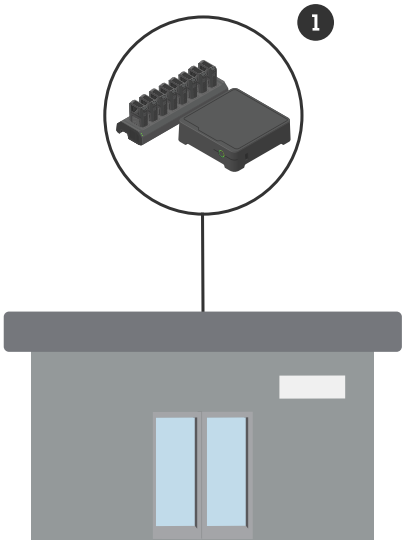
AXIS W401 Body Worn Activation Kit

Manuale dell'utente

Indice

Informazioni sul dispositivo

Panoramica del sistema



Sistema della sede centrale

1 Sistema body worn Axis

Requisiti software

Sistema body worn Axis – AXIS OS versione 12.3 o successiva

Installazione

Per ulteriori informazioni su come installare l'AXIS W401 Body Worn Activation Kit, consultare la guida all'installazione nella pagina di *supporto del prodotto*.

1. Collegare il dispositivo di attivazione della registrazione al connettore I/O. Vedere .

AVVISO

Consigliamo l'installazione di un fusibile da 2 A tra il terminale positivo della batteria e AXIS W401 Body Worn Activation Kit. In caso di dubbi su come procedere all'installazione di hardware, contattare un professionista degli allestimenti per auto perché la esegua.

2. Collegare l'alimentazione al connettore di alimentazione oppure utilizzare PoE per alimentare il dispositivo. Vedere .

Nota

Se sono collegati sia il connettore di alimentazione che il PoE, la rete verrà collegata tramite cavo Ethernet.

Il dispositivo passa alla connessione wireless quando si scollega il cavo Ethernet.

Impostazioni preliminari

Individuazione del dispositivo sulla rete

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

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

Supporto browser

Il dispositivo può essere utilizzato con i seguenti browser:

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

Per usare l'interfaccia Web di AXIS OS con iOS 15 o iPadOS 15, andare su **Settings > Safari > Advanced > Experimental Features**(Impostazioni > Safari > Avanzate > Funzioni sperimentali) e disabilitare NSURLSession Websocket.

Per ulteriori informazioni sui browser consigliati, andare al *Portale AXIS OS*.

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

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

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

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.

Rilevamento manomissione con segnale di input

In questo esempio viene spiegato come inviare un e-mail in caso di interruzione o corto circuito del segnale di input. Per ulteriori informazioni sul connettore I/O, vedere .

1. Andare in **System (Sistema) > Accessories (Accessori) > I/O ports (Porte I/O)** e attivare **Supervised (Supervisionate)** per la rispettiva porta.

Aggiungere un destinatario e-mail:

1. Andare a **System > Events > Recipients (Sistema > Eventi > Destinatari)** e aggiungere un destinatario.
2. Immettere un nome per il destinatario.
3. Selezionare **Email (E-mail)**.
4. Immettere un indirizzo e-mail a cui inviare l'e-mail.
5. La telecamera non ha un proprio server e-mail, quindi deve accedere a un altro server e-mail per inviare e-mail. Compilare il resto delle informazioni sulla base del provider e-mail.
6. Fare clic su **Test (Test)** per inviare un'e-mail di prova.
7. Fare clic su **Salva**.

Creare una regola:

1. Andare a **System > Events > Rules (Sistema > Eventi > Regole)** e aggiungere una regola.
2. Inserire un nome per la regola.
3. Nell'elenco delle condizioni, in **I/O**, selezionare **Supervised input tampering is active (Supervisione manomissione input attiva)**.
4. Selezionare la relativa porta.
5. Nell'elenco delle azioni, in **Notifications (Notifiche)**, selezionare **Send notification to email (Invia notifica all'indirizzo e-mail)**, quindi selezionare il destinatario dall'elenco.
6. Digitare un oggetto e un messaggio per l'e-mail.
7. Fare clic su **Salva**.

Attiva una lampada quando si apre la finestra

Questo esempio mostra come connettere un contatto di una finestra a un kit di attivazione body cam e come impostare un evento che attivi una lampada quando si apre una finestra con un contatto.

Prerequisiti

- Collegare un cavo con 2 fili (massa, I/O) al contatto della finestra e al connettore I/O sul kit di attivazione body cam.
- Collegare la lampada all'alimentazione e al connettore relè sul kit di attivazione body cam.

Configurazione delle porte I/O del kit di attivazione body cam

1. Andare a **System > Accessories (Sistema > Accessori)**.
2. Immetti le seguenti informazioni in **Port 1 (Porta 1)**:
   - **Nome**: Sensore finestra
   - **Direction (Direzione)**: **Ingresso**
   - **Normal state (Stato normale)**: **Circuito chiuso**
3. Immetti le seguenti informazioni in **Port 2 (Porta 2)**:
   - **Nome**: Lampada
   - **Direction (Direzione)**: **Uscita**
   - **Normal state (Stato normale)**: **Circuito aperto**

Creare due regole nel kit di attivazione body cam

1. Andare a **System > Events (Sistema > Eventi)** e aggiungere una regola.
2. Immettere le seguenti informazioni:
   - **Nome**: Sensore finestra
   - **Condition (Condizione)**: **Ingresso digitale**
     Seleziona **Use this condition as a trigger (Utilizza questa condizione come trigger)**
   - **Porta**: **Sensore finestra**
   - **Action (Azione)**: **Attiva/disattiva I/O mentre la regola è attiva**
   - **Porta**: **Lampada**
   - **State (Stato)**: **Attivo**
3. Fare clic su **Salva**.

Attivare il kit di attivazione body cam tramite MQTT quando la telecamera rileva un movimento

Prerequisiti

- Configurare un dispositivo per la porta I/O 1 del kit di attivazione body cam.
- Imposta un broker MQTT e ottieni l'indirizzo IP, il nome utente e la password del broker.
- Configurare AXIS Motion Guard nella telecamera.

Configura il client MQTT nella telecamera

1. Nell'interfaccia dispositivo della telecamera, vai su **System > MQTT > MQTT client > Broker (Sistema > MQTT > Client MQTT > Broker)** e immetti le seguenti informazioni:
   - **Host**: Indirizzo IP broker
   - **Client ID (ID client)**: Ad es., Telecamera 1
   - **Protocol (Protocollo)**: Il protocollo su cui è impostato il broker
   - **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 **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 **Salva**.

Impostazione del client MQTT nel kit di attivazione body cam

1. Nell'interfaccia dispositivo del kit di attivazione body cam, andare in **System (Sistema) > MQTT > MQTT client (Client MQTT) > Broker** e immettere le seguenti informazioni:
   - **Host**: Indirizzo IP broker
   - **Client ID (ID client)**: Porta 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 **Salva**.

Creare una regola nel kit di attivazione body cam per le sottoscrizioni MQTT

1. Andare a **System > Events > Rules (Sistema > Eventi > Regole)** e aggiungere una regola.
2. Immettere le seguenti informazioni:
   - **Nome**: Oggetti in movimento rilevati
   - **Condition (Condizione)**: **MQTT > Stateful (MQTT > Dotato di stato)**
   - **Subscription filter (Filtro sottoscrizione)**: **Movimento**
   - **Payload**: attivato
   - **Action (Azione)**: **I/O > Toggle I/O while the rule is active (Attiva/disattiva l'I/O mentre la regola è attiva)**

- **Port (Porta)**: I/O 1.

3. Fare clic su **Salva**.

Apertura di una serratura quando si preme un pulsante

Questo esempio mostra come collegare un relè al kit di attivazione body cam e come impostare un evento di apertura di una serratura quando qualcuno preme un pulsante collegato al kit di attivazione body cam.

Prerequisiti

- Collegare un cavo con 2 fili (COM, NO) alla serratura e al connettore relè sul kit di attivazione body cam.
- Collegare un cavo con 2 fili (massa, I/O) al pulsante e al connettore I/O sul kit di attivazione body cam.

Configurazione delle porte I/O del kit di attivazione body cam

1. Andare a **System > Accessories (Sistema > Accessori)**.
2. Immetti le seguenti informazioni in **Port 1 (Porta 1)**:
   - **Nome**: Pulsante
   - **Direction (Direzione)**: **Ingresso**
   - **Normal state (Stato normale)**: **Circuito aperto**
3. Immetti le seguenti informazioni in **Port 9 (Porta 9)**:
   - **Nome**: Serratura
   - **Normal state (Stato normale)**: **Circuito aperto**

Creare una regola nel kit di attivazione body cam

1. Andare a **System > Events (Sistema > Eventi)** e aggiungere una regola.
2. Immettere le seguenti informazioni:
   - **Nome**: Apri serratura
   - **Condition (Condizione)**: **I/O > Digital input is active (Input digitale attivo)**
     Seleziona **Use this condition as a trigger (Utilizza questa condizione come trigger)**
   - **Porta**: **Pulsante**
   - **Action (Azione)**: **I/O > Toggle I/O once (Attiva/disattiva I/O una volta)**
   - **Porta**: **Serratura**
   - **State (Stato)**: **Attivo**
   - **Duration (Durata):** 10 s
3. Fare clic su **Salva**.

Interfaccia Web

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

Mostra o nascondi il menu principale.

Accedere alle note di rilascio.

Accedere alla guida dispositivo.

Modificare la lingua.

Imposta il tema chiaro o il tema scuro.

Il menu contestuale contiene:

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

Il menu contestuale contiene:

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

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.

Clienti 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.

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.

Consenti app con privilegi root : Abilitare per consentire l'accesso completo al dispositivo alle app con privilegi root.

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

Nota

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

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

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.
  - **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.

- **Format (Formatta)**: Seleziona il formato da utilizzare quando si inseriscono la latitudine e la longitudine del dispositivo.
- **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.

WLAN

Configurazione di una rete personalizzata

Nota

Il dispositivo è attualmente collegato tramite cavo Ethernet.

Il dispositivo passa alla connessione wireless quando si scollega il cavo Ethernet.

Se si desidera unirsi a una rete nascosta o configurare una rete in anticipo, utilizzare il pulsante **Configure custom network (Configurazione rete personalizzata)**.

Configure custom network (Configurazione rete personalizzata): Aggiungere una rete wireless che non trasmetta il proprio SSID (nome). Immetti il SSID e tutte le impostazioni necessarie per la rete. contattare l'amministratore di rete per avere le impostazioni necessarie.

Refresh (Aggiorna): Aggiornare l'elenco delle reti wireless disponibili.

Il menu contestuale contiene:

- **Info (Informazioni)**: mostra l'intensità del segnale, il canale e il tipo di sicurezza della rete.
- **Configura**: modifica le impostazioni di 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.

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.

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.

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

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

Host: Inserire l'indirizzo del server del proxy.

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.
    - **Warm start (Avvio a caldo)**: Invia un messaggio trap quando si modifica un'impostazione SNMP.
    - **Link up**: invia un messaggio trap quando un collegamento cambia dal basso verso l'alto.
    - **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 impostare 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 impostazione 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.

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

Il menu contestuale contiene:

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

Secure keystore (Archivio chiavi sicuro) :

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

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

Activate (Attivare): Attivare il firewall.

Default Policy (Criterio predefinito): Selezionare lo stato predefinito per il firewall.

- **Allow: (Consenti)** Permette tutte le connessioni al dispositivo. Questa opzione è impostata per impostazione predefinita.
- **Deny: (Rifiuta)** Nega tutte le connessioni al dispositivo.

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

- **Indirizzo**: inserire un indirizzo in formato IPv4/IPv6 o CIDR al quale si vuole permettere o rifiutare l'accesso.
- **Protocol (Protocollo)**: selezionare un protocollo al quale permettere o negare l'accesso.
- **Porta**: Inserire un numero di porta alla quale permettere o negare l'accesso. Si può aggiungere un numero di porta tra 1 e 65535.
- **Policy (Criteri)** Selezionare il criterio della regola.

: Fare clic per la creazione di un'altra regola.

Add rules: (Aggiungi regole) Fare clic per l'aggiunta di regole definite.

- **Time in seconds: (Tempo in secondi)** Impostare un limite di tempo al fine di mettere alla prova le regole. Il limite di tempo predefinito è impostato su 300 secondi. Per l'attivazione immediata delle regole, impostare il tempo su 0 secondi.
- **Confirm rules: (Conferma regole)** Eseguire la conferma delle regole e il relativo limite di tempo. Se si è impostato un limite di tempo superiore a 1 secondo, le regole saranno attive durante tale periodo. Se il tempo è stato impostato su 0, le regole saranno subito attive.

Pending rules (Regole in sospeso): Una panoramica delle ultime regole testate da confermare.

Nota

Le regole con un limite di tempo appaiono in **Active rules (Regole attive)** fino a quando non termina il conteggio del timer visualizzato o fino a quando non vengono confermate. Se non si confermano, appaiono in **Pending rules (Regole in sospeso)** fino a quando non termina il conteggio del timer visualizzato e il firewall torna alle impostazioni precedentemente definite. Se si confermano, sostituiranno le regole attive correnti.

Confirm rules (Conferma regole): Fare clic per eseguire l'attivazione delle regole in sospeso.

Active rules (Regole attive): una panoramica delle regole in esecuzione al momento sul proprio dispositivo.

: Fare clic per eseguire l'eliminazione di una regola attiva.

: Fare clic per eseguire l'eliminazione di tutte le regole, sia in sospeso che attive.

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.

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

Account: Inserire un nome account univoco.

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

Repeat password (Ripeti password): 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.

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 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.

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

ALPN (RETE ALPN)

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

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.

Sovrapposizioni testo MQTT

Nota

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

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

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

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

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

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

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.

Impostazione dell'alimentazione

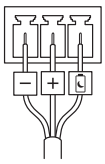
Ingresso alimentazione CC:

Importante

Per evitare arresti indesiderati, attiva **Delayed shutdown (Arresto ritardato)** unicamente quando l'accensione è fisicamente connessa all'unità principale.

Nota

Se il dispositivo è stato privo di alimentazione prima di essere acceso, si verifica un ritardo prima che si attivi il **Delayed shutdown (Arresto ritardato)**.



1. Connetti al controllo dell'accensione sulla morsettiera a 3 pin.
2. Andare all'interfaccia Web del dispositivo.
3. Vai su **System > Power settings (Sistema > Impostazioni di alimentazione)** e attiva **Delayed shutdown (Arresto ritardato)**.
4. imposta un periodo di ritardo compreso tra 1 e 60 minuti.

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.

Analisi della rete

Importante

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

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

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

Registro di sistema remoto

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

Server: Fare clic per aggiungere un nuovo server.

Host: 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.

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

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*.

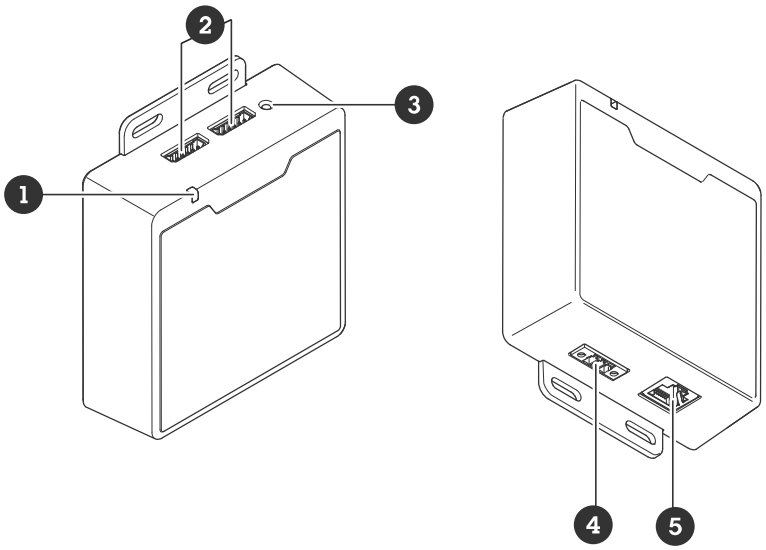
Quando conduci l'aggiornamento, puoi scegliere fra tre opzioni:

- **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.
- **Autorollback (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.

Dati tecnici

Panoramica dei prodotti



1 *LED di stato*
2 *2 connettori I/O*
3 *Pulsante di comando*
4 *Connettore di alimentazione*
5 *Connettore Ethernet RJ45*

Pulsanti

Pulsante di comando

Il pulsante di comando viene utilizzato per:

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

Connettori

Connettore di rete

Connettore Ethernet RJ45.

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

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

Connettore I/O

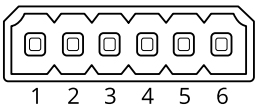
Utilizzare il connettore I/O con dispositivi esterni in combinazione con, ad esempio, rilevamento movimento, attivazione di eventi e notifiche di allarme. Oltre al punto di riferimento 0 V CC e all'alimentazione (output 12 V CC), il connettore I/O fornisce l'interfaccia per:

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.

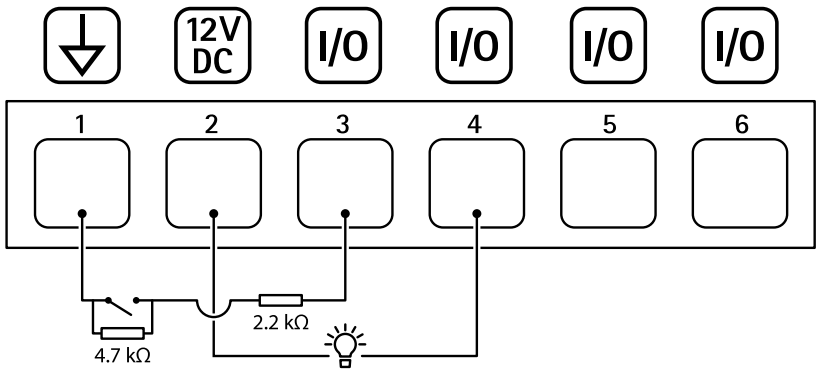
Uscita digitale – Per il collegamento di dispositivi esterni come relè e LED. I dispositivi collegati possono essere attivati tramite l'API (interfaccia per la programmazione di applicazioni) VAPIX® attraverso un evento oppure dall'interfaccia Web del dispositivo.

Morsettiera a 6 pin



Funzione	Pin	Note	Dati tecnici
Terra CC	1		0 V CC
Uscita CC	2	Questo terminale può essere utilizzato anche per alimentare una periferica ausiliaria. Nota: questo pin può essere usato solo come uscita alimentazione.	12 V CC Carico massimo = 50 mA
Configurabile (ingresso o uscita)	3–6	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:

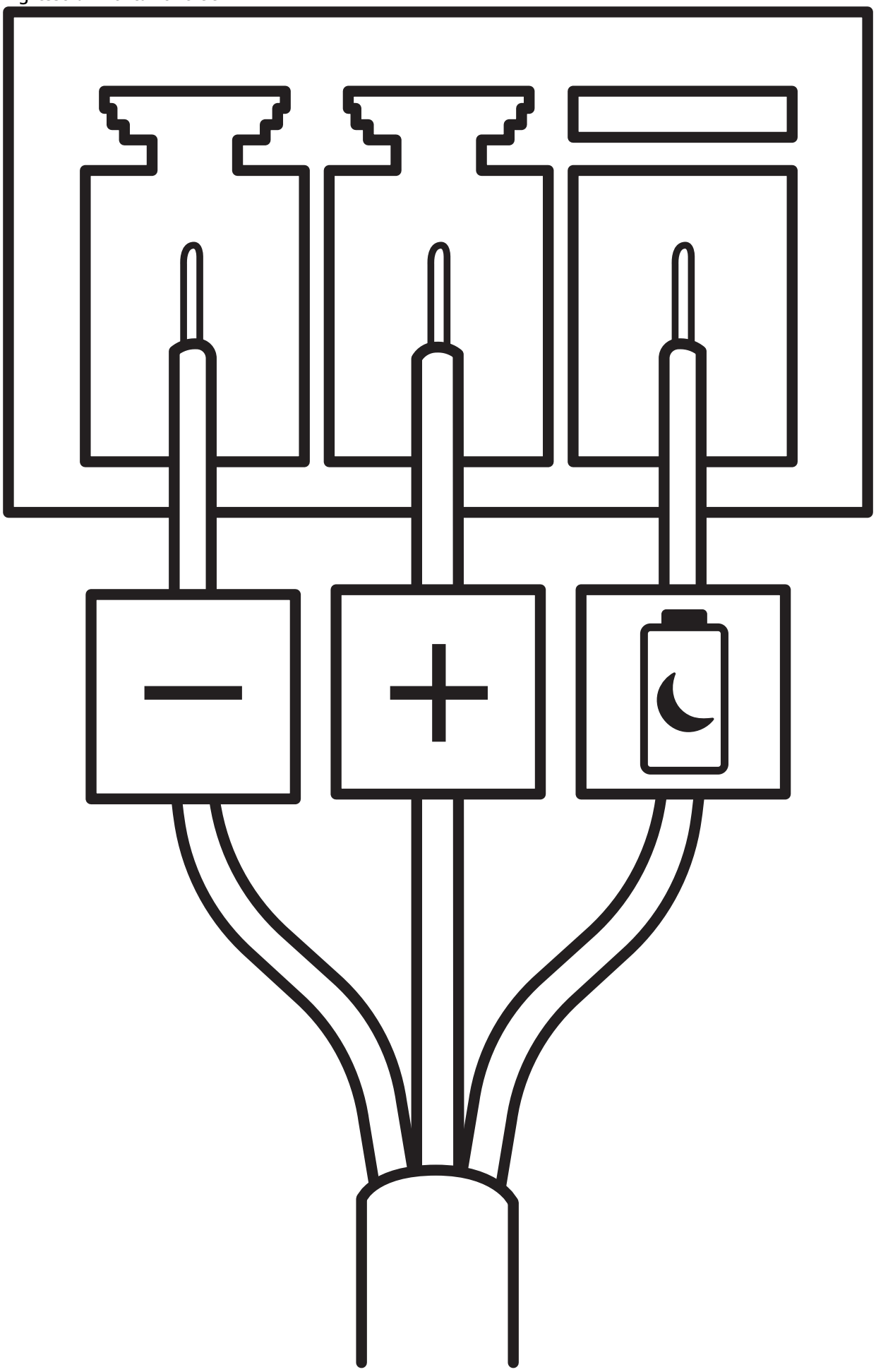


1 *Terra CC*
2 *Output CC 12 V, max 50 mA*
3 *I/O configurato come ingresso supervisionato*
4 *I/O configurato come output*
5 *I/O configurabile*
6 *I/O configurabile*

Connettore di alimentazione

Morsettiera a 3 pin per ingresso alimentazione. Utilizzare una sorgente di alimentazione limitata (LPS) compatibile con una bassissima tensione di sicurezza (SELV) con una potenza di uscita nominale limitata a ≤100 W o una corrente nominale di uscita limitata a ≤5 A.

Ingresso alimentazione CC:



Arresto ritardato

Importante

Per evitare arresti indesiderati, attiva **Delayed shutdown (Arresto ritardato)** unicamente quando l'accensione è fisicamente connessa all'unità principale.

Nota

Se il dispositivo è stato privo di alimentazione prima di essere acceso, si verifica un ritardo prima che si attivi il **Delayed shutdown (Arresto ritardato)**.

1. Connetti al controllo dell'accensione sulla morsettiera a 3 pin.
2. Andare all'interfaccia Web del dispositivo.
3. Vai su **System > Power settings (Sistema > Impostazioni di alimentazione)** e attiva **Delayed shutdown (Arresto ritardato)**.
4. imposta un periodo di ritardo compreso tra 1 e 60 minuti.

Configurazione del sistema

Ricezione del segnale del beacon Bluetooth

La seguente configurazione spiega in che modo l'AXIS Body Worn Activation Kit riceve il segnale del beacon Bluetooth.

Configurazione del kit di attivazione body cam

1. Andare a **System > Events (Sistema > Eventi)** e aggiungere una regola.
2. Nell'elenco delle condizioni, selezionare **Bluetooth beacon signal received (Segnale beacon Bluetooth ricevuto)**.
3. In **System ID (ID sistema)**, inserire l'ID del sistema body cam. È possibile trovarlo nel menu **About (Info)** di AXIS Body Worn Manager.
4. Selezionare la porta a cui è collegato il dispositivo.
5. Nell'elenco delle azioni, selezionarne una.

Configurare il sistema Body Cam

1. Installare il sistema indossabile seguendo il *manuale per l'utente della soluzione indossabile Axis*.
2. In AXIS Body Worn Manager, andare a **Camera profiles (Profili della telecamera)** e selezionare il profilo della telecamera che si desidera utilizzare per il sistema integrato.
3. In **Recording activation (Attivazione registrazione)**, selezionare **Broadcast wireless signal (Trasmissione del segnale wireless)**.

Trasmissione del segnale del beacon Bluetooth

La seguente configurazione spiega come l'AXIS Body Worn Activation Kit trasmette il segnale del beacon Bluetooth.

Configurazione dell'AXIS Body Worn Activation Kit

1. Configurare l'ingresso di attivazione della registrazione:
   1.1. Andare a **System (Sistema)** > **Accessories (Accessori)**.
   1.2. Nella porta a cui è stato collegato il dispositivo, fare clic su per impostare la direzione di ingresso.
2. Creare una regola:
   2.1. Andare a **System > Events (Sistema > Eventi)** e aggiungere una regola.
   2.2. Nell'elenco delle condizioni, selezionare **Digital input is active (Input digitale è attivo)**.
   2.3. Selezionare la porta a cui è collegato il dispositivo.
   2.4. Nell'elenco delle azioni, selezionare **Broadcast signal (Segnale di broadcast)**.
   2.5. In **System ID (ID sistema)**, inserire l'ID del sistema body cam. È possibile trovarlo nel menu **About (Info)** di AXIS Body Worn Manager.
   2.6. In **Message type (Tipo messaggio)**, immettere `1` per inviare in modalità broadcast il messaggio `barra luminosa attiva`.

Configurare il sistema Body Cam

1. Installare il sistema indossabile seguendo il *manuale per l'utente della soluzione indossabile Axis*.
2. In AXIS Body Worn Manager, andare a **Camera profiles (Profili della telecamera)** e selezionare il profilo della telecamera che si desidera utilizzare per il sistema integrato.
3. In **Recording activation (Attivazione registrazione)**, selezionare **Receive wireless broadcast (Ricevi trasmissione wireless)**.

Risoluzione dei problemi

Ripristino delle impostazioni predefinite di fabbrica

Importante

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

Per ripristinare il dispositivo alle impostazioni predefinite di fabbrica:

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

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

Opzioni AXIS OS

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

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

Controllo della versione corrente del AXIS OS

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

Per controllare la versione corrente di AXIS OS:

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

Aggiornare AXIS OS

Importante

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

Nota

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

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

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

Problemi tecnici, indicazioni e soluzioni

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

Problemi durante l'aggiornamento 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	Scollegare il dispositivo Axis dalla rete. Eseguire il comando ping (in una finestra di comando/DOS digitare `ping` e l'indirizzo IP del dispositivo): • Se si riceve: `Reply from <IP address> (Risposta dall'indirizzo IP): bytes=32; time=10...` significa che l'indirizzo IP potrebbe già essere utilizzato da un altro dispositivo nella rete. Contattare l'amministratore di rete per un nuovo indirizzo IP e reinstallare il dispositivo. • Se si riceve: `Request timed out` significa che l'indirizzo IP può essere utilizzato con il dispositivo Axis. Controllare tutti i cablaggi e reinstallare il dispositivo.
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 `http` o `https` 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.

Contattare l'assistenza

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

T10220834_it

2025-03 (M3.2)