

AXIS D6310 Air Quality Sensor

Indice

Installazione.....	4
Impostazioni preliminari	5
.....	5
Individuazione del dispositivo sulla rete.....	5
Supporto browser	5
Aprire l'interfaccia Web del dispositivo.....	5
Crea un account amministratore.....	5
Password sicure	6
Verificare che nessuno abbia alterato il software del dispositivo.....	6
Configurare il dispositivo	7
Configurare il monitoraggio della qualità dell'aria.....	7
Configurare il dashboard del sensore di qualità dell'aria	7
Impostare il sensore di qualità dell'aria	8
Scaricare le statistiche dati sensore	8
Calibrazione per il primo funzionamento del dispositivo.....	9
Configura un profilo	9
Configurare un profilo con un file audio personalizzato per la sirena	9
Importa o esporta un profilo	10
Impostazione SIP diretto (P2P)	10
Configurazione di SIP tramite un server (PBX).....	11
Imposta regole per eventi.....	11
Attivazione di un'azione	12
Registrare un video quando si rileva il vapore di sigarette elettroniche	12
Riprodurre clip audio quando il livello di CO2 è troppo alto	12
Attivare i LED di segnalazione e la sirena tramite sensore PIR.....	13
Inizia un profilo quando avviene l'attivazione di un allarme	13
Inizia un profilo attraverso SIP	14
Controlla più di un profilo con le estensioni SIP	14
Esecuzione di due profili con priorità diverse	15
Attivare un profilo di luce e sirena tramite HTTP Post quando una telecamera rileva movimento	15
Attivare un profilo di luce e sirena tramite input virtuale quando una telecamera rileva movimento	17
Attivare il profilo luce e sirena tramite MQTT quando la telecamera rileva un movimento.....	18
Invia un'e-mail se una verifica dell'altoparlante ha esito negativo.....	19
Riproduzione di una clip personalizzato quando viene attivato un allarme	20
Interrompi audio con DTMF	21
Impostazione dell'audio per le chiamate SIP in entrata	21
Interfaccia Web	23
Stato	23
Video	24
Flusso.....	24
Sensore di qualità dell'aria	25
Dashboard	25
Impostazioni	29
Statistiche	31
Analitiche.....	31
AXIS Audio Analytics.....	31
Audio.....	32
Impostazioni dispositivo	32
Flusso.....	33
Clip audio	33
Ottimizzazione audio	33
Panoramica	33

Profili.....	34
Registrazioni.....	36
Media	37
App.....	37
Sistema.....	38
Ora e ubicazione.....	38
Rete	40
Sicurezza.....	43
Account.....	48
Eventi.....	51
MQTT	56
SIP.....	59
Archiviazione	64
Profili di flusso	65
ONVIF.....	66
Rilevatori.....	69
Impostazioni energetiche	69
Accessori	69
Registri.....	70
Configurazione normale	71
Manutenzione.....	72
Manutenzione.....	72
Risoluzione di problemi	73
Dati tecnici	74
Panoramica dei prodotti.....	74
.....	74
LED di stato	75
Pulsanti.....	75
Pulsante di comando.....	75
Interruttore microfono	75
Connettori.....	75
Connettore di rete	75
Connettore I/O	75
Connettore RS485/RS422	76
Nomi dei pattern di luce	77
Nomi modelli sirena	77
Pulizia del dispositivo	79
Risoluzione dei problemi.....	80
Ripristino delle impostazioni predefinite di fabbrica.....	80
Problemi tecnici, indicazioni e soluzioni.....	80
Considerazioni sulle prestazioni	81
Contattare l'assistenza.....	82

Installazione

Importante

- Tenersi a una distanza di almeno 1,5 metri (4,9 piedi) da aree con bocchette di ventilazione o fonti di inquinamento significative. Questo include bocchette di aerazione, porte, finestre, aree di cottura, ecc.
- Installare il dispositivo in una posizione che consenta il libero flusso dell'aria.
- Per un rilevamento efficace del vapore delle sigarette elettroniche o del fumo, installare il dispositivo sul soffitto a un'altezza di 2,4-2,7 metri (7,9-8,9 piedi) dal pavimento.
- Per un monitoraggio efficace della qualità dell'aria e dell'ambiente, installare il dispositivo a un'altezza di 0,9-1,8 metri (3,0-5,9 piedi) dal pavimento.

Per istruzioni dettagliate sull'installazione, vedere la guida all'installazione.

Impostazioni preliminari

▲ AWISO

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

Individuazione del dispositivo sulla rete

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

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

Supporto browser

Il dispositivo può essere utilizzato con i seguenti browser:

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

✓: Consigliato

*: Supportato con limitazioni

Aprire l'interfaccia Web del dispositivo

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

Per le descrizioni di tutti i comandi e le opzioni nell'interfaccia Web del dispositivo, consultare .

Crea un account amministratore

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

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

Importante

Il dispositivo non ha un account predefinito. In caso di smarrimento della password dell'account amministratore, è necessario reimpostare il dispositivo. Vedere .

Password sicure

Importante

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

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

Per proteggere i dati consigliamo vivamente di:

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

Verificare che nessuno abbia alterato il software del dispositivo

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

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

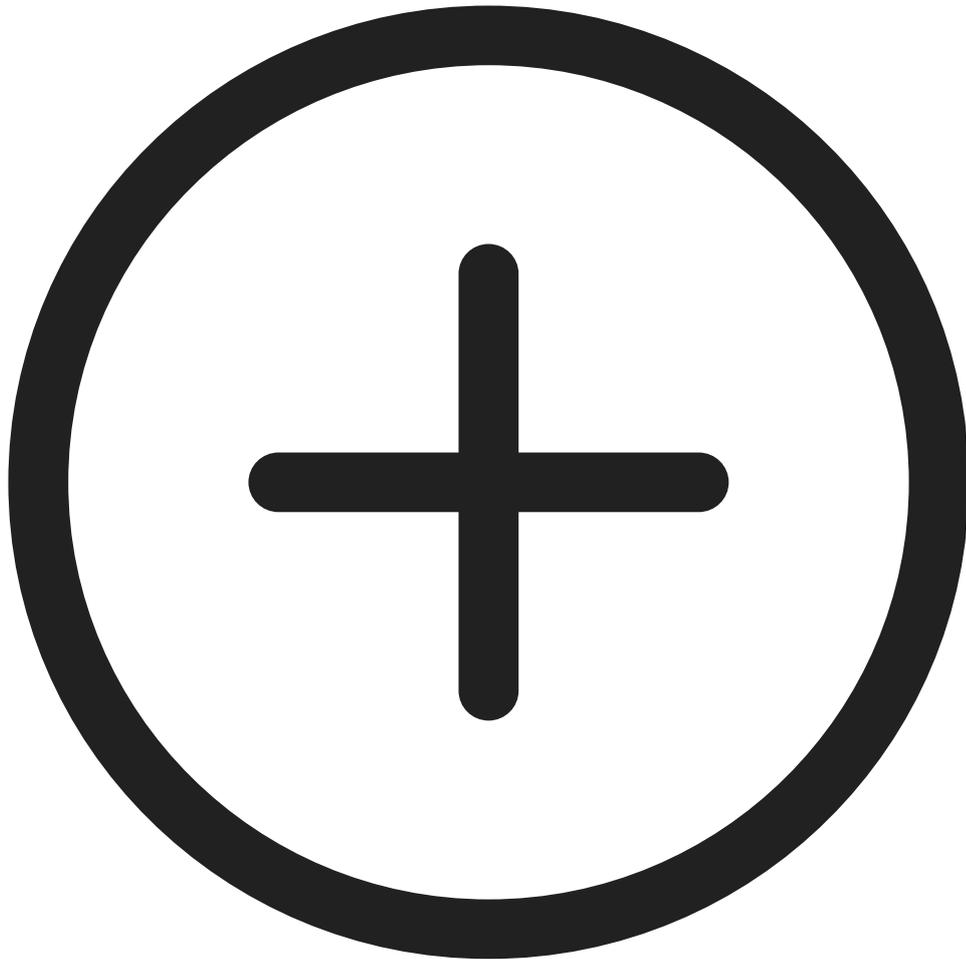
Configurare il dispositivo

Configurare il monitoraggio della qualità dell'aria

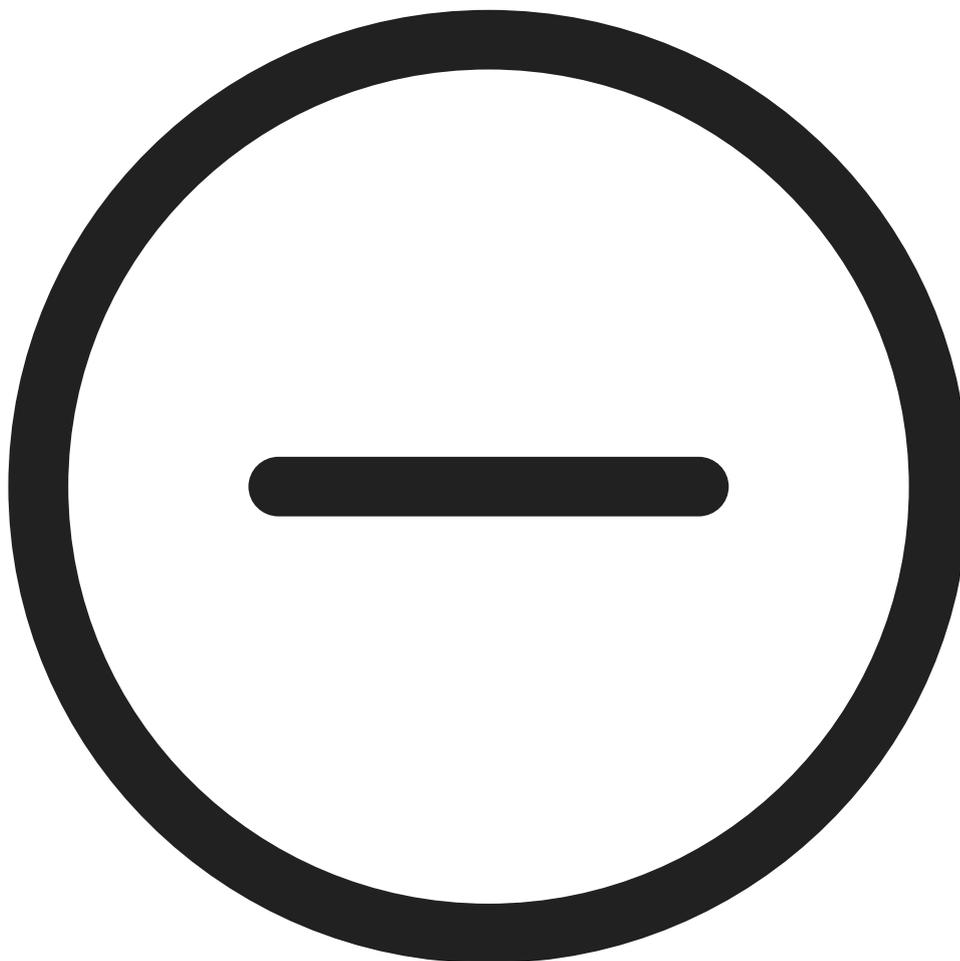
Configurare il dashboard del sensore di qualità dell'aria

Nella pagina web del dispositivo, andare a Air quality monitor > Dashboard (Monitor qualità dell'aria, Dashboard).

- Per modificare il nome del dashboard, fare clic su  sulla sinistra.
- Per visualizzare i dati sul dashboard, fare clic su  Edit (Modifica) >



- Per nascondere i dati sul dashboard, fare clic su  **Edit (Modifica)** >



Impostare il sensore di qualità dell'aria

Nella pagina web del dispositivo, andare a **Air quality sensor** > **Settings** (Sensore qualità dell'aria, Impostazioni).

- Impostare le soglie di temperatura, umidità, CO2, NOx, PM1.0, PM2.5, PM4.0, PM10.0, VOC e AQI, vedere .
- Imposta le unità di misura della temperatura, vedere .
- Impostare la sensibilità di rilevamento del vapore di sigarette elettroniche, vedere .
- Impostare il tempo di conservazione dei dati, vedere .
- Impostare la frequenza dei metadati cloud, vedere .
- Impostare il periodo di convalida, vedere .

Scaricare le statistiche dati sensore

È possibile esportare fino a 365 giorni di statistiche del sensore in un file CSV da utilizzare in applicazioni quali Microsoft® Excel.

1. Nella pagina Web del dispositivo, andare a **Air quality monitor (Monitor qualità dell'aria) > Statistics (Statistiche) > Sensor Data Statistics (Statistiche dei dati del sensore)**.
2. Scegliere un intervallo di date:
 - **Custom range (Intervallo personalizzato)**: Negli elenchi **From** e **To (Da, A)** selezionare le date di inizio e fine (massimo 365 giorni).
 - **Predefined range (Intervallo predefinito)**: Nell'elenco **Predefined date range (Intervallo di date predefinito)**, selezionare un periodo disponibile.

Nota

Se vengono selezionati sia un intervallo personalizzato che uno predefinito, ha la precedenza l'intervallo personalizzato.

Nota

L'intervallo massimo di download è limitato dal tempo di conservazione configurato in .

3. Nell'elenco **Source (Fonte)**, selezionare la fonte desiderata; per esportare i dati di tutte le fonti, fare clic su **Download all data (Esporta tutti i dati)**.
4. Fare clic su **Download data (Scarica dati)** per esportare le statistiche selezionate.

Nota

Fare clic su **Download all data (Scarica tutti i dati)** per esportare tutti i dati di tutte le fonti nell'arco temporale selezionato.

Calibrazione per il primo funzionamento del dispositivo

Nota

- Per la precisione totale della CO2 sono necessari 2 giorni al primo avvio del dispositivo.
- L'indice AQI (Air Quality Index) richiede 12 ore per essere funzionante al primo avvio del dispositivo. L'AQI mostrerà **Calculating (Calcolo in corso)** finché non disporrà di dati sufficienti. Il tempo di calibrazione è necessario ogni volta che il dispositivo viene riavviato.
- La precisione totale VOC si ottiene dopo un'ora di funzionamento del dispositivo. Il tempo di calibrazione è necessario ogni volta che il dispositivo viene riavviato.
- La precisione totale NOx si ottiene dopo 6 ore di funzionamento del dispositivo. Il tempo di calibrazione è necessario ogni volta che il dispositivo viene riavviato.

Configura un profilo

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

Per impostare un nuovo profilo:

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

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

Configurare un profilo con un file audio personalizzato per la sirena

È possibile configurare un profilo con un file audio personalizzato. Sul dispositivo è possibile salvare file audio di dimensioni fino a 100 Mb. Per file audio di grandi dimensioni, utilizzare una scheda SD, se il dispositivo è dotato di uno slot per schede SD.

Caricare un file audio:

1. Andare su **Media (Supporti multimediali)** e fare clic su  **Add (Aggiungi)**.
2. Sfogliare per selezionare il file dal computer.
3. Selezionare **Punto di archiviazione**.
4. Fare clic su **Save (Salva)**.

Per utilizzare il file audio in un profilo:

1. Accedere a **Profili** e creare un profilo. Per ulteriori informazioni, vedere .
2. Quando si configura **Siren (Sirena)**, selezionare il file audio caricato come **Pattern (Modello)**.

Importa o esporta un profilo

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

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

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

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

Impostazione SIP diretto (P2P)

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

Per ulteriori informazioni sulle opzioni di impostazione, consultare .

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

Nota

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

6. In **Audio**, selezionare almeno un codec audio con la qualità audio desiderata per le chiamate SIP. Trascina e rilascia per modificare la priorità.
7. In **Additional (Aggiuntivo)**, selezionare opzioni aggiuntive.
 - **UDP-to-TCP switching (Passaggio da UDP a TCP)**: selezionare questa opzione per consentire alle chiamate di scambiare 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 1300 byte.
 - **Allow via rewrite (Consenti tramite riscrittura)**: selezionare per inviare l'indirizzo IP locale e non l'indirizzo IP pubblico del router.
 - **Allow contact rewrite (Consenti riscrittura contatto)**: selezionare questa opzione per inviare l'indirizzo IP locale e non l'indirizzo IP pubblico del router.
 - **Register with server every (registra con il server ogni)**: impostare la frequenza con cui si desidera che il dispositivo si sincronizzi con il server SIP per gli account SIP esistenti.
 - **DTMF payload type (Tipo payload DTMF)**: modificare il tipo di payload per DTMF.
8. Fare clic su **Save (Salva)**.

Configurazione di SIP tramite un server (PBX)

Utilizzare un server PBX quando gli agenti utente comunicano all'interno e all'esterno della rete IP. Altre funzionalità possono essere aggiunte alla configurazione a seconda del provider PBX. Per capire meglio il funzionamento del P2P, consultare .

Per ulteriori informazioni sulle opzioni di impostazione, consultare .

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, vedere .

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. Immettere un **Name (Nome)**.
3. Selezionare la **Condition (Condizione)** che deve essere soddisfatta per attivare l'azione. Se si specifica più di una condizione per la regola, devono essere soddisfatte tutte le condizioni per attivare l'azione.
4. Selezionare l'**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.

Registrare un video quando si rileva il vapore di sigarette elettroniche

L'esempio seguente spiega come configurare un sensore di qualità dell'aria per registrare video sull'archivio di rete quando il sensore di qualità dell'aria rileva la presenza di vapore di sigarette elettroniche.

1. Nella pagina Web del sensore di qualità dell'aria, andare **Settings > System > Storage** (Impostazioni, Sistema, Archiviazione) per verificare che l'archiviazione di rete sia impostata.
2. Andare a **Settings > System > Events** (Impostazioni > Sistema > Eventi) e aggiungere una regola. Immettere le seguenti informazioni:
 - **Nome:** Inserire un nome per la regola.
 - **Condition (Condizione):** **Air quality monitor (Monitor della qualità dell'aria) > Vaping or smoking detected (Rilevamento di vapore delle sigarette elettroniche o fumo)**.
 - **Action (Azione) :** **Recordings (Registrazioni) > Record video (Registrazione di video)**.
 - **Dispositivo di archiviazione:** **Network storage (Archiviazione di rete)**. Assicurarsi che l'archiviazione di rete sia impostata.
 - **Telecamera:** Seleziona un'area di visione telecamera.
 - **Stream profile (Profilo di streaming):** Selezionare un profilo di streaming o **Create a stream profile (Crea un profilo di streaming)**.
 - **Prebuffer (Pre-buffer) e Postbuffer (post-buffer):** Impostare i valori desiderati.
3. Fare clic su **Save (Salva)**.

Riprodurre clip audio quando il livello di CO2 è troppo alto

Questo esempio spiega come riprodurre una clip audio quando il livello di CO2 è troppo elevato.

Creazione di una regola

1. Nella pagina Web, andare a **Events > Rules > Add a rule** (Eventi, Regole, Aggiungi una regola) per creare una regola.
2. Immettere le seguenti informazioni:
 - **Nome:** Inserire un nome per la regola.
 - **Conditions (Condizioni):** **Air quality monitor > Air quality outside acceptable range** (Monitoraggio della qualità dell'aria, Qualità dell'aria al di fuori dell'intervallo accettabile)
 - **Sensor:** **CO2 (Sensore, CO2)**
 - **Action (Azione):** **Riproduzione clip audio**
 - **Clip:** seleziona una clip audio.
3. Fare clic su **Save (Salva)**.

Impostare l'intervallo di allarme per la CO2

- Nella pagina Web, andare a **Air quality monitor > Settings > CO2** (Monitor qualità dell'aria, Impostazioni, CO2).
- Inserire i dati **MIN** e **MAX** per impostare l'intervallo CO2.

Attivare i LED di segnalazione e la sirena tramite sensore PIR

Questo esempio spiega come attivare i LED di segnalazione e la sirena tramite il sensore PIR. Vedere per le posizioni dei LED di segnalazione e della sirena.

Creare un profilo LED di segnalazione e sirena:

1. Nella pagina Web del dispositivo, andare a **Profiles > Create** (Profili, crea).
2. Immettere le seguenti informazioni:
 - **Nome:** Profile 1 (Profilo 1)
 - **Description (Descrizione):** Aggiungere la descrizione del profilo.
 - **Light (Luce):** Selezionare **Pattern, Speed, Intensity, Color** e **Duration** (Modello, velocità, intensità, colore e durata).
 - **Siren (Sirena):** Selezionare **Pattern, Intensity** e **Duration** (Modello, Intensità e Durata).

Nota

I profili con numeri più elevati hanno una priorità maggiore.

- **Priority (Priorità):** Selezionare **Light priority** e **Siren priority** (Priorità luce, Priorità sirena).

Crea un evento:

1. Andare a **System > Events > Rules** (Sistema, Eventi, Regole) e aggiungere una regola.
2. Immettere le seguenti informazioni:
 - **Nome:** Attivare i LED di segnalazione e la sirena
 - **Condition (Condizione):** sensore PIR
 - **Action (Azione):** Eseguire profilo luce e sirena
 - **Profile (Profilo):** Profile 1 (Profilo 1)
 - **Action (Azione):** Inizio
3. Fare clic su **Save (Salva)**.

Inizia un profilo quando avviene l'attivazione di un allarme

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

Impostare la direzione su input per la porta:

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

Creare una regola:

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

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

Inizia un profilo attraverso SIP

Questo esempio illustra come si attiva un allarme attraverso SIP.

Attivazione SIP:

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

Creare una regola:

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

Controlla più di un profilo con le estensioni SIP

Attivazione SIP:

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

Crea una regola per avviare un profilo:

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

Crea una regola per arrestare un profilo:

1. Vai su **System (Sistema) > Events (Eventi)** e aggiungi una regola.
2. Inserire un nome per la regola.
3. Nell'elenco delle condizioni, seleziona **Call (Chiama) > State change (Cambio di stato)**.
4. Nell'elenco dei motivi, seleziona **Terminated (Terminato)**.

5. In **Call direction (Direzione di chiamata)**, seleziona **Incoming (In entrata)**.
6. In **Local SIP URI (URI SIP locale)**, digita `sip:[Ext]@[indirizzo IP]` dove [Ext] è l'estensione usata per il profilo e [indirizzo IP] è l'indirizzo del dispositivo. Ad esempio `sip:1001@192.168.0.90`.
7. Nella lista di azioni, selezionare **Light and Siren (Luce e sirena) > Run light and siren profile (Esegui profilo luce e sirena)**.
8. Seleziona il profilo che vuoi fermare.
9. Seleziona l'azione **Stop (Arresta)**.
10. Fare clic su **Save (Salva)**.

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

Esecuzione di due profili con priorità diverse

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

Nota

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

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

Crea profili:

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

Creare una regola:

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

Attivare un profilo di luce e sirena tramite HTTP Post quando una telecamera rileva movimento

In questo esempio viene spiegato come collegare una telecamera al sensore di qualità dell'aria e come attivare un profilo di luce e sirena nel sensore qualità dell'aria quando l'applicazione AXIS Motion Guard, installata nella telecamera, rileva movimento.

Operazioni preliminari:

- Creare un nuovo utente con il ruolo Operatore o Amministratore nel sensore di qualità dell'aria.
- Creare un profilo nel sensore di qualità dell'aria chiamato: "Profilo luci e sirena".
- Configurare AXIS Motion Guard nella telecamera e creare un profilo denominato: "Profilo telecamera".
- Assicurarsi di utilizzare AXIS Device Assistant con la versione firmware 10.8.0 o successiva.

Crea un destinatario nella telecamera:

1. Nell'interfaccia del dispositivo della telecamera, vai a **System > Events > Recipients (Sistema > Eventi > Destinatari)** e aggiungi un destinatario.

2. Immettere le seguenti informazioni:
 - **Name (Nome):** sensore della qualità dell'aria
 - **Tipo:** HTTP
 - **URL:** http://<IPaddress>/axis-cgi/siren_and_light.cgi
Sostituire <Indirizzo IP> con l'indirizzo del sensore di qualità dell'aria.
 - Il nome utente e la password dell'utente del sensore qualità dell'aria appena creato.
3. Fare clic su **Test (Verifica)** per assicurarsi che tutti i dati siano validi.
4. Fare clic su **Save (Salva)**.

Creare due regole nella telecamera:

1. Andare a **Rules (Regole)** e aggiungere una regola.
2. Immettere le seguenti informazioni:
 - **Nome:** Attivare il sensore di qualità dell'aria con movimento
 - **Condition (Condizione):** Applications (Applicazioni) > Motion Guard: Camera profile (Motion Guard: profilo telecamera)
 - **Action (Azione):** Notifications > Send notification through HTTP (Notifiche > Invia notifica tramite HTTP)
 - **Recipient (Destinatario):** sensore della qualità dell'aria.
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": "Light and siren profile" } }
```

Assicurarsi di inserire le stesse informazioni in **"profile" (profilo)** : <>' come già effettuato nella sirena, in questo caso: "Profilo luce e sirena"

3. Fare clic su **Save (Salva)**.
4. Aggiungere un'altra regola con le seguenti informazioni:
 - **Nome:** Disattivare il sensore di qualità dell'aria con movimento
 - **Condition (Condizione):** Applications (Applicazioni) > Motion Guard: Camera profile (Motion Guard: profilo telecamera)
 - Seleziona **Invert this condition (Inverti questa condizione)**.
 - **Action (Azione):** Notifications > Send notification through HTTP (Notifiche > Invia notifica tramite HTTP)
 - **Recipient (Destinatario):** sensore della qualità dell'aria
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": "stop", "params": { "profile": "Light and siren
profile" } }
```

Assicurarsi di inserire le stesse informazioni in **"profile" (profilo)** : <>' come già effettuato nella sirena, in questo caso: "Profilo luce e sirena"

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

Attivare un profilo di luce e sirena tramite input virtuale quando una telecamera rileva movimento

In questo esempio viene spiegato come collegare una telecamera al sensore di qualità dell'aria e come attivare un profilo nel sensore qualità dell'aria quando l'applicazione AXIS Motion Guard, installata nella telecamera, rileva movimento.

Operazioni preliminari:

- Creare un nuovo account con privilegi Operatore o Amministratore nel sensore qualità dell'aria.
- Creare un profilo nel sensore qualità dell'aria. Vedere .
- 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. Immettere le seguenti informazioni:
 - **Nome:** Attiva la porta virtuale
 - **Tipo:** HTTP
 - **URL:** `http://<indirizzoIP>/axis-cgi/virtualinput/activate.cgi`
Sostituire <Indirizzo IP> con l'indirizzo del sensore di qualità dell'aria.
 - L'account e la password dell'account del sensore qualità dell'aria appena creato.
3. Fare clic su **Test (Verifica)** per assicurarsi che tutti i dati siano validi.
4. Fare clic su **Save (Salva)**.
5. Aggiungere un secondo destinatario con le seguenti informazioni:
 - **Nome:** disattivare la porta virtuale
 - **Tipo:** HTTP
 - **URL:** `http://<indirizzoIP>/axis-cgi/virtualinput/deactivate.cgi`
Sostituire <Indirizzo IP> con l'indirizzo del sensore di qualità dell'aria.
 - L'account e la password dell'account del sensore qualità dell'aria appena creato.
6. Fare clic su **Test (Verifica)** per assicurarsi che tutti i dati siano validi.
7. Fare clic su **Save (Salva)**.

Creare due regole nella telecamera:

1. Andare a **Rules (Regole)** e aggiungere una regola.
2. Immettere le seguenti informazioni:
 - **Nome:** attivare la porta virtuale IO1
 - **Condition (Condizione):** Applications (Applicazioni) > Motion Guard: Camera profile (Motion Guard: profilo telecamera)
 - **Action (Azione):** Notifications > Send notification through HTTP (Notifiche > Invia notifica tramite HTTP)
 - **Recipient (Destinatario):** Attiva la porta virtuale
 - **Suffisso della stringa di query:** `schemaversion=1&port=1`
3. Fare clic su **Save (Salva)**.
4. Aggiungere un'altra regola con le seguenti informazioni:
 - **Nome:** Disattivare la porta virtuale IO1
 - **Condition (Condizione):** Applications (Applicazioni) > Motion Guard: Camera profile (Motion Guard: profilo telecamera)
 - **Seleziona Invert this condition (Inverti questa condizione).**
 - **Action (Azione):** Notifications > Send notification through HTTP (Notifiche > Invia notifica tramite HTTP)

- **Recipient (Destinatario):** disattivare la porta virtuale
- **Suffisso della stringa di query:** schemaversion=1&port=1

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

Creare una regola nel sensore di qualità dell'aria:

1. Nell'interfaccia Web del sensore di qualità dell'aria, andare a **System > Events (Sistema > Eventi)** e aggiungere una regola.
2. Immettere le seguenti informazioni:
 - **Nome:** attivazione su ingresso virtuale 1
 - **Condition (Condizione):** I/O > Virtual input is active (Input virtuale attivo)
 - **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)**.

Attivare il profilo luce e sirena tramite MQTT quando la telecamera rileva un movimento

Questo esempio spiega come collegare una telecamera al sensore di qualità dell'aria e attivare un profilo nel sensore di qualità dell'aria ogni volta che la telecamera rileva un movimento.

Operazioni preliminari:

- Creare un profilo nel sensore di qualità dell'aria.
- Imposta un broker MQTT e ottieni l'indirizzo IP, il nome utente e la password del broker.
- Accertarsi che l'applicazione di rilevamento del movimento è configurata e in esecuzione sulla telecamera.

Configura il client MQTT nella telecamera:

1. Nell'interfaccia Web della telecamera, andare su **System > MQTT > MQTT client > Broker (Sistema, MQTT, Client MQTT, Broker)** e immettere 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
 - **Porta:** Il numero di porta utilizzato dal broker
 - **Username (Nome utente) e Password** del broker
2. Fare clic su **Save (Salva)** e **Connect (Connetti)**.

Creazione di due regole nella telecamera per la pubblicazione MQTT:

1. Andare a **System > Events > Rules (Sistema > Eventi > Regole)** e aggiungere una regola.
2. Immettere le seguenti informazioni:
 - **Nome:** Oggetti in movimento rilevati
 - **Condition (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:
 - **Nome:** Nessun movimento

- **Condition (Condizione): Applications > Motion alarm (Applicazioni > Allarme di movimento)**
 - Seleziona **Invert this condition (Inverti questa condizione)**.
- **Action (Azione): MQTT > Send MQTT publish message (MQTT > Invia messaggio di pubblicazione MQTT)**
- **Topic (Argomento): Movimento**
- **Payload: Disattivato**
- **QoS: 0, 1 o 2**

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

Configurare il client MQTT nel sensore di qualità dell'aria:

1. Nell'interfaccia Web del sensore di qualità dell'aria, andare su **System > MQTT > MQTT client > Broker (Sistema, MQTT, Client MQTT, Broker)** e immettere le seguenti informazioni:

- **Host: Indirizzo IP broker**
- **Client ID (ID client): Sirena 1**
- **Protocol (Protocollo): Il protocollo su cui è impostato il broker**
- **Porta: Il numero di porta utilizzato dal broker**
- **Username (Nome utente) e Password**

2. Fare clic su **Save (Salva)** e **Connect (Connetti)**.

3. Vai su **MQTT subscriptions (Sottoscrizioni MQTT)** e aggiungi una sottoscrizione. Immettere le seguenti informazioni:

- **Subscription filter (Filtro sottoscrizione): Movimento**
- **Subscription type (Tipo di sottoscrizione): Dotato di stato**
- **QoS: 0, 1 o 2**

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

Creare una regola nel sensore di qualità dell'aria per gli abbonamenti MQTT:

1. Andare a **System > Events > Rules (Sistema > Eventi > Regole)** e aggiungere una regola.

2. Immettere le seguenti informazioni:

- **Nome: Oggetti in movimento rilevati**
- **Condition (Condizione): MQTT > Stateful (MQTT > Dotato di stato)**
- **Subscription filter (Filtro sottoscrizione): 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)**.

Invia un'e-mail se una verifica dell'altoparlante ha esito negativo

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

1. Impostare una pianificazione per la verifica dell'altoparlante:

1.1. Andare all'interfaccia del dispositivo > **System (Sistema) > Events (Eventi) > Schedules (Pianificazioni)**.

1.2. Creare una pianificazione che inizi alle 18:00 e finisca alle 18:01 ogni giorno. Assegnare il nome "Tutti i giorni alle 18:00".

2. Creare un destinatario e-mail:

- 2.1. Andare all'interfaccia del dispositivo > **System (Sistema)** > **Events (Eventi)** > **Recipients (Destinatari)**.
- 2.2. Fare clic su **Add recipient (Aggiungi destinatario)**.
- 2.3. Assegnare al destinatario il nome "Destinatari test altoparlante"
- 2.4. In **Type (Tipo)**, selezionare **Email (E-mail)**.
- 2.5. In **Send email to (Invia e-mail a)**, inserire gli indirizzi e-mail dei destinatari. Utilizzare la virgola per separare più indirizzi.
- 2.6. Inserire i dettagli per l'account e-mail del mittente.
- 2.7. Fare clic su **Test** per inviare un messaggio e-mail di testo.

Nota

Alcuni provider e-mail hanno filtri di sicurezza che impediscono agli utenti di ricevere o visualizzare allegati di grandi dimensioni, ad esempio e-mail pianificate e simili. Controllare i criteri di sicurezza del provider e-mail per evitare problemi di consegna e account e-mail bloccati.

- 2.8. Fare clic su **Save (Salva)**.
3. Impostare la verifica degli altoparlanti automatica:
 - 3.1. Andare all'interfaccia del dispositivo > **System (Sistema)** > **Events (Eventi)** > **Rules (Regole)**.
 - 3.2. Fare clic su **Add a rule (Aggiungi una regola)**.
 - 3.3. Immettere un nome per la regola.
 - 3.4. In **Condition (Condizione)**, selezionare **Schedule (Pianificazione)** e selezionare dall'elenco dei trigger
 - 3.5. In **Schedule (Pianificazione)**, selezionare la pianificazione (Tutti i giorni alle 18:00).
 - 3.6. In **Action (Azione)**, selezionare **Run automatic speaker test (Esegui test automatico dell'altoparlante)**.
 - 3.7. Fare clic su **Save (Salva)**.
4. Impostare la condizione per l'invio di un messaggio e-mail quando la verifica dell'altoparlante ha esito negativo:
 - 4.1. Andare all'interfaccia del dispositivo > **System (Sistema)** > **Events (Eventi)** > **Rules (Regole)**.
 - 4.2. Fare clic su **Add a rule (Aggiungi una regola)**.
 - 4.3. Immettere un nome per la regola.
 - 4.4. In **Condition (Condizione)**, selezionare **Speaker test result (Risultato test dell'altoparlante)**.
 - 4.5. In **Speaker test status (Stato test dell'altoparlante)**, selezionare **Didn't pass the test (Test non superato)**.
 - 4.6. In **Action (Azione)**, selezionare **Send notification to email (Invia notifica a e-mail)**.
 - 4.7. In **Recipient (Destinatario)**, selezionare il destinatario ("Destinatari test altoparlante")
 - 4.8. Inserire un oggetto e un messaggio e fare clic su **Save (Salva)**.

Riproduzione di una clip personalizzato quando viene attivato un allarme

Questo esempio spiega come attivare un file audio personalizzato quando cambia il segnale di ingresso digitale.

Caricare un file audio:

1. Andare su **Media (Supporti multimediali)** e fare clic su  **Add (Aggiungi)**.
2. Fare clic per sfogliare e selezionare il file audio dal computer.
3. Selezionare **Punto di archiviazione**.
4. Fare clic su **Save (Salva)**.

Creare un profilo con il file audio:

1. Andare in **Profiles (Profili)** e fare clic su  **Create (Crea)**.
2. Immettere **Name (Nome)** e selezionare il modello di luce per il profilo.
3. Nella sezione sirena, selezionare il file audio caricato.
4. Selezionare **Intensity (Intensità)** e **Duration (Durata)**.
5. Fare clic su **Save (Salva)**.

Impostare la direzione su input per la porta:

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

Creare una regola:

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

Interrompi audio con DTMF

Questo esempio spiega come:

- configurare DTMF su un dispositivo.
 - impostare un evento per interrompere l'audio quando un comando DTMF viene inviato al dispositivo.
1. Vai a **System (Sistema) > SIP > SIP settings (Impostazioni SIP)**.
 2. Assicurarsi che **Enable SIP (Abilita SIP)** sia attivata.
Se è necessario attivarla, ricordare di fare clic su **Save (Salva)** in un secondo momento.
 3. Andare a **SIP accounts (Account SIP)**.
 4. Vicino all'account SIP, fare clic su  **> Edit (Modifica)**.
 5. In **DTMF**, fare clic su **+ DTMF sequence (Aggiungi sequenza DTMF)**.
 6. In **Sequence (Sequenza)**, inserire "1".
 7. In **Description (Descrizione)**, inserire "stop audio".
 8. Fare clic su **Save (Salva)**.
 9. Andare a **System (Sistema) > Events (Eventi) > Rules (Regole)** e fare clic su **+ Add a rule (Aggiungi una regola)**.
 10. In **Name (Nome)**, inserire "DTMF stop audio".
 11. In **Condition (Condizione)**, selezionare **DTMF**.
 12. In **DTMF Event ID (ID evento DTMF)**, selezionare **stop audio**.
 13. In **Action (Azione)**, selezionare **Stop playing audio clip (Interrompi riproduzione di clip audio)**.
 14. Fare clic su **Save (Salva)**.

Impostazione dell'audio per le chiamate SIP in entrata

È possibile impostare una regola che riproduce una clip audio quando si riceve una chiamata SIP.

È inoltre possibile impostare una regola aggiuntiva che risponde automaticamente alla chiamata SIP una volta terminata la clip audio. Ciò può essere utile nei casi in cui un operatore di allarme desidera richiamare l'attenzione di qualcuno vicino a un dispositivo audio e stabilire una linea di comunicazione. Questa operazione viene eseguita effettuando una chiamata SIP al dispositivo audio, che riprodurrà una clip audio per avvisare le persone vicine al dispositivo audio. Quando la riproduzione della clip audio è terminata, il dispositivo audio risponde automaticamente alla chiamata SIP e può avere luogo la comunicazione tra l'operatore dell'allarme e le persone vicine al dispositivo audio.

Abilitare le impostazioni SIP:

1. Accedere all'interfaccia del dispositivo dell'altoparlante inserendo il proprio indirizzo IP in un browser Web.
2. Andare su **System (Sistema) > SIP > SIP settings (Impostazioni SIP)** e selezionare **Enable SIP (Abilita SIP)**.
3. Per consentire al dispositivo di ricevere chiamate in entrata, selezionare **Allow incoming SIP calls (Consenti chiamate SIP in arrivo)**.
4. Fare clic su **Save (Salva)**.
5. Andare su **SIP accounts (Account SIP)**.
6. Vicino all'account SIP, fare clic su  > **Edit (Modifica)**.
7. Deselezionare **Risposta automatica**.

Riprodurre audio quando viene ricevuta una chiamata SIP:

1. Andare su **Settings > System > Events > Rules (Impostazioni > Sistema > Eventi > Regole)** e aggiungere una regola.
2. Inserire un nome per la regola.
3. Nell'elenco delle condizioni, selezionare **State (Stato)**.
4. Nell'elenco degli stati, selezionare **Chiamata**.
5. Nell'elenco delle azioni, selezionare **Play audio clip (Riprodurre clip audio)**.
6. Nell'elenco delle clip, selezionare la clip audio che si desidera riprodurre.
7. Selezionare quante volte ripetere la clip audio. 0 indica "riproduci una volta".
8. Fare clic su **Save (Salva)**.

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

1. Andare su **Settings > System > Events > Rules (Impostazioni > Sistema > Eventi > Regole)** e aggiungere una regola.
2. Inserire un nome per la regola.
3. Nell'elenco delle condizioni, selezionare **Audio clip playing (Riproduzione clip audio)**.
4. Selezionare **Utilizza questa condizione come trigger**.
5. Selezionare **Inverti questa condizione**.
6. Fare clic su **+ Aggiungi una condizione** per aggiungere una seconda condizione all'evento.
7. Nell'elenco delle condizioni, selezionare **State (Stato)**.
8. Nell'elenco degli stati, selezionare **Chiamata**.
9. Nell'elenco delle azioni, selezionare **Answer call (Rispondi alla chiamata)**.
10. Fare clic su **Save (Salva)**.

Interfaccia Web

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

Stato

Informazioni sui dispositivi

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

Upgrade AXIS OS (Aggiorna AXIS OS): Aggiorna il software sul dispositivo. Porta l'utente sulla pagina Manutenzione dove è possibile eseguire l'aggiornamento.

Stato sincronizzazione ora

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

NTP settings (Impostazioni NTP): visualizza e aggiorna le impostazioni NTP. Porta l'utente alla pagina **Time and location (Ora e posizione)** dove è possibile modificare le impostazioni NTP.

Sicurezza

Mostra il tipo di accesso attivo al dispositivo, i protocolli di crittografia in uso e se sono consentite app non firmate. I consigli di impostazione sono basati sulla Guida alla protezione AXIS OS.

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

Individua dispositivo

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

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

Stato alimentazione

Mostra informazioni relative allo stato dell'alimentazione. Le informazioni differiscono in base al dispositivo.

Registrazioni in corso

Mostra le registrazioni in corso e il relativo spazio di archiviazione designato.

Registrazioni: Consente di visualizzare le registrazioni in corso e quelle filtrate oltre alla relativa origine. Per ulteriori informazioni, vedere



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

Clients collegati

Mostra il numero di connessioni e client connessi.

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

Video

Flusso

Generale

Risoluzione: Selezionare la risoluzione dell'immagine adatta per la scena di sorveglianza. Una risoluzione più elevata necessita di più larghezza di banda e spazio di archiviazione.

Frequenza dei fotogrammi: Per evitare problemi di larghezza di banda nella rete o ridurre le dimensioni di archiviazione, puoi limitare la velocità in fotogrammi a una quantità fissa di fotogrammi. Se la velocità in fotogrammi è zero, il valore viene impostato sul valore massimo possibile nelle condizioni correnti. Una velocità in fotogrammi più elevata necessita di larghezza di banda e spazio di archiviazione maggiori.

P-frames (P-frame): Un P-frame è un'immagine predetta che mostra solo le modifiche nell'immagine rispetto al fotogramma precedente. Immetti il numero desiderato di P-frame. Più è alto il numero, minore è la larghezza di banda necessaria. Tuttavia, se è presente una congestione di rete, potrebbe verificarsi un deterioramento della qualità video.

Compressione: Utilizzare il cursore per regolare la compressione d'immagine. Un'elevata compressione si traduce in velocità di trasmissione e qualità dell'immagine inferiori. Una compressione bassa migliora la qualità dell'immagine ma utilizza larghezza di banda e spazio di archiviazione maggiori durante la registrazione.

Video con firma  : Attivare per aggiungere la funzione video firmata al video. Il video firmato protegge il video dalle manomissioni aggiungendo firme crittografiche al video.

Controllo velocità di trasferimento

- **Average (Media):** Seleziona per la regolazione automatica della velocità in bit per un periodo di tempo più lungo e la migliore qualità di immagine possibile sulla base dell'archiviazione a disposizione.
 -  Fare clic per il calcolo della velocità in bit di destinazione sulla base dell'archiviazione disponibile, del tempo di conservazione e del limite della velocità in bit.
 - **Target bitrate (Velocità in bit di destinazione):** Immetti la velocità in bit di destinazione voluta.
 - **Retention time (Tempo di conservazione):** Immetti il numero di giorni per la conservazione delle registrazioni.
 - **Dispositivo di archiviazione:** mostra lo spazio di archiviazione stimato che può essere utilizzato per il flusso.
 - **Maximum bitrate (Velocità di trasmissione massima):** Attiva per l'impostazione di un limite di velocità in bit.
 - **Bitrate limit (Limite velocità in bit):** Immettere un limite per la velocità in bit che sia maggiore rispetto alla velocità in bit di destinazione.
- **Maximum (Massimo):** selezionare per impostare una velocità di trasmissione massima istantanea del flusso in base alla larghezza di banda di rete.
 - **Maximum (Massimo):** Immetti la velocità in bit massima.
- **Variable (Variabile):** Seleziona per permettere che la velocità in bit vari sulla base del livello di attività nella scena. Un'attività maggiore necessita di più larghezza di banda. Raccomandiamo questa opzione per la gran parte delle situazioni.

Audio

Include (Includi): Attiva per usare l'audio nel flusso video.

Source (Sorgente)  : Seleziona la sorgente audio da usare.

Stereo  : Attiva per l'inclusione dell'audio incorporato nonché dell'audio da un microfono esterno.

Sensore di qualità dell'aria

Dashboard

Dati in tempo reale

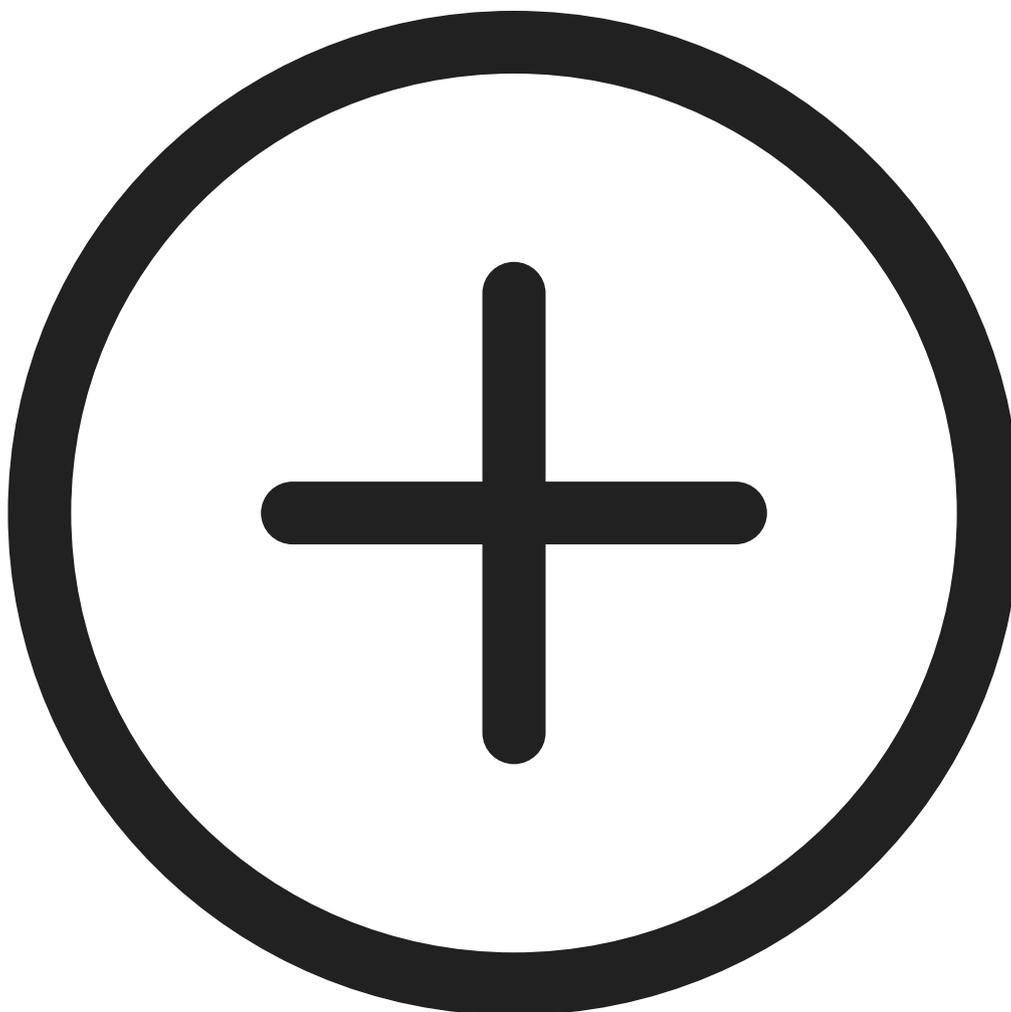
Mostra i dati del sensore in tempo reale.

Nota

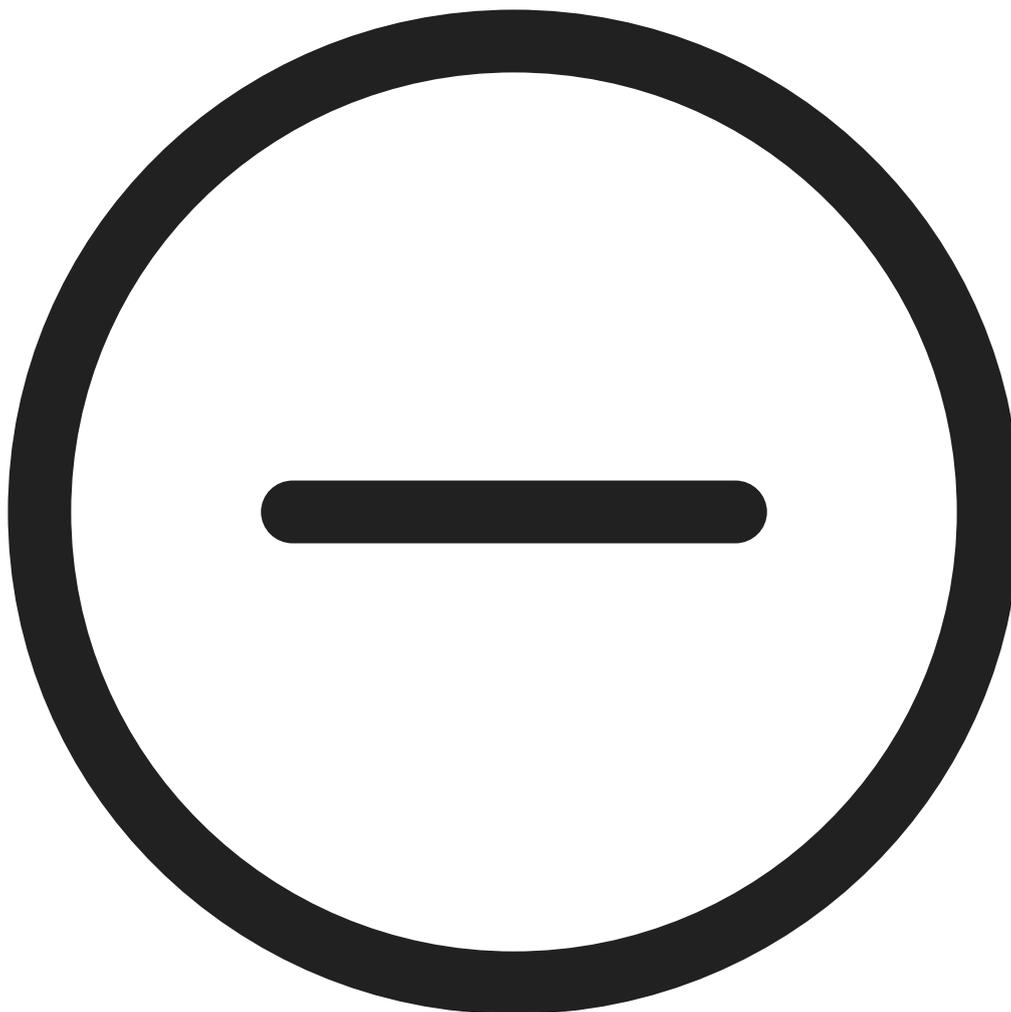
- Per la precisione totale della CO2 sono necessari 2 giorni al primo avvio del dispositivo.
- L'indice AQI (Air Quality Index) richiede 12 ore per essere funzionante al primo avvio del dispositivo. L'AQI mostrerà **Calculating (Calcolo in corso)** finché non disporrà di dati sufficienti. Il tempo di calibrazione è necessario ogni volta che il dispositivo viene riavviato.
- La precisione totale VOC si ottiene dopo un'ora di funzionamento del dispositivo. Il tempo di calibrazione è necessario ogni volta che il dispositivo viene riavviato.
- La precisione totale NOx si ottiene dopo 6 ore di funzionamento del dispositivo. Il tempo di calibrazione è necessario ogni volta che il dispositivo viene riavviato.

 : fare clic per impostare il nome del dashboard.

 Edit (Modifica): Fare clic per mostrare o nascondere i dati.



 : Fare clic per aggiungere dati al dashboard.



: Fare clic per rimuovere i dati dal dashboard.

Temperature (Temperatura): Visualizzare la temperatura in tempo reale del sensore di qualità dell'aria.

Humidity (Umidità): Visualizzare l'umidità in tempo reale del sensore di qualità dell'aria.

CO2: visualizzare l'anidride carbonica in tempo reale.

I significati dei colori delle barre di stato della CO2 sono i seguenti:

- **Verde (0-1000): Buono.** I dati sono considerati soddisfacenti.
- **Arancione (1001-2000): Insalubre per un gruppo sensibile.** I membri dei gruppi sensibili possono subire effetti sulla salute. Il pubblico in generale ha meno probabilità di essere colpito.
- **Rosso (2001-5000): Insalubre.** Gli effetti sulla salute possono riguardare tutte le persone; i membri di gruppi sensibili possono subire effetti più gravi sulla salute.
- **Viola (5001-40000): Molto insalubre.** Avvisi sanitari sulle condizioni di emergenza. È più probabile che venga colpita l'intera popolazione.

NOx: visualizzare l'ossido di azoto e il biossido di azoto in tempo reale.

I significati dei colori delle barre di stato NOx sono i seguenti:

- **Verde (0–30): Buono.** I dati sono considerati soddisfacenti.
- **Giallo (31–150): Moderato.** I dati sono accettabili. Può verificarsi un problema di salute moderato per un numero molto ristretto di persone insolitamente sensibili.
- **Arancione (151–300): Insalubre per un gruppo sensibile.** Gli effetti sulla salute possono riguardare tutte le persone; i membri di gruppi sensibili possono subire effetti più gravi sulla salute.
- **Rosso (301–500): Insalubre.** Gli effetti sulla salute possono riguardare tutte le persone; i membri di gruppi sensibili possono subire effetti più gravi sulla salute.

PM 1.0: visualizzare le particelle 1.0 in tempo reale.

PM 2.5: visualizzare le particelle 2.5 in tempo reale.

I significati dei colori delle barre di stato PM 2.5 sono i seguenti:

- **Verde (0–9): Buono.** I dati sono considerati soddisfacenti.
- **Giallo (9.1–35.4): Moderato.** I dati sono accettabili. Può verificarsi un problema di salute moderato per un numero molto ristretto di persone insolitamente sensibili.
- **Arancione (35.5–55.4): Insalubre per un gruppo sensibile.** Gli effetti sulla salute possono riguardare tutte le persone; i membri di gruppi sensibili possono subire effetti più gravi sulla salute.
- **Rosso (55.5–125.4): Insalubre.** Gli effetti sulla salute possono riguardare tutte le persone; i membri di gruppi sensibili possono subire effetti più gravi sulla salute.
- **Viola (125.5–225.4): Molto insalubre.** Avvisi sanitari sulle condizioni di emergenza. È più probabile che venga colpita l'intera popolazione.
- **Rosso granata (225.5–1000): Pericoloso.** Condizioni di emergenza. È più probabile che venga colpita l'intera popolazione.

PM 4.0: visualizzare le particelle 4.0 in tempo reale.

PM 10.0: visualizzare le particelle 10.0 in tempo reale.

I significati dei colori delle barre di stato PM 10.0 sono i seguenti:

- **Verde (0–54): Buono.** I dati sono considerati soddisfacenti.
- **Giallo (55–154): Moderato.** I dati sono accettabili. Può verificarsi un problema di salute moderato per un numero molto ristretto di persone insolitamente sensibili.
- **Arancione (155–254): Insalubre per un gruppo sensibile.** Gli effetti sulla salute possono riguardare tutte le persone; i membri di gruppi sensibili possono subire effetti più gravi sulla salute.
- **Rosso (255–354): Insalubre.** Gli effetti sulla salute possono riguardare tutte le persone; i membri di gruppi sensibili possono subire effetti più gravi sulla salute.
- **Viola (355–424): Molto insalubre.** Avvisi sanitari sulle condizioni di emergenza. È più probabile che venga colpita l'intera popolazione.
- **Rosso granata (425–1000): Pericoloso.** Condizioni di emergenza. È più probabile che venga colpita l'intera popolazione.

Vapore di sigarette elettroniche/Fumo: visualizzare il vapore delle sigarette elettroniche o il fumo rilevato o non rilevato.

I significati dei colori delle barre di stato del vapore delle sigarette elettroniche/del fumo sono i seguenti:

- **Verde: Undetected (Non rilevato).** L'attività di vapore di sigarette elettroniche o di fumo sospetta non viene rilevata.
- **Rosso: Rilevato.** L'attività di vapore di sigarette elettroniche o di fumo sospetta viene rilevata.

VOC: visualizzare l'indice dei composti organici volatili.

I significati dei colori delle barre di stato VOC sono i seguenti:

- **Verde (0–100): Buono.** I dati sono considerati soddisfacenti.
- **Giallo (101–300): Moderato.** I dati sono accettabili. Può verificarsi un problema di salute moderato per un numero molto ristretto di persone insolitamente sensibili.

- **Arancione (301–400): Insalubre per un gruppo sensibile.** Gli effetti sulla salute possono riguardare tutte le persone; i membri di gruppi sensibili possono subire effetti più gravi sulla salute.
- **Rosso (401–500): Insalubre.** Gli effetti sulla salute possono riguardare tutte le persone; i membri di gruppi sensibili possono subire effetti più gravi sulla salute.

AQI: visualizzare l'indice di qualità dell'aria.

I significati dei colori delle barre di stato dell'AQI sono i seguenti:

- **Verde (0–50): Buono.** I dati sono considerati soddisfacenti.
- **Giallo (51–100): Moderato.** I dati sono accettabili. Può verificarsi un problema di salute moderato per un numero molto ristretto di persone insolitamente sensibili.
- **Arancione (101–150): Insalubre per un gruppo sensibile.** Gli effetti sulla salute possono riguardare tutte le persone; i membri di gruppi sensibili possono subire effetti più gravi sulla salute.
- **Rosso (151–200): Insalubre.** Gli effetti sulla salute possono riguardare tutte le persone; i membri di gruppi sensibili possono subire effetti più gravi sulla salute.
- **Viola (201–300): Molto insalubre.** Avvisi sanitari sulle condizioni di emergenza. È più probabile che venga colpita l'intera popolazione.
- **Rosso granata (301–500): Pericoloso.** Condizioni di emergenza. È più probabile che venga colpita l'intera popolazione.

Impostazioni

Soglia

Imposta i dati del sensore di qualità dell'aria.

Temperature (Temperatura): Impostare la temperatura **MIN** e **MAX** nell'intervallo tra -10 e 45.

Humidity (Umidità) : impostare l'umidità **MIN** e **MAX** nell'intervallo tra 0 e 100.

CO2 : impostare l'anidride carbonica **MIN** e **MAX** nell'intervallo tra 0 e 40000.

NOx : Impostare i valori **MIN** e **MAX** dell'ossido di azoto e il biossido di azoto nell'intervallo da 0 a 500.

PM1.0 : impostare i composti organici volatili 1.0 **MIN** e **MAX** nell'intervallo tra 0 e 1000.

PM2.5 : impostare i composti organici volatili 2.5 **MIN** e **MAX** nell'intervallo tra 0 e 1000.

PM4.0 : impostare i composti organici volatili 4.0 **MIN** e **MAX** nell'intervallo tra 0 e 1000.

PM10.0 : impostare i composti organici volatili **MIN** e **MAX** nell'intervallo tra 0 e 1000.

VOC : impostare l'indice dei composti organici volatili **MIN** e **MAX** nell'intervallo tra 0 e 500.

AQI : impostare l'indice di qualità dell'aria **MIN** e **MAX** entro l'intervallo tra 0 e 500.

Unità di temperatura

Show temperature in (Mostra temperatura in): Celsius o Fahrenheit

Sensibilità del rilevamento del vapore delle sigarette elettroniche

Imposta la sensibilità del rilevamento del vapore delle sigarette elettroniche.

Low sensitivity (Bassa sensibilità) ,High sensitivity (Alta sensibilità): Utilizza il cursore per regolare la differenza tra sensibilità bassa e sensibilità alta alla quale il dispositivo deve generare un allarme. Un'elevata sensibilità significa che il dispositivo rileverà anche piccole quantità di fumo o vapore di sigaretta elettronica e sarà più propenso ad attivare un allarme; una bassa sensibilità significa che risponderà solo a quantità maggiori di fumo o vapore, riducendo la possibilità di falso allarme.

Impostazioni archiviazione

- **Retention time 1 month, frequency 1s (Tempo di conservazione 1 mese, frequenza 1s):** i dati vengono raccolti ogni secondo e conservati solo per gli ultimi 30 giorni.
- **Retention time 3 month, frequency 5s (Tempo di conservazione 3 mesi, frequenza 5s):** i dati vengono raccolti ogni 5 secondi e conservati solo per gli ultimi 90 giorni.
- **Retention time 1 year, frequency 10s (Tempo di conservazione 1 anno, frequenza 10s):** i dati vengono raccolti ogni 10 secondi e conservati solo per gli ultimi 365 giorni.

Nota

Modificando l'opzione di archiviazione, i dati esistenti verranno cancellati.

Frequenza dei metadati cloud

La frequenza dei metadati cloud viene utilizzata dalle piattaforme di terze parti che desiderano sottoscrivere i metadati dei sensori con una frequenza di trasmissione regolabile. I metadati cloud includono tutti i dati dei sensori visualizzati sul dashboard.

Cloud metadata (Metadati cloud): Attiva per utilizzare i metadati cloud.

Nota

Per impostazione predefinita questa funzione è disabilitata; non vengono inviati metadati per l'argomento. Dopo l'abilitazione, i metadati relativi all'argomento vengono trasmessi nell'intervallo di frequenza impostato di seguito.

Set frequency range (Intervallo di frequenza impostato) (00:00:01 – 23:59:59): Immettere un valore per impostare l'intervallo di frequenza.

Periodo di convalida

È possibile impostare un periodo di convalida per le impostazioni relative alla qualità dell'aria riportate di seguito. Il periodo di convalida serve da soglia temporale e la lettura deve rimanere al di sopra del limite dell'intervallo del periodo di convalida per attivare un allarme.

Esempio

Se il periodo di convalida della CO₂ è di 5 secondi, il livello di CO₂ deve rimanere al di sopra del limite per tutti i 5 secondi affinché scatti l'allarme.

Impostare l'intervallo del periodo di convalida (0-60 secondi) per i dati riportati di seguito:

- Temperatura
- Umidità
- CO2
- NOx
- PM1.0
- PM2.5
- PM4.0
- PM10.0
- VOC
- AQI
- Vapore di sigarette elettroniche/fumo

Statistiche

Statistiche dei dati del sensore

È possibile esportare fino a 365 giorni di statistiche del sensore in un file CSV da utilizzare in applicazioni quali Microsoft® Excel.

- **Predefined date range (Intervallo di date predefinito):** per selezionare l'intervallo di date predefinito che si desidera scaricare dall'elenco.
- **From e To (Da, A):** per selezionare l'intervallo personalizzato che si desidera scaricare. È possibile scaricare i dati fino a 365 giorni.

Nota

Se vengono selezionati sia un intervallo personalizzato che uno predefinito, ha la precedenza l'intervallo personalizzato.

Nota

L'intervallo massimo di download è limitato dal tempo di conservazione configurato in .

- **Select a source (Seleziona una fonte):** per selezionare la fonte desiderata che si desidera scaricare.
- **Download data (Scarica dati):** per selezionare **Download selected sensor data (Scarica i dati del sensore selezionato)** dal menu a discesa.
- **Download data for all sources (Scarica dati per tutte le fonti):** per esportare tutti i dati di tutte le fonti nell'arco temporale selezionato.

Il file viene scaricato nella cartella dei download. Lo scaricamento potrebbe impiegare del tempo in base alle dimensioni del file.

Analitiche

AXIS Audio Analytics

Livello di pressione sonora

Show threshold and events in graph (Mostra la soglia e gli eventi nel grafico): Attivare per mostrare nel grafico quando è stato rilevato un picco sonoro.

Threshold (Soglia): Regolare i valori di soglia per il rilevamento. L'applicazione registrerà un evento audio per tutti i suoni che non rientrano nei valori di soglia.

Rilevamento di suoni adattivo

Show events in graph (Mostra eventi nel grafico): Attivare per mostrare nel grafico quando è stato rilevato un picco sonoro.

Threshold (Soglia): Muovere il cursore per adattare la soglia di rilevamento. Con la soglia minima, anche leggeri picchi sonori saranno registrati come rilevamento, mentre con la soglia massima solo picchi significativi saranno registrati come rilevamento.

Test alarms (Test allarmi): Fare clic su Test per l'attivazione di un evento di rilevamento ai fini di un test.

Classificazione audio

Show events in graph (Mostra eventi nel grafico)  : Attivare per visualizzare nel grafico quando è stato rilevato un tipo specifico di suono.

Classifications (Classificazioni)  : Selezionare quali tipi di suoni l'applicazione deve rilevare.

Test alarms (Test allarmi)  : Fare clic su Test (Test) per l'attivazione del rilevamento di un evento di un suono specifico ai fini di un test.

Audio

Impostazioni dispositivo

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

Input type (Tipo di ingresso)  : selezionare il tipo di input, ad esempio se si tratta di microfono interno o ingresso linea.

Power type (Tipo di alimentazione)  : Selezionare il tipo di alimentazione per l'input.

Apply changes (Applica modifiche)  : applicare la selezione.

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

Separate gain controls (Controlli del guadagno separati)  : Attiva per regolare il guadagno in modo separato per i diversi tipi di input.

Automatic gain control (Controllo automatico del guadagno)  : Attiva per adattare dinamicamente il guadagno alle modifiche del suono.

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

Output: Mostra il tipo di output.

Gain (Guadagno): Utilizzare il cursore per modificare il guadagno. Fai clic sull'icona dell'altoparlante per disattivare o attivare l'audio.

Controllo automatico del volume  : Attivare per fare in modo che il dispositivo regoli automaticamente e dinamicamente il guadagno in base al livello di rumore ambientale. Il controllo automatico del volume influisce su tutte le uscite audio, comprese linea e telecoil.

Flusso

Codifica: selezionare la codifica da usare per il flusso di sorgente input. È possibile scegliere la codifica solo se l'ingresso audio è attivato. Se l'ingresso audio è disattivato, fare clic su **Enable audio input (Abilita input audio)** per attivarlo.

Clip audio

 **Add clip (Aggiungi clip):** aggiungi una nuova clip audio. Puoi usare file .au, .mp3, .opus, .vorbis, .wav.

 Riproduci la clip audio.

Interrompi riproduzione della clip audio.



Il menu contestuale contiene:

- **Rename (Rinomina):** Modificare il nome della clip audio.
- **Create link (Crea collegamento):** creare un URL che, quando usato, riproduce la clip audio sul dispositivo. Specifica il volume e il numero di riproduzioni della clip.
- **Download (Scarica):** Scarica la clip audio sul tuo computer.
- **Elimina;** Elimina la clip audio dal dispositivo.

Ottimizzazione audio

Ingresso

Ten Band Graphic Audio Equalizer (Equalizzatore audio grafico a dieci bande): Attiva per la regolazione del livello delle diverse bande di frequenza in un segnale audio. Questa funzione è per utenti avanzati con esperienza nella configurazione audio.

Talkback range (Intervallo talkback)  : Scegli l'intervallo operativo per la raccolta dei contenuti audio. Un incremento dell'intervallo operativo provoca una riduzione delle capacità di comunicazione bidirezionale simultanea.

Voice enhancement (Ottimizzazione voce)  : Attiva per il miglioramento del contenuto vocale in relazione ad altri suoni.

Panoramica

Stato del LED di segnalazione

Consente di visualizzare le diverse attività del LED di segnalazione in esecuzione sul dispositivo. Nell'elenco di stato del LED di segnalazione ci possono essere fino a 10 attività contemporaneamente. Quando due o più

attività vengono eseguite contemporaneamente, l'attività con la priorità più alta mostra lo stato del LED di segnalazione. La riga verrà evidenziata nell'elenco di stato.

Stato dell'altoparlante audio

Visualizza le diverse attività dell'altoparlante audio in esecuzione sul dispositivo. Nell'elenco di stato dell'altoparlante audio 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.

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.



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

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

Nota

Non è possibile avere due profili con lo stesso nome.

- **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.
 - **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 con un numero compreso tra 1 e 10. Le attività con numeri di priorità superiori a 10 non possono essere rimosse dall'elenco di stato. Esistono tre attività con priorità superiore a 10; **Maintenance (Manutenzione)** (11), **Identify (Identifica)** (12) e **Health check (Controllo integrità)** (13).



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

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

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



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



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

Registrazioni

Registrazioni in corso: Mostrare tutte le registrazioni in corso.

- Iniziare una registrazione.



Scegliere una archiviazione di rete configurata.

- Interrompere una registrazione.

Le registrazioni attivate termineranno in caso di arresto manuale o in caso di spegnimento del dispositivo.

Le registrazioni continue continueranno fino all'arresto manuale. Anche se il dispositivo si arresta, la registrazione prosegue quando il dispositivo si avvia nuovamente.



Riproduci la registrazione.



Interrompi la riproduzione della registrazione.



Mostra o nascondi le informazioni e le opzioni sulla registrazione.

Set export range (Impostare l'intervallo di esportazione): Se vuoi esportare solo parte della registrazione, indica un intervallo di tempo. Notare che se si lavora in un fuso orario diverso rispetto alla posizione del dispositivo, l'intervallo di tempo si basa sul fuso orario del dispositivo.

Encrypt (Codifica): selezionare per impostare una password per le registrazioni esportate. Non è possibile aprire il file esportato senza la password.



Fare clic per eliminare una registrazione.

Export (Esporta): esporta l'intera registrazione o una sua parte.



Fare clic per filtrare le registrazioni.

From (Da): Mostra le registrazioni avvenute dopo un certo punto temporale.

To (A): Mostra le registrazioni fino a un certo punto temporale.

Source (Sorgente) ⓘ: mostra le registrazioni sulla base della sorgente. La sorgente si riferisce al sensore.

Event (Evento): mostra le registrazioni sulla base degli eventi.

Dispositivo di archiviazione: mostra le registrazioni in base al tipo di dispositivo di archiviazione.

Media

+ **Add (Aggiungi)**: Fare clic per aggiungere un nuovo file.

Punto di archiviazione: Selezionare per archiviare il file nella memoria interna o nell'archiviazione integrata (scheda SD, se disponibile).



Il menu contestuale contiene:

- **Informazioni**: Visualizza le informazioni sul file.
- **Copy link (Copia collegamento)**: Copiare il link alla posizione del file sul dispositivo.
- **Elimina**: Eliminare il file dal punto di archiviazione.

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.

Consenti app prive di firma  : Attiva per permettere che siano installate app senza firma.



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.

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

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

- **DHCP:** Adotta il fuso orario del server DHCP. Il dispositivo si deve connettere a un server DHCP prima di poter selezionare questa opzione.
- **Manual (Manuale):** Selezionare un fuso orario dall'elenco a discesa.

Nota

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

Ubicazione dei dispositivi

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

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

Rete

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.

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.

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.

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 -.

Abilitare gli aggiornamenti DNS dinamici: Consentire al proprio dispositivo di aggiornare automaticamente le registrazioni del server dei nomi di dominio ogni volta che cambia l'indirizzo IP.

Registra nome DNS: Inserire un nome dominio univoco che punti all'indirizzo IP del dispositivo. I caratteri consentiti sono A-Z, a-z, 0-9 e -.

TTL: il Time To Live (TTL) stabilisce per quanto tempo una registrazione DNS resta valida prima che debba essere aggiornata.

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 e HTTPS

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

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

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

Nota

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

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

Certificato: selezionare un certificato per abilitare HTTPS per il dispositivo.

Protocolli di individuazione in rete

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

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

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

LLDP e CDP: attivare per consentire il rilevamento automatico sulla rete. La disattivazione di LLDP e CDP può influire sulla negoziazione dell'alimentazione PoE. Per risolvere eventuali problemi con la negoziazione dell'alimentazione PoE, configurare lo switch PoE solo per la negoziazione dell'alimentazione PoE dell'hardware.

Proxy globali

Http proxy: specificare un host o un indirizzo IP del proxy globale secondo il formato consentito.

Https proxy: specificare un host o un indirizzo IP del proxy globale secondo il formato consentito.

Formati consentiti per i proxy http e https:

- `http(s)://host:porta`
- `http(s)://user@host:porta`
- `http(s)://user:pass@host:porta`

Nota

Riavviare il dispositivo per applicare le impostazioni proxy globali.

No proxy (Nessun proxy): Utilizzare **No proxy (Nessun proxy)** per bypassare i proxy globali. Immettere una delle opzioni dell'elenco o più opzioni separate da una virgola:

- Lasciare vuoto
- Indicare un indirizzo IP
- Indicare un indirizzo IP in formato CIDR
- Indicare un nome dominio, ad esempio: `www.<nome dominio>.com`
- Specificare tutti i sottodomini di un dominio specifico, ad esempio `.<nome dominio>.com`

Connessione al cloud con un clic

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

Allow O3C (Consenti O3C):

- **One-click:** Questa è l'opzione predefinita. Per connettersi a O3C, premere il pulsante di comando sul dispositivo. A seconda del modello di dispositivo, premere e rilasciare oppure tenere premuto, finché il LED di stato non lampeggia. Registrare il dispositivo con il servizio O3C entro 24 ore per abilitare **Always (Sempre)** e rimanere connessi. Se non si effettua la registrazione, il dispositivo si disconnette da O3C.
- **Sempre:** Il dispositivo tenta continuamente di collegarsi a un servizio O3C via Internet. Una volta registrato il dispositivo, questo rimane connesso. Utilizzare questa opzione se il pulsante di comando non è disponibile.
- **No:** disconnette dal 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.

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

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

Metodo di autenticazione:

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

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

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

Nota

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

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

Sicurezza

Certificati

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

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

Questi formati sono supportati:

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

Importante

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



Add certificate (Aggiungi certificato): fare clic sull'opzione per aggiungere un certificato. Si apre una guida passo dopo passo.

- Più  : mostra altri campi da compilare o selezionare.
- **Secure keystore (Archivio chiavi sicuro):** selezionare questa opzione per utilizzare **Trusted Execution Environment (SoC TEE)**, **Secure Element** 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/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) ⓘ:

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

Controllo degli accessi di rete e crittografia

IEEE 802.1x

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

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

IEEE 802.1AE MACsec

IEEE 802.1AE MACsec rappresenta uno standard IEEE per la sicurezza MAC (Media Access Control) che definisce la riservatezza e l'integrità dati senza connessione per i protocolli indipendenti di accesso ai media.

Certificati

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

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

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

Metodo di autenticazione: selezionare un tipo EAP impiegato per l'autenticazione.

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.

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

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

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

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

Le impostazioni sono a disposizione solo se si usa IEEE 802.1x PEAP-MSCHAPv2 come metodo di autenticazione:

- **Password:** immettere la password per l'identità utente.
- **Peap version (Versione Peap):** selezionare la versione Peap utilizzata nello switch di rete.
- **Label (Etichetta):** Selezionare 1 per utilizzare la codifica EAP del client; selezionare 2 per utilizzare la crittografia PEAP del client. Selezionare l'etichetta usata dallo switch di rete quando si utilizza Peap versione 1.

Le impostazioni sono a disposizione solo se si usa IEEE 802.1ae MACsec (chiave Static CAK/Pre-Shared) come metodo di autenticazione:

- **Key agreement connectivity association key name (Nome della chiave di associazione della connettività del contratto chiave):** immettere il nome dell'associazione della connettività (CKN). Deve essere composto da 2 a 64 caratteri esadecimali (divisibili per 2). Il CKN deve essere configurato manualmente nell'associazione della connettività e deve corrispondere su entrambe le estremità del collegamento per abilitare inizialmente MACsec.
- **Key agreement connectivity association key (Chiave di associazione della connettività del contratto chiave):** immettere la chiave di associazione della connettività (CAK). Deve essere composta da 32 o 64 caratteri esadecimali. Il CAK deve essere configurato manualmente nell'associazione della

connettività e deve corrispondere su entrambe le estremità del collegamento per abilitare inizialmente MACsec.

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): Immettere il numero di secondi per cui si blocca un attacco di forza bruta.

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

Firewall

Firewall: Attivare per abilitare il firewall.

Default Policy (Criterio predefinito): Selezionare come si desidera che il firewall gestisca le richieste di connessione non coperte da regole.

- **ACCEPT: (ACCETTA)** Permette tutte le connessioni al dispositivo. Questa opzione è impostata per impostazione predefinita.
- **DROP (BLOCCA):** Blocca tutte le connessioni al dispositivo.

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

+ New rule (+ Nuova regola): Fare clic per la creazione di una regola.

Rule type (Tipo di regola):

- **FILTER (FILTRO):** Selezionare per consentire o bloccare le connessioni dai dispositivi che corrispondono ai criteri definiti nella regola.
 - **Policy (Criteri):** Selezionare **Accept (Accetta)** o **Drop (Blocca)** per la regola del firewall.
 - **IP range (Intervallo IP):** Selezionare per specificare un intervallo di indirizzi da consentire o bloccare. Utilizzare IPv4/IPv6 in **Start (Inizio)** e **End (Fine)**.
 - **Indirizzo IP:** Immettere l'indirizzo che si desidera consentire o bloccare. Usare il formato IPv4/IPv6 o CIDR.
 - **Protocol (Protocollo):** Selezionare un protocollo di rete (TCP, UDP o entrambi) da consentire o bloccare. Se si seleziona un protocollo, è necessario specificare anche una porta.
 - **MAC:** inserire l'indirizzo MAC di un dispositivo che si desidera consentire o bloccare.
 - **Intervallo porta:** Selezionare per specificare l'intervallo di porte da consentire o bloccare. Aggiungerlo in **Start (Inizio)** e **End (Fine)**.
 - **Porta:** Inserire un numero di porta che si desidera consentire o bloccare. I numeri di porta devono essere compresi tra 1 e 65535.
 - **Traffic type (Tipo di traffico):** Selezionare il tipo di traffico che si desidera consentire o bloccare.
 - **UNICAST:** traffico da un singolo mittente a un singolo destinatario.
 - **BROADCAST (Broadcasting):** traffico da un singolo mittente a tutti i dispositivi della rete.
 - **MULTICAST:** traffico da uno o più mittenti a uno o più destinatari.
- **LIMIT (LIMITE):** Selezionare per accettare le connessioni dai dispositivi che corrispondono ai criteri definiti nella regola, ma applicare dei limiti per ridurre il traffico eccessivo.
 - **IP range (Intervallo IP):** Selezionare per specificare un intervallo di indirizzi da consentire o bloccare. Utilizzare IPv4/IPv6 in **Start (Inizio)** e **End (Fine)**.
 - **Indirizzo IP:** Immettere l'indirizzo che si desidera consentire o bloccare. Usare il formato IPv4/IPv6 o CIDR.
 - **Protocol (Protocollo):** Selezionare un protocollo di rete (TCP, UDP o entrambi) da consentire o bloccare. Se si seleziona un protocollo, è necessario specificare anche una porta.
 - **MAC:** inserire l'indirizzo MAC di un dispositivo che si desidera consentire o bloccare.
 - **Intervallo porta:** Selezionare per specificare l'intervallo di porte da consentire o bloccare. Aggiungerlo in **Start (Inizio)** e **End (Fine)**.
 - **Porta:** Inserire un numero di porta che si desidera consentire o bloccare. I numeri di porta devono essere compresi tra 1 e 65535.
 - **Unit (Unità):** Selezionare il tipo di connessioni da consentire o bloccare.
 - **Period (Periodo):** Selezionare il periodo di tempo relativo a **Amount (Quantità)**.
 - **Amount (Quantità):** Impostare il numero massimo di volte in cui un dispositivo è autorizzato a connettersi entro il **Period (Periodo)** impostato. La quantità massima è 65535.

- **Burst (Eccezione):** Immettere il numero di connessioni che possono superare la **Amount (Quantità)** una volta durante il **Period (periodo)** impostato. Una volta raggiunto il numero, è consentita solo la quantità impostata durante il periodo stabilito.
- **Traffic type (Tipo di traffico):** Selezionare il tipo di traffico che si desidera consentire o bloccare.
 - **UNICAST:** traffico da un singolo mittente a un singolo destinatario.
 - **BROADCAST (Broadcasting):** traffico da un singolo mittente a tutti i dispositivi della rete.
 - **MULTICAST:** traffico da uno o più mittenti a uno o più destinatari.

Test rules (Testa regole): Fare clic per testare le regole definite.

- **Time in seconds: (Tempo di test in secondi):** Impostare un limite di tempo al fine di mettere alla prova le regole.
- **Roll back:** Fare clic per riportare il firewall allo stato precedente, prima di aver testato le regole.
- **Apply rules (Applica regole):** Fare clic su per attivare le regole senza eseguire il test. Si sconsiglia questa procedura.

Certificato AXIS con firma personalizzata

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

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

⋮

Il menu contestuale contiene:

- **Delete certificate (Elimina certificato):** Elimina il certificato.

Account

Account

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

Account: Inserire un nome account univoco.

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

Repeat password (Ripeti password): Immettere 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)**.
- **Viewer (Visualizzatore):** non ha l'accesso alla modifica di alcuna impostazioni.

⋮
• Il menu contestuale contiene:

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

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

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.

- **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): Immettere di nuovo la stessa password.

Commento: Inserire un commenti (facoltativo).

⋮
• Il menu contestuale contiene:

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

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

Virtual host (Host virtuale)

 **Add virtual host (Aggiungi host virtuale):** fare clic su questa opzione per aggiungere un nuovo host virtuale.

Abilitata: selezionare questa opzione per utilizzare l'host virtuale.

Server name (Nome del server): inserire il nome del server. Utilizzare solo i numeri da 0 a 9, le lettere dalla A alla Z e il trattino (-).

Porta: inserire la porta a cui è connesso il server.

Tipo: selezionare il tipo di autenticazione da utilizzare. Scegliere tra **Basic (Base)**, **Digest** e **Open ID**.



Il menu contestuale contiene:

- **Update (Aggiorna):** aggiornare l'host virtuale.
- **Elimina;** eliminare l'host virtuale.

Disabled (Disabilitato): il server è disabilitato.

Configurazione concessione credenziali client

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

Verification URI (URI di verifica): inserire il collegamento Web per l'autenticazione dell'endpoint API.

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.

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

Configurazione OpenID

Importante

Se non è possibile utilizzare OpenID per eseguire l'accesso, utilizzare le credenziali Digest o Basic utilizzate quando è stato configurato OpenID per eseguire l'accesso.

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

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

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

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

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

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

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

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

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

Client secret (Segreto client): inserire la password OpenID

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

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

Eventi

Regole

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

Nota

Puoi creare un massimo di 256 regole di azione.



Aggiungere una regola: Creare una regola.

Nome: Immettere un nome per la regola.

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

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

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

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



Aggiungere una condizione: fare clic per l'aggiunta di un'ulteriore condizione.

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

Destinatari

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

Nota

Se si imposta il dispositivo per l'utilizzo di FTP o SFTP, non modificare o rimuovere il numero di sequenza univoco aggiunto ai nomi dei file. Se ciò accadesse sarebbe possibile inviare solo un'immagine per evento.

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.

Nome: immettere un nome per il destinatario.

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

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

 - **Host:** Immettere il nome host o l'indirizzo IP per il dispositivo di archiviazione di rete.
 - **Condivisione:** Immettere il nome della condivisione nell'host.

- **Folder (Cartella):** inserisci il percorso alla directory nella quale vuoi conservare i file.
- **Username (Nome utente):** immettere il nome utente per l'accesso.
- **Password:** immettere la password per l'accesso.
- **SFTP** 
 - **Host:** Inserire l'indirizzo IP o il nome host del server. Se inserisci un nome host, accertati che sia specificato un server DNS in **System > Network > IPv4 and IPv6 (Sistema > Rete > IPv4 e IPv6)**.
 - **Porta:** Immettere il numero della porta utilizzata dal server SFTP. Quello predefinito è 22.
 - **Folder (Cartella):** inserisci il percorso alla directory nella quale vuoi conservare i file. Se questa directory non esiste già sul server SFTP, durante il caricamento dei file riceverai un messaggio di errore.
 - **Username (Nome utente):** immettere il nome utente per l'accesso.
 - **Password:** immettere la password per l'accesso.
 - **SSH host public key type (MD5) (Tipo di chiave pubblica host SSH (MD5)):** Immetti l'impronta digitale della chiave pubblica dell'host remoto (una stringa di 32 cifre 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 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.
- **E-mail**
 - **Send email to (Invia e-mail a):** Inserire l'indirizzo e-mail a cui inviare i messaggi e-mail. Per immettere più indirizzi, separarli utilizzando le virgole.
 - **Send email from (Invia e-mail da):** immettere l'indirizzo e-mail del server mittente.
 - **Username (Nome utente):** Immettere il nome utente per il server mail. Lasciare vuoto questo campo se il server mail non necessita di autenticazione.
 - **Password:** Immettere la password per il server mail. Lasciare vuoto questo campo se il server mail non necessita di autenticazione.

- **Email server (SMTP) – Server e-mail (SMTP):** inserire il nome del server SMTP, ad esempio, smtp.gmail.com, smtp.mail.yahoo.com.
- **Porta:** immettere il numero della porta per il server SMTP, utilizzando i valori nell'intervallo da 0 a 65535. Il valore predefinito è 587.
- **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 di e-mail dispongono di filtri di sicurezza che impediscono agli utenti di ricevere o visualizzare grandi quantità di allegati, ricevere 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)**.
 - **Port (Porta):** Immettere il numero della porta utilizzata per l'accesso al server.

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



Il menu contestuale contiene:

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

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

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

Pianificazioni

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



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

Trigger manuali

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

MQTT

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

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

Per maggiori informazioni relative a MQTT consultare l'*AXIS OS Knowledge base*.

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.

Client MQTT

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

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

Broker

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

Protocol (Protocollo): Selezionare il protocollo da utilizzare.

Porta: Immettere il numero di porta.

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

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

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

Password: immettere una password per il nome utente.

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

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

HTTP proxy (Proxy HTTP): Un URL dotato di una lunghezza non superiore a 255 byte. È possibile lasciare il campo vuoto se non si vuole usare un proxy HTTP.

HTTPS proxy (Proxy HTTPS): Un URL dotato di una lunghezza non superiore a 255 byte. È possibile lasciare il campo vuoto se non si vuole usare un proxy HTTPS.

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

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

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

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

Messaggio connessione

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

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

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

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

Payload: Immettere il contenuto per il messaggio predefinito.

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

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

Messaggio di ultime volontà e testamento

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

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

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

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

Payload: Immettere il contenuto per il messaggio predefinito.

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

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

Pubblicazione MQTT

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

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

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

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



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

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

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

QoS: Seleziona il livello desiderato per la pubblicazione MQTT.

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.

SIP

Impostazioni

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

SIP setup assistant (Assistente alla configurazione SIP): fare clic su questa opzione per impostare e configurare SIP passo dopo passo.

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

Permetti chiamate in entrata: Selezionare questa opzione per consentire le chiamate in arrivo da altri dispositivi SIP.

Gestione chiamate

- **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.

Porte

Un numero di porta deve essere compreso tra 1024 e 65 535.

- **Porta SIP:** La 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 differente.
- **Porta TLS:** La porta di rete utilizzata per la comunicazione SIP codificata. Il traffico di segnalazione attraverso la porta viene crittografato tramite TLS (Transport Layer Security). Il numero di porta predefinito è 5061. Se necessario, inserire un numero di porta differente.
- **Porta di avvio RTP:** porta di rete utilizzata per il primo flusso multimediale RTP in una chiamata SIP. Il numero di porta per l'inizio predefinito è 4000. Alcuni firewall bloccano il traffico RTP su determinati numeri di porta.

NAT Traversal

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 la 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 un indirizzo server STUN, ad esempio un indirizzo IP.
- **TURN:** TURN (Traversal Using Relays around NAT) è un protocollo che consente a un dispositivo dietro un router NAT o un firewall di ricevere i dati in entrata da altri host su TCP o UDP. Inserire l'indirizzo server TURN e le informazioni di login.
- **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.

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 1300 byte.

- **Allow via rewrite (Consenti tramite riscrittura):** Seleziona per inviare l'indirizzo IP locale e non l'indirizzo IP pubblico del router.
- **Allow contact rewrite (Consenti riscrittura contatto):** Seleziona per inviare l'indirizzo IP locale e non l'indirizzo IP pubblico del router.
- **Register with server every (Registra con il server ogni):** Consente di impostare la frequenza con cui si desidera che il dispositivo registri con il server SIP per gli account SIP esistenti.
- **DTMF payload type (Tipo payload DTMF):** Modifica il tipo di payload predefinito per DTMF.
- **Max retransmissions (Massimo numero di ritrasmissioni):** Imposta il numero massimo di volte in cui il dispositivo tenta di connettersi al server SIP prima di smettere di provare.
- **Seconds until failback (Secondi fino al failback):** Imposta il numero di secondi entro i quali il dispositivo tenta di riconnettersi al server SIP primario dopo aver effettuato il failover su un server SIP secondario.

Account

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

- L'account viene registrato con successo con il server SIP.
- È stato riscontrato un 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. L'account predefinito viene sempre utilizzato quando si effettua una chiamata API (interfaccia per la programmazione di applicazioni) VAPIX® senza specificare da quale account SIP effettuare la chiamata.



Add account (Aggiungi account): Fai 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 (assegnare le 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.
- **Nome:** Immettere un nome descrittivo. Ciò può essere, ad esempio, il nome e il cognome, un ruolo o una posizione. Il nome non è univoco.
- **ID utente:** immettere il numero di telefono o estensione univoci assegnati al dispositivo.
- **Peer-to-peer:** utilizzare questo account per le chiamate dirette a un altro dispositivo SIP nella rete locale.
- **Registrato:** utilizzare questo account per le chiamate a dispositivi SIP al di fuori della rete locale, tramite un server SIP.
- **Domain (Dominio):** se disponibile, immettere il nome dominio pubblico. Tale nome verrà visualizzato come parte dell'indirizzo SIP durante la chiamata ad altri account.
- **Password:** Immettere la password associata con l'account SIP per effettuare l'autenticazione sul server SIP.
- **ID di autenticazione:** immettere l'ID autenticazione utilizzato per l'autenticazione al server SIP. Se è lo stesso dell'ID utente, non è necessario immettere l'ID autenticazione.
- **ID chiamante:** nome indicato al destinatario delle chiamate dal dispositivo.
- **Registrar:** immettere l'indirizzo IP per l'account registrar.
- **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):** attiva 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.
- **Proxy**
 -  **Proxy:** fare clic sull'opzione per aggiungere un proxy.
 - **Prioritize (Dai priorità):** se sono stati aggiunti due o più proxy, fare clic per assegnare la relativa priorità.
 - **Server address (Indirizzo server):** immettere l'indirizzo IP del server proxy SIP.
 - **Username (Nome utente):** se richiesto, immettere il nome utente per il server proxy SIP.
 - **Password:** se necessario, immettere la password per il server proxy SIP.
- **Video **
 - **View area (Area di visione):** selezionare l'area di visione da utilizzare per le chiamate video. Se si seleziona Nessuna, viene utilizzata la visualizzazione nativa.
 - **Risoluzione:** selezionare la risoluzione da utilizzare per le chiamate video. La risoluzione influisce sulla larghezza di banda necessaria.
 - **Frequenza dei fotogrammi:** selezionare il numero di fotogrammi al secondo per le chiamate video. La velocità in fotogrammi influisce sulla larghezza di banda necessaria.
 - **Profilo H.264:** selezionare il profilo da utilizzare per le chiamate video.

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)**.

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.

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 sul livello dell'applicazione, in genere correlate alla sessione.

Chiamata di prova

Account SIP: Seleziona da quale account eseguire la chiamata di prova.

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

Elenco di accessi

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 sorgente): fare clic per creare una nuova voce nell'elenco di accesso.

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

Controller multicast

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

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



Source (Sorgente): Aggiungere un nuova sorgente controller multicast.

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



Il menu contestuale contiene:

Edit (Modifica): Modifica la sorgente controller multicast.

Elimina; Eliminare l'origine del dispositivo di controllo multicast.

Archiviazione

Archiviazione di rete

Ignore (Ignora): Attiva per ignorare l'archiviazione di rete.

Add network storage (Aggiungi archiviazione di rete): fare clic su questa opzione per eseguire l'aggiunta di una condivisione di rete nella quale poter salvare le registrazioni.

- **Indirizzo:** Inserire l'indirizzo IP o il nome host del server host, generalmente NAS (Network Attached Storage). Si consiglia di configurare l'host per utilizzare un indirizzo IP fisso (non DHCP perché un indirizzo IP dinamico potrebbe cambiare) o di utilizzare DNS. I nomi Windows SMB/CIFS non sono supportati.
- **Network share (Condivisione di rete):** Inserire il nome dell'ubicazione condivisa nel server host. Diversi dispositivi Axis possono utilizzare la stessa condivisione di rete dal momento che ogni dispositivo ha una propria cartella.
- **User (Utente):** inserire il nome utente se serve eseguire il login per il server. Digitare DOMAIN \username per accedere a un server di dominio specifico.
- **Password:** Immetti la password se serve eseguire il login per il server.
- **SMB version (Versione SMB):** Seleziona la versione del protocollo di archiviazione SMB da collegare al NAS. Se selezioni **Auto (Automatico)**, il dispositivo cerca di negoziare una delle versioni sicure SMB: 3.02, 3.0, o 2.1. Seleziona 1.0 o 2.0 per la connessione a NAS meno recenti che non sono dotati di supporto per versioni superiori. Puoi leggere maggiori dettagli sul supporto SMB nei dispositivi Axis *qui*.
- **Add share without testing (Aggiungi condivisione senza test):** seleziona questa opzione per eseguire l'aggiunta della condivisione di rete a prescindere dal rilevamento di un errore durante il test della connessione. Ad esempio, l'errore può consistere nel non aver inserito una password nonostante sia necessaria per il server.

Remove network storage (Rimuovi archiviazione di rete): Fare clic su questa opzione per smontare, disassociare ed eseguire la rimozione della connessione alla condivisione di rete. Ciò elimina ogni impostazione per la condivisione di rete.

Unbind (Disassocia): fare clic per annullare l'associazione e scollegare la condivisione di rete.

Bind (Associa): Fare clic per associare e connettere la condivisione di rete.

Unmount (Smonta): Fare clic per smontare la condivisione di rete.

Mount (Monta): Fare clic su questa opzione per montare la condivisione di rete.

Write protect (Proteggi da scrittura): attiva questa opzione per interrompere la scrittura nella condivisione di rete e proteggere le registrazioni dalla rimozione. Una condivisione di rete protetta da scrittura non può essere formattata.

Retention time (Tempo di conservazione): Selezionare il periodo di conservazione delle registrazioni in modo da porre un limite al numero di vecchie registrazioni od ottemperare alle normative in merito alla conservazione dei dati. Le registrazioni precedenti sono cancellate prima della scadenza del periodo selezionato se l'archiviazione di rete diventa piena.

Strumenti

- **Test connection (Verifica connessione):** Verifica la connessione alla condivisione di rete.
- **Format (Formatta):** Formattare la condivisione di rete, ad esempio quando è necessario cancellare rapidamente tutti i dati. CIFS è l'opzione del file system disponibile.

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

Profili di flusso

Un profilo di streaming è un gruppo di impostazioni che incidono sul flusso video. Puoi usare i profili di streaming in situazioni diverse, ad esempio quando crei eventi e usi regole per registrare.



Add stream profile (Aggiungi profilo di streaming): Fare clic per creare un nuovo profilo di streaming.

Preview (Anteprima): Un'anteprima del flusso video con le impostazioni del profilo di streaming che selezioni. L'anteprima si aggiorna quando cambi le impostazioni nella pagina. Se il dispositivo ha aree di visione diverse, puoi cambiare l'area di visione nell'elenco a discesa nell'angolo in basso a sinistra dell'immagine.

Nome: aggiungi un nome per il tuo profilo.

Description (Descrizione): aggiungi una descrizione del tuo profilo.

Video codec (Codec video): selezionare il codec video che va applicato al profilo.

Risoluzione: Consulta per vedere una descrizione di questa impostazione.

Frequenza dei fotogrammi: Consulta per vedere una descrizione di questa impostazione.

Compressione: Consulta per vedere una descrizione di questa impostazione.

Zipstream  : Consulta per vedere una descrizione di questa impostazione.

Optimize for storage (Ottimizza per archiviazione)  : Consulta per vedere una descrizione di questa impostazione.

Dynamic FPS (FPS dinamico)  : Vedere per una descrizione di questa impostazione.

Dynamic GOP (GOP dinamico)  : Vedere per una descrizione di questa impostazione.

Mirror (Specularità)  : Consulta per vedere una descrizione di questa impostazione.

GOP length (Lunghezza GOP)  : Consulta per vedere una descrizione di questa impostazione.

Bitrate control (Controllo velocità di trasmissione): Consulta per vedere una descrizione di questa impostazione.

Include overlays (Includi sovrapposizioni)  : Selezionare il tipo di sovrapposizione da includere. Consulta per informazioni su come aggiungere sovrapposizioni.

Include audio (Includi audio)  : Consulta per vedere una descrizione di questa impostazione.

ONVIF

Account ONVIF

ONVIF (Open Network Video Interface Forum) è uno standard di interfaccia globale che rende più semplice a utenti finali, integratori, consulenti e produttori di avvalersi delle possibilità offerte dalla tecnologia video di rete. ONVIF consente interoperabilità tra dispositivi di fornitori differenti, massima flessibilità, costi ridotti e sistemi a prova di futuro.

Quando si crea un account ONVIF, la comunicazione ONVIF è abilitata automaticamente. Utilizzare il nome account e la password per tutte le comunicazioni ONVIF con il dispositivo. Per ulteriori informazioni, visitare l'Axis Developer Community sul sito Web axis.com.



Add accounts (Aggiungi account): Per creare un nuovo account ONVIF.

Account: Inserire un nome account univoco.

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

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

Role (Ruolo):

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



Il menu contestuale contiene:

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

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

Profili di supporti ONVIF

Un profilo di supporti ONVIF è costituito da una serie di configurazioni utilizzabili per modificare le impostazioni di flusso dei supporti. Puoi creare nuovi profili con il tuo set di configurazioni o utilizzare profili preconfigurati per una configurazione rapida.



Aggiungere profilo multimediale: Fare clic per aggiungere un nuovo profilo di supporti ONVIF.

Nome profilo: Aggiungi un nome per il profilo multimediale.

Video source (Sorgente video): Seleziona la sorgente video per la tua configurazione.

- **Select configuration (Selezionare configurazione):** Selezionare una configurazione definita dall'utente dall'elenco. Le configurazioni nell'elenco a discesa corrispondono ai canali video del dispositivo, comprese le multiview, le aree di visione e i canali virtuali.

Video encoder (Codificatore video): Selezionare il formato di codifica video per la tua configurazione.

- **Select configuration (Selezionare configurazione):** Selezionare una configurazione definita dall'utente dall'elenco e regolare le impostazioni di codifica. Le configurazioni nell'elenco a discesa fungono da identificatori/nomi della configurazione del video encoder. Selezionare l'utente da 0 a 15 per applicare le tue impostazioni oppure selezionare uno degli utenti predefiniti se si desidera utilizzare le impostazioni predefinite per un formato di codifica specifico.

Nota

Abilita l'audio nel dispositivo per avere la possibilità di selezionare una sorgente audio e la configurazione del codificatore audio.

Audio source (Sorgente audio)  : Selezionare la sorgente di ingresso audio per la tua configurazione.

- **Select configuration (Selezionare configurazione):** Selezionare una configurazione definita dall'utente dall'elenco e regolare le impostazioni audio. Le configurazioni nell'elenco a discesa corrispondono agli ingressi audio del dispositivo. Se il dispositivo ha un ingresso audio, è user0. Se il dispositivo dispone di più ingressi audio, nell'elenco saranno presenti altri utenti.

Codificatore audio  : Selezionare il formato di codifica audio per la tua configurazione.

- **Select configuration (Selezionare configurazione):** Selezionare una configurazione definita dall'utente dall'elenco e regolare le impostazioni di codifica audio. Le configurazioni nell'elenco a discesa fungono da identificatori/nomi della configurazione dell'audio encoder.

Decoder audio  : Selezionare il formato di codifica audio per la tua configurazione.

- **Select configuration (Selezionare configurazione):** Selezionare una configurazione definita dall'utente dall'elenco e regolare le impostazioni. Le configurazioni nell'elenco a discesa fungono da identificatori/nomi della configurazione.

Uscita audio  : Selezionare il formato di uscita audio per la tua configurazione.

- **Select configuration (Selezionare configurazione):** Selezionare una configurazione definita dall'utente dall'elenco e regolare le impostazioni. Le configurazioni nell'elenco a discesa fungono da identificatori/nomi della configurazione.

Metadata: Selezionare i metadati da includere nella configurazione.

- **Select configuration (Selezionare configurazione):** Selezionare una configurazione definita dall'utente dall'elenco e regolare le impostazioni dei metadati. Le configurazioni nell'elenco a discesa fungono da identificatori/nomi della configurazione dei metadati.

PTZ  : Selezionare le impostazioni PTZ per la tua configurazione.

- **Select configuration (Selezionare configurazione):** Selezionare una configurazione definita dall'utente dall'elenco e regolare le impostazioni PTZ. Le configurazioni nell'elenco a discesa corrispondono ai canali video del dispositivo con supporto PTZ.

Create (Crea): Fare clic per salvare le impostazioni e creare il profilo.

Cancel (Annulla): Fare clic per annullare la configurazione e cancellare tutte le impostazioni.

profile_x (profilo_x): Fare clic sul nome del profilo per aprire e modificare il profilo preconfigurato.

Rilevatori

Rilevamento audio

Queste impostazioni sono disponibili per ogni ingresso audio.

Sound level (Volume sonoro): Regolare il volume sonoro su un valore da 0 a 100, dove 0 è la sensibilità massima e 100 quella minima. Quando si imposta il volume sonoro, utilizzare l'indicatore relativo all'attività come riferimento. Quando crei eventi, puoi usare il volume sonoro come condizione. Puoi scegliere di attivare un'azione se il volume sonoro è superiore, inferiore o corrispondente al valore impostato.

Sensore PIR

Il sensore PIR esegue la misurazione della luce IR irradiata dagli oggetti nel suo campo visivo.

Sensitivity level (Livello di sensibilità): Regola il livello su un valore da 0 a 100, dove 0 è la sensibilità minima e 100 quella massima.

Impostazioni energetiche

Stato alimentazione

Mostra informazioni relative allo stato dell'alimentazione. Le informazioni differiscono in base al dispositivo.

Accessori

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.

Porta

Nome: modificare il testo per rinominare la porta.

Direction:  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 VCC.

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

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.

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.
- **View the audit log (Visualizza il registro audit):** Fare clic per visualizzare le informazioni relative alle attività dell'utente e del sistema, ad esempio autenticazioni e configurazioni riuscite oppure no.

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

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

- Axis
- RFC 3164
- RFC 5424

Protocol (Protocollo): Selezionare il protocollo da utilizzare:

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

Porta: Cambiare il numero di porta per impiegare una porta diversa.

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

Tipo: Selezionare il tipo di log che si desidera inviare.

Test server setup (Test della configurazione del server): Inviare un messaggio di prova a tutti i server prima di salvare le impostazioni.

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

Configurazione normale

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

Manutenzione

Manutenzione

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

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

Importante

Dopo il ripristino, le uniche impostazioni salvate sono:

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

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

Nota

Tutti i software per dispositivi Axis sono firmati digitalmente per assicurare di installare solo software verificato sul dispositivo. Ciò aumenta ulteriormente il livello di sicurezza informatica minimo globale dei dispositivi Axis. Per ulteriori informazioni, visitare il white paper "Axis Edge Vault" su axis.com.

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

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

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

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

Risoluzione di problemi

Reset PTR (Reimposta PTR)  : reimpostare PTR se per qualche motivo le impostazioni di **Pan (Panoramica)**, **Tilt (Inclinazione)**, o **Roll (Rotazione)** non funzionano come desiderato. I motori PTR sono sempre calibrati in una nuova telecamera. Tuttavia, la calibrazione può essere persa, ad esempio, se la telecamera perde alimentazione o se i motori vengono spostati manualmente. Quando si reimposta il PTR, la telecamera viene calibrata nuovamente e torna al valore predefinito di fabbrica.

Calibration (Calibrazione)  : Fare clic su **Calibrate (Calibra)** per ricalibrare i motori di panoramica, inclinazione e rotazione nelle rispettive posizioni predefinite.

Ping: Per verificare se il dispositivo è in grado di raggiungere un indirizzo specifico, inserire il nome host o l'indirizzo IP dell'host su cui si desidera eseguire un ping e fare clic su **Start (Avvia)**.

Controllo porta: Per verificare la connettività dal dispositivo a un indirizzo IP e a una porta TCP/UDP specifici, immettere il nome host o l'indirizzo IP e il numero di porta da controllare e fare clic su **Start (Avvia)**.

Analisi della rete

Importante

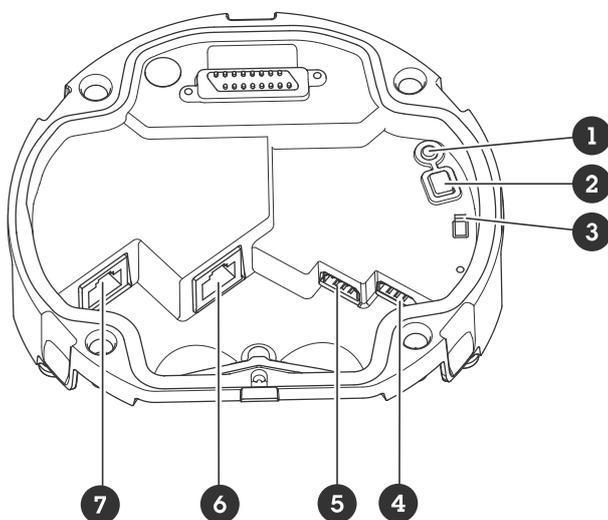
È possibile che un file di analisi della rete contenga informazioni riservate, come certificati o password.

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

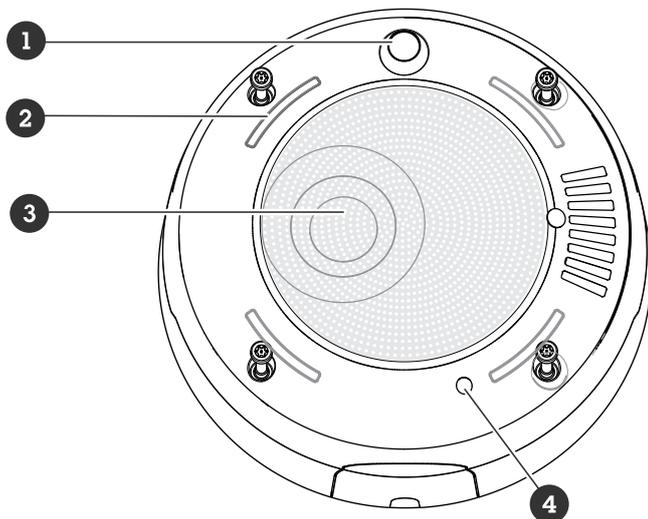
Trace time (Tempo di analisi): Selezionare la durata dell'analisi in secondi o minuti e fare clic su **Download**.

Dati tecnici

Panoramica dei prodotti



- 1 *Indicatore LED di stato*
- 2 *Pulsante di comando*
- 3 *Interruttore microfono*
- 4 *Connettore I/O*
- 5 *Connettore RS-485*
- 6 *Connettore di rete (PoE OUT)*
- 7 *Connettore di rete (PoE IN)*



- 1 *Sensore PIR*
- 2 *LED di segnalazione*
- 3 *Altoparlante*
- 4 *Microfono interno*

LED di stato

LED di stato	Significato
Spento	Spento per condizioni di normale funzionamento.
Verde	Luce fissa per 10 secondi per il normale funzionamento una volta completato l'avvio.
Giallo	Luce fissa durante l'avvio. Lampeggia durante l'aggiornamento del software del dispositivo o il ripristino delle impostazioni predefinite.
Giallo/rosso	Lampeggia se il collegamento di rete non è disponibile o si è interrotto.

Pulsanti

Pulsante di comando

Il pulsante di comando viene utilizzato per:

- Ripristino del dispositivo alle impostazioni predefinite di fabbrica. Vedere .

Interruttore microfono

Per la posizione dello switch del microfono, vedere .

Lo switch del microfono viene utilizzato per posizionare il microfono meccanicamente su **ON** oppure **OFF**. L'impostazione predefinita di fabbrica per questo switch è **OFF**.

Connettori

Connettore di rete

Ingresso: Connettore Ethernet RJ45 con Power over Ethernet (PoE).

Documentazione prodotta: Connettore Ethernet RJ45 con Power over Ethernet (PoE).

Connettore I/O

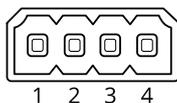
Utilizzare il connettore I/O con dispositivi esterni in combinazione con, ad esempio, rilevamento movimento, attivazione di eventi e notifiche di allarme. Oltre al punto di riferimento 0 V CC e all'alimentazione (output 12 V CC), il connettore I/O fornisce l'interfaccia per:

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

Input supervisionato - Consente di rilevare le manomissioni su un input digitale.

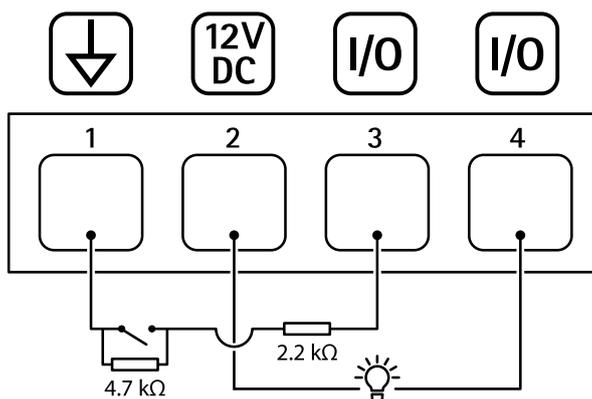
Uscita digitale - Per il collegamento di dispositivi esterni come relè e LED. I dispositivi collegati possono essere attivati tramite l'API (interfaccia per la programmazione di applicazioni) VAPIX® attraverso un evento oppure dall'interfaccia Web del dispositivo.

Morsettiera a 4 pin



Funzione	Pin	Note	Dati tecnici
Terra CC	1		0 V CC
Uscita CC	2	 <p>Questo terminale può essere utilizzato anche per alimentare una periferica ausiliaria. Nota: questo pin può essere usato solo come uscita alimentazione.</p>	12 V CC Carico massimo: 25 mA
Configurabile (ingresso o uscita)	3-4	Ingresso digitale o ingresso supervisionato - collegarlo al pin 1 per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo. Per utilizzare l'ingresso supervisionato, installare resistori terminali. Vedere il diagramma di connessione per informazioni su come collegare i resistori.	Da 0 a max 30 V CC
		Uscita digitale: collegato internamente al pin 1 (terra CC) quando attivo e isolato (scollegato) quando inattivo. Se utilizzata con un carico induttivo, ad esempio un relè, collegare un diodo in parallelo al carico per proteggere il dispositivo da sovratensioni.	Da 0 a max 30 V CC, open-drain, 100 mA

Esempio:

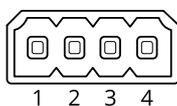


- 1 Terra CC
- 2 Uscita CC 12 V, max 25 mA
- 3 I/O configurato come ingresso supervisionato
- 4 I/O configurato come output

Connettore RS485/RS422

Due morsettiere a 2 pin per interfaccia seriale RS485/RS422. La porta seriale può essere configurata per supportare:

- RS485 a due fili, half-duplex
- RS485 a quattro fili, full-duplex
- RS422 a due fili, simplex
- Comunicazione full-duplex punto a punto con RS422 a quattro fili



Funzione	Pin	Note
RS485/RS422 RX/TX A	1	(RX) Per RS485/RS422 full-duplex (RX/TX) per RS485 half-duplex
RS485/RS422 RX/TX B	2	
RS485/RS422 TX A	3	(TX) Per RS485/RS422 full-duplex
RS485/RS422 TX B	4	

Nomi dei pattern di luce

Disattivato
Fisso
alternata
Impulso
Intensificazione 3 passaggi
Lampeggiante
Intermittenza 3 volte
Intermittenza 4 volte
Intermittenza 3 volte dissolvenza
Intermittenza 4 volte dissolvenza
Lampeggio 1 volta
Lampeggio 3 volte

Nomi modelli sirena

Disattivato
Allarme: suono allarme di altezza elevata
Allarme: suono allarme di altezza bassa
Allarme: Uccello
Allarme: sirena navale
Allarme: Allarme auto
Allarme: allarme auto veloce
Allarme: orologio classico
Allarme: pronto intervento
Allarme: orrore
Allarme: Stabilimenti industriali
Allarme: segnale acustico singolo
Allarme: segnale acustico quadruplo discreto
Allarme: segnale acustico triplo discreto
Allarme: triplo suono ad altezza elevata

Notifica: Accettato
Notifica: Chiamata in corso
Notifica: Negato
Notifica: Fine
Notifica: ingresso
Notifica: Non superato
Notifica: fretta
Notifica: Messaggio
Notifica: Successiva
Notifica: Aperta
Siren (Sirena): alternata
Siren (Sirena): scattante
Siren (Sirena): evac.
Siren (Sirena): altezza in calo
Siren (Sirena): residenziale discreta

Pulizia del dispositivo

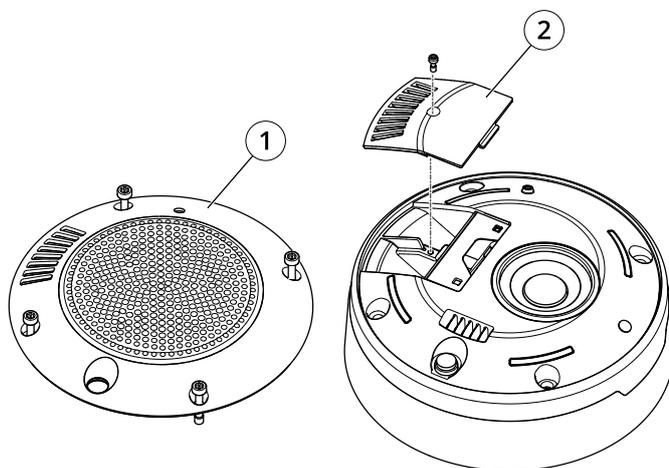
È possibile pulire il dispositivo con acqua tiepida.

AVVISO

- Le sostanze chimiche possono danneggiare il dispositivo. Non utilizzare sostanze chimiche come detersivi per vetri o acetone per pulire il dispositivo.
1. Utilizzare una bomboletta d'aria compressa per rimuovere polvere e sporcizia dal dispositivo.
 2. Se necessario, pulire il dispositivo con un panno morbido in microfibra inumidito con acqua tiepida.
 3. Per evitare macchie, asciugare il dispositivo con un panno pulito e non abrasivo.

Nota

- Rimuovere il coperchio (1) e lo sportello (2).
- Utilizzare una spazzola per rimuovere la polvere.



1 Copertura

2 Porta

Risoluzione dei problemi

Ripristino delle impostazioni predefinite di fabbrica

Importante

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

Per ripristinare il dispositivo alle impostazioni predefinite di fabbrica:

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)**.

Problemi tecnici, indicazioni e soluzioni

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

Problemi durante l'aggiornamento di AXIS OS

Errore di aggiornamento di AXIS OS	Se l'aggiornamento non riesce, il dispositivo ricarica la versione precedente. Il motivo più comune è il caricamento di un AXIS OS errato. Controllare che il nome del file di AXIS OS corrisponda al dispositivo e riprovare.
Problemi dopo l'aggiornamento di AXIS OS	Se si riscontrano problemi dopo l'aggiornamento, ripristinare la versione installata in precedenza dalla pagina Maintenance (Manutenzione) .

Problemi durante l'impostazione dell'indirizzo IP

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	<p>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):</p> <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.

Impossibile accedere al dispositivo da un browser

Non è possibile eseguire l'accesso	Quando HTTPS è abilitato, verifica che sia usato il protocollo giusto (HTTP o HTTPS) quando tenti di eseguire l'accesso. Potrebbe essere necessario digitare manualmente <code>http</code> o <code>https</code> nel campo dell'indirizzo del browser.
------------------------------------	---

Se si dimentica la password per l'account root, il dispositivo deve essere ripristinato alle impostazioni predefinite di fabbrica. Vedere .

L'indirizzo IP è stato modificato dal server DHCP

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

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

Errore del certificato durante l'utilizzo di IEEE 802.1X

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

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 Camera Station Edge: gratuito, ideale per piccoli sistemi con esigenze di sorveglianza di base.
- AXIS Camera Station 5: versione di prova di 30 giorni gratuita, ideale per sistemi di piccole e medie dimensioni.
- AXIS Camera Station Pro: versione di prova di 90 giorni gratuita, ideale per sistemi di piccole e medie dimensioni.

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

Impossibile collegarsi tramite la porta 8883 con MQTT su SSL

Il firewall blocca il traffico utilizzando la porta 8883 poiché è insicuri.

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

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

Il dispositivo non si avvia dopo averlo collegato a un altro prodotto

Classe PoE errata

Verificare che venga utilizzato un alimentatore di Classe PoE 4, quando il dispositivo è collegato a un altro prodotto.

I dati del sensore non sono accurati

I dati del sensore sono imprecisi

L'AQI (Air Quality Index), il CO₂, il VOC e il NO_x richiedono tempo per diventare operativi. Vedere .

Considerazioni sulle prestazioni

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

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

Contattare l'assistenza

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

T10222990_it

2025-02 (M1.49)

© 2025 Axis Communications AB