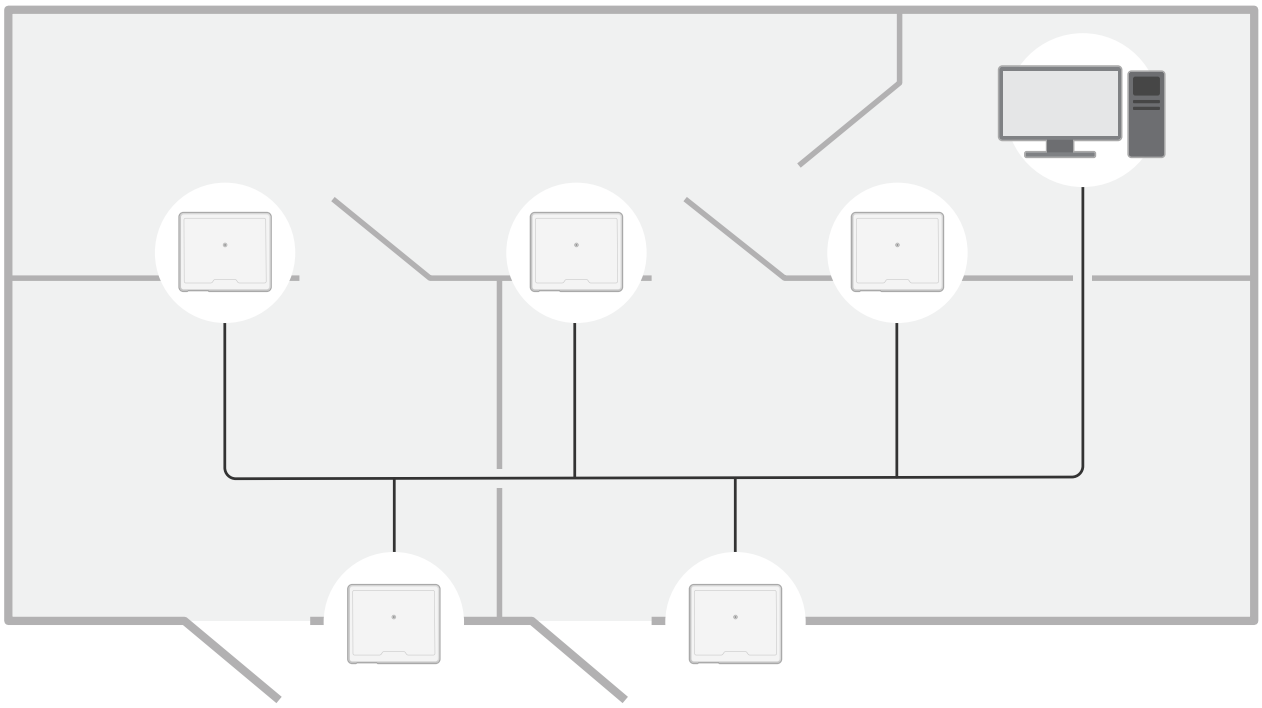
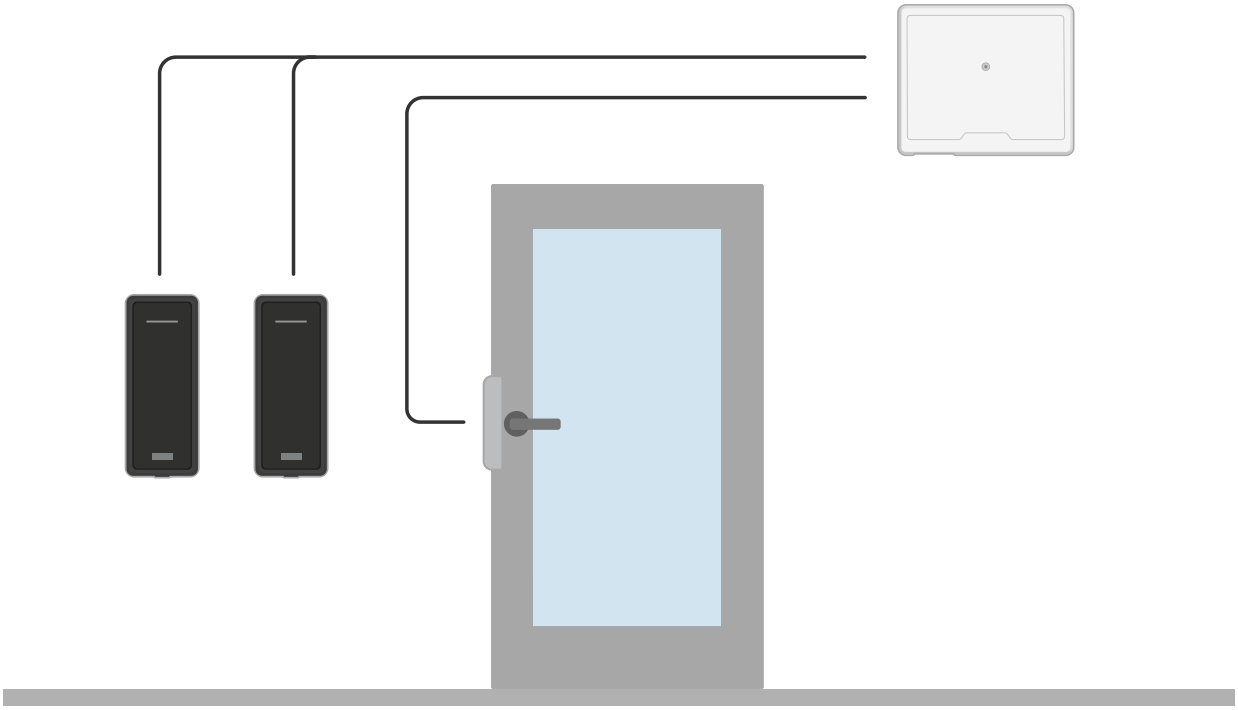
## Indice


Panoramica delle soluzioni ..... 2
Installazione ..... 3
..... 3
Impostazioni preliminari ..... 4
Individuazione del dispositivo sulla rete ..... 4
Supporto browser ..... 4
Aprire l'interfaccia Web del dispositivo ..... 4
Creare un account amministratore ..... 4
Password sicure ..... 5
Accertarsi che nessuno abbia manomesso il software del dispositivo ..... 5
Panoramica dell'interfaccia Web ..... 5
Configurare il dispositivo ..... 6
Override porta ..... 6
Profilo LED OSDP ..... 6
Formato tessera ..... 7
Interfaccia Web ..... 9
Per saperne di più ..... 10
Cyber security ..... 10
SO firmato ..... 10
Avvio sicuro ..... 10
Axis Edge Vault ..... 10
ID dispositivo Axis ..... 10
Dati tecnici ..... 11
Panoramica dei prodotti ..... 11
..... 11
Indicatori LED ..... 11
Pulsanti ..... 12
Pulsante di comando ..... 12
Connettori ..... 12
Connettore di rete ..... 12
Priorità alimentazione ..... 12
Connettore lettore ..... 12
Connettore porta ..... 14
Connettore relè ..... 14
Connettore ausiliario ..... 15
Connettore esterno ..... 16
Connettore di alimentazione ..... 17
Ingressi con supervisione ..... 17
Risoluzione dei problemi ..... 19
Ripristinare le impostazioni predefinite di fabbrica ..... 19
Opzioni AXIS OS ..... 19
Controllo della versione corrente del AXIS OS ..... 19
Aggiornare AXIS OS ..... 19
Problemi tecnici e possibili soluzioni ..... 20
Contattare l'assistenza ..... 22
Cyber security ..... 23
Gestione delle vulnerabilità ..... 23
Notifiche di sicurezza ..... 23
Ciclo di vita sicuro del prodotto ..... 23

## Panoramica delle soluzioni



Il door controller di rete può essere facilmente collegato a e alimentato dalla rete IP esistente senza bisogno di cablaggi speciali.



Ciascun dispositivo di controllo delle porte di rete è un dispositivo intelligente che può essere facilmente montato vicino a una porta. È in grado di alimentare e controllare fino a due lettori.

## Installazione



# 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 oppure 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 *Creare un account amministratore, on page 4*.

Per delle descrizioni di tutte le funzioni e le impostazioni dell'interfaccia web dei dispositivi con AXIS OS, consultare *Guida all'interfaccia web di AXIS OS*.

## Creare un account amministratore

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

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

Importante

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

## Password sicure

Importante

Utilizza il protocollo HTTPS (abilitato per impostazione predefinita) per configurare la password o altre configurazioni sensibili tramite la rete. Il protocollo HTTPS abilita collegamenti di rete sicuri e crittografati, garantendo così la protezione dei dati sensibili, come le password.

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

Per proteggere i dati consigliamo vivamente di:

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

## Accertarsi che nessuno abbia manomesso 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 *Ripristinare le impostazioni predefinite di fabbrica, on page 19*.
   Dopo il ripristino, l'avvio sicuro garantisce lo stato del dispositivo.
2. Configurare e installare il dispositivo.

## Panoramica dell'interfaccia Web

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




*Interfaccia Web dei dispositivi Axis*

## Configurare il dispositivo

Per sapere in che modo si configura il dispositivo, consulta il *manuale per l'utente AXIS Camera Station* o soluzioni di terze parti.

### Override porta

Importante

Questa funzione assume il controllo diretto dei relè delle porte e bypassa la configurazione dei relè in AXIS Camera Station. Utilizzarla solo se l'assistenza Axis ha indicato di procedere in tal senso.

1. Interrompere il servizio Secure Entry in AXIS Camera Station.
2. Nell'interfaccia Web del door controller, andare ad **, Advanced > Door override** (Avanzate, Bypass porta).
3. Leggere attentamente le informazioni riportate nella pagina, quindi fare clic su **I understand** (Accetto).
4. Attivare **Door override** (Bypass porta) e fare clic su **Enable** (Abilita).
5. Andare al relè della porta, fare clic su **Lock**, **Unlock**, oppure **Access** (Blocca, Sblocca oppure Accesso) per bloccare, sbloccare o accedere alla porta.
6. Andare al relè che si desidera configurare e fare clic su **Activate** (Attiva) o **Deactivate** (Disattiva) per attivare o disattivare il relè.

### Profilo LED OSDP

È possibile personalizzare i profili LED del lettore OSDP per definire le luci e i suoni da utilizzare in base ai diversi eventi. Per un elenco completo dei profili, consultare la sezione *Profili LED*.

**Impostare i livelli di luce e audio**

1. Andare a **Peripherals (Periferiche)** > **Readers (Lettori)** > **OSDP LED profile (Profilo LED OSDP)**.
2. Aprire il menu a discesa **Light and audio levels (Livelli di luce e volume dell'audio)**.
3. Utilizzare il cursore per regolare l'intensità della striscia LED, della retroilluminazione LED e del suono.
4. Fare clic su **Save (Salva)**.

Nota

Quando si effettuano delle modifiche di luminosità e audio, le impostazioni vengono aggiornate per tutti i lettori collegati al controller.

**Verificare le impostazioni LED OSDP:**

È possibile utilizzare il menu **OSDP LED test (test LED OSDP)** per visualizzare le impostazioni audio e di illuminazione di ogni profilo del lettore.

Per verificare le impostazioni dei profili LED OSDP:

1. Andare a **Peripherals (Periferiche)** > **Readers (Lettori)** > **OSDP LED profile (Profilo LED OSDP)**.
2. Espandere il menu a discesa **OSDP LED test (Test LED OSDP)**.
3. Scegliere una retroazione LED.
4. Scegli il lettore che si desidera testare.
5. Fare clic su **Avvia**.
6. Fare clic su **Edit feedback (Modifica retroazione)** per modificare le impostazioni di luce e audio del profilo.
   - Scegliere un nuovo colore dal menu a discesa **Color (Colore)**.
   - Scegliere una frequenza audio dal menu a discesa **Audio**, se del caso.

- È inoltre possibile ripristinare le impostazioni del profilo facendo clic su **Reset to default values (Ripristina valori predefiniti)**.
- Fare clic su **Save (Salva)**.

**Modifica delle impostazioni del profilo LED OSDP:**

1. Andare a **Peripherals (Periferiche)** > **Readers (Lettori)** > **OSDP LED profile (Profilo LED OSDP)**.
2. Accedere a **OSDP LED profile (Profilo LED OSDP)**.
3. Fare clic su accanto al profilo che si desidera modificare.
4. Modifica delle impostazioni pertinenti:
   - Scegliere il comportamento che i LED dovranno seguire dal menu a discesa **Behavior (Comportamento)**.
   - Scegli il colore dei LED dal menu a discesa **Color (Colore)**.
   - Impostare **Duration on (Durata acceso)** e **Duration off (Durata spento)** per i LED.
   - Impostare la **Recurrence (Periodicità)** della risposta del LED.
   - Dal menu a discesa **Audio**, scegliere **Beep duration, on (Durata del segnale acustico in funzione)** e **Beep duration, off (Durata del segnale acustico spento)**, quindi impostare la **Recurrence (Periodicità)** della risposta acustica. Assicurarsi che la **Beep duration, on (Durata del segnale acustico in funzione)** e **Beep duration, off (Durata del segnale acustico spento)** siano uguali.
5. Fare clic su **Save (Salva)**.

**Importare le impostazioni esistenti da un altro controller**

1. Andare a **Peripherals (Periferiche)** > **Readers (Lettori)** > **OSDP LED profile (Profilo LED OSDP)**.
2. Fare clic su **Import (Importa)**.
3. Scegliere il file che si desidera caricare.
4. Fare clic su **Import (Importa)**.

**Esportare le impostazioni attuali**

1. Andare a **Peripherals (Periferiche)** > **Readers (Lettori)** > **OSDP LED profile (Profilo LED OSDP)**.
2. Fare clic su **Export (Esporta.**
3. Scegliere dove si desidera salvare il file JSON e fare clic su **Save (Salva)**.

## Formato tessera

Questa funzione è riservata esclusivamente agli utenti esperti. Non appena l'opzione **Card format (Formato scheda)** è attiva:

- Se si utilizza una credenziale a 37 bit, gli ultimi 5 bit vengono rimossi.
- Se si utilizza una credenziale a 64 bit (codice QR), la prima sequenza di 24 bit viene rimossa.

Per visualizzare le credenziali è possibile utilizzare sia i dati campione sia il lettore di schede.

1. Andare ad **Advanced (Avanzate)** > **Card format (Formato scheda)**.
2. Leggere l'avviso e fare clic su **I understand (Ho compreso)** per abilitare **Card format (Formato scheda)**.
3. Nel menu a discesa **Reader data visualization (Visualizzazione dati del lettore)**, scegliere il lettore.
4. Fare clic su **Get reader data (Ottieni dati del lettore)** oppure **Use sample data (Usa dati di esempio)** per generare un output di scheda. Verrà applicata a tutti i titolari di carte presenti sul dispositivo.

5. Attivare l'opzione **Trim reader data (Ritaglia i dati del lettore)** per rimuovere i bit finali delle credenziali della carta.
6. Fare clic su **Enable (Abilita)**.

## Interfaccia Web

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

## Per saperne di più

### Cyber security

Per informazioni specifiche sulla sicurezza informatica, consultare la scheda tecnica del prodotto su axis.com.

Per informazioni approfondite sulla cybersecurity in AXIS OS, leggere la guida *AXIS OS Hardening*.

#### SO firmato

Il SO firmato viene implementato dal fornitore del software che firma l'immagine di AXIS OS con una chiave privata. Quando la firma è allegata al sistema operativo, il dispositivo convalida il software prima di installarlo. Se il dispositivo rileva che l'integrità del software è compromessa, l'aggiornamento di AXIS OS verrà rifiutato.

#### Avvio sicuro

Secure Boot è un processo di avvio costituito da una catena ininterrotta di software crittograficamente convalidati eseguita da una memoria non modificabile (bootrom). Essendo basato sull'uso del SO firmato, l'avvio sicuro assicura che un dispositivo possa essere avviato solo con software autorizzato.

#### Axis Edge Vault

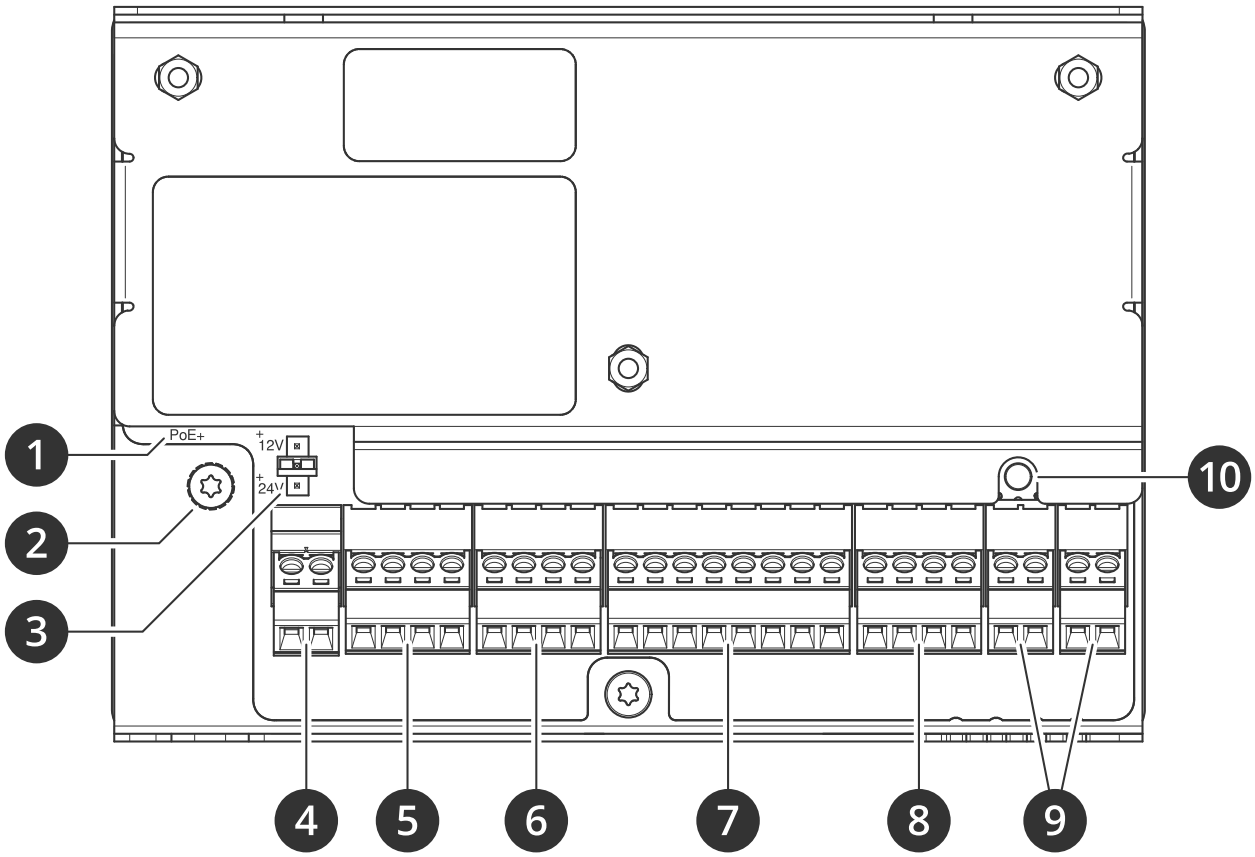
Axis Edge Vault è una piattaforma hardware di cybersecurity che protegge il dispositivo Axis. Offre funzionalità per garantire l'identità e l'integrità del dispositivo e per proteggere le informazioni sensibili da accessi non autorizzati. Si basa su solidi moduli di calcolo crittografico (Secure Element e TPM) e sicurezza del SoC (TEE e Secure Boot), combinati con le competenze di Axis nella sicurezza dei dispositivi edge.

#### ID dispositivo Axis

poter verificare l'origine del dispositivo è fondamentale per stabilire che la sua identità è attendibile. Durante la produzione, ai dispositivi con Axis Edge Vault viene assegnato un certificato ID univoco e conforme a IEEE 802.1AR. È come avere un passaporto per dimostrare l'origine del dispositivo. L'ID del dispositivo viene archiviato in modo sicuro e permanente nell'archivio chiavi come certificato firmato dal certificato radice Axis. L'ID del dispositivo può essere sfruttato dall'infrastruttura IT del cliente per l'onboarding sicuro automatizzato di dispositivi e l'identificazione sicura dei dispositivi

## Dati tecnici

### Panoramica dei prodotti




1 *Connettore di rete*
2 *Posizione di messa a terra*
3 *Ponticello relè*
4 *Connettore di alimentazione*
5 *Connettore relè*
6 *Connettore porta*
7 *Connettore lettore*
8 *Connettore ausiliario*
9 *Connettori esterni*
10 *Pulsante di comando*

### Indicatori LED

| LED | Colore | Significato |
|---|---|---|
| Stato | Verde | Luce verde fissa in condizioni di normale utilizzo. |
| | Giallo | Luce fissa durante l'avvio e quando si ripristinano le impostazioni. |
| | Rosso | Luce lampeggiante lenta per aggiornamento non riuscito. |
| Rete | Verde | Luce fissa per connessione di rete a 100 MBit/s. Lampeggiante per attività di rete. |
| | Giallo | Luce fissa per connessione di rete a 10 MBit/s. Lampeggiante per attività di rete. |
| | Spento | Assenza di collegamento di rete. |

| | | |
|---|---|---|
| Potenza | Verde | Funzionamento normale. |
| | Giallo | Luce lampeggiante verde/gialla durante l'aggiornamento del firmware. |
| Relè | Verde | Relè attivo.[1] |
| | Spento | Relè inattivo. |

## Pulsanti

### Pulsante di comando

Il pulsante di comando viene utilizzato per:

- Ripristino del dispositivo alle impostazioni predefinite di fabbrica. Vedere *Ripristinare le impostazioni predefinite di fabbrica, on page 19*.

## Connettori

### Connettore di rete

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

**UL**: Power over Ethernet (PoE) deve essere over Ethernet IEEE 802.3af/802.3at Tipo 1 Classe 3 o Power over Ethernet Plus (PoE+) IEEE 802.3at Tipo 2 Classe 4 Iniettore limitato all'alimentazione che fornisce 44–57 V CC, 15,4 W/30 W. Power over Ethernet (PoE) è stato valutato da UL con AXIS T8133 Midspan 30 W 1-port.

### Priorità alimentazione

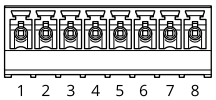
Questo dispositivo può essere alimentato tramite input PoE o CC. Vedere *Connettore di rete, on page 12* e *Connettore di alimentazione, on page 17*.

- Quando PoE e CC sono entrambi collegati prima dell'accensione del dispositivo, PoE viene utilizzato per l'alimentazione.
- PoE e CC sono entrambi collegati e PoE è attualmente in fase di alimentazione. Quando si perde l'alimentazione PoE, il dispositivo utilizza CC per l'alimentazione senza riavvio.
- PoE e CC sono entrambi collegati e CC è attualmente in fase di alimentazione. In caso di perdita di alimentazione CC, il dispositivo si riavvia e utilizza PoE per l'alimentazione.
- Quando CC viene utilizzato durante l'avvio e PoE viene collegato dopo l'avvio del dispositivo, viene utilizzato CC per l'alimentazione.
- Quando PoE viene utilizzato durante l'avvio e CC viene collegato dopo l'avvio del dispositivo, viene utilizzato PoE per l'alimentazione.

### Connettore lettore

Una morsettiera a 8 pin che supporta i protocolli OSDP e Wiegand per la comunicazione con il lettore.

Può collegare fino a due lettori OSDP (multicascata) o un lettore Wiegand. 500 mA a 12 V CC sono riservati a tutti i lettori collegati al door controller.




**Configurato per un lettore OSDP**

1. *Il relè è attivo quando COM è connesso a NO.*

| Funzione | Pin | Nota | Dati tecnici |
|---|---|---|---|
| Massa CC (GND) | 1 | | 0 V CC |
| Output CC (+12 V) | 2 | Fornisce alimentazione al lettore. | 12 V CC, max 500 mA |
| A | 3 | Half-duplex | |
| B | 4 | Half-duplex | |

**Configurato per due lettori OSDP (multi-drop)**

| Funzione | Pin | Nota | Dati tecnici |
|---|---|---|---|
| Massa CC (GND) | 1 | | 0 V CC |
| Output CC (+12 V) | 2 | Fornisce alimentazione ad entrambi i lettori. | 12 V CC, Max 500 mA combinata per entrambi i lettori |
| A | 3 | Half-duplex | |
| B | 4 | Half-duplex | |

Importante

- Quando il lettore è alimentato dal controller, la lunghezza del cavo certificata raggiunge il massimo di 200 m (656 piedi). Verificato unicamente per i lettori Axis.
- Quando il lettore non è alimentato dal controller, la lunghezza del cavo certificata per i dati del lettore raggiunge il massimo di 1000 m (3280,8 piedi) se sono soddisfatti i seguenti requisiti del cavo: 1 doppino con schermatura, AWG 24, impedenza 120 ohm. Verificato unicamente per i lettori Axis.

**Configurato per un lettore Wiegand**

| Funzione | Pin | Nota | Dati tecnici |
|---|---|---|---|
| Massa CC (GND) | 1 | | 0 V CC |
| Output CC (+12 V) | 2 | Fornisce alimentazione al lettore. | 12 V CC, max 500 mA |
| D0 | 3 | | |
| D1 | 4 | | |
| LED 1 | 5 | LED rosso | |
| LED 2 | 6 | LED verde | |
| MANOMISSIONE | 7 | Ingresso digitale - collegare al pin 1 per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo. | Da 0 a max 30 V CC |
| SEGNALE ACUSTICO | 8 | Output digitale: se utilizzato 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 |

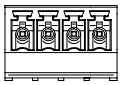
Importante

- Quando il lettore è alimentato dal controller, la lunghezza del cavo certificata raggiunge il massimo di 150 m (500 piedi).
- Quando il lettore non è alimentato dal controller, la lunghezza del cavo certificata per i dati del lettore raggiunge il massimo di 150 m (500 piedi) se è soddisfatto il seguente requisito del cavo: AWG 22.

### Connettore porta

Una morsettiera a 4 pin utilizzata per i monitor porte (input digitale).

Il monitor porte supporta la supervisione con resistori di linea. Se il collegamento viene interrotto, viene attivato un allarme. Per utilizzare gli input supervisionati, installare resistenze di fine linea. Per gli input supervisionati utilizzare lo schema delle connessioni. Vedere *page 17*.



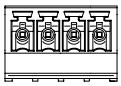

| Funzione | Pin | Note | Dati tecnici |
|---|---|---|---|
| Terra CC | 1, 3 | | 0 V CC |
| Ingresso | 2, 4 | Per comunicare con il monitoraggio porte. Input digitale o input supervisionato: collegare al pin 1 o 3 rispettivamente per attivare oppure lasciare svolazzante (scollegato) per disattivare. | Da 0 a max 30 V CC |

Importante

La lunghezza certificata del cavo è massimo fino a 200 m (656 piedi) se è soddisfatto il seguente requisito del cavo: AWG 24.

### Connettore relè

Una morsettiera a 4 pin per relè a forma di C che possono essere utilizzati, ad esempio, per controllare un blocco o un'interfaccia di un cancello.




| Funzione | Pin | Note | Dati tecnici |
|---|---|---|---|
| Massa CC (GND) | 1 | | 0 V CC |
| NO | 2 | Normalmente aperto. Per il collegamento di relè. Collegare un blocco di protezione intrinseca tra NO e massa CC. I due pin relè sono separati con isolamento galvanico dal resto dei circuiti se i ponticelli non vengono utilizzati. | Corrente massima = 2 A Tensione max. = 30 V CC |
| COM | 3 | Comune | |

| | | | |
|---|---|---|---|
| NC | 4 | Normalmente chiuso.<br>Per il collegamento di relè. Collegare un blocco di sicurezza intrinseca tra NC e massa CC.<br>I due pin relè sono separati con isolamento galvanico dal resto dei circuiti se i ponticelli non vengono utilizzati. | |

**Ponticello di alimentazione relè**

Quando montato, il ponticello di alimentazione del relè si collega a 12 V CC o 24 V CC al pin COM del relè.

Può essere utilizzato per collegare un blocco tra i pin GND e NO o tra i pin GND e NC.

| Sorgente di alimentazione | Potenza massima a 12 V CC | Potenza massima a 24 V CC |
|---|---|---|
| **IN CC** | 1.600 mA | 800 mA |
| **PoE** | 900 mA | 450 mA |

*AVVISO*

Se il blocco non è polarizzato, si consiglia di aggiungere un diodo di ritorno esterno.

## Connettore ausiliario

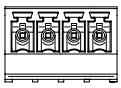
Utilizzare il connettore ausiliario con dispositivi esterni in combinazione con, ad esempio, rilevamento del movimento, attivazione di eventi e notifiche di allarme. Oltre al punto di riferimento 0 V CC e all'alimentazione (output CC), il connettore ausiliario fornisce l'interfaccia per:

**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.

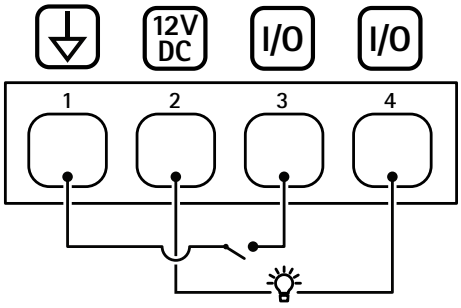
**Uscita digitale –** Per il collegamento di dispositivi esterni come relè e LED. I dispositivi collegati possono essere attivati tramite l'API (interfaccia per la programmazione di applicazioni) VAPIX® oppure dalla pagina Web del dispositivo.

Morsettiera a 4 pin




| Funzione | Pin | Note | Dati tecnici |
|---|---|---|---|
| Terra CC | 1 | | 0 V CC |
| Uscita CC | 2 | Questo terminale può essere utilizzato anche per alimentare una periferica ausiliaria.<br>Nota: questo pin può essere usato solo come uscita alimentazione. | 12 V CC<br>Carico massimo = 50 mA in totale |

| | | | |
|---|---|---|---|
| Configurabile (ingresso o uscita) | 3-4 | Ingresso digitale o ingresso supervisionato - collegarlo al pin 1 per attivarlo oppure lasciarlo svolazzante (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. Ogni I/O è in grado di guidare 12 V CC, 50 mA (combinata max) carico esterno, se si utilizza l'uscita interna 12 V CC (pin 2). In caso di utilizzo di connessioni di scarico aperte in combinazione con un alimentatore esterno, gli I/O possono gestire l'alimentazione CC di 0 – 30 V CC, 100 mA. | Da 0 a max 30 V CC, open-drain, 100 mA |

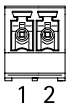



1 *Terra CC*
2 *Output CC 12 V*
3 *I/O configurato come input*
4 *I/O configurato come output*

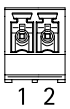
### Connettore esterno

Due morsettiere a 2 pin per dispositivi esterni, ad esempio rottura vetri o rivelatori di incendio.

**UL**: Il connettore non è stato valutato da UL per l'uso di antifurto o allarme antincendio.




| Funzione | Pin | Note | Dati tecnici |
|---|---|---|---|
| Terra CC | 1 | | 0 V CC |
| MANOMISSIONE | 2 | Ingresso digitale - collegare al pin 1 per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo. | Da 0 a max 30 V CC |



| Funzione | Pin | Note | Dati tecnici |
|---|---|---|---|
| Terra CC | 1 | | 0 V CC |
| ALLARME | 2 | Ingresso digitale - collegare al pin 1 per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo. | Da 0 a max 30 V CC |

## Connettore di alimentazione

Morsettiera a 2 pin per ingresso alimentazione CC. 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.




| Funzione | Pin | Note | Dati tecnici |
|---|---|---|---|
| Massa CC (GND) | 1 | | 0 V CC |
| Input CC | 2 | Per l'alimentazione del dispositivo quando non si utilizza Power over Ethernet.<br>Nota: questo pin può essere usato solo come alimentazione. | 12 V CC, max 36 W |

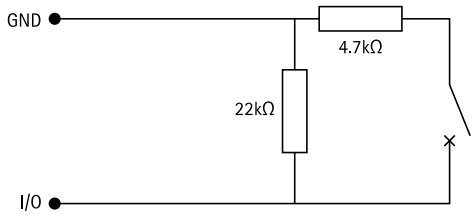
**UL**: l'alimentazione CC deve essere fornita da un alimentatore conforme a UL 603, a seconda dell'applicazione, dotato delle classificazioni appropriate.

## Ingressi con supervisione

Per utilizzare gli input supervisionati, installare resistori terminali in base al diagramma di seguito riportato.

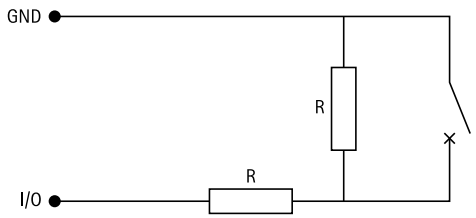
### Prima connessione parallela

I valori dei resistori devono essere 4,7 kΩ e 22 kΩ.




### Prima connessione in serie

I valori dei resistori devono essere gli stessi e i possibili valori sono 1 kΩ, 2,2 kΩ, 4,7 kΩ e 10 kΩ.



Nota

Si consiglia l'uso di cavi intrecciati e schermati. Connetti schermatura a 0 V CC.

## Risoluzione dei problemi

### Ripristinare le impostazioni predefinite di fabbrica

Importante

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

Per ripristinare il dispositivo alle impostazioni predefinite di fabbrica:

1. Scollegare l'alimentazione dal dispositivo.
2. Tenere premuto il pulsante di comando quando si ricollega l'alimentazione. Vedere *Panoramica dei prodotti, on page 11*.
3. Tenere premuto il pulsante di comando per 25 secondi finché l'indicatore LED di stato non emette nuovamente una luce gialla.
4. Rilasciare il pulsante di comando. La procedura è terminata quando il LED di stato diventa verde. Se nella rete non è disponibile un server DHCP, l'indirizzo IP del dispositivo sarà predefinito con uno dei seguenti valori:
   - **Dispositivi con AXIS OS 12.0 e versioni successive:** ottenuti dalla subnet degli indirizzi di collegamento locale (169.254.0.0/16)
   - **Dispositivi con AXIS OS 11.11 e precedenti:** 192.168.0.90/24
5. Utilizzare gli strumenti per l'installazione e la gestione del software per assegnare un indirizzo IP, impostare la password e accedere al dispositivo.

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

### Opzioni AXIS OS

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

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

### Controllo della versione corrente del AXIS OS

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

Per controllare la versione corrente di AXIS OS:

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

### Aggiornare AXIS OS

Importante

- Quando si esegue l'aggiornamento del software del dispositivo, le impostazioni preconfigurate e personalizzate vengono salvate. Axis Communications AB non può garantire il salvataggio delle

impostazioni, anche se le funzionalità sono disponibili nella nuova versione del sistema operativo AXIS OS.

- A partire da AXIS OS 12.6, è necessario installare tutte le versioni LTS comprese tra la versione attuale del dispositivo e la versione di destinazione. Ad esempio, se la versione del software attualmente installata sul dispositivo è AXIS OS 11.2, è necessario installare la versione LTS AXIS OS 11.11 prima di poter effettuare l'aggiornamento del dispositivo ad AXIS OS 12.6. Per ulteriori informazioni, vedere *Guida al ciclo di vita AXIS OS: percorso di aggiornamento*.
- Assicurarsi che il dispositivo rimanga collegato alla fonte di alimentazione durante il processo di aggiornamento.

Nota

- Quando si aggiorna il dispositivo con la versione più recente di AXIS OS nella traccia attiva, il dispositivo riceve le ultime funzionalità disponibili. Leggere sempre le istruzioni di aggiornamento e le note di rilascio disponibili con ogni nuova versione prima dell'aggiornamento. Per la versione AXIS OS più aggiornata e le note sul rilascio, visitare il sito Web *axis.com/support/device-software*.
- Dal momento che il database di utenti, gruppi, credenziali e altri dati viene aggiornato dopo un aggiornamento di AXIS OS, il completamento del primo avvio potrebbe richiedere alcuni minuti. Il tempo richiesto dipende dalla quantità di dati.

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.

4. Una volta riavviato il dispositivo, cancellare la cache del browser Web.

## Problemi tecnici e possibili soluzioni

### Problemi durante l'aggiornamento di AXIS OS

**Aggiornamento di AXIS OS non riuscito**

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

**Problemi dopo l'aggiornamento di AXIS OS**

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

### Problemi durante l'impostazione dell'indirizzo IP

**Impossibile impostare l'indirizzo IP**

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

**Problemi di accesso al dispositivo**

**Impossibile effettuare l'accesso al dispositivo tramite un browser.**

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

Se si è smarrita la password per l'account root, è necessario ripristinare le impostazioni predefinite di fabbrica del dispositivo. Per le istruzioni, vedere *Ripristinare le impostazioni predefinite di fabbrica, on page 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 4*.

**Impossibile accedere al dispositivo dall'esterno**

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

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

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

**Problemi con MQTT**

**Impossibile collegarsi tramite la porta 8883 con MQTT su SSL**

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

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

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

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

## Contattare l'assistenza

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

## Cyber security

La sicurezza informatica sostiene un ciclo di vita del prodotto ottimale con rischi ridotti al minimo. È possibile trovare informazioni approfondite e documentazione sul nostro approccio alla sicurezza informatica all'indirizzo *axis.com/about-axis/cybersecurity*. Segui le linee guida sulla sicurezza informatica riportate di seguito per ricevere le notifiche di sicurezza relative al prodotto da parte di Axis e per configurare il prodotto per garantirne un ciclo di vita e una dismissione sicuri.

All'indirizzo *Axis Trust Center*, è possibile trovare informazioni su come Axis garantisce la conformità alle norme di sicurezza, la trasparenza, la protezione dei dati e la privacy.

### Gestione delle vulnerabilità

Axis è una *Common Vulnerability and Exposures (CVE) Numbering Authority (CNA)*. Per ridurre al minimo il rischio di esposizione, seguiamo gli standard del settore nell'identificazione e nella risoluzione delle vulnerabilità presenti nei nostri dispositivi, software e servizi. Per informazioni sulla nostra politica di gestione delle vulnerabilità o per segnalare una vulnerabilità, fare riferimento a: *axis.com/vulnerability-management*.

### Notifiche di sicurezza

Iscriversi alle e-mail di notifica sulla sicurezza di Axis all'indirizzo *axis.com/security-notification-service*. Ti invieremo informazioni relative alle vulnerabilità, alle relative note di sicurezza e ad altre questioni relative alla sicurezza del tuo prodotto Axis.

### Ciclo di vita sicuro del prodotto

Axis riduce al minimo i rischi durante l'intero ciclo di vita dei propri prodotti grazie a una gestione sicura del ciclo di vita. Utilizzi le nostre guide al consolidamento disponibili su *help.axis.com* per configurare e utilizzare in modo più sicuro i prodotti Axis e per trovare informazioni su:

**Primo utilizzo sicuro –** I prodotti Axis sono pre-configurati con un elevato livello di protezione predefinito per garantire un'inizializzazione sicura e comunicazioni crittografate sin dall'inizio.

**Uso previsto ed errori comuni di configurazione –** Le nostre guide forniscono informazioni sull'uso previsto dei prodotti Axis, compresi gli errori di configurazione e gli usi impropri più comuni che possono compromettere la sicurezza e che è opportuno evitare.

**Gestione delle vulnerabilità e trasparenza della catena di fornitura –** Ad ogni rilascio del software viene pubblicata una distinta base dei componenti software (SBOM) su *axis.com* al fine di rendere note le vulnerabilità e migliorare la trasparenza della catena di fornitura.

**Messa fuori servizio e cancellazione sicura dei dati –** Per mettere fuori servizio in modo sicuro un prodotto quando raggiunge la fine del suo ciclo di vita, ripristinare le impostazioni predefinite di fabbrica. In questo modo le configurazioni, i dati salvati e le informazioni sensibili verranno cancellati.

T10181041_it

2026-10 (M11.6)

© 2022 – 2026 Axis Communications AB