

## **AXIS C12 Series**

**AXIS C1210-E Network Ceiling Speaker**

**AXIS C1211-E Network Ceiling Speaker**

# AXIS C12 Series

## Sommario

---

<b>Panoramica delle soluzioni</b> .....	3
<b>Installazione</b> .....	4
<b>Introduzione</b> .....	5
Individuazione del dispositivo sulla rete .....	5
Accesso al dispositivo .....	5
<b>Impostazioni supplementari</b> .....	7
Calibrazione ed esecuzione di un test dell'altoparlante da remoto .....	7
Impostazione SIP diretto (P2P) .....	7
Configurazione di SIP tramite un server (PBX) .....	8
Imposta regole per eventi .....	9
<b>Ulteriori informazioni</b> .....	13
Session Initiation Protocol (SIP) .....	13
Peer-to-peer SIP (P2PSIP) .....	13
Private Branch Exchange (PBX) .....	13
NAT traversal .....	14
Applicazioni .....	14
<b>Interfaccia Web</b> .....	15
Stato .....	15
Audio .....	16
Luce .....	18
Registrazioni .....	19
App .....	20
Sistema .....	21
Manutenzione .....	45
<b>Risoluzione di problemi</b> .....	47
Ripristino delle impostazioni predefinite di fabbrica .....	47
Controllo della versione corrente del AXIS OS .....	47
Aggiornare AXIS OS .....	47
Problemi tecnici, indicazioni e soluzioni .....	48
Considerazioni sulle prestazioni .....	49
<b>Specifiche</b> .....	50
Panoramica del dispositivo .....	50
Indicatori LED .....	50
Slot per schede di memoria .....	51
Pulsanti .....	51
Connettori .....	51
<b>Comandi API</b> .....	54

# AXIS C12 Series

## Panoramica delle soluzioni

---

### Panoramica delle soluzioni

Questo manuale descrive come rendere il dispositivo accessibile al sistema audio e come configurare il dispositivo direttamente dalla relativa interfaccia (ad esempio quando si utilizza il dispositivo senza un software per la gestione audio o video).

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:** software di gestione video avanzato per sistemi di grandi dimensioni.
  - *Guida per l'utente di AXIS Camera Station*
- **AXIS Companion:** software per la gestione video per sistemi di piccole dimensioni.
  - *Manuale per l'utente di AXIS Companion*

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



Per guardare questo video, visitare la versione Web di questo documento.

[help.axis.com/?Etpiald=70655&tsection=solution-overview](http://help.axis.com/?Etpiald=70655&tsection=solution-overview)

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

# AXIS C12 Series

## Installazione

---

### Installazione



Per guardare questo video, visitare la versione Web di questo documento.

*[help.axis.com/?etpiald=70655&tsection=solution-overview](http://help.axis.com/?etpiald=70655&tsection=solution-overview)*

Scarica la guida all'installazione (pdf):

- AXIS C1210-E Network Ceiling Speaker  
*[axis.com/products/axis-c1210-e/support#support-resources](http://axis.com/products/axis-c1210-e/support#support-resources)*
- AXIS C1211-E Network Ceiling Speaker  
*[axis.com/products/axis-c1211-e/support#support-resources](http://axis.com/products/axis-c1211-e/support#support-resources)*

# AXIS C12 Series

## Introduzione

---

### Introduzione

#### Individuazione del dispositivo sulla rete

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

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

#### Supporto browser

Il dispositivo può essere utilizzato con i seguenti browser:

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

\*Per usare l'interfaccia Web di AXIS OS con iOS 15 o iPadOS 15, vai a **Impostazioni > Safari > Avanzate > Funzioni sperimentali e disabilita NSURLConnection Websocket**.

Per ulteriori informazioni sui browser consigliati, andare al *Portale AXIS OS*.

#### Accesso al dispositivo

1. Aprire un browser ed inserire il nome di host o l'indirizzo IP del dispositivo Axis.
2. Inserire nome utente e password. Se si accede al dispositivo per la prima volta, è necessario impostare la password di default. Consultare *Impostazione di una nuova password per l'account root alla pagina 5*.

#### Impostazione di una nuova password per l'account root

##### Importante

Il nome utente predefinito dell'amministratore è root. Se si smarrisce la password di root, ripristinare le impostazioni predefinite di fabbrica del dispositivo. Consultare *Ripristino delle impostazioni predefinite di fabbrica alla pagina 47*



Per guardare questo video, visitare la versione Web di questo documento.

[help.axis.com/?&pid=70655&section=set-a-new-password-for-the-root-account](http://help.axis.com/?&pid=70655&section=set-a-new-password-for-the-root-account)

*Suggerimento per il supporto: controllo di conferma sicurezza della password*

1. Digitare una password. Attenersi alle istruzioni sulle password sicure. Consultare *Password sicure alla pagina 6*.

# AXIS C12 Series

## Introduzione

---

2. Ridigitare la password per confermarne la correttezza.
3. Fare clic su **Save (Salva)**. La password è stata configurata.

### Password sicure

#### Importante

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

La password del dispositivo è il sistema di protezione principale dei dati e dei servizi. I dispositivi Axis non impongono un criterio password in quanto potrebbero essere utilizzati in vari tipi di installazioni.

Per proteggere i tuoi dati ti consigliamo vivamente di:

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

# AXIS C12 Series

## Impostazioni supplementari

---

### Impostazioni supplementari

#### 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 l'ambiente circostante cambia, ad esempio, se un muro viene costruito o rimosso, l'altoparlante deve 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.

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. Consultare *Panoramica del dispositivo alla pagina 50* per identificare il pulsante di comando.

#### 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 capire meglio il funzionamento del P2P, consultare *Peer-to-peer SIP (P2PSIP) alla pagina 13*.

Per ulteriori informazioni sulle opzioni di impostazione, consultare *SIP alla pagina 36*.

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 calls (Consenti chiamate 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 diverso.
  - **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 5.061. Se necessario, inserire un numero di porta diverso.
  - **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 il trasporto multimediale è 4.000. Alcuni firewall potrebbero bloccare il traffico RTP su alcuni 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.

# AXIS C12 Series

## Impostazioni supplementari

---

### Nota

Utilizzare NAT traversal quando il dispositivo è collegato alla rete da un router NAT o un firewall. Per ulteriori informazioni, consultare *NAT traversal alla pagina 14*.

6. In **Audio**, selezionare almeno un codec audio con la qualità audio desiderata per le chiamate SIP. Trascinare e rilasciare 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). Il motivo dello scambio è evitare la frammentazione e lo scambio 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 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 capire meglio il funzionamento del P2P, consultare *Private Branch Exchange (PBX) alla pagina 13*.

Per ulteriori informazioni sulle opzioni di impostazione, consultare *SIP alla pagina 36*.

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, consultare *Impostazione SIP diretto (P2P)* alla pagina 7.

### 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.

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

### Invio di un'e-mail in caso di esito negativo di una verifica dell'altoparlante

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

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 Inserire 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)**.

# AXIS C12 Series

## Impostazioni supplementari


---

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 Inserire 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 Fai 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 Vai 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 (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)**.

# AXIS C12 Series

## Impostazioni supplementari

---


### 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. Andare 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. Accanto 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.

# AXIS C12 Series

## Impostazioni supplementari

---

2. Andare a **Sistema > SIP > Impostazioni SIP** e selezionare **Abilita SIP**.
3. Per consentire al dispositivo di ricevere chiamate in entrata, selezionare **Allow incoming calls (Consenti chiamate in arrivo)**.
4. Fare clic su **Salva**.
5. Andare ad **Account SIP**.
6. Accanto all'account SIP, fare clic su  **> Modifica**.
7. Deselezionare **Risposta automatica**.

Riprodurre audio quando viene ricevuta una chiamata SIP:

1. Andare a **Impostazioni > Sistema > Eventi > Regole** e aggiungere una regola.
2. Inserire un nome per la regola.
3. Nell'elenco delle condizioni, selezionare **Stato**.
4. Nell'elenco degli stati, selezionare **Chiamata**.
5. Nell'elenco delle azioni, selezionare **Riproduzione di 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 **Salva**.

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

1. Andare a **Impostazioni > Sistema > Eventi > Regole** e aggiungere una regola.
2. Inserire un nome per la regola.
3. Nell'elenco delle condizioni, selezionare **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 **Stato**.
8. Nell'elenco degli stati, selezionare **Chiamata**.
9. Nell'elenco delle azioni, selezionare **Rispondi alla chiamata**.
10. Fare clic su **Salva**.

# AXIS C12 Series

## Ulteriori informazioni

---

### Ulteriori informazioni

#### 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.

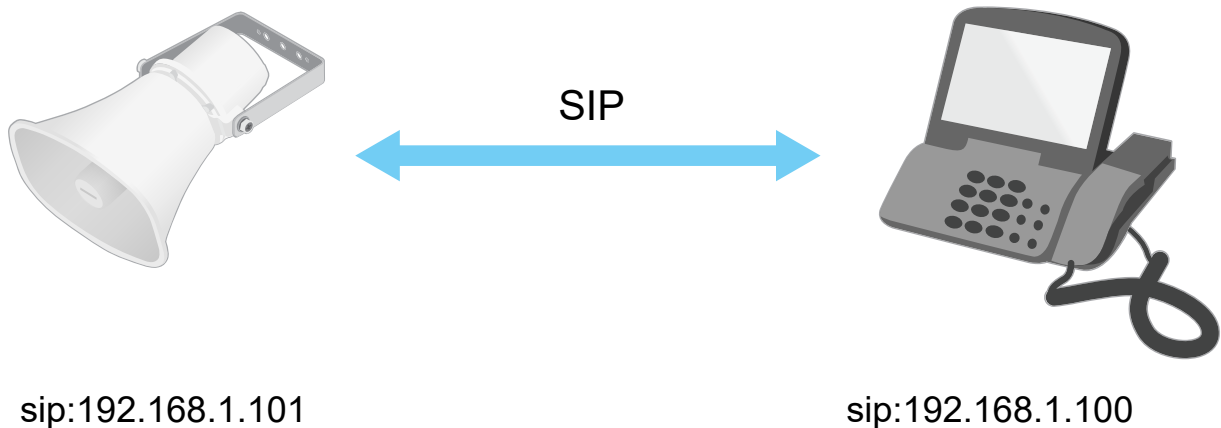
L'audio o il video effettivo viene scambiato tra gli agenti utente SIP con un protocollo di trasporto, ad esempio RTP (Real-Time Transport Protocol).

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.

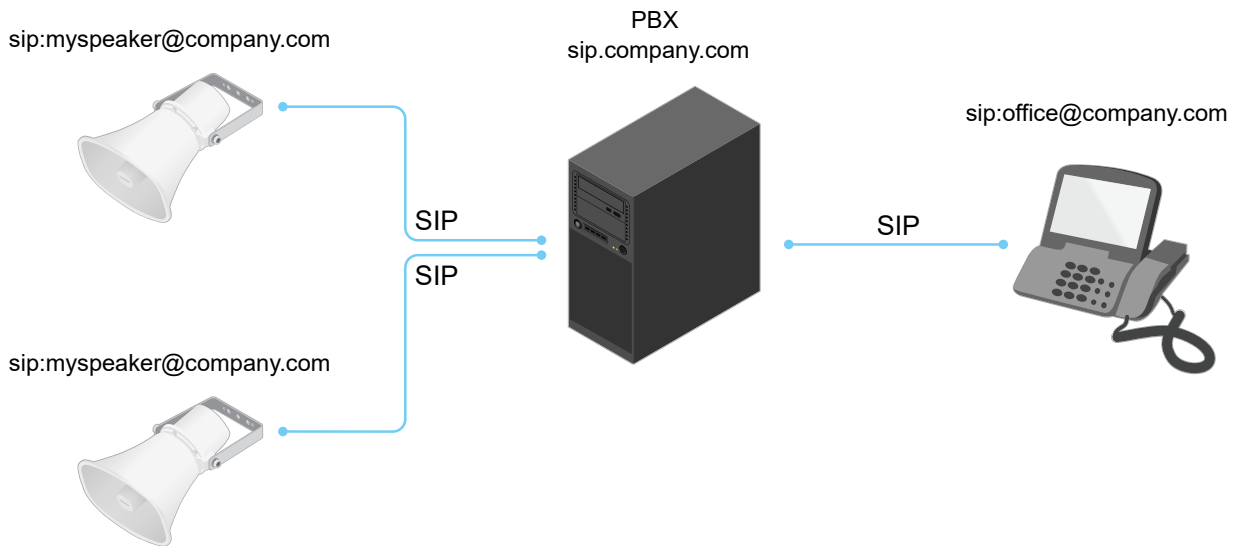
Ogni agente utente SIP si registra con il PBX e può quindi raggiungere gli altri componendo l'estensione corretta. Un tipico indirizzo SIP in questo caso potrebbe essere `sip:<user>@<dominio>` o `sip:<user>@<registrar-ip>`. L'indirizzo SIP è indipendente dal suo indirizzo IP e il PBX rende il dispositivo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

# AXIS C12 Series

## Ulteriori informazioni

---

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®.

Ogni protocollo NAT trasversale può essere utilizzato separatamente o in combinazioni diverse 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 abiliti anche STUN e TURN, migliori le possibilità del protocollo ICE.
- **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 l'indirizzo del 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.

## 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](http://help.axis.com)

# AXIS C12 Series

## Interfaccia Web

### 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 (Cambia account)**: Disconnettersi dall'account corrente e accedere a un nuovo account.
- **Log out (Disconnetti)**: 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 sul sistema audio

Tali informazioni sono mostrate solo per i dispositivi appartenenti a un sito AXIS Audio Manager Edge.

**AXIS Audio Manager Edge**: Lanciare AXIS Audio Manager Edge.

### Individua dispositivo

Mostra le informazioni relative alla posizione dispositivo, compreso il numero di serie e l'indirizzo IP.

**Locate device (Individua dispositivo)**: Riproduce un suono che consente di riconoscere l'altoparlante. Per alcuni dispositivi, sul dispositivo lampeggia un LED.


### Test dell'altoparlante

# AXIS C12 Series

## Interfaccia Web

---

Mostra se l'altoparlante è stato calibrato o no.

 **Speaker test (Test altoparlante):** : Calibra l'altoparlante. Porta alla pagina **Speaker test (Test degli altoparlanti)** dove si può eseguire la calibrazione e il test degli altoparlanti.

### Informazioni dispositivo

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 **Date and time (Data e ora)** 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.

### Connected clients (Client 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.

**Recordings (Registrazioni):** Consente di visualizzare le registrazioni in corso e quelle filtrate oltre alla relativa origine. Per ulteriori informazioni, vedere *Registrazioni alla pagina 19*



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

## Audio

### AXIS Audio Manager Edge

**AXIS Audio Manager Edge:** Avviare l'applicazione.



# AXIS C12 Series

## Interfaccia Web

---

### Impostazioni dispositivo

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

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

**Input type (Tipo di input)**  : selezionare il tipo di input.

**Power type (Tipo di alimentazione)**  : Selezionare il tipo di alimentazione.

**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.


### Flusso


**Encoding (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.

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

### 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.
- **Delete (Elimina):** Elimina la clip audio dal dispositivo.

# AXIS C12 Series

## Interfaccia Web

---

### Ascolta e registra



Fare clic per ascoltare.



Avvia una registrazione continua del flusso audio in diretta. Fare clic di nuovo per arrestare la registrazione. Se è in corso una registrazione, riprenderà in automatico dopo un riavvio.

#### Nota

È possibile ascoltare e registrare solo se l'input è attivato per il dispositivo. Andare a **Audio > Device settings (Audio > Impostazioni dispositivo)** per verificare che l'input sia attivato.



Mostra la memoria configurata per il dispositivo. Per configurare il dispositivo di archiviazione è necessario aver eseguito l'accesso come amministratore.

### Sicurezza del sito audio

**CA certificate (Certificato CA):** Selezionare il certificato da utilizzare quando si aggiungono dispositivi al sito audio. È necessario abilitare l'autenticazione TLS in AXIS Audio Manager Edge.

**Save (Salva):** Attivare e salvare la selezione.

### Test altoparlante

Puoi usare la verifica dell'altoparlante per verificare in modo remoto se l'altoparlante funziona come previsto.

**Calibrate (Calibra):** È necessario calibrare l'altoparlante prima della prima verifica. Durante la calibrazione, l'altoparlante riproduce una serie di tonalità di test misurate dal microfono incorporato. Quando calibri l'altoparlante, deve essere installato nella sua posizione finale. Se sposti l'altoparlante in seguito o se le zone circostanti cambiano, ad esempio, se un muro viene costruito o rimosso, devi ricalibrare l'altoparlante.

**Run the test (Esegui il test):** Esegui la riproduzione della stessa serie di tonalità di verifica riprodotte durante la calibrazione e paragonale ai valori registrati della calibrazione.

## Luce

### Panoramica

#### Stato della luce

Visualizza le diverse attività di illuminazione in esecuzione sul dispositivo. Nell'elenco di stato della luce possono essere eseguite fino a 10 attività contemporaneamente. Quando due o più attività vengono eseguite contemporaneamente, quella con la priorità più alta mostra lo stato della luce. La riga verrà evidenziata in verde nell'elenco di stato.

### Profili

#### Profili

Un profilo è una raccolta di configurazioni impostate. È possibile avere fino a 30 profili con diverse priorità e schemi. I profili vengono elencati per fornire una panoramica del nome, della priorità e delle impostazioni della luce e delle sirene.

# AXIS C12 Series



## Interfaccia Web

**+** **Create (Crea):** Fai clic per creare un nuovo profilo.

- **Preview/Stop preview (Anteprima/Arresta anteprima):** Avviare o arrestare un'anteprima del profilo prima di salvarlo.

**Nota**  
Non è possibile avere due profili con lo stesso nome.



- **Name (Nome):** inserire un nome per il profilo.
- **Description (Descrizione):** inserire una descrizione del profilo.
- **Light (Luce):** selezionare dal menu a discesa il tipo di **Pattern (schema)**, **Speed (velocità)**, **Intensity (intensità)** e **Color (colore)** della luce desiderato.
- **Siren (Sirena):** selezionare dal menu a discesa il tipo di **Pattern (schema)** e **Intensity (intensità)** della sirena desiderato.

-   Avviare o interrompere un'anteprima solo della luce o della sirena.
- **Duration (Durata):** impostare la durata delle attività.
  - **Continuous (Continua):** una volta avviata, viene eseguita fino all'arresto.
  - **Time (Ora):** impostare un tempo specificato per la durata dell'attività.
  - **Repetitions (Ripetizioni):** impostare quante volte l'attività deve ripetersi.
- **Priority (Priorità):** impostare la priorità di un'attività su un numero compreso tra 1 e 10. Le attività con numero di priorità al di sopra di 10 non si possono rimuovere dall'elenco di stato. Esistono tre attività con priorità superiore a 10; **Maintenance (Manutenzione)** (11), **Identify (Identifica)** (12) e **Health check (Controllo integrità)** (13).


**+** **Import (Importa):** aggiungere uno o più profili con configurazione predefinita.

- **Add (Aggiungi):** aggiungere nuovi profili.
- **Delete and add (Elimina e aggiungi):** i profili vecchi vengono eliminati ed è possibile caricare i nuovi profili.
- **Overwrite (Sovrascrivi):** i profili aggiornati sovrascrivono i profili esistenti.

Per copiare un profilo e salvarlo in altri dispositivi, selezionare uno o più profili e fare clic su **Export (Esporta)**. Viene esportato un file .json.

-  Avvia profilo. Il profilo e le sue attività vengono visualizzati nell'elenco di stato.
-  Scegliere le seguenti operazioni per il profilo **Edit (Modifica)**, **Copy (Copia)**, **Export (Esporta)** o **Delete (Elimina)**.

## Registrazioni

-  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.

**Storage (Archiviazione):** mostra le registrazioni in base al tipo di dispositivo di archiviazione.

# AXIS C12 Series


## Interfaccia Web


**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.


## App

 **Add 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.

**Allow unsigned apps (Consenti app non firmate)**  : Attiva per permettere che siano installate app senza firma.

**Allow root-privileged apps (Permetti app con privilegi root)**  : Abilitare per consentire l'accesso completo al dispositivo alle app con privilegi root.

 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.

# AXIS C12 Series

## Interfaccia Web

**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](http://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.
- **Deactivate the license (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.
- **Delete (Elimina):** Cancella permanentemente l'app dal dispositivo. La licenza resta attiva a meno che non la disattivi prima.

## Sistema

### Ora e ubicazione

#### Data e ora

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

#### Nota

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

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

- **Automatic date and time (manual NTS KE servers) (Data e ora automatiche (server NTS KE manuali)):** eseguire la sincronizzazione con i server NTP key establishment sicuri connessi al server DHCP.
  - **Manual NTS KE servers (Server NTS KE manuali):** inserisci l'indirizzo IP di uno o due server NTP. Quando usi due server NTP, l'ora del dispositivo viene sincronizzata e adattata sulla base dell'input di entrambi.
  - **Max NTP poll time (Tempo massimo poll NTP):** Selezionare il tempo massimo di attesa del dispositivo prima di eseguire il polling del server NTP per ottenere un'ora aggiornata.
  - **Min NTP poll time (Tempo min poll NTP):** Selezionare il tempo minimo di attesa del dispositivo prima di eseguire il polling del server NTP per ottenere un'ora aggiornata.
- **Automatic date and time (NTP servers using DHCP) (Data e ora automatiche (server NTP tramite DHCP)):** esegui la sincronizzazione con i server NTP connessi al server DHCP.
  - **Fallback NTP servers (Server NTP di fallback):** inserisci l'indirizzo IP di uno o due server fallback.
  - **Max NTP poll time (Tempo massimo poll NTP):** Selezionare il tempo massimo di attesa del dispositivo prima di eseguire il polling del server NTP per ottenere un'ora aggiornata.
  - **Min NTP poll time (Tempo min poll NTP):** Selezionare il tempo minimo di attesa del dispositivo prima di eseguire il polling del server NTP per ottenere un'ora aggiornata.
- **Automatic date and time (manual NTP servers) (Data e ora automatiche (server NTP manuali)):** esegui la sincronizzazione con i server NTP scelti.
  - **Manual NTP servers (Server NTP manuali):** inserisci l'indirizzo IP di uno o due server NTP. Quando usi due server NTP, l'ora del dispositivo viene sincronizzata e adattata sulla base dell'input di entrambi.
  - **Max NTP poll time (Tempo massimo poll NTP):** Selezionare il tempo massimo di attesa del dispositivo prima di eseguire il polling del server NTP per ottenere un'ora aggiornata.
  - **Min NTP poll time (Tempo min poll NTP):** Selezionare il tempo minimo di attesa del dispositivo prima di eseguire il polling del server NTP per ottenere un'ora aggiornata.

# AXIS C12 Series

## Interfaccia Web

• **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)**.  
**Time zone (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):** Inserire la direzione della bussola verso cui è diretto il dispositivo. 0 punta a nord.
- **Label (Etichetta):** Inserire un nome descrittivo per il dispositivo.
- **Save (Salva):** Fare clic per salvare la posizione del dispositivo.

## Rete

### IPv4 (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.

**IP address (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.

### Hostname (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.

**Hostname (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 -.

# AXIS C12 Series

## Interfaccia Web

---

### DNS servers (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 and HTTPS (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 inserire 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 inserire qualsiasi porta nell'intervallo da 1 a 1023. Se si utilizza una porta in questo intervallo, viene visualizzato un avviso.

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

### Protocolli di rilevamento della rete

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

**Bonjour name (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 (Nome UPnP):** 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.

### One-click cloud connection (Connessione a 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](https://axis.com/end-to-end-solutions/hosted-services).

# AXIS C12 Series

## Interfaccia Web

### Allow O3C (Consenti O3C):

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

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

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

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

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

### Authentication method (Metodo di autenticazione):

- **Basic (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.
- **Auto (Automatica):** questa opzione consente al dispositivo Axis di selezionare il metodo di autenticazione a seconda dei metodi supportati, dando priorità a **Digest** rispetto al metodo **Basic (Base)**.

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

## SNMP (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 (pubblico)**.
  - **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 (scrittura)**.
  - **Activate traps (Attiva trap):** Attivare la segnalazione di trap. Il dispositivo utilizza i trap per inviare messaggi per eventi importanti o cambi di stato a un sistema di gestione. Nell'interfaccia Web, è possibile impostare trap per SNMP v1 e v2c. I trap vengono disattivati automaticamente se si cambia in SNMP v3 o si disattiva SNMP. Se si utilizza SNMP v3, è possibile impostare i trap tramite l'applicazione di gestione SNMP v3.
  - **Trap address (Indirizzo trap):** immettere l'indirizzo IP o il nome host del server di gestione.
  - **Trap community (Comunità trap):** Immettere la comunità da utilizzare quando il dispositivo invia un messaggio trap al sistema di gestione.
  - **Traps (Trap):**
    - **Cold start (Avvio a freddo):** Invia un messaggio di trap all'avvio del dispositivo.
    - **Warm start (Avvio a caldo):** Invia un messaggio trap quando si modifica un'impostazione SNMP.
    - **Link up:** invia un messaggio trap quando un collegamento cambia dal basso verso l'alto.
    - **Authentication failed (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



# AXIS C12 Series

## Interfaccia Web

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 impostata 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

### Certificates (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 impostazioni 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.

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



Il menu contestuale contiene:

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

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

- **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

# AXIS C12 Series

## Interfaccia Web

---

### 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.

**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.

**Prevent brute-force attacks (Prevenire gli attacchi di forza bruta)**

# AXIS C12 Series

## Interfaccia Web

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

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

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

### Firewall

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

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

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

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

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



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

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

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

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

#### Nota

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

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

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



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



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

### Certificato AXIS con firma personalizzata

# AXIS C12 Series

## Interfaccia Web

---

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):** inserire 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)**.
  - L'aggiunta di app.
- **Viewer (Visualizzatore):** non ha l'accesso alla modifica di alcuna impostazioni.




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.

#### Anonymous access (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

# AXIS C12 Series

## Interfaccia Web

---



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

- **Restrict root access (Limita accesso root):** Attivare per limitare la funzionalità che richiede l'accesso root.
- **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):** inserire 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.

**Enabled (Abilitato):** 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 (-).

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

**Type (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.
- **Delete (Elimina):** eliminare l'host virtuale.

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

### OpenID Configuration (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 essere `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.

# AXIS C12 Series

## Interfaccia Web

---

**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.



**Add a rule (Aggiungi una regola):** Creare una regola.

**Name (Nome):** Inserire 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.



**Add a condition (Aggiungi 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.

# AXIS C12 Series

## Interfaccia Web

Il dispositivo potrebbe avere alcune delle seguenti regole preconfigurate:

**Front-facing LED Activation: LiveStream (Attivazione LED frontale: LiveStream):** quando il microfono è acceso e viene ricevuto un flusso dal vivo, il LED frontale sul dispositivo audio diventa verde.

**Front-facing LED Activation: Recording (Attivazione LED frontale: Registrazione):** quando il microfono è acceso ed è in corso una registrazione, il LED frontale sul dispositivo audio diventa verde.

**Front-facing LED Activation: SIP (Attivazione LED frontale: SIP):** quando il microfono è acceso e una chiamata SIP è attiva, il LED frontale sul dispositivo audio diventa verde. SIP deve essere abilitato sul dispositivo audio prima che questo evento possa essere attivato.

**Pre-announcement tone: Play tone on incoming call (Tono pre-annuncio: Riproduci tono in caso di chiamata in arrivo):** quando viene effettuata una chiamata SIP al dispositivo audio, viene riprodotta una clip audio predefinita. SIP deve essere abilitato per il dispositivo audio. Per consentire al chiamante SIP di ascoltare una suoneria durante la riproduzione della clip audio, è necessario configurare l'account SIP per il dispositivo audio in modo da non rispondere automaticamente alla chiamata.

**Pre-announcement tone: Answer call after incoming call-tone (Tono di preannuncio: rispondi alla chiamata dopo tono chiamata in arrivo):** una volta terminata la clip audio, la chiamata SIP in entrata riceve risposta. SIP deve essere abilitato per il dispositivo audio.

**Loud ringer (Suoneria ad alto volume):** quando viene effettuata una chiamata SIP al dispositivo audio, viene riprodotta una clip audio predefinita fino a quando la regola è attiva. SIP deve essere abilitato per il dispositivo audio.

### Destinatari

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


**Name (Nome):** immettere un nome per il destinatario.

**Type (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)**.
  - **Port (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:** Inserire 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.

# AXIS C12 Series

## Interfaccia Web

- **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:** Inserire 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.
  - **Share (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)**.
  - **Port (Porta):** Immettere il numero della porta utilizzata dal server SFTP. Il valore 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 esadecimale). 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 or VMS (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.
- **Email (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.



# AXIS C12 Series

## Interfaccia Web

- **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.
- **Port (Porta):** inserire il numero della porta per il server SMTP, utilizzando i valori nell'intervallo da 0 a 65535. Il valore predefinito è 587.
- **Encryption (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 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 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)**.
- **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 una vasta gamma di settori per collegare dispositivi remoti con un'impronta di codice ridotta e una larghezza di banda di rete minima. 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.

Potrai trovare maggiori informazioni relative a MQTT consultando l'*AXIS OS Portal*.

### ALPN (RETE ALPN)

# AXIS C12 Series

## Interfaccia Web

---

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.

### MQTT client (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.

**Port (Porta):** Immettere il numero di porta.

- 1883 è il valore predefinito per MQTT su 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.

### Connect message (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.

# AXIS C12 Series

## Interfaccia Web

---

**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.

### Last Will and Testament message (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.

### MQTT publication (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.

### MQTT subscriptions (Sottoscrizioni MQTT)

# AXIS C12 Series

## Interfaccia Web



**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.

### MQTT overlays (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 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.

## SIP

### Settings (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):** selezionare questa opzione per rendere possibile l'avvio e la ricezione di chiamate SIP.

**Allow incoming calls (Permetti chiamate in arrivo):** Selezionare questa opzione per consentire le chiamate in arrivo da altri dispositivi SIP.

#### Call handling (Gestione chiamate)

- **Calling timeout (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.

#### Ports (Porte)

Un numero di porta deve essere compreso tra 1.024 e 65.535.

- **SIP port (Porta SIP):** 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, immettere un numero di porta diverso.

# AXIS C12 Series

## Interfaccia Web

- **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, immettere un numero di porta diverso.
- **Porta di avvio RTP:** porta di rete utilizzata per il primo streaming multimediale RTP in una chiamata SIP. Il numero di porta di avvio predefinito è 4.000. Alcuni firewall bloccano il traffico RTP su determinati numeri di porta.

### NAT traversal (Attraversamento NAT)

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 le 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. Immettere l'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. Immettere l'indirizzo del server TURN e le informazioni di accesso.

### Audio (Audio)

- **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.

### Additional (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 1.300 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.
- 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. Quando si effettua una chiamata API (interfaccia per la programmazione di applicazioni) VAPIX\* senza specificare da quale account SIP effettuare la chiamata viene sempre utilizzato l'account predefinito.

**+** **Add account (Aggiungi account):** Fare 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 (Dai 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.
- **Name (Nome):** inserire un nome descrittivo. Può, ad esempio, essere il nome e il cognome, un ruolo o una posizione. Il nome non è univoco.
- **User ID (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, immetti il nome dominio pubblico. Verrà visualizzato come parte dell'indirizzo SIP durante la chiamata ad altri account.
- **Password:** immettere la password associata all'account SIP per l'autenticazione al server SIP.
- **Authentication ID (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.
- **Caller ID (ID chiamante):** nome indicato al destinatario delle chiamate dal dispositivo.
- **Registrar:** immettere l'indirizzo IP per l'account registrar.
- **Transport mode (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):** attivare 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.
- **Proxies (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.

# AXIS C12 Series

## Interfaccia Web

---

- **Resolution (Risoluzione):** selezionare la risoluzione da utilizzare per le chiamate video. La risoluzione influisce sulla larghezza di banda necessaria.
- **Frame rate (Velocità in fotogrammi):** selezionare il numero di fotogrammi al secondo per le chiamate video. La velocità in fotogrammi influisce sulla larghezza di banda necessaria.
- **H.264 profile (Profilo H.264):** selezionare il profilo da utilizzare per le chiamate video.

### DTMF (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)**.

**Sequence (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.

### Protocols (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 al livello applicativo, in genere correlate alla sessione.

### Chiamata di prova

**SIP account (Account SIP):** selezionare da quale account eseguire la chiamata di prova.

**SIP address (Indirizzo SIP):** immettere un indirizzo SIP e fare clic su  per effettuare una chiamata di test e verificare il funzionamento dell'account.

### Elenco di accesso

**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 origine):** 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.

### Controller multicast

# AXIS C12 Series

## Interfaccia Web

User multicast controller (Controller multicast utente): Attivare il controller multicast.

Audio codec (Codec audio): Seleziona un codec audio.



Sorgente: Aggiungere un nuova sorgente controller multicast.

- Label (Etichetta): Inserire il nome di un'etichetta che non è già utilizzata da un'origine.
- Origine: Inserire un'origine.
- Port (Porta): Inserire una porta.
- Priority (Priorità): Selezionare una priorità.
- Profile (Profilo): Selezionare un profilo.
- SRTP key (Chiave SRTP): Inserire una chiave SRTP.



Il menu contestuale contiene:

Edit (Modifica): Modifica la sorgente controller multicast.

Delete (Elimina): Eliminare l'origine del dispositivo di controllo multicast.

## Archiviazione

### Network storage (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.

- Address (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. Digita 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 disassociare 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.

Tools (Strumenti)



# AXIS C12 Series

## Interfaccia Web

- **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.

### Onboard storage (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 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 la scheda di memoria diventa piena.

#### Tools (Strumenti)

- **Check (Controlla):** verificare la presenza di eventuali errori nella scheda di memoria. Questa opzione è valida solo per il file system ext4.
- **Repair (Ripara):** corregge gli errori nel file system ext4. Per correggere gli errori in una scheda di memoria con file system VFAT, espellere la scheda di memoria, inserirla in un computer ed eseguire un riparazione degli errori del disco.
- **Format (Formatta):** formatta la scheda di memoria, ad esempio quando necessario per modificare il file system o per cancellare rapidamente tutti i dati. VFAT e ext4 sono le due opzioni di file system disponibili. Il formato consigliato è ext4, grazie alla relativa resilienza rispetto alla perdita di dati se la scheda viene espulsa o in caso di drastica perdita di alimentazione. Tuttavia, avrai bisogno di un'applicazione o un driver ext4 di terze parti per accedere al file system da Windows®.
- **Encrypt (Codifica):** Utilizza questo strumento per la formattazione della scheda di memoria e l'abilitazione della crittografia. **Encrypt (Codifica)** risulta nell'eliminazione di tutti i dati archiviati sulla scheda di memoria. Dopo aver usato **Encrypt (Codifica)**, i dati archiviati nella scheda di memoria saranno protetti da crittografia.
- **Decrypt (Decodifica):** Usa questo strumento per la formattazione della scheda di memoria senza crittografia. **Decrypt (Decodifica)** risulta nell'eliminazione di tutti i dati archiviati sulla scheda di memoria. Dopo aver usato **Decrypt (Decodifica)**, i dati archiviati nella scheda di memoria non saranno protetti da crittografia.
- **Change password (Cambia password):** modifica la password che serve per la crittografia della scheda di memoria.

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

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

## ONVIF

Account ONVIF

# AXIS C12 Series

## Interfaccia Web

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](http://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.

**+** **Add media profile (Aggiungi profilo multimediale):** Fare clic per aggiungere un nuovo profilo di supporti ONVIF.

**Profile name (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.


# AXIS C12 Series

## Interfaccia Web


- **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.

**Audio encoder (Registratore 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.

**Audio decoder (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.

**Audio output (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

### Audio detection (Rilevamento di suoni)

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 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.

## Accessori

### I/O ports (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.



# AXIS C12 Series

## Interfaccia Web

### Port (Porta)

**Name (Nome):** modificare il testo per rinominare la porta.


**Direction (Direzione):**  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 V CC.

#### 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.

## Registri

### Report e registri

#### Reports (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.

#### Logs (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.

### Network trace (Analisi della rete)

#### Importante

È possibile che un file di analisi della rete contenga informazioni riservate, ad esempio 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**.

### Registro di sistema remoto

# AXIS C12 Series

## Interfaccia Web

---

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:** inserire 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)

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

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

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

### Configurazione normale

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

### Manutenzione

**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)
- Static IP address (Indirizzo IP statico)
- Default router (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](http://axis.com).

# AXIS C12 Series

## Interfaccia Web

---

**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](http://axis.com/support).

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

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

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

# AXIS C12 Series

## Risoluzione di problemi

---

### Risoluzione di 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 ai valori predefiniti di fabbrica:

1. Scollegare l'alimentazione dal dispositivo.
2. Tenere premuto il pulsante di comando quando si ricollega l'alimentazione. Consultare *Panoramica del dispositivo alla pagina 50*.
3. Tenere premuto il pulsante di comando per 10 secondi finché l'indicatore LED di stato non emette nuovamente una luce gialla.
4. Rilasciare il pulsante di comando. Il processo è completo quando il LED di stato diventerà verde. Il dispositivo è stato reimpostato alle impostazioni di fabbrica predefinite. Se nessun server DHCP è disponibile sulla rete, l'indirizzo IP predefinito è 192.168.0.90.
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)**.

#### 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. Consultare 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](http://axis.com/support/device-software).

1. Scarica il file AXIS OS sul tuo computer, disponibile gratuitamente su [axis.com/support/device-software](http://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)**.

# AXIS C12 Series

## Risoluzione di problemi

---

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

### Problemi tecnici, indicazioni e soluzioni

Se non si riesce a individuare qui ciò che si sta cercando, provare a vedere la sezione relativa alla risoluzione dei problemi all'indirizzo [axis.com/support](http://axis.com/support).

#### Problemi durante l'aggiornamento del firmware

---

Errore durante l'aggiornamento del firmware	Se l'aggiornamento del firmware non riesce, il dispositivo ricarica il firmware precedente. Il motivo più comune è il caricamento di un firmware errato. Controllare che il nome del file del firmware corrisponda al dispositivo e riprovare.
---	--

#### 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 <code>ping</code> 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

---

Impossibile eseguire l'accesso	Se HTTPS è abilitato, assicurarsi di utilizzare il protocollo corretto (HTTP o HTTPS) quando si tenta di eseguire l'accesso. Potrebbe essere necessario digitare manualmente <code>http</code> o <code>https</code> nel campo dell'indirizzo del browser.
--------------------------------	---

Se si dimentica la password per l'utente root, il dispositivo deve essere ripristinato alle impostazioni predefinite di fabbrica. Consultare *Ripristino delle impostazioni predefinite di fabbrica alla pagina 47*.

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).
---	---

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 <b>Settings &gt; System &gt; Date and Time (Impostazioni &gt; Sistema &gt; Data e ora)</b> .
--	--

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

---

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

- AXIS Camera Station: versione di prova di 30 giorni gratuita, ideale per sistemi di piccole e medie dimensioni. Per istruzioni e download, visitare [axis.com/vms](http://axis.com/vms).



# AXIS C12 Series

## Risoluzione di problemi

---

### Problemi relativi ai file audio

---

Caricamento clip multimediale non riuscito

Sono supportati i seguenti formati di clip audio:

- formato au, codifica in  $\mu$ -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.

### Considerazioni sulle prestazioni

Durante la configurazione del sistema, è importante considerare come le varie impostazioni e situazioni influiscono sulla quantità di larghezza di banda (velocità di trasmissione) necessaria.

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

- 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.

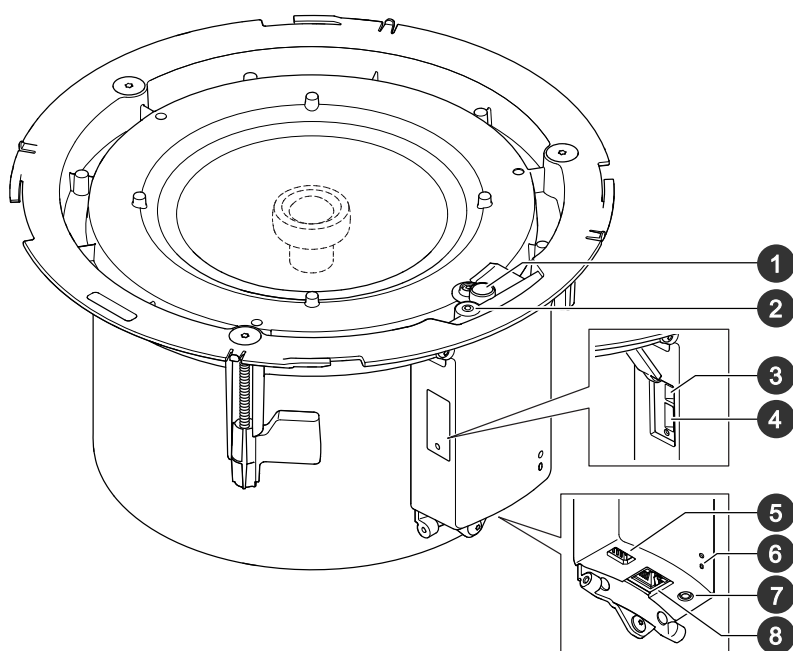
# AXIS C12 Series

## Specifiche

---

### Specifiche

#### Panoramica del dispositivo



- 1 LED frontale
- 2 Pulsante di comando alla pagina 51
- 3 Switch di disabilitazione microfono alla pagina 51
- 4 Slot per schede di memoria alla pagina 51
- 5 Connettore I/O alla pagina 52
- 6 LED di stato
- 7 Connettore audio alla pagina 51
- 8 Connettore di rete alla pagina 51

#### Indicatori LED

LED di stato	Indicazione
Spento	Spento per condizioni di normale funzionamento.
Verde	Luce verde fissa: condizioni di normale utilizzo.
Giallo	Luce fissa durante l'avvio e quando si ripristinano le impostazioni.
Rosso	Luce lampeggiante lenta per aggiornamento non riuscito.
Rosso/Verde	Luce lampeggiante veloce tra rosso e verde quando identifica la selezione di un dispositivo audio.

# AXIS C12 Series

## Specifiche

---

### Slot per schede di memoria

#### **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](http://axis.com) per i consigli sulla scheda di memoria.



I loghi SD, SDHC e SDXC sono marchi di SD-3C LLC. SD, SDHC e SDXC sono marchi di fabbrica o registrati di proprietà di SD-3C, LLC negli Stati Uniti, in altri Paesi o in entrambi.

### 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. Consultare *Ripristino delle impostazioni predefinite di fabbrica alla pagina 47*.

#### Switch di disabilitazione microfono

Per la posizione dello switch di disabilitazione del microfono, vedere *Panoramica del dispositivo alla pagina 50*.

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

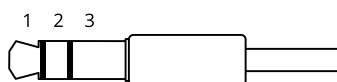
Connettore Ethernet RJ45 con Power over Ethernet (PoE+).

#### **AVVISO**

Il dispositivo deve essere collegato tramite 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](http://www.axis.com).

#### Connettore audio

- Ingresso audio - input da 3,5 mm per microfono stereo o segnale stereo.



Input audio

# AXIS C12 Series

## Specifiche

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

### Output audio

1 Punta	2 Anello	3 Guaina
Canale 1, linea non bilanciata, mono	Canale 1, linea non bilanciata, mono	Massa
Linea bilanciata, segnale "caldo"	Linea bilanciata, segnale "freddo"	Massa
Linea non bilanciata stereo, "sinistra"	Linea non bilanciata stereo, "destra"	Massa
Canale 1, linea non bilanciata	Canale 2, linea non bilanciata	Massa

Il microfono interno viene utilizzato per impostazione predefinita; il microfono esterno viene utilizzato quando connesso.

### Connettore I/O

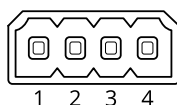
Utilizzare il connettore I/O con dispositivi esterni in combinazione con, ad esempio, rilevamento movimento, attivazione di eventi e notifiche di allarme. Oltre al punto di riferimento 0 V CC e all'alimentazione (output 12 V CC), il connettore I/O fornisce l'interfaccia per:

**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 rilevatori di rottura.

**Ingresso supervisionato** – Consente di rilevare le manomissioni su un ingresso 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



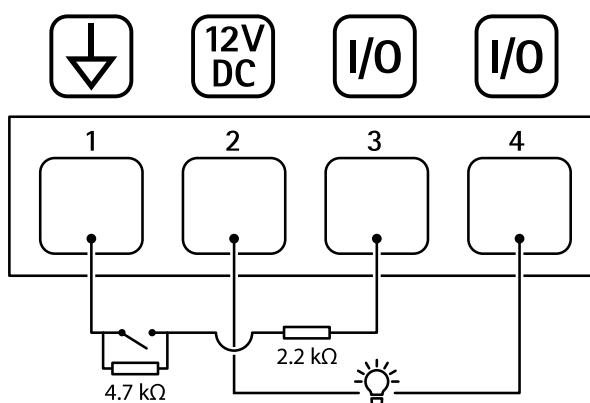
Funzione	Pin	Note	Specifiche
Terra CC	1		0 V CC
Uscita CC	2	Può essere utilizzato per alimentare una periferica ausiliaria. Nota: questo pin può essere usato solo come uscita alimentazione.	12 V CC Carico massimo = 50 mA

# AXIS C12 Series

## Specifiche

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 Uscita CC 12 V, max 50 mA
- 3 I/O configurato come ingresso supervisionato
- 4 I/O configurato come uscita

# AXIS C12 Series

## Comandi API

---

### Comandi API

VAPIX® è l'API aperta (interfaccia per la programmazione di applicazioni) di Axis. È possibile controllare quasi tutte le funzionalità disponibili nei dispositivi Axis tramite VAPIX®. Per accedere alla documentazione VAPIX® completa, unisciti alla Axis Developer Community all'indirizzo [axis.com/developer-community](http://axis.com/developer-community)

Inserire i comandi in un browser Web e sostituire <deviceIP> con l'indirizzo IP o il nome host del dispositivo.

#### Importante

I comandi API vengono eseguiti immediatamente. Se il dispositivo viene ripristinato, tutte le impostazioni andranno perse. Ad esempio le regole di azione.

#### Esempio:

Riavviare il dispositivo

#### Richiesta

`http://<deviceIP>/axis-cgi/restart.cgi`

#### Esempio:

Ripristinare il dispositivo. La richiesta restituisce la maggior parte delle impostazioni ai valori predefiniti, ma mantiene il numero IP.

#### Richiesta

`http://<deviceIP>/axis-cgi/factorydefault.cgi`

#### Esempio:

Reimpostare il dispositivo. La richiesta restituisce tutte le impostazioni incluso il numero IP ai valori predefiniti.

#### Richiesta

`http://<deviceIP>/axis-cgi/hardfactorydefault.cgi`

#### Esempio:

Vedere un elenco di tutti i parametri del dispositivo.

#### Richiesta

`http://<deviceIP>/axis-cgi/param.cgi?action=list`

#### Esempio:

Ottieni un archivio di debug

#### Richiesta

`http://<deviceIP>/axis-cgi/debug/debug.tgz`

#### Esempio:

Ottieni un report del server

#### Richiesta

`http://<deviceIP>/axis-cgi/serverreport.cgi`

#### Esempio:

Acquisizione di una traccia di rete di 300 secondi

#### Richiesta

`http://<deviceIP>/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=300`

#### Esempio:

Abilita FTP

#### Richiesta

`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=yes`

# AXIS C12 Series

## Comandi API

---

Esempio:

Disabilita FTP

**Richiesta**

`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no`

Esempio:

Abilita SSH

**Richiesta**

`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=yes`

Esempio:

Disabilita SSH

**Richiesta**

`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no`

