AXIS D4100-VE Mk II Network Strobe Siren

Manuale dell'utente

Indice

Installazione....4
....4
Impostazioni preliminari....5
....5
Individuazione del dispositivo sulla rete....5
Supporto browser....5
Aprire l'interfaccia Web del dispositivo....5
Creare un account amministratore....5
Password sicure....5
Configurare il dispositivo....7
Disattiva la modalità manutenzione dopo l'installazione della sirena....7
Attiva modalità manutenzione....7
Configura un profilo....7
Importa o esporta un profilo....7
Impostazione SIP diretto (P2P)....7
Configurazione di SIP tramite un server (PBX)....8
Imposta regole per eventi....9
Attivazione di un'azione....9
Inizia un profilo quando avviene l'attivazione di un allarme....9
Inizia un profilo attraverso SIP....9
Controlla più di un profilo con le estensioni SIP....10
Esecuzione di due profili con priorità diverse....11
Attivazione di una sirena tramite input virtuale quando una videocamera rileva movimento....11
Attivazione di una sirena tramite un quando HTTP Post quando una videocamera rileva movimento....13
Attivazione della sirena stroboscopica su MQTT quando la telecamera rileva movimento....14
Interfaccia Web....16
Per saperne di più....17
Session Initiation Protocol (SIP)....17
Peer-to-peer SIP (P2PSIP)....17
Private Branch Exchange (PBX)....17
NAT Traversal....17
Dati tecnici....18
Panoramica dei prodotti....18
....18
Indicatori LED....18
Pulsanti....18
Pulsante di comando....18
Connettori....19
Connettore di rete....19
Connettore I/O....19
Nomi dei pattern di luce....20
Nomi delle sequenze sonore....20
Pulizia del dispositivo....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
....26
Considerazioni sulle prestazioni....26
Contattare l'assistenza....26

Cyber security....27
Gestione delle vulnerabilità....27
Notifiche di sicurezza....27
Ciclo di vita sicuro del prodotto....27

Installazione



Impostazioni preliminari

⚠ AVVISO

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

Individuazione del dispositivo sulla rete

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. 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 5*.
3. Reinserire la password.
4. Accettare il contratto di licenza.
5. Fare clic su **Add account (Aggiungi account)**.

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.

Configurare il dispositivo

Disattiva la modalità manutenzione dopo l'installazione della sirena

⚠ ATTENZIONE

Per tutelare l'installatore da danni all'udito e dall'abbaglio da luce intensa, consigliamo di mantenere attiva la modalità di manutenzione nel corso dell'installazione del dispositivo.

Al momento dell'installazione del dispositivo per la prima volta, la modalità di manutenzione è attiva per impostazione predefinita. Quando il dispositivo è in modalità di manutenzione, la sirena non produce suoni e la luce produce pattern di luce bianca pulsante.

Vai su **Overview (Panoramica)** > **Maintenance (Manutenzione)** per disattivare la **Maintenance mode (Modalità di manutenzione)**.

Attiva modalità manutenzione

Per eseguire il servizio del dispositivo, vai su **Overview (Panoramica)** > **Maintenance (Manutenzione)** e attiva la **Maintenance mode (Modalità di manutenzione)**. Le normali attività di illuminazione e sirena vengono così messe in pausa.

Configura un profilo

Un profilo è una raccolta di configurazioni impostate. È possibile avere fino a 30 profili con diverse priorità e schemi.

Per impostare un nuovo profilo:

1. Andare in **Profiles (Profili)** e fare clic su + **Create (Crea)**.
2. Immetti un **Name (Nome)** e **Description (Descrizione)**.
3. Seleziona le impostazioni **Light (Luce)** e **Siren (Sirena)** che vuoi per il profilo.
4. Imposta la **Priority (Priorità)** di luce e sirena e fai clic su **Save (Salva)**.

Per la modifica di un profilo, fare clic su ⋮ e selezionare **Edit (Modifica)**.

Importa o esporta un profilo

Se vuoi usare un profilo con configurazioni predefinite, puoi importarlo:

1. Andare in **Profiles (Profili)** e fare clic su + **Import (Importa)**.
2. Sfoglia per trovare il file o trascina e rilascia il file che vuoi importare.
3. Fare clic su **Save (Salva)**.

Per eseguire la copia di uno o molteplici profili e salvarli in altri dispositivi, puoi esportarli:

1. Seleziona i profili.
2. fare clic su **Esporta**.
3. Sfoglia per individuare i file .json.

Impostazione SIP diretto (P2P)

Utilizzare peer-to-peer quando la comunicazione si trova tra pochi agenti utente all'interno della stessa rete IP e non è necessario disporre di funzionalità aggiuntive che un server PBX può fornire.

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

1. Andare a **System (Sistema)** > **SIP** > **SIP settings (Impostazioni SIP)** e selezionare **Enable SIP (Abilita SIP)**.
2. Per consentire al dispositivo di ricevere chiamate in entrata, selezionare **Allow incoming SIP calls (Consenti chiamate SIP in arrivo)**.
3. In **Call handling (Gestione chiamate)**, impostare il timeout e la durata della chiamata.
4. In **Ports (Porte)**, inserire i numeri delle porte.
   - **SIP port (Porta SIP)**: la porta di rete utilizzata per le comunicazioni SIP. Il traffico di segnalazione tramite la porta non viene crittografato. Il numero di porta predefinito è 5060. Se necessario, inserire un numero di porta differente.
   - **TLS port (Porta TLS)**: porta di rete utilizzata per la comunicazione SIP crittografata. Il traffico di segnalazione attraverso la porta viene crittografato tramite TLS (Transport Layer Security). Il numero di porta predefinito è 5061. Se necessario, inserire un numero di porta differente.
   - **RTP start port (Porta di avvio RTP)**: inserire la porta utilizzata per il primo flusso RTP in una chiamata SIP. La porta di avvio predefinita per i trasporti multimediali è la 4000. Alcuni firewall potrebbero bloccare il traffico RTP su determinati numeri di porta. Un numero di porta deve essere compreso tra 1024 e 65 535.
5. In **NAT traversal**, selezionare i protocolli che si desidera abilitare per NAT traversal.

Nota

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

6. In **Audio**, selezionare almeno un codec audio con la qualità audio desiderata per le chiamate SIP. Trascina e rilascia per modificare la priorità.
7. In **Additional (Aggiuntivo)**, selezionare opzioni aggiuntive.
   - **UDP-to-TCP switching (Passaggio da UDP a TCP)**: selezionare questa opzione per consentire alle chiamate di scambiare i protocolli di trasporto da UDP (User Datagram Protocol) a TCP (Transmission Control Protocol). La ragione per il passaggio è evitare la frammentazione e il passaggio può essere eseguito se una richiesta rientra nei 200 byte del parametro MTU (Maximum Transmission Unit) o supera i 1300 byte.
   - **Allow via rewrite (Consenti tramite riscrittura)**: selezionare per inviare l'indirizzo IP locale e non l'indirizzo IP pubblico del router.
   - **Allow contact rewrite (Consenti riscrittura contatto)**: selezionare questa opzione per inviare l'indirizzo IP locale e non l'indirizzo IP pubblico del router.
   - **Register with server every (registra con il server ogni)**: impostare la frequenza con cui si desidera che il dispositivo si sincronizzi con il server SIP per gli account SIP esistenti.
   - **DTMF payload type (Tipo payload DTMF)**: modificare il tipo di payload per DTMF.
8. Fare clic su **Save (Salva)**.

Configurazione di SIP tramite un server (PBX)

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

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

1. Richiedere le seguenti informazioni dal provider PBX:

- ID utente
- Dominio
- Password
- ID di autenticazione
- ID chiamante

- Registrar
- Porta di avvio RTP

2. Per aggiungere un nuovo account, andare a **System (Sistema)** > **SIP** > **SIP accounts (Account SIP)** e fare clic su **+ Account (Aggiungi account)**.
3. Inserire i dettagli ricevuti dal provider PBX.
4. Selezionare **Registered (Registrato)**.
5. Selezionare una modalità di trasporto.
6. Fare clic su **Save (Salva)**.
7. Configurare le impostazioni SIP allo stesso modo del peer-to-peer. Consultare *SIP* per ulteriori informazioni.

Imposta regole per eventi

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.

Inizia un profilo quando avviene l'attivazione di un allarme

In questo esempio viene spiegato come attivare un allarme in caso di modifica del segnale di input digitale.

Impostare la direzione su input per la porta:

1. Andare su **System (Sistema)** > **Accessories (Accessori)** > **I/O ports (Porte I/O)**.
2. Vai su **Port 1 (Porta 1)** > **Normal state (Stato normale)** fai clic su **Circuit closed (Circuito chiuso)**.

Creare una regola:

1. Vai su **System (Sistema)** > **Events (Eventi)** e aggiungi una regola.
2. Inserire un nome per la regola.
3. Nell'elenco delle condizioni, selezionare **I/O** > **Digital input is active (Input digitale è attivo)**.
4. Seleziona **Port 1 (Porta 1)**.
5. Nella lista di azioni, selezionare **Run light and siren profile while the rule is active (Esegui profilo luce e sirena mentre la regola è attiva)**.
6. Seleziona il profilo che vuoi avviare.
7. Fare clic su **Save (Salva)**.

Inizia un profilo attraverso SIP

Questo esempio illustra come si attiva un allarme attraverso SIP.

Attivazione SIP:

1. Vai a **System (Sistema)** > **SIP** > **SIP settings (Impostazioni SIP)**.
2. Seleziona **Enable SIP (Abilita SIP)** e **Allow incoming calls (Consenti chiamate in entrata)**.

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

Creare una regola:

1. Vai su **System (Sistema)** > **Events (Eventi)** e aggiungi una regola.
2. Inserire un nome per la regola.
3. Nell'elenco delle condizioni, seleziona **Call (Chiama)** > **State (Stato)**.
4. Nell'elenco dello stato, seleziona **Active (Attivo)**.
5. Nella lista di azioni, selezionare **Run light and siren profile while the rule is active (Esegui profilo luce e sirena mentre la regola è attiva)**.
6. Seleziona il profilo che vuoi avviare.
7. Fare clic su **Save (Salva)**.

Controlla più di un profilo con le estensioni SIP

Attivazione SIP:

1. Vai a **System (Sistema)** > **SIP** > **SIP settings (Impostazioni SIP)**.
2. Seleziona **Enable SIP (Abilita SIP)** e **Allow incoming calls (Consenti chiamate in entrata)**.
3. Fare clic su **Save (Salva)**.

Crea una regola per avviare un profilo:

1. Vai su **System (Sistema)** > **Events (Eventi)** e aggiungi una regola.
2. Inserire un nome per la regola.
3. Nell'elenco delle condizioni, seleziona **Call (Chiama)** > **State change (Cambio di stato)**.
4. Nella lista dei motivi, seleziona **Accepted by device (Accettato dal dispositivo)**.
5. In **Call direction (Direzione di chiamata)**, seleziona **Incoming (In entrata)**.
6. In **Local SIP URI (URI SIP locale)**, digita **<sip:[Ext]@[indirizzo IP]>** dove [Ext] è l'estensione usata per il profilo e [indirizzo IP] è l'indirizzo del dispositivo. Ad esempio **sip:1001@192.168.0.90**.
7. Nella lista di azioni, selezionare **Light and Siren (Luce e sirena)** > **Run light and siren profile (Esegui profilo luce e sirena)**.
8. Seleziona il profilo che vuoi avviare.
9. Seleziona l'azione **Start (Avvia)**.
10. Fare clic su **Save (Salva)**.

Crea una regola per arrestare un profilo:

1. Vai su **System (Sistema)** > **Events (Eventi)** e aggiungi una regola.
2. Inserire un nome per la regola.
3. Nell'elenco delle condizioni, seleziona **Call (Chiama)** > **State change (Cambio di stato)**.
4. Nell'elenco dei motivi, seleziona **Terminated (Terminato)**.
5. In **Call direction (Direzione di chiamata)**, seleziona **Incoming (In entrata)**.
6. In **Local SIP URI (URI SIP locale)**, digita **sip:[Ext]@[indirizzo IP]** dove [Ext] è l'estensione usata per il profilo e [indirizzo IP] è l'indirizzo del dispositivo. Ad esempio **sip:1001@192.168.0.90**.
7. Nella lista di azioni, selezionare **Light and Siren (Luce e sirena)** > **Run light and siren profile (Esegui profilo luce e sirena)**.
8. Seleziona il profilo che vuoi fermare.
9. Seleziona l'azione **Stop (Arresta)**.
10. Fare clic su **Save (Salva)**.

Ripeti la procedura per la creazione di regole di avvio e arresto per ogni profilo che si vuole controllare tramite SIP.

Esecuzione di due profili con priorità diverse

Se esegui due profili con priorità diverse, quello con un numero di priorità più alto interromperà quello con un numero di priorità più basso.

Nota

Se esegui due profili della stessa priorità, quello più recente annullerà quello precedente.

Questo esempio illustra come si imposta il dispositivo in modo da mostrare un profilo con priorità 4 invece di un altro profilo con priorità 3 quando attivato dalla porta I/O digitale.

Crea profili:

1. Crea un profilo con priorità 3.
2. Crea un altro profilo con priorità 4.

Creare una regola:

1. Vai su **System (Sistema)** > **Events (Eventi)** e aggiungi una regola.
2. Inserire un nome per la regola.
3. Nell'elenco delle condizioni, selezionare **I/O** > **Digital input is active (Input digitale è attivo)**.
4. Seleziona una porta.
5. Nella lista di azioni, selezionare **Run light and siren profile while the rule is active (Esegui profilo luce e sirena mentre la regola è attiva)**.
6. Seleziona il profilo dal numero di priorità più alto.
7. Fare clic su **Save (Salva)**.
8. Vai su **Profiles (Profili)** e avvia il profilo dotato di numero di priorità più basso.

Attivazione di una sirena tramite input virtuale quando una videocamera rileva movimento

In questo esempio viene spiegato come collegare una telecamera alla sirena stroboscopica e come attivare un profilo nella sirena stroboscopica quando l'applicazione AXIS Motion Guard, installata nella telecamera, rileva movimento.

Prima di iniziare:

- Crea un nuovo account con privilegi Operatore o Amministratore nella sirena stroboscopica.
- Crea un profilo nella sirena stroboscopica.
- Configurare AXIS Motion Guard nella telecamera e creare un profilo denominato "Profilo telecamera".

Creare due destinatari nella telecamera:

1. Nell'interfaccia del dispositivo della telecamera, vai a **System > Events > Recipients (Sistema > Eventi > Destinatari)** e aggiungi un destinatario.
2. Immettere le seguenti informazioni:
   - **Nome**: Attiva la porta virtuale
   - **Tipo**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/virtualinput/activate.cgi
     Sostituire l'<indirizzo IP> con l'indirizzo della sirena stroboscopica.
   - L'account e la password dell'account sirena stroboscopica appena creato.
3. Fare clic su **Test (Verifica)** per assicurarsi che tutti i dati siano validi.
4. Fare clic su **Save (Salva)**.

5. Aggiungere un secondo destinatario con le seguenti informazioni:
   - **Nome**: disattivare la porta virtuale
   - **Tipo**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi
     Sostituire l'<indirizzo IP> con l'indirizzo della sirena stroboscopica.
   - L'account e la password dell'account sirena stroboscopica appena creato.
6. Fare clic su **Test (Verifica)** per assicurarsi che tutti i dati siano validi.
7. Fare clic su **Save (Salva)**.

Creare due regole nella telecamera:

1. Andare a **Rules (Regole)** e aggiungere una regola.
2. Immettere le seguenti informazioni:
   - **Nome**: attivare la porta virtuale IO1
   - **Condition (condizione)**: **Applications (Applicazioni) > Motion Guard: Camera profile (Motion Guard: profilo telecamera)**
   - **Action (Azione)**: **Notifications > Send notification through HTTP (notifiche, invia notifiche tramite HTTP)**
   - **Recipient (Destinatario)**: **Activate virtual port (Attiva porta virtuale)**
   - **Query string suffix (Suffisso stringa richiesta)**: schemaversion=1&port=1
3. Fare clic su **Save (Salva)**.
4. Aggiungere un'altra regola con le seguenti informazioni:
   - **Nome**: Disattivare la porta virtuale IO1
   - **Condition (condizione)**: **Applications (Applicazioni) > Motion Guard: Camera profile (Motion Guard: profilo telecamera)**
   - Seleziona **Invert this condition (Inverti questa condizione)**.
   - **Action (Azione)**: **Notifications > Send notification through HTTP (notifiche, invia notifiche tramite HTTP)**
   - **Recipient (Destinatario)**: **Deactivate virtual port (Disattiva porta virtuale)**
   - **Query string suffix (Suffisso stringa richiesta)**: schemaversion=1&port=1
5. Fare clic su **Save (Salva)**.

Creare una regola nella sirena stroboscopica:

1. Nell'interfaccia web della sirena stroboscopica, andare a **System > Events (Sistema > Eventi)** e aggiungere una regola.
2. Immettere le seguenti informazioni:
   - **Nome**: attivazione su ingresso virtuale 1
   - **Condition (Condizione)**: **I/O > Virtual input (Ingresso virtuale)**
   - **Porta**: **1**
   - **Action (Azione)**, **Light and siren (Luce e sirena) > Run light profile while the rule is active (Esegui il profilo luce mentre la regola è attiva)**
   - **Profile (Profilo)**: selezionare il profilo appena creato
3. Fare clic su **Save (Salva)**.

Attivazione di una sirena tramite un quando HTTP Post quando una videocamera rileva movimento

In questo esempio viene spiegato come collegare una telecamera alla sirena stroboscopica e come attivare un profilo nella sirena stroboscopica quando l'applicazione AXIS Motion Guard, installata nella telecamera, rileva movimento.

Prima di iniziare:

- Crea un nuovo utente con il ruolo Operatore o Amministratore nella sirena stroboscopica.
- Crea un profilo nella sirena stroboscopica chiamata: "Profilo sirena di allarme".
- Configurare AXIS Motion Guard nella telecamera e creare un profilo denominato: "Camera profile (Profilo telecamera)".
- Assicurarsi di utilizzare AXIS Device Assistant con la versione firmware 10.8.0 o successiva.

Crea un destinatario nella telecamera:

1. Nell'interfaccia del dispositivo della telecamera, vai a **System > Events > Recipients (Sistema > Eventi > Destinatari)** e aggiungi un destinatario.
2. Immettere le seguenti informazioni:
   - **Nome**: Sirena stroboscopica
   - **Tipo**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/siren_and_light.cgi
     Sostituire l'<indirizzo IP> con l'indirizzo della sirena stroboscopica.
   - Il nome utente e la password dell'utente della sirena stroboscopica appena creato.
3. Fare clic su **Test (Verifica)** per assicurarsi che tutti i dati siano validi.
4. Fare clic su **Save (Salva)**.

Creare due regole nella telecamera:

1. Andare a **Rules (Regole)** e aggiungere una regola.
2. Immettere le seguenti informazioni:
   - **Nome**: Attivare la sirena di allarme con movimento
   - **Condition (condizione)**: **Applications (Applicazioni) > Motion Guard: Camera profile (Motion Guard: profilo telecamera)**
   - **Action (Azione)**: **Notifications > Send notification through HTTP (notifiche, invia notifiche tramite HTTP)**
   - **Recipient (Destinatario)**: **Strobe siren (Sirena stroboscopica)**.
     Le informazioni devono essere le stesse immesse in precedenza in **Events > Recipients > Name (Eventi > Destinatari > Nome)**.
   - **Method (Metodo)**:**Post**
   - **Body (Corpo)**:

```
{  "apiVersion": "1.0",  "method": "start",  "params": {
"profile" : "Strobe siren profile"  } }
```

Assicurarsi di inserire le stesse informazioni in '**"profile" : <>**' (profilo) che sono state create per il sensore di qualità dell'aria, in questo caso: "Profilo sirena di allarme".

3. Fare clic su **Save (Salva)**.
4. Aggiungere un'altra regola con le seguenti informazioni:
   - **Nome**: Disattivare la sirena di allarme con movimento
   - **Condition (condizione)**: **Applications (Applicazioni) > Motion Guard: Camera profile (Motion Guard: profilo telecamera)**
   - Seleziona **Invert this condition (Inverti questa condizione)**.

- **Action (Azione)**: **Notifications > Send notification through HTTP (notifiche, invia notifiche tramite HTTP)**
- **Recipient (Destinatario)**: **Strobe siren (Sirena stroboscopica)**
  Le informazioni devono essere le stesse immesse in precedenza in **Events > Recipients > Name (Eventi > Destinatari > Nome)**.
- **Method (Metodo)**:**Post**
- **Body (Corpo)**:

```
{  "apiVersion": "1.0",  "method": "stop",  "params": {    "profile" : "Strobe siren profile"  } }
```

Assicurarsi di inserire le stesse informazioni in '**"profile" : <>**' (profilo) che sono state create per il sensore di qualità dell'aria, in questo caso: "Profilo sirena di allarme".

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

Attivazione della sirena stroboscopica su MQTT quando la telecamera rileva movimento

In questo esempio viene descritto come collegare una telecamera alla sirena stroboscopica su MQTT e come attivare un profilo nella sirena stroboscopica quando l'applicazione AXIS Motion Guard, installata nella telecamera, rileva movimento.

Prima di iniziare:

- Crea un profilo nella sirena stroboscopica.
- Imposta un broker MQTT e ottieni l'indirizzo IP, il nome utente e la password del broker.
- Configurare AXIS Motion Guard nella telecamera.

Configura il client MQTT nella telecamera:

1. Nell'interfaccia dispositivo della telecamera, vai su **System > MQTT > MQTT client > Broker (Sistema > MQTT > Client MQTT > Broker)** e immetti le seguenti informazioni:
   - **Host**: Indirizzo IP broker
   - **Client ID (ID client)**: Ad es., Telecamera 1
   - **Protocol (Protocollo)**: Il protocollo su cui è impostato il broker
   - **Port (Porta)**: Il numero di porta utilizzato dal broker
   - **Username (Nome utente)** e **Password** del broker
2. Fare clic su **Save (Salva)** e **Connect (Connetti)**.

Creazione di due regole nella telecamera per la pubblicazione MQTT:

1. Andare a **System > Events > Rules (Sistema > Eventi > Regole)** e aggiungere una regola.
2. Immettere le seguenti informazioni:
   - **Nome**: Oggetti in movimento rilevati
   - **Condition (condizioni)**: **Applications (applicazioni) > Motion alarm (allarme di movimento)**
   - **Action (Azione)**: **MQTT > Send MQTT publish message (MQTT > Invia messaggio di pubblicazione MQTT)**
   - **Topic (Argomento)**: Movimento
   - **Payload**: On
   - **QoS**: 0, 1 o 2
3. Fare clic su **Save (Salva)**.
4. Aggiungere un'altra regola con le seguenti informazioni:
   - **Nome**: Nessun movimento
   - **Condition (condizioni)**: **Applications (applicazioni) > Motion alarm (allarme di movimento)**

- Seleziona **Invert this condition (Inverti questa condizione)**.
- **Action (Azione)**: **MQTT > Send MQTT publish message (MQTT > Invia messaggio di pubblicazione MQTT)**
- **Topic (Argomento)**: Movimento
- **Payload**: Off
- **QoS**: 0, 1 o 2

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

Imposta il client MQTT nella sirena stroboscopica:

1. Nell'interfaccia dispositivo della sirena stroboscopica, vai su **System > MQTT > MQTT client > Broker (Sistema > MQTT > Client MQTT > Broker)** e immetti le seguenti informazioni:
   - **Host**: Indirizzo IP broker
   - **Client ID (ID client)**: Sirena 1
   - **Protocol (Protocollo)**: Il protocollo su cui è impostato il broker
   - **Port (Porta)**: Il numero di porta utilizzato dal broker
   - **Username (Nome utente)** e **Password**
2. Fare clic su **Save (Salva)** e **Connect (Connetti)**.
3. Vai su **MQTT subscriptions (Sottoscrizioni MQTT)** e aggiungi una sottoscrizione.
   Immettere le seguenti informazioni:
   - **Subscription filter (Filtro sottoscrizione)**: Movimento
   - **Subscription type (Tipo di sottoscrizione)**: Dotato di stato
   - **QoS**: 0, 1 o 2
4. Fare clic su **Save (Salva)**.

Creazione di una regola nella sirena stroboscopica per le sottoscrizioni MQTT:

1. Andare a **System > Events > Rules (Sistema > Eventi > Regole)** e aggiungere una regola.
2. Immettere le seguenti informazioni:
   - **Nome**: Oggetti in movimento rilevati
   - **Condition (Condizione)**: **MQTT > Stateful (MQTT > Dotato di stato)**
   - **Subscription filter (Filtro sottoscrizione)**: **Motion (Movimento)**
   - **Payload**: On
   - **Action (Azione)**, **Light and siren (Luce e sirena) > Run light profile while the rule is active (Esegui il profilo luce mentre la regola è attiva)**
   - **Profile (Profilo)**: seleziona il profilo che vuoi sia attivo.
3. Fare clic su **Save (Salva)**.

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

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>`.

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. In questo caso un indirizzo IP statico 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.

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

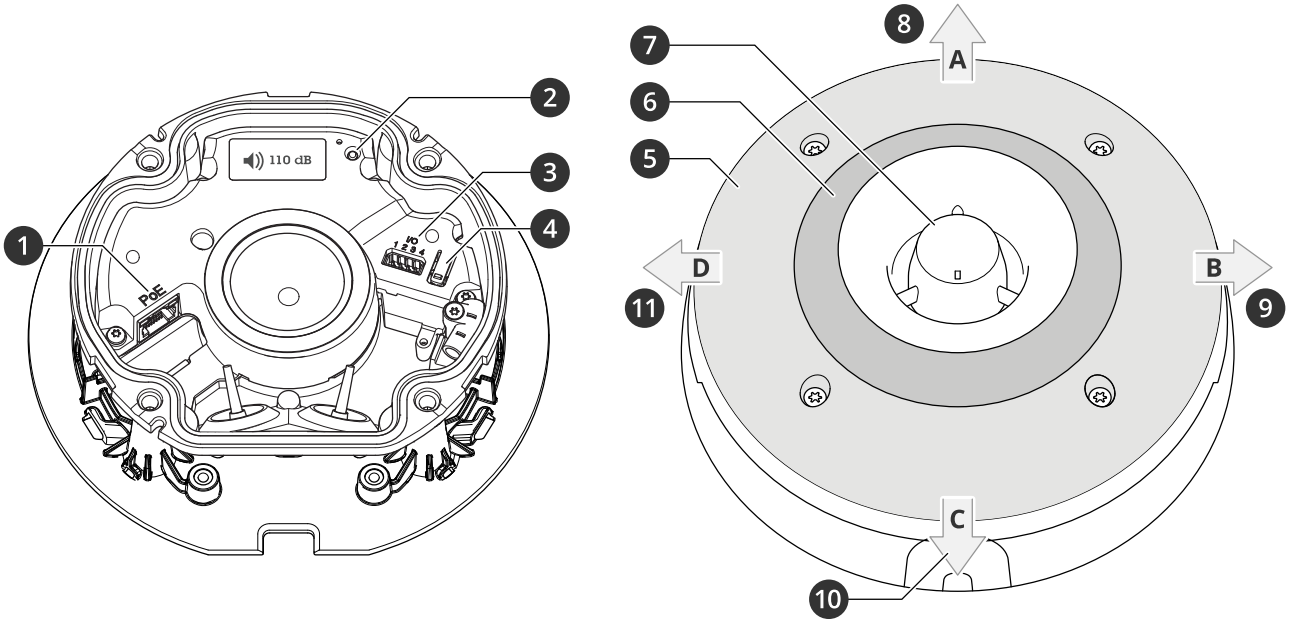
Il router deve supportare NAT traversal e UPnP®.

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.

Dati tecnici

Panoramica dei prodotti



1 *Connettore di rete PoE*
2 *Indicatore LED di stato*
3 *Connettore I/O*
4 *Pulsante di comando*
5 *LED bianchi*
6 *LED rosso, blu, verde, giallo (RGBA)*
7 *Siren (Sirena):*
8 *Direzione della luce A*
9 *Direzione della luce B*
10 *Direzione della luce C*
11 *Direzione della luce D*

Indicatori LED

LED di stato	Significato
Verde	Una luce verde fissa per 10 secondi indica il normale funzionamento una volta completato l'avvio.
Giallo	Luce fissa: durante l'avvio o il ripristino delle impostazioni predefinite o della configurazione.

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

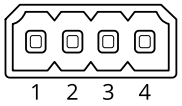
Connettore Ethernet RJ45 con Power over Ethernet (PoE).

Connettore I/O

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.

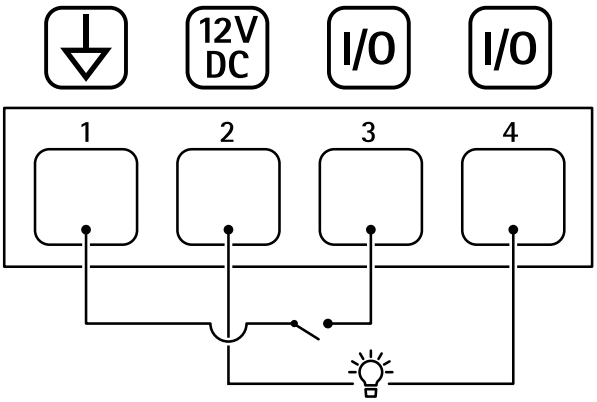
Uscita digitale – Per il collegamento di dispositivi esterni come relè e LED. I dispositivi collegati possono essere attivati tramite l'API (interfaccia per la programmazione di applicazioni) VAPIX® attraverso un evento oppure dall'interfaccia Web del dispositivo.

Morsettiera a 4 pin



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)	3-4	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:



1 *Terra CC*
2 *Uscita CC 12 V, max 50 mA*
3 *I/O configurato come input*
4 *I/O configurato come output*

Nomi dei pattern di luce

Off
Fisso
Bianco fisso + colore lampeggiante
alternata
Pulse (Impulso):
Intensificazione 3 passaggi
Lampeggiante
Intermittenza 3 volte
Intermittenza 4 volte
Intermittenza 3 volte dissolvenza
Intermittenza 4 volte dissolvenza
Lampeggio 1 volta
Lampeggio 3 volte
Lampeggio 1 volta bianco + colore fisso
Lampeggio 3 volte bianco + colore fisso
Direzione A + colore fisso
Direzione B + colore fisso
Direzione C + colore fisso
Direzione D + colore fisso
Rotazione bianco + colore fisso
Rotazione coda bianco + colore fisso
Bianco + colore fisso casuale
Giro bianco + colore fisso
Bianco fisso + colore fisso

Nomi delle sequenze sonore

Off
Allarme: suono allarme di altezza elevata
Allarme: suono allarme di altezza bassa
Allarme: Uccello
Allarme: sirena navale
Allarme: Allarme auto
Allarme: allarme auto veloce
Allarme: orologio classico
Allarme: pronto intervento

Allarme: orrore
Allarme: Stabilimenti industriali
Allarme: segnale acustico singolo
Allarme: segnale acustico quadruplo discreto
Allarme: segnale acustico triplo discreto
Allarme: triplo suono ad altezza elevata
Notifica: Negato
Notifica: Fine
Notifica: ingresso
Notifica: Fallito
Notifica: fretta
Notifica: Messaggio
Notifica: Successiva
Notifica: Aperta
Siren (Sirena): alternata
Siren (Sirena): scattante
Siren (Sirena): evac.
Siren (Sirena): altezza in calo
Siren (Sirena): residenziale discreta

Pulizia del dispositivo

È possibile pulire il dispositivo con acqua tiepida e sapone delicato, non abrasivo.

AVVISO

- Le sostanze chimiche possono danneggiare il dispositivo. Non utilizzare sostanze chimiche come detergenti per vetri o acetone per pulire il dispositivo.
- Evitare la pulizia alla luce diretta del sole o a temperature elevate, poiché ciò può causare macchie.

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

Per ulteriori informazioni sulla pulizia dei dispositivi Axis, consultare il documento tecnico *Resistenza chimica ai comuni prodotti per la pulizia*.

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 18*.
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*.

Problemi relativi all'audio	
Il volume del dispositivo non è elevato come previsto	Assicurati che il dispositivo sia chiuso in modo esatto e che non siano presenti ostruzioni nella tromba o nell'elemento dell'altoparlante.
Il dispositivo non emette alcun suono	Verifica se il dispositivo è in **Maintenance mode (Modalità di manutenzione)**. Se si trova in modalità di manutenzione, disattivala.

Problemi di luce	
Il dispositivo non è luminoso come previsto	Assicurati di usare un alimentatore PoE di classe 4. Controlla la temperatura ambiente del dispositivo. Se il dispositivo è installato in un ambiente a temperatura elevata, le luci si abbasseranno in automatico.

Considerazioni sulle prestazioni

I fattori più importanti da considerare:

- Un utilizzo eccessivo della rete dovuto a una scarsa infrastruttura influisce sulla larghezza di banda.

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.

T10223803_it

2026-10 (M7.2)

© 2025 – 2026 Axis Communications AB