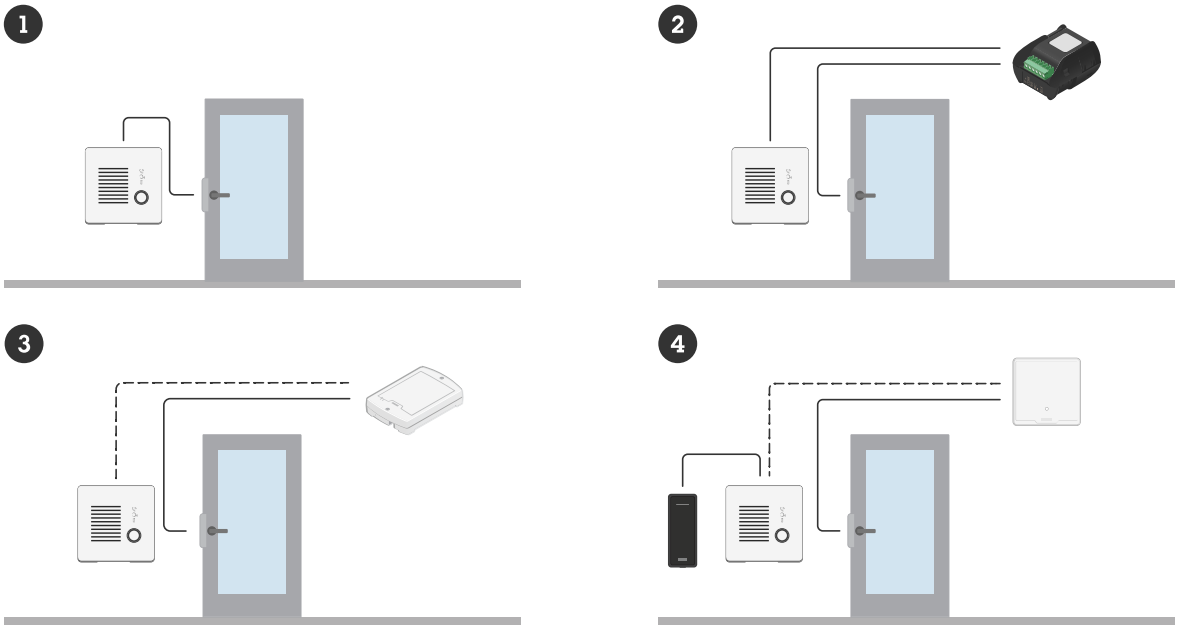
AXIS I7020 Network Intercom

Manuale dell'utente

Indice

Panoramica dell'impostazione



1 *Interfono*
2 *Interfono combinato con AXIS A9801*
3 *Interfono combinato con AXIS A9161*
4 *Interfono combinato con un lettore e un sistema di controllo degli accessi*

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™	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 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.

Configurare il dispositivo

In questa sezione sono illustrate tutte le configurazioni importanti che un installatore deve eseguire per rendere il dispositivo operativo dopo aver completato l'installazione dell'hardware.

Impostazione SIP diretto (P2P)

VoIP (Voice over IP) è un gruppo di tecnologie che consentono la comunicazione vocale e multimediale su reti IP. Per ulteriori informazioni, vedere .

In questo dispositivo VoIP è abilitato tramite il protocollo SIP. Per ulteriori informazioni su SIP, consultare

Esistono due tipi di impostazione SIP. Una di queste è la diretta o peer-to-peer (P2P). Utilizzare peer-to-peer quando la comunicazione si trova tra pochi agenti utente all'interno della stessa rete IP e non è necessario disporre di funzionalità aggiuntive che un server PBX può fornire. Per informazioni su come configurarlo, vedere .

1. Andare a **Communication > SIP > Settings (Comunicazione > SIP > Impostazioni)** e selezionare **Enable SIP (Abilita SIP)**.
2. Per consentire al dispositivo di ricevere chiamate in entrata, selezionare **Allow incoming SIP calls (Consenti chiamate SIP in arrivo)**.

AVVISO

Quando si consentono le chiamate in arrivo, il dispositivo accetta chiamate da qualsiasi dispositivo connesso alla rete. Se il dispositivo è accessibile da una rete pubblica o da Internet, si consiglia di non consentire le chiamate in entrata.

3. Fare clic su **Call handling (Gestione chiamate)**.
4. In **Calling timeout (Timeout chiamata)**, impostare il numero di secondi di durata di una chiamata prima della fine se non c'è una risposta.
5. Se sono state consentite chiamate in entrata, impostare il numero di secondi prima del timeout per le chiamate in entrata in **Incoming call timeout (Timeout chiamata in arrivo)**.
6. Fare clic su **Ports (Porte)**.
7. Inserire il numero per **SIP port (Porta SIP)** e il numero per **TLS port (Porta TLS)**.

Nota

- **SIP port (Porta SIP)**: per le sessioni SIP. Il traffico di segnalazione tramite la porta non viene crittografato. Il numero di porta predefinito è 5060.
- **TLS port (Porta TLS)**: per le sessioni SIPS e TLS protette da sessioni SIP. Il traffico di segnalazione attraverso la porta viene crittografato tramite TLS (Transport Layer Security). Il numero di porta predefinito è 5061.
- **RTP start port (Porta di avvio RTP)**: la porta utilizzata per il primo flusso RTP in una chiamata SIP. Il numero di porta di avvio predefinito è 4000. Alcuni firewall bloccano il traffico RTP su determinati numeri di porta. Il numero di porta deve essere compreso tra 1024 e 65535.

8. Fare clic su **NAT traversal**.
9. Selezionare i protocolli che si desidera abilitare per NAT traversal.

Nota

Utilizzare NAT traversal quando il dispositivo è collegato alla rete da dietro un router NAT o un firewall. Per ulteriori informazioni vedere .

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

Configurazione di SIP tramite un server (PBX)

VoIP (Voice over IP) è un gruppo di tecnologie che consentono la comunicazione vocale e multimediale su reti IP. Per ulteriori informazioni, vedere .

In questo dispositivo, VoIP è abilitato tramite il protocollo SIP. Per ulteriori informazioni su SIP, consultare

Esistono due tipi di impostazione SIP, uno dei quali è un server PBX. Utilizzare un server PBX quando la comunicazione deve essere compresa tra un numero infinito di agenti utente all'interno e all'esterno della rete IP. Altre funzionalità possono essere aggiunte alla configurazione a seconda del provider PBX. Per ulteriori informazioni, vedere .

1. Richiedere le seguenti informazioni dal provider PBX:
   - ID utente
   - Dominio
   - Password
   - ID di autenticazione
   - ID chiamante
   - Registrar
   - Porta di avvio RTP
2. Andare a **Communication > SIP > Accounts (Communication > SIP > Account)** e fare clic su **+ Add account (+ Aggiungi account)**.
3. Immettere un **Name (Nome)** per l'account.
4. Selezionare **Registered (Registrato)**.
5. Selezionare una modalità di trasporto.
6. Aggiungere le informazioni sull'account dal provider PBX.
7. Fare clic su **Save (Salva)**.
8. Configurare le impostazioni SIP allo stesso modo del peer-to-peer, consultare . Utilizzare la porta di avvio RTP dal provider PBX.

Include il flusso video dalla telecamera vicina nella chiamata SIP

Se si dispone di una telecamera Axis montata vicino all'intercom, è possibile includere il flusso video della telecamera nelle chiamate SIP e VMS dell'intercom.

Requisiti

Una telecamera Axis con risoluzione H.264 e 1280x720, 800x800 o 640x480.

Per collegare l'intercom alla telecamera:

1. Andare a **System > Edge-to-edge > Pairing (Sistema > Edge-to-edge > Associazione)**.
2. In **Camera pairing (Associazione telecamera)**, inserire l'indirizzo, il nome utente e la password della telecamera Axis.
3. Fare clic su **Connetti**.

Creazione di un contatto

In questo esempio viene illustrato come creare un nuovo contatto nella lista dei contatti. Prima di iniziare, abilitare SIP in **Communication > SIP (Comunicazione > SIP)**.

Per creare un nuovo contatto:

1. Andare a **Communication > Contact list > Contacts (Comunicazione > Lista dei contatti)**.
2. Fare clic su **+ Add contact (Aggiungi contatto)**.
3. Inserire il nome e il cognome del contatto.
4. Immettere l'indirizzo SIP del contatto.

Nota

Per informazioni sugli indirizzi SIP, consultare .

5. Selezionare l'account SIP da cui chiamare.

Nota

Le opzioni di disponibilità sono definite in **System (Sistema)** > **Events (Eventi)** > **Schedules (Pianificazioni)**.

6. Selezionare **Availability (Disponibilità)** per il contatto. Se c'è una chiamata quando il contatto non è disponibile, la chiamata viene annullata a meno che non si sia verificata una connessione di fallback.

Nota

Un fallback è un contatto al quale viene inoltrata la chiamata se il contatto originale non risponde o non è disponibile.

7. In **Fallback (Fallback)**, selezionare **None (Nessuno)**.
8. Fare clic su **Save (Salva)**.

Configurazione del pulsante di chiamata

Per impostazione predefinita, il pulsante di chiamata è configurato per poter effettuare chiamate VMS (software per la gestione video). Se si desidera mantenere questa configurazione, è sufficiente aggiungere l'interfono Axis al sistema VMS.

In questo esempio viene illustrato come configurare il sistema per chiamare un contatto nella lista dei contatti quando un visitatore preme il pulsante di chiamata.

1. Andare a **Communication > Calls > Call button (Comunicazione > Chiamate > Pulsante di chiamate)**.
2. In **Recipients (Destinatari)**, rimuovere **VMS**.
3. In **Recipients (Destinatari)**, selezionare un contatto esistente o crearne uno nuovo.

Per disabilitare il pulsante di chiamata, disattivare **Enable call button (Abilita pulsante di chiamata)**.

Utilizzare DTMF per sbloccare la porta per un visitatore

Quando un visitatore effettua una chiamata dall'interfono, la persona che risponde può utilizzare il segnale DTMF (Dual-Tone Multi-Frequency) del relativo dispositivo SIP per sbloccare la porta. Il dispositivo di controllo delle porte blocca e sblocca la porta.

Questo esempio spiega come:

- Definire il segnale DTMF nell'interfono
- impostare l'interfono per:
  - richiedere al door controller di sbloccare la porta, **oppure**
  - sbloccare la porta utilizzando il relè interno.

Configurare tutte le impostazioni dalla pagina Web del dispositivo di controllo dell'interfono.

Prima di iniziare

- Consentire le chiamate SIP dal dispositivo e creare un account SIP. Vedere e .

Definire il segnale DTMF nell'interfono

1. Andare a **Communication > SIP > DTMF (Comunicazione > SIP > DTMF)**.
2. Fare clic su **+ Add sequence (+ Aggiungi sequenza)**.
3. In **Sequence (Sequenza)**, inserire 1.
4. In **Description (Descrizione)**, inserire Unlock door (Sblocca la porta).
5. In **Accounts (Account)**, selezionare l'account SIP.
6. Fare clic su **Save (Salva)**.

Impostare l'interfono per sbloccare la porta utilizzando il relè interno

7. Andare a **System > Events > Rules (Sistema > Eventi > Regole)** e aggiungere una regola.

8. Nel campo **Name (Nome)**, inserire DTMF unlock door (DTMF sblocca porta).
9. Dall'elenco delle condizioni, in **Call (Chiamata)**, selezionare **DTMF** e **Unlock door (Sblocca porta)**.
10. Dall'elenco delle azioni, in **I/O**, selezionare **Toggle I/O once (Attiva/disattiva I/O una volta)**.
11. Dall'elenco delle porte, selezionare **Relay 1 (Relè 1)**.
12. Modificare **Duration (Durata)** in 00:00:07, il che significa che la porta è aperta da 7 secondi.
13. Fare clic su **Save (Salva)**.

Autorizzazione dei titolari credenziali per l'apertura della porta

Con l'elenco delle voci è possibile consentire ai titolari credenziali di utilizzare la propria tessera o PIN per attivare le azioni, come l'apertura di una porta. Questo esempio illustra come aggiungere un titolare credenziali che può utilizzare la propria tessera per aprire la porta 10 volte.

Prerequisiti

- Assicurarsi che il tipo di chip corretto sia attivo in **Reader > Chip types (Lettore > Tipi di chip)**.

Attivare l'elenco delle voci e aggiungere un titolare credenziali:

1. Andare a **Reader > Entry list (Lettore > Elenco delle voci)**.
2. Attivare **Use Entry list (Usa elenco delle voci)**.
3. Fare clic su **+ Add credential holder (+ Aggiungi titolare credenziali)**.
4. Inserire il nome e il cognome del titolare credenziali. Il nome deve essere univoco.
5. Selezionare **Card (Tessera)**.
6. Passare la tessera del titolare credenziali sul dispositivo e fare clic su **Get latest (Ottieni l'ultimo)**.
7. Mantenere la condizione dell'evento **Access granted (Accesso consentito)**.
8. In **Valid to (Valido fino al)**, selezionare **Number of times (Numero di volte)**.
9. In **Number of times (Numero di volte)**, inserire 10.
10. Fare clic su **Save (Salva)**.

Creare una regola:

1. Andare a **System > Events (Sistema > Eventi)**.
2. In **Rules (Regole)**, fare clic su **+ Add a rule (+ Aggiungi una regola)**.
3. In **Name (Nome)**, inserire Open door (Apri porta).
4. Nell'elenco delle condizioni, selezionare **Entry list > Access granted (Elenco delle voci > Accesso consentito)**.
5. Dall'elenco delle azioni, selezionare **I/O > Toggle I/O once (I/O > Attiva/disattiva I/O una volta)**.
6. Dall'elenco delle porte, selezionare **Door (Porta)**.
7. In **State (Stato)**, selezionare **Active (Attivo)**.
8. Impostare la durata su 00:00:07.
9. Fare clic su **Save (Salva)**.

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.

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.

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.

Video

Installazione

Capture mode (Modalità di acquisizione) : Una modalità di acquisizione costituisce una configurazione preset che definisce in che modo la telecamera esegue l'acquisizione delle immagini. Quando cambi la modalità di acquisizione, può influire su varie altre impostazioni, ad es. aree di visione e le privacy mask.

Mounting position (Posizione di montaggio) : l'orientamento dell'immagine può cambiare in base alla posizione di montaggio della telecamera.

Power line frequency (Frequenza della linea elettrica): per ridurre al minimo lo sfarfallio dell'immagine, selezionare la frequenza usata nella regione. Le regioni americane utilizzano generalmente una frequenza di 60 Hz. Il resto del mondo utilizza una frequenza di 50 Hz. Se non si è sicuri della frequenza della linea di alimentazione della regione, verificare con le autorità locali.

Rotate (Rotazione): Seleziona l'orientamento immagine preferito.

Immagine

Aspetto

Profilo scena : Seleziona un profilo scena idoneo allo scenario di sorveglianza. Un profilo scena ottimizza le impostazioni dell'immagine, tra cui il livello di colore, la luminosità, la nitidezza, il contrasto e il contrasto locale, per un ambiente o un fine specifico.

- **Forensic** : Idoneo per fini di sorveglianza.
- **Interno** : Adatto per ambienti interni.
- **Esterno** : Adatto per ambienti esterni.
- **Vivido** : Utile a fini dimostrativi.
- **Panoramica del traffico** : Idoneo per monitorare il traffico veicolare.
- **Targa** : Adatto per l'acquisizione di targhe.

Saturazione: utilizzare il cursore per regolare l'intensità del colore. Ad esempio è possibile ottenere un'immagine nella scala dei grigi.

Contrasto: utilizzare questo cursore per regolare la differenza tra luce e ombra.

Luminosità: Utilizzare il cursore per regolare la sensibilità alla luce. Ciò può rendere più facile vedere gli oggetti. La luminosità viene applicata dopo l'acquisizione dell'immagine e non influisce sulle informazioni nell'immagine. Per ottenere più dettagli da un'area scura, solitamente è meglio aumentare il guadagno o il tempo di esposizione.

Sharpness (Nitidezza): Utilizza il cursore per regolare il contrasto dei bordi e rendere gli oggetti più nitidi nell'immagine. Se incrementi la nitidezza, anche i requisiti di velocità in bit e spazio di archiviazione possono aumentare.

Wide Dynamic Range

WDR : Attiva per rendere visibili sia le aree chiare che quelle scure.

Contrasto locale : Usare il cursore per regolare il contrasto dell'immagine. Un valore più elevato incrementa il contrasto tra le aree chiare e scure.

Mappatura tonale : utilizzare questo cursore per regolare il livello di mappatura tonale applicato all'immagine. Se il valore è impostato su zero viene applicata solo la correzione della gamma standard, mentre un valore più alto aumenta la visibilità delle parti più buie e luminose nell'immagine.

Bilanciamento del bianco

Quando la telecamera rileva la temperatura di colore della luce in entrata, può regolare l'immagine per rendere i colori più naturali. Se ciò non è sufficiente, puoi selezionare una sorgente luminosa adatta dall'elenco.

L'impostazione di bilanciamento del bianco automatico riduce il rischio di sfarfallio del colore adattando variazioni graduali. Quando cambia l'illuminazione, o quando la telecamera viene avviata per la prima volta, potrebbero essere necessari fino a 30 secondi prima che la telecamera si adatti alla nuova sorgente luminosa. Se vi sono più tipi di sorgenti luminose in una scena, ovvero sorgenti luminose con temperature di colore differenti, la sorgente luminosa dominante agisce come riferimento per l'algoritmo di bilanciamento del bianco automatico. Questo comportamento può essere ignorato scegliendo un'impostazione di bilanciamento del bianco fissa che corrisponda alla sorgente luminosa che si desidera utilizzare come riferimento.

Light environment (Luminosità ambiente):

- **Automatic (Automatica)**: Identificazione e compensazione automatiche per il colore della sorgente luminosa. È l'impostazione consigliata, utilizzabile per la maggior parte delle situazioni.
- **Automatico – esterni** : Identificazione e compensazione automatiche per il colore della sorgente luminosa. È l'impostazione consigliata, utilizzabile per la maggior parte delle situazioni all'esterno.
- **Personalizzato – interni** : Regolazione colore fissa per una stanza con un'illuminazione artificiale diversa da quella fluorescente e ottimale per una temperatura di colore intorno a 2800 K.
- **Personalizzato – esterni** : Regolazione colore fissa per condizioni atmosferiche soleggiate con temperatura di colore intorno a 5500 K.
- **Fixed – fluorescent 1 (Fisso – illuminazione fluorescente 1)**: Regolazione colore fissa per un'illuminazione fluorescente con una temperatura di colore intorno a 4000 K.
- **Fixed – fluorescent 2 (Fisso – illuminazione fluorescente 2)**: Regolazione colore fissa per un'illuminazione fluorescente con una temperatura di colore intorno a 3000 K.
- **Fixed – indoors (Fisso – interni)**: Regolazione colore fissa per una stanza con un'illuminazione artificiale diversa da quella fluorescente e ottimale per una temperatura di colore intorno a 2800 K.
- **Fixed – outdoors 1 (Fisso – esterni 1)**: Regolazione colore fissa per condizioni atmosferiche soleggiate con temperatura di colore intorno a 5500 K.
- **Fixed – outdoors 2 (Fisso – esterni 2)**: Regolazione colore fissa per condizioni atmosferiche nuvolose con temperatura di colore intorno a 6500 K.
- **Illuminazione stradale – mercurio** : regolazione colore fissa per le emissioni ultraviolette nelle luci ai vapori di mercurio tipiche dell'illuminazione stradale.
- **Illuminazione stradale – sodio** : Regolazione colore fissa che compensa il colore giallo arancione delle luci ai vapori di sodio tipiche dell'illuminazione stradale.
- **Hold current (Mantieni opzioni correnti)**: Mantieni le impostazioni di corrente e non compensare i cambiamenti di luce.
- **Manuale** : correzione del bilanciamento del bianco con il supporto di un oggetto bianco. Trascinare il cerchio su un oggetto che si desidera venga interpretato come bianco dalla telecamera nell'immagine della visualizzazione in diretta. Utilizzare i cursori **Red balance (Bilanciamento del rosso)** e **Blue balance (Bilanciamento del blu)** per regolare manualmente il bilanciamento del bianco.

Esposizione

Seleziona una modalità di esposizione per ridurre gli effetti irregolari in rapida evoluzione nell'immagine, ad esempio lo sfarfallio dispositivo da differenti tipi di sorgenti luminose. Si consiglia di usare la modalità di esposizione automatica oppure la stessa frequenza della rete di alimentazione.

Modalità di esposizione:

- **Automatic (Automatica)**: la telecamera regola automaticamente l'apertura, il guadagno e l'otturatore.
- **Apertura automatica** : La telecamera regola automaticamente l'apertura e il guadagno. L'otturatore è fisso.
- **Otturatore automatico** : La telecamera regola automaticamente il guadagno e l'otturatore. L'apertura è fissa.
- **Hold current (Mantieni opzioni correnti)**: Blocca le impostazioni di esposizione correnti.
- **Privo di sfarfallio** : La telecamera regola automaticamente l'apertura e il guadagno e utilizza solo le seguenti velocità dell'otturatore: 1/50 s (50 Hz) e 1/60 s (60 Hz).
- **50 Hz senza sfarfallio** : La telecamera regola automaticamente l'apertura e il guadagno e usa la velocità otturatore 1/50 s.
- **60 Hz senza sfarfallio** : La telecamera regola automaticamente l'apertura e il guadagno e usa la velocità otturatore 1/60 s.
- **Con sfarfallio ridotto** : è identica all'opzione privo di sfarfallio, ma la telecamera può utilizzare una qualsiasi velocità dell'otturatore superiore a 1/100 s (50 Hz) e 1/120 s (60 Hz) per le scene più luminose.
- **50 Hz con sfarfallio ridotto** : è identica all'opzione privo di sfarfallio, ma la telecamera può utilizzare una qualsiasi velocità dell'otturatore superiore a 1/100 s per le scene più luminose.
- **60 Hz con sfarfallio ridotto** : è identica all'opzione privo di sfarfallio, ma la telecamera può utilizzare una qualsiasi velocità dell'otturatore superiore a 1/120 s per le scene più luminose.
- **Manuale** : l'apertura, il guadagno e l'otturatore sono fissi.

Zona di esposizione : usa le zone di esposizione per l'ottimizzazione dell'esposizione in una parte selezionata della scena, ad esempio l'area davanti a una porta di ingresso.

Nota

Le zone di esposizione sono correlate all'immagine originale (non ruotata) e i nomi delle zone si applicano all'immagine originale. Ciò significa che, ad esempio, se il flusso video viene ruotato di 90°, la zona **Upper (Superiore)** diventa la zona **Right (Destra)** nel flusso e **Left (Sinistra)** diventa **Lower (Inferiore)**.

- **Automatic (Automatica)**: Idoneo per la gran parte delle situazioni.
- **Center (Centro)**: Utilizza un'area fissa al centro dell'immagine per calcolare l'esposizione. L'area presenta dimensione e posizione fisse nella visualizzazione in diretta.
- **Pieno** : Utilizza l'intera visualizzazione in diretta per calcolare l'esposizione.
- **Superiore** : Utilizza un'area con dimensioni e posizione fisse nella parte superiore dell'immagine per calcolare l'esposizione.
- **Inferiore** : Utilizza un'area con dimensioni e posizione fisse nella parte inferiore dell'immagine per calcolare l'esposizione.

- **A sinistra** : Utilizza un'area con dimensioni e posizione fisse nella parte sinistra dell'immagine per calcolare l'esposizione.
- **A destra** : Utilizza un'area con dimensioni e posizione fisse nella parte destra dell'immagine per calcolare l'esposizione.
- **Spot**: Utilizza un'area con dimensioni e posizione fisse nella visualizzazione in diretta per calcolare l'esposizione.
- **Personalizzato**: Utilizza un'area nella visualizzazione in diretta per calcolare l'esposizione. Puoi regolare le dimensioni e la posizione dell'area.

Max shutter (Otturatore massimo): Selezionare la velocità otturatore per fornire l'immagine migliore. Velocità otturatore più basse (esposizione più lunga) potrebbe causare sfocatura da movimento quando c'è movimento e velocità otturatore troppo elevate potrebbero incidere sulla qualità dell'immagine. L'otturatore massimo lavora con il guadagno massimo per migliorare l'immagine.

Guadagno massimo: Seleziona il guadagno massimo idoneo. Se aumenti il guadagno massimo, esso migliora il livello visibile di dettaglio nelle immagini scure, ma crea anche il livello di rumore. Maggiore rumore può causare un maggiore utilizzo di larghezza di banda e spazio di archiviazione. Se imposti il guadagno massimo su un valore elevato, le immagini possono essere molto diverse se le condizioni di luce sono molto diverse durante il giorno e la notte. Il guadagno massimo lavora con l'otturatore massimo per migliorare l'immagine.

Esposizione motion-adaptive : Selezionare questa opzione per ridurre la sfocatura da movimento in condizioni di bassa luminosità.

Blur-noise trade-off (Compromessi disturbo-sfocatura): Usa questo cursore per regolare la priorità tra la sfocatura da movimento e il rumore. Se si desidera dare priorità a minori requisiti di banda e a meno rumore a scapito dei dettagli negli oggetti in movimento, spostare il cursore verso **Low noise (Disturbo ridotto)**. Se si desidera dare priorità ai dettagli negli oggetti in movimento a scapito del rumore e della larghezza di banda, sposta il cursore verso **Low motion blur (Sfocatura da movimento ridotta)**.

Nota

Puoi modificare l'esposizione regolando il tempo di esposizione o regolando il guadagno. Incrementando il tempo di esposizione, il risultato sarà una sfocatura da movimento maggiore e l'incremento del guadagno comporta maggiore rumore. Se regoli **Blur-noise trade-off (Compromessi disturbo-sfocatura)** verso **Low noise (Basso rumore)**, l'esposizione automatica darà la priorità a tempi di esposizione maggiori rispetto all'incremento del guadagno e l'opposto avverrà se regolerai il compromesso verso **Low motion blur (Sfocatura da movimento ridotta)**. Sia il guadagno che il tempo di esposizione raggiungeranno i valori massimi in condizioni di bassa luminosità, indipendentemente dalla priorità impostata.

Blocca apertura : Attiva per conservare le dimensioni dell'apertura impostate con il cursore **Aperture (Apertura)**. Disattiva per consentire alla telecamera di regolare automaticamente le dimensioni di apertura. Ad esempio, puoi bloccare l'apertura per le scene con condizioni di luce permanenti.

Apertura : Utilizza il cursore per regolare le dimensioni dell'apertura, ovvero quanta luce passa attraverso l'obiettivo. Per permettere che più luce entri nel sensore e far sì che, di conseguenza, l'immagine prodotta in condizioni di bassa luminosità sia più luminosa, sposta il cursore verso **Open (Apri)**. Un'apertura ampia riduce però la profondità di campo; gli oggetti vicini o troppo lontani dalla telecamera possono risultare sfocati. Per permettere che una porzione più grande dell'immagine sia messa a fuoco, sposta il cursore verso **Closed (Chiuso)**.

Exposure level (Livello esposizione): Utilizzare il cursore per regolare l'esposizione d'immagine.

Defog (Nitidezza) : Attiva per rilevare gli effetti della nebbia e li rimuoverà automaticamente per ottenere un'immagine più nitida.

Nota

Ti consigliamo di non attivare **Defog (Sbrinamento)** in scene con basso contrasto, elevate variazioni del livello di luce o quando la messa a fuoco automatica è leggermente sfocata. Ciò può influire sulla qualità d'immagine, ad esempio aumentando il contrasto. Inoltre, troppa luminosità può influire negativamente sulla qualità di immagine quando lo sbrinamento è attivo.

Flusso

Generale

Risoluzione: Selezionare la risoluzione dell'immagine adatta per la scena di sorveglianza. Una risoluzione più elevata necessita di più larghezza di banda e spazio di archiviazione.

Frequenza dei fotogrammi: Per evitare problemi di larghezza di banda nella rete o ridurre le dimensioni di archiviazione, puoi limitare la velocità in fotogrammi a una quantità fissa di fotogrammi. Se la velocità in fotogrammi è zero, il valore viene impostato sul valore massimo possibile nelle condizioni correnti. Una velocità in fotogrammi più elevata necessita di larghezza di banda e spazio di archiviazione maggiori.

P-frames (P-frame): Un P-frame è un'immagine predetta che mostra solo le modifiche nell'immagine rispetto al fotogramma precedente. Immetti il numero desiderato di P-frame. Più è alto il numero, minore è la larghezza di banda necessaria. Tuttavia, se è presente una congestione di rete, potrebbe verificarsi un deterioramento della qualità video.

Compressione: Utilizzare il cursore per regolare la compressione d'immagine. Un'elevata compressione si traduce in velocità di trasmissione e qualità dell'immagine inferiori. Una compressione bassa migliora la qualità dell'immagine ma utilizza larghezza di banda e spazio di archiviazione maggiori durante la registrazione.

Video con firma  : Attivare per aggiungere la funzione video firmata al video. Il video firmato protegge il video dalle manomissioni aggiungendo firme crittografiche al video.

Zipstream

Zipstream è una tecnologia di riduzione della velocità di trasmissione ottimizzata per il monitoraggio video e consente di ridurre la velocità di trasmissione media in un flusso H.264 o H.265 in tempo reale. La tecnologia Axis Zipstream applica una velocità in bit elevata nelle scene con molte regioni di interesse, ad esempio in scene con oggetti in movimento. Quando la scena è più statica, Zipstream applica una velocità in bit più bassa, riducendo pertanto l'archiviazione necessaria. Vedere *Riduzione della velocità in bit con Axis Zipstream* per saperne di più.

Selezionare il livello di **Strength (Intensità)** della riduzione della velocità in bit:

- **Off (Disattivato)**: Nessuna riduzione della velocità in bit.
- **Bassa**: Nessuna degradazione della qualità visibile nella maggior parte delle scene. Si tratta dell'opzione predefinita e si può usare in ogni tipo di scena per la riduzione della velocità in bit.
- **Media**: effetti visibili in alcune scene tramite minore rumore e un livello di dettagli leggermente inferiore nelle regioni di minore interesse, ad esempio dove non c'è nessun movimento.
- **Alta**: effetti visibili in alcune scene tramite minore rumore e un livello di dettagli inferiore nelle regioni di minore interesse, ad esempio dove non c'è nessun movimento. Consigliamo questo livello per i dispositivi connessi al cloud e quelli che usano l'archiviazione locale.
- **Higher (Più elevato)**: effetti visibili in alcune scene tramite minore rumore e un livello di dettagli inferiore nelle regioni di minore interesse, ad esempio dove non c'è nessun movimento.
- **Extreme (Estrema)**: effetti visibile nella maggior parte delle scene. La velocità in bit è ottimizzata per occupare il minore spazio di archiviazione possibile.

Optimize for storage (Ottimizza per archiviazione): attivare per ridurre al minimo la velocità in bit mantenendo la qualità. L'ottimizzazione non si applica al flusso mostrato nel client Web. Questa opzione può essere utilizzata solo se il VMS supporta B-frame. L'attivazione di **Optimize for storage (Ottimizza per archiviazione)** attiva anche **Dynamic GOP (dynamic group of pictures)**.

Dynamic FPS (FPS dinamico) (fotogrammi al secondo): Attiva per permettere che la larghezza di banda vari in base al livello di attività nella scena. Un'attività maggiore necessita di più larghezza di banda.

Lower limit (Limite inferiore): Immetti un valore per regolare la velocità in fotogrammi tra fps minimo e fps predefinito del flusso sulla base del movimento nella scena. Ti consigliamo di usare un limite inferiore in scene caratterizzate da poco movimento, dove fps può scendere a 1 o a un valore inferiore.

Dynamic GOP (GOP dinamico) (Group of Pictures): Attiva per la regolazione dinamica dell'intervallo tra gli I-frame sulla base del livello di attività nella scena.

Upper limit (Limite superiore): Immetti una lunghezza GOP massima, vale a dire il numero massimo di P-frame tra due I-frame. Un I-frame è un fotogramma immagine a sé stante indipendente da altri fotogrammi.

Controllo velocità di trasferimento

- **Average (Media)**: Seleziona per la regolazione automatica della velocità in bit per un periodo di tempo più lungo e la migliore qualità di immagine possibile sulla base dell'archiviazione a disposizione.
  -  Fare clic per il calcolo della velocità in bit di destinazione sulla base dell'archiviazione disponibile, del tempo di conservazione e del limite della velocità in bit.
  - **Target bitrate (Velocità in bit di destinazione)**: Immetti la velocità in bit di destinazione voluta.
  - **Retention time (Tempo di conservazione)**: Immetti il numero di giorni per la conservazione delle registrazioni.
  - **Dispositivo di archiviazione**: mostra lo spazio di archiviazione stimato che può essere utilizzato per il flusso.
  - **Maximum bitrate (Velocità di trasmissione massima)**: Attiva per l'impostazione di un limite di velocità in bit.
  - **Bitrate limit (Limite velocità in bit)**: Immettere un limite per la velocità in bit che sia maggiore rispetto alla velocità in bit di destinazione.
- **Maximum (Massimo)**: selezionare per impostare una velocità di trasmissione massima istantanea del flusso in base alla larghezza di banda di rete.
  - **Maximum (Massimo)**: Immetti la velocità in bit massima.
- **Variable (Variabile)**: Seleziona per permettere che la velocità in bit vari sulla base del livello di attività nella scena. Un'attività maggiore necessita di più larghezza di banda. Raccomandiamo questa opzione per la gran parte delle situazioni.

Orientamento

Mirror (Specularità): abilitare questa impostazione per la specularità dell'immagine.

Audio

Include (Includi): Attiva per usare l'audio nel flusso video.

Source (Sorgente)  : Seleziona la sorgente audio da usare.

Stereo  : Attiva per l'inclusione dell'audio incorporato nonché dell'audio da un microfono esterno.

Sovrimpressioni

: Fare clic per aggiungere una sovrapposizione. Seleziona il tipo di sovrapposizione dall'elenco a discesa:

- **Text (Testo)**: Seleziona per mostrare un testo integrato nell'immagine della visualizzazione in diretta e visibile in tutte le viste, registrazioni ed istantanee. Puoi inserire un testo personalizzato e comprendere anche modificatori preconfigurati per mostrare in automatico, ad esempio, l'ora, la data e la velocità in fotogrammi.
  - : fare clic per aggiungere il campo di modifica della data `%F` per visualizzare il formato aaaa-mm-gg.
  - : fare clic per aggiungere il campo di modifica dell'ora `%X` per visualizzare hh:mm:ss (formato 24 ore).
  - **Modifiers (Campi di modifica)**: Fare clic per selezionare qualsiasi campo di modifica presente nell'elenco per aggiungerlo alla casella di testo. Ad esempio, `%a` mostra il giorno della settimana.
  - **Dimensioni**: Selezionare le dimensioni font desiderate.
  - **Aspetto**: selezionare il colore del testo e di sfondo, ad esempio, testo bianco su sfondo nero (valore predefinito).
  - : selezionare la posizione della sovrapposizione nell'immagine o fare clic e trascinare la sovrapposizione per spostarla nella visualizzazione in diretta.
- **Immagine**: Seleziona per mostrare un'immagine statica sovrimpressa sul flusso video. Puoi usare file .bmp, .png, .jpeg o .svg.
  Per caricare un'immagine, fare clic su **Manage images (Gestione immagini)**. Prima del caricamento di un'immagine, puoi scegliere di:
  - **Scale with resolution (Scala con risoluzione)**: Seleziona per adattare automaticamente l'immagine grafica sovrapposta alla risoluzione video.
  - **Use transparency (Usa trasparenza)**: Seleziona e inserisci il valore esadecimale RGB per quel colore. Usa il formato RRGGBB. Esempi di valori esadecimali: FFFFFF per bianco, 000000 per nero, FF0000 per rosso, 6633FF per blu e 669900 per verde. Solo per immagini .bmp.
- **Annotazioni scena** : Selezionare tale opzione per mostrare una sovrapposizione di testo nel flusso video che rimanga nella stessa posizione, anche nel momento in cui la telecamera esegue la panoramica o l'inclinazione in una direzione diversa. Si può decidere di mostrare la sovrapposizione solo in certi livelli di zoom.
  - : fare clic per aggiungere il campo di modifica della data `%F` per visualizzare il formato aaaa-mm-gg.
  - : fare clic per aggiungere il campo di modifica dell'ora `%X` per visualizzare hh:mm:ss (formato 24 ore).
  - **Modifiers (Campi di modifica)**: Fare clic per selezionare qualsiasi campo di modifica presente nell'elenco per aggiungerlo alla casella di testo. Ad esempio, `%a` mostra il giorno della settimana.
  - **Dimensioni**: Selezionare le dimensioni font desiderate.
  - **Aspetto**: selezionare il colore del testo e di sfondo, ad esempio, testo bianco su sfondo nero (valore predefinito).

-  : selezionare la posizione della sovrapposizione nell'immagine o fare clic e trascinare la sovrapposizione per spostarla nella visualizzazione in diretta. La sovrapposizione testo è salvata e resta nelle coordinate panoramica e inclinazione di tale ubicazione.
- **Annotation between zoom levels (%) (Annotazione tra livelli di zoom (%))**: Impostare i livelli di zoom nei quali sarà mostrata la sovrapposizione testo.
- **Annotation symbol (Simbolo annotazioni)**: Selezionare un simbolo che compare invece della sovrapposizione testo quando la telecamera non è nei livelli di zoom impostati.

- **Streaming indicator (Indicatore di streaming)**  : Seleziona per mostrare un'animazione sovrimpressa sul flusso video. Questa animazione indica che il flusso video è in diretta anche se la scena non contiene nessun movimento.
  - **Aspetto**: selezionare il colore dell'animazione e di sfondo, ad esempio, animazione rossa su sfondo trasparente (valore predefinito).
  - **Dimensioni**: Selezionare le dimensioni font desiderate.
  -  : selezionare la posizione della sovrapposizione nell'immagine o fare clic e trascinare la sovrapposizione per spostarla nella visualizzazione in diretta.
- **Widget: Linegraph (Grafico a linee)**  : Mostrare un grafico che illustri in che modo un valore misurato cambia nel corso del tempo.
  - **Titolo**: Immettere un titolo per il widget.
  - **Campo di modifica sovrapposizione testo**: Selezionare un campo di modifica di sovrapposizione testo come sorgente dati. Se sono state create delle sovrapposizioni testo MQTT, si troveranno alla fine dell'elenco.
  -  : selezionare la posizione della sovrapposizione nell'immagine o fare clic e trascinare la sovrapposizione per spostarla nella visualizzazione in diretta.
  - **Dimensioni**: Selezionare le dimensioni della sovrapposizione testo.
  - **Visibile su tutti i canali**: Disattivare perché appaia solo sul canale correntemente selezionato. Attivare perché appaia su tutti i canali attivi.
  - **Intervallo di aggiornamento**: Selezionare il periodo tra aggiornamenti di dati.
  - **Trasparenza**: Impostare la trasparenza di tutta la sovrapposizione testo.
  - **Trasparenza dello sfondo**: Impostare la trasparenza solamente dello sfondo della sovrapposizione testo.
  - **Punti**: Attivare per eseguire l'aggiunta di un punto alla linea del grafico quando i dati sono aggiornati.
  - Asse x
    - **Etichetta**: Inserire l'etichetta testo per l'asse x.
    - **Intervallo di tempo**: Inserire quanto a lungo i dati saranno visualizzati.
    - **Unità di tempo**: Inserire un'unità di tempo per l'asse x.
  - Asse y
    - **Etichetta**: Inserire l'etichetta testo per l'asse y.
    - **Scala dinamica**: Attivare questa opzione perché la scala si adatti in automatico ai valori dei dati. Disattivare questa opzione per inserire in modo manuale i valori per una scala fissa.
    - **Soglia allarme minima** e **Soglia allarme massima**: Tali valori aggiungeranno linee di riferimento orizzontali al grafico, facendo sì che si possa vedere più facilmente quando il valore dei dati diventa eccessivo o troppo basso.

- **Widget: Metro** : Mostrare un grafico a barre che illustra il valore dei dati misurati più di recente.
  - **Titolo**: Immettere un titolo per il widget.
  - **Campo di modifica sovrapposizione testo**: Selezionare un campo di modifica di sovrapposizione testo come sorgente dati. Se sono state create delle sovrapposizioni testo MQTT, si troveranno alla fine dell'elenco.
  - : selezionare la posizione della sovrapposizione nell'immagine o fare clic e trascinare la sovrapposizione per spostarla nella visualizzazione in diretta.
  - **Dimensioni**: Selezionare le dimensioni della sovrapposizione testo.
  - **Visibile su tutti i canali**: Disattivare perché appaia solo sul canale correntemente selezionato. Attivare perché appaia su tutti i canali attivi.
  - **Intervallo di aggiornamento**: Selezionare il periodo tra aggiornamenti di dati.
  - **Trasparenza**: Impostare la trasparenza di tutta la sovrapposizione testo.
  - **Trasparenza dello sfondo**: Impostare la trasparenza solamente dello sfondo della sovrapposizione testo.
  - **Punti**: Attivare per eseguire l'aggiunta di un punto alla linea del grafico quando i dati sono aggiornati.
  - **Asse y**
    - **Etichetta**: Inserire l'etichetta testo per l'asse y.
    - **Scala dinamica**: Attivare questa opzione perché la scala si adatti in automatico ai valori dei dati. Disattivare questa opzione per inserire in modo manuale i valori per una scala fissa.
    - **Soglia allarme minima** e **Soglia allarme massima**: Tali valori aggiungeranno linee di riferimento orizzontali al grafico a barre, facendo sì che si possa vedere più facilmente quando il valore dei dati diventa eccessivo o troppo basso.

Privacy mask

: Fare clic per la creazione di una nuova privacy mask.

Privacy masks (Privacy mask): Fare clic per modificare il colore di tutte le privacy mask o per eliminarle in modo permanente.

Mask x (Maschera x): Fare clic per la rinomina, disabilitazione o eliminazione permanente della maschera.

Comunicazione

Lista dei contatti

Contatti

Fare clic su per eseguire il download dell'elenco di contatti come file json.

Fare clic su per eseguire l'importazione di un elenco di contatti (json).

Add contact (Aggiungi contatto): fare clic qui per eseguire l'aggiunta di un nuovo contatto all'elenco di contatti.

Upload image (Carica immagine) : fare clic per caricare un'immagine che rappresenti il contatto.

First name (Nome): inserire il nome del contatto.

Last name (Cognome): inserire il cognome del contatto.

Speed dial (Chiamata rapida) : inserisci un numero di chiamata rapida disponibile per il contatto. Questo numero è usato per chiamare il contatto dal dispositivo.

Indirizzo SIP: se si utilizza SIP, inserire l'indirizzo IP o l'estensione del contatto.

: Fai clic per eseguire una chiamata di prova. Questa chiamata terminerà automaticamente quando riceverà risposta.

Account SIP: se si utilizza SIP, selezionare l'account SIP da usare per la chiamata dal dispositivo al contatto.

Availability (Disponibilità): Seleziona la pianificazione di disponibilità del contatto. È possibile aggiungere o modificare le pianificazioni in **System (Sistema) > Events (Eventi) > Schedules (Pianificazioni)**. Se si tenta una chiamata quando il contatto non è disponibile, la chiamata viene annullata a meno che non si sia verificata una connessione di fallback.

Fallback: se applicabile, selezionare un contatto di fallback dall'elenco.

Note: aggiunta di informazioni facoltative sul contatto.

Il menu contestuale contiene:

Edit contact (Modifica contatto): modificare le proprietà del contatto.

Delete contact (Elimina contatto): elimina contatto.

SIP

Impostazioni

Il protocollo SIP (Session Initiation Protocol) viene utilizzato per le sessioni di comunicazione interattiva tra gli utenti. Le sessioni possono includere audio e video.

SIP setup assistant (Assistente alla configurazione SIP): fare clic su questa opzione per impostare e configurare SIP passo dopo passo.

Enable SIP (Abilita SIP): Seleziona questa opzione per rendere possibile l'avvio e la ricezione di chiamate SIP.

Permetti chiamate in entrata: Selezionare questa opzione per consentire le chiamate in arrivo da altri dispositivi SIP.

Gestione chiamate

- **Timeout chiamata**: impostare la durata massima di un tentativo di chiamata in mancanza di risposta.
- **Incoming call duration (Durata chiamata in entrata)**: Impostare la durata massima di una chiamata in entrata (massimo 10 minuti).
- **End calls after (Termina chiamate dopo)**: impostare la durata massima di una chiamata (massimo 60 minuti). Seleziona **Infinite call duration (Durata infinita chiamata)** se non vuoi porre un limite alla lunghezza di una chiamata.

Porte

Un numero di porta deve essere compreso tra 1024 e 65 535.

- **Porta SIP**: La porta di rete utilizzata per la comunicazione SIP. Il traffico di segnalazione tramite la porta non viene crittografato. Il numero di porta predefinito è 5060. Se necessario, inserire un numero di porta differente.
- **Porta TLS**: La porta di rete utilizzata per la comunicazione SIP codificata. Il traffico di segnalazione attraverso la porta viene crittografato tramite TLS (Transport Layer Security). Il numero di porta predefinito è 5061. Se necessario, inserire un numero di porta differente.
- **Porta di avvio RTP**: porta di rete utilizzata per il primo flusso multimediale RTP in una chiamata SIP. Il numero di porta per l'inizio predefinito è 4000. Alcuni firewall bloccano il traffico RTP su determinati numeri di porta.

NAT Traversal

Utilizzare l'attraversamento NAT (Network Address Translation) quando il dispositivo si trova in una rete privata (LAN) e si desidera renderlo disponibile al di fuori di tale rete.

Nota

Affinché funzioni, l'attraversamento NAT deve essere supportato dal router. Il router inoltre deve supportare UPnP®.

Ciascun protocollo NAT traversal può essere utilizzato separatamente o in combinazioni differenti a seconda dell'ambiente di rete.

- **ICE**: Il protocollo ICE (Interactive Connectivity Establishment) aumenta la possibilità di trovare il percorso più efficiente per la corretta comunicazione tra i dispositivi associati. Se si abilitano anche STUN e TURN, tali possibilità migliorano ulteriormente.
- **STUN**: STUN (Session Traversal Utilities for NAT) è un protocollo di rete client-server che consente al dispositivo di determinare se si trova dietro un protocollo NAT o un firewall e, se così, ottenere l'indirizzo IP pubblico mappato e il numero di porta assegnato per le connessioni a host remoti. Inserire un indirizzo server STUN, ad esempio un indirizzo IP.
- **TURN**: TURN (Traversal Using Relays around NAT) è un protocollo che consente a un dispositivo dietro un router NAT o un firewall di ricevere i dati in entrata da altri host su TCP o UDP. Inserire l'indirizzo server TURN e le informazioni di login.

Audio e video

- **Audio codec priority (Priorità codec audio)**: Selezionare almeno un codec audio con la qualità audio desiderata per le chiamate SIP. Trascina e rilascia per modificare la priorità.

Nota

I codec selezionati devono corrispondere al codec del destinatario della chiamata, dal momento che il codec del destinatario è determinante quando si effettua una chiamata.

- **Audio direction (Direzione dell'audio)**: Seleziona le direzioni audio consentite.
- **H.264 packetization mode (Modalità di pacchettizzazione H.264)**: Seleziona quale modalità di pacchettizzazione usare.

  - **Automatico**: (Consigliato) Il dispositivo decide la modalità di pacchettizzazione da usare.
  - **None (Nessuno)**: Non è impostata alcuna modalità di pacchettizzazione. Questa modalità è spesso interpretata come modalità **0**.
  - **0**: Modalità non interfogliata.
  - **1**: Modalità unità NAL singola.
- **Direzione del video**: Seleziona le direzioni video consentite.
- **Mostra video nella chiamata** : Mostra il flusso video in arrivo sul display del dispositivo.

Aggiuntivo

- **UDP-to-TCP switching (Passaggio da UDP a TCP)**: Seleziona per consentire alle chiamate di scambiare temporaneamente i protocolli di trasporto da UDP (User Datagram Protocol) a TCP (Transmission Control Protocol). La ragione per il passaggio è evitare la frammentazione e il passaggio può essere eseguito se una richiesta rientra nei 200 byte del parametro MTU (Maximum Transmission Unit) o supera i 1300 byte.
- **Allow via rewrite (Consenti tramite riscrittura)**: Seleziona per inviare l'indirizzo IP locale e non l'indirizzo IP pubblico del router.
- **Allow contact rewrite (Consenti riscrittura contatto)**: Seleziona per inviare l'indirizzo IP locale e non l'indirizzo IP pubblico del router.
- **Register with server every (Registra con il server ogni)**: Consente di impostare la frequenza con cui si desidera che il dispositivo registri con il server SIP per gli account SIP esistenti.
- **DTMF payload type (Tipo payload DTMF)**: Modifica il tipo di payload predefinito per DTMF.
- **Max retransmissions (Massimo numero di ritrasmissioni)**: Imposta il numero massimo di volte in cui il dispositivo tenta di connettersi al server SIP prima di smettere di provare.
- **Seconds until failback (Secondi fino al failback)**: Imposta il numero di secondi entro i quali il dispositivo tenta di riconnettersi al server SIP primario dopo aver effettuato il failover su un server SIP secondario.

Account

Tutti gli account SIP correnti sono elencati sotto **SIP accounts (Account SIP)**. Per gli account registrati, il cerchio colorato consente di conoscerne lo stato.

L'account viene registrato con successo con il server SIP.

È stato riscontrato un problema con l'account. Tra le possibili cause possono esserci la mancata autorizzazione, errate credenziali dell'account o impossibilità per il server SIP di trovare l'account.

L'account **peer to peer (default) (Peer-to-peer (predefinito))** è un account creato automaticamente. È possibile eliminarlo se si crea almeno un altro account e lo si imposta come predefinito. L'account predefinito viene sempre utilizzato quando si effettua una chiamata API (interfaccia per la programmazione di applicazioni) VAPIX® senza specificare da quale account SIP effettuare la chiamata.

Add account (Aggiungi account): Fai clic per creare un nuovo account SIP.

- **Active (Attivo)**: selezionare questa opzione per poter utilizzare l'account.
- **Make default (Imposta come predefinito)**: selezionare questa opzione per impostare l'account in questione come predefinito. Deve essere presente un account predefinito e può essercene uno solo.
- **Answer automatically (Risposta automatica)**: Selezionare questa opzione per rispondere automaticamente a una chiamata in entrata.
- **Prioritize IPv6 over IPv4 (assegnare le priorità a iPv6 rispetto a IPv4)** : selezionare questa opzione per dare la priorità agli indirizzi IPv6 rispetto agli indirizzi IPv4. Ciò è utile quando ci si connette ad account peer-to-peer o a nomi di dominio che vengono risolti in indirizzi IPv4 e IPv6. È possibile dare la priorità agli indirizzi IPv6 solo per i nomi di dominio mappati su indirizzi IPv6.
- **Nome**: Immettere un nome descrittivo. Ciò può essere, ad esempio, il nome e il cognome, un ruolo o una posizione. Il nome non è univoco.
- **ID utente**: immettere il numero di telefono o estensione univoci assegnati al dispositivo.
- **Peer-to-peer**: utilizzare questo account per le chiamate dirette a un altro dispositivo SIP nella rete locale.
- **Registrato**: utilizzare questo account per le chiamate a dispositivi SIP al di fuori della rete locale, tramite un server SIP.
- **Domain (Dominio)**: se disponibile, immettere il nome dominio pubblico. Tale nome verrà visualizzato come parte dell'indirizzo SIP durante la chiamata ad altri account.
- **Password**: Immettere la password associata con l'account SIP per effettuare l'autenticazione sul server SIP.
- **ID di autenticazione**: immettere l'ID autenticazione utilizzato per l'autenticazione al server SIP. Se è lo stesso dell'ID utente, non è necessario immettere l'ID autenticazione.
- **ID chiamante**: nome indicato al destinatario delle chiamate dal dispositivo.
- **Registrar**: immettere l'indirizzo IP per l'account registrar.
- **Modalità di trasporto**: Selezionare la modalità di trasporto SIP per l'account: UPD, TCP o TLS.
- **TLS version (Versione TLS)** (solo con modalità di trasporto TLS): Selezionare la versione di TLS da utilizzare. Le versioni **v1.2** e **v1.3** sono le più sicure. **Automatic (Automatica)** seleziona la versione più sicura che il sistema può gestire.
- **Media encryption (Codifica media)** (solo con modalità di trasporto TLS): selezionare il tipo di codifica dei supporti (audio e video) nelle chiamate SIP.
- **Certificate (Certificato)** (solo con modalità di trasporto TLS): selezionare un certificato.
- **Verify server certificate (Verifica certificato server)** (solo con modalità di trasporto TLS): selezionare questa opzione per verificare il certificato server.
- **Secondary SIP server (Server SIP secondario)**: attiva se vuoi che il dispositivo tenti di registrare su un server SIP secondario in caso di errore di registrazione sul server SIP principale.

- **SIP secure (SIP sicuro)**: selezionare questa opzione per utilizzare SIPS (Secure Session Initiation Protocol). SIPS utilizza la modalità di trasporto TLS per codificare il traffico.
- **Proxy**
  - **Proxy**: fare clic sull'opzione per aggiungere un proxy.
  - **Prioritize (Dai priorità)**: se sono stati aggiunti due o più proxy, fare clic per assegnare la relativa priorità.
  - **Server address (Indirizzo server)**: immettere l'indirizzo IP del server proxy SIP.
  - **Username (Nome utente)**: se richiesto, immettere il nome utente per il server proxy SIP.
  - **Password**: se necessario, immettere la password per il server proxy SIP.
- **Video**
  - **View area (Area di visione)**: selezionare l'area di visione da utilizzare per le chiamate video. Se si seleziona Nessuna, viene utilizzata la visualizzazione nativa.
  - **Risoluzione**: selezionare la risoluzione da utilizzare per le chiamate video. La risoluzione influisce sulla larghezza di banda necessaria.
  - **Frequenza dei fotogrammi**: selezionare il numero di fotogrammi al secondo per le chiamate video. La velocità in fotogrammi influisce sulla larghezza di banda necessaria.
  - **Profilo H.264**: selezionare il profilo da utilizzare per le chiamate video.

DTMF

Add sequence (Aggiungi sequenza): Fare clic per creare una nuova sequenza DTMF (Dual-Tone Multifrequency). Per creare una regola che viene attivata dal tono di tocco, andare a **Events > Rules (Eventi > Regole)**.

Sequenza: inserire i caratteri per attivare la regola. I caratteri consentiti sono: 0–9, A-D, # e *.

Description (Descrizione): inserire una descrizione dell'azione da attivare attraverso la sequenza.

Accounts (Account): Selezionare gli account che utilizzeranno la sequenza DTMF. Se si sceglie **peer-to-peer**, tutti gli account peer-to-peer condivideranno la stessa sequenza DTMF.

Protocolli

Selezionare i protocolli da utilizzare per ogni account. Tutti gli account peer-to-peer condividono le stesse impostazioni di protocollo.

Use RTP (RFC2833) (Usa RTP (RFC2833)): attivare questa opzione per consentire la segnalazione DTMF (Dual-Tone Multi-Frequency), altri segnali di suono ed eventi di sistemi di telefonia in pacchetti RTP.

Use SIP INFO (RFC2976) (Usa SIP INFO (RFC2976)): attivare questa opzione per includere il metodo INFO nel protocollo SIP. Il metodo INFO consente di aggiungere informazioni opzionali sul livello dell'applicazione, in genere correlate alla sessione.

Chiamata di prova

Account SIP: Seleziona da quale account eseguire la chiamata di prova.

Indirizzo SIP: Immettere un indirizzo SIP e fare clic su per effettuare una chiamata di test e verificare il funzionamento dell'account.

Elenco di accessi

Use access list (Usa elenco di accesso): attivare per limitare le persone che possono effettuare chiamate al dispositivo.

Policy (Criteri):

- **Allow (Consenti)**: selezionare questa opzione per consentire le chiamate in entrata solo dalle origini incluse nell'elenco di accesso.
- **Block (Blocca)**: selezionare questa opzione per bloccare le chiamate in entrata dalle origini incluse nell'elenco di accesso.

Add source (Aggiungi sorgente): fare clic per creare una nuova voce nell'elenco di accesso.

SIP source (Sorgente SIP): inserire l'ID del chiamante o l'indirizzo del server SIP della sorgente.

Chiamate

Pulsante di chiamata

Use call button (Utilizza il tasto di chiamata): attivare per permettere l'uso del pulsante di chiamata.

Button functionality during a call (Funzionalità dei tasti durante una chiamata): Selezionare la funzionalità del pulsante di chiamata una volta avviata una chiamata dal dispositivo.

- **End the call (Termina la chiamata)**: Quando un visitatore preme il pulsante di chiamata durante una chiamata in uscita, la chiamata termina. Utilizzare questa opzione per consentire ai visitatori di terminare una chiamata in qualsiasi momento.
- **No functionality until the call has ended (Nessuna funzionalità fino al termine della chiamata)**: Quando un visitatore preme il pulsante di chiamata durante una chiamata in uscita, non accade nulla. Utilizzare questa opzione per vietare ai visitatori di terminare le chiamate.
- **Delay before you can end the call (Ritardo prima di poter terminare la chiamata)**: Quando un visitatore preme il pulsante di chiamata entro il tempo impostato in **Delay (seconds) Ritardo (secondi)** dopo aver avviato una chiamata, non succede nulla. Se il tempo di ritardo è trascorso, premendo il tasto di chiamata si termina la chiamata. Utilizzare questa opzione per evitare che i visitatori terminino accidentalmente le chiamate a causa di una doppia pressione.
  - **Delay (seconds) Ritardo (secondi)**: inserire il tempo che deve trascorrere prima che una seconda pressione del tasto di chiamata faccia terminare la chiamata.

Standby light (Luce di stand-by): selezionare un'opzione per la luce integrata attorno al pulsante di chiamata.

- **Auto (Automatico)** : il dispositivo accende e spegne la luce integrata sulla base della luminosità circostante.
- **On**: quando il dispositivo si trova nella modalità stand-by, la luce integrata è sempre accesa.
- **Off (Disattivato)**: quando il dispositivo si trova nella modalità stand-by, la luce integrata è sempre spenta.

Recipients (Destinatari): seleziona o crea uno o molteplici contatti da chiamare quando viene premuto il pulsante di chiamata. Se aggiungi molteplici destinatari, la chiamata sarà eseguita verso tutti in contemporanea. Il numero massimo di destinatari della chiamata SIP è sei, mentre si può disporre di un numero illimitato di destinatari di chiamata VMS.

Fallback: Aggiungi un contatto di fallback dalla lista nell'eventualità che nessuno dei destinatari risponda.

Generale

Audio

Nota

- La clip audio selezionata è riprodotta unicamente quando si esegue una chiamata.
- Se modifichi la clip audio o il guadagno durante una chiamata in corso, la modifica non ha effetto fino alla chiamata successiva.

Ringtone (Suoneria): selezionare la clip audio da riprodurre quando qualcuno chiama il dispositivo. Utilizzare il cursore per regolare il guadagno.

Ringback tone (Tono di ringback): selezionare la clip audio da riprodurre quando qualcuno chiama dal dispositivo. Utilizzare il cursore per regolare il guadagno.

chiamate VMS

chiamate VMS

Allow calls in the video management software (VMS) (Consenti chiamate nel Software per la gestione video (VMS)): selezionare per consentire le chiamate dal dispositivo al VMS. È possibile effettuare chiamate VMS anche se il SIP è disattivo.

Timeout chiamata: impostare la durata massima di un tentativo di chiamata in mancanza di risposta.

Analitiche

Configurazione metadati

Produttori metadati RTSP

Visualizzare e gestire i canali di dati che trasmettono metadati e i canali che utilizzano.

Nota

Queste impostazioni riguardano il flusso di metadati RTSP che utilizza ONVIF XML. Le modifiche apportate qui non influiscono sulla pagina di visualizzazione dei metadati.

Producer (Produttore): Un canale dati che utilizza il Real-Time Streaming Protocol (RTSP) per inviare metadati.

Canale: Il canale utilizzato per inviare metadati da un produttore. Selezionare per abilitare il flusso di metadati. Deselezionare per ragioni di compatibilità o gestione delle risorse.

MQTT

Configurare i produttori che generano e trasmettono metadati tramite MQTT (Message Queuing Telemetry Transport).

- **Create (Crea)**: Fare clic per creare un nuovo produttore MQTT.
  - **Key** (Chiave): Selezionare un identificatore predefinito dall'elenco a discesa per specificare l'origine del flusso di metadati.
  - **MQTT topic** (Argomento MQTT): Inserire un nome per l'argomento MQTT.
  - **QoS (Quality of Service)** (Qualità del servizio): Impostare il livello di garanzia di consegna dei messaggi (0-2).

Retain messages (Conserva i messaggi): Scegliere se conservare l'ultimo messaggio sull'argomento MQTT.

Use MQTT client device topic prefix (Utilizzare prefisso argomento dispositivo client MQTT): Scegliere se aggiungere un prefisso all'argomento MQTT per aiutare a identificare il dispositivo di origine.

Il menu contestuale contiene:

- **Update (Aggiorna)**: Modificare le impostazioni del produttore selezionato.
- **Elimina**; Eliminare il produttore selezionato.

Object snapshot (Istantanea dell'oggetto): Attivare per includere un'immagine ritagliata di ogni oggetto rilevato.

Additional crop margin (Margine di ritaglio aggiuntivo): Attivare per aggiungere un ulteriore margine intorno alle immagini ritagliate degli oggetti rilevati.

Lettore

Connessione

Lettore esterno (ingresso)

Use external OSDP reader (Utilizza lettore OSDP esterno): accendere per utilizzare il dispositivo con un lettore esterno. Collegare il lettore al connettore del lettore (IO1, IO2, 12V e GND).

Status (Stato):
- **Connected (Collegato)**: il dispositivo è collegato al lettore esterno attivo.
- **Connecting (Connessione in corso)**: il dispositivo sta tentando di connettersi al lettore esterno.
- **Not connected (Non collegato)**: OSDP è disattivo.

Protocollo lettore

Reader protocol type (Tipo di protocollo lettore): Seleziona il protocollo da usare per la funzione lettore.

- **VAPIX reader (Lettore VAPIX)**: Si può usare solo con un door controller Axis.
  - **Protocol (Protocollo)**: Seleziona **HTTPS** o **HTTP**.
  - **Door controller address (Indirizzo door controller)**: Inserire l'indirizzo IP per il door controller.
  - **User name (Nome utente)**: inserisci il nome utente del door controller.
  - **Password**: inserisci la password del door controller.
  - **Connect (Connetti)**: Fare clic su per connetterti al door controller.
  - **Select reader (Seleziona lettore)**: Selezionare il lettore di ingresso per la porta appropriata.
- **OSDP**:
  - **OSDP address (Indirizzo OSDP)**: Inserire l'indirizzo del lettore OSDP. 0 è l'indirizzo predefinito e più comune per i lettori singoli.
- **Wiegand** :
  - **Beeper (Avvisatore acustico)**: attivalo per attivare l'ingresso dell'avvisatore acustico.
  - **Input for beeper (Ingresso per avvisatore acustico)**: selezionare la porta I/O usata per l'avvisatore acustico.
  - **Input used for LED control (Ingresso usato per il comando LED)**: seleziona quante porte I/O usare per il controllo del feedback LED sul dispositivo.
  - **Input per LED1/LED2 (Ingresso LED1/LED2)**: selezionare le porte I/O da utilizzare per l'ingresso LED.
  - **Idle color (Colore inattività)**: Se nessuna porta I/O per è usata per il controllo di LED, puoi selezionare un colore statico da visualizzare sull'indicatore del lettore di tessere.
  - **Color for state low/high (Colore per stato basso/alto)**: se una porta I/O viene usata per il controllo LED, selezionare il colore da mostrare rispettivamente per lo stato basso o alto.
  - **Idle color/LED1 color/LED2 color/LED1 + LED2 color (Colore inattività/Colore LED1/Colore LED2/Colore LED1 + LED2)**: Se due porte I/O sono usate per il controllo LED, seleziona i colori da mostrare rispettivamente per inattività, LED1, LED2 e LED1 + LED2.
  - **Keypress format (Formato pressione)**: selezionare il formato del PIN quando è inviato all'unità di controllo degli accessi.
    - **FourBit (Quattro bit)**: il PIN `1234` viene codificato e inviato come 0x1 0x2 0x3 0x4. Questo è il comportamento predefinito e più comune.
    - **EightBitZeroPadded (Otto bit zero compensazione)**: il PIN `1234` viene codificato e inviato come 0x01 0x02 0x03 0x04.
    - **EightBitInvertPadded (Otto bit compensazione inversa)**: il PIN `1234` viene codificato e inviato come 0xE1 0xD2 0xC3 0xB4.
    - **Wiegand26**: il PIN viene codificato nel formato Wiegand26 con un codice struttura da 8 bit e un ID da 16 bit.
    - **Wiegand34**: il PIN viene codificato nel formato Wiegand34 con un codice struttura da 16 bit e un ID da 16 bit.
    - **Wiegand37**: il PIN è codificato in un formato Wiegand37 (H10302) con id da 35 bit.
    - **Wiegand37FacilityCode (Codice struttura Wiegand37)**: il PIN viene codificato nel formato Wiegand37 (H10304) con un codice struttura da 16 bit e un ID da 19 bit.
  - **Facility code (Codice struttura)**: Immetti il codice struttura da inviare. Questa opzione è a disposizione solo per alcuni formati pressione.

Formato di output

Select data format (Seleziona formato dati): selezionare in che formato mandare i dati della tessera all'unità di controllo degli accessi.

- **Raw (Non elaborati)**: trasmette i dati della tessera inalterati.
- **Wiegand26**: codifica i dati della scheda nel formato Wiegand26 con un codice struttura da 8 bit e un ID da 16 bit.
- **Wiegand34**: codifica i dati della scheda nel formato Wiegand34 con un codice struttura da 16 bit e un ID da 16 bit.
- **Wiegand37**: codifica i dati della tessera in formato Wiegand37 (H10302) con un ID da 35 bit.
- **Wiegand37FacilityCode (Codice struttura Wiegand37)**: codifica i dati della scheda nel formato Wiegand37 (H10304) con un codice struttura da 16 bit e un ID da 19 bit.
- **Personalizzato**: definisci il tuo formato personalizzato.

Facility code override mode (Modalità di sovrascrizione del codice struttura): selezionare un'opzione per la sovrascrizione del codice struttura.

- **Automatico**: non esegue la sovrascrizione del codice della struttura e creare un codice struttura dal rilevamento automatico dai dati in ingresso. Usa il codice struttura originale della tessera o lo crea da bit in eccesso di un codice carta.
- **Optional (Opzionale)**: usa il codice struttura dai dati in ingresso o sovrascrive con un valore facoltativo configurato.
- **Override (Sovrascrizione)**: esegue sempre la sovrascrizione con un codice struttura specificato.

PIN

Le impostazioni del PIN devono corrispondere a quelle configurate nell'unità di controllo degli accessi.

Length (Lunghezza) (0–32): inserire il numero di cifre del PIN. Se agli utenti non è richiesto l'uso di un PIN quando utilizzano il lettore, impostare la lunghezza su 0.

Timeout (seconds, 3–50) (Timeout (secondi, 3–50)): immettere il numero di secondi che devono trascorrere prima che il dispositivo torni alla modalità inattiva quando non viene ricevuto alcun PIN.

Elenco delle voci

Con l'elenco delle voci è possibile configurare il dispositivo per consentire ai titolari credenziali di utilizzare la propria tessera o PIN o un codice QR® per eseguire diverse azioni, come l'apertura di una porta. Le credenziali vengono archiviate localmente nel dispositivo. È inoltre possibile combinare questa funzionalità con un door controller esterno.

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

Titolari credenziali

Use Entry list (Usa elenco delle voci): attivare questa opzione per usare la funzionalità Elenco delle voci.

Use connected door controller (Usa il door controller connesso): attivare questa opzione se il dispositivo è già collegato a un door controller. Se qualcuno presenta credenziali inesistenti nell'elenco delle voci, la richiesta viene inviata al door controller connesso. Le credenziali disponibili nell'elenco delle voci non vengono inviate.

Add credential holder (Aggiungi titolare credenziali): fare clic su questa opzione per aggiungere un nuovo titolare credenziali.

First name (Nome): inserire un nome.

Last name (Cognome): inserire un cognome.

Credential type (Tipo di credenziali):

- **PIN**:
  - **PIN**: inserire un PIN univoco o fare clic su **Generate (Genera)** per crearne uno automaticamente.
- **Card (Tessera)**:
  - **UID**: inserire l'UID e la lunghezza in bit della tessera oppure fare clic su **Get latest (Ottieni l'ultimo)** per recuperare i dati dall'ultimo passaggio della tessera.
- **Codice QR®**

Event condition (Condizione evento): selezionare una o più condizioni da attivare quando il titolare credenziali utilizza le proprie credenziali. Per impostare l'azione risultante, andare a **System > Events (Sistema > Eventi)** e creare una regola, utilizzando la stessa condizione selezionata.

Valid from (Valido da): selezionare **Current device time (Ora attuale dispositivo)** per attivare immediatamente le credenziali. Deselezionare per specificare quando attivare le credenziali.

Valid to (Valido fino al):

- **No end date (Nessuna data di fine)**: le credenziali sono sempre valide.
- **End date (Data di fine)**: specificare la data e l'ora di fine validità delle credenziali.
- **Number of times (Numero di volte)**: specificare quante volte il titolare credenziali può utilizzare le credenziali. Il valore nel campo si riduce man mano che le credenziali vengono utilizzate, per mostrare gli usi rimanenti.

Note: inserire informazioni facoltative.

Suspend (Sospendi): selezionare per rendere le credenziali temporaneamente non valide.

Download QR Code when saving (Scaricare il codice QR quando si salva): Se è stato selezionato Codice QR come tipo di credenziale, selezionare questa casella di controllo per scaricare il codice QR quando si fa clic su **Save (Salva)**.

Registro eventi

Il registro eventi mostra un elenco di eventi dell'elenco voci. Le dimensioni massime del file di accesso sono di 2 MB, pari a circa 6000 eventi.

Export all (Esporta tutti): fare clic su per esportare tutti gli eventi dell'elenco. Per esportare solo un sottoinsieme, selezionare gli eventi che interessano. Gli eventi vengono esportati in un file CSV.

Filtro: Fare clic su per mostrare gli eventi verificatisi in un intervallo di tempo specifico.

: digitare per cercare tutti i contenuti corrispondenti nell'elenco.

Audio

Impostazioni dispositivo

Input: Attivare o disattivare l'ingresso audio. Mostra il tipo di input.

Input type (Tipo di ingresso) : selezionare il tipo di input, ad esempio se si tratta di microfono interno o ingresso linea.

Power type (Tipo di alimentazione) : Selezionare il tipo di alimentazione per l'input.

Apply changes (Applica modifiche) : applicare la selezione.

Noise cancellation (Cancellazione del rumore): attivare per migliorare la qualità dell'audio rimuovendo il rumore di fondo.

Echo cancellation (Cancellazione eco) : Attiva per la rimozione dell'eco nel corso della comunicazione bidirezionale.

Separate gain controls (Controlli del guadagno separati) : Attiva per regolare il guadagno in modo separato per i diversi tipi di input.

Automatic gain control (Controllo automatico del guadagno) : Attiva per adattare dinamicamente il guadagno alle modifiche del suono.

Gain (Guadagno): Utilizzare il cursore per modificare il guadagno. Fare clic sull'icona del microfono per disattivare o attivare l'audio.

Output: Mostra il tipo di output.

Gain (Guadagno): Utilizzare il cursore per modificare il guadagno. Fai clic sull'icona dell'altoparlante per disattivare o attivare l'audio.

Controllo automatico del volume : Attivare per fare in modo che il dispositivo regoli automaticamente e dinamicamente il guadagno in base al livello di rumore ambientale. Il controllo automatico del volume influisce su tutte le uscite audio, comprese linea e telecoil.

Flusso

Codifica: selezionare la codifica da usare per il flusso di sorgente input. È possibile scegliere la codifica solo se l'ingresso audio è attivato. Se l'ingresso audio è disattivato, fare clic su **Enable audio input (Abilita input audio)** per attivarlo.

Clip audio

Add clip (Aggiungi clip): aggiungi una nuova clip audio. Puoi usare file .au, .mp3, .opus, .vorbis, .wav.

Riproduci la clip audio.

Interrompi riproduzione della clip audio.

Il menu contestuale contiene:

- **Rename (Rinomina)**: Modificare il nome della clip audio.
- **Create link (Crea collegamento)**: creare un URL che, quando usato, riproduce la clip audio sul dispositivo. Specifica il volume e il numero di riproduzioni della clip.
- **Download (Scarica)**: Scarica la clip audio sul tuo computer.
- **Elimina**; Elimina la clip audio dal dispositivo.

Registrazioni

Registrazioni in corso: mostra tutte le registrazioni in corso sul dispositivo.

Avvia una registrazione sul dispositivo.

Scegli il dispositivo di archiviazione in cui salvare.

Arresta una registrazione sul dispositivo.

Le registrazioni attivate termineranno in caso di arresto manuale o in caso di spegnimento del dispositivo.

Le registrazioni continue continueranno fino all'arresto manuale. Anche se il dispositivo si arresta, la registrazione prosegue quando il dispositivo si avvia nuovamente.

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. Notare che se si lavora in un fuso orario diverso rispetto alla posizione del dispositivo, l'intervallo di tempo si basa sul fuso orario del dispositivo.

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 (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 CA NTS KE affidabili)**: Selezionare i certificati CA attendibili da utilizzare per la sincronizzazione temporale sicura di NTS KE, oppure lasciare l'opzione nessuno.
  - **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.

Ubicazione dei dispositivi

Immettere la posizione del dispositivo. Il sistema di gestione video può utilizzare queste informazioni per posizionare il dispositivo su una mappa.

- **Latitude (Latitudine)**: i valori positivi puntano a nord dell'equatore.
- **Longitude (Longitudine)**: i valori positivi puntano a est del primo meridiano.
- **Heading (Intestazione)**: Immettere la direzione della bussola verso cui è diretto il dispositivo. 0 punta a nord.
- **Label (Etichetta)**: Inserire un nome descrittivo per il proprio dispositivo.
- **Save (Salva)**: Fare clic per salvare la posizione del dispositivo.

Controllo configurazione

Immagine dispositivo interattiva: Fai clic sui pulsanti nell'immagine per simulare pressioni di tasti reali. Questo ti permette di provare le configurazioni o risolvere eventuali problemi dell'hardware senza accedere fisicamente al dispositivo.

Latest credentials (Credenziali più recenti) : Mostra informazioni sulle ultime credenziali registrate.

Visualizzare i dati delle credenziali più recenti.

Il menu contestuale contiene:

- **Reverse UID (Inverti UID)**: inverte l'ordine dei byte dell'UID.
- **Revert UID (Ripristina UID)**: riporta l'ordine dei byte dell'UID a quello originale.
- **Copy to clipboard (Copia negli appunti)**: copia l'UID.

Check credentials (Controlla le credenziali) : immettere un UID o un PIN e inoltrare per controllare le credenziali. Il sistema risponderà nello stesso modo in cui avrebbe fatto se le credenziali fossero state utilizzate sul dispositivo. Se sono necessari sia UID che PIN, iniziare inserendo l'UID.

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'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.
  - **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+) (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

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 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.

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.

Configurazione OpenID

Importante

Se non è possibile utilizzare OpenID per eseguire l'accesso, utilizzare le credenziali Digest o Basic utilizzate quando è stato configurato OpenID per eseguire l'accesso.

Client ID (ID client): inserire il nome utente OpenID.

Outgoing Proxy (Proxy in uscita): inserire l'indirizzo proxy che può essere utilizzato dalla connessione OpenID.

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

Provider URL (URL provider): inserire il collegamento Web per l'autenticazione dell'endpoint API. Il formato deve https://[inserire URL]/.well-known/openid-configuration

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.

Remote user (Utente remoto): inserire un valore per identificare gli utenti remoti. In questo modo sarà possibile visualizzare l'utente corrente nell'interfaccia Web del dispositivo.

Scopes (Ambiti): Ambiti opzionali che potrebbero far parte del token.

Client secret (Segreto client): inserire la password OpenID

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

Enable OpenID (Abilita OpenID): attivare per chiudere la connessione corrente e consentire l'autenticazione del dispositivo dall'URL del provider.

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.

Sovrapposizioni testo MQTT

Nota

Connetti a un broker MQTT prima dell'aggiunta dei campi di modifica di sovrapposizione testo MQTT.

Add overlay modifier (Aggiungi campo di modifica per sovrapposizione testo): Fare clic per l'aggiunta di un nuovo campo di modifica di sovrapposizione testo.

Topic filter (Filtro argomenti): Aggiungi l'argomento MQTT contenente i dati che vuoi mostrare nella sovrapposizione testo.

Data field (Campo dati): Specifica la chiave per il payload del messaggio che vuoi visualizzare nella sovrapposizione testo, purché il messaggio sia in formato JSON.

Modifier (Campo di modifica): Usa il campo di modifica risultante quando crei la sovrapposizione testo.

- I campi di modifica che cominciano con **#XMP** mostrano tutti i dati ricevuti dall'argomento.
- I campi di modifica che cominciano con **#XMD** mostrano i dati specificati nel campo dati.

Archiviazione

Archiviazione di rete

Ignore (Ignora): Attiva per ignorare l'archiviazione di rete.

Add network storage (Aggiungi archiviazione di rete): fare clic su questa opzione per eseguire l'aggiunta di una condivisione di rete nella quale poter salvare le registrazioni.

- **Indirizzo**: Inserire l'indirizzo IP o il nome host del server host, generalmente NAS (Network Attached Storage). Si consiglia di configurare l'host per utilizzare un indirizzo IP fisso (non DHCP perché un indirizzo IP dinamico potrebbe cambiare) o di utilizzare DNS. I nomi Windows SMB/CIFS non sono supportati.
- **Network share (Condivisione di rete)**: Inserire il nome dell'ubicazione condivisa nel server host. Diversi dispositivi Axis possono utilizzare la stessa condivisione di rete dal momento che ogni dispositivo ha una propria cartella.
- **User (Utente)**: inserire il nome utente se serve eseguire il login per il server. Digitare `DOMAIN\username` per accedere a un server di dominio specifico.
- **Password**: Immetti la password se serve eseguire il login per il server.
- **SMB version (Versione SMB)**: Seleziona la versione del protocollo di archiviazione SMB da collegare al NAS. Se selezioni **Auto (Automatico)**, il dispositivo cerca di negoziare una delle versioni sicure SMB: 3.02, 3.0, o 2.1. Seleziona 1.0 o 2.0 per la connessione a NAS meno recenti che non sono dotati di supporto per versioni superiori. Puoi leggere maggiori dettagli sul supporto SMB nei dispositivi Axis *qui*.
- **Add share without testing (Aggiungi condivisione senza test)**: seleziona questa opzione per eseguire l'aggiunta della condivisione di rete a prescindere dal rilevamento di un errore durante il test della connessione. Ad esempio, l'errore può consistere nel non aver inserito una password nonostante sia necessaria per il server.

Remove network storage (Rimuovi archiviazione di rete): Fare clic su questa opzione per smontare, disassociare ed eseguire la rimozione della connessione alla condivisione di rete. Ciò elimina ogni impostazione per la condivisione di rete.

Unbind (Disassocia): fare clic per annullare l'associazione e scollegare la condivisione di rete.
Bind (Associa): Fare clic per associare e connettere la condivisione di rete.

Unmount (Smonta): Fare clic per smontare la condivisione di rete.
Mount (Monta): Fare clic su questa opzione per montare la condivisione di rete.

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

Retention time (Tempo di conservazione): Selezionare il periodo di conservazione delle registrazioni in modo da porre un limite al numero di vecchie registrazioni od ottemperare alle normative in merito alla conservazione dei dati. Le registrazioni precedenti sono cancellate prima della scadenza del periodo selezionato se l'archiviazione di rete diventa piena.

Strumenti

- **Test connection (Verifica connessione)**: Verifica la connessione alla condivisione di rete.
- **Format (Formatta)**: Formattare la condivisione di rete, ad esempio quando è necessario cancellare rapidamente tutti i dati. CIFS è l'opzione del file system disponibile.

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

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.

Profili di flusso

Un profilo di streaming è un gruppo di impostazioni che incidono sul flusso video. Puoi usare i profili di streaming in situazioni diverse, ad esempio quando crei eventi e usi regole per registrare.

Add stream profile (Aggiungi profilo di streaming): Fare clic per creare un nuovo profilo di streaming.

Preview (Anteprima): Un'anteprima del flusso video con le impostazioni del profilo di streaming che selezioni. L'anteprima si aggiorna quando cambi le impostazioni nella pagina. Se il dispositivo ha aree di visione diverse, puoi cambiare l'area di visione nell'elenco a discesa nell'angolo in basso a sinistra dell'immagine.

Nome: aggiungi un nome per il tuo profilo.

Description (Descrizione): aggiungi una descrizione del tuo profilo.

Video codec (Codec video): selezionare il codec video che va applicato al profilo.

Risoluzione: Consulta per vedere una descrizione di questa impostazione.

Frequenza dei fotogrammi: Consulta per vedere una descrizione di questa impostazione.

Compressione: Consulta per vedere una descrizione di questa impostazione.

Zipstream : Consulta per vedere una descrizione di questa impostazione.

Optimize for storage (Ottimizza per archiviazione) : Consulta per vedere una descrizione di questa impostazione.

Dynamic FPS (FPS dinamico) : Vedere per una descrizione di questa impostazione.

Dynamic GOP (GOP dinamico) : Vedere per una descrizione di questa impostazione.

Mirror (Specularità) : Consulta per vedere una descrizione di questa impostazione.

GOP length (Lunghezza GOP) : Consulta per vedere una descrizione di questa impostazione.

Bitrate control (Controllo velocità di trasmissione): Consulta per vedere una descrizione di questa impostazione.

Include overlays (Includi sovrapposizioni) : Selezionare il tipo di sovrapposizione da includere. Consulta per informazioni su come aggiungere sovrapposizioni.

Include audio (Includi audio) : Consulta per vedere una descrizione di questa impostazione.

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.

Profili di supporti ONVIF

Un profilo di supporti ONVIF è costituito da una serie di configurazioni utilizzabili per modificare le impostazioni di flusso dei supporti. Puoi creare nuovi profili con il tuo set di configurazioni o utilizzare profili preconfigurati per una configurazione rapida.

Aggiungere profilo multimediale: Fare clic per aggiungere un nuovo profilo di supporti ONVIF.

Nome profilo: Aggiungi un nome per il profilo multimediale.

Video source (Sorgente video): Seleziona la sorgente video per la tua configurazione.

- **Select configuration (Selezionare configurazione)**: Selezionare una configurazione definita dall'utente dall'elenco. Le configurazioni nell'elenco a discesa corrispondono ai canali video del dispositivo, comprese le multiview, le aree di visione e i canali virtuali.

Video encoder (Codificatore video): Selezionare il formato di codifica video per la tua configurazione.

- **Select configuration (Selezionare configurazione)**: Selezionare una configurazione definita dall'utente dall'elenco e regolare le impostazioni di codifica. Le configurazioni nell'elenco a discesa fungono da identificatori/nomi della configurazione del video encoder. Selezionare l'utente da 0 a 15 per applicare le tue impostazioni oppure selezionare uno degli utenti predefiniti se si desidera utilizzare le impostazioni predefinite per un formato di codifica specifico.

Nota

Abilita l'audio nel dispositivo per avere la possibilità di selezionare una sorgente audio e la configurazione del codificatore audio.

Audio source (Sorgente audio) : Selezionare la sorgente di ingresso audio per la tua configurazione.

- **Select configuration (Selezionare configurazione)**: Selezionare una configurazione definita dall'utente dall'elenco e regolare le impostazioni audio. Le configurazioni nell'elenco a discesa corrispondono agli ingressi audio del dispositivo. Se il dispositivo ha un ingresso audio, è user0. Se il dispositivo dispone di più ingressi audio, nell'elenco saranno presenti altri utenti.

Codificatore audio : Selezionare il formato di codifica audio per la tua configurazione.

- **Select configuration (Selezionare configurazione)**: Selezionare una configurazione definita dall'utente dall'elenco e regolare le impostazioni di codifica audio. Le configurazioni nell'elenco a discesa fungono da identificatori/nomi della configurazione dell'audio encoder.

Decoder audio : Selezionare il formato di codifica audio per la tua configurazione.

- **Select configuration (Selezionare configurazione)**: Selezionare una configurazione definita dall'utente dall'elenco e regolare le impostazioni. Le configurazioni nell'elenco a discesa fungono da identificatori/nomi della configurazione.

Uscita audio : Selezionare il formato di uscita audio per la tua configurazione.

- **Select configuration (Selezionare configurazione)**: Selezionare una configurazione definita dall'utente dall'elenco e regolare le impostazioni. Le configurazioni nell'elenco a discesa fungono da identificatori/nomi della configurazione.

Metadata: Selezionare i metadati da includere nella configurazione.

- **Select configuration (Selezionare configurazione)**: Selezionare una configurazione definita dall'utente dall'elenco e regolare le impostazioni dei metadati. Le configurazioni nell'elenco a discesa fungono da identificatori/nomi della configurazione dei metadati.

PTZ : Selezionare le impostazioni PTZ per la tua configurazione.

- **Select configuration (Selezionare configurazione)**: Selezionare una configurazione definita dall'utente dall'elenco e regolare le impostazioni PTZ. Le configurazioni nell'elenco a discesa corrispondono ai canali video del dispositivo con supporto PTZ.

Create (Crea): Fare clic per salvare le impostazioni e creare il profilo.

Cancel (Annulla): Fare clic per annullare la configurazione e cancellare tutte le impostazioni.

profile_x (profilo_x): Fare clic sul nome del profilo per aprire e modificare il profilo preconfigurato.

Rilevatori

Manomissione telecamera

Il rilevatore di manomissione telecamera genera un allarme quando avviene un cambiamento nella scena, ad es. quando l'obiettivo è coperto, soggetto a spruzzi o ne viene gravemente alterata la relativa messa a fuoco e il tempo in **Trigger delay (Ritardo attivazione)** è trascorso. Il rilevatore di manomissione viene attivato unicamente in caso di mancanza di movimento della telecamera per almeno 10 secondi. Durante questo periodo, tramite il rilevatore viene configurato un modello di scena da utilizzare come confronto per rilevare manomissioni nelle immagini correnti. Per poter configurare correttamente il modello di scena, verificare che la messa a fuoco della telecamera e le condizioni di illuminazione siano corrette e che la telecamera non punti su una scena priva di contorni, ad esempio una parete bianca. La manomissione della telecamera può essere utilizzata come condizione per attivare le azioni.

Trigger delay (Ritardo attivazione): Inserisci il tempo minimo di attività delle condizioni di manomissione che deve trascorrere prima che l'allarme si attivi. In questo modo è possibile evitare falsi allarmi per condizioni note che influiscono sull'immagine.

Trigger on dark images (Attiva sulle immagini scure): È molto difficile generare un allarme quando l'obiettivo della telecamera è soggetto a spruzzi poiché è impossibile distinguere l'evento dalle altre situazioni in cui l'immagine diventa così scura, ad esempio quando cambiano le condizioni di illuminazione. Attivare questo parametro per generare gli allarmi per tutti i casi in cui l'immagine diventa scura. Quando è disattivato, il dispositivo non genera alcun allarme quando l'immagine diventa scura.

Nota

Per il rilevamento di tentativi di manomissione in scene statiche e non affollate.

Rilevamento audio

Queste impostazioni sono disponibili per ogni ingresso audio.

Sound level (Volume sonoro): Regolare il volume sonoro su un valore da 0 a 100, dove 0 è la sensibilità massima e 100 quella minima. Quando si l'imposta il volume sonoro, utilizzare l'indicatore relativo all'attività come riferimento. Quando crei eventi, puoi usare il volume sonoro come condizione. Puoi scegliere di attivare un'azione se il volume sonoro è superiore, inferiore o corrispondente al valore impostato.

Rilevamento degli urti

Shock detector (Rilevatore urti): Attiva per generare un allarme se il dispositivo viene colpito da un oggetto o manomesso.

Sensitivity level (Livello di sensibilità): Sposta il cursore per regolare il livello di sensibilità in base al quale il dispositivo deve generare un allarme. Un valore basso indica che il dispositivo genera un allarme solo se l'urto è potente. Un valore elevato significa che il dispositivo genera un allarme anche solo con un urto di media entità.

Accessori

Porte I/O

Utilizzare l'input digitale per collegare i dispositivi esterni che possono passare da un circuito aperto a un circuito chiuso, ad esempio i sensori PIR, i contatti porta o finestra e i rivelatori di rottura del vetro.

Utilizzare l'uscita digitale per collegare dispositivi esterni come relè e LED. È possibile attivare i dispositivi collegati tramite l'API VAPIX® o l'interfaccia Web.

Porta

Nome: modificare il testo per rinominare la porta.

Usage (Uso): L'opzione predefinita nell'ambito della porta relè è **Door (Porta)**. Per i dispositivi dotati di icone indicatore,  diventa verde quando avviene il cambio di stato e la porta si sblocca. Se si impiega il relè per qualcosa che non sia una porta e non si desidera che l'icona si illumini al momento del cambio di stato, è possibile selezionare una delle altre opzioni per la porta.

Direction:  indica che la porta è una porta di input.  indica che si tratta di una porta di output. Se la porta è configurabile, è possibile fare clic sulle icone per passare dall'input all'output.

Normal state (Stato normale): Fare clic su  per il circuito aperto e su  per il circuito chiuso.

Current state (Stato corrente): indica lo stato attuale della porta. L'input e l'output vengono attivati quando lo stato corrente è diverso dallo stato normale. Un input sul dispositivo ha un circuito aperto se disconnesso o in caso di tensione superiore a 1 VCC.

Nota

Durante il riavvio, il circuito di output è aperto. Al completamento del riavvio, il circuito torna alla posizione normale. Se si modificano le impostazioni in questa pagina, i circuiti di output tornano alle relative posizioni normali, indipendentemente dai trigger attivi.

Supervised (Supervisionato)  : Attivare per rendere possibile il rilevamento e l'attivazione di azioni se qualcuno manomette la connessione ai dispositivi I/O digitali. Oltre a rilevare se un ingresso è aperto o chiuso, è anche possibile rilevare se qualcuno l'ha manomesso (ovvero se è stato tagliato o corto). Per supervisionare la connessione è necessario un ulteriore hardware (resistori terminali) nel loop I/O esterno.

Edge-to-edge

Camera pairing (Associazione telecamera) consente di associare un intercom Axis a una telecamera Axis compatibile, per includere il flusso dal vivo della telecamera nelle chiamate SIP e VMS.

Aggiungi: aggiunta di un dispositivo da associare.

Discover devices (Rileva dispositivi): Fare clic per trovare i dispositivi in rete. Una volta effettuata la scansione della rete, viene visualizzato un elenco dei dispositivi disponibili.

Nota

L'elenco mostra tutti i dispositivi Axis trovati, non solo quelli che possono essere associati.

È possibile trovare solo i dispositivi con **Bonjour** abilitato. Per abilitare **Bonjour** per un dispositivo, aprire l'interfaccia web del dispositivo e andare su **System > Network > Network discovery protocols** (Sistema, rete, protocolli di individuazione rete).

Nota

Per i dispositivi già associati viene visualizzata un'icona informativa. Passare il mouse sull'icona per ottenere informazioni sulle associazioni già attive.

Per associare un dispositivo dall'elenco, fare clic su .

Select pairing type (Seleziona il tipo di associazione): Selezionare dall'elenco a discesa.

Indirizzo: immettere il nome host o l'indirizzo IP della telecamera.

Username (Nome utente): immettere il nome utente per la telecamera.

Password: immettere la password per la telecamera.

Streaming protocol (Protocollo di streaming): selezionare **RTSP** o **SRTSP**.

Verify certificate (Verifica certificato): Selezionare per verificare.

Close (Chiudi): fare clic per cancellare il contenuto di tutti i campi.

Connect (Connetti): fare clic per collegare la telecamera.

Per visualizzare ulteriori informazioni su un dispositivo associato, fare clic su .

Video channel (Canale video): Selezionare il canale video o l'area di visione da visualizzare.

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 di audit)**: Fare clic per visualizzare le informazioni sulle attività utente e di sistema, ad esempio le autenticazioni e le configurazioni riuscite o meno.

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.

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.
- **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**.

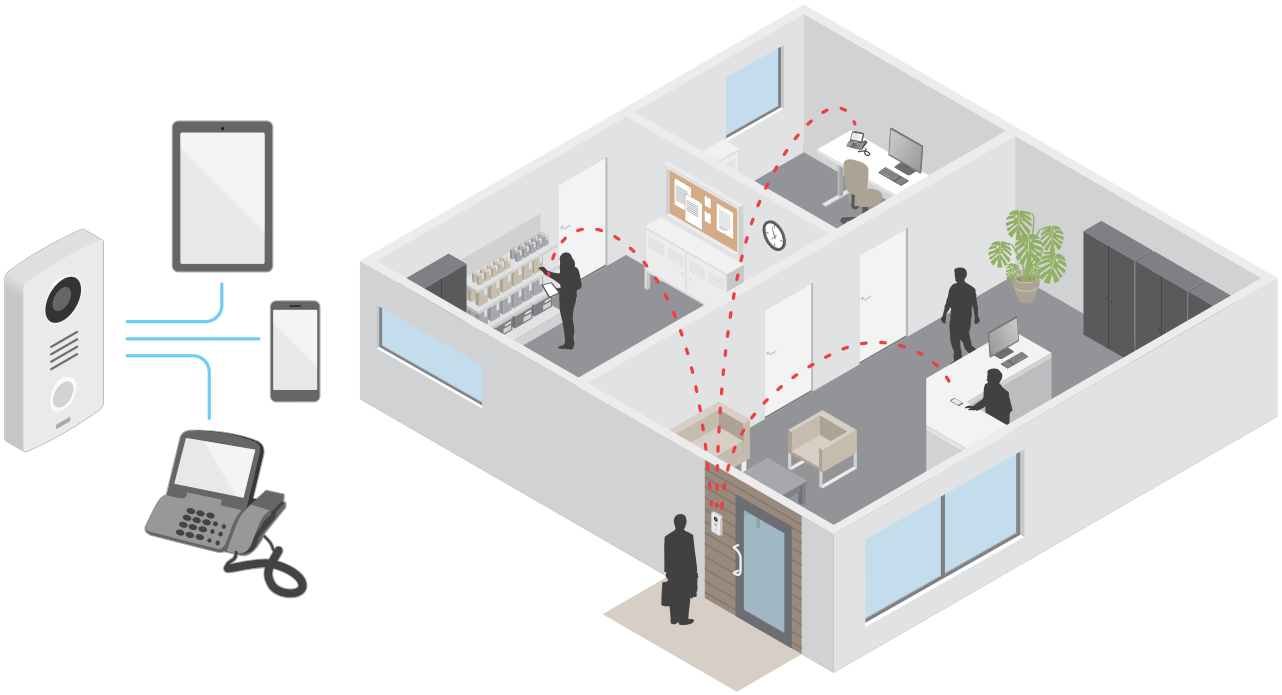
Per saperne di più

Voice over IP (VoIP)

Voice over IP (VoIP) è un gruppo di tecnologie che consente la comunicazione vocale e sessioni multimediali su reti IP, come Internet. Nelle tradizionali chiamate telefoniche, i segnali analogici vengono inviati attraverso le trasmissioni del circuito tramite la rete telefonica pubblica commutata (PSTN). In una chiamata VoIP, i segnali analogici vengono trasformati in segnali digitali per consentire di inviarli in pacchetti di dati attraverso reti IP locali o Internet.

Nel dispositivo Axis, VoIP è abilitato tramite SIP (Session Initiation Protocol) e segnalazione DTMF (Dual-Tone Multi-Frequency).

Esempio:



Quando si preme il pulsante di chiamata su un intercom Axis, viene avviata una chiamata a uno o più destinatari predefiniti. Quando un destinatario risponde, viene stabilita una chiamata. La voce e il video vengono trasferiti tramite le tecnologie VoIP.

Session Initiation Protocol (SIP)

Il protocollo SIP (Session Initiation Protocol) viene utilizzato per impostare, gestire e terminare le chiamate VoIP. È possibile effettuare chiamate tra due o più parti, denominate agenti utente SIP. Per effettuare una chiamata SIP è possibile utilizzare, ad esempio, telefoni SIP, softphone o dispositivi Axis abilitati SIP.

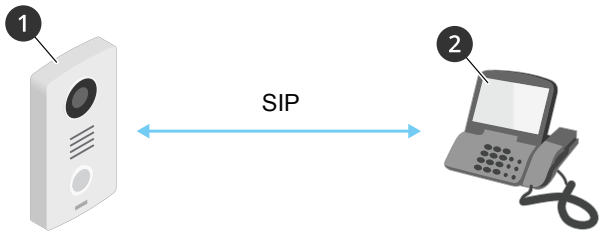
L'audio o il video effettivo viene scambiato tra gli agenti utente SIP con un protocollo di trasporto, ad esempio RTP (Real-Time Transport Protocol).

È possibile effettuare chiamate su reti locali utilizzando una configurazione peer-to-peer o attraverso reti che utilizzano un PBX.

Peer-to-peer SIP (P2PSIP)

Il tipo più semplice di comunicazione SIP avviene direttamente tra due o più agenti utente SIP. Questo è chiamato SIP peer-to-peer (P2PSIP). Se si verifica su una rete locale, sono sufficienti solo gli indirizzi SIP degli agenti utente. Un tipico indirizzo SIP in questo caso può essere `sip:<local-ip>`.

Esempio:



1 *Agente utente A: interfono. Indirizzo SIP: sip:192.168.1.101*
2 *Agente utente B: telefono abilitato SIP. Indirizzo SIP: sip:192.168.1.100*

È possibile impostare l'interfono Axis affinché chiami un telefono abilitato SIP, ad esempio, sulla stessa rete utilizzando un'impostazione SIP peer-to-peer.

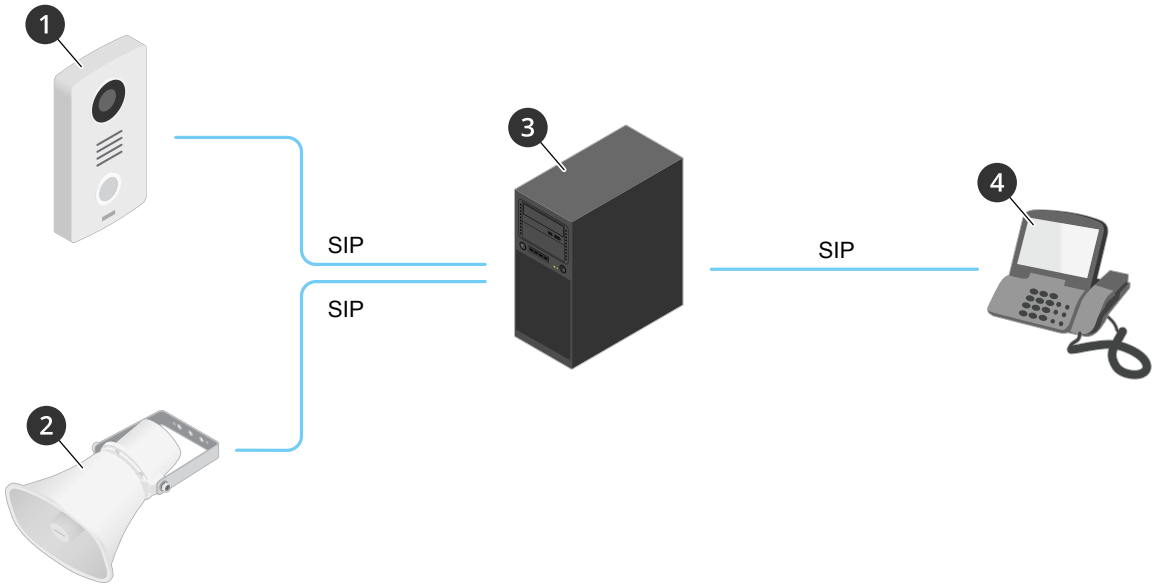
Private Branch Exchange (PBX)

Quando si effettuano chiamate SIP al di fuori della propria rete IP locale, un Private Branch Exchange (PBX) può fungere da hub centrale. Il componente principale di un PBX è un server SIP, che viene anche definito proxy SIP o registrar. Un PBX funziona come un centralino tradizionale, mostrando lo stato corrente del client e consentendo ad esempio trasferimenti di chiamata, posta vocale e reindirizzamenti.

Il server PBX SIP può essere impostato come entità locale o fuori sede. Può essere ospitato su una intranet o da un fornitore di terze parti. Quando si effettuano chiamate SIP tra reti, le chiamate vengono instradate attraverso un gruppo di PBX che interrogano la posizione dell'indirizzo SIP da raggiungere.

Ogni agente utente SIP si registra con il PBX e può quindi raggiungere gli altri componendo l'estensione corretta. Un tipico indirizzo SIP in questo caso può essere `sip:<user>@<domain>` o `sip:<user>@<registrar-ip>`. L'indirizzo SIP è indipendente dal suo indirizzo IP e il PBX rende il dispositivo accessibile purché sia registrato sul PBX.

Esempio:



1 *sip:mydoor@company.com*
2 *sip:myspeaker@company.com*
3 ***PBX** sip.company.com*
4 *sip:office@company.com*

Quando si preme il pulsante di chiamata su un intercom Axis, la chiamata viene inoltrata attraverso uno o più PBX a un indirizzo SIP sulla rete IP locale o su Internet.

NAT Traversal

Utilizzare l'attraversamento NAT (Network Address Translation) quando il dispositivo Axis si trova su una rete privata (LAN) e si desidera accedervi dall'esterno della rete.

Nota

Il router deve supportare NAT traversal e UPnP®.

Ciascun protocollo NAT traversal può essere utilizzato separatamente o in combinazioni differenti a seconda dell'ambiente di rete.

- **ICE** Il protocollo ICE Interactive Connectivity Establishment) aumenta le possibilità di trovare il percorso più efficiente per una comunicazione di successo tra dispositivi peer. Se si abilitano anche STUN e TURN, tali possibilità migliorano ulteriormente.
- **STUN** - STUN (Session Traversal Utilities per NAT) è un protocollo di rete client-server che consente al dispositivo Axis di determinare se si trova dietro un NAT o un firewall e, in tal caso, ottenere l'indirizzo IP e la porta pubblici mappati numero assegnato per le connessioni agli host remoti. Inserire un indirizzo server STUN, ad esempio un indirizzo IP.
- **TURN** - TURN (Traversal Using Relays around NAT) è un protocollo che consente a un dispositivo dietro un router o firewall NAT di ricevere i dati in arrivo da altri host su TCP o UDP. Immettere l'indirizzo del server TURN e le informazioni di accesso.

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*.

Servizio di notifica di sicurezza Axis

Axis fornisce un servizio di notifica con informazioni sulla vulnerabilità e altre questioni relative alla sicurezza per i dispositivi Axis. Per ricevere le notifiche, è possibile iscriversi a *axis.com/security-notification-service*.

Gestione delle vulnerabilità

Per ridurre al minimo il rischio di esposizione dei clienti, Axis, in qualità di **autorità per la numerazione delle Vulnerabilità ed Esposizioni (CNA, Common Vulnerability and Exposures)**, segue gli standard di settore per gestire e rispondere alle vulnerabilità rilevate nei nostri dispositivi, software e servizi. Per ulteriori informazioni sui criteri di gestione delle vulnerabilità di Axis, sulla modalità di segnalazione delle vulnerabilità, sulle vulnerabilità già sfruttate e sui corrispondenti avvisi di sicurezza, consultare *axis.com/vulnerability-management*.

Funzionamento sicuro dei dispositivi Axis

I dispositivi Axis con impostazioni predefinite di fabbrica sono preconfigurati con meccanismi di protezione predefiniti sicuri. Si consiglia di utilizzare più configurazione di sicurezza quando si installa il dispositivo. Per saperne di più sull'approccio di Axis alla cybersecurity, comprese le pratiche migliori, le risorse e le linee guida per la protezione dei dispositivi, consultare *https://www.axis.com/about-axis/cybersecurity*.

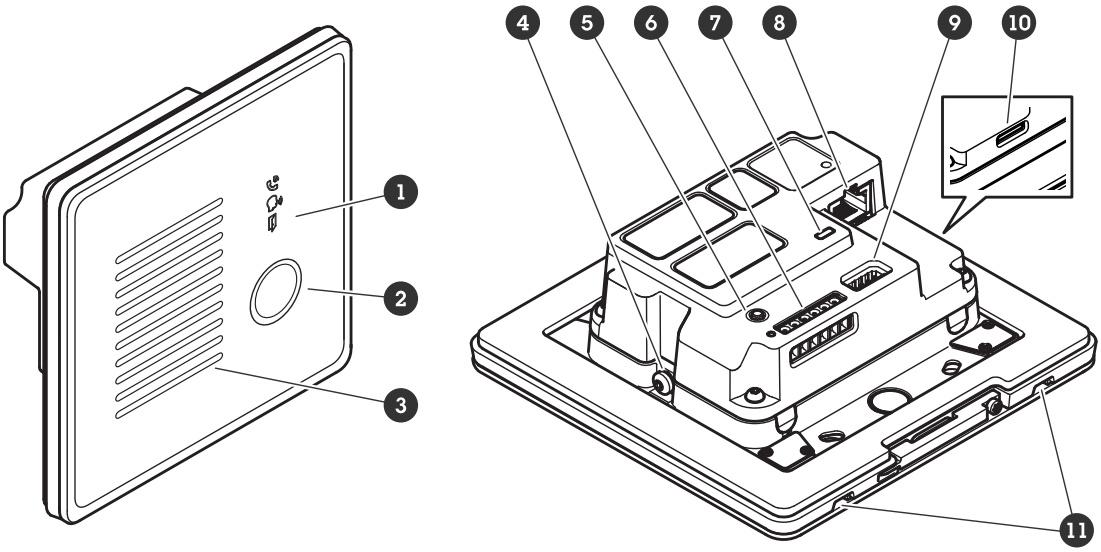
Applicazioni

Le applicazioni permettono di ottenere di più dal proprio dispositivo Axis. AXIS Camera Application Platform (ACAP) è una piattaforma aperta che permette a terze parti di sviluppare analisi e altre applicazioni per i dispositivi Axis. Le applicazioni possono essere preinstallate sul dispositivo oppure è possibile scaricarle gratuitamente o pagando una licenza.

Per trovare i manuali per l'utente delle applicazioni Axis, visitare *help.axis.com*.

Dati tecnici

Panoramica dei prodotti



1
2 Pulsante di chiamata
3 Altoparlante
4 Vite di messa a terra
5
6
7 LED di stato
8
9
10 (microSD/microSDHC/microSDXC)
11 Microfono (2x)

Indicatori e comandi del pannello anteriore

Quando si collega il prodotto all'alimentazione, gli indicatori del pannello frontale si accendono per alcuni secondi.

Icone degli indicatori

Icona	Significato
	Giallo fisso quando viene inizializzata una chiamata in uscita. Giallo lampeggiante quando viene inizializzata una chiamata in entrata.
	Blu fisso per la chiamata in corso.
	Verde fisso quando la porta è aperta.

Indicatori LED

LED di stato	Significato
Verde	Luce verde fissa in condizioni di normale utilizzo.

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 connettersi, premere e rilasciare il pulsante, quindi attendere che il LED di stato verde lampeggi tre volte.

Connettori

Connettore di rete

Connettore Ethernet RJ45 con Power over Ethernet (PoE).

Connettore audio

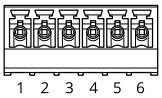
Morsettiera a 4 pin per ingresso e uscita audio.

Funzione	Pin	Note
Ingresso linea	1	Ingresso linea (mono)
TERRA	2	Massa audio
Uscita linea	3	Uscita linea (mono)
TERRA	4	Massa audio

I/O, lettore e connettore relè

È possibile utilizzare questo connettore per I/O e relè o per la connettività lettore.

Morsettiera a 6 pin



1 -
2 12V
3 A/IO1
4 B/IO2
5 COM
6 NO/NC

Funzione	Pin	Note	Dati tecnici
Terra CC	1		0 V CC
Uscita CC	2	Può essere utilizzato per alimentare apparecchiature ausiliarie se il dispositivo è alimentato in Classe PoE 4. Nota: questo pin può essere usato solo come uscita alimentazione.	12 V CC **I/O** : Carico massimo = 50 mA **Reader/relay (Lettore/ relè)**: carico massimo = 350 mA
I/O: configurabile (input o output) **Reader (Lettore)**: A	3	**I/O**: ingresso digitale - collegarlo al pin 1 per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo. Uscita digitale: collegato internamente al pin 1 (terra CC) quando attivo e isolato (scollegato) quando inattivo. Se utilizzata con un carico induttivo, ad esempio un relè, collegare un diodo in parallelo al carico per proteggere il dispositivo da sovratensioni. **Reader (Lettore)**: RS485 – A	**I/O** : input – Da 0 a max 30 V CC Output – da 0 a max 30 V CC, open-drain, 100 mA
I/O: configurabile (input o output) **Reader (Lettore)**: B	4	**I/O**: come il PIN 3 **Reader (Lettore)**: RS485 – B	**I/O**: come il PIN 3
Relay (Relè): COM	5	Comune	
Relay (Relè): NO/NC	6	Normalmente aperto/normalmente chiuso. Per il collegamento di relè. I due pin dei relè sono separati con isolamento galvanico dal resto dei circuiti.	Corrente max 700 mA, tensione max 30 V CC

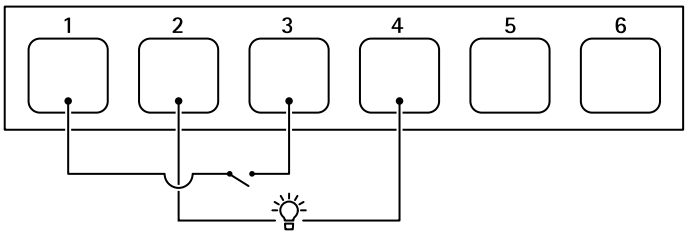
Connettore I/O

Un'opzione è utilizzare il connettore come un connettore I/O con dispositivi esterni in combinazione con, ad esempio, rilevamento movimento, attivazione di eventi e notifiche di allarme. Oltre al punto di riferimento 0 V CC e all'alimentazione (output 12 V CC), il connettore I/O fornisce l'interfaccia per:

Ingresso digitale – Per il collegamento di dispositivi che possono passare da un circuito chiuso ad uno aperto, ad esempio i sensori PIR, i contatti porta/finestra e i rivelatori di rottura.

Uscita digitale – Per il collegamento di dispositivi esterni come relè e LED. I dispositivi collegati possono essere attivati tramite l'API (interfaccia per la programmazione di applicazioni) VAPIX® attraverso un evento oppure dall'interfaccia del dispositivo.

Esempio:



1 *Terra CC*
2 *Output CC 12 V, max 50 mA*
3 *I/O configurato come input*
4 *I/O configurato come output*
5 *Solo relè*
6 *Solo relè*

Connettore relè

In combinazione con I/O, è possibile utilizzare il connettore come connettore relè per collegare un relè a stato solido e utilizzarlo:

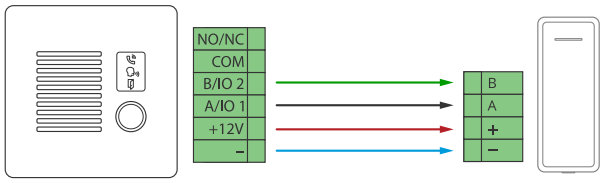
- come relè standard che apre e chiude i circuiti ausiliari,
- per controllare direttamente un blocco,
- per controllare un blocco tramite un relè di sicurezza. L'uso di un relè di sicurezza sul lato sicuro della porta impedisce la manomissione.

Connettore lettore

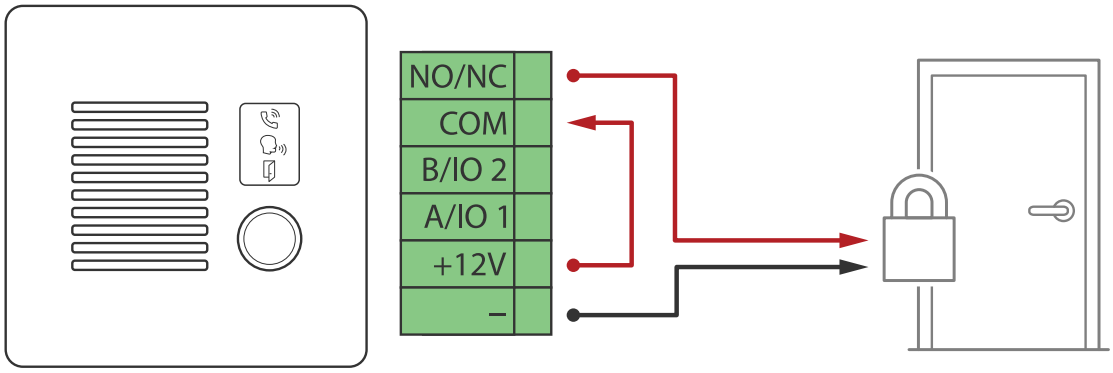
Una terza opzione è utilizzare il connettore come connettore lettore per collegare un lettore esterno.

Collegare le apparecchiature

Lettore Axis

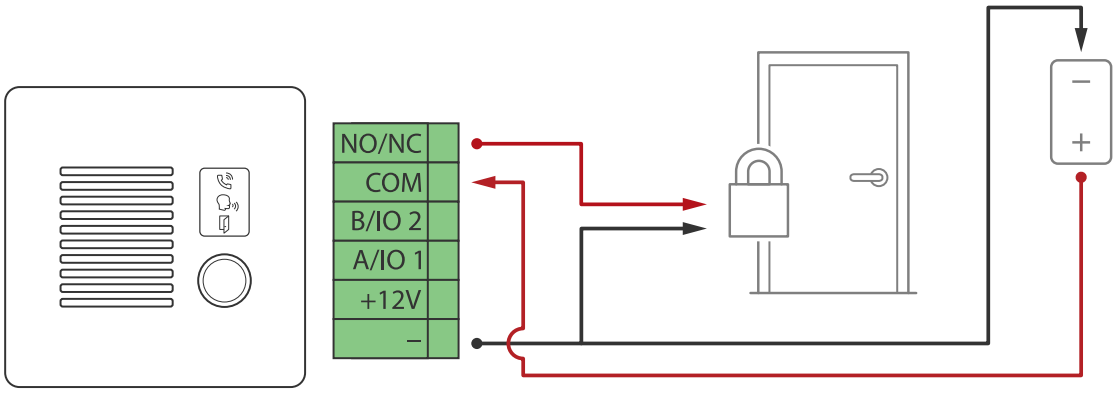


Relè alimentato da PoE (12V)



1. Per controllare lo stato del relè, andare a **System > Accessories (Sistema > Accessori)** e cercare la porta del relè.
2. Impostare **Normal state (Stato normale)** su:
   - per un blocco di protezione intrinseca.
   - per blocco di sicurezza intrinseca.

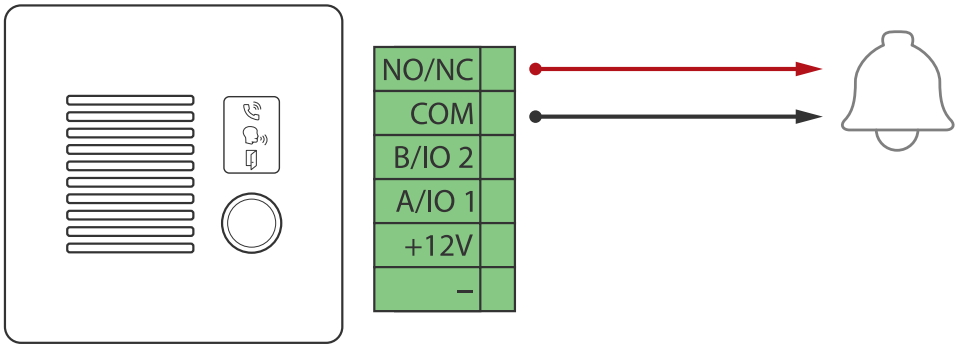
Relè alimentato da un alimentatore separato



1. Per controllare lo stato del relè, andare a **System > Accessories (Sistema > Accessori)** e cercare la porta del relè.
2. Impostare **Normal state (Stato normale)** su:
   - per un blocco di protezione intrinseca.

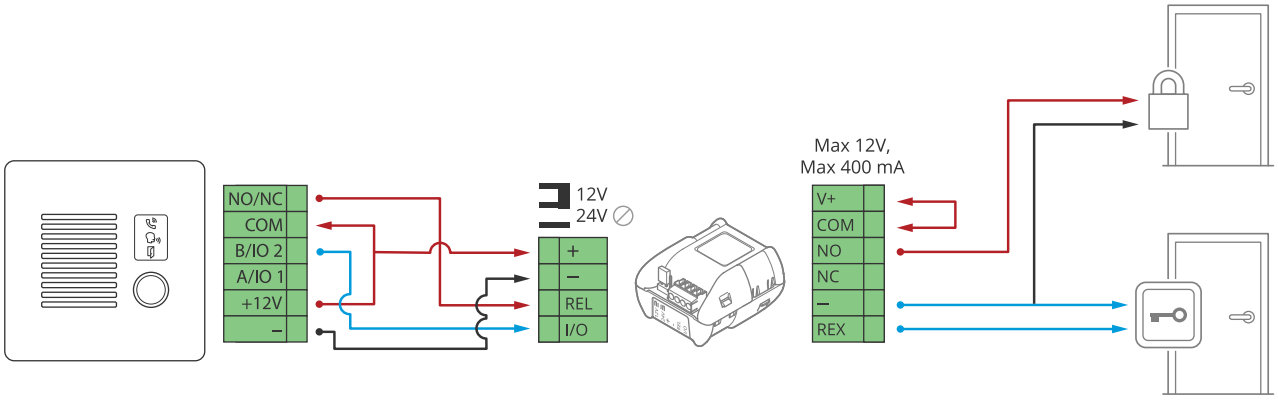
– per blocco di sicurezza intrinseca.

Relè senza potenziali



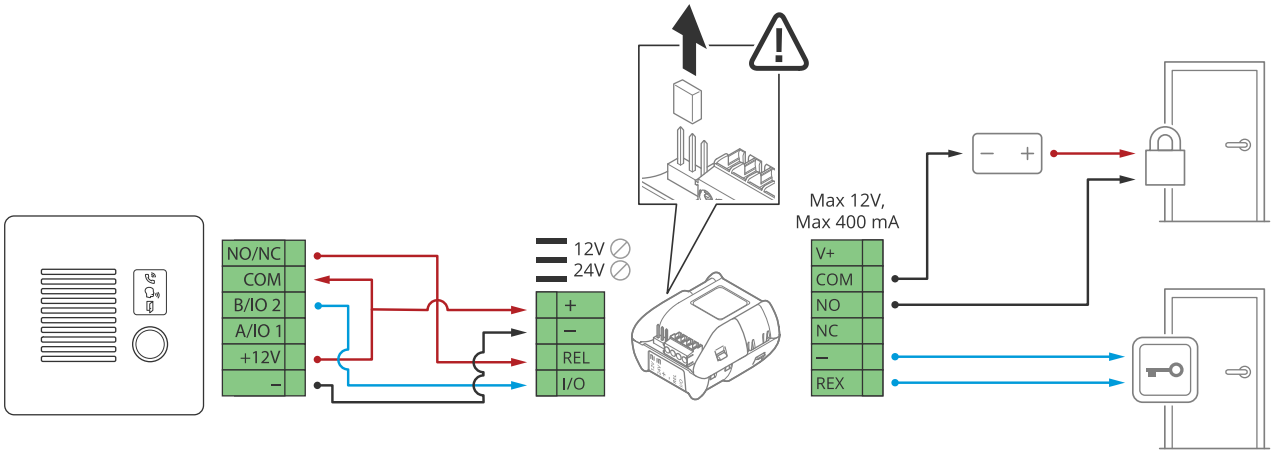
1. Per controllare lo stato del relè, andare a **System > Accessories (Sistema > Accessori)** e cercare la porta del relè.
2. Impostare **Normal state (Stato normale)** su:
   – per un blocco di protezione intrinseca.
   – per blocco di sicurezza intrinseca.

Blocco di protezione intrinseca a 12V alimentato da PoE dall'interfono



1. Per controllare lo stato del relè, andare a **System > Accessories (Sistema > Accessori)** e cercare la porta del relè.
2. Impostare **Normal state (Stato normale)** su:
   – per un blocco di protezione intrinseca.
   – per blocco di sicurezza intrinseca.

Blocco di protezione intrinseca a 12 V alimentato da alimentatore esterno



1. Per controllare lo stato del relè, andare a **System > Accessories (Sistema > Accessori)** e cercare la porta del relè.
2. Impostare **Normal state (Stato normale)** su:
   - per un blocco di protezione intrinseca.
   - per blocco di sicurezza intrinseca.

Pulizia del dispositivo

È possibile pulire il dispositivo con acqua tiepida e detergenti che contengono i seguenti prodotti chimici:

- Isopropanolo 70% (IPA)
- perossido di idrogeno 3% (H_2O_2)
- Ipoclorito di sodio <5% (NaClO)

ATTENZIONE

Prima di utilizzare un detergente, leggere e rispettare la scheda dati di sicurezza (SDS) fornita dal produttore del detergente.

AVVISO

- Le sostanze chimiche possono danneggiare il dispositivo. Non utilizzare sostanze chimiche come acetone o benzina per pulire il dispositivo.
- Non spruzzare il detergente direttamente sul dispositivo. Spruzzare il detergente su un panno non abrasivo e utilizzarlo per pulire il dispositivo.
- Evitare la pulizia alla luce diretta del sole o a temperature elevate, poiché ciò può causare macchie.

1. Utilizzare una bomboletta d'aria compressa per rimuovere polvere e sporcizia dal dispositivo.
2. Se necessario, pulire il dispositivo con un panno morbido in microfibra inumidito con acqua tiepida e detergente.
3. Per evitare macchie, asciugare il dispositivo con un panno pulito e non abrasivo.

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.

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): • Se si riceve: `Reply from <IP address>: 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. • 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. 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). 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. • 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. • 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

Durante l'impostazione del sistema, è importante considerare come le varie impostazioni e situazioni influiscono sulle prestazioni. Alcuni fattori influiscono sulla quantità di larghezza di banda (velocità di trasmissione) richiesta, altri possono influire sul frame rate e alcuni influiscono su entrambe. Se il carico sulla CPU raggiunge il relativo valore massimo, tale valore influisce anche sul velocità in fotogrammi.

I fattori seguenti sono i più importanti di cui tener conto:

- Una risoluzione elevata dell'immagine o livelli di compressione inferiori generano immagini con più dati che, a loro volta, influiscono sulla larghezza di banda.

- L'accesso da parte di numerosi client Motion JPEG o unicast H.264/H.265/AV1 influisce sulla larghezza di banda.
- La vista simultanea di flussi differenti (risoluzione, compressione) di client diversi influisce sia sulla velocità in fotogrammi che sulla larghezza di banda.
  Utilizzare flussi identici quando possibile per mantenere un frame rate elevato. Per garantire che i flussi siano identici, è possibile utilizzare i profili di streaming.
- L'accesso simultaneo a flussi video con codec differenti influisce sulla velocità in fotogrammi e sulla larghezza di banda. Per ottenere prestazioni ottimali, impiegare flussi con lo stesso codec.
- L'uso eccessivo di impostazioni evento influisce sul carico CPU del dispositivo che, a sua volta, influisce sul frame rate.
- L'uso di HTTPS può ridurre il frame rate, in particolare se streaming Motion JPEG.
- Un utilizzo eccessivo della rete dovuto a una scarsa infrastruttura influisce sulla larghezza di banda.
- La visualizzazione in client computer con prestazioni scarse abbassa la qualità delle prestazioni percepite e influisce sul frame rate.
- L'esecuzione simultanea di più applicazioni di Piattaforma applicativa per telecamere AXIS (ACAP) può influire sulla velocità in fotogrammi e sulle prestazioni generali.

Contattare l'assistenza

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

Informazioni di sicurezza

Livelli di pericolo

PERICOLO
Indica una situazione pericolosa che, se non evitata, provoca morte o lesioni gravi.

AVVISO
Indica una situazione pericolosa che, se non evitata, potrebbe provocare la morte o lesioni gravi.

ATTENZIONE
Indica una situazione pericolosa che, se non evitata, potrebbe provocare lesioni medie o minori.

AVVISO
Indica una situazione che, se non evitata, potrebbe danneggiare la proprietà.

Altri livelli di messaggio

Importante
Indica informazioni importanti, essenziali per il corretto funzionamento del dispositivo.

Nota
Indica informazioni utili che aiutano a ottenere il massimo dal dispositivo.

T10213215_it

2025-09 (M7.2)