AXIS I7010-VE Network Intercom

AXIS I7010-VE Network Intercom
AXIS I7010-VE Safety Network Intercom

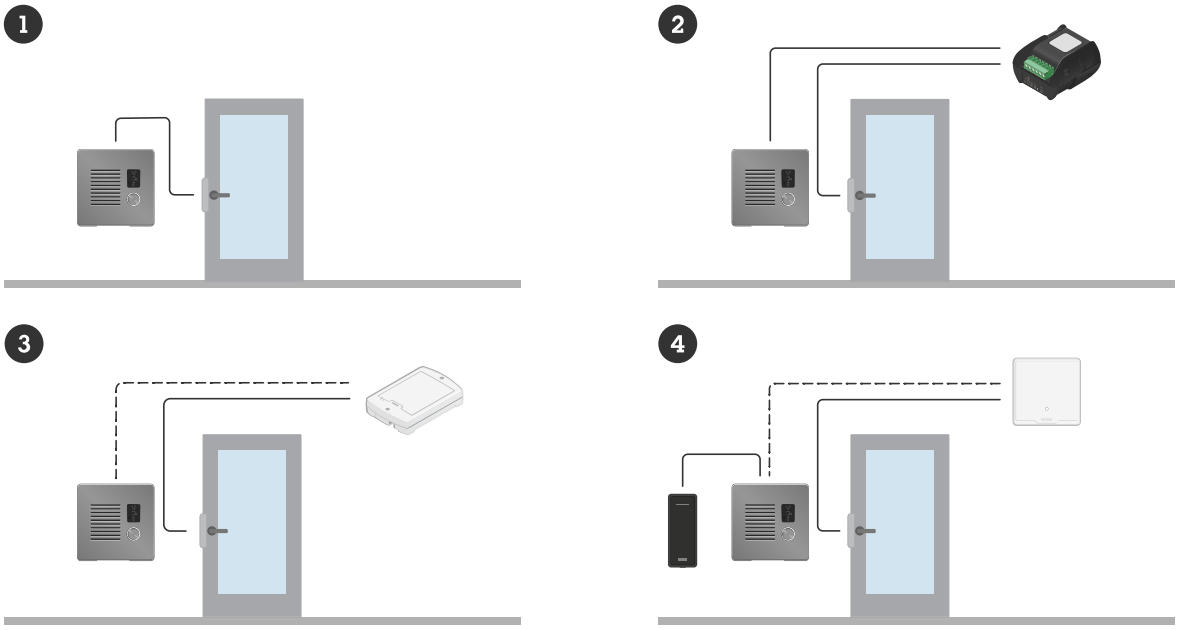
Manuale dell'utente

Indice

Panoramica dell'impostazione 4
Impostazioni preliminari 5
Individuazione del dispositivo sulla rete 5
Supporto browser 5
Aprire l'interfaccia Web del dispositivo 5
Creare un account amministratore 5
Password sicure 6
Accertarsi che nessuno abbia manomesso il software del dispositivo 6
Configurare il dispositivo 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
Include il flusso video dalla telecamera vicina nella chiamata SIP 9
Creazione di un contatto 9
Configurazione del pulsante di chiamata 9
Utilizzare DTMF per sbloccare la porta per un visitatore 10
Utilizzare l'Elenco accessi per consentire ai titolari credenziali di aprire la porta. 10
Imposta regole per eventi 11
Attivazione di un'azione 11
Interfaccia Web 12
Per saperne di più 13
Voice over IP (VoIP) 13
Session Initiation Protocol (SIP) 13
Peer-to-peer SIP (P2PSIP) 13
Private Branch Exchange (PBX) 14
NAT Traversal 15
Analisi e app 15
AXIS Client for Unified Communication Systems 15
Dati tecnici 16
Panoramica dei prodotti 16
Indicatori e comandi del pannello anteriore 16
Icone degli indicatori 16
Indicatori LED 17
Slot per scheda SD 17
Pulsanti 17
Pulsante di comando 17
Connettori 17
Connettore di rete 17
Connettore audio 17
I/O, lettore e connettore relè 18
Collegare le apparecchiature 20
Lettore Axis 20
Relè alimentato da PoE (12V) 20
Relè alimentato da un alimentatore separato 20
Relè senza potenziali 21
Blocco di protezione intrinseca a 12V alimentato da PoE dall'interfono 21
Blocco di protezione intrinseca a 12 V alimentato da alimentatore esterno 22
Risoluzione dei problemi 23
Ripristinare le impostazioni predefinite di fabbrica 23
Opzioni AXIS OS 23
Controllo della versione corrente del AXIS OS 23
Aggiornare AXIS OS 24
Problemi tecnici e possibili soluzioni 24

Considerazioni sulle prestazioni 26
Contattare l'assistenza 27
Cyber security 28
Gestione delle vulnerabilità 28
Notifiche di sicurezza 28
Ciclo di vita sicuro del prodotto 28
Informazioni di sicurezza 29
Livelli di pericolo 29
Altri livelli di messaggio 29

Panoramica dell'impostazione



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

Impostazioni preliminari

Individuazione del dispositivo sulla rete

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

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

Supporto browser

Il dispositivo può essere utilizzato con i seguenti browser:

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

✓: Consigliato

*: Supportato con limitazioni

Aprire l'interfaccia Web del dispositivo

1. Aprire un browser e digitare il nome di host o l'indirizzo IP del dispositivo Axis.
   Se non si conosce l'indirizzo IP, utilizzare AXIS IP Utility oppure AXIS Device Manager per individuare il dispositivo sulla rete.
2. Digitare il nome utente e password. Se si accede al dispositivo per la prima volta, è necessario creare un account amministratore. Vedere *Creare un account amministratore, on page 5*.

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

Creare un account amministratore

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

1. Inserire un utente.
2. Inserire una password. Vedere *Password sicure, on page 6*.
3. Reinserire la password.
4. Accettare il contratto di licenza.
5. Fare clic su **Add account (Aggiungi account)**.

Importante

Il dispositivo non ha un account predefinito. In caso di smarrimento della password dell'account amministratore, è necessario reimpostare il dispositivo. Vedere *Ripristinare le impostazioni predefinite di fabbrica, on page 23*.

Password sicure

Importante

Utilizza il protocollo HTTPS (abilitato per impostazione predefinita) per configurare la password o altre configurazioni sensibili tramite la rete. Il protocollo HTTPS abilita collegamenti di rete sicuri e crittografati, garantendo così la protezione dei dati sensibili, come le password.

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

Per proteggere i dati consigliamo vivamente di:

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

Accertarsi che nessuno abbia manomesso il software del dispositivo

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

1. Ripristinare le impostazioni predefinite di fabbrica. Vedere *Ripristinare le impostazioni predefinite di fabbrica, on page 23*.
   Dopo il ripristino, l'avvio sicuro garantisce lo stato del dispositivo.
2. Configurare e installare il dispositivo.

Configurare il dispositivo

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

Calibrazione ed esecuzione di un test dell'altoparlante da remoto

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

Nota

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

Durante la calibrazione, si consiglia di essere fisicamente presenti nel sito di installazione per ascoltare i toni di test e verificare che non siano ovattati o bloccati da ostacoli indesiderati nel percorso acustico dell'altoparlante.

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

Nota

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

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

Nota

È inoltre possibile eseguire la calibrazione premendo il pulsante di comando sul dispositivo fisico. Vedere *Panoramica dei prodotti, on page 16* per identificare il pulsante di comando.

Impostazione SIP diretto (P2P)

VoIP (Voice over IP) è un gruppo di tecnologie che consentono la comunicazione vocale e multimediale su reti IP. Per maggiori informazioni, vedere *Voice over IP (VoIP), on page 13*.

In questo dispositivo VoIP è abilitato tramite il protocollo SIP. Per ulteriori informazioni su SIP, consultare *Session Initiation Protocol (SIP), on page 13*

Esistono due tipi di impostazioni per SIP. Diretto o peer-to-peer (P2P) è uno dei due. Utilizzare peer-to-peer quando la comunicazione si trova tra pochi agenti utente all'interno della stessa rete IP e non è necessario disporre di funzionalità aggiuntive che un server PBX può fornire. Per informazioni sulla configurazione, vedere *Peer-to-peer SIP (P2PSIP), on page 13*.

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

AVVISO

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

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

6. Fare clic su **Ports (Porte)**.
7. Inserire il numero per **SIP port (Porta SIP)** e il numero per **TLS port (Porta TLS)**.

Nota

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

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

Nota

Utilizzare NAT traversal quando il dispositivo è collegato alla rete da dietro un router NAT o un firewall. Per maggiori informazioni vedere *NAT Traversal, on page 15*.

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

Configurazione di SIP tramite un server (PBX)

VoIP (Voice over IP) è un gruppo di tecnologie che consentono la comunicazione vocale e multimediale su reti IP. Per maggiori informazioni, vedere *Voice over IP (VoIP), on page 13*.

In questo dispositivo, VoIP è abilitato tramite il protocollo SIP. Per ulteriori informazioni su SIP, consultare *Session Initiation Protocol (SIP), on page 13*

Esistono due tipi di impostazioni per SIP. Un server PBX è uno di questi. 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 maggiori informazioni, vedere *Private Branch Exchange (PBX), on page 14*.

1. Richiedere le seguenti informazioni dal provider PBX:
   - ID utente
   - Dominio
   - Password
   - ID di autenticazione
   - ID chiamante
   - Registrar
   - Porta di avvio RTP
2. Andare a **Communication > SIP > Accounts (Communication > SIP > Account)** e fare clic su **+ Add account (+ Aggiungi account)**.
3. Immettere un **Name (Nome)** per l'account.
4. Selezionare **Registered (Registrato)**.
5. Selezionare una modalità di trasporto.
6. Aggiungere le informazioni sull'account dal provider PBX.
7. Fare clic su **Save (Salva)**.
8. Configurare le impostazioni SIP allo stesso modo del peer-to-peer, consultare *Impostazione SIP diretto (P2P), on page 7*. Utilizzare la porta di avvio RTP dal provider PBX.

Include il flusso video dalla telecamera vicina nella chiamata SIP

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

Requisiti

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

Per collegare l'intercom alla telecamera:

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

Creazione di un contatto

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

Per creare un nuovo contatto:

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

Nota

Per informazioni sugli indirizzi SIP, vedere *Session Initiation Protocol (SIP), on page 13*.

5. Selezionare l'account SIP da cui chiamare.

Nota

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

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

Nota

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

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

Configurazione del pulsante di chiamata

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

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

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

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

Utilizzare DTMF per sbloccare la porta per un visitatore

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

Questo esempio spiega come:

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

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

Prima di iniziare

- Consentire le chiamate SIP dal dispositivo e creare un account SIP. Vedere *Impostazione SIP diretto (P2P), on page 7* e *Configurazione di SIP tramite un server (PBX), on page 8*.

Definire il segnale DTMF nell'intercom

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

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

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

Utilizzare l'Elenco accessi per consentire ai titolari credenziali di aprire la porta.

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

Prerequisiti

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

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

1. Andare a **Reader > Entry list (Lettore > Elenco delle voci)**.
2. Attivare **Use Entry list (Usa elenco delle voci)**.
3. Fare clic su **+ Add credential holder (+ Aggiungi titolare credenziali)**.
4. Inserire il nome e il cognome del titolare credenziali. Il nome deve essere univoco.
5. Selezionare **Card (Tessera)**.
6. Passare la tessera del titolare credenziali sul dispositivo e fare clic su **Get latest (Ottieni l'ultimo)**.
7. Mantenere la condizione dell'evento **Access granted (Accesso consentito)**.

8. In **Valid to (Valido fino al)**, selezionare **Number of times (Numero di volte)**.
9. In **Number of times (Numero di volte)**, inserire 10.
10. Fare clic su **Save (Salva)**.

Creare una regola:

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

Imposta regole per eventi

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

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

Attivazione di un'azione

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

Interfaccia Web

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

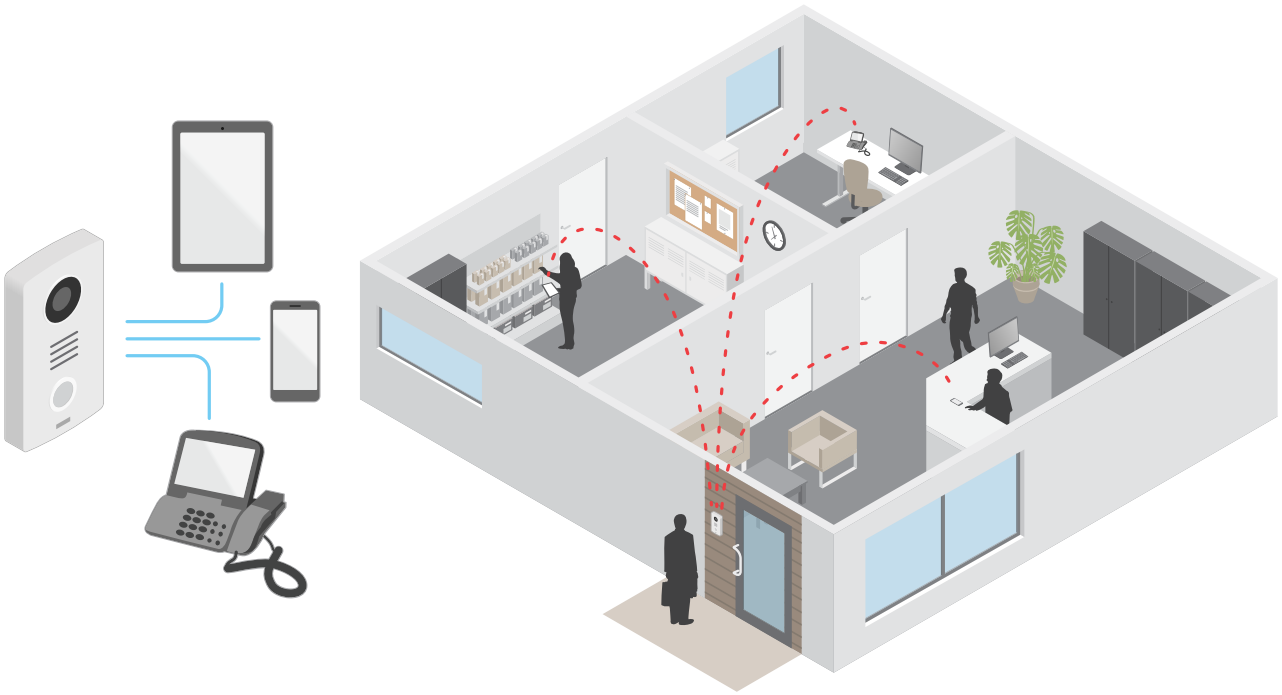
Per saperne di più

Voice over IP (VoIP)

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

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

Esempio:



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

Session Initiation Protocol (SIP)

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

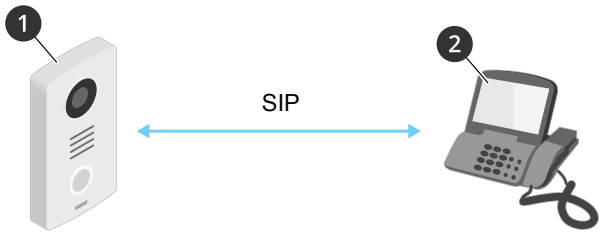
L'audio o il video effettivo viene scambiato tra gli agenti utente SIP con un protocollo di trasporto, ad esempio RTP (Real-Time Transport Protocol).

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

Peer-to-peer SIP (P2PSIP)

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

Esempio:



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

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

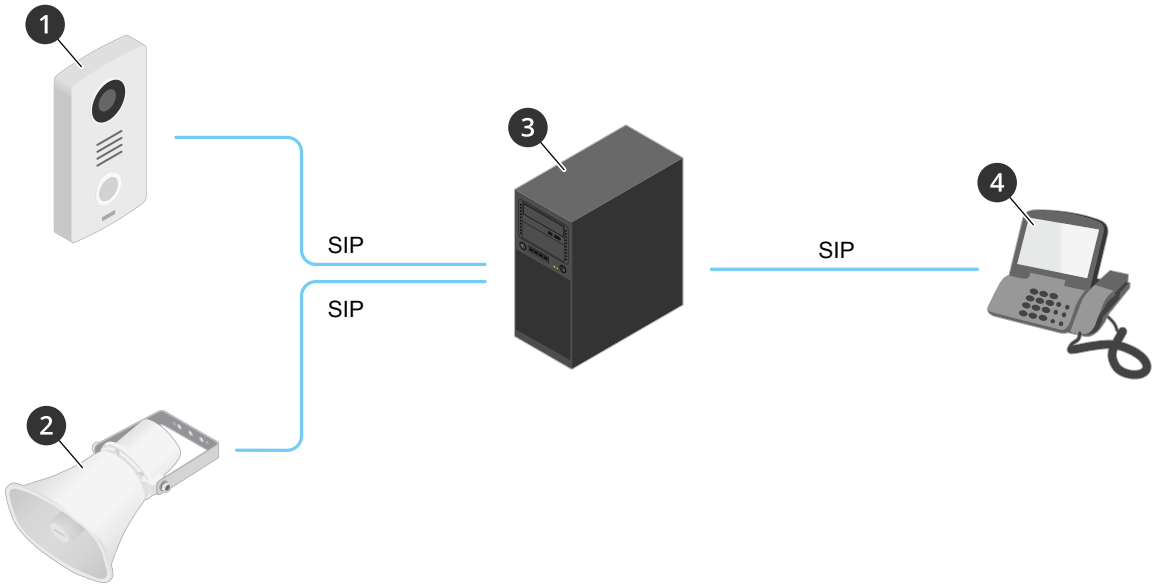
Private Branch Exchange (PBX)

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

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

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

Esempio:



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

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

NAT Traversal

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

Nota

Il router deve supportare NAT traversal e UPnP®.

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

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

Analisi e app

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

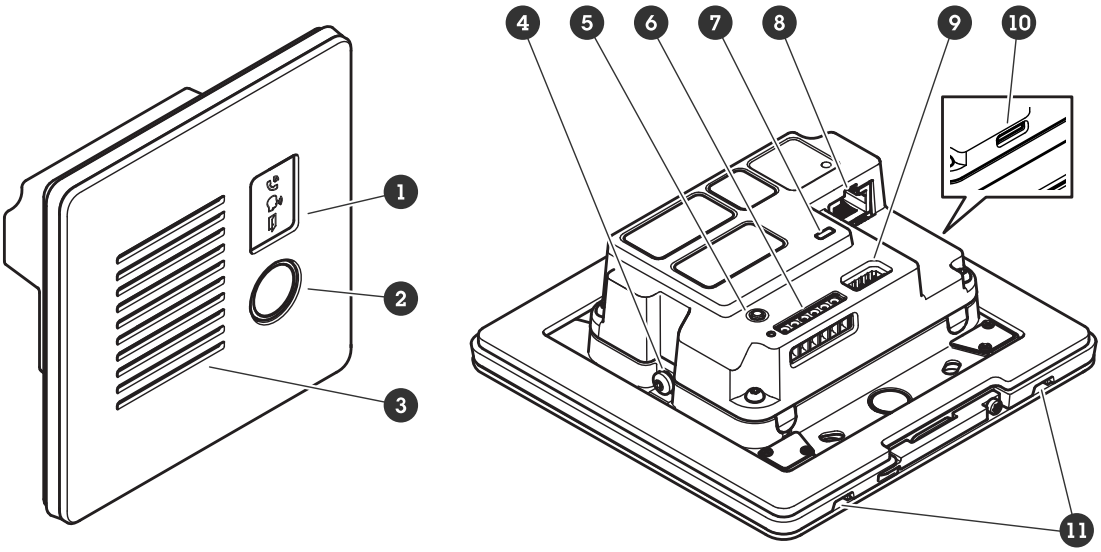
Per trovare i manuali per l'utente delle analisi e delle app Axis, visitare *help.axis.com*

AXIS Client for Unified Communication Systems

Con questa applicazione è possibile effettuare chiamate tra dispositivi Axis abilitati SIP e account Microsoft® Teams collegati. Per ulteriori informazioni, consultare il *manuale per l'utente per AXIS Client for Unified Communication Systems*.

Dati tecnici

Panoramica dei prodotti



1 *Icone degli indicatori, on page 16*
2 *Pulsante di chiamata*
3 *Speaker (Altoparlante)*
4 *Vite di messa a terra*
5 *Pulsante di comando, on page 17*
6 *I/O, lettore e connettore relè, on page 18*
7 *LED di stato*
8 *Connettore di rete, on page 17*
9 *Connettore audio, on page 17*
10 *Slot per scheda SD, on page 17 (microSD/microSDHC/microSDXC)*
11 *Microfono (2x)*

Indicatori e comandi del pannello anteriore

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

Icone degli indicatori

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

Indicatori LED

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

Slot per scheda SD

AVVISO

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

Questo dispositivo supporta schede microSD/microSDHC/microSDXC.

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

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

Pulsanti

Pulsante di comando

Il pulsante di comando viene utilizzato per:

- Ripristino del dispositivo alle impostazioni predefinite di fabbrica. Vedere *Ripristinare le impostazioni predefinite di fabbrica, on page 23*.
- Connessione a servizio one-click cloud connection (O3C) su Internet. Per connettersi, premere e rilasciare il pulsante, quindi attendere che il LED di stato verde lampeggi tre volte.

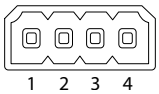
Connettori

Connettore di rete

Connettore Ethernet RJ45 con Power over Ethernet (PoE).

Connettore audio

Morsettiera a 4 pin per ingresso e uscita audio.

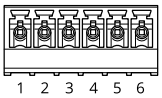


Funzione	Pin	Note
Ingresso linea	1	Ingresso linea (mono)
TERRA	2	Massa audio
Uscita linea	3	Uscita linea (mono)
TERRA	4	Massa audio

I/O, lettore e connettore relè

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

Morsettiera a 6 pin



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

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

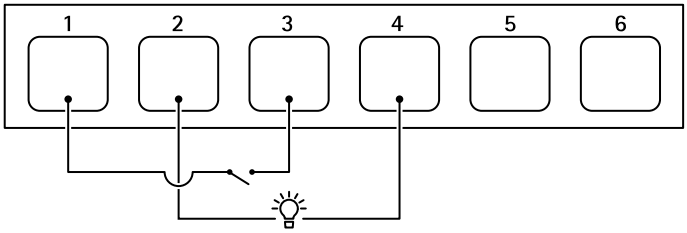
Connettore I/O

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

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

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

Esempio:



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

Connettore relè

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

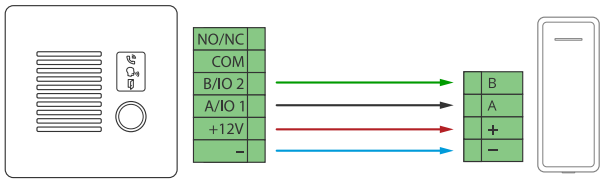
- come relè standard che apre e chiude i circuiti ausiliari,
- per controllare direttamente un blocco,
- per controllare un blocco tramite un relè di sicurezza. L'uso di un relè di sicurezza sul lato sicuro della porta impedisce la manomissione.

Connettore lettore

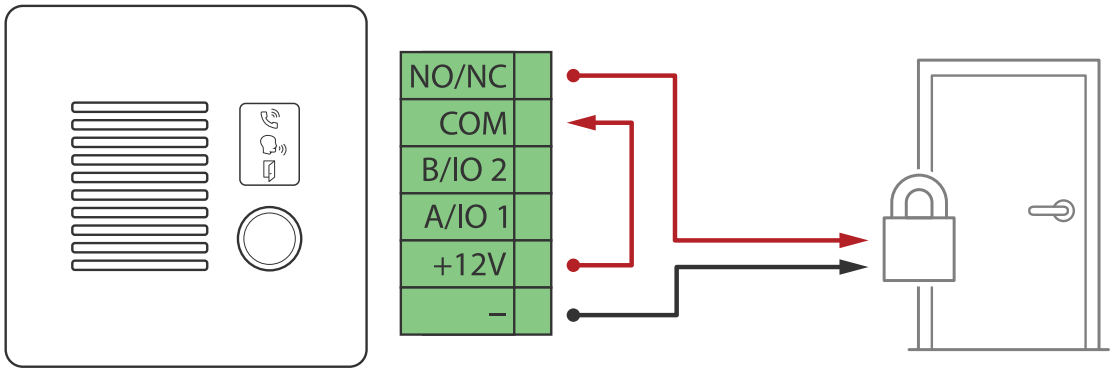
Una terza opzione è utilizzare il connettore come connettore lettore per collegare un lettore esterno.

Collegare le apparecchiature

Lettore Axis

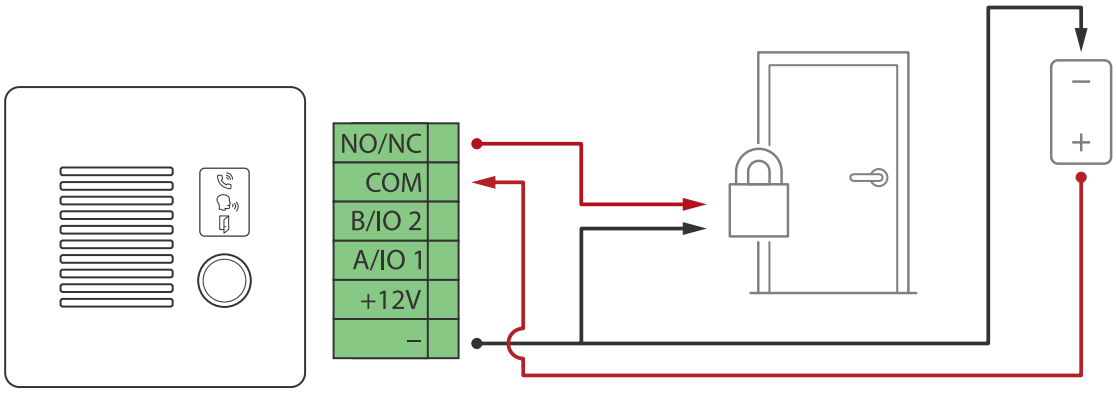


Relè alimentato da PoE (12V)



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

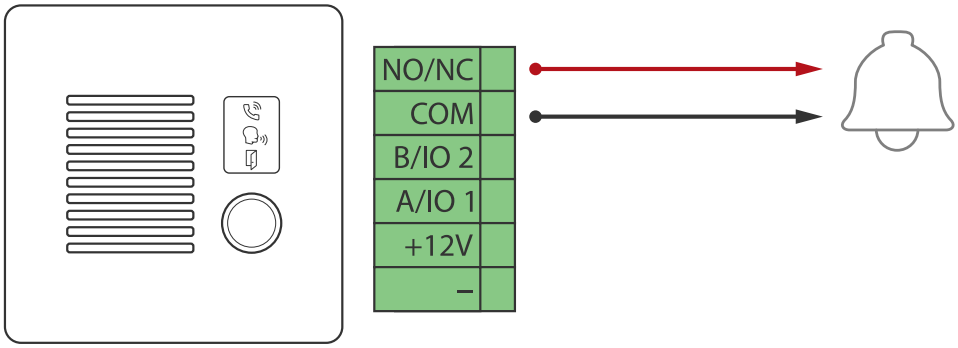
Relè alimentato da un alimentatore separato



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

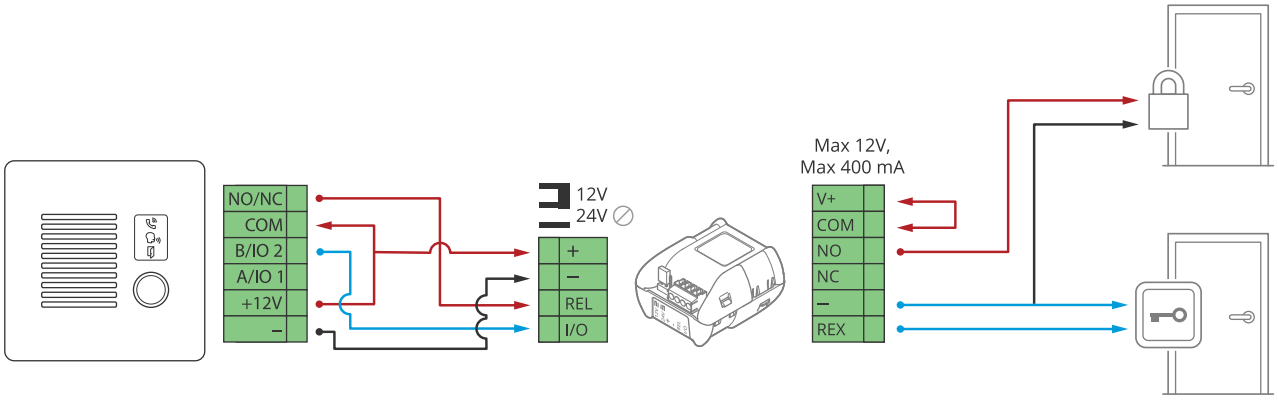
– per blocco di sicurezza intrinseca.

Relè senza potenziali



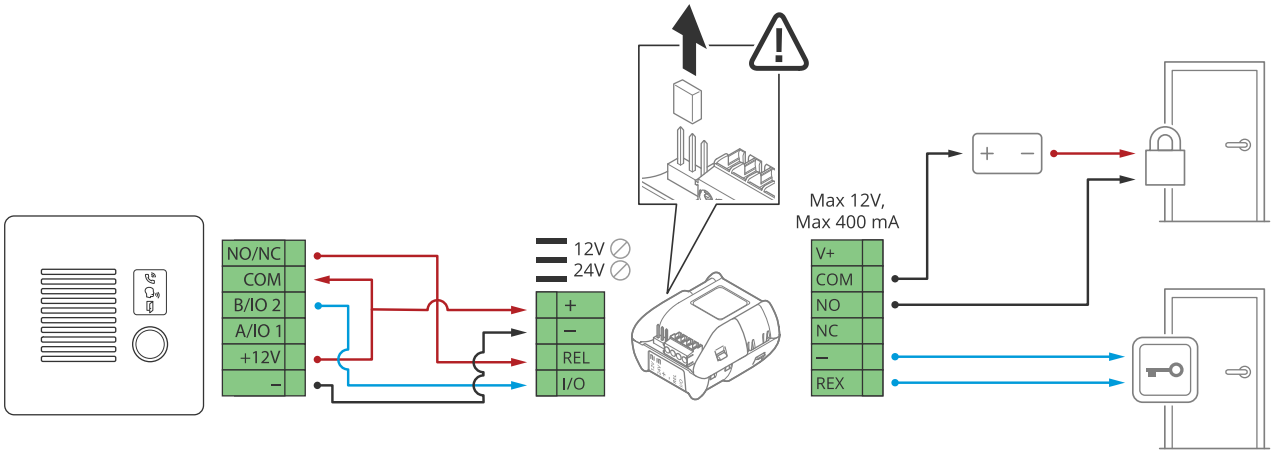
1. Per controllare lo stato del relè, andare a **System > Accessories (Sistema > Accessori)** e cercare la porta del relè.
2. Impostare **Normal state (Stato normale)** su:
   – per un blocco di protezione intrinseca.
   – per blocco di sicurezza intrinseca.

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



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

Blocco di protezione intrinseca a 12 V alimentato da alimentatore esterno



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

Risoluzione dei problemi

Ripristinare le impostazioni predefinite di fabbrica

Importante

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

Per ripristinare il dispositivo alle impostazioni predefinite di fabbrica:

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

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

Opzioni AXIS OS

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

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

Controllo della versione corrente del AXIS OS

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

Per controllare la versione corrente di AXIS OS:

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

Aggiornare AXIS OS

Importante

- Quando si esegue l'aggiornamento del software del dispositivo, le impostazioni preconfigurate e personalizzate vengono salvate. Axis Communications AB non può garantire il salvataggio delle impostazioni, anche se le funzionalità sono disponibili nella nuova versione del sistema operativo AXIS OS.
- A partire da AXIS OS 12.6, è necessario installare tutte le versioni LTS comprese tra la versione attuale del dispositivo e la versione di destinazione. Ad esempio, se la versione del software attualmente installata sul dispositivo è AXIS OS 11.2, è necessario installare la versione LTS AXIS OS 11.11 prima di poter effettuare l'aggiornamento del dispositivo ad AXIS OS 12.6. Per ulteriori informazioni, vedere *Guida al ciclo di vita AXIS OS: percorso di aggiornamento*.
- Assicurarsi che il dispositivo rimanga collegato alla fonte di alimentazione durante il processo di aggiornamento.

Nota

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

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

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

Problemi tecnici e possibili soluzioni

Problemi durante l'aggiornamento di AXIS OS

Aggiornamento di AXIS OS non riuscito

Se l'aggiornamento non riesce, il dispositivo ricarica la versione precedente. Il motivo più comune è il caricamento di un AXIS OS errato. Controllare che il nome del file di AXIS OS corrisponda al dispositivo e riprovare.

Problemi dopo l'aggiornamento di AXIS OS

Se si riscontrano problemi dopo l'aggiornamento, ripristinare la versione installata in precedenza dalla pagina **Maintenance (Manutenzione)**.

Problemi durante l'impostazione dell'indirizzo IP

Impossibile impostare l'indirizzo IP

- Se l'indirizzo IP destinato al dispositivo e l'indirizzo IP del computer utilizzato per accedere al dispositivo si trovano in subnet diverse, non è possibile impostare l'indirizzo IP. Contattare l'amministratore di rete per ottenere un indirizzo IP.
- L'indirizzo IP potrebbe già essere utilizzato da un altro dispositivo. Per verificare:
  1. Scollegare il dispositivo Axis dalla rete.
  2. In una finestra di comando/DOS digitare `ping` e l'indirizzo IP del dispositivo.
  3. Se la risposta ricevuta è `Reply from <IP address>: bytes=32; time=10...` significa che l'indirizzo IP potrebbe già essere utilizzato da un altro dispositivo nella rete. Contattare l'amministratore di rete per un nuovo indirizzo IP e reinstallare il dispositivo.
  4. Se si riceve: `Request timed out`, significa che l'indirizzo IP può essere utilizzato con il dispositivo Axis. Controllare tutti i cablaggi e reinstallare il dispositivo.
- Potrebbe verificarsi un conflitto di indirizzi IP con un altro dispositivo sulla stessa subnet. Prima che il server DHCP imposti un indirizzo dinamico viene utilizzato l'indirizzo IP statico del dispositivo Axis. Ciò significa che se lo stesso indirizzo IP statico viene utilizzato anche da un altro dispositivo, si potrebbero verificare dei problemi durante l'accesso al dispositivo.

Problemi di accesso al dispositivo

Impossibile effettuare l'accesso al dispositivo tramite un browser.

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

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

L'indirizzo IP è stato modificato dal server DHCP

Gli indirizzi IP ottenuti da un server DHCP sono dinamici e potrebbero cambiare. Se l'indirizzo IP è stato modificato, utilizzare AXIS IP Utility o AXIS Device Manager per individuare il dispositivo sulla rete. Identificare il dispositivo utilizzando il relativo numero di serie o modello oppure il nome DNS (se è stato configurato).

Se necessario, è possibile assegnare manualmente un indirizzo IP statico. Per istruzioni, vedere *axis.com/support*.

Errore del certificato durante l'utilizzo di IEEE 802.1X

Per un corretto funzionamento dell'autenticazione, le impostazioni della data e dell'ora nel dispositivo Axis devono essere sincronizzate con un server NTP. Andare a **System > Date and time (Sistema > Data e ora)**.

Il browser non è supportato

Per un elenco dei browser consigliati, consultare *Supporto browser, on page 5*.

Impossibile accedere al dispositivo dall'esterno

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

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

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

Problemi con MQTT

Impossibile collegarsi tramite la porta 8883 con MQTT su SSL

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

In alcuni casi il server/broker potrebbe non fornire una porta specifica per la comunicazione MQTT. Potrebbe essere ancora possibile utilizzare MQTT su una porta normalmente utilizzata per il traffico HTTP/HTTPS.

- Se il server/broker supporta WebSocket/WebSocket Secure (WS/WSS), in genere sulla porta 443, utilizzare questo protocollo. Controllare con il provider del server/broker se è supportato WS/WSS e quale porta e base utilizzare.
- Se il server/broker supporta ALPN, l'uso di MQTT può essere negoziato su una porta aperta, come la 443. Verificate con il proprio server/broker provider se ALPN è supportato e quale protocollo e porta ALPN utilizzare.

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

Considerazioni sulle prestazioni

Quando s'imposta il sistema, è importante considerare come le diverse impostazioni e situazioni influiscono sulle prestazioni. Alcuni fattori influiscono sulla larghezza di banda (velocità in bit), altri sulla velocità in fotogrammi e altri ancora influenzano entrambi.

I fattori più importanti da considerare:

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

Contattare l'assistenza

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

Cyber security

La sicurezza informatica sostiene un ciclo di vita del prodotto ottimale con rischi ridotti al minimo. È possibile trovare informazioni approfondite e documentazione sul nostro approccio alla sicurezza informatica all'indirizzo *axis.com/about-axis/cybersecurity*. Segui le linee guida sulla sicurezza informatica riportate di seguito per ricevere le notifiche di sicurezza relative al prodotto da parte di Axis e per configurare il prodotto per garantirne un ciclo di vita e una dismissione sicuri.

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

Gestione delle vulnerabilità

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

Notifiche di sicurezza

Iscriversi alle e-mail di notifica sulla sicurezza di Axis all'indirizzo *axis.com/security-notification-service*. Ti invieremo informazioni relative alle vulnerabilità, alle relative note di sicurezza e ad altre questioni relative alla sicurezza del tuo prodotto Axis.

Ciclo di vita sicuro del prodotto

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

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

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

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

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

Informazioni di sicurezza

Livelli di pericolo

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

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

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

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

Altri livelli di messaggio

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

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

T10208511_it

2026-10 (M19.2)

© 2024 – 2026 Axis Communications AB