenari:

- Arresti del server controllato.
- Interruzioni brevi inferiori a 10 secondi nella connessione.

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 5.

Hardware del client	
Verificare che il driver della scheda grafica o dell'adattatore di rete sia aggiornato	1. Aprire DirectX Diagnostic Tool (cercare dxdiag sul computer). 2. Andare al sito Web del produttore per verificare se il driver è il più recente per questo OS. 3. Verificare che il client e il server siano in esecuzione sullo stesso computer. 4. Provare a eseguire il client su un computer dedicato.
Verificare il numero di monitor	Se si usa una scheda grafica interna, si consiglia di non utilizzare più di due monitor per scheda grafica. 1. Aprire DirectX Diagnostic Tool (cerca dxdiag sul computer) 2. Assicurarsi che AXIS Camera Station 5 supporti la scheda grafica dedicata, vedere *axis.com/products/axis-camera-station/hardware-guidelines*. Nota Non è possibile eseguire il client su una macchina virtuale.

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 *axis.com/products/axis-camera-station/hardware-guidelines*.
La telecamera è collegata a un Video Management System diverso da quello di AXIS Camera Station 5	Disconnettere la telecamera dall'altro client e impostarla come predefinita prima di connetterla a AXIS Camera Station 5.
Una telecamera impiega molti flussi diversi, specialmente la risoluzione elevata	Potrebbe essere un problema specialmente per le stesse telecamere M-Line. • Far passare il flusso verso lo stesso profilo di streaming o una risoluzione inferiore. Vedere *Profili di streaming* nel manuale per l'utente di AXIS Camera Station 5.

Sovraccarico del server	
Utilizzo inusuale di CPU/RAM corrispondente allo stesso orario del problema	Verificare che nessun'altra applicazione di consumo CPU/RAM sia in esecuzione allo stesso momento.

Problema di connessione di rete	
Utilizzo larghezza di banda inusuale corrispondente allo stesso orario del problema	Verificare che nessun'altra applicazione di consumo di larghezza di banda sia in esecuzione allo stesso momento.
Larghezza di banda sufficiente/ Rete remota o locale	• Esaminare la propria topologia di rete. • 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. La decodifica hardware si attiva per impostazione predefinita. Vedere Decodifica hardware in *Streaming* nel manuale per l'utente di AXIS Camera Station 5.

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*.
- Crea un report del server delle telecamere, vai a *axis.com/support/troubleshooting*.
- Se è installato un software antivirus, è possibile che blocchi i flussi dal vivo.
- Consentire le cartelle e i processi di AXIS Camera Station 5. A tale scopo, vedere *Domande frequenti*.
- Verificare che il firewall non blocchi le connessioni su certe porte. A tale scopo, vedere *Impostazioni generali controllo del servizio* nel manuale per l'utente di AXIS Camera Station 5.
- Verificare di aver installato Desktop Experience per le versioni del sistema operativo del server Windows supportate. Vedere *Esportazione pianificata* nel manuale per l'utente di AXIS Camera Station 5.
- Assicurarsi che il flusso a risoluzione inferiore funzioni.

Se nessuna delle opzioni precedenti è di aiuto, contattare l'assistenza Axis andando a *Processo di escalation, on page 214*.

Archiviazione

Archiviazione di rete non accessibile

Se si utilizza l'account di sistema locale per accedere al controllo del servizio AXIS Camera Station 5, 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 5 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

Impossibile installare l'applicazione AXIS Video Motion Detection	
Impossibile installare AXIS Video Motion Detection 2 o 4. Per la registrazione del movimento la telecamera usa il rilevamento movimento integrato.	Per eseguire l'installazione manuale dell'applicazione, andare a *Installare l'applicazione per telecamera* nel manuale per l'utente di AXIS Camera Station 5.

Impossibile recuperare Rilevamento movimento corrente	
Il Video Management System non è in grado di recuperare i parametri di rilevamento movimento dalla telecamera. Per la registrazione del movimento la telecamera usa il rilevamento movimento integrato.	Per eseguire l'installazione manuale dell'applicazione, andare a *Installare l'applicazione per telecamera* nel manuale per l'utente di AXIS Camera Station 5.

Rilevamento movimento non configurato	
Impossibile configurare il rilevamento movimento per le telecamere elencate.	1. Per configurare manualmente il rilevamento del movimento, andare a **Configuration (Configurazione) > Registrazione ed eventi > Metodo di registrazione**. 2. Selezionare la telecamera e fare clic su **Motion settings (Impostazioni movimento)** per configurare il rilevamento movimento.

Il rilevamento movimento non è abilitato	
La registrazione del movimento non è attivata nelle telecamere nella lista.	1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Metodo di registrazione**. 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* nel manuale per l'utente di AXIS Camera Station 5.
Funzione di rilevazione movimento incorporata	Si possono configurare i riquadri di inclusione e di esclusione. Vedere *Modifica di rilevamento movimento incorporato* nel manuale per l'utente di AXIS Camera Station 5.

Regolazione del periodo di attivazione

Il periodo di trigger è un intervallo di tempo tra due trigger successivi. Usare questa impostazione per ridurre il numero di registrazioni successive. La registrazione prosegue se si verifica un ulteriore trigger entro questo intervallo. Se si verifica un'ulteriore attivazione, il periodo di attivazione inizia da tale punto temporale.

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.

Audio

Niente audio nella visualizzazione in diretta

Se l'audio è assente 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 5.

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 saperne di più, vedere *Profili di streaming* nel manuale per l'utente di AXIS Camera Station 5.

Audio assente in riproduzione

Durante la riproduzione, l'audio è disponibile se è stato abilitato 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 eseguito l'accesso a più server, il client si avvia e si vede lo stato della connessione sulla barra di stato. Per ulteriori informazioni sullo stato di connessione, vedere *Stato connessione* nel manuale per l'utente di AXIS Camera Station 5.

Nome utente o password non corretta	La combinazione di nome utente e password non è valida per accedere al server specificato.	• Rivedere l'ortografia o utilizzare un altro account. • Assicurarsi che l'utente abbia diritti di accesso al server AXIS Camera Station 5. • Gli orologi del server e del client AXIS Camera Station 5 devono essere sincronizzati. Per gli utenti del dominio, l'orologio del server del dominio deve essere sincronizzato con il server e il client. • Un utente che non è stato aggiunto al server ma è un membro del gruppo degli amministratori locali sul server deve eseguire il client come amministratore. • Per informazioni relative ai diritti di accesso degli utenti, vedere *Configurare autorizzazioni utente* nel manuale per l'utente di AXIS Camera Station 5.
L'utente non è autorizzato ad accedere al server	Impossibile per l'utente utilizzare AXIS Camera Station 5 sul server specificato.	aggiungere l'utente nella finestra di dialogo delle autorizzazioni utente;
Impossibile verificare la sicurezza del messaggio	Si è verificato un errore durante la configurazione della connessione protetta al server. Molto probabilmente, l'errore è dovuto alla mancata sincronizzazione dell'ora del client o del server.	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	Il client non è in grado di stabilire una connessione di qualsiasi tipo con il server.	• Assicurarsi che il computer server possa essere collegato alla rete. • Assicurarsi che il computer server sia in esecuzione. • Assicurarsi che il firewall sia stato configurato correttamente. • Controllare l'ortografia dell'indirizzo del server. • Controllare le impostazioni proxy del client.
Nessuna risposta dal server	Il client può contattare il computer server, ma nessun server AXIS Camera Station 5 è in esecuzione.	Assicurarsi di connettersi al computer corretto e che il server AXIS Camera Station 5 sia in esecuzione.
Il client non può collegarsi al server	Il client non è in grado di connettersi al server e viene visualizzato un messaggio di errore.	Verificare che la rete sia stata configurata correttamente: • Verificare che il SO sia supportato. Per una lista completa dei sistemi operativi supportati, andare alle *note sul rilascio* • Dal controllo del servizio, verificare che il server AXIS Camera Station 5 sia in esecuzione o avviarlo, se necessario.

		• 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. • Verificare se esiste un server proxy tra il server e il client. – Configurare il proxy server nel controllo del servizio. – Eseguire la configurazione dell'impostazione proxy del client nella pagina di accesso, selezionare **Change proxy settings (Modifica impostazioni proxy)**. – Configurare le impostazioni del proxy client in Opzioni Internet di Windows e selezionarlo per utilizzare l'opzione predefinita in **Change Proxy settings (Modifica impostazioni proxy)**.
Impossibile connettersi al server	Si è verificato un errore sconosciuto durante la connessione al server.	• Verificare che l'indirizzo e la porta del server AXIS Camera Station 5 siano corretti. • Assicurarsi che un NAT, un firewall o un software antivirus non blocchino la connessione al server. Per ulteriori informazioni, vedere *Configurare il firewall per consentire l'accesso ad AXIS Secure Remote Access*. • Usare il controllo del servizio AXIS Camera Station 5 per verificare che il server sia in esecuzione. – Aprire il controllo del servizio AXIS Camera Station 5. A tale scopo vedere *Controllo del servizio AXIS Camera Station* nel manuale per l'utente di AXIS Camera Station 5. – 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	Il client non riesce a risolvere l'indirizzo immesso per un indirizzo IP.	• Assicurarsi che il computer server possa essere collegato alla rete. • Verificare che l'indirizzo e la porta del server AXIS Camera Station 5 siano corretti. • Assicurarsi che un NAT, un firewall o un software antivirus non blocchino la connessione al server. Per ulteriori informazioni, vedere *Configurare il firewall per consentire l'accesso ad AXIS Secure Remote Access*.

La versione del client e del server differiscono	Il client esegue una versione più recente di AXIS Camera Station 5 rispetto al server.	Aggiornare il server in modo che esegua la stessa versione del client.
	Il server esegue una versione più recente di AXIS Camera Station 5 rispetto al client.	Aggiornare il client in modo che esegua la stessa versione del server.
Impossibile connettersi al server. Server occupato.	Il server non ha potuto rispondere a causa di problemi di prestazioni.	Verificare che il computer server e la rete non siano sovraccarichi.
Il server AXIS Camera Station 5 locale non viene eseguito	Si usa **This computer (Questo computer)** per connettersi, ma il server AXIS Camera Station 5 installato non è in esecuzione.	Utilizzare il controllo del servizio per avviare AXIS Camera Station 5 o selezionare un server remoto a cui accedere.
Su questo computer non è installato il server AXIS Camera Station 5	Si usa **This computer (Questo computer)** per connettersi, ma non esistono server installati sul computer.	Installare il server AXIS Camera Station 5 o scegliere un altro server.
L'elenco dei server selezionato è vuoto	L'elenco dei server selezionato per l'accesso 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:

- Controllare che la chiave di licenza sia stata inserita nel modo giusto.
- Modificare le impostazioni proxy del client per consentire a AXIS Camera Station 5 di accedere a Internet.
- Registrare la propria licenza offline. A tale scopo, vedere *Ottenimento di una licenza per un sistema offline* nel manuale per l'utente di AXIS Camera Station 5.
- Annotare l'ID del server e attivare la licenza AXIS Camera Station 5 da *license-portal.lp.axis.com*.
- Verifica che l'ora del server sia aggiornata.

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 5 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

AXIS Camera Station 5 non è in grado di comunicare con il dispositivo finché non si risolve l'errore del certificato.

Possibili errori		
Certificato non trovato	Se è stato rimosso il certificato del dispositivo.	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: • il dispositivo è stato reimpostato ai valori predefiniti di fabbrica; • la comunicazione sicura HTTPS è stata disabilitata. • il dispositivo ha subito modifiche a seguito di accesso non autorizzato.
Certificato non attendibile	Il certificato del dispositivo è stato modificato al di fuori di AXIS Camera Station 5. Questo può indicare che un utente non autorizzato ha eseguito l'accesso e ha apportato modifiche sul dispositivo.	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.

Password mancante per autorità di certificazione

Se si dispone di un'autorità di certificazione in AXIS Camera Station 5 senza una password memorizzata, viene visualizzato l'allarme riportato di seguito.

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.)

Puoi risolvere questo problema in tre modi diversi:

- 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 un 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 il 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 device certificate (Convalida certificato dispositivo)**.

Nota

AXIS Camera Station 5 perde la sua connessione ai dispositivi e alcuni componenti di sistema si riavviano.

Per consentire a AXIS Camera Station 5 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 il 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 device certificate (Convalida certificato dispositivo)**.

Nota

AXIS Camera Station 5 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. La causa può essere l'impossibilità di raggiungere il server NTP da parte del servizio Ora di Windows.

- Verificare che il server NTP sia online.
- Assicurarsi che le impostazioni del firewall siano esatte.
- Verificare 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 della data e dell'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. Assicurati 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 a sufficienza per sincronizzare l'ora.
   3.1. Deseleziona **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 disabilitare gli allarmi.

Per ricevere aiuto, contatta l'assistenza Axis.

Assistenza tecnica

L'assistenza tecnica è disponibile per i clienti che possiedono una versione con licenza di AXIS Camera Station 5.

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 Axis, vedere *helpdesk online Axis*. Per permettere al nostro team di assistenza di capire il problema e risolverlo, si devono includere le seguenti informazioni:

- Una descrizione chiara su come riprodurre il problema o delle circostanze nelle quali si verifica.
- L'ora e il nome e l'indirizzo IP della telecamera interessata dove si verifica il problema.
- AXIS Camera Station 5 report di sistema generato direttamente dopo che si è verificato il problema. Il report di sistema deve essere generato dal client o dal server in cui è stato riprodotto tale problema.
- Screenshot o registrazioni opzionali da tutti i monitor che illustrano il problema. Attivare la funzione di sovrapposizione debug quando si realizzano screenshot o registrazioni.
- Se serve, includere i file del database. Escluderli per velocizzare il caricamento.

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

Nota

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

Informazioni aggiuntive	
Log livello di debug	A volte usiamo la registrazione al livello di debug per raccogliere altre informazioni. Eseguibile solo dietro richiesta di un tecnico dell'assistenza Axis. Si possono trovare istruzioni *nell'helpdesk online Axis*.
Sovrapposizione debug visualizzazione in diretta	Talvolta è utile mettere a disposizione screenshot delle informazioni in sovrapposizione testo o un video che illustri la modifica dei valori nel periodo di

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

T10122292_it

2026-02 (M72.2)

© 2018 – 2026 Axis Communications AB