

AXIS A8207-VE Mk II Network Video Door Station

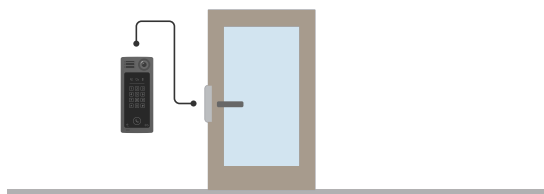
Indice

Panoramica delle soluzioni.....	4
Panoramica dei prodotti	5
Installazione.....	7
Impostazioni preliminari.....	8
Individuazione del dispositivo sulla rete.....	8
Supporto browser	8
Aprire l'interfaccia Web del dispositivo.....	8
Crea un account amministratore.....	8
Password sicure	9
Verificare che nessuno abbia alterato il software del dispositivo.....	9
Panoramica dell'interfaccia Web.....	9
Impostazioni supplementari	10
Cambiare la password root.	10
Calibrazione ed esecuzione di un test dell'altoparlante da remoto	10
Impostazione SIP diretto (P2P).....	10
Configurazione di SIP tramite un server (PBX)	11
Creazione di un contatto.....	12
Configurazione del pulsante di chiamata	12
Impostazione come lettore	12
Utilizzare l'Elenco accessi per consentire ai titolari credenziali di aprire la porta.....	13
Impostazione come lettore tessere utilizzando un door controller	13
Utilizzare i dati protetti sulle schede per aumentare la sicurezza	15
Utilizzare DTMF per sbloccare la porta per un visitatore	15
Trasmissione di video in diretta su un monitor.....	16
Interfaccia Web	17
Per saperne di più	18
Voice over IP (VoIP)	18
Session Initiation Protocol (SIP).....	18
Peer-to-peer SIP (P2PSIP).....	18
Private Branch Exchange (PBX)	19
Imposta regole per eventi.....	20
Analisi e app.....	20
AXIS Client for Unified Communication Systems	20
Utilizzo quotidiano.....	21
Utilizzo del tastierino.....	21
Risoluzione dei problemi.....	22
Ripristino delle impostazioni predefinite di fabbrica.....	22
Controllo della versione corrente del AXIS OS.....	22
Aggiornare AXIS OS	22
Problemi tecnici, indicazioni e soluzioni.....	23
Considerazioni sulle prestazioni	24
Dati tecnici	25
Indicatori e comandi del pannello anteriore	25
Icône degli indicatori	25
Striscia indicatore lettore di schede	25
Pulsante di chiamata	25
Indicatori LED	25
Slot per scheda SD	25
Pulsanti.....	26
Pulsante di comando.....	26
Connettori.....	26
Connettore HDMI	26
Connettore di rete	26

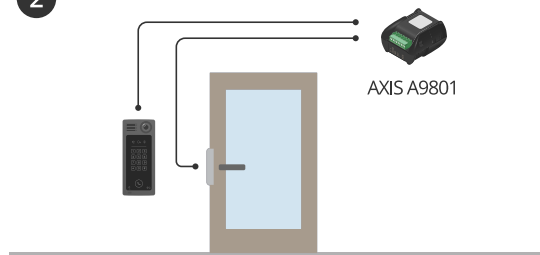
Connettore audio.....	26
Connettore relè	26
Connettore lettore	27
Connettore I/O	27
Connettore di alimentazione.....	28
Informazioni di sicurezza	29
Livelli di pericolo	29
Altri livelli di messaggio.....	29
Cyber security.....	30
Gestione delle vulnerabilità	30
Notifiche di sicurezza	30
Ciclo di vita sicuro del prodotto	30

Panoramica delle soluzioni

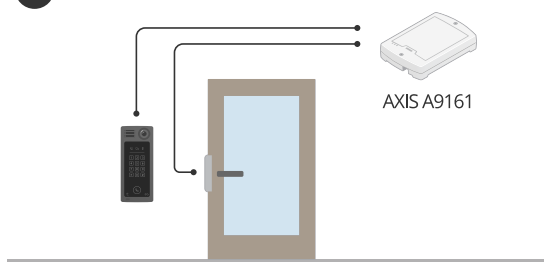
1



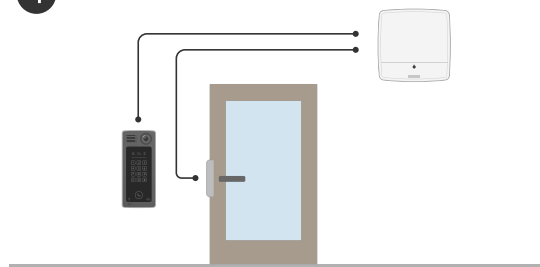
2



3



4



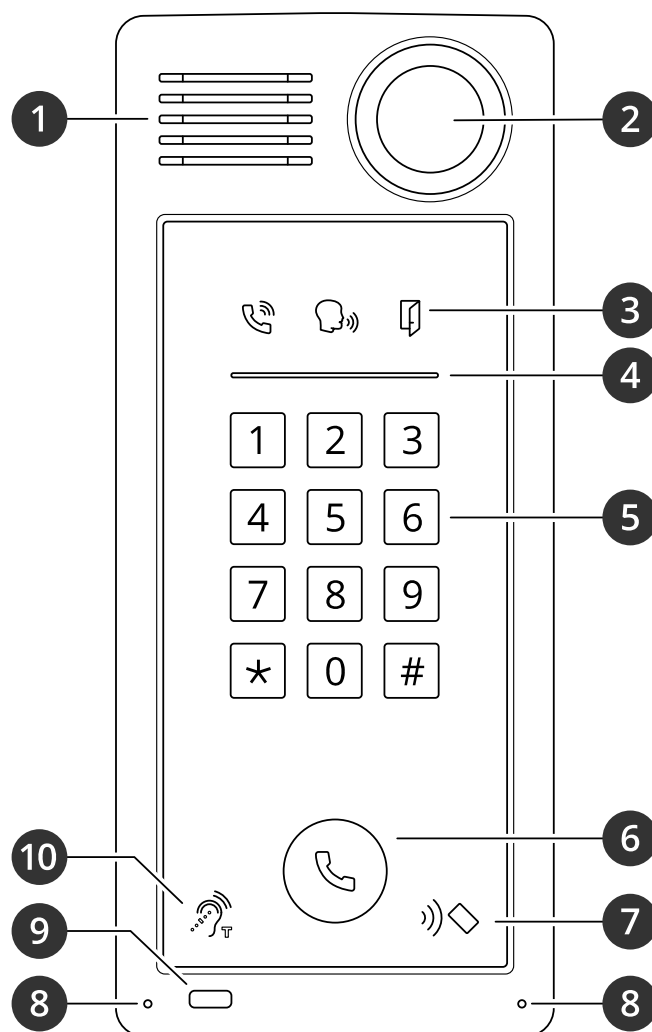
1 Door station

2 Videocitofono combinato con AXIS A9801

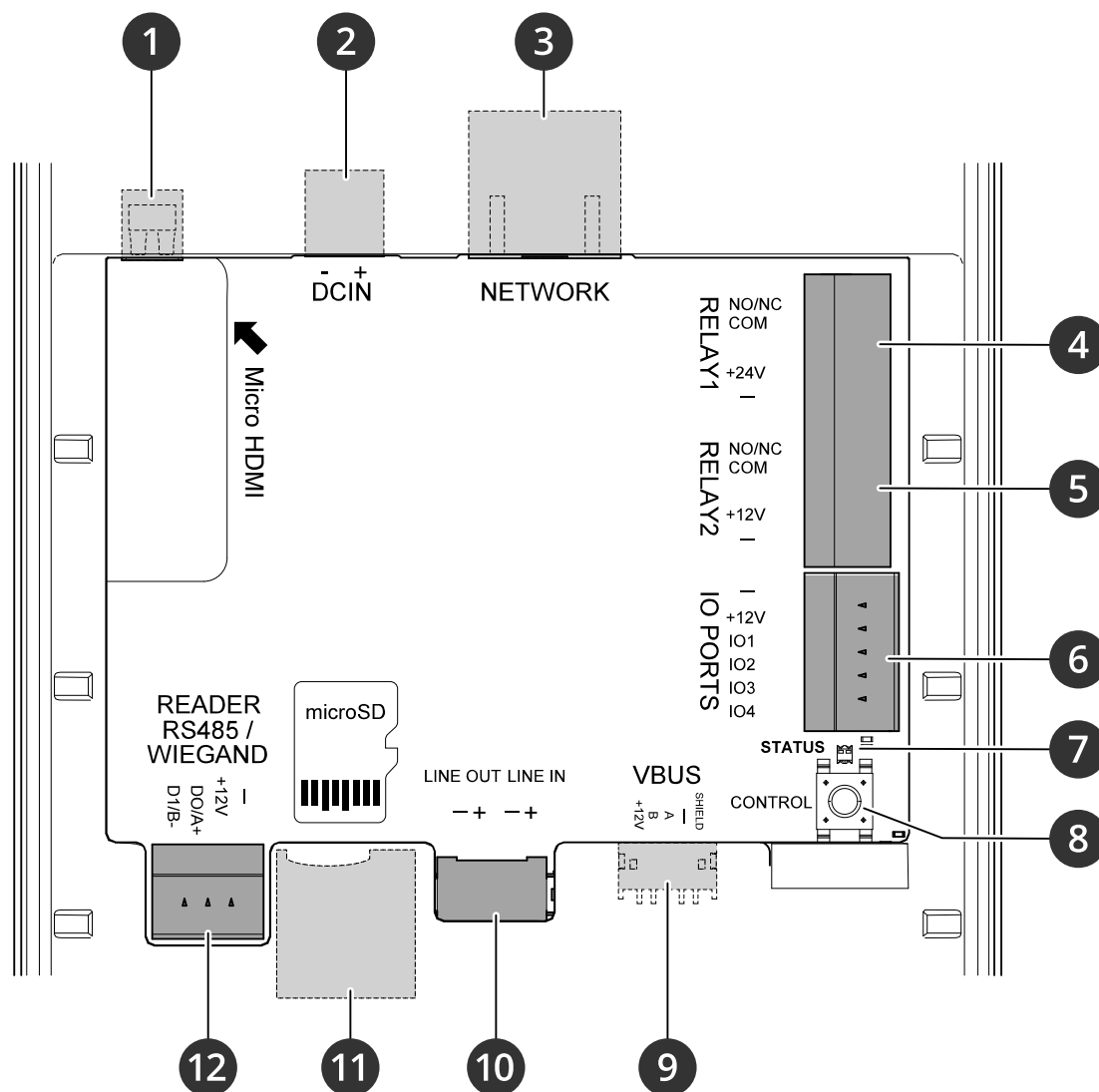
3 Videocitofono combinato con AXIS A9161

4 Videocitofono combinato con un sistema di controllo degli accessi, ad esempio AXIS A1001 o AXIS A1601

Panoramica dei prodotti



- 1 Altoparlante
- 2 Telecamera
- 3 Icone degli indicatori, on page 25
- 4 Striscia indicatore lettore di schede, on page 25
- 5 Tastierino
- 6 Pulsante di chiamata, on page 25
- 7 Icona lettore di schede
- 8 Microfono
- 9 Sensore PIR
- 10 Icona Bobina a T



- 1 Connettore HDMI, on page 26 (microHDMI)
- 2 Connettore di alimentazione, on page 28
- 3 Connettore di rete, on page 26 (PoE+)
- 4 Connettore relè, on page 26
- 5 Connettore relè, on page 26
- 6 Connettore I/O, on page 27
- 7 LED di stato
- 8 Pulsante di comando, on page 26
- 9 2N VBUS (non utilizzato)
- 10 Connettore audio, on page 26
- 11 Slot per scheda SD, on page 25 (microSD/microSDHC/microSDXC)
- 12 Connettore lettore, on page 27

Installazione



Per guardare questo video, andare alla versione web di questo documento.

Video di installazione per lettore A8207-VE.



Per guardare questo video, andare alla versione web di questo documento.

Video di installazione per relè A8207-VE.

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 *Crea un account amministratore, on page 8*.

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

Crea un account amministratore

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

1. Inserire un nome utente.
2. Inserire una password. Vedere *Password sicure, on page 9*.
3. Reinserire la password.
4. Accettare il contratto di licenza.
5. Fare clic su **Add account (Aggiungi account)**.

Importante

Il dispositivo non ha un account predefinito. In caso di smarrimento della password dell'account amministratore, è necessario reimpostare il dispositivo. Vedere *Ripristino delle impostazioni predefinite di fabbrica, on page 22*.

Password sicure

Importante

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

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

Per proteggere i dati consigliamo vivamente di:

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

Verificare che nessuno abbia alterato il software del dispositivo

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

1. Ripristinare le impostazioni predefinite di fabbrica. Vedere *Ripristino delle impostazioni predefinite di fabbrica, on page 22*.
Dopo il ripristino, l'avvio sicuro garantisce lo stato del dispositivo.
2. Configurare e installare il dispositivo.

Panoramica dell'interfaccia Web

Questo video mette a disposizione una panoramica dell'interfaccia Web del dispositivo.



Per guardare questo video, andare alla versione web di questo documento.

Interfaccia Web dei dispositivi Axis

Impostazioni supplementari

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.

Cambiare la password root.

1. Accedere all'interfaccia del dispositivo e andare a **System > Users (Sistema > Utenti)**.
2. Per l'utente root, fare clic su  > **Update user (Aggiorna utente)**.
3. Inserisci una nuova password e salva.

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. Vedere *Panoramica dei prodotti*, on page 5 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 ulteriori informazioni, vedere *Voice over IP (VoIP)*, on page 18.

In questo dispositivo VoIP è abilitato tramite il protocollo SIP. Per ulteriori informazioni su SIP, consultare *Session Initiation Protocol (SIP)*, on page 18

Esistono due tipi di impostazione SIP. Una di queste è la diretta o peer-to-peer (P2P). Utilizzare peer-to-peer quando la comunicazione si trova tra pochi agenti utente all'interno della stessa rete IP e non è necessario disporre di funzionalità aggiuntive che un server PBX può fornire. Per informazioni su come configurarlo, vedere *Peer-to-peer SIP (P2PSIP)*, on page 18.

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

AVVISO

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

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

Nota

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

Nota

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

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

Configurazione di SIP tramite un server (PBX)

VoIP (Voice over IP) è un gruppo di tecnologie che consentono la comunicazione vocale e multimediale su reti IP. Per ulteriori informazioni, vedere *Voice over IP (VoIP)*, on page 18.

In questo dispositivo, VoIP è abilitato tramite il protocollo SIP. Per ulteriori informazioni su SIP, consultare *Session Initiation Protocol (SIP)*, on page 18

Esistono due tipi di impostazione SIP, uno dei quali è un server PBX. Utilizzare un server PBX quando la comunicazione deve essere compresa tra un numero infinito di agenti utente all'interno e all'esterno della rete IP. Altre funzionalità possono essere aggiunte alla configurazione a seconda del provider PBX. Per ulteriori informazioni, vedere *Private Branch Exchange (PBX)*, on page 19.

1. Richiedere le seguenti informazioni dal provider PBX:
 - ID utente
 - Dominio
 - Password
 - ID di autenticazione
 - ID chiamante
 - Registrare
 - 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 10. Utilizzare la porta di avvio RTP dal provider PBX.

Creazione di un contatto

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

Per creare un nuovo contatto:

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

Nota

Per informazioni sugli indirizzi SIP, consultare *Session Initiation Protocol (SIP)*, on page 18.

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)**.

Impostazione come lettore

È possibile impostare la door station come lettore per consentire ai titolari credenziali di aprire la porta.

Utilizzando l'Elenco accessi, la door station memorizza le credenziali localmente e può funzionare come lettore autonomo per un massimo di cinquanta titolari credenziali.

Quando si collega la door station a un door controller, la door station può comunque memorizzare fino a cinquanta credenziali e, se le credenziali richieste sono presenti nell'Elenco accessi, la door station gestisce le autorizzazioni di accesso. Se le credenziali richieste non sono presenti nell'Elenco accessi e l'opzione **Use connected door controller** (Usa door controller collegato) è abilitata, la richiesta viene inoltrata al door controller, che gestisce le autorizzazioni di accesso.

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 **Open door** (Apri porta).
4. Nell'elenco delle condizioni, selezionare **Entry list > Access granted** (Elenco delle voci > Accesso consentito).
5. Dall'elenco delle azioni, selezionare **I/O > Toggle I/O once** (I/O > Attiva/disattiva I/O una volta).
6. Dall'elenco delle porte, selezionare **Door** (Porta).
7. In **State** (Stato), selezionare **Active** (Attivo).
8. Impostare la durata su **00:00:07**.
9. Fare clic su **Save** (Salva).

Impostazione come lettore tessere utilizzando un door controller

Connessione di rete

Per utilizzare la door station come lettore di tessere, è possibile collegarla a un door controller. Il dispositivo di controllo delle porte memorizza tutte le credenziali e tiene traccia degli accessi consentiti. In questo esempio, i dispositivi vengono collegati in rete. Vengono modificati anche i tipi di schede consentiti.

Importante

La connessione di rete funziona solo con i dispositivi di controllo delle porte di Axis. Per connettersi a un dispositivo di controllo delle porte non Axis, è necessario collegare fisicamente i dispositivi con i cavi. Vedere *Connessione via cavo, on page 14*.

Impostare il videocitofono come lettore di schede

1. Vai a **Reader (Lettore) > Connection (Connessione)**.
2. Selezionare il tipo di protocollo **VAPIX reader (Lettore VAPIX)**.
3. Selezionare il protocollo per la comunicazione con il door controller.

Nota

Si consiglia di abilitare **Verify certificate (Verifica certificato)** se si usa HTTPS.

4. Inserire l'indirizzo IP per il door controller.
5. Inserire le credenziali per il door controller.
6. Fare clic su **Connetti**.
7. Selezionare il lettore di ingresso per la porta appropriata.
8. Fare clic su **Save (Salva)**.

Connessione via cavo

Per utilizzare la door station come lettore di tessere, è possibile collegarla a un door controller. Il dispositivo di controllo delle porte memorizza tutte le credenziali e tiene traccia degli accessi consentiti. In questo esempio, i dispositivi vengono collegati tramite cavo, viene utilizzato il protocollo Wiegand, viene attivato l'avvisatore acustico e viene usata una porta I/O per il LED. Inoltre, modifichiamo i tipi di scheda consentiti.

Importante

Utilizzare le porte I/O che non sono già in uso. Se si utilizzano le porte I/O già in uso, tutti gli eventi creati per queste porte smetteranno di funzionare.

Prima di iniziare

- Collegare il videocitofono a un dispositivo di controllo delle porte.
Vedere gli schemi elettrici scaricabili da axis.com/products/axis-a8207-ve-mk-ii/support.
- Configurare l'hardware del dispositivo di controllo delle porte utilizzando il protocollo Wiegand per il lettore. Per le istruzioni, consultare il manuale per l'utente del dispositivo di controllo delle porte.

Impostare il videocitofono come lettore di schede

1. Vai a **Reader (Lettore) > Connection (Connessione)**.
2. Seleziona **Wiegand** come tipo di protocollo.
3. Abilitare **Beeper (Avvisatore acustico)**.
4. In **Input for beeper (Ingresso per avvisatore acustico)**, selezionare **I3 (I3)**.
5. In **Input used for LED control (Input usato per il comando LED)**, seleziona **1**.
6. In **Input for LED1 (Ingresso per LED1)**, selezionare **I1 (I1)**.
7. Selezionare i colori da utilizzare per ogni stato.
8. In **Keypress format (Formato pressione)**, selezionare **FourBit**.
9. Fare clic su **Save (Salva)**.
10. Andare a **Reader > Chip types (Lettore > Tipi di chip)** e attivare i tipi di chip che si desidera utilizzare.

Nota

Puoi mantenere il set predefinito di tipi di chip, ma ti consigliamo di modificare l'elenco in base alle esigenze specifiche.

11. Fare clic su **Add data set (Aggiungi set di dati)** per specificare i set di dati per i diversi tipi di chip.
12. Fare clic su **Save (Salva)**.

Utilizzare i dati protetti sulle schede per aumentare la sicurezza

Per aumentare la sicurezza nel sistema di controllo degli accessi, è possibile scegliere di utilizzare dati tessera sicuri memorizzati su alcuni tipi di schede. I dati sono protetti da una chiave segreta. Per leggere i dati della tessera, è necessario archiviare la chiave segreta e altre informazioni sulla scheda del dispositivo.

1. Andare a **Reader > Chip types (Lettore > Tipi di chip)**.
2. In **Data sets (Set di dati)**, selezionare il tipo di chip che si desidera modificare e fare clic su **Add data set (Aggiungi set di dati)**.
3. Immettere le informazioni sui dati della tessera. Le informazioni da immettere dipendono dal tipo di tessera e dalla modalità di registrazione delle tessere.
4. Se si utilizzano i protocolli OSDP o Wiegand, selezionare **Use as UID (Usa come UID)** per inviare i dati protetti come UID/CSN invece della normale tessera UID/CSN.
5. Per consentire solo le tessere che sono conformi ai dati della tessera specificata da inviare al dispositivo di controllo degli accessi, selezionare **Required data (Dati richiesti)**. Le tessere che non sono conformi vengono ignorate dal lettore.
6. Fare clic su **Save (Salva)**.

Utilizzare DTMF per sbloccare la porta per un visitatore

Quando un visitatore effettua una chiamata dal videocitofono, 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 nel videocitofono
- impostare il citofono 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 door controller.

Prima di iniziare

- Consentire le chiamate SIP dal dispositivo e creare un account SIP. Vedere *Impostazione SIP diretto (P2P)*, on page 10 e *Configurazione di SIP tramite un server (PBX)*, on page 11.

Definire il segnale DTMF nel videocitofono

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 il citofono 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)**.

Trasmissione di video in diretta su un monitor

Il dispositivo può trasmettere un flusso video in diretta su un monitor HDMI senza una connessione di rete. Utilizzare il monitor per vedere chi si trova alla porta.

1. Collegare un monitor esterno al connettore HDMI.
2. Regolare le impostazioni HDMI in **System > Video out (Sistema > Uscita video)**.

Interfaccia Web

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

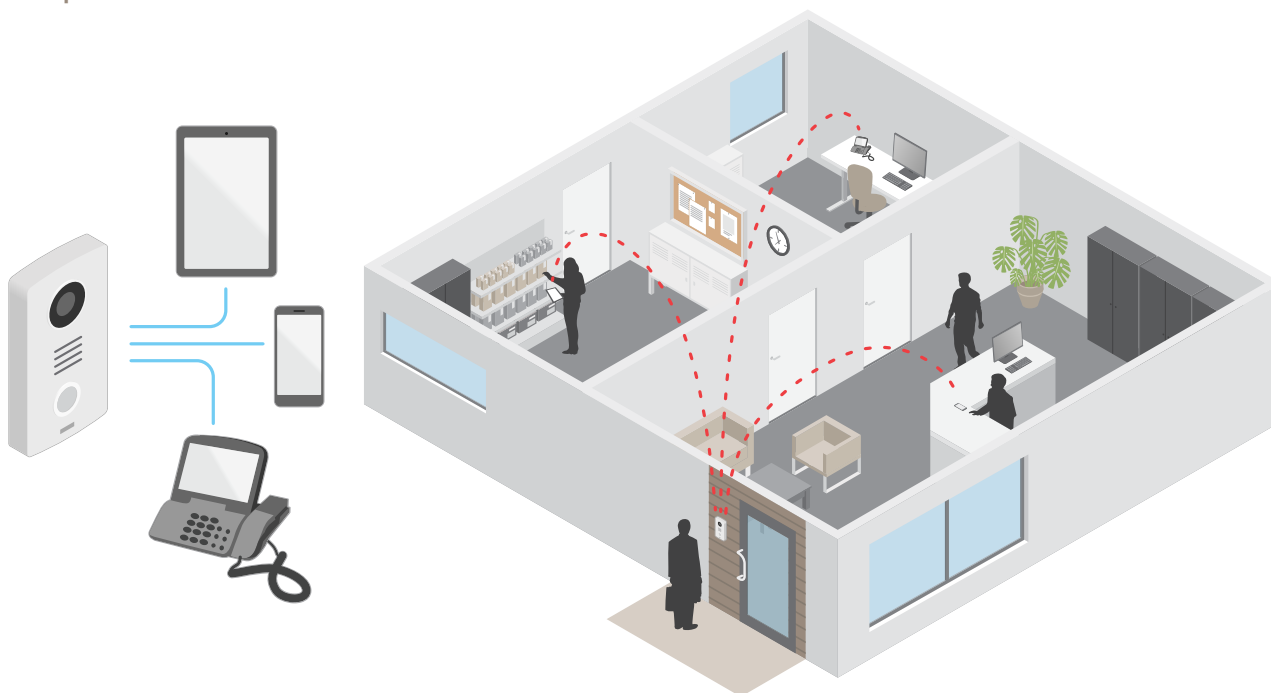
Per saperne di più

Voice over IP (VoIP)

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

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

Esempio:



Quando si preme il pulsante di chiamata su una Axis door station, 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.

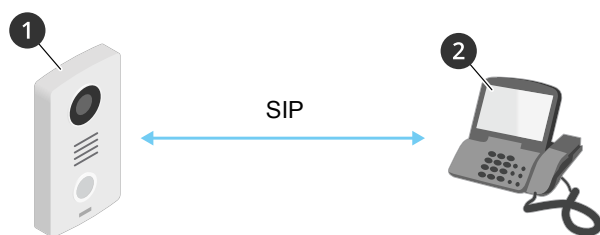
L'audio o il video effettivo viene scambiato tra gli agenti utente SIP con un protocollo di trasporto, ad esempio RTP (Real-Time Transport Protocol).

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: videocitofono. Indirizzo SIP: sip:192.168.1.101
- 2 Agente utente B: telefono abilitato SIP. Indirizzo SIP: sip:192.168.1.100

È possibile impostare Axis door station per chiamare ad esempio un telefono abilitato SIP sulla stessa rete utilizzando un'impostazione SIP peer-to-peer.

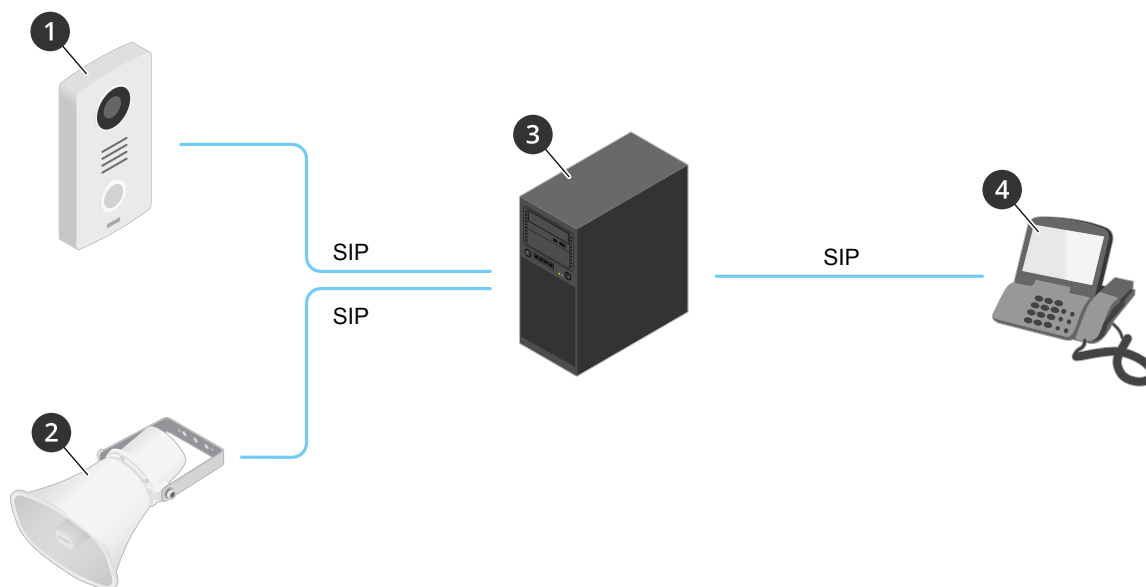
Private Branch Exchange (PBX)

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

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

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

Esempio:



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

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

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 sovrapposizione mentre il dispositivo registra.

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

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*.

Utilizzo quotidiano

Utilizzo del tastierino

Vorrei...	Operazione
Chiamare qualcuno che può farmi entrare nell'edificio.	Stampa  .
Chiamare una persona nell'edificio.	Inserire il numero di chiamata rapida della persona e premere  .
Aprire la porta con la scheda e il PIN.	Appoggiare la scheda e immettere il PIN.
Aprire la porta con il PIN.	Inserire il PIN e premere #.
Aprire la porta con la mia scheda.	Appoggiare la scheda.

Risoluzione dei problemi

Ripristino delle impostazioni predefinite di fabbrica

Importante

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

Per ripristinare il dispositivo alle impostazioni predefinite di fabbrica:

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

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

Controllo della versione corrente del AXIS OS

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

Per controllare la versione corrente di AXIS OS:

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

Aggiornare AXIS OS

Importante

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

Nota

- Quando si aggiorna il dispositivo con la versione più recente di AXIS OS nella traccia attiva, il dispositivo riceve le ultime funzionalità disponibili. Leggere sempre le istruzioni di aggiornamento e le note di rilascio disponibili con ogni nuova versione prima dell'aggiornamento. Per la versione AXIS OS più aggiornata e le note sul rilascio, visitare il sito Web axis.com/support/device-software.
1. Scarica il file AXIS OS sul tuo computer, disponibile gratuitamente su axis.com/support/device-software.
 2. Accedi al dispositivo come amministratore
 3. Andare a **Maintenance > AXIS OS upgrade (Manutenzione > Aggiornamento AXIS OS)** e fare clic su **Upgrade (Aggiorna)**.

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

Problemi tecnici, indicazioni e soluzioni

Se non si riesce a trovare qui ciò che si sta cercando, provare ad accedere alla sezione relativa alla risoluzione dei problemi all'indirizzo axis.com/support.

Problemi durante l'aggiornamento 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: <code>Reply from <IP address>: bytes=32; time=10...</code> 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: <code>Request timed out</code>, 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	Quando HTTPS è abilitato, verifica che sia usato il protocollo giusto (HTTP o HTTPS) quando tenti di eseguire l'accesso. Potrebbe essere necessario digitare manualmente <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. Vedere <i>Ripristino delle impostazioni predefinite di fabbrica, on page 22</i> .
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).

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 Companion: gratuito, ideale per piccoli sistemi con esigenze di sorveglianza di base.
- 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.

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.

Dati tecnici

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

Striscia indicatore lettore di schede

La striscia indica il feedback del lettore.

Pulsante di chiamata

È possibile utilizzare la luce integrata attorno al pulsante di chiamata per illuminare i volti dei visitatori.

Indicatori LED

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

Slot per scheda SD

AVVISO

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

Questo dispositivo supporta schede microSD/microSDHC/microSDXC.

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



I loghi 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 *Ripristino delle impostazioni predefinite di fabbrica*, on page 22.

Connettori

Connettore HDMI

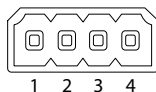
Utilizzare il connettore microHDMI™ per collegare un display o un monitor dedicato alla visualizzazione pubblica.

Connettore di rete

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

Connettore audio

Morsettiera a 4 pin per ingresso e uscita audio.

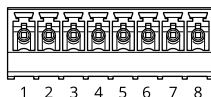


Funzione	Pin	Note
Ingresso linea	1	Ingresso linea (mono)
TERRA	2	Massa audio
Uscita linea	3	Uscita linea
TERRA	4	Massa audio

Connettore relè

Morsettiera a 8 pin per relè a stato solido che può essere utilizzato nei seguenti modi:

- 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.



Funzione	Pin	Note	Dati tecnici
NO/NC	1	Normalmente aperto/normalmente chiuso Per il collegamento di relè. I due pin dei relè sono separati con isolamento galvanico dal resto dei circuiti.	Corrente massima 1 A Tensione max. 30 V CC
COM	2	Comune	

24 V CC	3	Per alimentare periferiche ausiliarie. Nota: questo pin può essere usato solo come uscita alimentazione.	Tensione in uscita 24 V CC Corrente max. 50 mA ¹ Corrente max. 350 mA ²
Terra CC	4		0 V CC
NO/NC	5	Normalmente aperto/normalmente chiuso Per il collegamento di relè. I due pin dei relè sono separati con isolamento galvanico dal resto dei circuiti.	Corrente massima 1 A Tensione max. 30 V CC
COM	6	Comune	
12 V CC	7	Per alimentare periferiche ausiliarie. Nota: questo pin può essere usato solo come uscita alimentazione.	Tensione in uscita 12 V CC Corrente max. 100 mA ¹ Corrente max. 700 mA ²
Terra CC	8		0 V CC

Connettore lettore

Morsettiera a 4 pin per collegare il lettore esterno.

Funzione	Pin	Note	Dati tecnici
Terra CC	1		0 V CC
12 V CC	2	Per alimentare periferiche ausiliarie. Nota: questo pin può essere usato solo come uscita alimentazione.	Tensione in uscita 12 V CC
D0/A+	3	Wiegand: output DATA0 RS485: A+	
D1/B-	4	Wiegand: output DATA1 RS485: B-	

Connettore I/O

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

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

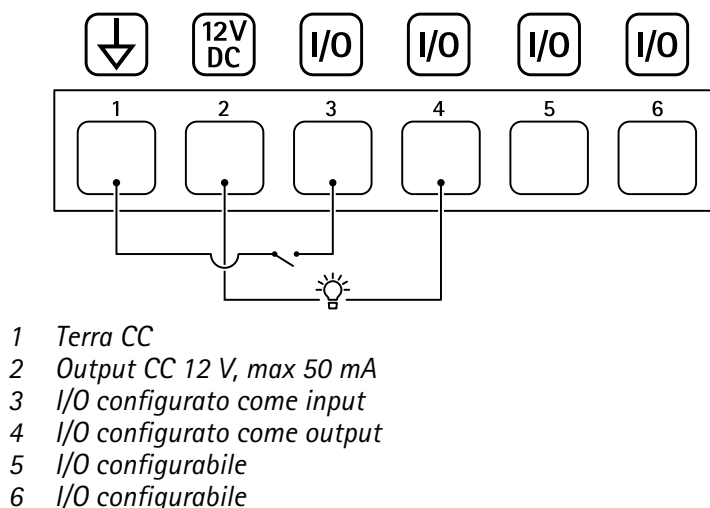
Uscita digitale – Per il collegamento di dispositivi esterni come relè e LED. I dispositivi collegati possono essere attivati tramite l'API (interfaccia per la programmazione di applicazioni) VAPIX® attraverso un evento oppure dall'interfaccia Web del dispositivo.



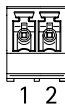
1. Quando l'alimentazione avviene tramite Power over Ethernet IEEE 802.3af/802.3at Tipo 1 Classe 3.

2. Quando l'alimentazione avviene tramite Power over Ethernet Plus (PoE+) IEEE 802.3at Tipo 2 Classe 4 o input elettrico CC.

Funzione	Pin	Note	Dati tecnici
Terra CC	1		0 V CC
Uscita CC	2	 Questo terminale può essere utilizzato anche per alimentare una periferica ausiliaria. Nota: questo pin può essere usato solo come uscita alimentazione.	12 V CC Carico massimo = 50 mA
Configurabile (ingresso o uscita)	3-6	Ingresso digitale - collegare al pin 1 per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo.	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:

Connettore di alimentazione

Morsettiera a 2 pin per ingresso alimentazione CC. Utilizzare una sorgente di alimentazione limitata (LPS) compatibile con una bassissima tensione di sicurezza (SELV) con una potenza di uscita nominale limitata a ≤ 100 W o una corrente nominale di uscita limitata a ≤ 5 A.



Funzione	Pin	Note	Dati tecnici
Terra CC	1		0 V CC
Input CC	2	Per l'alimentazione del controller quando non si utilizza Power over Ethernet. Nota: questo pin può essere usato solo come alimentazione.	8-28 V CC, max 22 W Carico massimo in uscita 9 W

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.

Cyber security

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

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

Gestione delle vulnerabilità

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

Notifiche di sicurezza

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

Ciclo di vita sicuro del prodotto

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

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

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

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

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

T10176599_it

2026-07 (M25.2)

© 2021 – 2026 Axis Communications AB