

AXIS D4100-E Network Strobe Siren

Manuale per l'utente

AXIS D4100-E Network Strobe Siren

Sommario

Installazione	3
Introduzione	4
Individuazione del dispositivo sulla rete	4
Aprire l'interfaccia web del dispositivo	4
Panoramica dell'interfaccia web	5
Configurare il dispositivo	6
Disattiva la modalità manutenzione dopo l'installazione della sirena	6
Attiva modalità manutenzione	6
Configura un profilo	6
Importa o esporta un profilo	6
Impostazione SIP diretto (P2P)	6
Configurazione di SIP tramite un server (PBX)	7
Imposta regole per eventi	8
Ulteriori informazioni	16
Session Initiation Protocol (SIP)	16
Peer-to-peer SIP (P2PSIP)	16
Private Branch Exchange (PBX)	16
NAT traversal	16
Interfaccia web	17
Stato	17
Panoramica	18
Profili	18
App	19
Sistema	20
Manutenzione	38
Specifiche	39
Panoramica del dispositivo	39
Indicatori LED	39
Pulsanti	39
Connettori	40
Nomi dei pattern di luce	41
Livelli di pressione sonora massimi	41
Consigli per la pulizia	43
Risoluzione di problemi	44
Ripristino delle impostazioni predefinite di fabbrica	44
Opzioni firmware	44
Controllo della versione firmware corrente	44
Aggiornamento del firmware	44
Problemi tecnici, indicazioni e soluzioni	45
Considerazioni sulle prestazioni	46
Contattare l'assistenza	47

AXIS D4100-E Network Strobe Siren

Installazione

Installazione



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

help.axis.com/?&pid=62021&tsection=install

AXIS D4100-E Network Strobe Siren

Introduzione

Introduzione

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

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

Aprire l'interfaccia web del dispositivo

1. Digitare il nome utente e la password. Se si accede al dispositivo per la prima volta, è necessario creare un account amministratore. Consultare *Creare un account amministratore alla pagina 4*.

Creare 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. Consultare *Password sicure alla pagina 4*.
3. Reinserire la password.
4. Fare clic su **Add user (Aggiungi utente)**.

Password sicure

Importante

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

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

Per proteggere i tuoi dati ti consigliamo vivamente di:

- Utilizzare una password con almeno 8 caratteri, preferibilmente creata da un generatore di password.
- Non mostrare la password.

AXIS D4100-E Network Strobe Siren

Introduzione

- Cambiare la password a intervalli regolari, almeno una volta all'anno.

Panoramica dell'interfaccia web

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



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

help.axis.com/?Etpiald=62021&tsection=web-interface-overview

Interfaccia web dei dispositivi Axis

AXIS D4100-E Network Strobe Siren

Configurare il dispositivo

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. Vai su **Profiles (Profili)** e fai 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, fai clic su  e seleziona **Edit (Modifica)**.

Importa o esporta un profilo

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

1. Vai a **Profiles (Profili)** e fai 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 **Export (Esporta)**.
3. Sfoglia per individuare i file .json.

AXIS D4100-E Network Strobe Siren

Configurare il dispositivo

Impostazione SIP diretto (P2P)

Utilizzare peer-to-peer quando la comunicazione si trova tra pochi agenti utente all'interno della stessa rete IP e non è necessario disporre di funzionalità aggiuntive che un server PBX può fornire. Per capire meglio il funzionamento del P2P, consultare *Peer-to-peer SIP (P2PSIP) alla pagina 16*.

Per ulteriori informazioni sulle opzioni di impostazione, consultare *SIP alla pagina 32*.

1. Andare a **System (Sistema) > SIP > SIP settings (Impostazioni SIP)** e selezionare **Enable SIP (Abilita SIP)**.
2. Per consentire al dispositivo di ricevere chiamate in entrata, selezionare **Allow incoming calls (Consenti chiamate in arrivo)**.
3. In **Call handling (Gestione chiamate)**, impostare il timeout e la durata della chiamata.
4. In **Ports (Porte)**, inserire i numeri delle porte.
 - **SIP port (Porta SIP)**: la porta di rete utilizzata per le comunicazioni SIP. Il traffico di segnalazione tramite la porta non viene crittografato. Il numero di porta predefinito è 5.060. Se necessario, inserire un numero di porta diverso.
 - **TLS port (Porta TLS)**: porta di rete utilizzata per la comunicazione SIP crittografata. Il traffico di segnalazione attraverso la porta viene crittografato tramite TLS (Transport Layer Security). Il numero di porta predefinito è 5.061. Se necessario, inserire un numero di porta diverso.
 - **RTP start port (Porta di avvio RTP)**: inserire la porta utilizzata per il primo flusso RTP in una chiamata SIP. La porta di avvio predefinita per il trasporto multimediale è 4.000. Alcuni firewall potrebbero bloccare il traffico RTP su alcuni numeri di porta. Un numero di porta deve essere compreso tra 1.024 e 65.535.
5. In **NAT traversal**, selezionare i protocolli che si desidera abilitare per NAT traversal.

Nota

Utilizzare NAT traversal quando il dispositivo è collegato alla rete da un router NAT o un firewall. Per ulteriori informazioni, consultare *NAT traversal alla pagina 16*.

6. In **Audio**, selezionare almeno un codec audio con la qualità audio desiderata per le chiamate SIP. Trascinare e rilasciare per modificare la priorità.
7. In **Additional (Aggiuntivo)**, selezionare opzioni aggiuntive.
 - **UDP-to-TCP switching (Passaggio da UDP a TCP)**: selezionare questa opzione per consentire alle chiamate di scambiare temporaneamente i protocolli di trasporto da UDP (User Datagram Protocol) a TCP (Transmission Control Protocol). Il motivo dello scambio è evitare la frammentazione e lo scambio può essere eseguito se una richiesta rientra nei 200 byte del parametro MTU (Maximum Transmission Unit) o supera i 1.300 byte.
 - **Allow via rewrite (Consenti tramite riscrittura)**: selezionare per inviare l'indirizzo IP locale e non l'indirizzo IP pubblico del router.
 - **Allow contact rewrite (Consenti riscrittura contatto)**: selezionare questa opzione per inviare l'indirizzo IP locale e non l'indirizzo IP pubblico del router.
 - **Register with server every (registra con il server ogni)**: impostare la frequenza con cui si desidera che il dispositivo si sincronizzi con il server SIP per gli account SIP esistenti.
 - **DTMF payload type (Tipo payload DTMF)**: modificare il tipo di payload per DTMF.
8. Fare clic su **Save (Salva)**.

Configurazione di SIP tramite un server (PBX)

Utilizzare un server PBX quando la comunicazione deve essere compresa tra un numero infinito di agenti utente all'interno e all'esterno della rete IP. Altre funzionalità possono essere aggiunte alla configurazione a seconda del provider PBX. Per capire meglio il funzionamento del P2P, consultare *Private Branch Exchange (PBX) alla pagina 16*.

AXIS D4100-E Network Strobe Siren

Configurare il dispositivo

Per ulteriori informazioni sulle opzioni di impostazione, consultare *SIP alla pagina 32*.

1. Richiedere le seguenti informazioni dal provider PBX:
 - ID utente
 - Dominio
 - Password
 - ID di autenticazione
 - ID chiamante
 - Registrar
 - Porta di avvio RTP
2. Per aggiungere un nuovo account, andare a **System (Sistema) > SIP > SIP accounts (Account SIP)** e fare clic su **+ Account (Aggiungi account)**.
3. Inserire i dettagli ricevuti dal provider PBX.
4. Selezionare **Registered (Registrato)**.
5. Selezionare una modalità di trasporto.
6. Fare clic su **Save (Salva)**.
7. Configurare le impostazioni SIP allo stesso modo del peer-to-peer. Per ulteriori informazioni, consultare *Impostazione SIP diretto (P2P) alla pagina 6*.

Imposta regole per eventi

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

Attivazione di un'azione

1. Andare a **System > Events (Sistema > Eventi)** e aggiungere una regola. La regola consente di definire quando il dispositivo eseguirà determinate azioni. È possibile impostare regole pianificate, ricorrenti o attivate manualmente.
2. Inserire 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 **Action (Azione)** che deve eseguire il dispositivo quando le condizioni sono soddisfatte.

Nota

Se vengono apportate modifiche a una regola attiva, tale regola deve essere abilitata nuovamente per rendere valide le modifiche.

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 position (Posizione normale)** fai clic su **Circuit closed (Circuito chiuso)**.

Creare una regola:

AXIS D4100-E Network Strobe Siren

Configurare il dispositivo

1. Vai su **System (Sistema) > Events (Eventi)** e aggiungi una regola.
2. Inserire un nome per la regola.
3. Dall'elenco delle condizioni, seleziona **I/O > Digital input (Input digitale)**.
4. Seleziona **Port 1 (Porta 1)**.
5. Nella lista di azioni, seleziona **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, seleziona **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)**.

AXIS D4100-E Network Strobe Siren

Configurare il dispositivo

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, seleziona **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, seleziona **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. Dall'elenco delle condizioni, seleziona **I/O > Digital input (Input digitale)**.
4. Seleziona una porta.

AXIS D4100-E Network Strobe Siren

Configurare il dispositivo

5. Nella lista di azioni, seleziona **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 utente con il ruolo Operatore o Amministratore nella sirena stroboscopica.
- Crea un profilo nella sirena stroboscopica.
- Configura AXIS Motion Guard nella telecamera e crea 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. Inserire le seguenti informazioni:
 - **Name (Nome):** Attiva la porta virtuale
 - **Type (Tipo):** HTTP
 - **URL:** `http://<IPaddress>/axis-cgi/virtualinput/activate.cgi`
Sostituire <IPaddress> 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)**.
5. Aggiungere un secondo destinatario con le seguenti informazioni:
 - **Name (Nome):** disattivare la porta virtuale
 - **Type (Tipo):** HTTP
 - **URL:** `http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi`
Sostituire <IPaddress> con l'indirizzo della sirena stroboscopica.
 - Il nome utente e la password dell'utente della 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. Vai a **Rules (Regole)** e aggiungi una regola.
2. Inserire le seguenti informazioni:
 - **Name (Nome):** attivare la porta virtuale IO1

AXIS D4100-E Network Strobe Siren

Configurare il dispositivo

- Condition (Condizione): Applications > Motion Guard: Camera profile (Applicazioni > Motion Guard: Profilo telecamera)
 - Action (Azione): Notifications > Send notification through HTTP (Notifiche > Invia notifica tramite HTTP)
 - Recipient (Destinatario): Activate virtual port (Attiva la 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:
 - Name (Nome): Disattivare la porta virtuale IO1
 - Condition (Condizione): Applications > Motion Guard: Camera profile (Applicazioni > Motion Guard: Profilo telecamera)
 - Seleziona **Invert this condition (Inverti questa condizione)**.
 - Action (Azione): Notifications > Send notification through HTTP (Notifiche > Invia notifica tramite HTTP)
 - Recipient (Destinatario): Deactivate virtual port (Disattivare la 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 del dispositivo della sirena stroboscopica, andare a **System > Events (Sistema > Eventi)** e aggiungere una regola.
2. Inserire le seguenti informazioni:
 - Name (Nome): Attivazione su ingresso virtuale 1
 - Condition (Condizione): I/O > Virtual input (I/O > Ingresso virtuale)
 - Port (Porta): 1
 - Action (Azione): Light and siren > Run light and siren profile while the rule is active (Luce e sirena > Eseguire il profilo della luce e della sirena 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".
- Configura AXIS Motion Guard nella telecamera e crea un profilo denominato: "Profilo telecamera".
- Assicurarsi di utilizzare AXIS Device Assistant con la versione firmware 10.8.0 o successiva.

Creare un destinatario nella telecamera:

AXIS D4100-E Network Strobe Siren

Configurare il dispositivo

1. Nell'interfaccia del dispositivo della telecamera, vai a **System > Events > Recipients (Sistema > Eventi > Destinatari)** e aggiungi un destinatario.
2. Inserire le seguenti informazioni:
 - **Name (Nome):** Sirena stroboscopica
 - **Type (Tipo):** HTTP
 - **URL:** http://<IPaddress>/axis-cgi/siren_and_light.cgi
Sostituire <IPaddress> 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. Inserire le seguenti informazioni:
 - **Name (Nome):** Attivare la sirena di allarme con movimento
 - **Condition (Condizione):** Applications > Motion Guard: Profilo telecamera (Applicazioni > Motion Guard: Profilo telecamera)
 - **Action (Azione):** Notifications > Send notification through HTTP (Notifiche > Invia notifica 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 (Post)
 - **Body (Corpo):**

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

Assicurarsi di inserire le stesse informazioni in **"profile": <> ("profilo": <>)** come è stato creato nella sirena, in questo caso: **"Profilo sirena di allarme"**.

3. Fare clic su **Save (Salva)**.
4. Aggiungere un'altra regola con le seguenti informazioni:
 - **Name (Nome):** Disattivare la sirena di allarme con movimento
 - **Condition (Condizione):** Applications > Motion Guard: Profilo telecamera (Applicazioni > Motion Guard: Profilo telecamera)
 - Seleziona **Invert this condition (Inverti questa condizione)**.
 - **Action (Azione):** Notifications > Send notification through HTTP (Notifiche > Invia notifica 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 (Post)

AXIS D4100-E Network Strobe Siren

Configurare il dispositivo

- **Body (Corpo):**

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

Assicurarsi di inserire le stesse informazioni in **"profile": <> ("profilo": <>)** come è stato creato nella sirena, 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. Vai a **System > Events > Rules (Sistema > Eventi > Regole)** e aggiungi una regola.
2. Inserire le seguenti informazioni:
 - **Name (Nome):** Movimento rilevato
 - **Condition (Condizione):** Applications > Motion alarm (Applicazioni > Allarme di movimento)
 - **Action (Azione):** MQTT > Send MQTT publish message (MQTT > Invia messaggio di pubblicazione MQTT):
 - **Topic (Argomento):** Movimento
 - **Payload:** attivato
 - **QoS:** 0, 1 o 2
3. Fare clic su **Save (Salva)**.
4. Aggiungere un'altra regola con le seguenti informazioni:
 - **Name (Nome):** Nessun movimento
 - **Condition (Condizione):** Applications > Motion alarm (Applicazioni > Allarme di movimento)

AXIS D4100-E Network Strobe Siren

Configurare il dispositivo

- Seleziona **Invert this condition (Inverti questa condizione)**.
 - **Action (Azione): MQTT > Send MQTT publish message (MQTT > Invia messaggio di pubblicazione MQTT):**
 - **Topic (Argomento): Movimento**
 - **Payload: disattivato**
 - **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.

Inserire 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. Vai a **System > Events > Rules (Sistema > Eventi > Regole)** e aggiungi una regola.
2. Inserire le seguenti informazioni:
 - **Name (Nome): Movimento rilevato**
 - **Condition (Condizione): MQTT > Stateful (MQTT > Dotato di stato)**
 - **Subscription filter (Filtro sottoscrizione): Motion (In movimento)**
 - **Payload: attivato**
 - **Action (Azione): Light and siren > Run light and siren profile while the rule is active (Luce e sirena > Eseguire il profilo della luce e della sirena mentre la regola è attiva)**
 - **Profile (Profilo):** seleziona il profilo che vuoi sia attivo.
3. Fare clic su **Save (Salva)**.

AXIS D4100-E Network Strobe Siren

Ulteriori informazioni

Ulteriori informazioni

Session Initiation Protocol (SIP)

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

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

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

Peer-to-peer SIP (P2PSIP)

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

Private Branch Exchange (PBX)

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

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

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

NAT traversal

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

Nota

Il router deve supportare NAT traversal e UPnP®.

Ogni protocollo NAT trasversale può essere utilizzato separatamente o in combinazioni diverse a seconda dell'ambiente di rete.


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


AXIS D4100-E Network Strobe Siren


Interfaccia web


Interfaccia web


Per raggiungere l'interfaccia web del dispositivo, digita l'indirizzo IP del dispositivo in un browser web.




 Mostra o nascondi il menu principale.



 Accedere alle note di rilascio.


 Accedere alla guida dispositivo.

 Modificare la lingua.

 Imposta il tema chiaro o il tema scuro.

   Il menu contestuale contiene:

- Informazioni relative all'utente che ha eseguito l'accesso.
-  **Change account (Cambia account):** Disconnettersi dall'account corrente e accedere a un nuovo account.
-  **Log out (Disconnetti):** Disconnettersi dall'account corrente.

 Il menu contestuale contiene:

- **Analytics data (Dati di analisi):** acconsenti alla condivisione dei dati non personali del browser.
- **Feedback:** condividi qualsiasi feedback per contribuire a rendere migliore la tua esperienza utente.
- **Legal (Informazioni legali):** visualizzare informazioni sui cookie e le licenze.
- **About (Informazioni):** visualizza le informazioni relative al dispositivo, compresa la versione del firmware e il numero di serie.

Stato

Sicurezza

Mostra quali tipi di accesso al dispositivo sono attivati e quali protocolli di crittografia sono in uso. I consigli di impostazione sono basati sulla Guida alla protezione AXIS OS.

Hardening guide (Guida alla protezione): fare clic per andare su *Guida alla protezione di AXIS OS*, dove è possibile ottenere ulteriori informazioni sulla cybersecurity per i dispositivi Axis e le best practice.

Stato sincronizzazione ora

Mostra le informazioni di sincronizzazione NTP, inclusa l'eventuale sincronizzazione del dispositivo con un server NTP e il tempo che rimane fino alla sincronizzazione successiva.

NTP settings (Impostazioni NTP): visualizza e aggiorna le impostazioni NTP. Porta l'utente alla pagina **Date and time (Data e ora)** dove è possibile modificare le impostazioni NTP.

Informazioni dispositivo

Mostra le informazioni relative al dispositivo, compresa la versione del firmware e il numero di serie.

AXIS D4100-E Network Strobe Siren

Interfaccia web

Upgrade firmware (Aggiorna il firmware): aggiorna il firmware sul dispositivo. Porta l'utente sulla pagina Manutenzione dove è possibile aggiornare il firmware.

Connected clients (Client collegati)

Mostra il numero di connessioni e client connessi.

View details (Visualizza dettagli): Consente di visualizzare e aggiornare l'elenco dei client connessi. L'elenco mostra l'indirizzo IP, il protocollo, la porta e il PID/processo di ogni client.

Panoramica

Stato della luce

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

Stato della sirena

Consente di visualizzare le diverse attività della sirena in esecuzione sul dispositivo. Nell'elenco di stato della sirena possono essere eseguite fino a 10 attività contemporaneamente. Quando due o più attività vengono eseguite contemporaneamente, viene riprodotta l'attività con la priorità più alta. La riga verrà evidenziata in verde nell'elenco di stato.

Manutenzione

Maintenance mode (Modalità manutenzione): attivare questa opzione per mettere in pausa le ordinarie attività di luce e sirena nel corso della manutenzione del dispositivo. Quando si attiva la modalità di manutenzione, il dispositivo mostra un pattern di luce bianca pulsante in un triangolo e la sirena è silenziosa. Protegge l'installatore da danni udibili e dall'abbaglio di luce intensa.

La priorità della manutenzione è 11. Solo attività specifiche del sistema dalla priorità più elevata possono interrompere la modalità di manutenzione.

La modalità di manutenzione sopravvive al riavvio. Ad es., se imposti il tempo su 2 ore, spegni il dispositivo e lo riavvii un'ora dopo, il dispositivo rimarrà in modalità manutenzione per un'altra ora.

Quando esegui un ripristino delle impostazioni predefinite, il dispositivo torna alla modalità di manutenzione.

Duration (Durata)

- **Continuous (Continua):** Selezionare questa opzione per lasciare il dispositivo in modalità manutenzione fino alla disattivazione da parte dell'utente.
- **Time (Ora):** selezionare questa opzione per impostare il momento in cui la modalità di manutenzione sarà disattivata.

Controllo integrità

Check (Controlla): esegue un controllo di integrità del dispositivo per assicurarti che la luce e la sirena funzionino. Accende ogni sezione di luce una dopo l'altra e riproduce un segnale di verifica per controllare che il dispositivo funzioni correttamente. Se fallisce il controllo dell'integrità, accedere ai registri di sistema per maggiori informazioni.

Profili

Profili

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

AXIS D4100-E Network Strobe Siren

Interfaccia web





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

Nota

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

Non è possibile avere due profili con lo stesso nome.

- **Name (Nome):** inserire un nome per il profilo.
- **Description (Descrizione):** inserire una descrizione del profilo.
- **Light (Luce):** selezionare dal menu a discesa il tipo di **Pattern (schema)**, **Speed (velocità)**, **Intensity (intensità)** e **Color (colore)** della luce desiderato.
- **Siren (Sirena):** selezionare dal menu a discesa il tipo di **Pattern (schema)** e **Intensity (intensità)** della sirena desiderato.
-   Avviare o interrompere un'anteprima solo della luce o della sirena.
- **Duration (Durata):** impostare la durata delle attività.
 - **Continuous (Continua):** una volta avviata, viene eseguita fino all'arresto.
 - **Time (Ora):** impostare un tempo specificato per la durata dell'attività.
 - **Repetitions (Ripetizioni):** impostare quante volte l'attività deve ripetersi.
- **Priority (Priorità):** impostare la priorità di un'attività su un numero compreso tra 1 e 10. Le attività con numero di priorità al di sopra di 10 non si possono rimuovere dall'elenco di stato. Esistono tre attività con priorità superiore a 10; **Maintenance (Manutenzione)** (11), **Identify (Identifica)** (12) e **Health check (Controllo integrità)** (13).



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

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

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



Avvia profilo. Il profilo e le sue attività vengono visualizzati nell'elenco di stato.



Scegliere le seguenti operazioni per il profilo **Edit (Modifica)**, **Copy (Copia)**, **Export (Esporta)** o **Delete (Elimina)**.

App



Add app (Aggiungi app): Installa una nuova app.

Find more apps (Trova altre app): Trova altre app da installare. Verrà visualizzata una pagina panoramica delle app Axis.

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

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



Visualizzare gli aggiornamenti sulla sicurezza nelle app AXIS OS e ACAP.

Nota

Eseguire più app allo stesso tempo può avere un impatto sulle prestazioni del dispositivo.

Usa l'interruttore vicino al nome dell'app per l'avvio o l'arresto dell'app.

AXIS D4100-E Network Strobe Siren

Interfaccia web

Open (Apri): Accedi alle impostazioni dell'app. Le impostazioni disponibili dipendono dall'applicazione. Alcune applicazioni non sono dotate di impostazioni.



Il menu contestuale può contenere una o più delle seguenti opzioni:

- **Open-source license (Licenza open-source):** Visualizza le informazioni relative alle licenze open source usate nell'app.
- **App log (Registro app):** Visualizza un registro degli eventi relativi all'app. Il registro è utile quando si contatta l'assistenza.
- **Activate license with a key (Attiva licenza con una chiave):** nel caso l'app necessiti di una licenza, devi attivarla. Se il dispositivo non ha accesso a Internet, usa questa opzione. Se non si dispone di una chiave di licenza, andare a axis.com/products/analytics. Per generare una chiave di licenza, sono necessari il codice di licenza e il numero di serie del dispositivo Axis.
- **Activate license automatically (Attiva automaticamente la licenza):** Nel caso l'app necessiti di una licenza, devi attivarla. Se il dispositivo ha accesso a Internet, usa questa opzione. È necessario un codice di licenza per attivare la licenza.
- **Deactivate the license (Disattiva la licenza):** Disattivare la licenza per sostituirla con un'altra licenza, ad esempio quando si passa da una licenza di prova a una licenza completa. Se si disattiva la licenza, verrà eliminata anche dal dispositivo.
- **Settings (Impostazioni):** Configurare i parametri del dispositivo.
- **Delete (Elimina):** Cancella permanentemente l'app dal dispositivo. La licenza resta attiva a meno che non la disattivi prima.

Sistema

Ora e ubicazione

Data e ora

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

Nota

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

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

- **Automatic date and time (manual NTS KE servers) (Data e ora automatiche (server NTS KE manuali)):** eseguire la sincronizzazione con i server NTP key establishment sicuri connessi al server DHCP.
 - **Manual NTS KE servers (Server NTS KE manuali):** inserisci l'indirizzo IP di uno o due server NTP. Quando usi due server NTP, l'ora del dispositivo viene sincronizzata e adattata sulla base dell'input di entrambi.
- **Automatic date and time (NTP servers using DHCP) (Data e ora automatiche (server NTP tramite DHCP)):** esegui la sincronizzazione con i server NTP connessi al server DHCP.
 - **Fallback NTP servers (Server NTP di fallback):** inserisci l'indirizzo IP di uno o due server fallback.
- **Automatic date and time (manual NTP servers) (Data e ora automatiche (server NTP manuali)):** esegui la sincronizzazione con i server NTP scelti.
 - **Manual NTP servers (Server NTP manuali):** inserisci l'indirizzo IP di uno o due server NTP. Quando usi due server NTP, l'ora del dispositivo viene sincronizzata e adattata sulla base dell'input di entrambi.
- **Custom date and time (Data e ora personalizzate):** impostare manualmente la data e l'ora. Per recuperare una volta dal computer o dal dispositivo mobile le impostazioni di data e ora, fare clic su **Get from system (Ottieni dal sistema)**.

Time zone (Fuso orario): selezionare il fuso orario da utilizzare. L'ora legale e l'ora solare si alterneranno automaticamente.

Nota

Il sistema utilizza le impostazioni di data e ora in tutte le registrazioni, i registri e le impostazioni di sistema.

Ubicazione dei dispositivi

Inserire la posizione del dispositivo. Il sistema di gestione video può utilizzare queste informazioni per posizionare il dispositivo su una mappa.

AXIS D4100-E Network Strobe Siren

Interfaccia web

- **Latitude (Latitudine):** i valori positivi puntano a nord dell'equatore.
- **Longitude (Longitudine):** i valori positivi puntano a est del primo meridiano.
- **Heading (Intestazione):** Inserire la direzione della bussola verso cui è diretto il dispositivo. 0 punta a nord.
- **Label (Etichetta):** Inserire un nome descrittivo per il dispositivo.
- **Save (Salva):** Fare clic per salvare la posizione del dispositivo.

Rete

IPv4 (IPv4)

Assign IPv4 automatically (Assegna automaticamente IPv4): Selezionare questa opzione per consentire al router di rete di assegnare automaticamente un indirizzo IP al dispositivo. Si consiglia l'IP automatico (DHCP) per la maggior parte delle reti.

IP address (Indirizzo IP): Inserire un indirizzo IP univoco per il dispositivo. Gli indirizzi IP fissi possono essere assegnati casualmente in reti isolate, a condizione che ogni indirizzo sia univoco. Per evitare conflitti, si consiglia di contattare l'amministratore di rete prima di assegnare un indirizzo IP statico.

Subnet mask: Immetti la subnet mask per definire quali indirizzi sono all'interno della rete locale. Qualsiasi indirizzo fuori dalla rete locale passa attraverso il router.

Router: Inserire l'indirizzo IP del router predefinito (gateway) utilizzato per connettere i dispositivi collegati a reti diverse e a segmenti di rete.

Fallback to static IP address if DHCP isn't available (Fallback all'indirizzo IP fisso se DHCP non è disponibile): selezionalo se vuoi aggiungere un indirizzo IP statico da usare come fallback se DHCP non è disponibile e non è possibile assegnare in automatico un indirizzo IP.

Nota

Se DHCP non è disponibile e il dispositivo utilizza un fallback dell'indirizzo statico, l'indirizzo statico viene configurato con un ambito limitato.

IPv6

Assign IPv6 automatically (Assegna automaticamente IPv6): Selezionare questa opzione per attivare IPv6 e consentire al router di rete di assegnare automaticamente un indirizzo IP al dispositivo.

Hostname (Nome host)

Assign hostname automatically (Assegna automaticamente il nome host): Selezionare questa opzione per consentire al router di rete di assegnare automaticamente un nome host al dispositivo.

Hostname (Nome host): Immetti manualmente il nome host da usare come metodo alternativo per accedere al dispositivo. Il report del server e il registro di sistema utilizzano il nome host. I caratteri consentiti sono A-Z, a-z, 0-9 e -.

DNS servers (Server DNS)

Assign DNS automatically (Assegna automaticamente DNS): Selezionare questa opzione per consentire al server DHCP di assegnare automaticamente i domini di ricerca e gli indirizzi del server DNS al dispositivo. Si consiglia il DNS automatico (DHCP) per la maggior parte delle reti.

Search domains (Domini di ricerca): Quando si utilizza un nome host non completo, fare clic su **Add search domain (Aggiungi dominio di ricerca)** e inserire un dominio in cui cercare il nome host utilizzato dal dispositivo.

DNS servers (Server DNS): Fare clic su **Add DNS server (Aggiungi server DNS)** e inserire l'indirizzo IP del server DNS. Offre la conversione dei nomi host in indirizzi IP nella rete.

HTTP and HTTPS (HTTP e HTTPS)

AXIS D4100-E Network Strobe Siren

Interfaccia web

HTTPS è un protocollo che fornisce la crittografia per le richieste di pagine da parte di utenti e per le pagine restituite dal server web. Lo scambio di informazioni crittografate è regolato dall'utilizzo di un certificato HTTPS, che garantisce l'autenticità del server.

Per utilizzare HTTPS nel dispositivo, è necessario installare un certificato HTTPS. Andare a **System > Security (Sistema > Sicurezza)** per creare e installare i certificati.

Allow access through (Consenti l'accesso tramite): Selezionare questa opzione se a un utente è consentito connettersi al dispositivo tramite HTTP, HTTPS o entrambi i protocolli HTTP e HTTPS.

Nota

Se si visualizzano pagine web crittografate tramite HTTPS, è possibile che si verifichi un calo delle prestazioni, soprattutto quando si richiede una pagina per la prima volta.

HTTP port (Porta HTTP): inserire la porta HTTP da utilizzare. Il dispositivo consente l'utilizzo della porta 80 o di qualsiasi porta nell'intervallo 1024-65535. Se è stato eseguito l'accesso come amministratore, è possibile inserire qualsiasi porta nell'intervallo da 1 a 1023. Se si utilizza una porta in questo intervallo, viene visualizzato un avviso.

HTTPS port (Porta HTTPS): inserire la porta HTTPS da utilizzare. Il dispositivo consente l'utilizzo della porta 443 o di qualsiasi porta nell'intervallo 1024-65535. Se è stato eseguito l'accesso come amministratore, è possibile inserire qualsiasi porta nell'intervallo da 1 a 1023. Se si utilizza una porta in questo intervallo, viene visualizzato un avviso.

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

Protocolli di rilevamento della rete

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

Bonjour name (Nome Bonjour): Inserire un nome descrittivo che deve essere visibile sulla rete. Il nome predefinito è il nome del dispositivo e l'indirizzo MAC.

UPnP®: attivare per consentire il rilevamento automatico sulla rete.

UPnP name (Nome UPnP): Inserire un nome descrittivo che deve essere visibile sulla rete. Il nome predefinito è il nome del dispositivo e l'indirizzo MAC.

WS-Discovery: attivare per consentire il rilevamento automatico sulla rete.

One-click cloud connection (Connessione a cloud con un clic)

One-Click Cloud Connect (O3C), utilizzato in combinazione con un servizio O3C, offre un accesso Internet facile e sicuro a video in diretta e registrati, accessibili da qualsiasi ubicazione. Per ulteriori informazioni, consultare axis.com/end-to-end-solutions/hosted-services.

Allow O3C (Consenti O3C):

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

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

Host: Inserire l'indirizzo del server del proxy.

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

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

Authentication method (Metodo di autenticazione):

AXIS D4100-E Network Strobe Siren

Interfaccia web

- **Basic (Base):** questo metodo è lo schema di autenticazione maggiormente compatibile per HTTP. È meno sicuro del metodo **Digest** perché invia il nome utente e la password non crittografati al server.
- **Digest:** questo metodo è più sicuro perché la password viene sempre trasferita crittografata nella rete.
- **Auto (Automatica):** questa opzione consente al dispositivo Axis di selezionare il metodo di autenticazione a seconda dei metodi supportati, dando priorità a **Digest** rispetto al metodo **Basic (Base)**.

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

SNMP (SNMP)

SNMP (Simple Network Management Protocol) consente il monitoraggio e la gestione in remoto dei dispositivi di rete.

SNMP: Selezionare la versione di SNMP da utilizzare.

- **v1 and v2c (v1 e v2c):**
 - **Read community (Comunità con privilegi in lettura):** Inserire il nome della comunità che dispone solo dell'accesso in lettura a tutti gli oggetti SNMP supportati. Il valore predefinito è **public (pubblico)**.
 - **Write community (Comunità con privilegi in scrittura):** Specificare il nome della comunità che dispone di accesso in lettura o scrittura a tutti gli oggetti SNMP supportati (ad eccezione degli oggetti in sola lettura). Il valore predefinito è **write (scrittura)**.
 - **Activate traps (Attiva trap):** Attivare la segnalazione di trap. Il dispositivo utilizza i trap per inviare messaggi per eventi importanti o cambi di stato a un sistema di gestione. Nell'interfaccia web, è possibile impostare trap per SNMP v1 e v2c. I trap vengono disattivati automaticamente se si cambia in SNMP v3 o si disattiva SNMP. Se si utilizza SNMP v3, è possibile impostare i trap tramite l'applicazione di gestione SNMP v3.
 - **Trap address (Indirizzo trap):** inserire l'indirizzo IP o il nome host del server di gestione.
 - **Trap community (Comunità trap):** Inserire la comunità da utilizzare quando il dispositivo invia un messaggio trap al sistema di gestione.
 - **Traps (Trap):**
 - **Cold start (Avvio a freddo):** Invia un messaggio di trap all'avvio del dispositivo.
 - **Warm start (Avvio a caldo):** Invia un messaggio trap quando si modifica un'impostazione SNMP.
 - **Link up:** invia un messaggio trap quando un collegamento cambia dal basso verso l'alto.
 - **Authentication failed (Autenticazione non riuscita):** invia un messaggio trap quando un tentativo di autenticazione non riesce.

Nota

Tutti i trap Axis Video MIB vengono abilitati quando si attivano i trap SNMP v1 e v2c. Per ulteriori informazioni, consultare [AXIS OS Portal > SNMP \(Poortale sistema operativo AXIS > SNMP\)](#).

- **v3:** SNMP v3 è una versione più sicura che fornisce crittografia e password sicure. Per utilizzare SNMP v3, si consiglia di attivare HTTPS poiché la password verrà successivamente inviata via HTTPS. Ciò impedisce inoltre alle parti non autorizzate di accedere ai trap SNMP v1 e v2c non crittografati. Se si utilizza SNMP v3, è possibile impostare i trap tramite l'applicazione di gestione SNMP v3.
 - **Password for the account "initial" (Password per l'account "iniziale"):** Inserire la password SNMP per l'account denominato "iniziale". Sebbene la password possa essere inviata senza attivare HTTPS, non è consigliabile. La password SNMP v3 può essere impostata solo una volta e preferibilmente solo quando è attivato HTTPS. Una volta impostata la password, il relativo campo non verrà più visualizzato. Per impostare di nuovo la password, il dispositivo deve essere ripristinato alle impostazioni predefinite di fabbrica.

Sicurezza

Certificates (Certificati)

AXIS D4100-E Network Strobe Siren

Interfaccia web

I certificati sono utilizzati per autenticare i dispositivi in una rete. I tipi di certificati supportati da questo dispositivo sono due:

- **Client/server certificates (Certificati client/server)**
Un certificato client/server convalida l'identità del dispositivo e può essere autofirmato o emesso da un'autorità di certificazione (CA). Un certificato autofirmato offre una protezione limitata e può essere utilizzato prima che sia stato ottenuto un certificato emesso da un'autorità di certificazione.
- **Certificati CA**
È possibile utilizzare un certificato CA per autenticare un certificato peer, ad esempio per convalidare l'identità di un server di autenticazione nel caso in cui il dispositivo venga collegato a una rete protetta da IEEE 802.1X. Il dispositivo dispone di diversi certificati CA preinstallati.

Questi formati sono supportati:

- Formati dei certificati: .PEM, .CER e .PFX
- Formati delle chiavi private: PKCS#1 e PKCS#12

Importante


Se il dispositivo viene ripristinato alle impostazioni di fabbrica, tutti i certificati vengono eliminati. Qualsiasi certificato CA preinstallato viene reinstallato.



Filtra i certificati nell'elenco.



Add certificate (Aggiungi certificato): fare clic per aggiungere un certificato.

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



Il menu contestuale contiene:

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

Secure keystore (Archivio chiavi sicuro) ⓘ :

- **Secure element (CC EAL6+) (Elemento sicuro)**: Selezionare questa opzione per utilizzare un elemento sicuro per l'archivio chiavi sicuro.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Level 2)** Selezionare questa opzione per utilizzare TPM 2.0 per il keystore sicuro.

IEEE 802.1x

IEEE 802.1x è uno standard IEEE per il controllo di ammissione alla rete in base alla porta che fornisce un'autenticazione sicura di dispositivi di rete cablati e wireless. IEEE 802.1x è basato su EAP (Extensible Authentication Protocol).

Per accedere a una rete protetta da IEEE 802.1x, i dispositivi di rete devono autenticarsi. L'autenticazione viene eseguita da un server di autenticazione, generalmente un server RADIUS (ad esempio FreeRADIUS e Microsoft Internet Authentication Server).

Certificates (Certificati)

Se configurato senza un certificato CA, la convalida del certificato del server verrà disabilitata e il dispositivo cercherà in questo caso di autenticarsi a prescindere dalla rete a cui è connesso.

Nell'implementazione di Axis, quando si utilizza un certificato, il dispositivo e il server di autenticazione si autenticano con certificati digitali mediante EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).

AXIS D4100-E Network Strobe Siren

Interfaccia web

Per consentire al dispositivo di accedere a una rete protetta tramite certificati, è necessario installare un certificato client firmato sul dispositivo.

Client Certificate (Certificato client): Selezionare un certificato client per utilizzare IEEE 802.1x. Il server di autenticazione utilizza il certificato per convalidare l'identità del client.

CA Certificate (Certificato CA): Selezionare certificati CA per convalidare l'identità del server di autenticazione. Quando non ne viene selezionato nessun certificato, il dispositivo tenterà di autenticarsi a prescindere dalla rete a cui è connesso.

EAP identity (Identità EAP): Inserire l'identità utente associata al certificato del client.

EAPOL version (Versione EAPOL): selezionare la versione EAPOL utilizzata nello switch di rete.

Use IEEE 802.1x (Usa IEEE 802.1x): Selezionare questa opzione per utilizzare il protocollo IEEE 802.1x.

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

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

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

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

IP address filter (Filtro indirizzi IP)

Use filter (Usa filtro): Selezionare questa opzione per filtrare gli indirizzi IP a cui è consentito accedere al dispositivo.

Policy (Criteri) Scegliere se **Allow (Consentire)** o **Deny (Negare)** l'accesso per determinati indirizzi IP.

Addresses (Indirizzi): Inserire i numeri IP a cui è consentito o negato l'accesso al dispositivo. È inoltre possibile utilizzare il formato CIDR.

Custom-signed firmware certificate (Certificato firmware con firma personalizzata)

Serve un certificato firmware con firma personalizzata per l'installazione di firmware di prova o firmware personalizzato di altro tipo di Axis sul dispositivo. Il certificato verifica che il firmware è stato approvato sia dal proprietario del dispositivo che da Axis. È possibile eseguire il firmware unicamente su uno specifico dispositivo identificabile tramite il suo numero di serie univoco e l'ID del chip. Solo Axis può creare certificati firmware con firma personalizzata poiché Axis detiene la chiave per firmarli.

Install (Installa): Fare clic per eseguire l'installazione del certificato. Il certificato deve essere installato prima del firmware.

Account

Account

AXIS D4100-E Network Strobe Siren

Interfaccia web



Add account (Aggiungi account): Fare clic per aggiungere un nuovo account. Puoi aggiungere un massimo di 100 account.

Account: Inserire un nome account univoco.

New password (Nuova password): inserire una password per l'account. La lunghezza delle password deve essere compresa tra 1 e 64 caratteri. La password può contenere solo caratteri ASCII stampabili (codice da 32 a 126), quali lettere, numeri, segni di punteggiatura e alcuni simboli.

Repeat password (Ripeti password): inserire di nuovo la stessa password.

Privileges (Privilegi):

- **Administrator (Amministratore):** ha accesso completo a tutte le impostazioni. Gli amministratori possono anche aggiungere, aggiornare e rimuovere altri account.
- **Operator (Operatore):** ha accesso a tutte le impostazioni ad eccezione di:
 - Tutte le impostazioni **System (Sistema)**.
 - L'aggiunta di app.



Il menu contestuale contiene:

Update account (Aggiorna account): Modifica le proprietà dell'account.

Delete account (Elimina account): Elimina l'account. Non puoi cancellare l'account root.

Anonymous access (Accesso anonimo)

Allow anonymous viewing (Consenti visualizzazione anonima): attiva questa opzione per permettere a chiunque l'accesso al dispositivo in qualità di visualizzatore senza accedere con un account utente.

Allow anonymous PTZ operating (Consenti uso anonimo di PTZ): per permettere agli utenti anonimi di eseguire la panoramica, inclinazione e zoom dell'immagine, attiva questa opzione.

Account SSH



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

- **Restrict root access (Limita accesso root):** Attivare per limitare la funzionalità che richiede l'accesso root.
- **Abilita SSH:** Attivare per utilizzare il servizio SSH.

Account: Inserire un nome account univoco.

New password (Nuova password): inserire una password per l'account. La lunghezza delle password deve essere compresa tra 1 e 64 caratteri. La password può contenere solo caratteri ASCII stampabili (codice da 32 a 126), quali lettere, numeri, segni di punteggiatura e alcuni simboli.

Repeat password (Ripeti password): inserire di nuovo la stessa password.

Commento: Inserire un commenti (facoltativo).



Il menu contestuale contiene:

Update SSH account (Aggiorna account SSH): Modifica le proprietà dell'account.

Delete SSH account (Elimina account SSH): Elimina l'account. Non puoi cancellare l'account root.

OpenID Configuration (Configurazione OpenID):

Importante

inserire i valori appropriati per assicurare che sia possibile accedere nuovamente al dispositivo.

AXIS D4100-E Network Strobe Siren

Interfaccia web

Client ID (ID client): inserire il nome utente OpenID.

Outgoing Proxy (Proxy in uscita): inserire l'indirizzo proxy che può essere utilizzato dalla connessione OpenID.

Admin claim (Richiesta amministratore): inserire un valore per il ruolo di amministratore.

Provider URL (URL provider): inserire il collegamento web per l'autenticazione dell'endpoint API. Il formato deve essere `https://[inserire URL]/well-known/openid-configuration`

Operator claim (Richiesta operatore): inserire un valore per il ruolo di operatore.

Require claim (Richiesta obbligatoria): inserire i dati che devono essere contenuti nel token.

Viewer claim (Richiesta visualizzatore): inserire il valore per il ruolo visualizzatore.

Remote user (Utente remoto): inserire un valore per identificare gli utenti remoti. In questo modo sarà possibile visualizzare l'utente corrente nell'interfaccia web del dispositivo.

Scopes (Ambiti): Ambiti opzionali che potrebbero far parte del token.

Client secret (Segreto client): inserire la password OpenID

Save (Salva): Fare clic per salvare i valori OpenID.

Enable OpenID (Abilita OpenID): attivare per chiudere la connessione corrente e consentire l'autenticazione del dispositivo dall'URL del provider.

Eventi

Regole

Una regola consente di definire le condizioni che attivano il prodotto per l'esecuzione di un'azione. L'elenco mostra tutte le regole correntemente configurate nel dispositivo.

Nota

Puoi creare un massimo di 256 regole di azione.



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

Name (Nome): Inserire un nome per la regola.

Wait between actions (Attesa tra le azioni): Inserisci il periodo di tempo minimo (hh:mm:ss) che deve trascorrere tra le attivazioni della regola. Risulta utile se la regola si attiva, ad esempio, nelle condizioni della modalità diurna/notturna, per evitare che piccole variazioni di luce durante l'alba e il tramonto attivino ripetutamente la regola.

Condition (Condizione): Selezionare una condizione dall'elenco. Una condizione che deve essere soddisfatta affinché il dispositivo esegua un'azione. Se vengono definite più condizioni, devono essere tutte soddisfatte per attivare l'azione. Consultare *Introduzione alle regole per gli eventi* per ottenere informazioni riguardo a condizioni specifiche.

Use this condition as a trigger (Utilizza questa condizione come trigger): Selezionare questa opzione affinché questa prima condizione operi solo in qualità di trigger di avvio. Vuol dire che una volta attivata la regola, essa rimane attiva purché tutte le altre condizioni siano soddisfatte, a prescindere dallo stato della prima condizione. Se non selezioni questa opzione, la regola sarà semplicemente attiva quando tutte le condizioni sono soddisfatte.

Invert this condition (Inverti questa condizione): Selezionala se desideri che la condizione sia l'opposto della tua selezione.



Add a condition (Aggiungi una condizione): fare clic per l'aggiunta di un'ulteriore condizione.

AXIS D4100-E Network Strobe Siren

Interfaccia web

Action (Azione): seleziona un'azione dalla lista e inserisci le informazioni necessarie. Consultare *Introduzione alle regole per gli eventi* per ottenere informazioni riguardo ad azioni specifiche.

Destinatari

Hai la possibilità di configurare il dispositivo perché invii ai destinatari notifiche relative ad eventi o dei file. Nell'elenco vengono mostrati i destinatari configurati al momento nel dispositivo insieme alle varie informazioni sulla relativa configurazione.

Nota

È possibile creare fino a 20 destinatari.



Add a recipient (Aggiungi un destinatario): fare clic per aggiungere un destinatario.

Name (Nome): inserire un nome per il destinatario.

Type (Tipo): Seleziona dall'elenco:


- **FTP**
 - **Host:** Inserire l'indirizzo IP o il nome host del server. Se inserisci un nome host, accertati che sia specificato un server DNS in **System > Network > IPv4 and IPv6 (Sistema > Rete > IPv4 e IPv6)**.
 - **Port (Porta):** Inserire il numero di porta utilizzata dal server FTP. Il valore predefinito è 21.
 - **Folder (Cartella):** inserisci il percorso alla directory nella quale vuoi conservare i file. Se questa directory non esiste già sul server FTP, durante il caricamento dei file riceverai un messaggio di errore.
 - **Username (Nome utente):** inserire il nome utente per l'accesso.
 - **Password:** inserire la password per l'accesso.
 - **Use temporary file name (Usa nome file temporaneo):** seleziona questa opzione per il caricamento dei file con nomi file temporanei generati in automatico. Ai file sono assegnati i nomi desiderati quando viene completato il caricamento. Se il caricamento viene annullato/interrotto, non si avrà alcun file corrotto. Tuttavia, probabilmente avrai comunque i file temporanei. In questo modo è possibile sapere che tutti i file con il nome desiderato sono corretti.
 - **Use passive FTP (Usa FTP passivo):** in circostanze normali il dispositivo richiede semplicemente il server FTP di destinazione per aprire la connessione dati. Il dispositivo inizializza attivamente il comando FTP e le connessioni dati sul server di destinazione. Ciò è necessario generalmente se esiste un firewall tra il dispositivo e il server FTP di destinazione.
- **HTTP**
 - **URL:** Inserire l'indirizzo di rete sul server HTTP e lo script che gestirà la richiesta. Ad esempio, `http://192.168.254.10/cgi-bin/notify.cgi`.
 - **Username (Nome utente):** inserire il nome utente per l'accesso.
 - **Password:** inserire la password per l'accesso.
 - **Proxy:** Attiva e inserisci le informazioni necessarie se si deve superare un server proxy per eseguire la connessione al server HTTP.
- **HTTPS**
 - **URL:** Inserire l'indirizzo di rete sul server HTTPS e lo script che gestirà la richiesta. Ad esempio, `https://192.168.254.10/cgi-bin/notify.cgi`.
 - **Validate server certificate (Convalida certificato server):** Selezionare per convalidare il certificato creato dal server HTTPS.
 - **Username (Nome utente):** inserire il nome utente per l'accesso.
 - **Password:** inserire la password per l'accesso.
 - **Proxy:** Attiva e inserisci le informazioni necessarie se si deve superare un server proxy per eseguire la connessione al server HTTPS.
- **Network storage (Archiviazione di rete)**

Puoi aggiungere dispositivi di archiviazione di rete, ad esempio NAS (Network Attached Storage) e utilizzarli come destinatario per archiviare i file. I file vengono archiviati in formato Matroska (MKV).

 - **Host:** Inserire il nome host o l'indirizzo IP per il dispositivo di archiviazione di rete.
 - **Share (Condivisione):** Inserire il nome della condivisione nell'host.
 - **Folder (Cartella):** inserisci il percorso alla directory nella quale vuoi conservare i file.
 - **Username (Nome utente):** inserire il nome utente per l'accesso.
 - **Password:** inserire la password per l'accesso.
- **SFTP**

AXIS D4100-E Network Strobe Siren

Interfaccia web

- **Host:** Inserire l'indirizzo IP o il nome host del server. Se inserisci un nome host, accertati che sia specificato un server DNS in **System > Network > IPv4 and IPv6 (Sistema > Rete > IPv4 e IPv6)**.
 - **Port (Porta):** Inserire il numero della porta utilizzata dal server SFTP. Il valore predefinito è 22.
 - **Folder (Cartella):** inserisci il percorso alla directory nella quale vuoi conservare i file. Se questa directory non esiste già sul server SFTP, durante il caricamento dei file riceverai un messaggio di errore.
 - **Username (Nome utente):** inserire il nome utente per l'accesso.
 - **Password:** inserire la password per l'accesso.
 - **SSH host public key type (MD5) (Tipo di chiave pubblica host SSH (MD5)):** Immetti l'impronta digitale della chiave pubblica dell'host remoto (una stringa di 32 cifre esadecimali). Il client SFTP supporta i server SFTP mediante SSH-2 con tipi di chiavi host RSA, DSA, ECDSA e ED25519. RSA è il metodo preferito durante la negoziazione, seguito da ECDSA, ED25519 e DSA. Assicurarsi di inserire la chiave host MD5 esatta utilizzata dal server SFTP. Benché il dispositivo Axis supporti chiavi hash sia MD5 sia SHA-256, consigliamo l'uso di SHA-256 per una maggiore sicurezza rispetto a MD5. Per maggiori informazioni su come si configura un server SFTP con un dispositivo Axis, vai sul *Portale AXIS OS*.
 - **SSH host public key type (SHA256) (Tipo di chiave pubblica host SSH (SHA256)):** Immetti l'impronta digitale della chiave pubblica dell'host remoto (una stringa di 43 cifre con codifica Base64). Il client SFTP supporta i server SFTP mediante SSH-2 con tipi di chiavi host RSA, DSA, ECDSA e ED25519. RSA è il metodo preferito durante la negoziazione, seguito da ECDSA, ED25519 e DSA. Assicurarsi di inserire la chiave host MD5 esatta utilizzata dal server SFTP. Benché il dispositivo Axis supporti chiavi hash sia MD5 sia SHA-256, consigliamo l'uso di SHA-256 per una maggiore sicurezza rispetto a MD5. Per maggiori informazioni su come si configura un server SFTP con un dispositivo Axis, vai sul *Portale AXIS OS*.
 - **Use temporary file name (Usa nome file temporaneo):** seleziona questa opzione per il caricamento dei file con nomi file temporanei generati in automatico. Ai file sono assegnati i nomi desiderati quando viene completato il caricamento. Se il caricamento viene annullato o interrotto, non si avrà alcun file corrotto. Tuttavia, probabilmente avrai comunque i file temporanei. In questo modo è possibile sapere che tutti i file con il nome desiderato sono corretti.
- 
- **SIP or VMS (SIP o VMS)** :
 - SIP: selezionare per eseguire una chiamata SIP.
 - VMS: selezionare per eseguire una chiamata VMS.
 - **From SIP account (Dall'account SIP):** Selezionare dall'elenco.
 - **To SIP address (All'indirizzo SIP):** Immetti l'indirizzo SIP.
 - **Test (Verifica):** fare clic per verificare che le impostazioni di chiamata funzionino.
 - **Email (E-mail)**
 - **Send email to (Invia e-mail a):** Inserire l'indirizzo e-mail a cui inviare i messaggi e-mail. Per inserire più indirizzi, separarli utilizzando le virgole.
 - **Send email from (Invia e-mail da):** inserire l'indirizzo e-mail del server mittente.
 - **Username (Nome utente):** Inserire il nome utente per il server mail. Lasciare vuoto questo campo se il server mail non necessita di autenticazione.
 - **Password:** Inserire la password per il server mail. Lasciare vuoto questo campo se il server mail non necessita di autenticazione.
 - **Email server (SMTP) – Server e-mail (SMTP):** inserire il nome del server SMTP, ad esempio, smtp.gmail.com, smtp.mail.yahoo.com.
 - **Port (Porta):** inserire il numero della porta per il server SMTP, utilizzando i valori nell'intervallo da 0 a 65535. Il valore predefinito è 587.
 - **Encryption (Crittografia):** Per usare la crittografia, seleziona SSL o TLS.
 - **Validate server certificate (Convalida certificato server):** Se usi la crittografia, seleziona questa opzione per convalidare l'identità del dispositivo. Il certificato può essere autofirmato o emesso da un'autorità di certificazione (CA).
 - **POP authentication (Autenticazione POP):** Attiva per inserire il nome del server POP, ad esempio pop.gmail.com.

Nota

Alcuni provider e-mail hanno filtri di sicurezza che impediscono agli utenti di ricevere o visualizzare allegati di grandi dimensioni, ad esempio e-mail pianificate e simili. Controllare i criteri di sicurezza del provider e-mail per evitare che l'account e-mail venga bloccato o perda i messaggi e-mail attendibili.

- **TCP**
 - **Host:** Inserire l'indirizzo IP o il nome host del server. Se inserisci un nome host, accertati che sia specificato un server DNS in **System > Network > IPv4 and IPv6 (Sistema > Rete > IPv4 e IPv6)**.
 - **Porta:** Inserire il numero della porta utilizzata per l'accesso al server.

Test (Verifica): Fare clic per testare l'impostazione.

AXIS D4100-E Network Strobe Siren

Interfaccia web



Il menu contestuale contiene:

View recipient (Visualizza destinatario): fare clic per visualizzare tutti i dettagli del destinatario.

Copy recipient (Copia destinatario): Fare clic per copiare un destinatario. Quando copi, puoi modificare il nuovo destinatario.

Delete recipient (Elimina destinatario): Fare clic per l'eliminazione permanente del destinatario.

Pianificazioni

Le pianificazioni e gli impulsi possono essere utilizzati come condizioni nelle regole. Nell'elenco vengono mostrati le pianificazioni e gli impulsi configurati al momento nel dispositivo, insieme alle varie informazioni sulla relativa configurazione.



Add schedule (Aggiungi pianificazione): Fare clic per la creazione di una pianificazione o un impulso.

Trigger manuali

È possibile utilizzare l'attivazione manuale per attivare manualmente una regola. L'attivazione manuale può, ad esempio, essere per convalidare le azioni durante l'installazione e la configurazione del dispositivo.

MQTT

MQTT (Message Queuing Telemetry Transport) è un protocollo di messaggistica standard per l'Internet of Things (IoT). È stato progettato per un'integrazione IoT semplificata ed è utilizzato in una vasta gamma di settori per collegare dispositivi remoti con un'impronta di codice ridotta e una larghezza di banda di rete minima. Il client MQTT nel firmware del dispositivo Axis può semplificare l'integrazione di dati ed eventi prodotti nel dispositivo con sistemi che non sono software per la gestione video (VMS).

Configurare il dispositivo come client MQTT. La comunicazione MQTT si basa su due entità, i client e il broker. I client possono inviare e ricevere messaggi. Il broker è responsabile del routing dei messaggi tra i client.

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

ALPN (RETE ALPN)

ALPN è un'estensione TLS/SSL che consente la selezione di un protocollo applicativo durante la fase di handshake della connessione tra client e server. Viene utilizzato per abilitare il traffico MQTT sulla stessa porta utilizzata per altri protocolli, ad esempio HTTP. In alcuni casi, potrebbe non esserci una porta dedicata aperta per la comunicazione MQTT. Una soluzione in tali casi consiste nell'utilizzare ALPN per trattare l'uso di MQTT come protocollo applicativo su una porta standard, consentito dai firewall.

MQTT client (Client MQTT)

Connect (Connetti): Attivare o disattivare il client MQTT.

Status (Stato): Visualizza lo stato corrente del client MQTT.

Broker

Host: inserire il nome host o l'indirizzo IP del server MQTT.

Protocol (Protocollo): Selezionare il protocollo da utilizzare.

Port (Porta): Inserire il numero di porta.

- 1883 è il valore predefinito per MQTT su TCP
- 8883 è il valore predefinito per MQTT su SSL
- 80 è il valore predefinito per MQTT su WebSocket

AXIS D4100-E Network Strobe Siren

Interfaccia web

- 443 è il valore predefinito per MQTT su WebSocket Secure

ALPN protocol (Protocollo ALPN): Inserire il nome del protocollo ALPN fornito dal provider MQTT. Ciò è applicabile solo con MQTT over SSL e MQTT over WebSocket Secure.

Username (Nome utente): inserire il nome utente che il client utilizzerà per accedere al server.

Password: inserire una password per il nome utente.

Client ID (ID client): Inserire un ID client. L'identificatore del client viene inviato al server al momento della connessione del client.

Clean session (Sessione pulita): Controlla il comportamento al momento della connessione e della disconnessione. Se selezionate, le informazioni sullo stato vengono ignorate al momento della connessione e della disconnessione.

Keep alive interval (Intervallo keep alive): Consente al client di rilevare quando il server non è più disponibile senza dover attendere il lungo tempo di timeout TCP/IP.

Timeout: L'intervallo di tempo in secondi per consentire il completamento di una connessione. Valore predefinito: 60

Device topic prefix (Prefisso argomento dispositivo): utilizzato nei valori predefiniti per l'argomento nel messaggio di connessione e nel messaggio Ultime volontà e testamento nella scheda MQTT client (Client MQTT) e nelle condizioni di pubblicazione nella scheda MQTT publication (Pubblicazione MQTT).

Reconnect automatically (Riconnetti automaticamente): specifica se il client deve riconnettersi automaticamente dopo una disconnessione.

Connect message (Messaggio connessione)

Specifica se un messaggio deve essere inviato quando viene stabilita una connessione.

Send message (Invia messaggio): Attivare per inviare messaggi.

Use default (Usa predefinito): Disattivare per inserire un messaggio predefinito.

Topic (Argomento): Inserire l'argomento per il messaggio predefinito.

Payload: Inserire il contenuto per il messaggio predefinito.

Retain (Conserva): Selezionare questa opzione per mantenere lo stato del client su questo Topic (Argomento)

QoS: Cambiare il livello QoS per il flusso di pacchetti.

Last Will and Testament message (Messaggio di ultime volontà e testamento)

Ultime volontà e testamento consente a un client di fornire un testamento insieme alle proprie credenziali quando si collega al broker. Se il client si disconnette in modo anomalo in un secondo momento (forse perché la sua sorgente di alimentazione non funziona), può lasciare che il broker recapiti un messaggio ad altri client. Questo messaggio Ultime volontà e testamento ha lo stesso formato di un messaggio ordinario e viene instradato tramite la stessa meccanica.

Send message (Invia messaggio): Attivare per inviare messaggi.

Use default (Usa predefinito): Disattivare per inserire un messaggio predefinito.

Topic (Argomento): Inserire l'argomento per il messaggio predefinito.

Payload: Inserire il contenuto per il messaggio predefinito.

Retain (Conserva): Selezionare questa opzione per mantenere lo stato del client su questo Topic (Argomento)

QoS: Cambiare il livello QoS per il flusso di pacchetti.

MQTT publication (Pubblicazione MQTT)

AXIS D4100-E Network Strobe Siren

Interfaccia web

Use default topic prefix (Usa prefisso di argomento predefinito): Selezionare questa opzione per usare il prefisso dell'argomento predefinito, definito nel prefisso argomento dispositivo nella scheda MQTT client (Client MQTT).

Include topic name (Includi nome argomento): selezionare questa opzione per l'inclusione dell'argomento che illustra la condizione nell'argomento MQTT.

Include topic namespaces (Includi spazi dei nomi degli argomenti): Selezionare questa opzione per includere gli spazi dei nomi degli argomenti di ONVIF nell'argomento MQTT.

Include serial number (Includi numero di serie): selezionare questa opzione per comprendere il numero di serie del dispositivo nel payload MQTT.

+ Add condition (Aggiungi condizione): fare clic sull'opzione per aggiungere una condizione.

Retain (Conserva): definire quali messaggi MQTT sono inviati come conservati.

- **None (Nessuno):** inviare tutti i messaggi come non conservati.
- **Property (Proprietà):** inviare solo messaggi con stato conservati.
- **All (Tutto):** Invia messaggi sia con che senza stato come conservati.

QoS: Seleziona il livello desiderato per la pubblicazione MQTT.

MQTT subscriptions (Sottoscrizioni MQTT)

+ Add subscription (Aggiungi sottoscrizione): Fai clic per aggiungere una nuova sottoscrizione MQTT.

Subscription filter (Filtro sottoscrizione): Inserisci l'argomento MQTT per il quale desideri eseguire la sottoscrizione.

Use device topic prefix (Usa prefisso argomento dispositivo): Aggiungi il filtro sottoscrizione come prefisso all'argomento MQTT.

Subscription type (Tipo di sottoscrizione):

- **Stateless (Privo di stato):** Seleziona per convertire i messaggi MQTT in messaggi senza stato.
- **Stateful (Dotato di stato):** Seleziona per convertire i messaggi MQTT in una condizione. Il payload è usato come stato.

QoS: Seleziona il livello desiderato per la sottoscrizione MQTT.

MQTT overlays (Sovrapposizioni testo MQTT)

Nota

Connetti a un broker MQTT prima dell'aggiunta dei campi di modifica di sovrapposizione testo MQTT.

+ Add overlay modifier (Aggiungi campo di modifica sovrapposizione testo): Fai clic per l'aggiunta di un nuovo campo di modifica di sovrapposizione testo.

Topic filter (Filtro argomenti): Aggiungi l'argomento MQTT contenente i dati che vuoi mostrare nella sovrapposizione testo.

Data field (Campo dati): Specifica la chiave per il payload del messaggio che vuoi visualizzare nella sovrapposizione testo, purché il messaggio sia in formato JSON.

Modifier (Campo di modifica): Usa il campo di modifica risultante quando crei la sovrapposizione testo.

- I campi di modifica che cominciano con **#XMP** mostrano tutti i dati ricevuti dall'argomento.
- I campi di modifica che cominciano con **#XMD** mostrano i dati specificati nel campo dati.

SIP

Settings (Impostazioni)

AXIS D4100-E Network Strobe Siren

Interfaccia web

Il protocollo SIP (Session Initiation Protocol) viene utilizzato per le sessioni di comunicazione interattiva tra gli utenti. Le sessioni possono includere audio e video.

Enable SIP (Abilita SIP): Seleziona questa opzione per rendere possibile l'avvio e la ricezione di chiamate SIP.

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

Call handling (Gestione chiamate)

- **Calling timeout (Timeout chiamata):** impostare la durata massima di un tentativo di chiamata in mancanza di risposta.
- **Incoming call duration (Durata chiamata in entrata):** impostare la durata massima di una chiamata in entrata (massimo 10 minuti).
- **End calls after (Termina chiamate dopo):** impostare la durata massima di una chiamata (massimo 60 minuti). Seleziona **Infinite call duration (Durata infinita chiamata)** se non vuoi porre un limite alla lunghezza di una chiamata.

Ports (Porte)

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

- **SIP port (Porta SIP):** porta di rete utilizzata per la comunicazione SIP. Il traffico di segnalazione tramite la porta non viene crittografato. Il numero di porta predefinito è 5060. Se necessario, inserire un numero di porta diverso.
- **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 diverso.
- **Porta di avvio RTP:** porta di rete utilizzata per il primo streaming multimediale RTP in una chiamata SIP. Il numero di porta di avvio predefinito è 4.000. Alcuni firewall bloccano il traffico RTP su determinati numeri di porta.

NAT traversal (Attraversamento NAT)

Utilizzare l'attraversamento NAT (Network Address Translation) quando il dispositivo si trova in una rete privata (LAN) e si desidera renderlo disponibile al di fuori di tale rete.

Nota

Affinché funzioni, l'attraversamento NAT deve essere supportato dal router. Il router inoltre deve supportare UPnP®.

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

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

Audio (Audio)

- **Audio codec priority (Priorità codec audio):** Selezionare almeno un codec audio con la qualità audio desiderata per le chiamate SIP. Trascina e rilascia per modificare la priorità.

Nota

I codec selezionati devono corrispondere al codec del destinatario della chiamata, dal momento che il codec del destinatario è determinante quando si effettua una chiamata.

- **Audio direction (Direzione dell'audio):** Seleziona le direzioni audio consentite.

Additional (Aggiuntivo)

- **UDP-to-TCP switching (Passaggio da UDP a TCP):** Seleziona per consentire alle chiamate di scambiare temporaneamente i protocolli di trasporto da UDP (User Datagram Protocol) a TCP (Transmission Control Protocol). La ragione per il passaggio è evitare la frammentazione e il passaggio può essere eseguito se una richiesta rientra nei 200 byte del parametro MTU (Maximum Transmission Unit) o supera i 1.300 byte.

AXIS D4100-E Network Strobe Siren

Interfaccia web

- **Allow via rewrite (Consenti tramite riscrittura):** Seleziona per inviare l'indirizzo IP locale e non l'indirizzo IP pubblico del router.
- **Allow contact rewrite (Consenti riscrittura contatto):** Seleziona per inviare l'indirizzo IP locale e non l'indirizzo IP pubblico del router.
- **Register with server every (Registra con il server ogni):** Consente di impostare la frequenza con cui si desidera che il dispositivo registri con il server SIP per gli account SIP esistenti.
- **DTMF payload type (Tipo payload DTMF):** Modifica il tipo di payload predefinito per DTMF.

Account

Tutti gli account SIP correnti sono elencati sotto **SIP accounts (Account SIP)**. Per gli account registrati, il cerchio colorato consente di conoscerne lo stato.

- L'account viene registrato con successo con il server SIP.
- Problema con l'account. Tra le possibili cause possono esserci la mancata autorizzazione, errate credenziali dell'account o impossibilità per il server SIP di trovare l'account.

L'account **peer to peer (default) (Peer-to-peer (predefinito))** è un account creato automaticamente. È possibile eliminarlo se si crea almeno un altro account e lo si imposta come predefinito. Quando si effettua una chiamata API (interfaccia per la programmazione di applicazioni) VAPIX® senza specificare da quale account SIP effettuare la chiamata viene sempre utilizzato l'account predefinito.





Add account (Aggiungi account): Fare clic per creare un nuovo account SIP.


- **Active (Attivo):** selezionare questa opzione per poter utilizzare l'account.
- **Make default (Imposta come predefinito):** selezionare questa opzione per impostare l'account in questione come predefinito. Deve essere presente un account predefinito e può essercene uno solo.
- **Answer automatically (Risposta automatica):** Selezionare questa opzione per rispondere automaticamente a una chiamata in entrata.
- **Prioritize IPv6 over IPv4 (Dai priorità a IPv6 rispetto a IPv4)** ⓘ : selezionare questa opzione per dare la priorità agli indirizzi IPv6 rispetto agli indirizzi IPv4. Ciò è utile quando ci si connette ad account peer-to-peer o a nomi di dominio che vengono risolti in indirizzi IPv4 e IPv6. È possibile dare la priorità agli indirizzi IPv6 solo per i nomi di dominio mappati su indirizzi IPv6.
- **Name (Nome):** inserire un nome descrittivo. Può, ad esempio, essere il nome e il cognome, un ruolo o una posizione. Il nome non è univoco.
- **User ID (ID utente):** inserire il numero di telefono o estensione univoci assegnati al dispositivo.
- **Peer-to-peer:** utilizzare questo account per le chiamate dirette a un altro dispositivo SIP nella rete locale.
- **Registrato:** utilizzare questo account per le chiamate a dispositivi SIP al di fuori della rete locale, tramite un server SIP.
- **Domain (Dominio):** Se disponibile, immetti il nome dominio pubblico. Verrà visualizzato come parte dell'indirizzo SIP durante la chiamata ad altri account.
- **Password:** inserire la password associata all'account SIP per l'autenticazione al server SIP.
- **Authentication ID (ID di autenticazione):** inserire l'ID autenticazione utilizzato per l'autenticazione al server SIP. Se è lo stesso dell'ID utente, non è necessario inserire l'ID autenticazione.
- **Caller ID (ID chiamante):** nome indicato al destinatario delle chiamate dal dispositivo.
- **Registrar:** inserire l'indirizzo IP per l'account registrar.
- **Transport mode (Modalità di trasporto):** Selezionare la modalità di trasporto SIP per l'account: UDP, TCP o TLS.
- **TLS version (Versione TLS) (solo con modalità di trasporto TLS):** Selezionare la versione di TLS da utilizzare. Le versioni v1.2 e v1.3 sono le più sicure. **Automatic (Automatica)** seleziona la versione più sicura che il sistema può gestire.
- **Media encryption (Codifica media) (solo con modalità di trasporto TLS):** selezionare il tipo di codifica dei supporti (audio e video) nelle chiamate SIP.
- **Certificate (Certificato) (solo con modalità di trasporto TLS):** selezionare un certificato.
- **Verify server certificate (Verifica certificato server) (solo con modalità di trasporto TLS):** selezionare questa opzione per verificare il certificato server.
- **Secondary SIP server (Server SIP secondario):** attivare se vuoi che il dispositivo tenti di registrare su un server SIP secondario in caso di errore di registrazione sul server SIP principale.
- **SIP secure (SIP sicuro):** selezionare questa opzione per utilizzare SIPS (Secure Session Initiation Protocol). SIPS utilizza la modalità di trasporto TLS per codificare il traffico.

AXIS D4100-E Network Strobe Siren

Interfaccia web

- Proxies (Proxy)
 -  Proxy: fare clic sull'opzione per aggiungere un proxy.
 - Prioritize (Dai priorità): se sono stati aggiunti due o più proxy, fare clic per assegnare la relativa priorità.
 - Server address (Indirizzo server): inserire l'indirizzo IP del server proxy SIP.
 - Username (Nome utente): se richiesto, inserire il nome utente per il server proxy SIP.
 - Password: se necessario, inserire la password per il server proxy SIP.
- Video 
 - View area (Area di visione): selezionare l'area di visione da utilizzare per le chiamate video. Se si seleziona Nessuna, viene utilizzata la visualizzazione nativa.
 - Resolution (Risoluzione): selezionare la risoluzione da utilizzare per le chiamate video. La risoluzione influisce sulla larghezza di banda necessaria.
 - Frame rate (Velocità in fotogrammi): selezionare il numero di fotogrammi al secondo per le chiamate video. La velocità in fotogrammi influisce sulla larghezza di banda necessaria.
 - H.264 profile (Profilo H.264): selezionare il profilo da utilizzare per le chiamate video.

DTMF (DTMF)

 Add sequence (Aggiungi sequenza): Fare clic per creare una nuova sequenza DTMF (Dual-Tone Multifrequency). Per creare una regola che viene attivata dal tono di tocco, andare a Events > Rules (Eventi > Regole).

Sequence (Sequenza): inserire i caratteri per attivare la regola. I caratteri consentiti sono: 0-9, A-D, # e *.

Description (Descrizione): inserire una descrizione dell'azione da attivare attraverso la sequenza.

Accounts (Account): Selezionare gli account che utilizzeranno la sequenza DTMF. Se si sceglie peer-to-peer, tutti gli account peer-to-peer condivideranno la stessa sequenza DTMF.

Protocols (Protocolli):


Selezionare i protocolli da utilizzare per ogni account. Tutti gli account peer-to-peer condividono le stesse impostazioni di protocollo.

Use RTP (RFC2833) (Usa RTP (RFC2833)): attivare questa opzione per consentire la segnalazione DTMF (Dual-Tone Multi-Frequency), altri segnali di suono ed eventi di sistemi di telefonia in pacchetti RTP.

Use SIP INFO (RFC2976) (Usa SIP INFO (RFC2976)): attivare questa opzione per includere il metodo INFO nel protocollo SIP. Il metodo INFO consente di aggiungere informazioni opzionali al livello applicativo, in genere correlate alla sessione.

Chiamata di prova

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

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

Elenco di accesso

AXIS D4100-E Network Strobe Siren

Interfaccia web

Use access list (Usa elenco di accesso): attivare per limitare le persone che possono effettuare chiamate al dispositivo.

Policy (Criteri):

- **Allow (Consenti):** selezionare questa opzione per consentire le chiamate in entrata solo dalle origini incluse nell'elenco di accesso.
- **Block (Blocca):** selezionare questa opzione per bloccare le chiamate in entrata dalle origini incluse nell'elenco di accesso.



Add source (Aggiungi origine): fare clic per creare una nuova voce nell'elenco di accesso.

SIP source (Sorgente SIP): inserire l'ID del chiamante o l'indirizzo del server SIP della sorgente.

Accessori



I/O ports (Porte I/O)



Utilizzare l'input digitale per collegare i dispositivi esterni che possono passare da un circuito aperto a un circuito chiuso, ad esempio i sensori PIR, i contatti porta o finestra e i rivelatori di rottura del vetro.

Utilizzare l'uscita digitale per collegare dispositivi esterni come relè e LED. È possibile attivare i dispositivi collegati tramite l'API VAPIX® o l'interfaccia web.

Port (Porta)

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


Direction (Direzione):  indica che la porta è una porta di input.  indica che si tratta di una porta di output. Se la porta è configurabile, è possibile fare clic sulle icone per passare dall'input all'output.

Normal state (Stato normale): Fare clic su  per il circuito aperto e su  per il circuito chiuso.

Current state (Stato corrente): Indica lo stato attuale della porta. L'input e l'output vengono attivati quando lo stato corrente è diverso dallo stato normale. Un input sul dispositivo ha un circuito aperto se disconnesso o in caso di tensione superiore a 1 V CC.

Nota

Durante il riavvio, il circuito di output è aperto. Al completamento del riavvio, il circuito torna alla posizione normale. Se si modificano le impostazioni in questa pagina, i circuiti di output tornano alle relative posizioni normali, indipendentemente dai trigger attivi.

Supervised (Supervisionato)  : Attivare per rendere possibile il rilevamento e l'attivazione di azioni se qualcuno manomette la connessione ai dispositivi I/O digitali. Oltre a rilevare se un ingresso è aperto o chiuso, è anche possibile rilevare se qualcuno l'ha manomesso (ovvero se è stato tagliato o corto). Per supervisionare la connessione è necessario un ulteriore hardware (resistori terminali) nel loop I/O esterno.

Registri

Report e registri

AXIS D4100-E Network Strobe Siren

Interfaccia web

Reports (Report)

- **View the device server report (Visualizza il report del server del dispositivo):** Visualizzare informazioni sullo stato del dispositivo in una finestra pop-up. Il registro degli accessi viene automaticamente incluso nel report del server.
- **Download the device server report (Scarica il report del server del dispositivo):** Crea un file .zip che contiene un file di testo del report del server completo in formato UTF-8 e un'istantanea dell'immagine corrente della visualizzazione in diretta. Includere sempre il file .zip del report del server quando si contatta l'assistenza.
- **Download the crash report (Scarica il report dell'arresto anomalo):** Scaricare un archivio con le informazioni dettagliate sullo stato del server. Il report di arresto anomalo contiene le informazioni presenti nel report del server e le informazioni dettagliate sul debug. Questo report potrebbe contenere informazioni riservate, ad esempio l'analisi della rete. Possono volerci alcuni minuti per generare il report.

Logs (Registri)

- **View the system log (Visualizza il registro di sistema):** Fare clic per visualizzare le informazioni sugli eventi di sistema come l'avvio del dispositivo, gli avvisi e i messaggi critici.
- **View the access log (Visualizza il registro degli accessi):** Fare clic per mostrare tutti i tentativi non riusciti di accedere al dispositivo, ad esempio quando si utilizza una password di accesso errata.

Network trace (Analisi della rete)

Importante

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

Un file di analisi della rete può facilitare la risoluzione dei problemi registrando l'attività sulla rete.

Trace time (Tempo di analisi): Selezionare la durata dell'analisi in secondi o minuti e fare clic su **Download**.

Registro di sistema remoto

Syslog è uno standard per la registrazione dei messaggi. Consente di separare il software che genera messaggi, il sistema che li archivia e il software che li riporta e li analizza. Ogni messaggio è contrassegnato con un codice struttura che indica il tipo di software che genera il messaggio. Inoltre viene assegnato un livello di gravità a tutti i messaggi.



Server: Fare clic per aggiungere un nuovo server.

Host: inserire il nome host o l'indirizzo IP del server proxy.

Format (Formatta): selezionare il formato del messaggio syslog da utilizzare.

- Axis
- RFC 3164
- RFC 5424

Protocol (Protocollo): selezionare il protocollo e la porta da utilizzare:

- UDP (la porta predefinita è 514)
- TCP (la porta predefinita è 601)
- TLS (la porta predefinita è 6514)

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

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

Configurazione normale

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

AXIS D4100-E Network Strobe Siren

Interfaccia web

Manutenzione

Restart (Riavvia): Riavviare il dispositivo. Non avrà effetti su nessuna delle impostazioni correnti. Le applicazioni in esecuzione verranno riavviate automaticamente.

Restore (Ripristina): Riporta la *maggior parte* delle impostazioni ai valori predefiniti di fabbrica. In seguito dovrai riconfigurare il dispositivo e le app, reinstallare tutte le app non preinstallate e ricreare eventuali eventi e preset PTZ.

Importante

Dopo il ripristino, le uniche impostazioni salvate sono:

- Protocollo di avvio (DHCP o statico)
- Indirizzo IP statico
- Router predefinito
- Subnet mask
- Impostazioni 802.1X
- Impostazioni O3C

Factory default (Valori predefiniti di fabbrica): Riporta *tutte* le impostazioni ai valori predefiniti di fabbrica. Dopo, per rendere accessibile il dispositivo, devi reimpostare l'indirizzo IP.

Nota

Tutti i firmware per dispositivi Axis sono firmati digitalmente per assicurare di installare solo firmware verificato sul dispositivo. Ciò aumenta ulteriormente il livello di sicurezza informatica minimo globale dei dispositivi Axis. Consultare il white paper "Firmware firmato, avvio sicuro e sicurezza delle chiavi private" presso l'indirizzo axis.com per maggiori informazioni.

Firmware upgrade (Aggiornamento del firmware): aggiorna a una versione nuova del firmware. Le nuove versioni di firmware possono contenere funzionalità migliorate, correzioni di bug e funzionalità completamente nuove. Si consiglia di utilizzare sempre l'ultima versione. Per scaricare l'ultima versione, andare a axis.com/support.

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

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

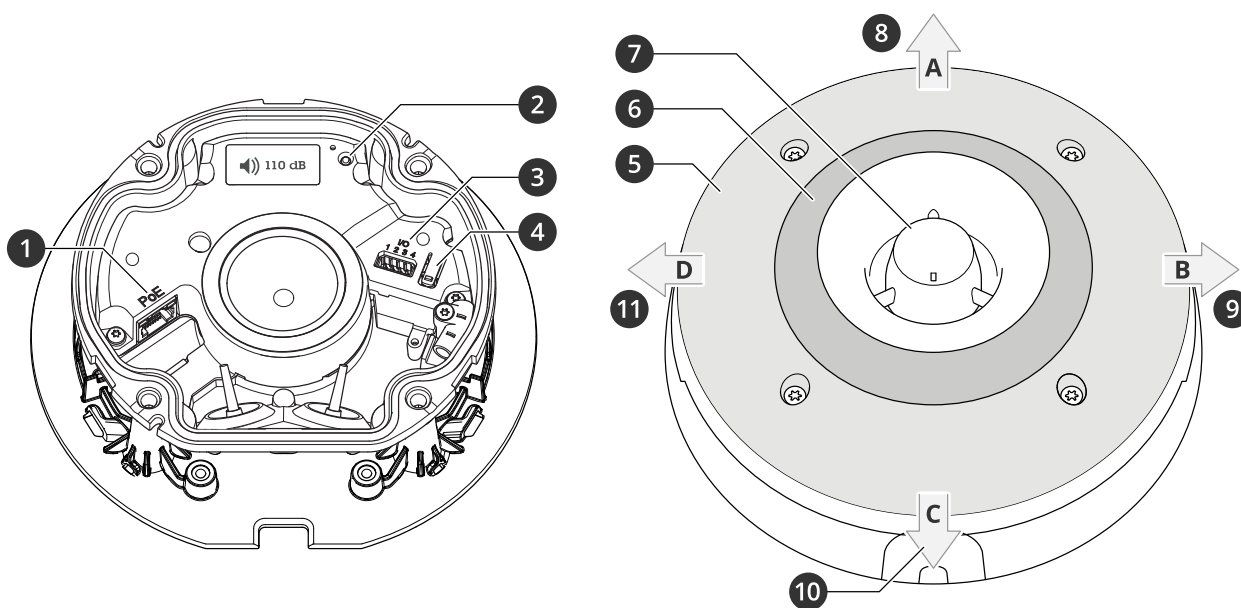
Firmware rollback (Rollback del firmware): eseguire il ripristino alla versione del firmware installata precedentemente.

AXIS D4100-E Network Strobe Siren

Specifiche

Specifiche

Panoramica del dispositivo



- 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 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	Indicazione
Verde	Una luce verde fissa per 10 secondi indica il normale funzionamento una volta completato l'avvio.
Giallo	Fisso all'avvio, durante il ripristino ai valori predefiniti di fabbrica o al ripristino delle impostazioni.

Pulsanti

Pulsante di comando

Il pulsante di comando viene utilizzato per:

- Ripristino del dispositivo alle impostazioni predefinite di fabbrica. Consultare *Ripristino delle impostazioni predefinite di fabbrica alla pagina 44*.

AXIS D4100-E Network Strobe Siren

Specifiche

- Connessione a servizio one-click cloud connection (O3C) su Internet. Per il collegamento, tenere premuto il tasto per circa 3 secondi finché il LED di stato non lampeggia in verde.

Connettori

Connettore di rete

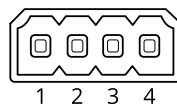
Connettore Ethernet RJ45 con Power over Ethernet (PoE+).

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 rilevatori di rottura.

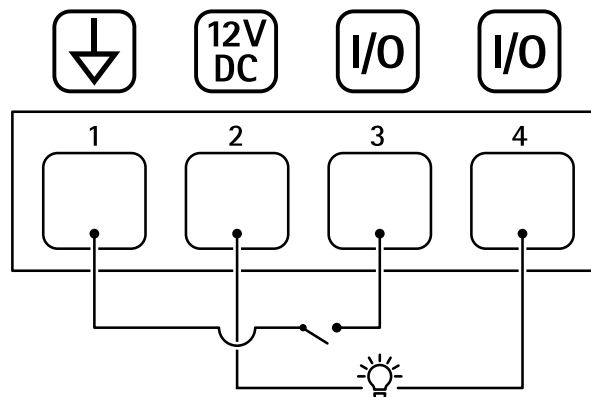
Uscita digitale – Per il collegamento di dispositivi esterni come relè e LED. I dispositivi collegati possono essere attivati tramite l'API (interfaccia per la programmazione di applicazioni) VAPIX® attraverso un evento oppure dall'interfaccia Web del dispositivo.

Morsettiera a 4 pin



Funzione	Pin	Note	Specifiche
Terra CC	1		0 V CC
Output CC	2	Può essere utilizzato per alimentare una periferica ausiliaria. Nota: questo pin può essere usato solo come uscita alimentazione.	12 V CC Carico massimo =50 mA
Configurabile (input o output)	3-4	Ingresso digitale - collegare al pin 1 per l'attivazione oppure lasciare isolato (scollegato) per la disattivazione.	Da 0 a max 30 V CC
		Uscita digitale - collegato internamente al pin 1 (ground 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 Ground CC
- 2 Uscita CC 12 V, max 50mA

AXIS D4100-E Network Strobe Siren

Specifiche

- 3 I/O configurato come input
- 4 I/O configurato come output

Nomi dei pattern di luce

disattivato
Fisso
Bianco fisso + colore lampeggiante
Alternata
Pulsante
Intensificazione 3 passaggi
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

Livelli di pressione sonora massimi

Nome pattern sonoro	Livelli di pressione sonora (dB)
	1
Allarme: suono allarme di altezza elevata	111
Allarme: suono allarme di altezza bassa	108
Allarme: uccello	112
Allarme: sirena navale	91
Allarme: allarme auto veloce	107
Allarme: allarme auto lento	110

AXIS D4100-E Network Strobe Siren

Specifiche

Allarme: orologio classico	96
Allarme: pronto intervento	98
Allarme: orrore	109
Allarme: industriale	103
Allarme: segnale acustico singolo	98
Allarme: segnale acustico quadruplo discreto	100
Allarme: segnale acustico triplo discreto	103
Allarme: triplo suono ad altezza elevata	112
Notifica: accettato	83
Notifica: in chiamata	92
Notifica: negato	89
Notifica: fatto	92
Notifica: ingresso	96
Notifica: fallito	97
Notifica: fretta	88
Notifica: messaggio	96
Notifica: avanti	85
Notifica: apri	100
Sirena: alternata	110
Sirena: scattante	112
Sirena: evac.	102
Sirena: altezza in calo	112
Sirena: residenziale discreta	111

1. Montato a parete a una distanza di 1 m sull'asse al volume impostato 5.

AXIS D4100-E Network Strobe Siren

Consigli per la pulizia

Consigli per la pulizia

Se il dispositivo si macchia di grasso o diventa molto sporco, è possibile pulirlo con sapone o detergente delicato e senza solventi.

AVISO

Non utilizzare mai detergenti aggressivi, ad esempio benzina, benzene o acetone.

1. Utilizzare una bomboletta d'aria compressa per rimuovere polvere o sporcizia dal dispositivo.
2. Pulire il dispositivo con un panno morbido inumidito con un detergente delicato e acqua tiepida.
3. Strofinare accuratamente con un panno asciutto.

Nota

Evitare la pulizia alla luce diretta del sole o a temperature elevate, poiché ciò potrebbe causare macchie quando le goccioline d'acqua si asciugano.

AXIS D4100-E Network Strobe Siren

Risoluzione di problemi

Risoluzione di problemi

Ripristino delle impostazioni predefinite di fabbrica

Importante

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

Per ripristinare il dispositivo ai valori predefiniti di fabbrica:

1. Scollegare l'alimentazione dal dispositivo.
2. Tenere premuto il pulsante di comando quando si ricollega l'alimentazione. Consultare *Panoramica del dispositivo alla pagina 39*.
3. Tenere premuto il pulsante di comando per 15-30 secondi finché l'indicatore LED di stato non lampeggia in giallo.
4. Rilasciare il pulsante di comando. Il processo è completo quando l'indicatore del LED di stato diventerà verde. Il dispositivo è stato reimpostato alle impostazioni di fabbrica predefinite. Se nessun server DHCP è disponibile sulla rete, l'indirizzo IP predefinito è 192.168.0.90.
5. Utilizzare gli strumenti per l'installazione e la gestione del software per assegnare un indirizzo IP, impostare la password e accedere al dispositivo.

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 firmware

Axis offre la gestione del firmware 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 il firmware 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 di firmware del dispositivo AXIS, visitare axis.com/support/firmware.

Controllo della versione firmware corrente

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

Per controllare il firmware corrente:

1. Vai all'interfaccia web del dispositivo > **Status (Stato)**.
2. Consultare la versione firmware in **Device info (Informazioni dispositivo)**.

AXIS D4100-E Network Strobe Siren

Risoluzione di problemi

Aggiornamento del firmware

Importante

- Le impostazioni preconfigurate e personalizzate vengono salvate quando aggiorni il firmware (a condizione che le funzioni siano disponibili nel nuovo firmware), sebbene ciò non sia garantito da Axis Communications AB.
- Assicurarsi che il dispositivo rimanga collegato alla fonte di alimentazione durante il processo di aggiornamento.

Nota

Quando si aggiorna il dispositivo con il firmware più recente 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 di aggiornare il firmware. Per il firmware più aggiornato e le note sul rilascio, visitare il sito Web axis.com/support/firmware.

1. Scarica il file del firmware sul tuo computer, disponibile gratuitamente su axis.com/support/firmware.
2. Accedi al dispositivo come amministratore.
3. Andare a **Maintenance > Firmware upgrade (Manutenzione > Aggiornamento firmware)** 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 individuare qui ciò che si sta cercando, provare a vedere la 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 dopo l'aggiornamento del firmware	Se si riscontrano problemi dopo l'aggiornamento del firmware, ripristinare la versione installata in precedenza dalla pagina Maintenance (Manutenzione) .

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): <ul style="list-style-type: none">• 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.

AXIS D4100-E Network Strobe Siren

Risoluzione di problemi

Impossibile accedere al dispositivo da un browser

Non è possibile eseguire l'accesso	<p>Se HTTPS è abilitato, assicurarsi di utilizzare il protocollo corretto (HTTP o HTTPS) quando si tenta di eseguire l'accesso. Potrebbe essere necessario digitare manualmente <code>http</code> o <code>https</code> nel campo dell'indirizzo del browser.</p> <p>Se si dimentica la password per l'account root, il dispositivo deve essere ripristinato alle impostazioni predefinite di fabbrica. Consultare <i>Ripristino delle impostazioni predefinite di fabbrica alla pagina 44</i>.</p>
L'indirizzo IP è stato modificato dal server DHCP	<p>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).</p> <p>Se necessario, è possibile assegnare manualmente un indirizzo IP statico. Per istruzioni, consultare axis.com/support.</p>
Errore del certificato durante l'utilizzo di IEEE 802.1X	<p>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).</p>

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

Per accedere al dispositivo esternamente, si consiglia di usare 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.

Impossibile collegarsi tramite la porta 8883 con MQTT su SSL

Il firewall blocca il traffico utilizzando la porta 8883 poiché è insicuri.	<p>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.</p> <ul style="list-style-type: none">• 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 la rete ALPN, l'uso di MQTT può essere negoziato su una porta aperta, ad esempio 443. Controllare con il provider del server/broker se è supportato ALPN e quale protocollo e porta ALPN utilizzare.
---	--

Problemi relativi all'audio

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

Problemi di luce

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

Considerazioni sulle prestazioni

È importante tenere conto dei fattori seguenti:

AXIS D4100-E Network Strobe Siren

Risoluzione di problemi

- Un utilizzo eccessivo della rete dovuto a una scarsa infrastruttura influisce sulla larghezza di banda.
- Per il massimo output luce, serve una sorgente di alimentazione PoE Classe 4.
- L'output luce può diminuire se il dispositivo è sporco o sottoposto a temperature elevate.
- In ambienti luminosi come la luce solare diretta, ti consigliamo di usare il parasole accessorio per incrementare la visibilità.
- L'output audio può diminuire se la sirena è bloccata o se il dispositivo non è chiuso in modo esatto.
- L'ambiente di installazione può incidere sull'output sonoro. Il volume dell'audio può incrementare se il dispositivo è installato a parete o in uno spazio chiuso e diminuire se è installato su un palo in un'area aperta.

Contattare l'assistenza

Contatta l'assistenza all'indirizzo axis.com/support.

