# AXIS C1710 Network Display Speaker

Manuale dell'utente

## Indice


Panoramica delle soluzioni....4
....4
Installazione....5
Impostazioni preliminari....6
....6
Individuazione del dispositivo sulla rete....6
Supporto browser....6
Aprire l'interfaccia Web del dispositivo....6
Crea un account amministratore....6
Password sicure....7
Verificare che nessuno abbia alterato il software del dispositivo....7
Configurare il dispositivo....8
Calibrazione ed esecuzione di un test dell'altoparlante da remoto....8
Creare un profilo luce....8
Impostazione SIP diretto (P2P)....8
Configurazione di SIP tramite un server (PBX)....9
Imposta regole per eventi....10
Invia un'e-mail se una verifica dell'altoparlante ha esito negativo....10
Riproduci l'audio quando una fotocamera rileva un movimento....11
Interrompi audio con DTMF....12
Impostazione dell'audio per le chiamate SIP in entrata....12
Mostra un messaggio sul display....13
Attivazione del LED di segnalazione con il sensore PIR....13
Interfaccia Web....15
Per saperne di più....16
Voice over IP (VoIP)....16
Session Initiation Protocol (SIP)....16
Peer-to-peer SIP (P2PSIP)....16
Private Branch Exchange (PBX)....16
NAT Traversal....17
Analisi e app....17
AXIS Audio Analytics....17
Dati tecnici....19
Panoramica dei prodotti....19
Indicatori LED....19
Slot per scheda SD....20
Pulsanti....20
Pulsante di comando....20
Switch di disabilitazione microfono....20
Connettori....20
Connettore di rete....20
Connettore audio....20
Connettore I/O....21
Risoluzione dei problemi....23
Ripristino delle impostazioni predefinite di fabbrica....23
Opzioni AXIS OS....23
Controllo della versione corrente del AXIS OS....23
Aggiornare AXIS OS....23
Problemi tecnici e possibili soluzioni....24
Considerazioni sulle prestazioni....27
Considerazioni sulla potenza....27
Contattare l'assistenza....27
Cyber security....28

Gestione delle vulnerabilità ..... 28
Notifiche di sicurezza ..... 28
Ciclo di vita sicuro del prodotto ..... 28

## Panoramica delle soluzioni

Questo manuale descrive come rendere il dispositivo accessibile al sistema audio e come configurare il dispositivo direttamente dalla sua interfaccia.

Se si utilizza un software per la gestione audio o video, è possibile utilizzare tale software per configurare il dispositivo. Il seguente software di gestione è disponibile per il controllo del sistema audio:

- **AXIS Audio Manager Edge**: software per la gestione audio per piccoli sistemi. Viene preinstallato su tutti i dispositivi audio con un firmware 10.0 o versione successiva.
  - *Manuale per l'utente di AXIS Audio Manager Edge*
- **AXIS Audio Manager Pro**: software di gestione dell'audio avanzato per sistemi di grandi dimensioni.
  - *Manuale per l'utente di AXIS Audio Manager Pro*
- **AXIS Camera Station Pro** - Software di gestione video avanzato per sistemi di grandi dimensioni.
  - *Manuale per l'utente di AXIS Camera Station Pro*

Per ulteriori informazioni, consultare *Software per la gestione audio*.

*Una panoramica di come funziona l'audio di rete.*

## Installazione

Questo video è un esempio di come installare AXIS C1710. Per le istruzioni di installazione complete e le informazioni sulla sicurezza, consultare la guida all'installazione: *axis.com/products/axis-c1710/support*

## Impostazioni preliminari

**⚠ AVVISO**

Luci lampeggianti o tremolanti possono scatenare crisi in soggetti affetti da epilessia fotosensibile.

### 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*.

Nota

Quando il prodotto ha i valori predefiniti di fabbrica, il suo indirizzo IP viene visualizzato sul display. Una volta aperta l'interfaccia Web e creato un utente, il display mostrerà invece l'orologio e la data.

#### Supporto browser

Il dispositivo può essere utilizzato con i seguenti browser:

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

### 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 oppure 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 *Crea un account amministratore, on page 6*.

Per le descrizioni di tutte le funzioni e impostazioni dell'interfaccia Web dei dispositivi con AXIS OS, consultare . *Guida all'interfaccia Web di AXIS OS*.

### 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 *Password sicure, on page 7*.
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 *Ripristino delle impostazioni predefinite di fabbrica, on page 23*.

## 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 *Ripristino delle impostazioni predefinite di fabbrica, on page 23*.
   Dopo il ripristino, l'avvio sicuro garantisce lo stato del dispositivo.
2. Configurare e installare il dispositivo.

# Configurare il dispositivo

## Calibrazione ed esecuzione di un test dell'altoparlante da remoto

È possibile eseguire un test dell'altoparlante per verificare da una postazione remota se l'altoparlante funziona come previsto. L'altoparlante esegue la verifica riproducendo una serie di toni di prova registrati dal microfono integrato. Ogni volta che si esegue la verifica, i valori registrati vengono confrontati con i valori registrati durante la calibrazione.

Nota

Il test deve essere calibrato dalla posizione di montaggio nel sito di installazione. Se l'altoparlante viene spostato o se le zone circostanti cambiano, ad esempio, se un muro viene costruito o rimosso, l'altoparlante dovrebbe essere ricalibrato.

Durante la calibrazione, si consiglia di essere fisicamente presenti nel sito di installazione per ascoltare i toni di test e verificare che non siano ovattati o bloccati da ostacoli indesiderati nel percorso acustico dell'altoparlante. Per evitare danni all'udito, l'installatore deve mantenere una distanza di sicurezza dall'altoparlante durante la prova.

1. Andare all'interfaccia del dispositivo > **Audio > Speaker test (Audio > Test altoparlante)**.
2. Per calibrare il dispositivo audio, fare clic su **Calibrate (Calibra)**.

Nota

Una volta calibrato il dispositivo Axis, il test dell'altoparlante può essere eseguito in qualsiasi momento.

3. Per eseguire il test dell'altoparlante, fare clic su **Run the test (Esegui il test)**.

Nota

È inoltre possibile eseguire la calibrazione premendo il pulsante di comando sul dispositivo fisico. Vedere *Panoramica dei prodotti, on page 19* per identificare il pulsante di comando.

## Creare un profilo luce

Un profilo è una raccolta di configurazioni impostate. È possibile avere fino a 30 profili per sorgente luminosa con diverse priorità e modelli. È possibile avere solo una sorgente luminosa per un profilo, quindi se si desidera creare profili per entrambe le sorgenti luminose, è necessario creare almeno due profili.

Creare un nuovo profilo:

1. Andare in **Light > Profiles** (Luce, Profili) e fare clic su **Create** (Crea).
2. Immetti un **Name (Nome)** e **Description (Descrizione)**.
3. Seleziona le impostazioni di **Light (Luce)** che si desiderano per il profilo.
4. Impostare la **Priority (Priorità)** di luce e fare clic su **Save (Salva)**.
5. Per la modifica di un profilo, fare clic su e selezionare **Edit (Modifica)**.

## Impostazione SIP diretto (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 ulteriori informazioni sulle opzioni di impostazione, consultare *SIP*.

1. Andare a **System (Sistema)** > **SIP** > **SIP settings (Impostazioni SIP)** 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)**.
3. In **Call handling (Gestione chiamate)**, impostare il timeout e la durata della chiamata.

4. In **Ports (Porte)**, inserire i numeri delle porte.
   - **SIP port (Porta SIP)**: la porta di rete utilizzata per le comunicazioni SIP. Il traffico di segnalazione tramite la porta non viene crittografato. Il numero di porta predefinito è 5.060. Se necessario, inserire un numero di porta differente.
   - **TLS port (Porta TLS)**: porta di rete utilizzata per la comunicazione SIP crittografata. 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.
   - **RTP start port (Porta di avvio RTP)**: inserire la porta utilizzata per il primo flusso RTP in una chiamata SIP. La porta di avvio predefinita per i trasporti multimediali è la 4000. Alcuni firewall potrebbero bloccare il traffico RTP su determinati numeri di porta. Un numero di porta deve essere compreso tra 1.024 e 65.535.
5. In **NAT traversal**, 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, consultare *NAT traversal*.

6. In **Audio**, selezionare almeno un codec audio con la qualità audio desiderata per le chiamate SIP. Trascina e rilascia per modificare la priorità.
7. In **Additional (Aggiuntivo)**, selezionare opzioni aggiuntive.
   - **UDP-to-TCP switching (Passaggio da UDP a TCP)**: selezionare questa opzione 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 1.300 byte.
   - **Allow via rewrite (Consenti tramite riscrittura)**: selezionare per inviare l'indirizzo IP locale e non l'indirizzo IP pubblico del router.
   - **Allow contact rewrite (Consenti riscrittura contatto)**: selezionare questa opzione per inviare l'indirizzo IP locale e non l'indirizzo IP pubblico del router.
   - **Register with server every (registra con il server ogni)**: impostare la frequenza con cui si desidera che il dispositivo si sincronizzi con il server SIP per gli account SIP esistenti.
   - **DTMF payload type (Tipo payload DTMF)**: modificare il tipo di payload per DTMF.
8. Fare clic su **Save (Salva)**.

## Configurazione di SIP tramite un server (PBX)

Utilizzare un server PBX quando gli agenti utente comunicano all'interno e all'esterno della rete IP. Altre funzionalità possono essere aggiunte alla configurazione a seconda del provider PBX.

Per ulteriori informazioni sulle opzioni di impostazione, consultare *SIP*.

1. Richiedere le seguenti informazioni dal provider PBX:

- ID utente
- Dominio
- Password
- ID di autenticazione
- ID chiamante
- Registrar
- Porta di avvio RTP

2. Per aggiungere un nuovo account, andare a **System (Sistema)** > **SIP** > **SIP accounts (Account SIP)** e fare clic su **+ Account (Aggiungi account)**.
3. Inserire i dettagli ricevuti dal provider PBX.

4. Selezionare **Registered (Registrato)**.
5. Selezionare una modalità di trasporto.
6. Fare clic su **Save (Salva)**.
7. Configurare le impostazioni SIP allo stesso modo del peer-to-peer. Per ulteriori informazioni, vedere *Impostazione SIP diretto (P2P), on page 8*.

## Imposta regole per eventi

È possibile creare regole per far sì che il dispositivo esegua azioni 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 riprodurre una clip audio in base ad una pianificazione o quando riceve una chiamata oppure può inviare una mail se il dispositivo cambia indirizzo IP.

Per ulteriori informazioni, consultare *Guida iniziale per le regole eventi*.

### Invia un'e-mail se una verifica dell'altoparlante ha esito negativo

In questo esempio, il dispositivo audio è configurato per inviare un'e-mail a un destinatario definito quando una verifica dell'altoparlante ha esito negativo. La verifica dell'altoparlante è configurata per essere eseguita ogni giorno alle 18:00.

1. Impostare una pianificazione per la verifica dell'altoparlante:
   1.1. Andare all'interfaccia del dispositivo > **System (Sistema)** > **Events (Eventi)** > **Schedules (Pianificazioni)**.
   1.2. Creare una pianificazione che inizi alle 18:00 e finisca alle 18:01 ogni giorno. Assegnare il nome "Tutti i giorni alle 18:00".
2. Creare un destinatario e-mail:
   2.1. Andare all'interfaccia del dispositivo > **System (Sistema)** > **Events (Eventi)** > **Recipients (Destinatari)**.
   2.2. Fare clic su **Add recipient (Aggiungi destinatario)**.
   2.3. Assegnare al destinatario il nome "Destinatari test altoparlante"
   2.4. In **Type (Tipo)**, selezionare **Email (E-mail)**.
   2.5. In **Send email to (Invia e-mail a)**, inserire gli indirizzi e-mail dei destinatari. Utilizzare la virgola per separare più indirizzi.
   2.6. Inserire i dettagli per l'account e-mail del mittente.
   2.7. Fare clic su **Test** per inviare un messaggio e-mail di testo.

   Nota

   Alcuni provider e-mail hanno filtri di sicurezza che impediscono agli utenti di ricevere o visualizzare allegati di grandi dimensioni, ad esempio e-mail pianificate e simili. Controllare i criteri di sicurezza del provider e-mail per evitare problemi di consegna e account e-mail bloccati.

   2.8. Fare clic su **Save (Salva)**.
3. Impostare la verifica degli altoparlanti automatica:
   3.1. Andare all'interfaccia del dispositivo > **System (Sistema)** > **Events (Eventi)** > **Rules (Regole)**.
   3.2. Fare clic su **Add a rule (Aggiungi una regola)**.
   3.3. Immettere un nome per la regola.
   3.4. In **Condition (Condizione)**, selezionare **Schedule (Pianificazione)** e selezionare dall'elenco dei trigger
   3.5. In **Schedule (Pianificazione)**, selezionare la pianificazione (Tutti i giorni alle 18:00).
   3.6. In **Action (Azione)**, selezionare **Run automatic speaker test (Esegui test automatico dell'altoparlante)**.

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

4. Impostare la condizione per l'invio di un messaggio e-mail quando la verifica dell'altoparlante ha esito negativo:
   4.1. Andare all'interfaccia del dispositivo > **System (Sistema)** > **Events (Eventi)** > **Rules (Regole)**.
   4.2. Fare clic su **Add a rule (Aggiungi una regola)**.
   4.3. Immettere un nome per la regola.
   4.4. In **Condition (Condizione)**, selezionare **Speaker test result (Risultato test dell'altoparlante)**.
   4.5. In **Speaker test status (Stato test dell'altoparlante)**, selezionare **Didn't pass the test (Test non superato)**.
   4.6. In **Action (Azione)**, selezionare **Send notification to email (Invia notifica a e-mail)**.
   4.7. In **Recipient (Destinatario)**, selezionare il destinatario ("Destinatari test altoparlante")
   4.8. Inserire un oggetto e un messaggio e fare clic su **Save (Salva)**.

### Riproduci l'audio quando una fotocamera rileva un movimento

Questo esempio spiega come configurare il dispositivo audio per riprodurre una clip audio quando una telecamera di rete Axis rileva il movimento.

**Prerequisiti**

- Il dispositivo audio e la telecamera di rete Axis condividono la stessa rete.
- L'applicazione di rilevamento del movimento è configurata e in esecuzione sulla telecamera.

1. Preparazione di un collegamento alla clip audio:
   1.1. Andare ad **Audio** > **Audio clips (Clip audio)**.
   1.2. Fare clic su ⋮ > **Create link (Crea un link)** per una clip audio.
   1.3. Impostare il volume e il numero di ripetizioni della clip.
   1.4. Fare clic sull'icona Copia per copiare il link.
2. Creare una regola di azione:
   2.1. Andare a **System (Sistema)** > **Events (Eventi)** > **Recipients (Destinatari)**.
   2.2. Fare clic su **+ Add recipient (+ Aggiungi destinatario)**.
   2.3. Digitare un nome per il destinatario, ad esempio "Altoparlante".
   2.4. Selezionare **HTTP** dal menu a discesa **Type (Tipo)**.
   2.5. Copiare il collegamento configurato dal dispositivo audio nel campo **URL**.
   2.6. Inserire il nome utente e la password del dispositivo audio.
   2.7. Fare clic su **Save (Salva)**.
   2.8. Vai a **Rules (Regole)** e fai clic su **+ Add a rule (+ Aggiungi una regola)**.
   2.9. Inserire un nome per la regola di azione, ad esempio "Riproduci clip".
   2.10. Dall'elenco **Condition (Condizione)** selezionare un rilevamento di oggetti in movimento nel video alternativo sotto **Applications (Applicazioni)**.

   Nota

   Se non sono disponibili opzioni per il rilevamento di oggetti in movimento nel video, andare a **Apps (App)**, fare clic su **AXIS Video Motion Detection** e attivare il rilevamento del movimento.

   2.11. Nell'elenco **Action (Azione)** selezionare **Send notification through HTTP (Invia notifica tramite HTTP)**.
   2.12. Selezionare il destinatario in **Recipient (Destinatario)**.
   2.13. Fare clic su **Save** (Salva).

### Interrompi audio con DTMF

Questo esempio spiega come:

- configurare DTMF su un dispositivo.
- impostare un evento per interrompere l'audio quando un comando DTMF viene inviato al dispositivo.

1. Vai a **System (Sistema)** > **SIP** > **SIP settings (Impostazioni SIP)**.
2. Assicurarsi che **Enable SIP (Abilita SIP)** sia attivata.
   Se è necessario attivarla, ricordare di fare clic su **Save (Salva)** in un secondo momento.
3. Andare a **SIP accounts (Account SIP)**.
4. Vicino all'account SIP, fare clic su ⋮ > **Edit (Modifica)**.
5. In **DTMF**, fare clic su **+ DTMF sequence (Aggiungi sequenza DTMF)**.
6. In **Sequence (Sequenza)**, inserire "1".
7. In **Description (Descrizione)**, inserire "stop audio".
8. Fare clic su **Save (Salva)**.
9. Andare a **System (Sistema)** > **Events (Eventi)** > **Rules (Regole)** e fare clic su **+ Add a rule (Aggiungi una regola)**.
10. In **Name (Nome)**, inserire "DTMF stop audio".
11. In **Condition (Condizione)**, selezionare **DTMF**.
12. In **DTMF Event ID (ID evento DTMF)**, selezionare **stop audio**.
13. In **Action (Azione)**, selezionare **Stop playing audio clip (Interrompi riproduzione di clip audio)**.
14. Fare clic su **Save (Salva)**.

### Impostazione dell'audio per le chiamate SIP in entrata

È possibile impostare una regola che riproduce una clip audio quando si riceve una chiamata SIP.

È inoltre possibile impostare una regola aggiuntiva che risponde automaticamente alla chiamata SIP una volta terminata la clip audio. Ciò può essere utile nei casi in cui un operatore di allarme desidera richiamare l'attenzione di qualcuno vicino a un dispositivo audio e stabilire una linea di comunicazione. Questa operazione viene eseguita effettuando una chiamata SIP al dispositivo audio, che riprodurrà una clip audio per avvisare le persone vicine al dispositivo audio. Quando la riproduzione della clip audio è terminata, il dispositivo audio risponde automaticamente alla chiamata SIP e può avere luogo la comunicazione tra l'operatore dell'allarme e le persone vicine al dispositivo audio.

Abilitare le impostazioni SIP:

1. Accedere all'interfaccia del dispositivo dell'altoparlante inserendo il proprio indirizzo IP in un browser Web.
2. Andare su **System (Sistema)** > **SIP** > **SIP settings (Impostazioni SIP)** e selezionare **Enable SIP (Abilita SIP)**.
3. Per consentire al dispositivo di ricevere chiamate in entrata, selezionare **Allow incoming SIP calls (Consenti chiamate SIP in arrivo)**.
4. Fare clic su **Save (Salva)**.
5. Andare su **SIP accounts (Account SIP)**.
6. Vicino all'account SIP, fare clic su ⋮ > **Edit (Modifica)**.
7. Deselezionare **Risposta automatica**.

Riprodurre audio quando viene ricevuta una chiamata SIP:

1. Andare su **Settings > System > Events > Rules (Impostazioni > Sistema > Eventi > Regole)** e aggiungere una regola.

2. Inserire un nome per la regola.
3. Nell'elenco delle condizioni, selezionare **State (Stato)**.
4. Nell'elenco degli stati, selezionare **Chiamata**.
5. Nell'elenco delle azioni, selezionare **Play audio clip (Riprodurre clip audio)**.
6. Nell'elenco delle clip, selezionare la clip audio che si desidera riprodurre.
7. Selezionare quante volte ripetere la clip audio. 0 indica "riproduci una volta".
8. Fare clic su **Save (Salva)**.

Una volta terminata la clip audio, rispondere automaticamente alla chiamata SIP:

1. Andare su **Settings > System > Events > Rules (Impostazioni > Sistema > Eventi > Regole)** e aggiungere una regola.
2. Inserire un nome per la regola.
3. Nell'elenco delle condizioni, selezionare **Audio clip playing (Riproduzione clip audio)**.
4. Selezionare **Utilizza questa condizione come trigger.**
5. Selezionare **Inverti questa condizione.**
6. Fare clic su **+ Aggiungi una condizione** per aggiungere una seconda condizione all'evento.
7. Nell'elenco delle condizioni, selezionare **State (Stato)**.
8. Nell'elenco degli stati, selezionare **Chiamata**.
9. Nell'elenco delle azioni, selezionare **Answer call (Rispondi alla chiamata)**.
10. Fare clic su **Save (Salva)**.

### Mostra un messaggio sul display

Mostrare un messaggio di testo sul display di un singolo altoparlante:

1. Aprire l'interfaccia Web inserendo l'indirizzo IP dell'altoparlante in un browser Web.
2. Andare a **System (Sistema)** > **Events (Eventi)** > **Rules (Regole)**.
3. Fare clic su **+ Add a rule (Aggiungi una regola)**.
4. Attribuire un nome alla regola.
5. In **Condition (Condizione)**, selezionare **Manual trigger (Attivazione manuale)**.
6. In **Action (Azione)**, selezionare **Speaker display notification (Visualizza notifica altoparlante)**.
7. In **Message (Messaggio)**, inserire il testo che si desidera visualizzare sull'altoparlante.
8. Compilare il resto dei campi sulla base delle proprie esigenze.
9. Fare clic su **Save (Salva)**.
10. Assicurarsi che la regola sia attivata.
11. Andare su **Manual triggers (Attivazioni manuali)**.
12. Attivare **Trigger 1**.
    La notifica viene ora inviata all'altoparlante.

### Attivazione del LED di segnalazione con il sensore PIR

1. Aprire l'interfaccia Web inserendo l'indirizzo IP dell'altoparlante in un browser Web.
2. Andare a **System (Sistema)** > **Events (Eventi)** > **Rules (Regole)**.
3. Fare clic su **+ Add a rule (Aggiungi una regola)**.
4. Attribuire un nome alla regola.
5. In **Condition (Condizione)**, selezionare **PIR Sensor (Sensore PIR)**.

6. In **Action (Azione)**, selezionare **Light and siren (Luce e sirena) > Run light profile while the rule is active (Esegui il profilo luce mentre la regola è attiva)**.
7. In **Profilo (Profile)**, selezionare uno dei profili dei LED di segnalazione (vedere il suggerimento dello strumento quando si passa il mouse su un'alternativa).
   Per creare un nuovo profilo, vedere *Creare un profilo luce, on page 8*.
8. Fare clic su **Save (Salva)**.

## Interfaccia Web

Per informazioni su tutte le funzionalità e le impostazioni disponibili nell'interfaccia Web dei dispositivi con AXIS OS, andare a *Guida all'interfaccia Web di AXIS OS*.

## 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).

### 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.

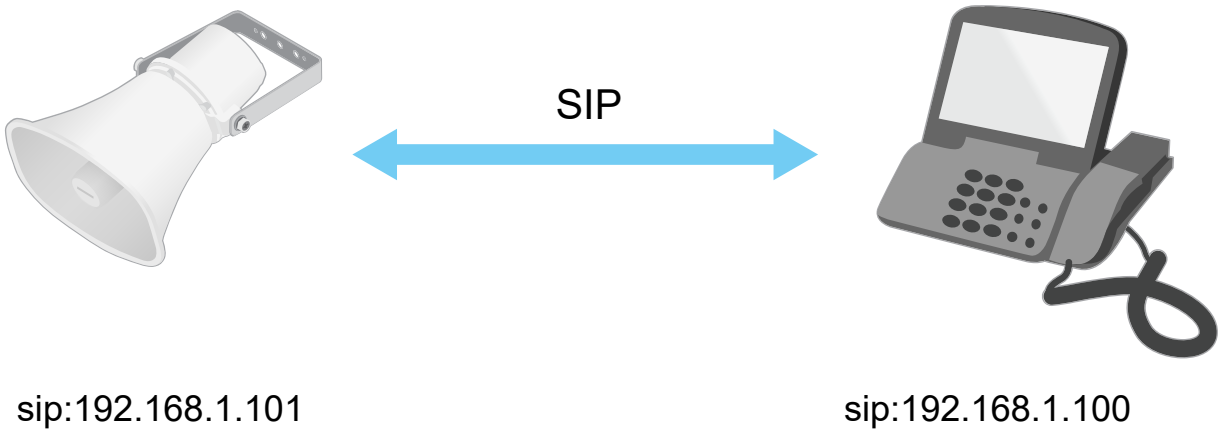
L'audio o il video effettivo viene scambiato tra gli agenti utente SIP con un protocollo di trasporto, ad esempio RTP (Real-Time Transport Protocol).

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:**




È possibile configurare un telefono abilitato SIP per chiamare un dispositivo audio sulla stessa rete utilizzando un'impostazione SIP peer-to-peer.

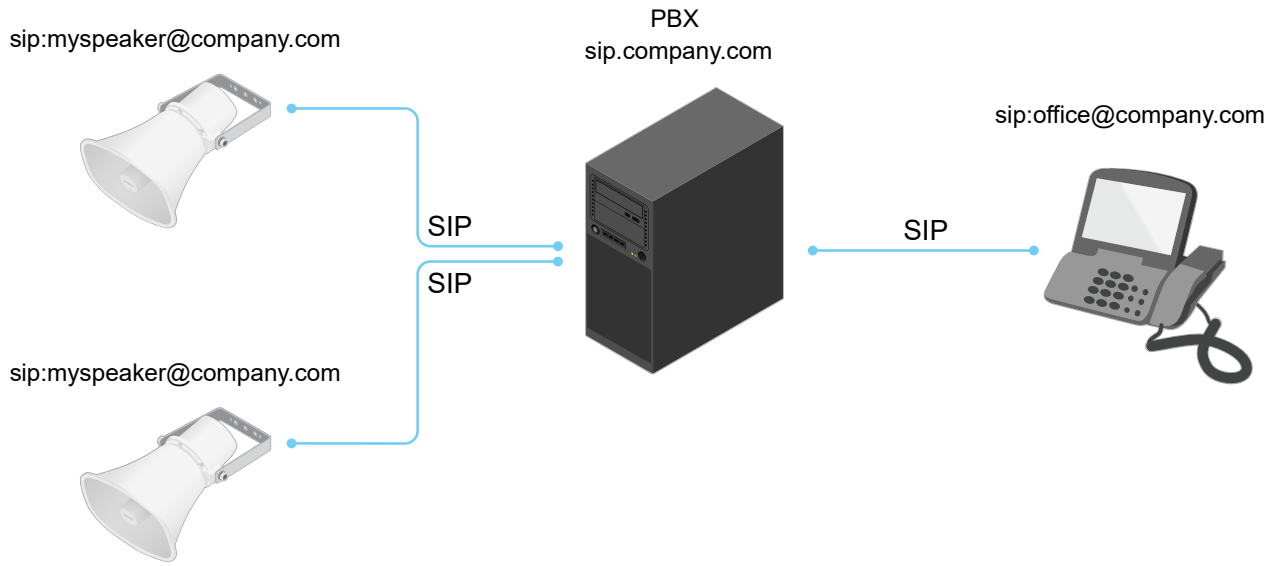
### Private Branch Exchange (PBX)

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:**




### 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.

## Analisi e app

Le analisi e le app 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 app per i dispositivi Axis. Le app possono essere preinstallate sul dispositivo oppure è possibile scaricarle gratuitamente o pagando una licenza.

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

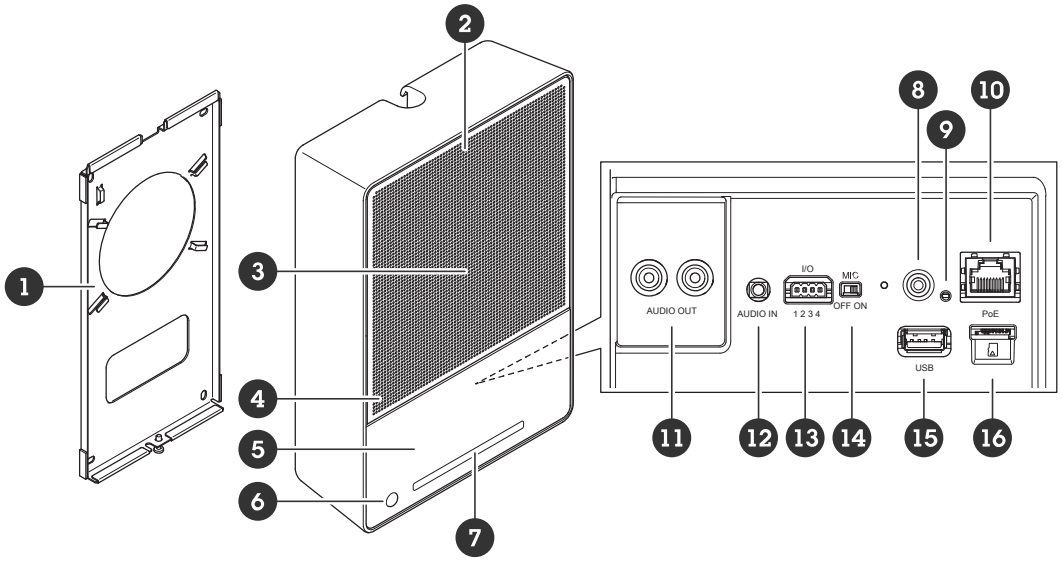
### AXIS Audio Analytics

AXIS Audio Analytics rileva aumenti improvvisi del volume sonoro e tipi specifici di suoni quali urla o grida entro la portata del dispositivo dov'è installato. Questi rilevamenti si possono configurare perché attivino una risposta,

come registrare video, riprodurre un messaggio audio o inviare avvisi al personale di sicurezza. Per ulteriori informazioni su come funziona l'applicazione, consultare il *manuale per l'utente di AXIS Audio Analytics*.

# Dati tecnici

## Panoramica dei prodotti




1 *Piastra posteriore*
2 *LED audio*
3 *Altoparlante*
4 *Microfono*
5 *Display*
6 *Sensore PIR*
7 *LED di segnalazione*
8 *Pulsante di comando*
9 *LED di stato*
10 *Connettore di rete*
11 *Uscita audio (connettore RCA)*
12 *Connettore audio*
13 *Connettore I/O*
14 *Switch di disabilitazione microfono*
15 *Connettore USB (disattivato, riservato per uso futuro)*
16 *Slot per scheda SD*

## Indicatori LED

| LED di stato | Significato |
|---|---|
| Spento | Spento per condizioni di normale funzionamento. |
| Verde | Luce fissa per 10 secondi per il normale funzionamento una volta completato l'avvio. |
| Giallo | Luce fissa durante l'avvio. Lampeggia durante l'aggiornamento del software del dispositivo o il ripristino delle impostazioni predefinite. |
| Giallo/rosso | Lampeggia se il collegamento di rete non è disponibile o si è interrotto. |

| | |
|---|---|
| Rosso | Lampeggia lentamente se l'aggiornamento non è riuscito. |
| Rosso/Verde | Lampeggia velocemente quando è selezionato **Individua dispositivo**. |

## 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.

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:

- Calibrare la verifica dell'altoparlante. Premere e rilasciare il pulsante di comando e verrà emesso un segnale di verifica.
- Ripristino del dispositivo alle impostazioni predefinite di fabbrica. Vedere *Ripristino delle impostazioni predefinite di fabbrica, on page 23*.

### Switch di disabilitazione microfono

Per la posizione dello switch di disabilitazione del microfono, vedere *Panoramica dei prodotti, on page 19*.

Lo switch di disabilitazione del microfono viene utilizzato per posizionare il microfono meccanicamente su **ON** oppure **OFF**. L'impostazione predefinita di fabbrica per questo switch è **ON**.

## Connettori

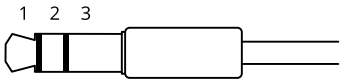
### Connettore di rete

Connettore Ethernet RJ45 con Power over Ethernet (PoE).

*AVVISO*

Il dispositivo deve essere collegato con un cavo di rete schermato (STP). Tutti i cavi che collegano il dispositivo alla rete sono destinati al loro uso specifico. Accertarsi che i dispositivi di rete siano installati secondo le istruzioni del produttore. Per ulteriori informazioni sui requisiti normativi, consultare la Guida all'installazione disponibile all'indirizzo *www.axis.com*.

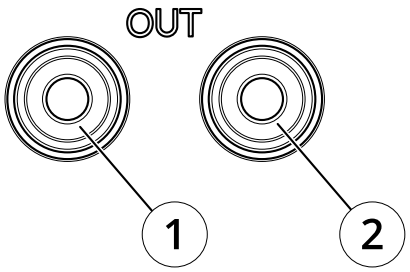
### Connettore audio




**Ingresso audio**

| 1 Punta | 2 Anello | 3 Guaina |
|---|---|---|
| Microfono non bilanciato (con o senza alimentazione a elettrete) o linea | Alimentazione a elettrete se selezionata | Terra |
| Microfono bilanciato (con o senza alimentazione phantom) o linea, segnale "caldo" | Microfono bilanciato (con o senza alimentazione phantom) o linea, segnale "freddo" | Terra |
| Segnale digitale | Alimentazione anello se selezionata | Terra |
| Microfono non bilanciato stereo (con o senza alimentazione a elettrete) o linea, "sinistra" | Microfono non bilanciato stereo (con o senza alimentazione a elettrete) o linea, "destra" | Terra |

**Uscita audio (connettore RCA)**




| | 1 Connettore bianco | 2 Connettore rosso |
|---|---|---|
| Output audio | Uscita audio (a sinistra) | Uscita audio (a destra) |

## Connettore I/O

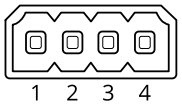
Utilizzare il connettore I/O con dispositivi esterni in combinazione con, ad esempio, rilevamento movimento, attivazione di eventi e notifiche di allarme. Oltre al punto di riferimento 0 V CC e all'alimentazione (output 12 V CC), il connettore I/O fornisce l'interfaccia per:

**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.

**Input supervisionato –** Consente di rilevare le manomissioni su un input digitale.

**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 Web del dispositivo.

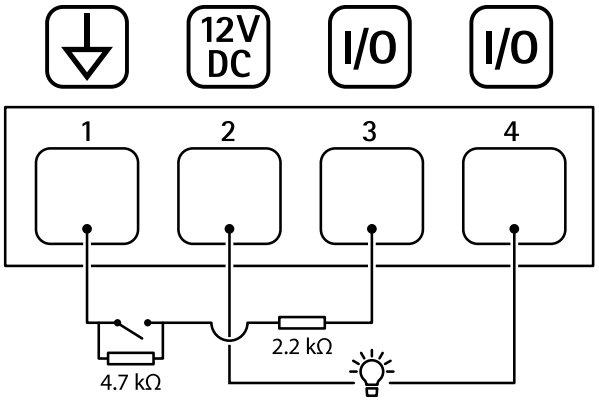
Morsettiera a 4 pin




| Funzione | Pin | Note | Dati tecnici |
|---|---|---|---|
| Terra CC | 1 | | 0 V CC |
| Uscita CC | 2 | ⚠<br>Questo terminale può essere utilizzato anche per alimentare una periferica ausiliaria.<br>Nota: questo pin può essere usato solo come uscita alimentazione. | 12 V CC<br>Carico massimo: 50 mA |

| | | | |
|---|---|---|---|
| Configurabile (ingresso o uscita) | 3–4 | Ingresso digitale o ingresso supervisionato - collegarlo al pin 1 per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo. Per utilizzare l'ingresso supervisionato, installare resistori terminali. Vedere il diagramma di connessione per informazioni su come collegare i resistori. | Da 0 a max 30 V CC |
| | | 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. | Da 0 a max 30 V CC, open-drain, 100 mA |

**Esempio:**




1 *Terra CC*
2 *Output CC 12 V, max 50 mA*
3 *I/O configurato come ingresso supervisionato*
4 *I/O configurato come output*

# 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 *Panoramica dei prodotti, on page 19*.
3. Tenere premuto il pulsante di comando per 10 secondi fino a quando l'indicatore LED di stato non diventa nuovamente di colore 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.

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

- Quando si esegue l'aggiornamento del software del dispositivo, le impostazioni preconfigurate e personalizzate vengono salvate. Axis Communications AB non può garantire il salvataggio delle

impostazioni, anche se le funzionalità sono disponibili nella nuova versione del sistema operativo AXIS OS.

- A partire da AXIS OS 12.6, è necessario installare tutte le versioni LTS comprese tra la versione attuale del dispositivo e la versione di destinazione. Ad esempio, se la versione del software di installazione del dispositivo è AXIS OS 11.2, è necessario installare la versione LTS AXIS OS 11.11 prima di poter effettuare l'aggiornamento del dispositivo ad AXIS OS 12.6. Per ulteriori informazioni, consultare *Guida al ciclo di vita AXIS OS: Percorso di aggiornamento*.
- 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 e possibili soluzioni

### Problemi durante l'aggiornamento di AXIS OS

**Aggiornamento di AXIS OS non riuscito**

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

**Impossibile impostare l'indirizzo IP**

- 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 potrebbe già essere utilizzato da un altro dispositivo. Per verificare:
  1. Scollegare il dispositivo Axis dalla rete.
  2. In una finestra di comando/DOS digitare `ping` e l'indirizzo IP del dispositivo.
  3. Se la risposta ricevuta è `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.
  4. 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.
- Potrebbe verificarsi un conflitto di indirizzi IP con un altro dispositivo sulla 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.

### Problemi di accesso al dispositivo

**Impossibile effettuare l'accesso al dispositivo tramite un browser.**

Quando HTTPS è abilitato, controllare di utilizzare il protocollo corretto (HTTP o HTTPS) durante il tentativo di accesso. Potrebbe essere necessario digitare manualmente `http` o `https` nel campo dell'indirizzo del browser.

Se si è smarrita la password per l'account root, è necessario ripristinare le impostazioni predefinite di fabbrica del dispositivo. Per le istruzioni, vedere *Ripristino delle impostazioni predefinite di fabbrica, on page 23*.

**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)**.

**Il browser non è supportato**

Per un elenco dei browser consigliati, consultare .

**Impossibile accedere al dispositivo dall'esterno**

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 Pro: versione di prova di 90 giorni gratuita, ideale per sistemi di piccole e medie dimensioni.

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

### Problemi relativi ai file audio

**Caricamento clip multimediale non riuscito**

Sono supportati i seguenti formati di clip audio:

- formato au, codifica in µ-law e campionato con 8 o 16 kHz.
- formato wav, codifica in audio PCM. Supporta la codifica come mono o stereo a 8 o 16 bit e frequenza di campionamento da 8 a 48 kHz.
- formato mp3, in mono o stereo con velocità in bit da 64 kbps a 320 kbps e frequenza di campionamento da 8 a 48 kHz.

**Le clip multimediali sono riprodotte a volumi diversi**

Un file audio viene registrato con un determinato guadagno. Se le clip audio sono state create con diversi guadagni, verranno riprodotte con un'intensità diversa. Assicurarsi di utilizzare clip con lo stesso guadagno.

### Problemi con MQTT

**Impossibile collegarsi tramite la porta 8883 con MQTT su SSL**

Il firewall blocca il traffico che utilizza la porta 8883 poiché è considerato non sicuro.

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.

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 relativi all'audio | |
|---|---|
| Il volume del dispositivo non è elevato come previsto | Assicurati che il dispositivo sia chiuso in modo esatto e che non siano presenti ostruzioni nella tromba o nell'elemento dell'altoparlante. |

| Problemi di luce | |
|---|---|
| Il dispositivo non è luminoso come previsto | Assicurati di usare un alimentatore PoE di classe 6.<br><br>Controlla la temperatura ambiente del dispositivo. Se il dispositivo è installato in un ambiente a temperatura elevata, le luci si abbasseranno in automatico. |

## Considerazioni sulle prestazioni

Quando s'imposta il sistema, è importante considerare come le diverse impostazioni e situazioni influiscono sulla larghezza di banda richiesta (bitrate).

I fattori più importanti da considerare:

- Un utilizzo eccessivo della rete dovuto a una scarsa infrastruttura influisce sulla larghezza di banda.
- L'esecuzione simultanea di più applicazioni AXIS Camera Application Platform (ACAP) potrebbe influire sulle prestazioni generali.

## Considerazioni sulla potenza

Le capacità possono essere limitate a seconda della classe PoE utilizzata.

| | |
|---|---|
| PoE classe 6 | Nessuna limitazione. |
| PoE classe 4 | Livello di pressione sonora, luminosità del display e luminosità del LED di segnalazione limitati. |
| Classe PoE 3 | È possibile configurare un prodotto per prepararlo all'installazione, ma il prodotto deve avere classe PoE 4 o 6 per essere utilizzato nell'installazione finale. |

## Contattare l'assistenza

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

## Cyber security

La sicurezza informatica sostiene un ciclo di vita del prodotto ottimale con rischi ridotti al minimo. È possibile trovare informazioni dettagliate e documentazione sul nostro approccio alla sicurezza informatica all'indirizzo *axis.com/about-axis/cybersecurity*. Seguire le linee guida sulla sicurezza informatica riportate di seguito per ricevere le notifiche di sicurezza sui prodotti da parte di Axis e per effettuare la configurazione del prodotto in modo da garantirne un ciclo di vita e una messa fuori servizio sicuri.

All'indirizzo *Axis Trust Center*, è possibile trovare informazioni su come Axis garantisce la conformità alle norme di sicurezza, la trasparenza, la protezione dei dati e la privacy.

### Gestione delle vulnerabilità

Axis è una *Common Vulnerability and Exposures (CVE) Numbering Authority (CNA)*. Per ridurre al minimo il rischio di esposizione, seguiamo gli standard del settore nell'identificazione e nella risoluzione delle vulnerabilità presenti nei nostri dispositivi, software e servizi. Per informazioni sulla nostra politica di gestione delle vulnerabilità o per segnalare una vulnerabilità, fare riferimento a: *axis.com/vulnerability-management*.

### Notifiche di sicurezza

Iscriversi alle e-mail di notifica sulla sicurezza di Axis all'indirizzo *axis.com/security-notification-service*. Verranno inviate informazioni relative alle vulnerabilità, alle relative avvertenze di sicurezza e ad altre questioni relative alla sicurezza del proprio prodotto Axis.

### Ciclo di vita sicuro del prodotto

Axis riduce al minimo i rischi durante l'intero ciclo di vita dei propri prodotti grazie a una gestione sicura del ciclo di vita. Utilizzi le nostre guide al consolidamento disponibili su *help.axis.com* per configurare e utilizzare in modo più sicuro i prodotti Axis e per trovare informazioni su:

**Primo utilizzo sicuro –** I prodotti Axis sono pre-configurati con un elevato livello di protezione predefinito per garantire un'inizializzazione sicura e comunicazioni crittografate sin dall'inizio.

**Uso previsto ed errori comuni di configurazione –** Le nostre guide forniscono informazioni sull'uso previsto dei prodotti Axis, compresi gli errori di configurazione e gli usi impropri più comuni che possono compromettere la sicurezza e che è opportuno evitare.

**Gestione delle vulnerabilità e trasparenza della catena di fornitura –** Ad ogni rilascio del software viene pubblicata una distinta base dei componenti software (SBOM) su *axis.com* al fine di rendere note le vulnerabilità e migliorare la trasparenza della catena di fornitura.

**Messa fuori servizio e cancellazione sicura dei dati –** Per mettere fuori servizio in modo sicuro un prodotto quando raggiunge la fine del suo ciclo di vita, ripristinare le impostazioni predefinite di fabbrica. In questo modo le configurazioni, i dati salvati e le informazioni sensibili verranno cancellati.

T10225649_it

2026-07 (M7.2)

© 2025 – 2026 Axis Communications AB