

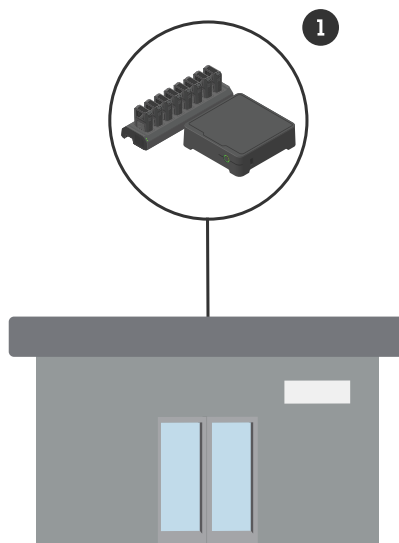
AXIS W401 Body Worn Activation Kit

Indice

Informazioni sul dispositivo	3
Panoramica del sistema	3
Requisiti software	3
Installazione.....	4
Impostazioni preliminari.....	5
Individuazione del dispositivo sulla rete.....	5
Supporto browser	5
Aprire l'interfaccia Web del dispositivo.....	5
Crea un account amministratore.....	5
Password sicure	6
Verificare che nessuno abbia alterato il software del dispositivo.....	6
Configurare il dispositivo	7
Imposta regole per eventi.....	7
Attivazione di un'azione	7
Rilevamento manomissione con segnale di input.....	7
Attiva una lampada quando si apre la finestra	8
Attivare il kit di attivazione body cam tramite MQTT quando la telecamera rileva un movimento	8
Apertura di una serratura quando si preme un pulsante	10
Interfaccia Web	11
Dati tecnici	12
Panoramica dei prodotti.....	12
.....	12
Indicatori LED	12
Pulsanti.....	12
Pulsante di comando.....	12
Connettori.....	12
Connettore di rete	12
Connettore I/O	13
Connettore di alimentazione.....	14
Configurazione del sistema	17
Ricezione di un segnale beacon Bluetooth®	17
Trasmissione di un segnale beacon Bluetooth®.....	17
Configurazione di una zona di privacy	17
Risoluzione dei problemi.....	19
Ripristino delle impostazioni predefinite di fabbrica.....	19
Opzioni AXIS OS.....	19
Controllo della versione corrente del AXIS OS.....	19
Aggiornare AXIS OS.....	20
Problemi tecnici e possibili soluzioni	20
Contattare l'assistenza.....	22

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 *Panoramica dei prodotti*, on page 12.

AWISO

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 *Panoramica dei prodotti*, on page 12.

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

✓: Consigliato

*: Supportato con limitazioni

Aprire l'interfaccia Web del dispositivo

1. Aprire un browser e digitare il nome di host o l'indirizzo IP del dispositivo Axis.
Se non si conosce l'indirizzo IP, utilizzare AXIS IP Utility o AXIS Device Manager per individuare il dispositivo sulla rete.
2. Digitare il nome utente e password. Se si accede al dispositivo per la prima volta, è necessario creare un account amministratore. Vedere *Crea un account amministratore*, on page 5.

Per una descrizione di tutte le funzioni e impostazioni dell'interfaccia web dei dispositivi con AXIS OS, consultare *Guida per l'interfaccia web di AXIS OS*.

Crea un account amministratore

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

1. Inserire un nome utente.
2. Inserire una password. Vedere *Password sicure*, on page 6.
3. Reinserire la password.
4. Accettare il contratto di licenza.
5. Fare clic su **Add account (Aggiungi account)**.

Importante

Il dispositivo non ha un account predefinito. In caso di smarrimento della password dell'account amministratore, è necessario reimpostare il dispositivo. Vedere *Ripristino delle impostazioni predefinite di fabbrica*, on page 19.

Password sicure

Importante

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

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

Per proteggere i dati consigliamo vivamente di:

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

Verificare che nessuno abbia alterato il software del dispositivo

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

1. Ripristinare le impostazioni predefinite di fabbrica. Vedere *Ripristino delle impostazioni predefinite di fabbrica, on page 19*.
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

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

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 quale **Action (Azione)** eseguire 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 *page 13*.

1. Andare in **System (Sistema) > Accessories (Accessori) > I/O ports (Porte I/O)** e attivare **Supervised (Supervisionato)** per una delle relative porte.

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)** come tipo di notifica.
4. Digitare l'indirizzo e-mail del destinatario.
5. Digitare l'indirizzo e-mail da cui si desidera che la telecamera invii le notifiche.
6. Indicare i dati di accesso all'account dell'e-mail di invio, insieme al nome host e al numero di porta SMTP.
7. Per verificare la configurazione della posta elettronica, fare clic su **Test (Prova)**.
8. Fare clic su **Save (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 il messaggio per l'e-mail.
7. Fare clic su **Save (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. Immettere le seguenti informazioni in **Port 1 (Porta 1)**:
 - **Nome**: Sensore finestra
 - **Direction (Direzione)**: Ingresso
 - **Normal state (Stato normale)**: Circuito chiuso
3. Immettere 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 **Save (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:** On
 - **QoS:** 0, 1 o 2
3. Fare clic su **Save (Salva)**.
4. Aggiungere un'altra regola con le seguenti informazioni:
 - **Nome:** Nessun movimento
 - **Condition (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:** Off
 - **QoS:** 0, 1 o 2
5. Fare clic su **Save (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 **Save (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:** On
 - **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 **Save (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. Immettere le seguenti informazioni in **Port 1 (Porta 1)**:
 - Nome: Pulsante
 - Direction (Direzione): Ingresso
 - Normal state (Stato normale): Circuito aperto
3. Immettere 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

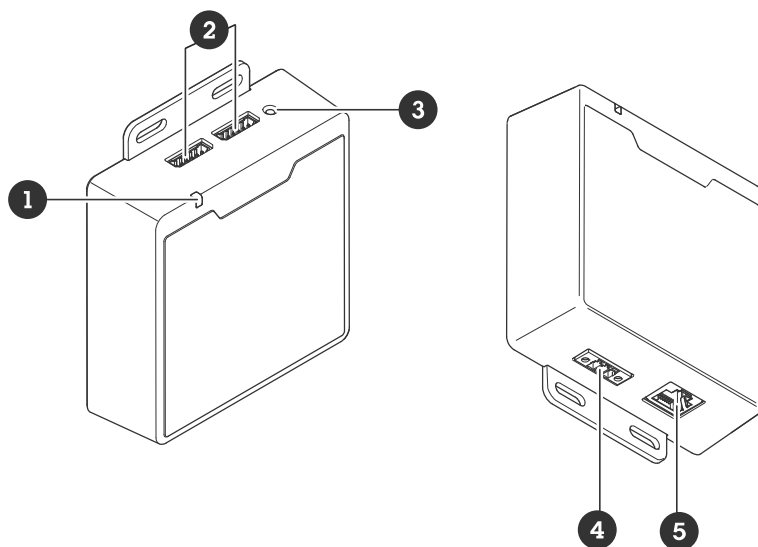
1. Andare a **System > Events (Sistema > Eventi)** e aggiungere una regola.
2. Immettere le seguenti informazioni:
 - Nome: Apri serratura
 - Condition (Condizione): I/O > Digital input is active (Input digitale attivo)
Seleziona Use this condition as a trigger (Utilizza questa condizione come trigger)
 - 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 **Save (Salva)**.

Interfaccia Web

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

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

Indicatori LED

LED di stato	Significato
Verde	Luce verde fissa in condizioni di normale utilizzo.
Giallo	Luce fissa durante l'avvio. Lampeggia durante l'aggiornamento del software del dispositivo.
Rosso	Lampeggia in rosso se l'aggiornamento del software del dispositivo non è riuscito.

Pulsanti

Pulsante di comando

Il pulsante di comando viene utilizzato per:

- Ripristino del dispositivo alle impostazioni predefinite di fabbrica. Vedere *Ripristino delle impostazioni predefinite di fabbrica*, on page 19.
- Connessione a servizio one-click cloud connection (O3C) su Internet. Per connettersi, premere e rilasciare il pulsante, quindi attendere che il LED di stato verde lampeggi tre volte.

Connettori

Connettore di rete

Connettore Ethernet RJ45.

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

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

Connettore I/O

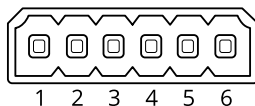
Utilizzare il connettore I/O con dispositivi esterni in combinazione con, ad esempio, rilevamento movimento, attivazione di eventi e notifiche di allarme. Oltre al punto di riferimento 0 V CC e all'alimentazione (output 12 V CC), il connettore I/O fornisce l'interfaccia per:

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.

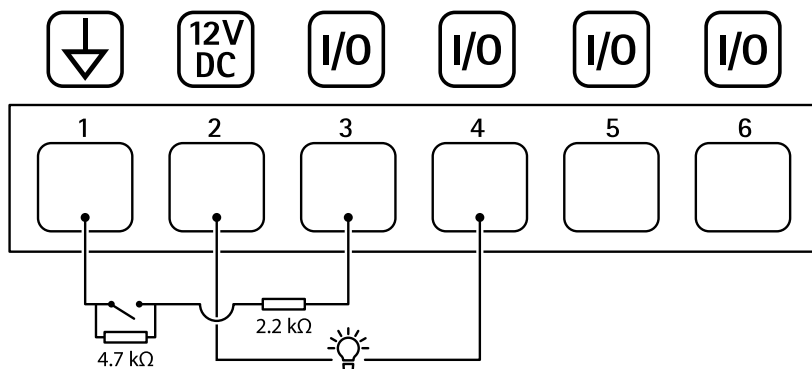
Uscita digitale – Per il collegamento di dispositivi esterni come relè e LED. I dispositivi collegati possono essere attivati tramite l'API (interfaccia per la programmazione di applicazioni) VAPIX® attraverso un evento oppure dall'interfaccia Web del dispositivo.

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:

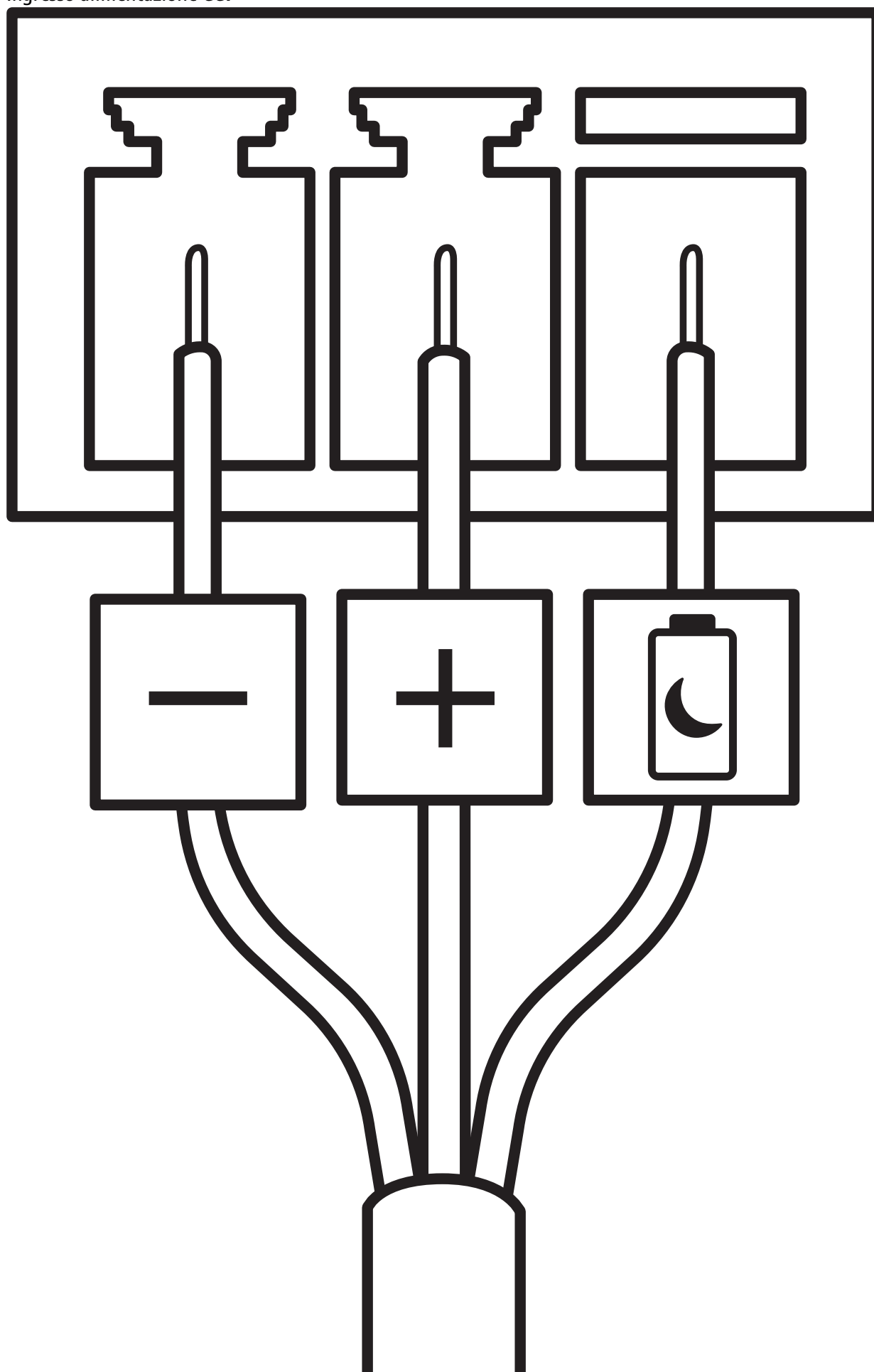


- 1 *Terra CC*
- 2 *Output CC 12 V, max 50 mA*
- 3 *I/O configurato come ingresso supervisionato*
- 4 *I/O configurato come output*
- 5 *I/O configurabile*
- 6 *I/O configurabile*

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 di un segnale beacon Bluetooth®

La seguente configurazione spiega come l'AXIS Body Worn Activation Kit riceve il segnale 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 di un segnale beacon Bluetooth®

La seguente configurazione spiega come l'AXIS Body Worn Activation Kit trasmette il segnale 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 `lightbar active`.

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)**.

Configurazione di una zona di privacy

Per informare gli utenti della telecamera che stanno accedendo a un'area sensibile in cui non si dovrebbe registrare, è possibile configurare una zona di privacy. Quando l'utente accede all'area sensibile, la telecamera

vibra ed emette tre segnali acustici, oppure riproduce un messaggio vocale. Se l'utente rimane nella zona di privacy per due minuti senza interrompere una registrazione in corso, riceve una nuova notifica.

Prerequisiti

AXIS W401 Body Worn Activation Kit installato in un'area sensibile.

In questo esempio, abbiamo impostato AXIS W401 Body Worn Activation Kit per trasmettere un segnale wireless ogni tre secondi.

1. Su AXIS Body Worn Manager, andare in **Camera profiles (Profili telecamera)** .
2. Aprire il profilo della telecamera che si desidera modificare e andare a **Privacy zone** (Zona di privacy).
3. In **Privacy zone broadcast response** (Risposta alla trasmissione della zona di privacy), quindi **Alert** (Avviso).
4. Per ricevere avvisi solo durante la registrazione, impostare **Alert settings** (Impostazioni avviso) su **Alert when recording** (Avvisa durante la registrazione). Per ricevere avvisi anche quando non si sta effettuando la registrazione, impostare l'opzione **Always alert** (Avvisa sempre).
5. Andare a **Settings**  > **Camera** > **Wireless broadcast** (Impostazioni, Telecamera, Trasmissione wireless).
6. Fare clic su **Show key** (Mostra chiave).
7. Immettere la passphrase per il Super amministratore e fare clic su **Confirm** (Conferma).
8. Copiare la chiave.
9. Nell'interfaccia web di AXIS W401, andare a **System** > **Events** > **Schedules** (Sistema, Eventi, Pianificazioni).
10. Assegnare un nome alla pianificazione, ad esempio **Every 3 seconds**.
11. In **Type (Tipo)**, selezionare **Pulse** (Impulso).
12. In **Recurrence** (Ricorrenza), digitare 3.
13. Fare clic su **Save** (Salva).
14. Fai clic su **Rules** (Regole) e aggiungere una regola.
15. Assegnare un nome alla regola, ad esempio **Privacy zone**.
16. Nell'elenco delle condizioni, in **Scheduled and recurring** (Pianificato e ricorrente), selezionare **Pulse** (Impulso).
17. In **Pulse** (Impulso), selezionare la pianificazione creata.
18. Nell'elenco delle azioni, in **Wireless**, selezionare **Broadcast signal** (Segnale trasmissione).
19. Nell'elenco dei protocolli, selezionare **Wireless broadcast key** (Chiave di trasmissione wireless).
20. Copiare la chiave dalla body cam in **Wireless broadcast key** (Chiave di trasmissione wireless).
21. In **Message type** (Tipo messaggio) selezionare **Activate privacy zone** (Attiva zona di privacy).
22. Fare clic su **Save** (Salva).
23. Per regolare la portata della trasmissione wireless:
 - Nell'interfaccia Web di AXIS W401, andare a **System** > **Plain config** (Sistema, Configurazione semplice).
 - Nell'elenco dei gruppi, selezionare **Wireless**.
 - In **Range** (Portata), impostare un numero compreso tra 0 e 30.
Impostare un numero inferiore se la zona di privacy è piccola o se le pareti sono sottili.
 - Fare clic su **Save** (Salva).

Risoluzione dei problemi

Ripristino delle impostazioni predefinite di fabbrica

Importante

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

Per ripristinare il dispositivo alle impostazioni predefinite di fabbrica:

1. Scollegare l'alimentazione dal dispositivo.
2. Tenere premuto il pulsante di comando quando si ricollega l'alimentazione. Vedere *Panoramica dei prodotti*, on page 12.
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

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

Nota

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

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

Problemi tecnici e possibili soluzioni

Problemi durante l'aggiornamento di AXIS OS

Aggiornamento di AXIS OS non riuscito

Se l'aggiornamento non riesce, il dispositivo ricarica la versione precedente. Il motivo più comune è il caricamento di un AXIS OS errato. Controllare che il nome del file di AXIS OS corrisponda al dispositivo e riprovare.

Problemi dopo l'aggiornamento di AXIS OS

Se si riscontrano problemi dopo l'aggiornamento, ripristinare la versione installata in precedenza dalla pagina **Maintenance (Manutenzione)**.

Problemi durante l'impostazione dell'indirizzo IP

Impossibile impostare l'indirizzo IP

- Se l'indirizzo IP destinato al dispositivo e l'indirizzo IP del computer utilizzato per accedere al dispositivo si trovano in subnet diverse, non è possibile impostare l'indirizzo IP. Contattare l'amministratore di rete per ottenere un indirizzo IP.
- L'indirizzo IP potrebbe già essere utilizzato da un altro dispositivo. Per verificare:
 1. Scollegare il dispositivo Axis dalla rete.
 2. In una finestra di comando/DOS digitare `ping` e l'indirizzo IP del dispositivo.
 3. Se la risposta ricevuta è `Reply from <IP address>: bytes=32; time=10...` significa che l'indirizzo IP potrebbe già essere utilizzato da un altro dispositivo nella rete. Contattare l'amministratore di rete per un nuovo indirizzo IP e reinstallare il dispositivo.
 4. Se si riceve: `Request timed out`, significa che l'indirizzo IP può essere utilizzato con il dispositivo Axis. Controllare tutti i cablaggi e reinstallare il dispositivo.
- Potrebbe verificarsi un conflitto di indirizzi IP con un altro dispositivo sulla stessa subnet. Prima che il server DHCP imposti un indirizzo dinamico viene utilizzato l'indirizzo IP statico del dispositivo Axis. Ciò significa che se lo stesso indirizzo IP statico viene utilizzato anche da un altro dispositivo, si potrebbero verificare dei problemi durante l'accesso al dispositivo.

Problemi di accesso al dispositivo

Impossibile effettuare l'accesso al dispositivo tramite un browser.

Quando HTTPS è abilitato, controllare di utilizzare il protocollo corretto (HTTP o HTTPS) durante il tentativo di accesso. Potrebbe essere necessario digitare manualmente `http` o `https` nel campo dell'indirizzo del browser.

Se si è smarrita la password per l'account root, è necessario ripristinare le impostazioni predefinite di fabbrica del dispositivo. Per le istruzioni, vedere *Ripristino delle impostazioni predefinite di fabbrica, on page 19*.

L'indirizzo IP è stato modificato dal server DHCP

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

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

Errore del certificato durante l'utilizzo di IEEE 802.1X

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

Il browser non è supportato

Per un elenco dei browser consigliati, consultare *Supporto browser, on page 5*.

Impossibile accedere al dispositivo dall'esterno

Per accedere al dispositivo esternamente, si consiglia di usare una delle seguenti applicazioni per Windows®:

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

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

Problemi con MQTT

Impossibile collegarsi tramite la porta 8883 con MQTT su SSL

Il firewall blocca il traffico che utilizza la porta 8883 poiché è considerato non sicuro.

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

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

Problemi con il funzionamento del dispositivo

Il riscaldatore anteriore e il tergicristallo non funzionano

Se il riscaldatore anteriore o il tergicristallo non si attivano, confermare che il coperchio superiore sia fissato correttamente alla parte inferiore dell'alloggiamento.

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.

Contattare l'assistenza

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

T10220834_it

2026-02 (M8.2)

© 2025 – 2026 Axis Communications AB