AXIS S3016 Recorder

Manuale dell'utente

Informazioni sul dispositivo

AXIS S3016 Recorder è un videoregistratore di rete con switch PoE integrato e dischi rigidi di classe sorveglianza. Inoltre include una porta USB 3.0 che consente di esportare facilmente le riprese video. Il registratore è disponibile in tre modelli: 8 TB, 16 TB e 32 TB.

Impostazioni preliminari

Accesso al dispositivo

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 Extend. 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™	Edge™	Firefox®	Safari®
Windows®	✓	✓	*	*
macOS®	✓	✓	*	*
Linux®	✓	✓	*	*
Altri sistemi operativi	*	*	*	*

✓: Consigliato

*: Supportato con limitazioni

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 Extend 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

Utilizzare HTTPS (abilitato per impostazione predefinita) per impostare la password o altre configurazioni sensibili in rete. HTTPS consente connessioni di rete sicure e crittografate, proteggendo così i dati sensibili, come le 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

Impostazioni preliminari

Nota

È necessario l'accesso a Internet durante la configurazione del sistema.

1.
2.
3.
4.
5.

Una volta terminata l'installazione:

- Tutti i dispositivi Axis nel sistema dispongono di AXIS OS più recente.
- Tutti i dispositivi hanno una password.
- La registrazione con le impostazioni predefinite è attiva.
- È possibile utilizzare Accesso remoto.

Registrazione di un account MyAxis

1. Registrazione di un account **My Axis** all'indirizzo *axis.com/my-axis/login*.
2. Scegliere uno dei metodi di autenticazione a più fattori (MFA) **Authenticator App (TOTP)** o **Email** e seguire le istruzioni a schermo. L'MFA è un sistema di sicurezza che aggiunge un ulteriore livello di verifica per garantire l'identità dell'utente.

Installazione dell'hardware

1. Installazione dell'hardware della telecamera.
2. Collegare il registratore alla rete tramite la porta LAN.
3. Collegare le telecamere allo switch PoE integrato dei registratori o a uno switch PoE esterno.
4. Collegare il computer alla stessa rete del registratore.
5. Collegare l'alimentatore al registratore.

Importante

È necessario prima collegare il cavo di alimentazione al registratore, quindi collegare il cavo di alimentazione alla presa di alimentazione.

6. Attendere alcuni minuti prima che il registratore e le telecamere si avviino prima di procedere.

⚠ ATTENZIONE

Mantenere il registratore in un ambiente ben ventilato e con un ampio spazio attorno ad esso per evitare il surriscaldamento.

Installare AXIS Camera Station Edge

1. Andare in *axis.com/products/axis-camera-station-edge* e fare clic su **Download (Scarica)**.
2. Aprire il file di impostazione e seguire l'assistente alla configurazione.
3. Accedi con l'*account MyAxis*.

Crea un sito

1. Avviare AXIS Camera Station Edge.
2. Accedi con l'*account MyAxis*.
3. Fare clic su **Create new site (Crea nuovo sito)** e assegnare un nome al sito.
4. Fare clic su **Next (Avanti)**.
5. Selezionare i dispositivi che si desidera aggiungere al sito.
6. Fare clic su **Next (Avanti)**.
7. Selezionare archiviazione.
8. Fare clic su **Next (Avanti)**.
9. Fare clic su **Install (Installa)** e attendi che AXIS Camera Station Edge configuri i dispositivi. La configurazione può durare alcuni minuti.

Una volta terminata l'installazione:

- Tutti i dispositivi Axis nel sistema dispongono di AXIS OS più recente.
- Tutti i dispositivi hanno una password.
- La registrazione con le impostazioni predefinite è attiva.
- È possibile utilizzare Accesso remoto.

Installazione dell'app per dispositivi mobili

Per Android

Fare clic su *Download* o scansiona il seguente codice QR®.

Per iOS

Fare clic su *Download* o scansiona il seguente codice QR.

Apri l'app mobile AXIS Camera Station Edge e effettuare l'accesso con le tue credenziali Axis.

Nel caso tu non abbia un account MyAxis, puoi andare all'indirizzo *axis.com/my-axis* per effettuare la registrazione di un nuovo account.

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

Introduzione a AXIS Camera Station Pro

Aggiungi il tuo registratore

Nota

AXIS Camera Station rimuove registrazioni da qualsiasi sistema precedente quando si aggiunge il registratore a un nuovo sistema.

1. andare a **Configurazione > Dispositivi > Aggiungi dispositivi**.
2. Selezionare il registratore nell'elenco e fare clic su **Add (Aggiungi)**. Se il registratore non è elencato, utilizzare la **ricerca manuale** per trovarlo manualmente.
3. Utilizzare le impostazioni predefinite e fare clic su **Next (Avanti)**.
4. Impostare la password per la crittografia dell'archiviazione. Fare clic su **Next (Avanti)**. Questa password è necessaria per accedere al disco rigido del registratore esterno di AXIS Camera Station o quando il registratore viene reimpostato sulle impostazioni predefinite di fabbrica dall'interfaccia web del dispositivo.

5. Andare su **Configuration > Devices > Other devices (Configurazione > Dispositivi > Altri dispositivi)** e verificare che il registratore sia stato aggiunto.
6. Andare a **Configuration > Storage > Management (Configurazione > Archiviazione > Gestione)** e verificare che il registratore sia stato aggiunto all'elenco di archiviazione.

Aggiungere dispositivi e selezionare il registratore come memoria di registrazione

1. andare a **Configurazione > Dispositivi > Aggiungi dispositivi**.
2. Selezionare i dispositivi nell'elenco e fare clic su **Add (Aggiungi)**. Se i dispositivi non sono elencati, utilizzare la **ricerca manuale** per trovarli manualmente.
3. Utilizzare le impostazioni predefinite e fare clic su **Next (Avanti)**.
4. Selezionare manualmente il registratore dall'elenco a discesa **Recording storage (Archiviazione registrazione)** e fare clic su **Install (Installa)**.

Nota

Il registratore non verrà selezionato come archiviazione della registrazione se si seleziona **Automatic (Automatico)**.

5. Andare a **Configurazione > Archiviazione > Selezione**. Fare clic sui dispositivi e verificare che la memoria di registrazione sia il registratore.

Configura registrazioni

1. Andare su **Configuration > Storage > Selection (Configurazione > Archiviazione > Selezione** e selezionare il dispositivo.
2. Configurare **Retention time (Tempo di conservazione)**.
   - Selezionare **Unlimited (Illimitato)** per il tempo di conservazione per mantenere le registrazioni fino ad esaurimento dello spazio sul dispositivo di archiviazione.
   - Selezionare **Limited (Limitato)** e impostare il numero massimo di giorni di conservazione delle registrazioni.
3. fare clic su **Applica**;

Nota

La registrazione di fallback è abilitata per impostazione predefinita per memorizzare le registrazioni sul registratore quando la connessione tra AXIS Camera Station e il registratore viene persa. Vedere *Registrazione di fallback*.

Configurare il dispositivo

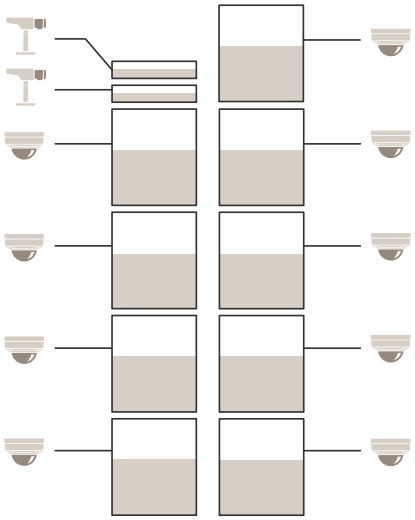
Allocazione dell'alimentazione

Il registratore riserva una certa quantità di energia per ogni porta. L'alimentazione riservata totale non può superare il power budget totale. Una porta non verrà alimentata se il registratore cerca di riservare più alimentazione di quanta ne sia disponibile. Questo assicura che tutti i dispositivi collegati vengano alimentati.

Esempio:
In questo esempio:

- AXIS S3016 Recorder ha un power budget totale di 305 W.
- Dispositivo PoE classe 3. Richiede 15,5 W di alimentazione ma in realtà consuma 7,5 W di alimentazione.
- Dispositivo PoE classe 4. Richiede 30 W di alimentazione ma in realtà consuma 15 W di alimentazione.
- Alimentazione riservata.
- Consumo energetico effettivo:

Alimentazione riservata



Consumo energetico effettivo

- Ogni porta riserva la quantità di alimentazione in base alla classe PoE del dispositivo.
- Il registratore può alimentare 9 dispositivi PoE di classe 4 e 2 dispositivi PoE di classe 3.
- L'alimentazione riservata totale è (9 x 30) + (2 x 15.5) =301 W.
- L'alimentazione effettiva consumata è (9 x 15) + (2 x 7.5) = 150 W.

Modifica del livello RAID

⚠ ATTENZIONE

La modifica del livello RAID riformatta il file system ed elimina tutti i dati dai dischi.

1. Nell'interfaccia web del dispositivo, andare a **System > Storage (Sistema > Archiviazione)**.
2. In **Tools (Strumenti)**, selezionare **Change RAID level (Modifica livello RAID)** e fare clic su **Use tool (Utilizza strumenti)**.
3. Selezionare un livello RAID e fare clic su **Next (Avanti)**.

4. Selezionare **Encrypt the disk (Crittografare il disco)** e digitare la tua password. Fare clic su **Next (Avanti)**.
5. Fare clic su **Sì**.
6. Il messaggio di stato viene visualizzato nell'angolo in alto a destra. Attendere finché l'operazione non viene completata e non compare `RAID configured` prima di chiudere la pagina.

Sostituzione di un disco rigido

Nota

Per evitare scariche elettrostatiche, si consiglia di utilizzare sempre un tappetino statico e un cinturino statico mentre si lavora su componenti all'interno del sistema.

1. Allentare le viti a sinistra e a destra della cornice e rimuovere la cornice.
2. Individuare il disco rigido rotto indicato da un LED rosso.
   Tutti i LED sono rossi in caso di guasto RAID. Per identificare il disco rigido rotto, accedere all'interfaccia web del dispositivo e selezionare **System > Storage > Hard drive status (Sistema > Archiviazione > Stato disco rigido)**.
3. Allentare la vite della slitta del disco rigido (T10).
4. Estrarre la slitta del disco rigido dall'alloggiamento del disco rigido.
5. Allentare le quattro viti del disco rigido (T8).
6. Estrarre il disco rigido dalla slitta del disco rigido.
7. Inserire un nuovo disco rigido nella slitta del disco rigido.
8. Fissare le quattro viti per il disco rigido.
9. Inserire e spingere la slitta del disco rigido fino in fondo nell'alloggiamento del disco rigido.
10. Fissare la vite per la slitta del disco rigido. Attendere che il LED diventi verde.
11. Collegare la cornice e serrare le viti a sinistra e a destra della cornice.

Crea un nuovo RAID

⚠ ATTENZIONE

Crea un nuovo RAID solo in caso di guasto del RAID. La creazione di un nuovo RAID elimina tutti i dati dai dischi rigidi.

1. Sostituisci i dischi rigidi rotti. Vedere .
2. Configurare il RAID. Vedere .
3. Configurare le registrazioni nel tuo sistema di gestione video. Vedere e .

Hard reset di un registratore

Importante

Sposta il registratore attentamente quando è acceso. Mosse improvvise o urti potrebbero danneggiare il disco rigido.

Nota

- Un hard reset ripristinerà tutte le impostazioni, compreso l'indirizzo IP.
- Un hard reset non rimuoverà le registrazioni.

1. Spegnere il registratore:
   Premere il pulsante dell'alimentazione nella parte anteriore del registratore per 4-5 secondi fino a quando viene emesso un segnale acustico.
2. Attendere che il registratore sia spento, quindi girarlo per accedere al pulsante di comando.

3. Tenere premuto il pulsante di comando. Premere e rilasciare il pulsante di alimentazione per avviare il registratore. Rilasciare il pulsante di comando dopo 15 - 30 secondi quando l'indicatore LED lampeggerà in giallo.
4. Riposiziona attentamente il registratore.
5. La procedura è terminata quando il LED di stato diventa verde. Il dispositivo è stato reimpostato alle impostazioni di fabbrica predefinite. 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
6. Se il disco rigido è crittografato, deve essere montato manualmente dopo il ripristino del registratore:
   6.1. Andare all'interfaccia Web del dispositivo.
   6.2. Andare a **System (Sistema)** > **Storage (Archiviazione)** e fare clic su **Mount (Monta)**.
   6.3. Inserire la password di crittografia utilizzata durante la crittografia del disco rigido.

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.

Porte di rete

Mostra lo stato delle porte di rete e le informazioni sull'alimentazione, inclusa l'alimentazione allocata e il consumo PoE totale.

Network ports settings (Impostazioni porte di rete): Fare clic per andare sulla pagina Porte di rete, dove è possibile modificare le impostazioni.

Archiviazione

Mostra lo stato di archiviazione e le informazioni tra cui lo spazio libero e la temperatura del disco.

Storage settings (Impostazioni di archiviazione): Fare clic per andare sulla pagina Archiviazione integrata, dove è possibile modificare le impostazioni.

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.

Registrazioni in corso

Mostra le registrazioni in corso e il relativo spazio di archiviazione designato.

Registrazioni: Consente di visualizzare le registrazioni in corso e quelle filtrate oltre alla relativa origine. Per ulteriori informazioni, vedere

Mostra lo spazio di archiviazione in cui è stata salvata la registrazione.

Registrazioni

Riproduci la registrazione.

Interrompi la riproduzione della registrazione.

Mostra o nascondi le informazioni e le opzioni sulla registrazione.

Set export range (Impostare l'intervallo di esportazione): Se vuoi esportare solo parte della registrazione, indica un intervallo di tempo.

Encrypt (Codifica): selezionare per impostare una password per le registrazioni esportate. Non è possibile aprire il file esportato senza la password.

Fare clic per eliminare una registrazione.

Export (Esporta): esporta l'intera registrazione o una sua parte.

Fare clic per filtrare le registrazioni.

From (Da): Mostra le registrazioni avvenute dopo un certo punto temporale.

To (A): Mostra le registrazioni fino a un certo punto temporale.

Source (Sorgente): mostra le registrazioni sulla base della sorgente. La sorgente si riferisce al sensore.

Event (Evento): mostra le registrazioni sulla base degli eventi.

Dispositivo di archiviazione: mostra le registrazioni in base al tipo di dispositivo di archiviazione.

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 (PTP)** (Data e ora automatizzate (PTP)): sincronizzazione tramite il protocollo di precisione temporale.
- **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.
  - **Trusted NTS KE CA certificates (Certificati NTS KE CA attendibili)**: Selezionare i certificati CA attendibili da utilizzare per la sincronizzazione temporale sicura NTS KE oppure lasciare il campo vuoto.
  - **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 IPv4 automatico (DHCP) per consentire alla rete di assegnare automaticamente l'indirizzo IP, la subnet mask e il router, senza necessità di configurazione manuale. Si consiglia l'uso dell'assegnazione IP automatica (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.

Nota

Se il DHCP è disabilitato, le funzionalità che dipendono dalla configurazione automatica della rete, quali nome host, server DNS, NTP e altre, potrebbero smettere di funzionare.

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.

Porte di rete

Alimentazione e Ethernet: Selezionare questa opzione per attivare la rete per la porta dello switch.

Power only (Solo alimentazione): Selezionare questa opzione per disattivare la rete per la porta dello switch. La porta continua a fornire alimentazione tramite Ethernet.

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'opzione predefinita. Per connettersi a O3C, premere il pulsante di comando sul dispositivo. A seconda del modello di dispositivo, premere e rilasciare oppure tenere premuto, finché il LED di stato non lampeggia. Registrare il dispositivo con il servizio O3C entro 24 ore per abilitare **Always** (Sempre) e rimanere connessi. Se non si effettua la registrazione, il dispositivo si disconnette da O3C.
- **Sempre**: Il dispositivo tenta continuamente di collegarsi a un servizio O3C via Internet. Una volta registrato il dispositivo, questo rimane connesso. Utilizzare questa opzione se il pulsante di comando non è disponibile.
- **No**: disconnette dal 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.
    - **Link up**: invia un messaggio trap quando un collegamento cambia dal basso verso l'alto.
    - **Link down (Collegamento in basso)**: invia un messaggio trap quando un collegamento passa dall'alto al basso.
    - **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.
  - **Privacy**: Selezionare la crittografia da utilizzare per proteggere i dati SNMP.
  - **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/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+, FIPS 140-3 Livello 3) (Elemento sicuro)** : Selezionare questa opzione per utilizzare un elemento sicuro per il keystore sicuro.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Livello 2)** : Selezionare questa opzione per utilizzare TPM 2.0 per il keystore sicuro.

Policy crittografica

La policy crittografica definisce il modo in cui viene utilizzata la crittografia per proteggere i dati.

Active (Attivo): Selezionare la policy crittografica da applicare al dispositivo:

- **Default (Predefinita) - OpenSSL**: sicurezza e prestazioni equilibrate per un uso generico.
- **FIPS - Policy to comply with FIPS 140-2 (FIPS - Policy conforme a FIPS 140-2)**: crittografia conforme a FIPS 140-2 per i settori industriali regolamentati.

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.

Firewall

Firewall: Attivare per abilitare il firewall.

Default Policy (Criterio predefinito): Selezionare come si desidera che il firewall gestisca le richieste di connessione non coperte da regole.

- **ACCEPT:** (ACCETTA) Permette tutte le connessioni al dispositivo. Questa opzione è impostata per impostazione predefinita.
- **DROP (BLOCCA):** Blocca tutte le connessioni al dispositivo.

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

+ New rule (+ Nuova regola): Fare clic per la creazione di una regola.

Rule type (Tipo di regola):

- **FILTER (FILTRO)**: Selezionare per consentire o bloccare le connessioni dai dispositivi che corrispondono ai criteri definiti nella regola.
  - **Policy (Criteri)**: Selezionare **Accept (Accetta)** o **Drop (Blocca)** per la regola del firewall.
  - **IP range (Intervallo IP)**: Selezionare per specificare un intervallo di indirizzi da consentire o bloccare. Utilizzare IPv4/IPv6 in **Start (Inizio)** e **End (Fine)**.
  - **Indirizzo IP**: Immettere l'indirizzo che si desidera consentire o bloccare. Usare il formato IPv4/IPv6 o CIDR.
  - **Protocol (Protocollo)**: Selezionare un protocollo di rete (TCP, UDP o entrambi) da consentire o bloccare. Se si seleziona un protocollo, è necessario specificare anche una porta.
  - **MAC**: inserire l'indirizzo MAC di un dispositivo che si desidera consentire o bloccare.
  - **Intervallo porta**: Selezionare per specificare l'intervallo di porte da consentire o bloccare. Aggiungerlo in **Start (Inizio)** e **End (Fine)**.
  - **Porta**: Inserire un numero di porta che si desidera consentire o bloccare. I numeri di porta devono essere compresi tra 1 e 65535.
  - **Traffic type (Tipo di traffico)**: Selezionare il tipo di traffico che si desidera consentire o bloccare.
    - **UNICAST**: traffico da un singolo mittente a un singolo destinatario.
    - **BROADCAST (Broadcasting)**: traffico da un singolo mittente a tutti i dispositivi della rete.
    - **MULTICAST**: traffico da uno o più mittenti a uno o più destinatari.
- **LIMIT (LIMITE)**: Selezionare per accettare le connessioni dai dispositivi che corrispondono ai criteri definiti nella regola, ma applicare dei limiti per ridurre il traffico eccessivo.
  - **IP range (Intervallo IP)**: Selezionare per specificare un intervallo di indirizzi da consentire o bloccare. Utilizzare IPv4/IPv6 in **Start (Inizio)** e **End (Fine)**.
  - **Indirizzo IP**: Immettere l'indirizzo che si desidera consentire o bloccare. Usare il formato IPv4/IPv6 o CIDR.
  - **Protocol (Protocollo)**: Selezionare un protocollo di rete (TCP, UDP o entrambi) da consentire o bloccare. Se si seleziona un protocollo, è necessario specificare anche una porta.
  - **MAC**: inserire l'indirizzo MAC di un dispositivo che si desidera consentire o bloccare.
  - **Intervallo porta**: Selezionare per specificare l'intervallo di porte da consentire o bloccare. Aggiungerlo in **Start (Inizio)** e **End (Fine)**.
  - **Porta**: Inserire un numero di porta che si desidera consentire o bloccare. I numeri di porta devono essere compresi tra 1 e 65535.
  - **Unit (Unità)**: Selezionare il tipo di connessioni da consentire o bloccare.
  - **Period (Periodo)**: Selezionare il periodo di tempo relativo a **Amount (Quantità)**.
  - **Amount (Quantità)**: Impostare il numero massimo di volte in cui un dispositivo è autorizzato a connettersi entro il **Period (Periodo)** impostato. La quantità massima è 65535.

- **Burst (Eccezione)**: Immettere il numero di connessioni che possono superare la **Amount (Quantità)** una volta durante il **Period (periodo)** impostato. Una volta raggiunto il numero, è consentita solo la quantità impostata durante il periodo stabilito.
- **Traffic type (Tipo di traffico)**: Selezionare il tipo di traffico che si desidera consentire o bloccare.
  - **UNICAST**: traffico da un singolo mittente a un singolo destinatario.
  - **BROADCAST (Broadcasting)**: traffico da un singolo mittente a tutti i dispositivi della rete.
  - **MULTICAST**: traffico da uno o più mittenti a uno o più destinatari.

Test rules (Testa regole): Fare clic per testare le regole definite.

- **Time in seconds: (Tempo di test in secondi)**: Impostare un limite di tempo al fine di mettere alla prova le regole.
- **Roll back**: Fare clic per riportare il firewall allo stato precedente, prima di aver testato le regole.
- **Apply rules (Applica regole)**: Fare clic su per attivare le regole senza eseguire il test. Si sconsiglia questa procedura.

Certificato AXIS OS 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.

Account SSH

Add SSH account (Aggiungi account SSH): Fare clic per aggiungere un nuovo account SSH.

- **Abilita SSH**: Attivare per utilizzare il servizio SSH.

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.

Commento: Inserire un commenti (facoltativo).

Il menu contestuale contiene:

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

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

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.

Configurazione concessione credenziali client

Admin claim (Richiesta amministratore): inserire un valore per il ruolo di amministratore.

Verification URI (URI di verifica): inserire il collegamento Web per l'autenticazione dell'endpoint API.

Operator claim (Richiesta operatore): inserire un valore per il ruolo di operatore.

Require claim (Richiesta obbligatoria): inserire i dati che devono essere contenuti nel token.

Viewer claim (Richiesta visualizzatore): inserire il valore per il ruolo visualizzatore.

Save (Salva): Fare clic per salvare i valori.

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.

Archiviazione

Archiviazione integrata

RAID

- **Free (Libero)**: La quantità di spazio libero su disco.
- **Status (Stato)**: se il disco è montato o meno.
- **File system**: Il file system utilizzato dal disco.
- **Encrypted (Crittografato)**: Se il disco è crittografato o meno.
- **Temperature (Temperatura)**: La temperatura corrente dell'hardware.
- **Overall health test (Test di integrità generale)**: Il risultato dopo aver controllato l'integrità del disco.
- **RAID level (Livello RAID)**: Il livello RAID utilizzato per l'archiviazione. I livelli RAID supportati sono 0, 1, 5, 6, 10.
- **RAID status (Stato RAID)**: Lo stato RAID dell'archiviazione. I valori possibili sono **Online (Online)**, **Degraded (Degradato)**, **Syncing (Sincronizzazione)** e **Failed (Non riuscito)**. Il processo di sincronizzazione potrebbe richiedere diverse ore.

Strumenti

Nota

Quando esegui i seguenti strumenti, assicurati di attendere il completamento dell'operazione prima di chiudere la pagina.

- **Check (Controlla)**: Controllare se sono presenti errori nel dispositivo di archiviazione e tentare di ripararlo automaticamente.
- **Repair (Ripara)**: Ripara il dispositivo di archiviazione. Le registrazioni attive verranno messe in pausa durante il ripristino. La riparazione di un dispositivo di archiviazione potrebbe comportare la perdita di dati.
- **Format (Formatta)**: Cancellare tutte le registrazioni e formattare il dispositivo di archiviazione. Scegli un file system.
- **Encrypt (Codifica)**: codifica i dati archiviati. Tutti i file sul dispositivo di archiviazione verranno cancellati.
- **Decrypt (Decodifica)**: decodifica i dati archiviati. Tutti i file sul dispositivo di archiviazione verranno cancellati.
- **Change password (Cambia password)**: Cambiare la password per la crittografia del disco. La modifica della password non interrompe le registrazioni in corso.
- **Change RAID level (Modifica livello RAID)**: Cancellare tutte le registrazioni e modificare il livello RAID per l'archiviazione.
- **Use tool (Utilizza strumento)**: Fare clic per eseguire lo strumento selezionato.

Hard drive status (Stato del disco rigido): Fare clic per visualizzare lo stato, la capacità e il numero di serie del disco rigido.

Write protect (Proteggi da scrittura): Attivare la protezione da scrittura per proteggere il dispositivo di archiviazione dalla sovrascrizione.

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.
- **View the audit log (Visualizza il registro audit)**: Fare clic per visualizzare le informazioni relative alle attività dell'utente e del sistema, ad esempio autenticazioni e configurazioni riuscite oppure no.

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.

Tipo: Selezionare il tipo di log che si desidera inviare.

Test server setup (Test della configurazione del server): Inviare un messaggio di prova a tutti i server prima di salvare le impostazioni.

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

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.
- **Automatic rollback** (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

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.

Modulo TPM

Il TPM (Trusted Platform Module) è un componente che fornisce funzionalità di crittografia per proteggere le informazioni da accessi non autorizzati. È sempre attivato e non esistono impostazioni che è possibile modificare.

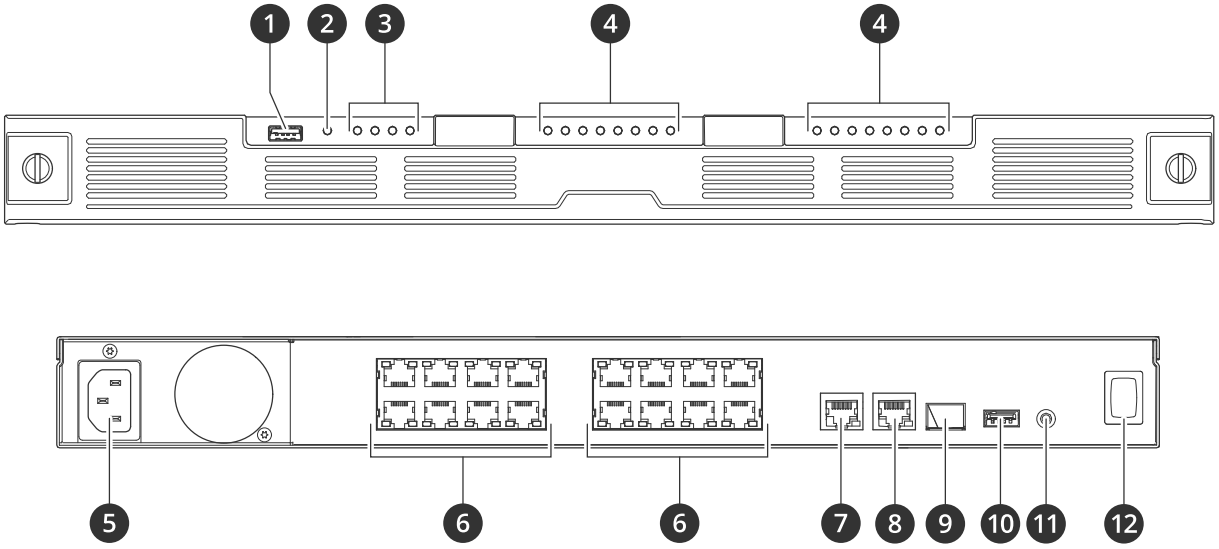
ID dispositivo Axis

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 *Porta USB 3.0*
2 *LED stato prodotto*
3 *LED stato dischi rigidi*
4 *Indicatori LED di stato PoE/rete*
5 *Connettore di alimentazione*
6 *Porte PoE*
7 *Porta AUX RJ45*
8 *Porta LAN RJ45*
9 *Porta LAN SFP*
10 *Porta USB 2.0*
11 *Pulsante di comando*
12 *Tasto di accensione*

Dati tecnici

LED anteriori

LED	Colore	Significato
Stato prodotto	Verde	indica che il registratore è acceso e lo stato è funzionante.
	Giallo	Indica che il registratore si sta avviando oppure che è in corso l'aggiornamento del software per il dispositivo. Attendere che il LED diventi verde.
	Rosso	Ciò può significare il superamento del budget PoE. Se un dispositivo è

		stato appena collegato al registratore, cercare di rimuoverlo.
Stato del disco rigido	Verde	L'unità è online.
	Lampeggia in modo alternato in verde	Il RAID è in fase di sincronizzazione. La registrazione è possibile, ma la ridondanza non è ancora stata raggiunta.
	Giallo	Questa unità è online, ma un'altra unità è danneggiata. Nel RAID manca la ridondanza.
	Rosso	L'unità è danneggiata.
	Tutti sono rossi	Il RAID è fallito. Il sistema non sta registrando. Per identificare il disco rigido rotto in caso di guasto RAID, accedere all'interfaccia web del dispositivo e andare su **System > Storage > Hard drive status (Sistema > Archiviazione > Stato del disco rigido)**.
	Off	Nessun disco rigido.
Stato PoE	Verde	Un dispositivo è connesso.
	Giallo	PoE è in uso ma non c'è collegamento di rete.
	Rosso	Il dispositivo connesso non può essere avviato. Il budget PoE è stato superato. Errore PoE.
	Off	La porta non è in uso o è disabilitata.

LED posteriori

LED	Colore	Significato
Porta di rete	Lampeggia in verde	2.5 Gbit/s
	Lampeggia in giallo	1 Gbit/s
	Off	Nessuna rete
Porta PoE LED sinistro	Verde	PoE è in uso.
	Rosso	Errore PoE. Il budget PoE è stato superato.
	Off	La porta non è in uso o è disabilitata.

Porta PoE LED destro	Lampeggia in verde	1 Gbit/s
	Lampeggia in giallo	100 Mbit/s
	Off	Nessuna rete

Tasto di accensione

- Per arrestare il registratore, premere a lungo il pulsante di alimentazione fino a quando il segnale acustico suona brevemente.
- Per silenziare il segnale acustico, premere brevemente il pulsante di alimentazione.

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.

Risoluzione dei problemi

Problemi tecnici, indicazioni e soluzioni

Rilascia	Soluzione
Le mie registrazioni non sono disponibili.	Andare in .
Non riesco a collegarmi alle mie telecamere.	Andare in .
Ricevo una notifica di errore: “No contact“ (Nessun contatto).	Andare in .
I miei siti non vengono visualizzati nell'app per dispositivi mobili.	Verificare di disporre dell'ultima versione dell'applicazione mobile AXIS Camera Station Edge.

Risoluzione dei problemi comuni

Prima di riavviare, configura o reimposta i tuoi dispositivi.

1. Controllare che le telecamere e il registratore siano alimentati.
2. Verificare di essere connessi a Internet.
3. Verificare che la rete funzioni.
4. Controllare che le telecamere siano connesse alla stessa rete del computer a meno che non ci si trovi in remoto.

Ancora problemi?

5. Verificare che le telecamere, l'unità di registrazione e AXIS Camera Station Edge dispongano del software per il dispositivo più recente.
   Consultare .
6. Riavviare AXIS Camera Station Edge.
7. Riavviare le telecamere e il registratore.

Ancora problemi?

8. Effettuare un hard reset delle telecamere e del registratore, per ripristinare completamente i valori predefiniti di fabbrica.
   Vedere .
9. Aggiungere nuovamente le telecamere ripristinate al sito.

Ancora problemi?

10. Aggiornare la scheda grafica con i driver più recenti.

Ancora problemi?

11. Salvare un report di sistema e contattare il supporto tecnico Axis.
    Vedere .

Aggiornare AXIS OS

I nuovi aggiornamenti software del dispositivo offrono una serie di funzionalità, funzioni e miglioramenti per la sicurezza più recenti e ottimizzati.

1. Andare all'interfaccia web del dispositivo principale.
2. Andare a **Maintenance > AXIS OS upgrade (Manutenzione > Aggiornamento AXIS OS)** e fare clic su **Upgrade (Aggiorna)**.

3. Seguire le istruzioni visualizzate sullo schermo.

Impossibile accedere all'interfaccia web del dispositivo

Se è stata impostata una password per il dispositivo durante la configurazione e successivamente è stato aggiunto un dispositivo al sito, non sarà più possibile accedere all'interfaccia web del dispositivo con la password impostata. Il software AXIS Camera Station Edge modifica le password di tutti i dispositivi nel sito.

Per accedere a un dispositivo nel sito, digitare il nome utente **root** e la password del sito.

Modalità di cancellazione di tutte le registrazioni

1. Nell'interfaccia web del dispositivo, andare a **System** > **Storage (Sistema > Archiviazione)**.
2. Selezionare **Format (Formatta)** e fare clic su **Use tool (Usa strumento)**.

Nota

Questa procedura cancella tutte le registrazioni dal disco rigido ma la configurazione del registratore e il sito non vengono modificati.

Salvataggio di un report di sistema

1. In AXIS Camera Station Edge, andare su  > **Save system report** (Salva report di sistema).
2. In AXIS Camera Station Pro, andare su  **> Help > System report** (Report di sistema).
3. Quando si registra un nuovo caso nell'helpdesk Axis, allegare il report di sistema.

Bisogno di assistenza?

Link utili

- *Guida per l'utente di AXIS Camera Station Edge*
- *Manuale per l'utente di AXIS Camera Station Pro*

Contattare l'assistenza

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

T10186767_it

2025-12 (M9.2)