# AXIS D1110 Video Decoder 4K

Manuale dell'utente

## Indice

# Impostazioni preliminari

## Individuazione del dispositivo sulla rete

Per trovare i dispositivi Axis sulla rete e assegnare loro un indirizzo IP in Windows®, utilizza AXIS IP Utility o AXIS Device Manager. Queste applicazioni sono entrambe gratuite e possono essere scaricate dal sito Web *axis.com/support*.

Per ulteriori informazioni su come trovare e assegnare indirizzi IP, andare alla sezione *Come assegnare un indirizzo IP e accedere al dispositivo*.

### Supporto browser

Il dispositivo può essere utilizzato con i seguenti browser:

| | Chrome™ | Firefox® | Edge™ | Safari® |
|---|---|---|---|---|
| Windows® | consigliato | consigliato | ✓ | |
| macOS® | consigliato | consigliato | ✓ | ✓ |
| Linux® | consigliato | consigliato | ✓ | |
| Altri sistemi operativi | ✓ | ✓ | ✓ | ✓* |

Per usare l'interfaccia Web di AXIS OS con iOS 15 o iPadOS 15, andare su **Settings > Safari > Advanced > Experimental Features**(Impostazioni > Safari > Avanzate > Funzioni sperimentali) e disabilitare NSURLSession Websocket.

## Aprire l'interfaccia Web del dispositivo

1. Aprire un browser e digitare il nome di host o l'indirizzo IP del dispositivo Axis.
   Se non si conosce l'indirizzo IP, utilizzare AXIS IP Utility o AXIS Device Manager per individuare il dispositivo sulla rete.
2. Digitare il nome utente e password. Se si accede al dispositivo per la prima volta, è necessario creare un account amministratore. Vedere .

Per le descrizioni di tutti i comandi e le opzioni nell'interfaccia Web del dispositivo, consultare .

## Crea un account amministratore

La prima volta che si accede al dispositivo, è necessario creare un account amministratore.

1. Inserire un nome utente.
2. Inserire una password. Vedere .
3. Reinserire la password.
4. Accettare il contratto di licenza.
5. Fare clic su **Add account (Aggiungi account)**.

Importante

Il dispositivo non ha un account predefinito. In caso di smarrimento della password dell'account amministratore, è necessario reimpostare il dispositivo. Vedere .

## Password sicure

Importante

I dispositivi Axis inviano la password inizialmente impostata in chiaro tramite la rete. Per proteggere il dispositivi dopo il primo accesso, impostare una connessione HTTPS sicura e crittografata e quindi cambiare la password.

La password del dispositivo è il sistema di protezione principale dei dati e dei servizi. I dispositivi Axis non impongono criteri relativi alla password poiché i dispositivi potrebbero essere utilizzati in vari tipi di installazioni.

Per proteggere i dati consigliamo vivamente di:

- Utilizzare una password con almeno 8 caratteri, creata preferibilmente da un generatore di password.
- Non mostrare la password.
- Cambiare la password a intervalli regolari, almeno una volta all'anno.

## Verificare che nessuno abbia alterato il software del dispositivo

Per verificare che il dispositivo disponga del firmware AXIS OS originale o per prendere il controllo completo del dispositivo dopo un attacco alla sicurezza:

1. Ripristinare le impostazioni predefinite di fabbrica. Vedere .
   Dopo il ripristino, l'avvio sicuro garantisce lo stato del dispositivo.
2. Configurare e installare il dispositivo.

## Panoramica dell'interfaccia Web

Questo video mette a disposizione una panoramica dell'interfaccia Web del dispositivo.


*Interfaccia Web dei dispositivi Axis*

# Configurare il dispositivo

## Aggiunta di una telecamera

1. Andare a **Video sources > Camera sources (Sorgenti video > Sorgenti telecamera)**.
2. Fare clic su **Add camera source (Aggiungi sorgente telecamera)**:
   - Per eseguire l'aggiunta di una telecamera predefinita da una lista, selezionare **Network discovery (Individuazione rete)**.
   - Per aggiungere una telecamera in modo manuale, selezionare **Manual (Manuale)**.
     - Per le telecamere Axis: inserire nome, indirizzo IP, protocollo di streaming, porta, nome utente e password della telecamera.
     - Per le telecamere di terze parti: inserire nome, indirizzo IP, nome utente e password della telecamera.
3. Fare clic su **Aggiungi**.

## Modificare una sorgente telecamera

Dopo l'aggiunta di una telecamera, sarà possibile modificare le impostazioni dalla vista **Edit (Modifica)**.

1. Andare a **Video sources > Camera sources (Sorgenti video > Sorgenti telecamera)**.
2. Selezionare la sorgente telecamera e fare clic su .
3. Fare clic su **Edit (Modifica)** ed eseguire le modifiche.
4. Fare clic su **Salva**.

## Rimuovere una telecamera

1. Andare a **Video sources > Camera sources (Sorgenti video > Sorgenti telecamera)**.
2. Selezionare la sorgente telecamera e fare clic su .
3. Fare clic su **Delete (Elimina)** e confermare.

## Aggiungere un file multimediale

1. Andare a **Video sources > Media sources (Sorgenti video > Sorgenti multimediali)**.
2. Fare clic su **Add media source (Aggiungi sorgente multimediale)**.
3. Caricare il file multimediale sul dispositivo e selezionare l'ubicazione dove posizionarlo.
4. Fare clic su **Aggiungi**.

## Configurazione di una sequenza

1. Andare a **Sequences > Sequences (Sequenze > Sequenze)**.
2. Fare clic su **+ Add sequence (+ Aggiungi sequenza)**.
3. Immettere un nome per la nuova sequenza.
4. Fare clic su e selezionare un layout per la vista.

5. Nella finestra della visualizzazione, **Click to select camera source or media for this segment (Fare clic per selezionare la sorgente della telecamera o il supporto per questo segmento)**.
6. Selezionare **Camera (Telecamera)** o **Media (Elemento multimediale)** e selezionare una sorgente dall'elenco.

Nota

Per le telecamere di terzi, aggiungere l'URL ottenuto dal produttore della telecamera.

7. Fare clic su **Add (Aggiungi)** e continuare ad aggiungere sorgenti finché la finestra di visualizzazione è piena.
8. Per aggiungere altre finestre vista alla sequenza, fare clic su  .
9. Fare clic su **Salva**.
10. Fare clic su  per la riproduzione della sequenza.

## Usare la scheda di controllo per la navigazione nelle viste e impiegare una telecamera

1. Eseguire l'aggiunta di una telecamera al decoder. Vedere .
2. Accertarsi di attivare PTZ per la propria telecamera Axis.
3. Connettere AXIS TU9001 Control Board al decoder.
4. Nell'interfaccia Web del decoder, andare a **Sequences > Joystick controls (Sequenze > Comandi del joystick)** e attivare il **Joystick**.

### Riferimento tasti scheda di controllo

Nota

Selezionare un riquadro sospenderà la modifica automatica della vista.

| Descrizione | AXIS TU9001 |
|---|---|
| Attivare telecamere PTZ in un'unica vista. | F1 |
| Attivare PTZ sulla telecamera nel riquadro <P> in una suddivisione dell'immagine. | <P> + F1 |
| Impostare telecamera nel riquadro <P> in una suddivisione dell'immagine a schermo intero e attivare PTZ. | <P> + |
| Disattivazione di PTZ e ritorno alla sequenza precedente a schermo intero. | |
| Eseguire un movimento panoramico della telecamera selezionata. | Spostare il joystick a sinistra o a destra |
| Inclinare la telecamera selezionata. | Spostare il joystick in alto o in basso |
| Eseguire lo zoom con la telecamera selezionata. | Spostare la testa del joystick a sinistra o a destra |
| Passare al preset PTZ <N> in un'unica vista e attivare PTZ. | J<N> |
| Impostare il preset PTZ <N> in un'unica vista e attivare PTZ. | ALT + J<N> |

| | |
|---|---|
| Passare al preset PTZ <N> nel riquadro <P> in una suddivisione dell'immagine in un'unica vista e attivare PTZ. | <P> + J<N> |
| Impostare il preset PTZ <N> nel riquadro <P> in una suddivisione dell'immagine in un'unica vista e attivare PTZ. | <P> + ALT + J<N> |

Esempio:

- Se si preme 2 su AXIS TU9003 e poi J1 su AXIS TU9002, la telecamera seleziona il preset PTZ 1 sul riquadro 2 nella suddivisione dell'immagine corrente.
- Se si premono 5 e poi F1 su AXIS TU9003, si attiva la telecamera PTZ sul riquadro 5 nella suddivisione dell'immagine corrente.

Per ulteriori informazioni relative alla scheda di controllo, vedere il *manuale per l'utente*.

## Imposta regole per eventi

È possibile creare delle regole per fare sì che il dispositivo esegua un'azione quando si verificano determinati eventi. Una regola consiste in condizioni e azioni. Le condizioni possono essere utilizzate per attivare le azioni. Ad esempio, il dispositivo può avviare una registrazione o inviare un e-mail quando rileva un movimento oppure può mostrare un testo in sovraimpressione mentre il dispositivo registra.

Consulta la nostra guida *Introduzione alle regole per gli eventi* per ottenere maggiori informazioni.

### Attivazione di un'azione

1. Andare a **System > Events (Sistema > Eventi)** e aggiungere una regola. La regola consente di definire quando il dispositivo eseguirà determinate azioni. È possibile impostare regole pianificate, ricorrenti o attivate manualmente.
2. Immettere un **Name (Nome)**.
3. Selezionare la **Condition (Condizione)** che deve essere soddisfatta per attivare l'azione. Se si specifica più di una condizione per la regola, devono essere soddisfatte tutte le condizioni per attivare l'azione.
4. Selezionare l'**Action (Azione)** che deve eseguire il dispositivo quando le condizioni sono soddisfatte.

Nota

Se vengono apportate modifiche a una regola attiva, tale regola deve essere abilitata nuovamente per rendere valide le modifiche.

## Audio

### File audio

Il dispositivo non supporta file con il solo audio.

## Interfaccia Web

Per raggiungere l'interfaccia Web del dispositivo, digita l'indirizzo IP del dispositivo in un browser Web.

Nota

Il supporto per le funzionalità e le impostazioni descritte in questa sezione varia da un dispositivo all'altro.

Questa icona indica che la funzione o l'impostazione è disponibile solo in certi dispositivi.

Mostra o nascondi il menu principale.

Accedere alle note di rilascio.

Accedere alla guida dispositivo.

Modificare la lingua.

Imposta il tema chiaro o il tema scuro.

Il menu contestuale contiene:

- Informazioni relative all'utente che ha eseguito l'accesso.
- **Change account (Modifica account)**: Disconnettersi dall'account corrente e accedere a un nuovo account.
- **Log out (Esci)**: Disconnettersi dall'account corrente.

Il menu contestuale contiene:

- **Analytics data (Dati di analisi)**: acconsenti alla condivisione dei dati non personali del browser.
- **Feedback**: condividi qualsiasi feedback per contribuire a rendere migliore la tua esperienza utente.
- **Legal (Informazioni legali)**: visualizzare informazioni sui cookie e le licenze.
- **About (Informazioni)**: visualizza le informazioni relative al dispositivo, compresa la versione di AXIS OS e il numero di serie.

### Stato

#### Informazioni sui dispositivi

Mostra le informazioni relative al dispositivo, compresa la versione AXIS OS e il numero di serie.

**Upgrade AXIS OS (Aggiorna AXIS OS)**: Aggiorna il software sul dispositivo. Porta l'utente sulla pagina Manutenzione dove è possibile eseguire l'aggiornamento.

#### Stato sincronizzazione ora

Mostra le informazioni di sincronizzazione NTP, inclusa l'eventuale sincronizzazione del dispositivo con un server NTP e il tempo che rimane fino alla sincronizzazione successiva.

**NTP settings (Impostazioni NTP)**: visualizza e aggiorna le impostazioni NTP. Porta l'utente alla pagina **Time and location (Ora e posizione)** dove è possibile modificare le impostazioni NTP.

### Sicurezza

Mostra il tipo di accesso attivo al dispositivo, i protocolli di crittografia in uso e se sono consentite app non firmate. I consigli di impostazione sono basati sulla Guida alla protezione AXIS OS.

**Hardening guide (Guida alla protezione)**: fare clic per andare su *Guida alla protezione di AXIS OS*, dove è possibile ottenere ulteriori informazioni sulla cybersecurity per i dispositivi Axis e le best practice.

### Clienti collegati

Mostra il numero di connessioni e client connessi.

**View details (Visualizza dettagli)**: Consente di visualizzare e aggiornare l'elenco dei client connessi. L'elenco mostra l'indirizzo IP, il protocollo, la porta, lo stato e il PID/processo di ogni connessione.

## Sequenze

### Monitoraggio

Mostra informazioni riguardanti la sequenza.

### Performance control (Controllo delle prestazioni)

**Latency threshold (Soglia della latenza)**: selezionare la latenza massima per i flussi. Quando la soglia viene superata, i fotogrammi vengono eliminati per raggiungere la latenza di destinazione. Non si applica alla decodifica del software.

### Joystick controls (Comandi joystick)

**Joystick**: attivarlo per avere la possibilità di usare la scheda di controllo per la navigazione nelle viste e l'uso di una telecamera.

### Sequenze

Importante

Per evitare problemi relativi alle riproduzioni multiflusso, attenersi ai consigli nell'interfaccia Web.

**Add sequence (Aggiungi sequenza)**: fare clic per creare una sequenza.

**Nome**: inserire un nome per la sequenza;

: Fare clic per eseguire la selezione di quante sorgenti si desidera visualizzare.

: fare clic su per aggiungerne un'altra .

: Fare clic per la riproduzione della sequenza.

Il menu contestuale contiene:

**Modifica sequenza**

**Elimina sequenza**

## Audio

### Impostazioni dispositivo

**Uscita audio**

**Enable Output (Abilita output)**: attivare o disattivare l'audio dal connettore di uscita audio.

**Audio out synchronization (Sincronizzazione uscita audio)**: impostare un tempo per adattare la differenza di ritardo tra la porta di uscita audio (3,5 mm) e il flusso video.

## Sorgenti video

**Sorgenti telecamera**

**Add camera source (Aggiungi sorgente telecamera)**: Fare clic per aggiungere una nuova sorgente della telecamera.

- **Network discovery (Individuazione rete)**: cercare in modo manuale un indirizzo IP o selezionare un dispositivo Axis dalla lista.
  - **Streaming protocol (Protocollo di streaming)**: selezionare il protocollo da utilizzare
  - **Porta**: Immettere il numero di porta.
    - 554 è il valore predefinito per **RTSPT**
    - 80 è il valore predefinito per **RTSP su HTTP**
    - 443 è il valore predefinito per **RTSP su HTTPS**
  - **Account**: immettere il nome utente per il dispositivo.
  - **Password**: immettere la password per il dispositivo.
  - **Include motion events (Includi eventi di movimento)**: Selezionare per consentire l'utilizzo del rilevamento movimento dalla telecamera come condizione di evento. Questa impostazione è disponibile solo per le telecamere Axis.
- **Manual (Manuale)**: Aggiunta manuale di un dispositivo.
  - **Nome**: Immettere il nome della sorgente video.
  - **Indirizzo IP**: Immettere l'indirizzo IP del dispositivo.
  - **Account**: immettere il nome utente per il dispositivo.
  - **Password**: immettere la password per il dispositivo.
  - **Include motion events (Includi eventi di movimento)**: Selezionare per consentire l'utilizzo del rilevamento movimento dalla telecamera come condizione di evento. Questa impostazione è disponibile solo per le telecamere Axis.

Il menu contestuale contiene:

**Edit (Modifica)**: Modifica le proprietà della sorgente video.

**Elimina**; Elimina sorgente video.

**Sorgenti multimediali**

**Add media source (Aggiungi sorgente multimediale)**: Fare clic per eseguire l'aggiunta di una nuova sorgente multimediale.

- Caricare o trascinare e rilasciare un file multimediale. Si possono usare file .mp4, .mkv, .jpeg o .png.
- **Upload location (Carica ubicazione)**: Selezionare l'ubicazione dall'elenco a discesa.

## App

**Aggiungi app**: Installa una nuova app.

**Find more apps (Trova altre app)**: Trova altre app da installare. Verrà visualizzata una pagina panoramica delle app Axis.

**Consenti app prive di firma** : Attiva per permettere che siano installate app senza firma.

Visualizzare gli aggiornamenti sulla sicurezza nelle app AXIS OS e ACAP.

Nota

Eseguire più app allo stesso tempo può avere un impatto sulle prestazioni del dispositivo.

Usa l'interruttore vicino al nome dell'app per l'avvio o l'arresto dell'app.

**Open (Apri)**: Accedi alle impostazioni dell'app. Le impostazioni disponibili dipendono dall'applicazione. Alcune applicazioni non sono dotate di impostazioni.

Il menu contestuale può contenere una o più delle seguenti opzioni:

- **Open-source license (Licenza open-source)**: Visualizza le informazioni relative alle licenze open source usate nell'app.
- **App log (Registro app)**: Visualizza un registro degli eventi relativi all'app. Il registro è utile quando si contatta l'assistenza.
- **Activate license with a key (Attiva licenza con una chiave)**: nel caso l'app necessiti di una licenza, devi attivarla. Se il dispositivo non ha accesso a Internet, usa questa opzione.
  Se non si dispone di una chiave di licenza, andare a *axis.com/products/analytics*. Per generare una chiave di licenza, sono necessari il codice di licenza e il numero di serie del dispositivo Axis.
- **Activate license automatically (Attiva automaticamente la licenza)**: nel caso l'app necessiti di una licenza, devi attivarla. Se il dispositivo ha accesso a Internet, usa questa opzione. È necessario un codice di licenza per attivare la licenza.
- **Disattiva la licenza**: Disattivare la licenza per sostituirla con un'altra licenza, ad esempio quando si passa da una licenza di prova a una licenza completa. Se si disattiva la licenza, verrà eliminata anche dal dispositivo.
- **Settings (Impostazioni)**: Configurare i parametri del dispositivo.
- **Elimina**; Cancella permanentemente l'app dal dispositivo. La licenza resta attiva a meno che non la disattivi prima.

## Sistema

### Ora e ubicazione

#### Data e ora

Le impostazioni della lingua del browser Web influenzano il formato dell'ora.

Nota

Consigliamo di eseguire la sincronizzazione di data e ora del dispositivo usando un server NTP.

**Synchronization (Sincronizzazione)**: selezionare un'opzione per la sincronizzazione di data e ora del dispositivo.

- **Automatic date and time (manual NTS KE servers) (Data e ora automatiche (server NTS KE manuali))**: eseguire la sincronizzazione con i server NTP key establishment sicuri connessi al server DHCP.
  - **Manual NTS KE servers (Server NTS KE manuali)**: inserisci l'indirizzo IP di uno o due server NTP. Quando usi due server NTP, l'ora del dispositivo viene sincronizzata e adattata sulla base dell'input di entrambi.
  - **Max NTP poll time (Tempo massimo poll NTP)**: Selezionare il tempo massimo di attesa del dispositivo prima di eseguire il polling del server NTP per ottenere un'ora aggiornata.
  - **Min NTP poll time (Tempo min poll NTP)**: Selezionare il tempo minimo di attesa del dispositivo prima di eseguire il polling del server NTP per ottenere un'ora aggiornata.
- **Automatic date and time (NTP servers using DHCP) (Data e ora automatiche (server NTP tramite DHCP))**: esegui la sincronizzazione con i server NTP connessi al server DHCP.
  - **Fallback NTP servers (Server NTP di fallback)**: inserisci l'indirizzo IP di uno o due server fallback.
  - **Max NTP poll time (Tempo massimo poll NTP)**: Selezionare il tempo massimo di attesa del dispositivo prima di eseguire il polling del server NTP per ottenere un'ora aggiornata.
  - **Min NTP poll time (Tempo min poll NTP)**: Selezionare il tempo minimo di attesa del dispositivo prima di eseguire il polling del server NTP per ottenere un'ora aggiornata.
- **Automatic date and time (manual NTP servers) (Data e ora automatiche (server NTP manuali))**: esegui la sincronizzazione con i server NTP scelti.
  - **Manual NTP servers (Server NTP manuali)**: inserisci l'indirizzo IP di uno o due server NTP. Quando usi due server NTP, l'ora del dispositivo viene sincronizzata e adattata sulla base dell'input di entrambi.
  - **Max NTP poll time (Tempo massimo poll NTP)**: Selezionare il tempo massimo di attesa del dispositivo prima di eseguire il polling del server NTP per ottenere un'ora aggiornata.
  - **Min NTP poll time (Tempo min poll NTP)**: Selezionare il tempo minimo di attesa del dispositivo prima di eseguire il polling del server NTP per ottenere un'ora aggiornata.
- **Custom date and time (Data e ora personalizzate)**: impostare manualmente la data e l'ora. Per recuperare una volta dal computer o dal dispositivo mobile le impostazioni di data e ora, fare clic su **Get from system (Ottieni dal sistema)**.

**Fuso orario**: selezionare il fuso orario da utilizzare. L'ora legale e l'ora solare si alterneranno automaticamente.

- **DHCP**: Adotta il fuso orario del server DHCP. Il dispositivo si deve connettere a un server DHCP prima di poter selezionare questa opzione.
- **Manual (Manuale)**: Selezionare un fuso orario dall'elenco a discesa.

Nota

Il sistema utilizza le impostazioni di data e ora in tutte le registrazioni, i registri e le impostazioni di sistema.

## Rete

### IPv4

**Assign IPv4 automatically (Assegna automaticamente IPv4)**: Selezionare questa opzione per consentire al router di rete di assegnare automaticamente un indirizzo IP al dispositivo. Si consiglia l'IP automatico (DHCP) per la maggior parte delle reti.

**Indirizzo IP**: Inserire un indirizzo IP univoco per il dispositivo. Gli indirizzi IP fissi possono essere assegnati casualmente in reti isolate, a condizione che ogni indirizzo sia univoco. Per evitare conflitti, si consiglia di contattare l'amministratore di rete prima di assegnare un indirizzo IP statico.

**Subnet mask**: Immetti la subnet mask per definire quali indirizzi sono all'interno della rete locale. Qualsiasi indirizzo fuori dalla rete locale passa attraverso il router.

**Router**: Inserire l'indirizzo IP del router predefinito (gateway) utilizzato per connettere i dispositivi collegati a reti diverse e a segmenti di rete.

**Fallback to static IP address if DHCP isn't available (Fallback all'indirizzo IP fisso se DHCP non è disponibile)**: selezionalo se vuoi aggiungere un indirizzo IP statico da usare come fallback se DHCP non è disponibile e non è possibile assegnare in automatico un indirizzo IP.

Nota

Se DHCP non è disponibile e il dispositivo utilizza un fallback dell'indirizzo statico, l'indirizzo statico viene configurato con un ambito limitato.

### IPv6

**Assign IPv6 automatically (Assegna automaticamente IPv6)**: Selezionare questa opzione per attivare IPv6 e consentire al router di rete di assegnare automaticamente un indirizzo IP al dispositivo.

### Nome host

**Assign hostname automatically (Assegna automaticamente il nome host)**: Selezionare questa opzione per consentire al router di rete di assegnare automaticamente un nome host al dispositivo.

**Nome host**: Immetti manualmente il nome host da usare come metodo alternativo per accedere al dispositivo. Il report del server e il registro di sistema utilizzano il nome host. I caratteri consentiti sono A–Z, a–z, 0–9 e -.

**Abilitare gli aggiornamenti DNS dinamici**: Consentire al proprio dispositivo di aggiornare automaticamente le registrazioni del server dei nomi di dominio ogni volta che cambia l'indirizzo IP.

**Registra nome DNS**: Inserire un nome dominio univoco che punti all'indirizzo IP del dispositivo. I caratteri consentiti sono A–Z, a–z, 0–9 e -.

**TTL**: il Time To Live (TTL) stabilisce per quanto tempo una registrazione DNS resta valida prima che debba essere aggiornata.

### Server DNS

**Assign DNS automatically (Assegna automaticamente DNS)**: Selezionare questa opzione per consentire al server DHCP di assegnare automaticamente i domini di ricerca e gli indirizzi del server DNS al dispositivo. Si consiglia il DNS automatico (DHCP) per la maggior parte delle reti.

**Search domains (Domini di ricerca)**: Quando si utilizza un nome host non completo, fare clic su **Add search domain (Aggiungi dominio di ricerca)** e inserire un dominio in cui cercare il nome host utilizzato dal dispositivo.

**DNS servers (Server DNS)**: Fare clic su **Add DNS server (Aggiungi server DNS)** e inserire l'indirizzo IP del server DNS. Offre la conversione dei nomi host in indirizzi IP nella rete.

### HTTP e HTTPS

HTTPS è un protocollo che fornisce la crittografia per le richieste di pagine da parte di utenti e per le pagine restituite dal server Web. Lo scambio di informazioni crittografate è regolato dall'utilizzo di un certificato HTTPS, che garantisce l'autenticità del server.

Per utilizzare HTTPS nel dispositivo, è necessario installare un certificato HTTPS. Andare a **System > Security (Sistema > Sicurezza)** per creare e installare i certificati.

**Allow access through (Consenti l'accesso tramite)**: Selezionare questa opzione se a un utente è consentito connettersi al dispositivo tramite **HTTP**, **HTTPS** o entrambi i protocolli **HTTP e HTTPS**.

Nota

Se si visualizzano pagine Web crittografate tramite HTTPS, è possibile che si verifichi un calo delle prestazioni, soprattutto quando si richiede una pagina per la prima volta.

**HTTP port (Porta HTTP)**: inserire la porta HTTP da utilizzare. Il dispositivo consente l'utilizzo della porta 80 o di qualsiasi porta nell'intervallo 1024-65535. Se è stato eseguito l'accesso come amministratore, è possibile immettere qualsiasi porta nell'intervallo da 1 a 1023. Se si utilizza una porta in questo intervallo, viene visualizzato un avviso.

**HTTPS port (Porta HTTPS)**: inserire la porta HTTPS da utilizzare. Il dispositivo consente l'utilizzo della porta 443 o di qualsiasi porta nell'intervallo 1024-65535. Se è stato eseguito l'accesso come amministratore, è possibile immettere qualsiasi porta nell'intervallo da 1 a 1023. Se si utilizza una porta in questo intervallo, viene visualizzato un avviso.

**Certificato**: selezionare un certificato per abilitare HTTPS per il dispositivo.

### Protocolli di individuazione in rete

**Bonjour®**: attivare per consentire il rilevamento automatico sulla rete.

**Nome Bonjour**: Inserire un nome descrittivo che deve essere visibile sulla rete. Il nome predefinito è il nome del dispositivo e l'indirizzo MAC.

**UPnP®**: attivare per consentire il rilevamento automatico sulla rete.

**UPnP name**: Inserire un nome descrittivo che deve essere visibile sulla rete. Il nome predefinito è il nome del dispositivo e l'indirizzo MAC.

**WS-Discovery**: attivare per consentire il rilevamento automatico sulla rete.

**LLDP e CDP**: attivare per consentire il rilevamento automatico sulla rete. La disattivazione di LLDP e CDP può influire sulla negoziazione dell'alimentazione PoE. Per risolvere eventuali problemi con la negoziazione dell'alimentazione PoE, configurare lo switch PoE solo per la negoziazione dell'alimentazione PoE dell'hardware.

### Proxy globali

**Http proxy**: specificare un host o un indirizzo IP del proxy globale secondo il formato consentito.

**Https proxy**: specificare un host o un indirizzo IP del proxy globale secondo il formato consentito.

Formati consentiti per i proxy http e https:

- http(s)://host:porta
- http(s)://user@host:porta
- http(s)://user:pass@host:porta

Nota

Riavviare il dispositivo per applicare le impostazioni proxy globali.

**No proxy (Nessun proxy)**: Utilizzare **No proxy (Nessun proxy)** per bypassare i proxy globali. Immettere una delle opzioni dell'elenco o più opzioni separate da una virgola:

- Lasciare vuoto
- Indicare un indirizzo IP
- Indicare un indirizzo IP in formato CIDR
- Indicare un nome dominio, ad esempio: www.<nome dominio>.com
- Specificare tutti i sottodomini di un dominio specifico, ad esempio .<nome dominio>.com

### Connessione al cloud con un clic

One-Click Cloud Connect (O3C), utilizzato in combinazione con un servizio O3C, offre un accesso Internet facile e sicuro a video in diretta e registrati, accessibili da qualsiasi ubicazione. Per ulteriori informazioni, vedere *axis.com/end-to-end-solutions/hosted-services*.

**Allow O3C (Consenti O3C)**:

- **One-click**: Questa è l'impostazione predefinita. Tenere premuto il pulsante di comando sul dispositivo per collegarsi a un servizio O3C via Internet. È necessario registrare il dispositivo con il servizio O3C entro 24 ore dopo aver premuto il pulsante di comando. In caso contrario, il dispositivo si disconnette dal servizio O3C. Una volta registrato il dispositivo, viene abilitata l'opzione **Always (Sempre)** e il dispositivo rimane collegato al servizio O3C.
- **Sempre**: il dispositivo Axis tenta costantemente di collegarsi a un servizio O3C via Internet. Una volta registrato, il dispositivo rimane collegato al servizio O3C. Utilizzare questa opzione se il pulsante di comando del dispositivo non è disponibile.
- **No**: disabilita il servizio O3C.

**Proxy settings (Impostazioni proxy)**: Se necessario, inserire le impostazioni proxy per collegarsi al server proxy.

**Host**: Inserire l'indirizzo del server del proxy.

**Porta**: inserire il numero della porta utilizzata per l'accesso.

**Accesso** e **Password**: se necessario, immettere un nome utente e una password per il server proxy.

**Metodo di autenticazione**:

- **Base**: questo metodo è lo schema di autenticazione maggiormente compatibile per HTTP. È meno sicuro del metodo **Digest** perché invia il nome utente e la password non crittografati al server.
- **Digest**: questo metodo è più sicuro perché la password viene sempre trasferita crittografata nella rete.
- **Automatico**: questa opzione consente al dispositivo Axis di selezionare il metodo di autenticazione a seconda dei metodi supportati, dando priorità a **Digest** rispetto al metodo **Base**.

**Owner authentication key (OAK) (Chiave di autenticazione proprietario (OAK))**: Fare clic su **Get key (Ottieni chiave)** per recuperare la chiave di autenticazione proprietaria. Questo è possibile solo se il dispositivo è connesso a Internet senza un firewall o un proxy.

### SNMP

SNMP (Simple Network Management Protocol) consente il monitoraggio e la gestione in remoto dei dispositivi di rete.

**SNMP**: Selezionare la versione di SNMP da utilizzare.

- **v1 and v2c (v1 e v2c)**:
  - **Read community (Comunità con privilegi in lettura)**: Inserire il nome della comunità che dispone solo dell'accesso in lettura a tutti gli oggetti SNMP supportati. Il valore predefinito è **public**.
  - **Write community (Comunità con privilegi in scrittura)**: Specificare il nome della comunità che dispone di accesso in lettura o scrittura a tutti gli oggetti SNMP supportati (ad eccezione degli oggetti in sola lettura). Il valore predefinito è **write**.
  - **Activate traps (Attiva trap)**: Attivare la segnalazione di trap. Il dispositivo utilizza i trap per inviare messaggi per eventi importanti o cambi di stato a un sistema di gestione. Nell'interfaccia Web, è possibile impostare trap per SNMP v1 e v2c. I trap vengono disattivati automaticamente se si cambia in SNMP v3 o si disattiva SNMP. Se si utilizza SNMP v3, è possibile impostare i trap tramite l'applicazione di gestione SNMP v3.
  - **Trap address (Indirizzo trap)**: immettere l'indirizzo IP o il nome host del server di gestione.
  - **Trap community (Comunità trap)**: Immettere la comunità da utilizzare quando il dispositivo invia un messaggio trap al sistema di gestione.
  - **Traps (Trap)**:
    - **Cold start (Avvio a freddo)**: Invia un messaggio di trap all'avvio del dispositivo.
    - **Warm start (Avvio a caldo)**: Invia un messaggio trap quando si modifica un'impostazione SNMP.
    - **Link up**: invia un messaggio trap quando un collegamento cambia dal basso verso l'alto.
    - **Autenticazione non riuscita**: invia un messaggio trap quando un tentativo di autenticazione non riesce.

Nota

Tutti i trap Axis Video MIB vengono abilitati quando si attivano i trap SNMP v1 e v2c. Per ulteriori informazioni, vedere *AXIS OS Portal > SNMP (Poortale sistema operativo AXIS > SNMP)*.

- **v3**: SNMP v3 è una versione più sicura che fornisce crittografia e password sicure. Per utilizzare SNMP v3, si consiglia di attivare HTTPS poiché la password verrà successivamente inviata via HTTPS. Ciò impedisce inoltre alle parti non autorizzate di accedere ai trap SNMP v1 e v2c non crittografati. Se si utilizza SNMP v3, è possibile impostare i trap tramite l'applicazione di gestione SNMP v3.
  - **Password for the account "initial" (Password per l'account "iniziale")**: Immettere la password SNMP per l'account denominato "iniziale". Sebbene la password possa essere inviata senza attivare HTTPS, non è consigliabile. La password SNMP v3 può essere impostare solo una volta e preferibilmente solo quando è attivato HTTPS. Una volta impostata la password, il relativo campo non verrà più visualizzato. Per impostare di nuovo la password, il dispositivo deve essere ripristinato alle impostazioni predefinite di fabbrica.

## Sicurezza

### Certificati

I certificati sono utilizzati per autenticare i dispositivi in una rete. I tipi di certificati supportati da questo dispositivo sono due:

- **Client/server certificates (Certificati client/server)**
  Un certificato client/server convalida l'identità del dispositivo e può essere autofirmato o emesso da un'autorità di certificazione (CA). Un certificato autofirmato offre una protezione limitata e può essere utilizzato prima che sia stato ottenuto un certificato emesso da un'autorità di certificazione.
- **Certificati CA**
  È possibile utilizzare un certificato CA per autenticare un certificato peer, ad esempio per convalidare l'identità di un server di autenticazione nel caso in cui il dispositivo venga collegato a una rete protetta da IEEE 802.1X. Il dispositivo dispone di diversi certificati CA preinstallati.

Questi formati sono supportati:

- Formati dei certificati: .PEM, .CER e .PFX
- Formati delle chiavi private: PKCS#1 e PKCS#12

Importante

Se il dispositivo viene ripristinato alle impostazione di fabbrica, tutti i certificati vengono eliminati. Qualsiasi certificato CA preinstallato viene reinstallato.

**Add certificate (Aggiungi certificato)**: fare clic sull'opzione per aggiungere un certificato. Si apre una guida passo dopo passo.

- **Più** : mostra altri campi da compilare o selezionare.
- **Secure keystore (Archivio chiavi sicuro)**: selezionare questa opzione per utilizzare **Trusted Execution Environment (SoC TEE)**, **Secure Element** o **Trusted Platform Module 2.0** per archiviare in modo sicuro la chiave privata. Per ulteriori informazioni su quale keystore sicuro selezionare, andare a *help.axis.com/en-us/axis-os#cryptographic-support*.
- **Key type (Tipo chiave)**: selezionare l'algoritmo di crittografia predefinito o diverso dall'elenco a discesa per proteggere il certificato.

Il menu contestuale contiene:

- **Certificate information (Informazioni certificato)**: visualizza le proprietà di un certificato installato.
- **Delete certificate (Elimina certificato)**: Elimina il certificato.
- **Create certificate signing request (Crea richiesta di firma certificato)**: Per fare richiesta di un certificato di identità digitale, crea una richiesta di firma del certificato da mandare a un'autorità di registrazione.

**Secure keystore (Archivio chiavi sicuro)** :

- **Trusted Execution Environment (SoC TEE)**: selezionare l'uso di SoC TEE per l'archivio chiavi sicuro.
- **Secure element (CC EAL6+) (Elemento sicuro)**: Selezionare questa opzione per utilizzare un elemento sicuro per l'archivio chiavi sicuro.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Level 2)** Selezionare questa opzione per utilizzare TPM 2.0 per il keystore sicuro.

**Controllo degli accessi di rete e crittografia**

**IEEE 802.1x**

IEEE 802.1x è uno standard IEEE per il controllo di ammissione alla rete in base alla porta che fornisce un'autenticazione sicura di dispositivi di rete cablati e wireless. IEEE 802.1x è basato su EAP (Extensible Authentication Protocol).

Per accedere a una rete protetta da IEEE 802.1x, i dispositivi di rete devono autenticarsi. L'autenticazione viene eseguita da un server di autenticazione, generalmente un server RADIUS (ad esempio FreeRADIUS e Microsoft Internet Authentication Server).

**IEEE 802.1AE MACsec**

IEEE 802.1AE MACsec rappresenta uno standard IEEE per la sicurezza MAC (Media Access Control) che definisce la riservatezza e l'integrità dati senza connessione per i protocolli indipendenti di accesso ai media.

**Certificati**

Se configurato senza un certificato CA, la convalida del certificato del server verrà disabilitata e il dispositivo cercherà in questo caso di autenticarsi a prescindere dalla rete a cui è connesso.

Nell'implementazione di Axis, quando si utilizza un certificato, il dispositivo e il server di autenticazione si autenticano con certificati digitali mediante EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).

Per consentire al dispositivo di accedere a una rete protetta tramite certificati, è necessario installare un certificato client firmato sul dispositivo.

**Metodo di autenticazione**: selezionare un tipo EAP impiegato per l'autenticazione.

**Client Certificate (Certificato client)**: selezionare un certificato client per utilizzare IEEE 802.1x. Il server di autenticazione utilizza il certificato per convalidare l'identità del client.

**Certificati CA**: selezionare i certificati CA per convalidare l'identità del server di autenticazione. Quando non ne viene selezionato nessun certificato, il dispositivo tenterà di autenticarsi a prescindere dalla rete a cui è connesso.

**EAP identity (Identità EAP)**: Immettere l'identità utente associata al certificato del client.

**EAPOL version (Versione EAPOL)**: Selezionare la versione EAPOL utilizzata nello switch di rete.

**Use IEEE 802.1x (Usa IEEE 802.1x)**: Selezionare questa opzione per utilizzare il protocollo IEEE 802.1x.

Le impostazioni sono a disposizione solo se si usa **IEEE 802.1x PEAP-MSCHAPv2** come metodo di autenticazione:

- **Password**: immettere la password per l'identità utente.
- **Peap version (Versione Peap)**: selezionare la versione Peap utilizzata nello switch di rete.
- **Label (Etichetta)**: Selezionare 1 per utilizzare la codifica EAP del client; selezionare 2 per utilizzare la crittografia PEAP del client. Selezionare l'etichetta usata dallo switch di rete quando si utilizza Peap versione 1.

Le impostazioni sono a disposizione solo se si usa **IEEE 802.1ae MACsec (chiave Static CAK/Pre-Shared)** come metodo di autenticazione:

- **Key agreement connectivity association key name (Nome della chiave di associazione della connettività del contratto chiave)**: immettere il nome dell'associazione della connettività (CKN). Deve essere composto da 2 a 64 caratteri esadecimali (divisibili per 2). Il CKN deve essere configurato manualmente nell'associazione della connettività e deve corrispondere su entrambe le estremità del collegamento per abilitare inizialmente MACsec.
- **Key agreement connectivity association key (Chiave di associazione della connettività del contratto chiave)**: immettere la chiave di associazione della connettività (CAK). Deve essere composta da 32 o 64 caratteri esadecimali. Il CAK deve essere configurato manualmente nell'associazione della

connettività e deve corrispondere su entrambe le estremità del collegamento per abilitare inizialmente MACsec.

**Prevenire gli attacchi di forza bruta**

**Blocking (Blocco)**: Attiva per bloccare gli attacchi di forza bruta. Un attacco di forza bruta usa tentativi ed errori per indovinare le informazioni di accesso o le chiavi di crittografia.

**Blocking period (Periodo di blocco)**: Immettere il numero di secondi per cui si blocca un attacco di forza bruta.

**Blocking conditions (Condizioni di blocco)**: Immettere il numero di errori di autenticazione consentiti al secondo prima dell'inizio del blocco. È possibile impostare il numero di errori consentiti a livello di pagina e di dispositivo.

**Firewall**

**Activate (Attivare)**: Attivare il firewall.

**Default Policy (Criterio predefinito)**: Selezionare lo stato predefinito per il firewall.

- **Allow: (Consenti)** Permette tutte le connessioni al dispositivo. Questa opzione è impostata per impostazione predefinita.
- **Deny: (Rifiuta)** Nega tutte le connessioni al dispositivo.

Per eccezioni al criterio predefinito, si può eseguire la creazione di regole che permettono o negano le connessioni al dispositivo da indirizzi, protocolli e porte specifici.

- **Indirizzo**: inserire un indirizzo in formato IPv4/IPv6 o CIDR al quale si vuole permettere o rifiutare l'accesso.
- **Protocol (Protocollo)**: selezionare un protocollo al quale permettere o negare l'accesso.
- **Porta**: Inserire un numero di porta alla quale permettere o negare l'accesso. Si può aggiungere un numero di porta tra 1 e 65535.
- **Policy (Criteri)**: Selezionare il criterio della regola.

: Fare clic per la creazione di un'altra regola.

**Add rules: (Aggiungi regole)** Fare clic per l'aggiunta di regole definite.

- **Time in seconds: (Tempo in secondi)** Impostare un limite di tempo al fine di mettere alla prova le regole. Il limite di tempo predefinito è impostato su 300 secondi. Per l'attivazione immediata delle regole, impostare il tempo su 0 secondi.
- **Confirm rules: (Conferma regole)** Eseguire la conferma delle regole e il relativo limite di tempo. Se si è impostato un limite di tempo superiore a 1 secondo, le regole saranno attive durante tale periodo. Se il tempo è stato impostato su 0, le regole saranno subito attive.

**Pending rules (Regole in sospeso)**: Una panoramica delle ultime regole testate da confermare.

Nota

Le regole con un limite di tempo appaiono in **Active rules (Regole attive)** fino a quando non termina il conteggio del timer visualizzato o fino a quando non vengono confermate. Se non si confermano, appaiono in **Pending rules (Regole in sospeso)** fino a quando non termina il conteggio del timer visualizzato e il firewall torna alle impostazioni precedentemente definite. Se si confermano, sostituiranno le regole attive correnti.

**Confirm rules (Conferma regole)**: Fare clic per eseguire l'attivazione delle regole in sospeso.

**Active rules (Regole attive)**: una panoramica delle regole in esecuzione al momento sul proprio dispositivo.

: Fare clic per eseguire l'eliminazione di una regola attiva.

: Fare clic per eseguire l'eliminazione di tutte le regole, sia in sospeso che attive.

**Certificato AXIS con firma personalizzata**

Serve un certificato AXIS OS con firma personalizzata per l'installazione di software di prova o software personalizzato di altro tipo di Axis sul dispositivo. Il certificato verifica che il software è stato approvato sia dal proprietario del dispositivo che da Axis. È possibile eseguire il software unicamente su uno specifico dispositivo identificabile tramite il suo numero di serie univoco e l'ID del chip. Solo Axis può creare certificati AXIS OS con firma personalizzata poiché Axis detiene la chiave per firmarli.

**Install (Installa)**: Fare clic per eseguire l'installazione del certificato. Il certificato deve essere installato prima del software.

Il menu contestuale contiene:

- **Delete certificate (Elimina certificato)**: Elimina il certificato.

## Account

### Account

**Add account (Aggiungi account)**: Fare clic per aggiungere un nuovo account. Puoi aggiungere un massimo di 100 account.

**Account**: Inserire un nome account univoco.

**New password (Nuova password)**: inserire una password per l'account. La lunghezza delle password deve essere compresa tra 1 e 64 caratteri. La password può contenere solo caratteri ASCII stampabili (codice da 32 a 126), quali lettere, numeri, segni di punteggiatura e alcuni simboli.

**Repeat password (Ripeti password)**: Immettere di nuovo la stessa password.

**Privileges (Privilegi)**:

- **Administrator (Amministratore)**: ha accesso completo a tutte le impostazioni. Gli amministratori possono anche aggiungere, aggiornare e rimuovere altri account.
- **Operator (Operatore)**: ha accesso a tutte le impostazioni ad eccezione di:
  - Tutte le impostazioni **System (Sistema)**.
- **Viewer (Visualizzatore)**: Ha accesso a:
  - Visione e scatto di istantanee di un flusso video.
  - Riproduci ed esporta le registrazioni.
  - Panoramica, inclinazione e zoom; con accesso **Account PTZ**.

Il menu contestuale contiene:

**Update account (Aggiorna account)**: Modifica le proprietà dell'account.

**Delete account (Elimina account)**: Elimina l'account. Non puoi cancellare l'account root.

### Accesso anonimo

**Allow anonymous viewing (Consenti visualizzazione anonima)**: attiva questa opzione per permettere a chiunque l'accesso al dispositivo in qualità di visualizzatore senza accedere con un account utente.

**Allow anonymous PTZ operating (Consenti uso anonimo di PTZ)** : per permettere agli utenti anonimi di eseguire la panoramica, inclinazione e zoom dell'immagine, attiva questa opzione.

### Virtual host (Host virtuale)

**Add virtual host (Aggiungi host virtuale)**: fare clic su questa opzione per aggiungere un nuovo host virtuale.

**Abilitata**: selezionare questa opzione per utilizzare l'host virtuale.

**Server name (Nome del server)**: inserire il nome del server. Utilizzare solo i numeri da 0 a 9, le lettere dalla A alla Z e il trattino (-).

**Porta**: inserire la porta a cui è connesso il server.

**Tipo**: selezionare il tipo di autenticazione da utilizzare. Scegliere tra **Basic (Base)**, **Digest** e **Open ID**.

Il menu contestuale contiene:

- **Update (Aggiorna)**: aggiornare l'host virtuale.
- **Elimina**; eliminare l'host virtuale.

**Disabled (Disabilitato)**: il server è disabilitato.

## Eventi

### Regole

Una regola consente di definire le condizioni che attivano il dispositivo per l'esecuzione di un'azione. L'elenco mostra tutte le regole correntemente configurate nel dispositivo.

Nota

Puoi creare un massimo di 256 regole di azione.

**Aggiungere una regola**: Creare una regola.

**Nome**: Immettere un nome per la regola.

**Wait between actions (Attesa tra le azioni)**: Inserisci il periodo di tempo minimo (hh:mm:ss) che deve trascorrere tra le attivazioni della regola. Risulta utile se la regola si attiva, ad esempio, nelle condizioni della modalità diurna/notturna, per evitare che piccole variazioni di luce durante l'alba e il tramonto attivino ripetutamente la regola.

**Condition (Condizione)**: Selezionare una condizione dall'elenco. Una condizione che deve essere soddisfatta affinché il dispositivo esegua un'azione. Se vengono definite più condizioni, devono essere tutte soddisfatte per attivare l'azione. Vedere *Introduzione alle regole per gli eventi* per ottenere informazioni riguardo a condizioni specifiche.

**Use this condition as a trigger (Utilizza questa condizione come trigger)**: Selezionare questa opzione affinché questa prima condizione operi solo in qualità di trigger di avvio. Vuol dire che una volta attivata la regola, essa rimane attiva purché tutte le altre condizioni siano soddisfatte, a prescindere dallo stato della prima condizione. Se non selezioni questa opzione, la regola sarà semplicemente attiva quando tutte le condizioni sono soddisfatte.

**Invert this condition (Inverti questa condizione)**: Selezionala se desideri che la condizione sia l'opposto della tua selezione.

**Aggiungere una condizione**: fare clic per l'aggiunta di un'ulteriore condizione.

**Action (Azione)**: seleziona un'azione dalla lista e inserisci le informazioni necessarie. Vedere *Introduzione alle regole per gli eventi* per ottenere informazioni riguardo ad azioni specifiche.

### Destinatari

Hai la possibilità di configurare il dispositivo perché invii ai destinatari notifiche relative ad eventi o dei file.

Nota

Se si imposta il dispositivo per l'utilizzo di FTP o SFTP, non modificare o rimuovere il numero di sequenza univoco aggiunto ai nomi dei file. Se ciò accadesse sarebbe possibile inviare solo un'immagine per evento.

Nell'elenco vengono mostrati i destinatari configurati al momento nel dispositivo insieme alle varie informazioni sulla relativa configurazione.

Nota

È possibile creare fino a 20 destinatari.

**Add a recipient (Aggiungi un destinatario)**: fare clic per aggiungere un destinatario.

**Nome**: immettere un nome per il destinatario.

**Tipo**: Seleziona dall'elenco:

- FTP
  - **Host**: Inserire l'indirizzo IP o il nome host del server. Se inserisci un nome host, accertati che sia specificato un server DNS in **System > Network > IPv4 and IPv6 (Sistema > Rete > IPv4 e IPv6)**.
  - **Porta**: Immettere il numero di porta utilizzata dal server FTP. Il valore predefinito è 21.
  - **Folder (Cartella)**: inserisci il percorso alla directory nella quale vuoi conservare i file. Se questa directory non esiste già sul server FTP, durante il caricamento dei file riceverai un messaggio di errore.
  - **Username (Nome utente)**: immettere il nome utente per l'accesso.
  - **Password**: immettere la password per l'accesso.
  - **Use temporary file name (Usa nome file temporaneo)**: seleziona questa opzione per il caricamento dei file con nomi file temporanei generati in automatico. Ai file sono assegnati i nomi desiderati quando viene completato il caricamento. Se il caricamento viene annullato/interrotto, non si avrà alcun file corrotto. Tuttavia, probabilmente avrai comunque i file temporanei. In questo modo è possibile sapere che tutti i file con il nome desiderato sono corretti.
  - **Use passive FTP (Usa FTP passivo)**: in circostanze normali il dispositivo richiede semplicemente il server FTP di destinazione per aprire la connessione dati. Il dispositivo inizializza attivamente il comando FTP e le connessioni dati sul server di destinazione. Ciò è necessario generalmente se esiste un firewall tra il dispositivo e il server FTP di destinazione.
- HTTP
  - **URL**: Immettere l'indirizzo di rete sul server HTTP e lo script che gestirà la richiesta. Ad esempio, http://192.168.254.10/cgi-bin/notify.cgi.
  - **Username (Nome utente)**: immettere il nome utente per l'accesso.
  - **Password**: immettere la password per l'accesso.
  - **Proxy**: Attiva e inserisci le informazioni necessarie se si deve superare un server proxy per eseguire la connessione al server HTTP.
- HTTPS
  - **URL**: Immettere l'indirizzo di rete sul server HTTPS e lo script che gestirà la richiesta. Ad esempio, https://192.168.254.10/cgi-bin/notify.cgi.
  - **Validate server certificate (Convalida certificato server)**: Selezionare per convalidare il certificato creato dal server HTTPS.
  - **Username (Nome utente)**: immettere il nome utente per l'accesso.
  - **Password**: immettere la password per l'accesso.
  - **Proxy**: Attiva e inserisci le informazioni necessarie se si deve superare un server proxy per eseguire la connessione al server HTTPS.
- Archiviazione di rete
  Puoi aggiungere dispositivi di archiviazione di rete, ad esempio NAS (Network Attached Storage) e utilizzarli come destinatario per archiviare i file. I file vengono archiviati in formato Matroska (MKV).
  - **Host**: Immettere il nome host o l'indirizzo IP per il dispositivo di archiviazione di rete.
  - **Condivisione**: Immettere il nome della condivisione nell'host.

- **Folder (Cartella)**: inserisci il percorso alla directory nella quale vuoi conservare i file.
- **Username (Nome utente)**: immettere il nome utente per l'accesso.
- **Password**: immettere la password per l'accesso.

- SFTP
  - **Host**: Inserire l'indirizzo IP o il nome host del server. Se inserisci un nome host, accertati che sia specificato un server DNS in **System > Network > IPv4 and IPv6 (Sistema > Rete > IPv4 e IPv6)**.
  - **Porta**: Immettere il numero della porta utilizzata dal server SFTP. Quello predefinito è 22.
  - **Folder (Cartella)**: inserisci il percorso alla directory nella quale vuoi conservare i file. Se questa directory non esiste già sul server SFTP, durante il caricamento dei file riceverai un messaggio di errore.
  - **Username (Nome utente)**: immettere il nome utente per l'accesso.
  - **Password**: immettere la password per l'accesso.
  - **SSH host public key type (MD5) (Tipo di chiave pubblica host SSH (MD5))**: Immetti l'impronta digitale della chiave pubblica dell'host remoto (una stringa di 32 cifre esadecimali). Il client SFTP supporta i server SFTP mediante SSH-2 con tipi di chiavi host RSA, DSA, ECDSA e ED25519. RSA è il metodo preferito durante la negoziazione, seguito da ECDSA, ED25519 e DSA. Assicurarsi di inserire la chiave host MD5 esatta utilizzata dal server SFTP. Benché il dispositivo Axis supporti chiavi hash sia MD5 sia SHA-256, consigliamo l'uso di SHA-256 per una maggiore sicurezza rispetto a MD5. Per maggiori informazioni su come si configura un server SFTP con un dispositivo Axis, vai sul *Portale AXIS OS*.
  - **SSH host public key type (SHA256) (Tipo di chiave pubblica host SSH (SHA256))**: Immetti l'impronta digitale della chiave pubblica dell'host remoto (una stringa di 43 cifre con codifica Base64). Il client SFTP supporta i server SFTP mediante SSH-2 con tipi di chiavi host RSA, DSA, ECDSA e ED25519. RSA è il metodo preferito durante la negoziazione, seguito da ECDSA, ED25519 e DSA. Assicurarsi di inserire la chiave host MD5 esatta utilizzata dal server SFTP. Benché il dispositivo Axis supporti chiavi hash sia MD5 sia SHA-256, consigliamo l'uso di SHA-256 per una maggiore sicurezza rispetto a MD5. Per maggiori informazioni su come si configura un server SFTP con un dispositivo Axis, vai sul *Portale AXIS OS*.
  - **Use temporary file name (Usa nome file temporaneo)**: seleziona questa opzione per il caricamento dei file con nomi file temporanei generati in automatico. Ai file sono assegnati i nomi desiderati quando viene completato il caricamento. Se il caricamento viene annullato o interrotto, non si avrà alcun file corrotto. Tuttavia, probabilmente avrai comunque i file temporanei. In questo modo è possibile sapere che tutti i file con il nome desiderato sono corretti.

- SIP o VMS :
  **SIP**: selezionare per eseguire una chiamata SIP.
  **VMS**: selezionare per eseguire una chiamata VMS.
  - **From SIP account (Dall'account SIP)**: Selezionare dall'elenco.
  - **To SIP address (All'indirizzo SIP)**: Immetti l'indirizzo SIP.
  - **Test (Verifica)**: fare clic per verificare che le impostazioni di chiamata funzionino.
- E-mail
  - **Send email to (Invia e-mail a)**: Inserire l'indirizzo e-mail a cui inviare i messaggi e-mail. Per immettere più indirizzi, separarli utilizzando le virgole.
  - **Send email from (Invia e-mail da)**: immettere l'indirizzo e-mail del server mittente.
  - **Username (Nome utente)**: Immettere il nome utente per il server mail. Lasciare vuoto questo campo se il server mail non necessita di autenticazione.
  - **Password**: Immettere la password per il server mail. Lasciare vuoto questo campo se il server mail non necessita di autenticazione.

- **Email server (SMTP) – Server e-mail (SMTP)**: inserire il nome del server SMTP, ad esempio, smtp.gmail.com, smtp.mail.yahoo.com.
- **Porta**: immettere il numero della porta per il server SMTP, utilizzando i valori nell'intervallo da 0 a 65535. Il valore predefinito è 587.
- **Crittografia**: Per usare la crittografia, seleziona SSL o TLS.
- **Validate server certificate (Convalida certificato server)**: Se usi la crittografia, seleziona questa opzione per convalidare l'identità del dispositivo. Il certificato può essere autofirmato o emesso da un'autorità di certificazione (CA).
- **POP authentication (Autenticazione POP)**: Attiva per inserire il nome del server POP, ad esempio pop.gmail.com.

Nota

alcuni provider di e-mail dispongono di filtri di sicurezza che impediscono agli utenti di ricevere o visualizzare grandi quantità di allegati, ricevere e-mail pianificate e simili. Controllare i criteri di sicurezza del provider e-mail per evitare che l'account e-mail venga bloccato o perda i messaggi e-mail attendibili.

- **TCP**
  - **Host**: Inserire l'indirizzo IP o il nome host del server. Se inserisci un nome host, accertati che sia specificato un server DNS in **System > Network > IPv4 and IPv6 (Sistema > Rete > IPv4 e IPv6)**.
  - **Port (Porta)**: Immettere il numero della porta utilizzata per l'accesso al server.

**Test (Verifica)**: Fare clic per testare l'impostazione.

⋮ Il menu contestuale contiene:

**View recipient (Visualizza destinatario)**: fare clic per visualizzare tutti i dettagli del destinatario.

**Copy recipient (Copia destinatario)**: Fare clic per copiare un destinatario. Quando copi, puoi modificare il nuovo destinatario.

**Delete recipient (Elimina destinatario)**: Fare clic per l'eliminazione permanente del destinatario.

### Pianificazioni

Le pianificazioni e gli impulsi possono essere utilizzati come condizioni nelle regole. Nell'elenco vengono mostrati le pianificazioni e gli impulsi configurati al momento nel dispositivo, insieme alle varie informazioni sulla relativa configurazione.

+ **Add schedule (Aggiungi pianificazione)**: Fare clic per la creazione di una pianificazione o un impulso.

### Trigger manuali

È possibile utilizzare l'attivazione manuale per attivare manualmente una regola. L'attivazione manuale può, ad esempio, essere per convalidare le azioni durante l'installazione e la configurazione del dispositivo.

## MQTT

MQTT (Message Queuing Telemetry Transport) è un protocollo di messaggistica standard per l'Internet of Things (IoT). È stato progettato per un'integrazione IoT semplificata ed è utilizzato in numerosi settori per connettere dispositivi remoti con un'impronta di codice ridotta e una larghezza di banda minima in rete. Il client MQTT nel software del dispositivo Axis può semplificare l'integrazione di dati ed eventi prodotti nel dispositivo con sistemi che non sono software per la gestione video (VMS).

Configurare il dispositivo come client MQTT. La comunicazione MQTT si basa su due entità, i client e il broker. I client possono inviare e ricevere messaggi. Il broker è responsabile del routing dei messaggi tra i client.

Per maggiori informazioni relative a MQTT consultare l'*AXIS OS Knowledge base*.

### ALPN (RETE ALPN)

ALPN è un'estensione TLS/SSL che consente la selezione di un protocollo applicativo durante la fase di handshake della connessione tra client e server. Viene utilizzato per abilitare il traffico MQTT sulla stessa porta utilizzata per altri protocolli, ad esempio HTTP. In alcuni casi, potrebbe non esserci una porta dedicata aperta per la comunicazione MQTT. Una soluzione in tali casi consiste nell'utilizzare ALPN per trattare l'uso di MQTT come protocollo applicativo su una porta standard, consentito dai firewall.

### Client MQTT

**Connect (Connetti)**: Attivare o disattivare il client MQTT.

**Status (Stato)**: Visualizza lo stato corrente del client MQTT.

**Broker**

**Host**: immettere il nome host o l'indirizzo IP del server MQTT.

**Protocol (Protocollo)**: Selezionare il protocollo da utilizzare.

**Porta**: Immettere il numero di porta.

- 1883 è il valore predefinito per **MQTT over TCP**
- 8883 è il valore predefinito per **MQTT su SSL**
- 80 è il valore predefinito per **MQTT su WebSocket**
- 443 è il valore predefinito per **MQTT su WebSocket Secure**

**ALPN protocol (Protocollo ALPN)**: Inserire il nome del protocollo ALPN fornito dal provider MQTT. Ciò è applicabile solo con MQTT over SSL e MQTT over WebSocket Secure.

**Username (Nome utente)**: inserire il nome utente che il client utilizzerà per accedere al server.

**Password**: immettere una password per il nome utente.

**Client ID (ID client)**: Immettere un ID client. L'identificatore del client viene inviato al server al momento della connessione del client.

**Clean session (Sessione pulita)**: Controlla il comportamento al momento della connessione e della disconnessione. Se selezionate, le informazioni sullo stato vengono ignorate al momento della connessione e della disconnessione.

**HTTP proxy (Proxy HTTP)**: Un URL dotato di una lunghezza non superiore a 255 byte. È possibile lasciare il campo vuoto se non si vuole usare un proxy HTTP.

**HTTPS proxy (Proxy HTTPS)**: Un URL dotato di una lunghezza non superiore a 255 byte. È possibile lasciare il campo vuoto se non si vuole usare un proxy HTTPS.

**Keep alive interval (Intervallo keep alive)**: Consente al client di rilevare quando il server non è più disponibile senza dover attendere il lungo tempo di timeout TCP/IP.

**Timeout**: L'intervallo di tempo in secondi per consentire il completamento di una connessione. Valore predefinito: 60

**Device topic prefix (Prefisso argomento dispositivo)**: utilizzato nei valori predefiniti per l'argomento nel messaggio di connessione e nel messaggio Ultime volontà e testamento nella scheda **MQTT client (Client MQTT)** e nelle condizioni di pubblicazione nella scheda **MQTT publication (Pubblicazione MQTT)**.

**Reconnect automatically (Riconnetti automaticamente)**: specifica se il client deve riconnettersi automaticamente dopo una disconnessione.

**Messaggio connessione**

Specifica se un messaggio deve essere inviato quando viene stabilita una connessione.

**Send message (Invia messaggio)**: Attivare per inviare messaggi.

**Use default (Usa predefinito)**: Disattivare per immettere un messaggio predefinito.

**Topic (Argomento)**: Immettere l'argomento per il messaggio predefinito.

**Payload**: Immettere il contenuto per il messaggio predefinito.

**Retain (Conserva)**: Selezionare questa opzione per mantenere lo stato del client su questo **Topic (Argomento)**

**QoS**: Cambiare il livello QoS per il flusso di pacchetti.

**Messaggio di ultime volontà e testamento**

Ultime volontà e testamento consente a un client di fornire un testamento insieme alle proprie credenziali quando si collega al broker. Se il client si disconnette in modo anomalo in un secondo momento (forse perché la sua sorgente di alimentazione non funziona), può lasciare che il broker recapiti un messaggio ad altri client. Questo messaggio Ultime volontà e testamento ha lo stesso formato di un messaggio ordinario e viene instradato tramite la stessa meccanica.

**Send message (Invia messaggio)**: Attivare per inviare messaggi.

**Use default (Usa predefinito)**: Disattivare per immettere un messaggio predefinito.

**Topic (Argomento)**: Immettere l'argomento per il messaggio predefinito.

**Payload**: Immettere il contenuto per il messaggio predefinito.

**Retain (Conserva)**: Selezionare questa opzione per mantenere lo stato del client su questo **Topic (Argomento)**

**QoS**: Cambiare il livello QoS per il flusso di pacchetti.

**Pubblicazione MQTT**

**Use default topic prefix (Usa prefisso di argomento predefinito)**: Selezionare questa opzione per usare il prefisso dell'argomento predefinito, definito nel prefisso argomento dispositivo nella scheda **MQTT client (Client MQTT)**.

**Include topic name (Includi nome argomento)**: selezionare questa opzione per l'inclusione dell'argomento che illustra la condizione nell'argomento MQTT.

**Include topic namespaces (Includi spazi dei nomi degli argomenti)**: Selezionare questa opzione per includere gli spazi dei nomi degli argomenti di ONVIF nell'argomento MQTT.

**Include serial number (Includi numero di serie)**: selezionare questa opzione per comprendere il numero di serie del dispositivo nel payload MQTT.

**Add condition (Aggiungi condizione)**: fare clic sull'opzione per aggiungere una condizione.

**Retain (Conserva)**: definire quali messaggi MQTT sono inviati come conservati.

- **None (Nessuno)**: inviare tutti i messaggi come non conservati.
- **Property (Proprietà)**: inviare solo messaggi con stato conservati.
- **All (Tutto)**: Invia messaggi sia con che senza stato come conservati.

**QoS**: Seleziona il livello desiderato per la pubblicazione MQTT.

**Sottoscrizioni MQTT**

**Add subscription (Aggiungi sottoscrizione)**: Fai clic per aggiungere una nuova sottoscrizione MQTT.

**Subscription filter (Filtro sottoscrizione)**: Inserisci l'argomento MQTT per il quale desideri eseguire la sottoscrizione.

**Use device topic prefix (Usa prefisso argomento dispositivo)**: Aggiungi il filtro sottoscrizione come prefisso all'argomento MQTT.

**Subscription type (Tipo di sottoscrizione)**:

- **Stateless (Privo di stato)**: Seleziona per convertire i messaggi MQTT in messaggi senza stato.
- **Stateful (Dotato di stato)**: Seleziona per convertire i messaggi MQTT in una condizione. Il payload è usato come stato.

**QoS**: Seleziona il livello desiderato per la sottoscrizione MQTT.

## Archiviazione

### Archiviazione integrata

Importante

Rischio di perdita di dati e danneggiamento delle registrazioni. Non rimuovere la scheda di memoria mentre il dispositivo è in funzione. Prima di rimuovere la scheda SD, smontala.

**Unmount (Smonta)**: fare clic su questa opzione per eseguire la rimozione sicura della scheda di memoria.

**Write protect (Proteggi da scrittura)**: attivare questa opzione per interrompere la scrittura nella scheda di memoria e proteggere le registrazioni dalla rimozione. Una scheda di memoria protetta da scrittura non può essere formattata.

**Autoformat (Formattazione automatica)**: Attiva per la formattazione automatica di una scheda di memoria appena inserita. Formatta il file system in ext4.

**Ignore (Ignora)**: attiva questa opzione per non archiviare più le registrazioni sulla scheda di memoria. Il dispositivo non riconosce più che la scheda di memoria esiste se la ignori. Solo gli amministratori hanno a disposizione questa impostazione.

**Retention time (Tempo di conservazione)**: Selezionare il periodo di conservazione delle registrazioni in modo da limitare il numero di registrazioni vecchie o rispettare le normative in merito alla conservazione dei dati. Quando la scheda di memoria è piena, elimina le registrazioni vecchie prima che sia trascorso il tempo di conservazione.

**Strumenti**

- **Check (Controlla)**: Verificare la presenza di eventuali errori nella scheda di memoria.
- **Repair (Ripara)**: corregge gli errori nel file system.
- **Format (Formatta)**: formatta la scheda di memoria per modificare il file system e cancellare tutti i dati. È possibile formattare la scheda di memoria solo con il file system ext4. Per accedere al file system da Windows®, occorre un'applicazione o un driver ext4 di terze parti.
- **Encrypt (Codifica)**: Utilizza questo strumento per la formattazione della scheda di memoria e l'abilitazione della crittografia. Elimina tutti i dati archiviati sulla scheda di memoria. Tutti i nuovi dati memorizzati sulla scheda di memoria saranno crittografati.
- **Decrypt (Decodifica)**: Usa questo strumento per la formattazione della scheda di memoria senza crittografia. Elimina tutti i dati archiviati sulla scheda di memoria. Tutti i nuovi dati memorizzati sulla scheda di memoria non saranno crittografati.
- **Change password (Cambia password)**: modifica la password che serve per la crittografia della scheda di memoria.

**Use tool (Utilizza strumento)**: Fare clic per attivare lo strumento selezionato.

**Wear trigger (Trigger usura)**: Imposta un valore per il livello di usura della scheda di memoria in corrispondenza del quale desideri che sia attivata un'azione. Il livello di usura spazia da 0 a 200%. Una nuova scheda di memoria mai usata è dotata di un livello di usura pari allo 0%. Un livello di usura pari al 100% indica che la scheda di memoria è vicina alla fine del suo ciclo di vita previsto. Quando il livello di usura raggiunge il 200%, sussiste un rischio elevato di malfunzionamento della scheda di memoria. Consigliamo l'impostazione dell'intervallo del trigger di usura tra 80% e 90%. Così avrai il tempo di scaricare tutte le registrazioni e sostituire la scheda di memoria prima che si usuri del tutto. Il trigger di usura permette di impostare un evento e ricevere una notifica quando il livello di usura raggiunge il valore che hai impostato.

## ONVIF

### Account ONVIF

ONVIF (Open Network Video Interface Forum) è uno standard di interfaccia globale che rende più semplice a utenti finali, integratori, consulenti e produttori di avvalersi delle possibilità offerte dalla tecnologia video di rete. ONVIF consente interoperabilità tra dispositivi di fornitori differenti, massima flessibilità, costi ridotti e sistemi a prova di futuro.

Quando si crea un account ONVIF, la comunicazione ONVIF è abilitata automaticamente. Utilizzare il nome account e la password per tutte le comunicazioni ONVIF con il dispositivo. Per ulteriori informazioni, visitare l'Axis Developer Community sul sito Web *axis.com*.

**Add accounts (Aggiungi account)**: Per creare un nuovo account ONVIF.

**Account**: Inserire un nome account univoco.

**New password (Nuova password)**: inserire una password per l'account. La lunghezza delle password deve essere compresa tra 1 e 64 caratteri. La password può contenere solo caratteri ASCII stampabili (codice da 32 a 126), quali lettere, numeri, segni di punteggiatura e alcuni simboli.

**Repeat password (Ripeti password)**: Immettere di nuovo la stessa password.

**Role (Ruolo)**:

- **Administrator (Amministratore)**: ha accesso completo a tutte le impostazioni. Gli amministratori possono anche aggiungere, aggiornare e rimuovere altri account.
- **Operator (Operatore)**: ha accesso a tutte le impostazioni ad eccezione di:
  - Tutte le impostazioni **System (Sistema)**.
  - L'aggiunta di app.
- **Media account (Account multimediale)**: Permette di accedere solo al flusso video.

Il menu contestuale contiene:

**Update account (Aggiorna account)**: Modifica le proprietà dell'account.

**Delete account (Elimina account)**: Elimina l'account. Non puoi cancellare l'account root.

## Registri

### Report e registri

**Report**

- **View the device server report (Visualizza il report del server del dispositivo)**: Visualizzare informazioni sullo stato del dispositivo in una finestra pop-up. Il registro degli accessi viene automaticamente incluso nel report del server.
- **Download the device server report (Scarica il report del server del dispositivo)**: Crea un file .zip che contiene un file di testo del report del server completo in formato UTF-8 e un'istantanea dell'immagine corrente della visualizzazione in diretta. Includere sempre il file .zip del report del server quando si contatta l'assistenza.
- **Download the crash report (Scarica il report dell'arresto anomalo)**: Scaricare un archivio con le informazioni dettagliate sullo stato del server. Il report di arresto anomalo contiene le informazioni presenti nel report del server e le informazioni dettagliate sul debug. Questo report potrebbe contenere informazioni riservate, ad esempio l'analisi della rete. Possono volerci alcuni minuti per generare il report.

**Registri**

- **View the system log (Visualizza il registro di sistema)**: Fare clic per visualizzare le informazioni sugli eventi di sistema come l'avvio del dispositivo, gli avvisi e i messaggi critici.
- **View the access log (Visualizza il registro degli accessi)**: Fare clic per mostrare tutti i tentativi non riusciti di accedere al dispositivo, ad esempio quando si utilizza una password di accesso errata.

### Registro di sistema remoto

Syslog è uno standard per la registrazione dei messaggi. Consente di separare il software che genera messaggi, il sistema che li archivia e il software che li riporta e li analizza. Ogni messaggio è contrassegnato con un codice struttura che indica il tipo di software che genera il messaggio. Inoltre viene assegnato un livello di gravità a tutti i messaggi.

**Server**: Fare clic per aggiungere un nuovo server.

**Host**: immettere il nome host o l'indirizzo IP del server proxy.

**Format (Formatta)**: selezionare il formato del messaggio syslog da utilizzare.

- Axis
- RFC 3164
- RFC 5424

**Protocol (Protocollo)**: Selezionare il protocollo da utilizzare:

- UDP (la porta predefinita è 514)
- TCP (la porta predefinita è 601)
- TLS (la porta predefinita è 6514)

**Porta**: Cambiare il numero di porta per impiegare una porta diversa.

**Severity (Gravità)**: Seleziona quali messaggi inviare al momento dell'attivazione.

**CA certificate set (Certificato CA impostato)**: Visualizza le impostazioni correnti o aggiungi un certificato.

### Configurazione normale

La configurazione normale è per utenti avanzati con esperienza nella configurazione di dispositivi Axis. La maggior parte dei parametri può essere impostata e modificata da questa pagina.

# Manutenzione

## Manutenzione

**Restart (Riavvia)**: Riavviare il dispositivo. Non avrà effetti su nessuna delle impostazioni correnti. Le applicazioni in esecuzione verranno riavviate automaticamente.

**Restore (Ripristina)**: Riporta la maggior parte delle impostazioni ai valori predefiniti di fabbrica. In seguito dovrai riconfigurare il dispositivo e le app, reinstallare tutte le app non preinstallate e ricreare eventuali eventi e preset.

Importante

Dopo il ripristino, le uniche impostazioni salvate sono:

- Protocollo di avvio (DHCP o statico)
- Indirizzo IP statico
- Router predefinito
- Subnet mask
- Impostazioni 802.1X
- Impostazioni O3C
- Indirizzo IP server DNS

**Factory default (Valori predefiniti di fabbrica)**: Riporta tutte le impostazioni ai valori predefiniti di fabbrica. Dopo, per rendere accessibile il dispositivo, devi reimpostare l'indirizzo IP.

Nota

Tutti i software per dispositivi Axis sono firmati digitalmente per assicurare di installare solo software verificato sul dispositivo. Ciò aumenta ulteriormente il livello di sicurezza informatica minimo globale dei dispositivi Axis. Per ulteriori informazioni, visitare il white paper "Axis Edge Vault" su *axis.com*.

**AXIS OS upgrade (Aggiornamento di AXIS OS)**: Aggiorna a una versione nuova di AXIS OS. nuove versioni possono contenere funzionalità migliorate, correzioni di bug e funzionalità completamente nuove. Si consiglia di utilizzare sempre l'ultima versione di AXIS OS. Per scaricare l'ultima versione, andare a *axis.com/support*.

Quando conduci l'aggiornamento, puoi scegliere fra tre opzioni:

- **Standard upgrade (Aggiornamento standard)**: Aggiorna a una nuova versione di AXIS OS.
- **Factory default (Valori predefiniti di fabbrica)**: Aggiorna e riporta tutte le impostazioni ai valori predefiniti di fabbrica. Se selezioni questa opzione, dopo l'aggiornamento non puoi eseguire il ripristino della versione precedente di AXIS OS.
- **Autorollback (Rollback automatico)**: Aggiorna e conferma l'aggiornamento entro il tempo impostato. Se non dai la conferma, il dispositivo tornerà alla precedente versione di AXIS OS.

**AXIS OS rollback (Rollback AXIS OS)**: Eseguire il ripristino alla versione di AXIS OS installata precedentemente.

## Risoluzione di problemi

**Reset PTR (Reimposta PTR)** : reimpostare PTR se per qualche motivo le impostazioni di **Pan (Panoramica)**, **Tilt (Inclinazione)**, o **Roll (Rotazione)** non funzionano come desiderato. I motori PTR sono sempre calibrati in una nuova telecamera. Tuttavia, la calibrazione può essere persa, ad esempio, se la telecamera perde alimentazione o se i motori vengono spostati manualmente. Quando si reimposta il PTR, la telecamera viene calibrata nuovamente e torna al valore predefinito di fabbrica.

**Calibration (Calibrazione)** : Fare clic su **Calibrate (Calibra)** per ricalibrare i motori di panoramica, inclinazione e rotazione nelle rispettive posizioni predefinite.

**Ping**: Per verificare se il dispositivo è in grado di raggiungere un indirizzo specifico, inserire il nome host o l'indirizzo IP dell'host su cui si desidera eseguire un ping e fare clic su **Start (Avvia)**.

**Controllo porta**: Per verificare la connettività dal dispositivo a un indirizzo IP e a una porta TCP/UDP specifici, immettere il nome host o l'indirizzo IP e il numero di porta da controllare e fare clic su **Start (Avvia)**.

**Analisi della rete**

Importante

È possibile che un file di analisi della rete contenga informazioni riservate, come certificati o password.

Un file di analisi della rete può facilitare la risoluzione dei problemi registrando l'attività sulla rete.

**Trace time (Tempo di analisi)**: Selezionare la durata dell'analisi in secondi o minuti e fare clic su **Download**.

# Per saperne di più

## Streaming e archiviazione

### Formati di compressione video

La scelta del metodo di compressione da utilizzare in base ai requisiti di visualizzazione e dalle proprietà della rete. Le opzioni disponibili sono:

**H.264 o MPEG-4 Parte 10/AVC**

Nota

H.264 è una tecnologia con licenza. Il dispositivo Axis include una licenza client per la visualizzazione H.264. L'installazione di copie aggiuntive senza licenza del client non è consentita. Per acquistare altre licenze, contattare il rivenditore Axis.

H.264 può, senza compromettere la qualità di immagine, ridurre le dimensioni di un file video digitale di più dell'80% rispetto al formato Motion JPEG e del 50% rispetto ai formati MPEG precedenti. Ciò significa che per un file video sono necessari meno larghezza di banda di rete e di spazio di archiviazione. In altre parole, è possibile ottenere una qualità video superiore per una determinata velocità in bit.

**H.265 o MPEG-H Parte 2/HEVC**

H.265 può, senza compromettere la qualità di immagine, ridurre le dimensioni di un file video digitale di più del 25% rispetto a H.264.

Nota

- H.265 è una tecnologia con licenza. Il dispositivo Axis include una licenza client per la visualizzazione H.265. L'installazione di copie aggiuntive senza licenza del client non è consentita. Per acquistare altre licenze, contattare il rivenditore Axis.
- La maggioranza dei browser non è dotata di supporto per la decodifica H.265 e per tale ragione l'interfaccia Web della telecamera non la supporta. Invece puoi utilizzare un'applicazione o un sistema di gestione video che supporta la codifica H.265.

### Dispositivo di archiviazione esterno

Perché il decoder video sia riconosciuto, la prima partizione del dispositivo di archiviazione esterno deve impiegare un file system exFAT o ext4.

## Cyber security

Per informazioni specifiche sulla cybersecurity (sicurezza informatica), consultare la scheda tecnica del dispositivo su axis.com.

Per informazioni approfondite sulla cybersecurity in AXIS OS, leggere la guida *AXIS OS Hardening*.

### SO firmato

Il SO firmato viene implementato dal fornitore del software che firma l'immagine di AXIS OS con una chiave privata. Quando la firma è allegata al sistema operativo, il dispositivo convalida il software prima di installarlo. Se il dispositivo rileva che l'integrità del software è compromessa, l'aggiornamento di AXIS OS verrà rifiutato.

### Secure Boot

Secure Boot è un processo di avvio costituito da una catena ininterrotta di software crittograficamente convalidati eseguita da una memoria non modificabile (bootrom). Essendo basato sull'uso del SO firmato, l'avvio sicuro assicura che un dispositivo possa essere avviato solo con software autorizzato.

## Axis Edge Vault

Axis Edge Vault è una piattaforma hardware di cybersecurity che protegge il dispositivo Axis. Offre funzionalità per garantire l'identità e l'integrità del dispositivo e per proteggere le informazioni sensibili da accessi non autorizzati. Si basa su solidi moduli di calcolo crittografico (Secure Element e TPM) e sicurezza del SoC (TEE e Secure Boot), combinati con le competenze di Axis nella sicurezza dei dispositivi edge.

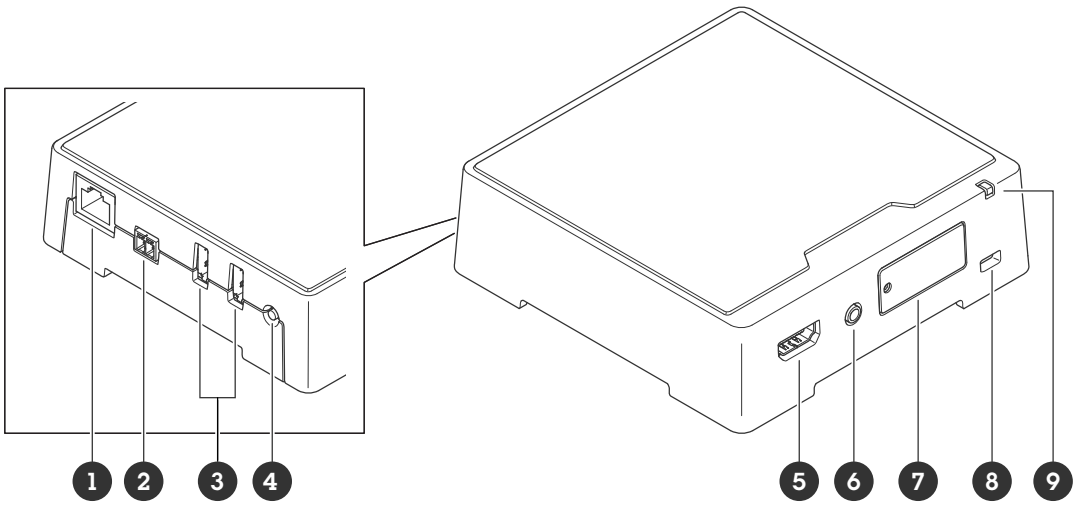
## ID dispositivo Axis

poter verificare l'origine del dispositivo è fondamentale per stabilire che la sua identità è attendibile. Durante la produzione, ai dispositivi con Axis Edge Vault viene assegnato un certificato ID univoco e conforme a IEEE 802.1AR. È come avere un passaporto per dimostrare l'origine del dispositivo. L'ID del dispositivo viene archiviato in modo sicuro e permanente nell'archivio chiavi come certificato firmato dal certificato radice Axis. L'ID del dispositivo può essere sfruttato dall'infrastruttura IT del cliente per l'onboarding sicuro automatizzato di dispositivi e l'identificazione sicura dei dispositivi

Per maggiori informazioni relativamente alle funzioni di cybersecurity nei dispositivi Axis, vai su *axis.com/learning/white-papers* e cerca cybersecurity.

# Dati tecnici

## Panoramica dei prodotti




1 *Connettore di rete PoE*
2 *Connettore di alimentazione*
3 *2 porte USB*
4 *Pulsante di comando*
5 *Connettore HDMI™ tipo A*
6 *Uscita audio*
7 *Slot per scheda MicroSD*
8 *Slot di sicurezza*
9 *LED di stato*

## Indicatori LED

| LED di stato | Significato |
|---|---|
| Giallo | Luce fissa: durante l'avvio o il ripristino delle impostazioni predefinite o della configurazione. |
| Giallo/rosso | Lampeggia durante l'avvio se il collegamento di rete non è disponibile o è stato perso. |
| Verde | Una luce verde fissa per 10 secondi indica il normale funzionamento una volta completato l'avvio.<br><br>Quando il LED si spegne dopo essersi acceso in verde, il dispositivo è in funzione. |
| Verde/Rosso | Lampeggiante a scopo identificativo. |

## Slot per scheda SD

*AVVISO*

- Rischio di danneggiamento della scheda di memoria. Non utilizzare strumenti appuntiti oppure oggetti metallici e non esercitare eccessiva forza durante l'inserimento o la rimozione della scheda di memoria. Utilizzare le dita per inserire e rimuovere la scheda.
- Rischio di perdita di dati e danneggiamento delle registrazioni. Smontare la scheda di memoria dall'interfaccia Web del dispositivo prima di rimuoverla. Non rimuovere la scheda di memoria mentre il dispositivo è in funzione.

Questo dispositivo supporta schede microSD/microSDHC/microSDXC.

Visitare *axis.com* per i consigli sulla scheda di memoria.

I logo microSD, microSDHC e microSDXC sono tutti marchi registrati di SD-3C LLC. microSD, microSDHC, microSDXC sono marchi o marchi registrati di SD-3C, LLC negli Stati Uniti e/o in altri paesi.

## Pulsanti

### Pulsante di comando

Il pulsante di comando viene utilizzato per:

- Ripristino del dispositivo alle impostazioni predefinite di fabbrica. Vedere .
- Connessione a servizio one-click cloud connection (O3C) su Internet. Per il collegamento, tenere premuto il tasto per circa 3 secondi finché il LED di stato non lampeggia in verde.

## Connettori

### Connettore HDMI

Utilizzare il connettore HDMI™ per collegare uno schermo o un monitor dedicato alla visualizzazione pubblica.

### Connettore di rete

Connettore Ethernet RJ45 con Power over Ethernet (PoE).

### Connettore USB

Utilizza il connettore USB per connettere accessori esterni. Consulta la scheda tecnica del dispositivo per conoscere gli accessori supportati.

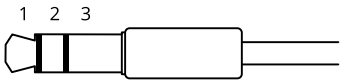
Importante

Si supporta un solo dispositivo di archiviazione USB alla volta.

Spegnere il dispositivo prima di rimuovere il dispositivo di archiviazione USB.

### Connettore audio

- **Uscita audio** - output da 3,5 mm per audio (line level) che è possibile collegare a un sistema di indirizzo pubblico (PA) o a un altoparlante attivo con amplificatore integrato. Per l'uscita audio è necessario utilizzare un connettore stereo.



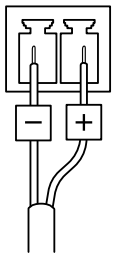

**Output audio**

| 1 Punta | 2 Anello | 3 Guaina |
|---|---|---|
| Canale 1, linea non bilanciata, mono | Canale 1, linea non bilanciata, mono | Terra |

### Connettore di alimentazione

Connettore CA/CC. Utilizzare l'adattatore fornito.

Morsettiera a 2 pin per ingresso alimentazione CC. Utilizzare una sorgente di alimentazione limitata (LPS) compatibile con una bassissima tensione di sicurezza (SELV) con una potenza di uscita nominale limitata a ≤100 W o una corrente nominale di uscita limitata a ≤5 A.



Nota

Quando CC è disponibile, ha la priorità su PoE.

# Risoluzione dei problemi

## Ripristino delle impostazioni predefinite di fabbrica

Importante

Il ripristino dei valori predefiniti di fabbrica deve essere effettuato con cautela. Tale operazione consentirà di ripristinare i valori predefiniti di fabbrica per tutte le impostazioni, incluso l'indirizzo IP.

Per ripristinare il dispositivo alle impostazioni predefinite di fabbrica:

1. Scollegare l'alimentazione dal dispositivo.
2. Tenere premuto il pulsante di comando quando si ricollega l'alimentazione. Vedere .
3. Tenere premuto il pulsante di comando per circa 15-30 secondi fino a quando il LED di stato non lampeggia in giallo.
4. Rilasciare il pulsante di comando. La procedura è terminata quando il LED di stato diventa verde. Se nella rete non è disponibile un server DHCP, l'indirizzo IP del dispositivo sarà predefinito con uno dei seguenti:
   - **Dispositivi con AXIS OS 12.0 e successivo:** Ottenuto dal subnet dell'indirizzo di collegamento locale (169.254.0.0/16)
   - **Dispositivi con AXIS OS 11.11 e precedente:** 192.168.0.90/24
5. Utilizzare gli strumenti per l'installazione e la gestione del software per assegnare un indirizzo IP, impostare la password e accedere al dispositivo.
   Gli strumenti per l'installazione e la gestione del software sono disponibili nelle pagine dedicate all'assistenza sul sito Web *axis.com/support*.

È inoltre possibile reimpostare i parametri ai valori predefiniti di fabbrica mediante l'interfaccia Web del dispositivo. Andare a **Maintenance (Manutenzione)** > **Factory default (Impostazione di fabbrica)** e fare clic su **Default (Predefinito)**.

## Opzioni AXIS OS

Axis offre la gestione del software dei dispositivi in base alla traccia attiva o alle tracce di supporto a lungo termine (LTS). La traccia attiva consente di accedere continuamente a tutte le funzionalità più recenti del dispositivo, mentre le tracce LTS forniscono una piattaforma fissa con versioni periodiche incentrate principalmente sulle correzioni di bug e sugli aggiornamenti della sicurezza.

Si consiglia di utilizzare AXIS OS della traccia attiva se si desidera accedere alle funzionalità più recenti o se si utilizzano le offerte del sistema end-to-end Axis. Le tracce LTS sono consigliate se si utilizzano integrazioni di terze parti che non vengono convalidate continuamente a fronte della traccia attiva più recente. Con il supporto a lungo termine (LTS), i dispositivi possono mantenere la sicurezza informatica senza introdurre modifiche funzionali significative o compromettere eventuali integrazioni presenti. Per informazioni più dettagliate sulla strategia del software del dispositivo AXIS, visitare *axis.com/support/device-software*.

## Controllo della versione corrente del AXIS OS

AXIS OS determina la funzionalità dei nostri dispositivi. Quando ti occupi della risoluzione di problemi, consigliamo di cominciare controllando la versione AXIS OS corrente. L'ultima versione potrebbe contenere una correzione che risolve il tuo particolare problema.

Per controllare la versione corrente di AXIS OS:

1. Andare all'interfaccia Web del dispositivo > **Status (Stato)**.
2. Vedere la versione AXIS OS in **Device info (Informazioni dispositivo)**.

## Aggiornare AXIS OS

Importante

- Le impostazioni preconfigurate e personalizzate vengono salvate quando aggiorni il software del dispositivo (a condizione che le funzioni siano disponibili nel AXIS OS), sebbene ciò non sia garantito da Axis Communications AB.
- Assicurarsi che il dispositivo rimanga collegato alla fonte di alimentazione durante il processo di aggiornamento.

Nota

Quando si aggiorna il dispositivo con la versione più recente di AXIS OS nella traccia attiva, il dispositivo riceve le ultime funzionalità disponibili. Leggere sempre le istruzioni di aggiornamento e le note di rilascio disponibili con ogni nuova versione prima dell'aggiornamento. Per la versione AXIS OS più aggiornata e le note sul rilascio, visitare il sito Web *axis.com/support/device-software*.

1. Scarica il file AXIS OS sul tuo computer, disponibile gratuitamente su *axis.com/support/device-software*.
2. Accedi al dispositivo come amministratore
3. Andare a **Maintenance > AXIS OS upgrade (Manutenzione > Aggiornamento AXIS OS)** e fare clic su **Upgrade (Aggiorna)**.

Al termine dell'operazione, il dispositivo viene riavviato automaticamente.

Puoi usare AXIS Device Manager per l'aggiornamento di più dispositivi allo stesso tempo. Maggiori informazioni sono disponibili sul sito Web *axis.com/products/axis-device-manager*.

## Problemi tecnici, indicazioni e soluzioni

Se non si riesce a trovare qui ciò che si sta cercando, provare ad accedere alla sezione relativa alla risoluzione dei problemi all'indirizzo *axis.com/support*.

| **Problemi durante l'aggiornamento di AXIS OS** | |
|---|---|
| Errore di aggiornamento di AXIS OS | Se l'aggiornamento non riesce, il dispositivo ricarica la versione precedente. Il motivo più comune è il caricamento di un AXIS OS errato. Controllare che il nome del file di AXIS OS corrisponda al dispositivo e riprovare. |
| Problemi dopo l'aggiornamento di AXIS OS | Se si riscontrano problemi dopo l'aggiornamento, ripristinare la versione installata in precedenza dalla pagina **Maintenance (Manutenzione)**. |

| **Problemi durante l'impostazione dell'indirizzo IP** | |
|---|---|
| Il dispositivo si trova su una subnet diversa | Se l'indirizzo IP destinato al dispositivo e l'indirizzo IP del computer utilizzato per accedere al dispositivo si trovano in subnet diverse, non è possibile impostare l'indirizzo IP. Contattare l'amministratore di rete per ottenere un indirizzo IP. |

| | |
|---|---|
| L'indirizzo IP è già utilizzato da un altro dispositivo | Scollegare il dispositivo Axis dalla rete. Eseguire il comando ping (in una finestra di comando/DOS digitare `ping` e l'indirizzo IP del dispositivo):<br>• Se si riceve: `Reply from <IP address> (Risposta dall'indirizzo IP): bytes=32; time=10...` significa che l'indirizzo IP potrebbe già essere utilizzato da un altro dispositivo nella rete. Contattare l'amministratore di rete per un nuovo indirizzo IP e reinstallare il dispositivo.<br>• Se si riceve: `Request timed out` significa che l'indirizzo IP può essere utilizzato con il dispositivo Axis. Controllare tutti i cablaggi e reinstallare il dispositivo. |
| Possibile conflitto dell'indirizzo IP con un altro dispositivo nella stessa subnet | Prima che il server DHCP imposti un indirizzo dinamico viene utilizzato l'indirizzo IP statico del dispositivo Axis. Ciò significa che se lo stesso indirizzo IP statico viene utilizzato anche da un altro dispositivo, si potrebbero verificare dei problemi durante l'accesso al dispositivo. |

### Impossibile accedere al dispositivo da un browser

| | |
|---|---|
| Non è possibile eseguire l'accesso | Quando HTTPS è abilitato, verifica che sia usato il protocollo giusto (HTTP o HTTPS) quando tenti di eseguire l'accesso. Potrebbe essere necessario digitare manualmente `http` o `https` nel campo dell'indirizzo del browser.<br><br>Se si dimentica la password per l'account root, il dispositivo deve essere ripristinato alle impostazioni predefinite di fabbrica. Vedere . |
| L'indirizzo IP è stato modificato dal server DHCP | Gli indirizzi IP ottenuti da un server DHCP sono dinamici e potrebbero cambiare. Se l'indirizzo IP è stato modificato, utilizzare AXIS IP Utility o AXIS Device Manager per individuare il dispositivo sulla rete. Identificare il dispositivo utilizzando il relativo numero di serie o modello oppure il nome DNS (se è stato configurato).<br><br>Se necessario, è possibile assegnare manualmente un indirizzo IP statico. Per istruzioni, vedere *axis.com/support*. |
| Errore del certificato durante l'utilizzo di IEEE 802.1X | Per un corretto funzionamento dell'autenticazione, le impostazioni della data e dell'ora nel dispositivo Axis devono essere sincronizzate con un server NTP. Andare a **System > Date and time (Sistema > Data e ora)**. |

### L'accesso al dispositivo può essere eseguito in locale ma non esternamente

Per accedere al dispositivo esternamente, si consiglia di usare una delle seguenti applicazioni per Windows®:

- AXIS Camera Station Edge: gratuito, ideale per piccoli sistemi con esigenze di sorveglianza di base.
- AXIS Camera Station 5: versione di prova di 30 giorni gratuita, ideale per sistemi di piccole e medie dimensioni.
- AXIS Camera Station Pro: versione di prova di 90 giorni gratuita, ideale per sistemi di piccole e medie dimensioni.

Per istruzioni e download, visitare *axis.com/vms*.

| Impossibile collegarsi tramite la porta 8883 con MQTT su SSL | |
|---|---|
| Il firewall blocca il traffico utilizzando la porta 8883 poiché è insicuri. | In alcuni casi il server/broker potrebbe non fornire una porta specifica per la comunicazione MQTT. Potrebbe essere ancora possibile utilizzare MQTT su una porta normalmente utilizzata per il traffico HTTP/HTTPS.<br>• Se il server/broker supporta WebSocket/WebSocket Secure (WS/WSS), in genere sulla porta 443, utilizzare questo protocollo. Controllare con il provider del server/broker se è supportato WS/WSS e quale porta e base utilizzare.<br>• Se il server/broker supporta ALPN, l'uso di MQTT può essere negoziato su una porta aperta, come la 443. Verificate con il proprio server/broker provider se ALPN è supportato e quale protocollo e porta ALPN utilizzare. |

## Considerazioni sulle prestazioni

- Usare HTTPS potrebbe ridurre la velocità in fotogrammi.
- Un utilizzo eccessivo della rete dovuto a una scarsa infrastruttura influisce sulla larghezza di banda.
- Una mancanza di correlazione tra input e output del flusso video può influire sulle prestazioni del decoder video.

## Contattare l'assistenza

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

T10192361_it

2025-04 (M9.2)