AXIS Secure Entry for XProtect

Manuale dell'utente

Indice

Controllo accessi

Il controllo degli accessi è una soluzione che combina il controllo fisico degli accessi con la videosorveglianza. Questa integrazione consente di configurare un sistema di controllo degli accessi Axis direttamente dal Management Client. Il sistema si integra perfettamente con XProtect, consentendo agli operatori di monitorare gli accessi ed eseguire azioni di controllo degli accessi nello Smart Client.

Nota

Requisiti

- VMS versione 2024 R1 o successiva.
- Licenze di accesso per XProtect, vedere *licenze di accesso*.
- Installare AXIS Optimizer sul server eventi e sul Management Client.

Le porte 53459 e 53461 si apriranno per il traffico in entrata (TCP) durante l'installazione di AXIS Optimizer tramite AXIS Secure Entry.

Configurazione controllo degli accessi

Nota

Prima di iniziare, fare quanto segue:

- Aggiornare il software del door controller. Consultare la tabella che segue per conoscere la versione minima e consigliata di AXIS OS per la tua versione VMS.
- Assicurarsi che la data e l'ora siano corrette.

Versione AXIS Optimizer	Versione minima AXIS OS	Versione AXIS OS consigliata
5.6	12.6.94.1	12.6.94.1

Per aggiungere un door controller di rete Axis al sistema:

1. Andare a **Site Navigation** > **Axis Optimizer** > **Access control** (Navigazione sito, Axis Optimizer, Controllo degli accessi).
2. In **Configuration** (Configurazione), selezionare **Devices** (Dispositivi).
3. Selezionare **Discovered devices** (Dispositivi rilevati) per visualizzare l'elenco delle unità che è possibile aggiungere al sistema.
4. Seleziona le unità che si desidera aggiungere.
5. Fare clic su **+ Add** (+ Aggiungi) nella finestra popup e fornire le credenziali per il controller.

Nota

Nella scheda **Management** (Gestione) si dovrebbero vedere i controller aggiunti.

Per aggiungere manualmente un controller al sistema, fare clic su **+ Add** (+ Aggiungi) nella scheda **Management** (Gestione).

Per integrare l'aggiornamento nel VMS ogni volta che si aggiunge, rimuove o si modifica il nome di un door controller:

- Andare a **Site Navigation** (navigazione del sito) > **Access control** (controllo degli accessi) e fare clic su Access Control integration (Integrazione del controllo degli accessi).
- Fare clic su **Refresh Configuration (Aggiorna configurazione)** nella scheda **General settings (Impostazioni generali)**.

Flusso di lavoro per configurare il controllo degli accessi

1. Andare a **Site Navigation** > **Axis Optimizer** > **Access control** (Navigazione sito, Axis Optimizer, Controllo degli accessi).
2. Per modificare i profili di identificazione predefiniti o creare un nuovo profilo di identificazione, vedere .
3. Per utilizzare un'impostazione personalizzata per i formati della tessera e la lunghezza del PIN, vedere .

4. Aggiungere una porta e applicare un profilo di identificazione alla porta. Vedere .
5. Aggiungere una zona e aggiungere porte alla zona. Vedere .

Compatibilità del software del dispositivo per i door controller

Importante

Quando si aggiorna il sistema operativo AXIS OS sul door controller, tenere presente quanto segue:

- **Versioni di AXIS OS supportate:** Le versioni del sistema operativo AXIS OS supportate elencate in precedenza sono valide solo in caso di aggiornamento dalla rispettiva versione VMS originale consigliata e quando il sistema è dotato di porta. Se il sistema non soddisfa queste condizioni, è necessario eseguire l'aggiornamento alla versione di AXIS OS consigliata per la versione VMS.
- **Versione minima AXIS OS supportata:** La versione di AXIS OS più vecchia installata nel sistema determina la versione minima supportata di AXIS OS, con un limite di due versioni precedenti.
- **Aggiornamento oltre la versione AXIS OS consigliata:** Supponiamo di aggiornare a una versione AXIS OS superiore a quella consigliata per una particolare versione di VMS. In tal caso, è sempre possibile eseguire il downgrade alla versione AXIS OS consigliata senza alcun problema, purché rientri nei limiti di supporto fissati per la versione di VMS.
- **Raccomandazioni per le prossime versioni AXIS OS:** Seguire sempre la versione AXIS OS consigliata per la rispettiva versione di VMS per garantire la stabilità del sistema e la piena compatibilità.

Integrazione controllo degli accessi

Per integrare il controllo degli accessi nel VMS:

1. Andare a **Site Navigation** > **Access Control** (Navigazione sito, Controllo degli accessi).
2. Fare clic con il pulsante destro del mouse su **Access Control** (Controllo degli accessi) e su **Create new...** (Crea nuovo).
3. Nella finestra di dialogo **Create Access Control System Integration** (Crea integrazione del sistemi di controllo degli accessi):
   - Immettere un nome per l'integrazione.
   - Selezionare **AXIS Secure Entry** dal menu a discesa in **Integration plug-in** (Plug-in di integrazione).
   - Fare clic su **Next** (Avanti) fino a quando non appare la finestra di dialogo **Associate cameras** (Associa telecamere).
     Per associare le telecamere agli access point delle porte:
     - Nel proprio dispositivo fare clic sulla voce **Cameras** (Telecamere) per visualizzare l'elenco delle telecamere configurate nel sistema XProtect.
     - Selezionare e trascinare una telecamera sull'access point a cui si desidera associarla.
     - Fare clic su **Close** (Chiudi) per chiudere la finestra di dialogo.

Nota

- Per ulteriori informazioni sull'integrazione del controllo degli accessi in XProtect, vedere *Utilizzo del controllo degli accessi in XProtect Smart Client*.
- Per ulteriori informazioni sulle proprietà del sistema di controllo degli accessi, quali le impostazioni generali, le porte e le telecamere associate, gli eventi di controllo degli accessi e così via, vedere *Proprietà del controllo degli accessi*.

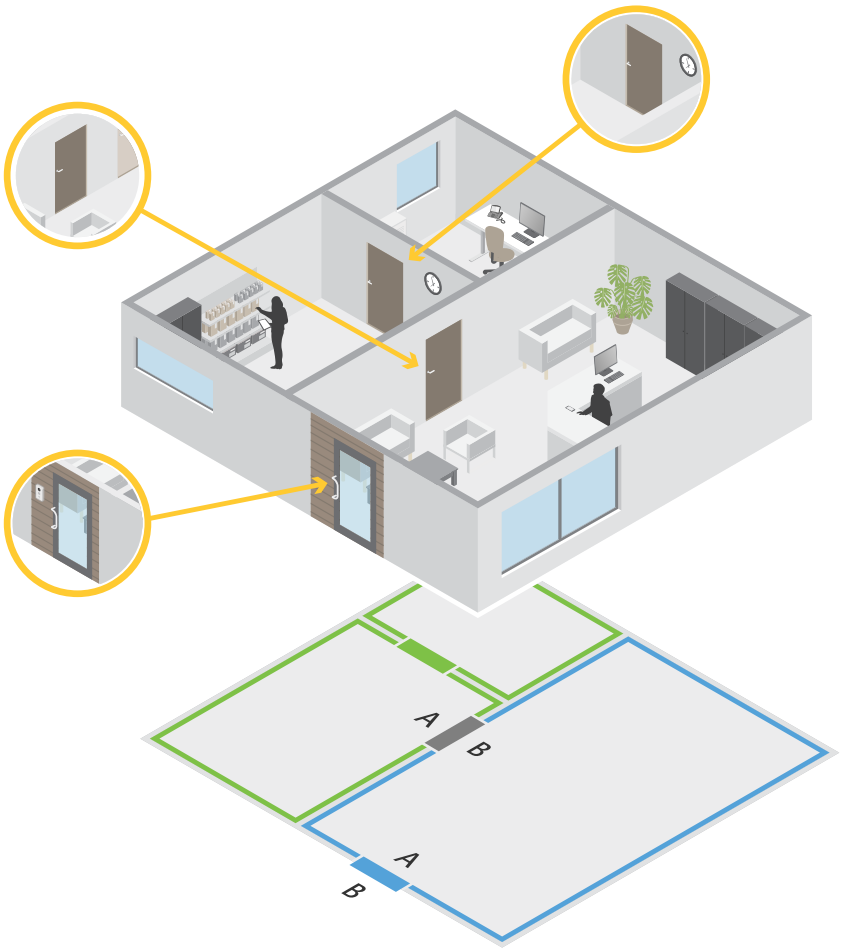
Porte e zone

Andare a **Site Navigation** > **Axis Optimizer** >**Access control** > **Doors and zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone) per ottenere una panoramica ed eseguire la configurazione di porte e zone.

Schema dei PIN	Visualizzare lo schema dei pin del controller associato a una porta. Per stampare lo schema dei pin, fare clic su **Print (Stampa)**.
Profilo di identificazione	Cambiare il profilo di identificazione delle porte.
Canale sicuro	Disattivare o attivare OSDP Secure Channel per uno specifico lettore.

Porte	
Nome	Il nome della porta.
Door controller	Il door controller connesso alla porta.
Lato A	La zona in cui si trova il lato A della porta.
Lato B	La zona in cui si trova il lato B della porta.
Profilo di identificazione	Il profilo di identificazione applicato alla porta.
Formati tessera e PIN	Mostra il tipo di formato tessera o la lunghezza del PIN.
Stato	lo stato della porta. • **Online:** la porta è online e funziona correttamente. • **Lettore offline:** il lettore nella configurazione della porta è offline. • **Errore lettore:** il lettore nella configurazione della porta non supporta il canale sicuro oppure il canale sicuro non è attivato per il lettore.
Zone	
Nome	Il nome della zona.
Numero di porte	Numero di porte incluse nella zona.

Esempio di porte e zone



- Esistono due zone: la zona verde e la zona blu.
- Esistono tre porte: porta verde, porta blu e porta marrone.
- La porta verde è una porta interna alla zona verde.
- La porta blu è una porta perimetrale solo per la zona blu.
- La porta a chiave è una porta perimetrale sia per la zona verde che per quella blu.

Aggiunta di una porta

Nota

- Si può configurare un door controller con una porta con due serrature o due porte con una serratura ciascuna.
- Se un door controller non ha porte e si sta utilizzando una nuova versione di AXIS Optimizer con software precedente sul door controller, il sistema impedirà di aggiungere una porta. Ciononostante, se c'è già una porta disponibile, il sistema consente nuove porte sui controller di sistema con software precedente.

Creare una nuova configurazione porta per aggiungere una porta:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone).
2. Fare clic su + **Add door (Aggiungi porta)**.

3. Immettere il nome della porta.
4. Nel menu a discesa **Controller (Dispositivo di controllo)**, selezionare un door controller. Il controller è disattivato (grigio) quando non si può aggiungere un'altra porta, quando è offline o HTTPS non è attivo.
5. Nel menu a discesa **Door type (Tipo di porta)**, selezionare il tipo di porta che si vuole creare.
6. Fare clic su **Next (Avanti)** per passare alla pagina di configurazione della porta.
7. Selezionare una porta relè dal menu a discesa **Primary lock (Blocco principale)**.
8. Per configurare due blocchi sulla porta, selezionare una porta relè dal menu a discesa **Secondary lock (Blocco secondario)**.
9. Selezionare un profilo di identificazione. Vedere .
10. Configurare le impostazioni della porta. Vedere .
11. Impostare una porta di monitoraggio. Vedere .
12. Fare clic su **Save (Salva)**.

Copiare una configurazione di porta esistente per aggiungere una porta:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone).
2. Fare clic su **Add door (Aggiungi porta)**.
3. Immettere il nome della porta.
4. Nel menu a discesa **Controller (Dispositivo di controllo)**, selezionare un door controller.
5. Fare clic su **Next (Avanti)**.
6. Nel menu a discesa **Copy configuration (Copia configurazione)** selezionare una configurazione di porta esistente. Mostra le porte connesse mentre il controller risulta disattivato (grigio) se è stato configurato con due porte o una porta con due serrature.
7. Modificare le impostazioni se si desidera.
8. Fare clic su **Save (Salva)**.

Per modificare una porta:

1. Andare a **Site Navigation** > **AXIS Optimizer**> **Access control** > **Doors and zones** > **Doors** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone, Porte).
2. Selezionare una porta dall'elenco.
3. Fare clic su **Edit (Modifica)**.
4. Modificare le impostazioni e fare clic su **Save (Salva)**.

Per rimuovere una porta:

1. Andare a **Site Navigation** > **AXIS Optimizer**> **Access control** > **Doors and zones** > **Doors** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone, Porte).
2. Selezionare una porta dall'elenco.
3. Fare clic su **Remove (Rimuovi)**.
4. Fare clic su **Sì**.

Per integrare l'aggiornamento nel VMS ogni volta che si aggiunge, rimuove o si modifica il nome di una porta:

1. Andare a **Site Navigation** (navigazione sito) > **Access control** (controllo degli accessi) e fare clic su Access Control integration (Integrazione del controllo degli accessi).
2. Fare clic su **Refresh Configuration (Aggiorna configurazione)** nella scheda **General settings (Impostazioni generali)**.

Impostazioni della porta

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone).
2. Selezionare la porta che si desidera modificare.
3. Fare clic su **Edit (Modifica)**.

Tempo di accesso (sec)	Impostare il numero di secondi per cui la porta rimane sbloccata dopo aver consentito l'accesso. La porta rimane sbloccata fino all'apertura della porta o alla fine del tempo impostato. La porta si blocca quando si chiude anche se rimane del tempo di accesso a disposizione.
Open-too-long time (sec) (Tempo di apertura eccessivo (sec))	Valido solo se si è configurato un monitor porta. Impostare il numero di secondi durante i quali la porta resta aperta. Se la porta è aperta al termine del tempo impostato, si attiva l'allarme tempo di apertura eccessivo. Impostare una regola di azione per configurare l'azione che verrà attivata dall'evento porta aperta troppo a lungo.
Tempo di accesso lungo (sec)	Impostare il numero di secondi per cui la porta rimane sbloccata dopo aver consentito l'accesso. Il tempo di accesso lungo sovrascrive il tempo di accesso per i titolari della tessera che ha questa impostazione attivata.
Long open-too-long time (sec) (Tempo di apertura eccessivo lungo (sec))	Valido solo se si è configurato un monitor porta. Impostare il numero di secondi durante i quali la porta resta aperta. Se la porta è aperta al termine del tempo impostato, si attiva l'evento tempo di apertura eccessivo. Il tempo di apertura eccessivo lungo sovrascrive il tempo di apertura eccessivo già impostato per i titolari della tessera se si attiva l'impostazione **Long access time (Tempo di accesso lungo)**.
Ritardo ripetizione blocco (ms)	Impostare il tempo di sblocco della porta in millisecondi dopo l'apertura o la chiusura.
Ripetizione blocco	• **After opening (Dopo l'apertura):** valido solo se è stato aggiunto un monitor porta. • **After closing (Dopo la chiusura):** valido solo se è stato aggiunto un monitor porta.

Livello di sicurezza porta

È possibile aggiungere le seguenti funzionalità di sicurezza alla porta:

Regola due persone – La regola per due persone richiede a due persone di utilizzare una credenziale valida per ottenere l'accesso.

Doppia passata – La doppia passata permette al titolare tessera di sovrascrivere lo stato corrente di una porta. Ad esempio, può usarla per il blocco o lo sblocco di una porta fuori della pianificazione normale, il che è più comodo che accedere al sistema per sbloccare la porta. Il doppio scorrimento non influisce su una pianificazione esistente. Ad esempio, se è pianificato il blocco di una porta all'ora di chiusura e un dipendente esce per la pausa pranzo, la porta si blocca comunque in base alla pianificazione.

È possibile configurare il livello di sicurezza quando si aggiunge una nuova porta o per una porta esistente.

Per aggiungere una **regola due persone** a una porta esistente:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone).
2. Selezionare la porta per la quale si desidera configurare un livello di sicurezza.
3. Fare clic su **Edit (Modifica)**.
4. Fare clic su **Security level (Livello di sicurezza)**.
5. Attiva una **regola due persone**.
6. fare clic su **Applica**;

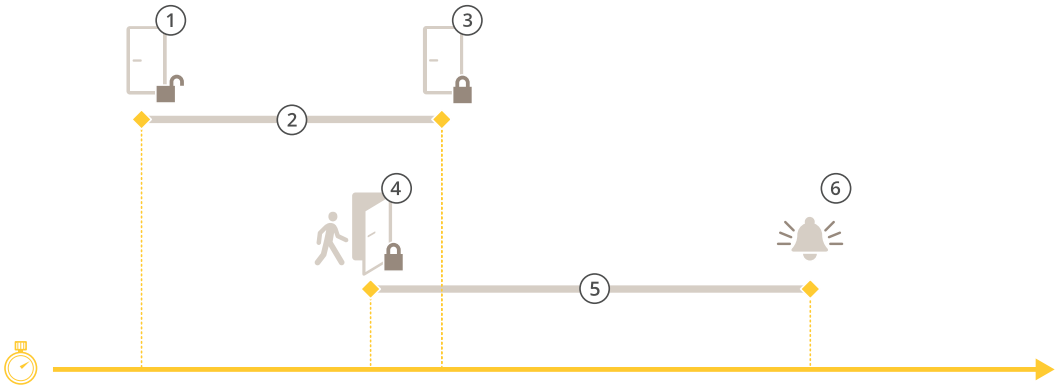
Regola due persone	
Side A (Lato A) e **Side B (Lato B)**	Selezionare i lati della porta su cui usare la regola.
Pianificazioni	Selezionare quando è attiva la regola.
Timeout (secondi)	Timeout è il tempo massimo consentito tra i passaggi di tessera o altri tipi di credenziali valide.

Per aggiungere una **Doppia passata** a una porta esistente:

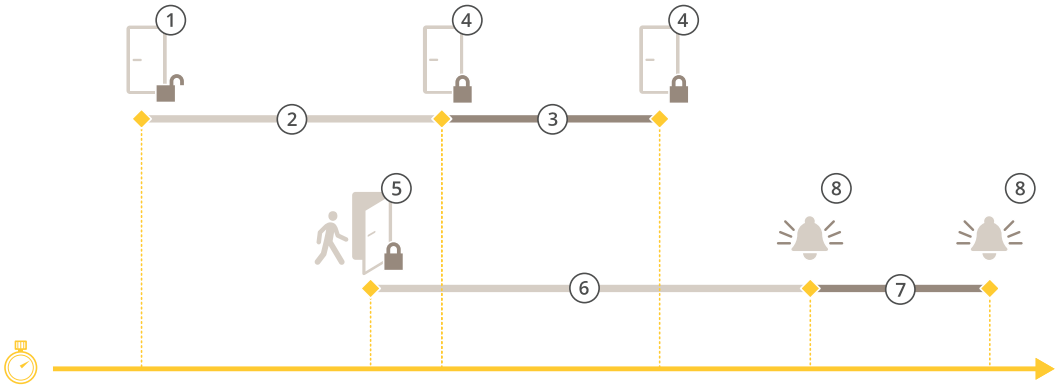
1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone).
2. Selezionare la porta per la quale si desidera configurare un livello di sicurezza.
3. Fare clic su **Edit (Modifica)**.
4. Fare clic su **Security level (Livello di sicurezza)**.
5. Attivare la **Doppia passata**.
6. fare clic su **Applica**;
7. Applicare la **Double-swipe (Doppia passata)** a un titolare della tessera.
   7.1. Andare in **Cardholder management (Gestione titolari tessere)**.
   7.2. Fare clic su ⋮ sul titolare della tessera che si desidera modificare e fare clic su **Edit (Modifica)**.
   7.3. Fare clic su **More (Altro)**.
   7.4. Selezionare **Allow double-swipe (Consenti doppia passata)**.
   7.5. fare clic su **Applica**;

Doppia passata	
Timeout (secondi)	Timeout è il tempo massimo consentito tra i passaggi di tessera o altri tipi di credenziali valide.

Opzioni relative all'orario



1 *Accesso consentito: la serratura si sblocca*
2 *Tempo di accesso*
3 *Nessuna azione compiuta: la serratura si blocca*
4 *Azione compiuta (porta aperta): la serratura si blocca o rimane sbloccata finché non si chiude la porta*
5 *Tempo di apertura eccessivo*
6 *Scatta l'allarme tempo di apertura eccessivo*



1 *Accesso consentito: la serratura si sblocca*
2 *Tempo di accesso*
3 *2+3: Tempo di accesso lungo*
4 *Nessuna azione compiuta: la serratura si blocca*
5 *Azione compiuta (porta aperta): la serratura si blocca o rimane sbloccata finché non si chiude la porta*
6 *Tempo di apertura eccessivo*
7 *6+7: Tempo di apertura eccessivo lungo:*
8 *Scatta l'allarme tempo di apertura eccessivo*

Aggiungi un monitor porta

Un monitor porta è uno switch di posizione della porta che controlla lo stato fisico di una porta. È possibile aggiungere un monitor porta alla porta e configurare la modalità di collegamento del monitor porta.

1. Andare alla pagina di configurazione della porta. Vedere
2. In **Sensors (Sensori)**, fare clic su **Add (Aggiungi)**.
3. Selezionare **Door monitor sensor (Sensore monitor porta)**.
4. Selezionare la porta I/O a cui si desidera collegare il monitor porta.

5. In **Door open if (Porta aperta se)**, selezionare la modalità di collegamento dei circuiti del monitor della porta.
6. Per ignorare le modifiche di stato dell'input digitale prima che entri in un nuovo stato stabile, imposta un **Debounce time (Tempo debounce)**.
7. Per attivare un evento quando avviene un'interruzione della connessione tra il door controller e il monitor porta, attivare il **Supervised input (Input supervisionato)**. Vedere .

Porta aperta se	
Circuito aperto	Il circuito del monitor porta è normalmente chiuso. Quando il circuito è aperto, il monitor porta invia un segnale di porta aperta. Quando il circuito è chiuso, il monitor porte invia un segnale di porta chiusa.
Circuito chiuso	Il circuito del monitor porta è normalmente aperto. Quando il circuito è chiuso, il monitor porta invia un segnale di porta aperta. Quando il circuito è aperto, il monitor porta invia un segnale di porta chiusa.

Aggiungere una porta di monitoraggio

Una porta di monitoraggio è un tipo di porta che può mostrare se è aperta o chiusa. Ad esempio, è possibile utilizzarla per una porta antincendio che non richiede una serratura, ma è necessario sapere se è aperta.

Una porta di monitoraggio è diversa da una porta normale dotata di monitor. Una porta normale con monitor supporta serrature e lettori, ma richiede un door controller. Una porta di monitoraggio supporta un sensore di posizione delle porte ma richiede solo un modulo relè I/O di rete collegato a un door controller. È possibile collegare fino a cinque sensori di posizione delle porte a un modulo relè I/O di rete.

Nota

Una porta di monitoraggio richiede un AXIS A9210 Network I/O Relay Module con il software più recente, inclusa l'applicazione AXIS Monitoring Door ACAP.

Per impostare una porta di monitoraggio:

1. Installare AXIS A9210 ed eseguire l'aggiornamento con l'ultima versione di AXIS OS.
2. Installare i sensori di posizione delle porte.
3. Nel VMS, andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone).
4. Fare clic su **Add door (Aggiungi porta)**.
5. Inserire un nome.
6. In **Type (Tipo)**, selezionare **Monitoring door (Porta di monitoraggio)**.
7. In **Device (Dispositivo)**, selezionare il modulo relè I/O di rete.
8. Fare clic su **Next (Avanti)**.
9. In **Sensors (Sensori)**, fare clic su **+ Add (+ Aggiungi)** e selezionare **Door position sensor (Sensore di posizione delle porte)**.
10. Selezionare la porta I/O connessa al sensore di posizione delle porte.
11. Fare clic su **Aggiungi**.

Aggiungi un lettore

Si può eseguire la configurazione di un door controller in modo da usare due lettori cablati. Scegliere di aggiungere un lettore su un lato o su entrambi i lati di una porta.

Se si applica un'impostazione personalizzata dei formati tessera o della lunghezza del PIN a un lettore, sarà visibile in **Card formats (Formati tessera)** in **Configuration > Access control > Doors and zones (Configurazione > Controllo degli accessi > Porte e zone)**. Vedere .

1. Andare alla pagina di configurazione della porta. Vedere
2. Sotto un lato della porta, fare clic su **Add (Aggiungi)**.
3. Selezionare **Card reader (Lettore di schede)**.
4. Selezionare **Reader type (Tipo di lettore)**.
5. Per usare una configurazione personalizzata della lunghezza del PIN per questo lettore.
   5.1. fare clic su **Avanzate**;
   5.2. Attivare **Custom PIN length (Lunghezza PIN personalizzata)**.
   5.3. Imposta la **Min PIN length (Lunghezza PIN minima)**, **Max PIN length (Lunghezza PIN massima)** e **End of PIN character (Fine del carattere PIN)**.
6. Per usare un formato tessera personalizzato per questo lettore.
   6.1. fare clic su **Avanzate**;
   6.2. Attivare i **Custom card formats (Formati tessera personalizzati)**.
   6.3. Selezionare i formati tessera che si desidera utilizzare per il lettore. Se è già in uso un formato tessera con la stessa lunghezza in bit, è necessario disattivarlo prima. Un'icona di avviso appare nel client quando la configurazione del formato scheda differisce dall'impostazione del sistema configurata.
7. Fare clic su **Aggiungi**.
8. Per l'aggiunta di un lettore all'altro lato della porta, ripetere questa procedura.

Tipo di lettore	
OSDP RS485 half-duplex	Per i lettori RS485, selezionare **OSDP RS485 half-duplex** e una porta per il lettore.
Wiegand	Per i lettori che usano i protocolli Wiegand, selezionare **Wiegand** e una porta per il lettore.

Wiegand	
Comando LED	Selezionare **Single wire (Cavo singolo)** o **Dual wire (R/G) (Cavo doppio (R/G))**. I lettori con controllo LED doppio utilizzano cavi diversi per i LED rossi e verdi.
Avviso manomissione	Selezionare quando l'input manomissione del lettore è attivo. • **Open circuit (Circuito aperto)**: Il lettore invia il segnale di manomissione alla porta quando il circuito è aperto. • **Closed circuit (Circuito chiuso)**: Il lettore invia il segnale di manomissione alla porta quando il circuito è chiuso.
Tamper debounce time (Tempo debounce manomissione)	Per ignorare le variazioni di stato dell'input manomissione del lettore prima che entri in un nuovo stato stabile, impostare un **Tamper debounce time (Tempo debounce manomissione)**.
Input supervisionato	Attivare per il trigger di un evento quando c'è un'interruzione della connessione tra il door controller e il lettore. Vedere .

Aggiungi un dispositivo REX

È possibile scegliere di aggiungere una richiesta per uscire da un dispositivo (REX) su un lato o su entrambi i lati della porta. Un dispositivo REX può essere un sensore PIR, un pulsante REX o un maniglione.

1. Andare alla pagina di configurazione della porta. Vedere
2. Sotto un lato della porta, fare clic su **Add (Aggiungi)**.
3. Selezionare **REX device (Dispositivo REX)**.
4. Selezionare la porta I/O a cui si desidera collegare il dispositivo REX. Se è disponibile una sola porta, verrà selezionata automaticamente.
5. Selezionare quale **Action (Azione)** attivare quando la porta riceve il segnale REX.
6. Selezionare la connessione circuiti del monitor della porta in **REX active (REX attivo)**.
7. Per ignorare le modifiche allo stato dell'ingresso digitale prima che entri in un nuovo stato stabile, configurare l'opzione **Debounce time (ms) (Tempo debounce (ms))**.
8. Per attivare un evento quando avviene un'interruzione della connessione tra il door controller e il dispositivo REX, attivare **Supervised input (Input supervisionato)**. Vedere .

Azione	
Sblocca porta	Sceglierlo per sbloccare la porta nel momento in cui riceve il segnale REX.
Nessuna	Selezionare questa opzione se non si desidera attivare alcuna azione quando la porta riceve il segnale REX.

REX attivo	
Circuito aperto	Selezionare questa opzione se il circuito REX è normalmente chiuso. Il dispositivo REX invia il segnale quando il circuito è aperto.
Circuito chiuso	Selezionare questa opzione se il circuito REX è normalmente aperto. Il dispositivo REX invia il segnale quando il circuito è chiuso.

Aggiunta di una zona

Una zona è un'area fisica specifica con un gruppo di porte. È possibile creare zone e aggiungere porte alle zone. Esistono due tipi di porte:

- **Perimeter door (Porta perimetrale):** Cardholders enter or leave the zone through this door (I titolari della tessera entrano nella zona o la abbandonano attraverso questa porta).
- **Internal door (Porta interna):** An internal door within the zone (Una porta interna all'interno della zona).

Nota

Una porta perimetrale può appartenere a due zone. Una porta interna può appartenere a una sola zona.

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** > **Zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone, Zone).
2. Fare clic su + **Add zone (Aggiungi zona)**.
3. Immettere il nome di una zona.
4. Fare clic su **Add door (Aggiungi porta)**.
5. Selezionare le porte che si vuole aggiungere alla zona e fare clic su **Add (Aggiungi)**.

6. La porta è impostata come porta perimetrale per impostazione predefinita. Per modificarla, selezionare **Internal door (Porta interna)** dal menu a discesa.
7. Per impostazione predefinita, una porta del perimetro impiega il lato della porta A come ingresso per la zona. Per modificare questa impostazione, selezionare **Leave (Abbandona)** dal menu a discesa.
8. Per rimuovere una porta dalla zona, selezionarla e fare clic su **Remove (Rimuovi)**.
9. Fare clic su **Save (Salva)**.

Per modificare una zona:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** > **Zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone, Zone).
2. Selezionare una zona dall'elenco.
3. Fare clic su **Edit (Modifica)**.
4. Modificare le impostazioni e fare clic su **Save (Salva)**.

Per rimuovere una zona:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** > **Zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone, Zone).
2. Selezionare una zona dall'elenco.
3. Fare clic su **Remove (Rimuovi)**.
4. Fare clic su **Sì**.

Livello di sicurezza zona

Si può aggiungere la funzionalità di sicurezza che segue ad una zona:

Anti-passback – Fa sì che le persone non possano impiegare le stesse credenziali di qualcuno entrato in un'area prima di loro. Impone l'uscita dall'area prima che si possano usare di nuovo le proprie credenziali.

Nota

- Con l'anti-passback, tutte le porte nella zona devono avere sensori di posizione della porta in modo che il sistema possa registrare che un utente ha aperto la porta dopo aver passato la carta.
- Se un door controller passa offline, l'anti-passback funziona finché tutte le porte nella zona appartengono allo stesso door controller. Tuttavia, se le porte nella zona appartengono a diversi door controller che passano offline, l'anti-passback smette di funzionare.

Si può eseguire la configurazione del livello di sicurezza quando si aggiunge una nuova area o si può fare in una zona esistente. Per eseguire l'aggiunta di un livello di sicurezza a una zona esistente:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone).
2. Eseguire la selezione della zona per la quale si desidera configurare un livello di sicurezza.
3. Fare clic su **Edit (Modifica)**.
4. Fare clic su **Security level (Livello di sicurezza)**.
5. Eseguire l'attivazione delle funzioni di sicurezza che si vogliono aggiungere alla porta.
6. fare clic su **Applica**;

Anti-passback	
Log violation only (Soft) (Solo log violazione (tollerante))	Usare se si vuole permettere a una seconda persona di entrare dalla porta usando le stesse credenziali della prima persona. Questa opzione risulta unicamente in un allarme di sistema.

Deny access (Hard) (Nega accesso (rigido))	Da usare se si vuole evitare che il secondo utente entri dalla porta nel caso usi le stesse credenziali della prima persona. Anche questa opzione risulta in un allarme di sistema.
Timeout (secondi)	Il tempo che deve trascorrere prima che il sistema consenta all'utente di entrare di nuovo. Immettere 0 se non si vuole un timeout, il che significa che la zona ha l'anti-passback finché l'utente non lascia la zona. Usare unicamente il timeout **0** con **Deny access (Hard) (Nega accesso (rigido))** se tutte le porte nella zona hanno lettori su entrambi i lati.

Ingressi con supervisione

Gli ingressi supervisionati sono in grado di attivare un evento se si verifica un'interruzione della connessione a un door controller.

- Collegamento tra Door controller e Door monitor. Vedere .
- Collegamento tra Door controller e lettore basato su protocolli Wiegand. Vedi .
- Collegamento tra Door controller e dispositivo REX. Vedere .

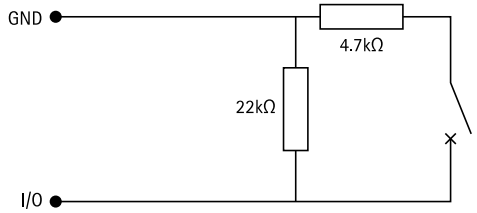
Per utilizzare gli input supervisionati:

1. Installare resistori terminali il più vicino possibile al dispositivo periferico secondo lo schema delle connessioni.
2. Andare alla pagina di configurazione di un lettore, di un monitor porta o di un dispositivo REX, attivare **Supervised input (Input supervisionato)**.
3. Se è stato seguito lo schema di prima connessione parallela, selezionare **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Prima connessione parallela con un resistore parallelo da 22 KΩ e un resistore seriale da 4,7 KΩ)**.
4. Se è stato seguito lo schema di prima connessione in serie, selezionare **Serial first connection (Prima connessione in serie)** e selezionare un valore dei resistori dal menu a discesa **Resistor values (Valori resistore)**.

Schemi delle connessioni

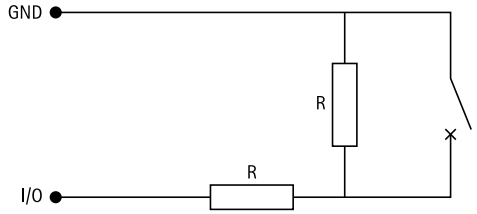
Prima connessione parallela

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



Connessione prima in serie

I valori dei resistori devono essere uguali nell'intervallo compreso tra 1 e 10 kΩ.



Azioni manuali

È possibile eseguire le seguenti azioni manuali su porte e zone:

Ripristina – Ritorna alle regole di sistema configurate.

Consenti accesso – Sblocca una porta o una zona per 7 secondi e poi la blocca di nuovo.

Sblocca – Mantiene la porta aperta fino al reset.

Serratura – Mantiene chiusa la porta finché il sistema non concede l'accesso a un titolare di tessera.

Chiusura totale – Nessuno può entrare o uscire finché non si resetta o si sblocca.

Per eseguire un'azione manuale:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone).
2. Selezionare la porta o la zona su cui si desidera eseguire un'azione manuale.
3. Fare clic su una qualsiasi delle azioni manuali.

Formati tessera e PIN

Un formato tessera definisce la modalità in cui una tessera memorizza i dati. Si tratta di una tabella di conversione tra i dati in ingresso e i dati convalidati nel sistema. Ciascun formato di tessera dispone di un set di regole diverso riguardante il modo di organizzare le informazioni memorizzate. Definendo un formato tessera si indica al sistema come interpretare le informazioni che il dispositivo di controllo ottiene dal lettore di tessere.

Esistono formati di tessera comunemente usati predefiniti che è possibile utilizzare così come sono o modificare in base alle necessità. È possibile inoltre creare formati tessera personalizzati.

Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Formati tessera e PIN) per la creazione, la modifica o l'attivazione dei formati tessera. È inoltre possibile configurare il PIN.

I formati della tessera personalizzati possono contenere i seguenti campi dati utilizzati per la convalida delle credenziali.

Numero tessera – Un sottoinsieme dei dati binari delle credenziali codificati come numeri decimali o esadecimali. Usare il codice carta per identificare un titolare o una tessera specifica.

Codice struttura – Un sottoinsieme dei dati binari delle credenziali codificati come numeri decimali o esadecimali. Usare il codice struttura per identificare un sito o un cliente finale specifico.

Per creare un formato tessera:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Formati tessera e PIN).
2. Fare clic su **Add card format (Aggiungi formato scheda)**.
3. Inserire un nome per il formato tessera.
4. Digitare una lunghezza in bit tra 1 e 256 nel campo **Bit length (Lunghezza in bit)**.
5. Selezionare **Invert bit order (Inverti ordine dei bit)** se si desidera invertire l'ordine dei bit dei dati ricevuti dal lettore di tessere.
6. Selezionare **Invert byte order (Inverti ordine dei byte)** se si desidera invertire l'ordine dei byte dei dati ricevuti dal lettore di tessere. Questa opzione è disponibile solo quando si specifica una lunghezza in bit che si può dividere per otto.
7. Selezionare e configurare i campi dati in modo che siano attivi nel formato tessera. Il **Card number (Codice carta)** o il **Facility code (Codice struttura)**.
8. Fare clic su **OK**.

9. Per attivare il formato della tessera, selezionare la casella di controllo davanti al nome del formato della tessera.

Nota

- Non è possibile che due formati scheda con la stessa lunghezza in bit possano essere attivi contemporaneamente. Ad esempio, se sono stati definiti due formati di tessera a 32 bit, solo uno può essere attivo. Eseguire la disattivazione del formato tessera per attivare l'altro.
- È possibile attivare e disattivare i formati scheda solo se il door controller è stato configurato con almeno un lettore.

ⓘ	Fare clic su ⓘ per vedere un esempio di output dopo l'inversione dell'ordine dei bit.
Intervallo	Impostare l'intervallo bit dei dati per il campo dati. L'intervallo deve essere compreso tra i valori specificati per **Bit length (Lunghezza in bit)**.
Formato di output	Selezionare il formato di output dei dati per il campo dati. **Decimal (Decimale)**: noto anche come sistema numerico posizionale in base 10, è composto dai numeri compresi tra 0 e 9. **Hexadecimal (esadecimale)**: noto anche come sistema numerico posizionale in base 16, è composto da 16 simboli unici: i numeri 0-9 e le lettere a-f.
Ordine bit di subrange	Selezionare l'ordine dei bit. **Little endian**: il primo bit è il più piccolo (meno significativo). **Big endian**: il primo bit è il più grande (più significativo).

Per modificare il formato di una tessera:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Formati tessera e PIN).
2. Selezionare un formato tessera e fare clic su ✎.
3. Se cambia un formato tessera predefinito, si può modificare solo **Invert bit order (Inverti ordine dei bit)** e **Invert byte order (Inverti ordine dei byte)**.
4. Fare clic su **OK**.

È possibile rimuovere solo i formati tessera personalizzati. Per rimuovere un formato tessera personalizzato:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Formati tessera e PIN).
2. Selezionare un formato tessera personalizzato, fare clic su 🗑 e **Yes (Sì)**.

Per il reset di un formato tessera predefinito:

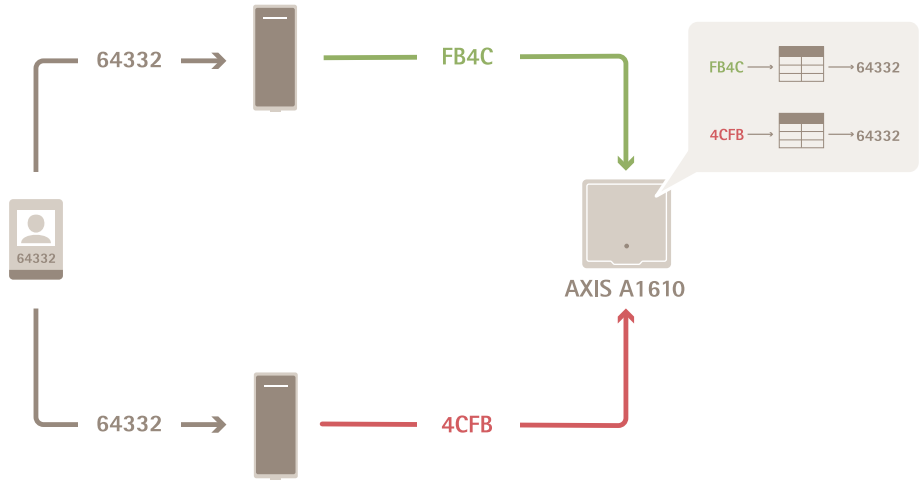
1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Formati tessera e PIN).
2. Fare clic su ↺ per ripristinare un formato tessera alla mappa dei campi predefinita.

Per configurare la lunghezza PIN:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Formati tessera e PIN).
2. In **PIN configuration (Configurazione PIN)** fare clic su .
3. Specificare **Min PIN length (Lunghezza PIN minima)**, **Max PIN length (Lunghezza PIN massima)** e **End of PIN character (Fine del carattere PIN)**.
4. Fare clic su **OK**.

Impostazioni formato tessera

Panoramica



- Il codice carta in decimale è `64332`.
- Un lettore trasferisce il codice carta al numero esadecimale `FB4C`. L'altro lettore la trasferisce al numero esadecimale `4CFB`.
- AXIS A1610 Network Door Controller riceve `FB4C` e lo trasferisce al numero decimale `64332` in base alle impostazioni del formato tessera nel lettore.
- AXIS A1610 Network Door Controller riceve `4CFB` e lo cambia in `FB4C` invertendo l'ordine dei byte e lo trasferisce al numero decimale `64332` in base alle impostazioni del formato tessera nel lettore.

Inverti ordine bit

Dopo aver capovolto l'ordine dei bit, i dati della scheda ricevuti dal lettore vengono letti da destra a sinistra bit per bit.

Inverti ordine byte

Un gruppo di otto bit è un byte. Dopo aver capovolto l'ordine dei byte, i dati della scheda ricevuti dal lettore vengono letti da destra a sinistra byte per byte.

Formato tessera Wiegand standard a 26 bit

1 *Parità principale*
2 *Codice struttura*
3 *Numero tessera*
4 *Parità finale*

Profili di identificazione

Un profilo di identificazione è una combinazione di tipi di identificazione e pianificazioni. Si può applicare un profilo di identificazione a una o molteplici porte per impostare come e quando un titolare tessera è in grado di accedere a una porta.

I tipi di identificazione sono vettori di credenziali necessarie per l'accesso a una porta. I tipi di identificazione più diffusi sono i token, i numeri di identificazione personale (PIN), le impronte digitali, le mappe facciali e i dispositivi REX. È possibile che un tipo di identificazione contenga uno o molteplici tipi di informazioni.

Le pianificazioni, note anche come **Profili temporali**, sono generate nel Management Client. Per impostare i profili temporali, consultare *Profili temporali (spiegazione)*.

Tipi di identificazione supportati: Tessera, PIN e REX.

Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Profili di identificazione).

Sono disponibili cinque profili di identificazione predefiniti da utilizzare così come sono o modificare secondo necessità.

Badge – I titolari della tessera devono strisciare la tessera per accedere alla porta.

Tessera e PIN – I titolari della tessera devono strisciare la tessera e inserire il PIN per accedere alla porta.

PIN – I titolari della tessera devono inserire il PIN per accedere alla porta.

Tessera o PIN – I titolari della tessera devono strisciare la tessera o inserire il PIN per accedere alla porta.

Targa – I titolari della tessera devono dirigersi verso la telecamera a bordo di un veicolo con targa omologata.

Per creare profilo di identificazione:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Profili di identificazione).
2. Fare clic su **Create identification profile (Creare profilo di identificazione)**.
3. Inserire un nome per il profilo di identificazione.
4. Selezionare **Include facility code for card validation (Includi codice struttura per convalida tessera)** per utilizzare il codice struttura come uno dei campi di convalida delle credenziali. Questo campo è disponibile solo se si attiva **Facility code (Codice struttura)** in **Access management > Settings (Gestione degli accessi > Impostazioni)**.
5. Eseguire la configurazione del profilo di identificazione per un lato della porta.
6. Sull'altro lato della porta, ripetere i passaggi precedenti.

7. Fare clic su **OK**.

Per modificare un profilo di identificazione:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Profili di identificazione).
2. Selezionare un profilo di identificazione e fare clic su .
3. Per cambiare il nome del profilo di identificazione, inserire un nuovo nome.
4. Eseguire le modifiche per il lato della porta.
5. Per modificare il profilo di identificazione dall'altro lato della porta, ripetere i passaggi precedenti.
6. Fare clic su **OK**.

Per rimuovere profilo di identificazione:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Profili di identificazione).
2. Selezionare un profilo di identificazione e fare clic su .
3. Se il profilo di identificazione è usato su una porta, selezionare un altro profilo di identificazione per la porta.
4. Fare clic su **OK**.

Modifica profilo di identificazione	
×	Per rimuovere un tipo di identificazione e la pianificazione correlata.
Tipo di identificazione	Per modificare un tipo di identificazione, selezionare uno o più tipi dal menu a discesa **Identification type (Tipo di identificazione)**.
Pianificazione	Per modificare una pianificazione, selezionare una o più pianificazioni dal menu a discesa **Schedule (Pianificazione)**.
+ **Aggiungi**	Aggiungere un tipo di identificazione e la pianificazione correlata, fare clic su **Add (Aggiungi)** e impostare i tipi di identificazione e le pianificazioni.

Comunicazione crittografata

Canale sicuro OSDP

Secure Entry supporta il canale sicuro OSDP (Open Supervised Device Protocol) per l'attivazione della crittografia della linea tra il dispositivo di controllo e i lettori Axis.

Per attivare il canale sicuro OSDP per un intero sistema:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Encrypted communication** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Comunicazione criptata).
2. Inserire la chiave di crittografia principale e fare clic su **OK**.
3. Attivare **OSDP Secure Channel (Canale sicuro OSDP)**. Solo dopo l'inserimento della chiave di crittografia principale questa opzione diventa disponibile.
4. Per impostazione predefinita, la chiave di crittografia principale genera una chiave del canale sicuro OSDP. Per impostare in modo manuale la chiave del canale sicuro OSDP:

   4.1. In **OSDP Secure Channel (Canale sicuro OSDP)** fare clic su .

4.2. Deselezionare **Use main encryption key to generate OSDP Secure Channel key (Utilizzare la chiave di crittografia principale per generare la chiave del canale sicuro OSDP)**.

4.3. Inserire la chiave del canale sicuro OSDP e fare clic su **OK**.

Per l'attivazione o la disattivazione del canale sicuro OSDP per un lettore specifico, vedere *Porte e zone*.

Multi-server BETA

I server secondari collegati possono, con multi server, usare i titolari di tessera e i gruppi di titolari di tessera globali dal server principale.

Nota

- Un sistema è un grado di supportare un massimo di 64 server secondari.
- Il server principale e i server secondari devono essere sulla stessa rete.
- Sui server principali e sui server secondari, assicurati di configurare Windows Firewall per permettere le connessioni TCP in entrata sulla porta Secure Entry. La porta predefinita è 53461.

Flusso di lavoro

1. Configura un server come server secondario e genera il file di configurazione. Vedere .
2. Configura un server come server principale e importa il file di configurazione dei server secondari. Vedere .
3. Configura i titolari di tessera e i gruppi di titolari di tessera globali nel server principale. Vedere e .
4. Visualizza e monitora i titolari di tessera e i gruppi di titolari di tessera globali dal server secondario. Consultare .

Genera il file di configurazione dal server secondario

1. Dal server secondario, andare a **AXIS Optimizer** > **Access control** > **Multi server** (AXIS Optimizer, Controllo degli accessi, Multiserver).
2. Fai clic su **Sub server (Server secondario)**.
3. Fare clic su **Generate (Genera)**. Viene generato un file di configurazione in formato .json.
4. Fai clic su **Download** e scegli una posizione per salvare il file.

Importa il file di configurazione sul server principale

1. Dal server principale, andare a **AXIS Optimizer** > **Access control** > **Multi server** (AXIS Optimizer, Controllo degli accessi, Multiserver).
2. Fai clic su **Main server (Server principale)**.
3. Fare clic su + **Add (Aggiungi)** e andare al file di configurazione generato dal server secondario.
4. Inserisci il nome del server, l'indirizzo IP e il numero di porta del server secondario.
5. Fare clic su **Import (Importa)** per eseguire l'aggiunta del server secondario.
6. Lo stato del server secondario indicato è `Connected`.

Revoca un server secondario

Si può revocare un server secondario solo prima di importarne il file di configurazione su un server principale.

1. Dal server principale, andare a **AXIS Optimizer** > **Access control** > **Multi server** (AXIS Optimizer, Controllo degli accessi, Multiserver).
2. Fai clic su **Sub server (Server secondario)** e fai clic su **Revoke server (Revoca server)**.
Ora puoi configurare questo server come server principale o secondario.

Rimuovi un server secondario

Dopo l'importazione del file di configurazione di un server secondario, connette il server secondario al server principale.

Per rimuovere un server secondario:

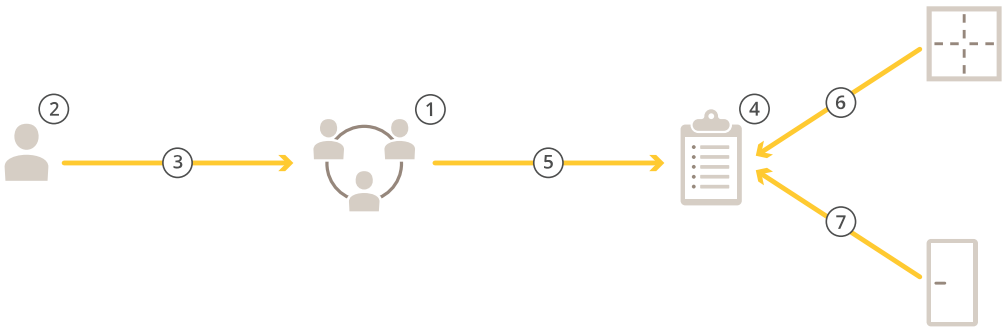
1. Dal server principale:
   1.1. Andare a **Access management** > **Dashboard** (Gestione degli accessi, Dashboard).
   1.2. Trasformare i titolari di tessera e i gruppi globali in titolari di tessera e gruppi locali.
   1.3. Andare a **AXIS Optimizer** > **Access control** > **Multi server** (AXIS Optimizer, Controllo degli accessi, Multiserver).
   1.4. Fare clic su **Main server (Server principale)** per mostrare l'elenco dei server secondari.
   1.5. Seleziona il server secondario e fai clic su **Delete (Elimina)**.
2. Dal server secondario:
   – Andare a **AXIS Optimizer** > **Access control** > **Multi server** (AXIS Optimizer, Controllo degli accessi, Multiserver).
   – Fare clic su **Sub server (Server secondario)** e su **Revoke server (Revoca server)**.

Gestione degli accessi

La scheda Access management (Gestione degli accessi) consente di configurare e gestire gli utenti, i titolari di tessere, i gruppi e le regole di accesso del sistema.

Flusso di lavoro di gestione degli accessi

La struttura di gestione degli accessi è flessibile. Questo consente all'utente di sviluppare un flusso di lavoro più adatto alle proprie esigenze. Di seguito è riportato un esempio di flusso di lavoro:



1. Aggiungi gruppi. Vedere .
2. Aggiungi titolari tessera. Vedere .
3. Aggiunta di titolari di tessera ai gruppi.
4. Aggiungi regole di accesso. Vedere .
5. Applicazione di gruppi alle regole di accesso.
6. Applicare le zone alle regole di accesso.
7. Applicare le porte alle regole di accesso.

Aggiungi un titolare tessera

Il titolare della tessera è una persona con un ID univoco registrato nel sistema. Eseguire la configurazione di un titolare della tessera con le credenziali che identificano la persona e il modo e il momento in cui lasciarla passare dalle porte.

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Cardholder management** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Gestione titolare tessera).
2. Andare su **Cardholders (Titolari tessera)** e fare clic su **+ Add (+ Aggiungi)**.
3. Immettere il nome e il cognome del titolare di tessere e fare clic su **Next (Avanti)**.
4. Oppure, fare clic su **Advanced (Avenzate)** e selezionare le opzioni.
5. Aggiungere una credenziale al titolare di tessere. Vedere
6. Fare clic su **Save (Salva)**.
7. Aggiunge il titolare di tessere a un gruppo.
   7.1. In **Groups (Gruppi)**, selezionare il gruppo a cui si vuole aggiungere il titolare di tessere e fare clic su **Edit (Modifica)**.
   7.2. Fare clic su **+Add (+Aggiungi)** e selezionare il titolare di tessere che si desidera aggiungere al gruppo. È possibile selezionare più titolari di tessere.
   7.3. Fare clic su **Aggiungi**.
   7.4. Fare clic su **Save (Salva)**.

Avanzata	
Tempo di accesso lungo	Selezionare per consentire al titolare della tessera un tempo di accesso lungo e un tempo di apertura eccessivo lungo quando c'è un monitor porta installato.
Sospendi titolare tessera	Selezionare per eseguire la sospensione del titolare tessera.
Allow double-swipe (Consenti doppia passata)	Selezionare per consentire a un titolare di tessere di ignorare lo stato corrente di una porta. Ad esempio, ha la possibilità di usarla per lo sblocco di una porta al di fuori della pianificazione normale.
Esente da blocco	Selezionare per permettere al titolare della tessera l'accesso durante il blocco.
Exempt from anti-passback (Esente da anti-passback)	Selezionare per dare al titolare della carta un'esenzione dalla regola anti-passback. L'anti-passback fa sì che le persone non possano impiegare le stesse credenziali di qualcuno entrato in un'area prima di loro. La prima persona deve uscire dall'area prima che le sue credenziali possano essere riutilizzate.
Titolare di tessera globale	Selezionare questa opzione per consentire la visualizzazione e il monitoraggio del titolare della tessera sui server secondari. Questa opzione è a disposizione solo per i titolari di tessere creati sul server principale. Vedere .

Aggiungi credenziali

È possibile aggiungere i seguenti tipi di credenziali al titolare della tessera:

- PIN
- Badge
- Targa
- Telefono cellulare

Per aggiungere una targa come credenziale di un titolare di tessere:

1. In **Credentials (Credenziali)**, fare clic su **+Add (+ Aggiungi)** e selezionare **License plate (Targa)**.
2. Inserire un nome credenziali che descriva il veicolo.
3. Inserisci il numero targa del veicolo.
4. Impostare la data di inizio e di fine delle credenziali.
5. Fare clic su **Aggiungi**.

Vedere l'esempio in .

Per aggiungere un PIN come credenziale di un titolare di tessere:

1. In **Credentials (Credenziali)**, fare clic su **+Add (+ Aggiungi)** e selezionare **PIN**.
2. Immettere un PIN.
3. Per utilizzare un PIN di coercizione per attivare un allarme silenzioso, attivare **Duress PIN (PIN di coercizione)** e inserire un PIN di coercizione.
4. Fare clic su **Aggiungi**.

Le credenziali del PIN sono sempre valide. È inoltre possibile configurare un PIN di coercizione che apre la porta e attiva un allarme silenzioso nel sistema.

Per aggiungere un badge come credenziale di un titolare di tessere:

1. In **Credentials (Credenziali)**, fare clic su **+Add (+ Aggiungi)** e selezionare **Card (Badge)**.
2. Per immettere manualmente i dati della tessera: inserire il nome della tessera, il numero della tessera e la lunghezza dei bit.

Nota

La lunghezza dei bit è configurabile solo quando si crea un formato tessera con una specifica lunghezza di bit non presente nel sistema.

3. Per ottenere automaticamente i dati della tessera dell'ultima tessera letta:
   3.1. Selezionare una porta dal menu a discesa **Select reader (Seleziona lettore)**.
   3.2. Passare la tessera sul lettore connesso a tale porta.
   3.3. Fare clic su **Get last swiped card data from the door's reader(s) (Acquisisci i dati dell'ultima tessera strisciata dal lettore/dai lettori della porta)**.
4. Inserire un codice struttura. Questo campo è disponibile solo se il **Facility code (Codice struttura)** è stato abilitato in **Access management > Settings (Gestione degli accessi > Impostazioni)**.
5. Impostare la data di inizio e di fine delle credenziali.
6. Fare clic su **Aggiungi**.

Data di scadenza	
Valido da	Impostare una data e un'ora di validità delle credenziali.
Valido fino a	Selezionare un'opzione dal menu a discesa.

Valido fino a	
Nessuna data di fine	Le credenziali non hanno scadenza.
Data	Impostare una data e un'ora di scadenza delle credenziali.
Dal primo utilizzo	Selezionare l'intervallo di scadenza delle credenziali, a partire dal primo utilizzo. Selezionare giorni, mesi, anni o numero di volte dopo il primo utilizzo.
Dall'ultimo utilizzo	Selezionare il periodo di validità delle credenziali, a partire dall'ultimo utilizzo. Selezionare giorni, mesi o anni dopo l'ultimo utilizzo.

Usare il numero di targa come credenziale

Questo esempio illustra il modo di impiegare un door controller, una telecamera dotata di AXIS License Plate Verifier e il numero targa di un veicolo come credenziali per concedere l'accesso.

1. Aggiungere il door controller e la telecamera a AXIS Secure Entry for XProtect.
2. Impostare la data e l'ora per i nuovi dispositivi con **Synchronize with server computer time (Sincronizza con l'ora del computer server)**.
3. Aggiornare il software sui nuovi dispositivi alla versione più recente a disposizione.
4. Aggiungi una nuova porta connessa al tuo door controller. Vedere .
   4.1. Aggiungere un lettore su **Lato A**. Vedere .
   4.2. In **Door settings (Impostazioni porta)**, seleziona **AXIS License Plate Verifier** come **Reader type (Tipo lettore)** e inserisci un nome per il lettore.
   4.3. In via facoltativa, aggiungi un lettore o un dispositivo REX su **Side B (Lato B)**.
   4.4. Fare clic su **OK**.
5. Installare e attivare AXIS License Plate Verifier sulla tua telecamera. Vedi il manuale per l'utente *AXIS License Plate Verifier*.
6. Avvia AXIS License Plate Verifier.
7. Configura AXIS License Plate Verifier.
   7.1. Andare a **Configuration > Access control > Encrypted communication (Configurazione > Controllo degli accessi > Comunicazione crittografata)**.
   7.2. In **External Peripheral Authentication Key (Chiave di autenticazione dispositivo periferico esterno)**, fare clic su **Show authentication key (Mostra chiave di autenticazione)** e **Copy key (Copia chiave)**.
   7.3. Apri AXIS License Plate Verifier dall'interfaccia Web della telecamera.
   7.4. Non effettuare l'impostazione.
   7.5. Andare a **Settings (Impostazioni)**.
   7.6. In **Access control (Controllo degli accessi)**, seleziona **Secure Entry** come **Type (Tipo)**.
   7.7. In **IP address (Indirizzo IP)**, immetti l'indirizzo IP e le credenziali per il door controller.
   7.8. In **Authentication key (Chiave di autenticazione)**, incolla la chiave di autenticazione che hai copiato in precedenza.
   7.9. Fare clic su **Connetti**.
   7.10. In **Door controller name (Nome door controller)**, seleziona il door controller.
   7.11. In **Reader name (Nome lettore)**, seleziona il lettore che hai aggiunto in precedenza.
   7.12. Attiva l'integrazione.

8. Aggiungi il titolare tessera a cui vuoi concedere l'accesso. Vedere .
9. Eseguire l'aggiunta di credenziali targa al nuovo titolare tessera. Vedere .
10. Aggiungi una regola di accesso. Vedere .
    10.1. Aggiungere una pianificazione.
    10.2. Aggiungi il titolare tessera a cui vuoi concedere l'accesso tramite targa.
    10.3. Aggiungi la porta con il lettore AXIS License Plate Verifier.

Aggiungi un gruppo

I gruppi consentono di gestire i titolari di tessera e le rispettive regole di accesso collettivamente e in modo efficiente.

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Cardholder management** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Gestione titolare tessera).
2. Andare su **Groups (Gruppi)** e fare clic su **+ Add (+ Aggiungi)**.
3. Inserire un nome e, facoltativamente, le iniziali del gruppo.
4. Selezionare **Global group (Gruppo globale)** per rendere possibile visualizzare e monitorare il titolare della tessera sui server secondari. Questa opzione è a disposizione solo per i titolari di tessere creati sul server principale. Vedere .
5. Aggiungere i titolari di tessere al gruppo:
    5.1. Fare clic su **+ Aggiungi**.
    5.2. Selezionare i titolari di tessere che si desidera aggiungere e fare clic su **Add (Aggiungi)**.
6. Fare clic su **Save (Salva)**.

Aggiungi una regola di accesso

Una regola di accesso definisce le condizioni che devono essere soddisfatte per consentire l'accesso.

Una regola di accesso è composta da:

Titolari tessera e gruppi titolari tessere – a chi concedere l'accesso.

Porte e zone – dove si applica l'accesso.

Pianificazioni – quando concedere l'accesso.

Per aggiungere una regola di accesso:

1. Andare a **Access control** > **Cardholder management** (Controllo degli accessi, gestione titolare tessera).
2. In **Access rules (Regole di accesso)**, fare clic su **+ Add (+Aggiungi)**.
3. Immettere un nome per la regola di accesso e fare clic su **Next (Avanti)**.
4. Configurazione dei titolari e dei gruppi:
    4.1. In **Cardholders (Titolari di tessera)** o **Groups (Gruppi)**, fare clic su **+ Add (+Aggiungi)**.
    4.2. Selezionare i titolari di tessera o i gruppi e fare clic su **Add (Aggiungi)**.
5. Configurazione di porte e zone:
    5.1. In **Doors (Porte)** o **Zones (Zone)**, fare clic su **+ Add (+Aggiungi)**.
    5.2. Selezionare le porte o le zone e fare clic su **Add (Aggiungi)**.
6. Configurazione delle pianificazioni:
    6.1. In **Schedules (Programmi)**, fare clic su **+Add (+Aggiungi)**.
    6.2. Selezionare uno o più programmi e fare clic su **Add (Aggiungi)**.
7. Fare clic su **Save (Salva)**.

Una regola di accesso priva di uno o più dei componenti descritti sopra è incompleta. È possibile visualizzare tutte le regole di accesso incomplete nella scheda **Incomplete**.

Sbloccare in modo manuale porte e zone

Per informazioni sulle azioni manuali, come lo sblocco manuale di una porta, vedere .

Per informazioni sulle azioni manuali, come lo sblocco manuale di una zona, vedere .

Esportazione dei report sulla configurazione del sistema

È possibile esportare report contenenti diversi tipi di informazioni sul sistema. AXIS Secure Entry for XProtect esporta il report come file CSV (comma-separated value) e lo salva nella cartella di download predefinita. Per esportare un report:

1. Andare in **Reports** > **System configuration (Configurazione del sistema)**.
2. Selezionare i rapporti da esportare e fare clic su **Download**.

Dettagli del titolare tessera	Include informazioni sui titolari di tessera, sulle credenziali, sulla convalida della tessera e sull'ultima transazione.
Accesso titolari tessera	Include le informazioni relative al titolare di tessera e le informazioni su gruppi titolari di tessera, regole di accesso, porte e zone correlate al titolare di tessera.
Accesso gruppo titolari tessera	Include il nome del gruppo titolare di tessera e le informazioni su titolari di tessera, regole di accesso, porte e zone correlate al gruppo titolare di tessera.
Regola di accesso	comprende il nome della regola di accesso e informazioni su titolari di tessera, gruppi titolari di tessera, porte e zone correlate alla regola di accesso.
Accesso porta	comprende il nome della porta e informazioni su titolari di tessera, gruppi titolari di tessera, regole di accesso e zone correlate alla porta.
Accesso zona	comprende il nome della zona e informazioni su titolari di tessera, gruppi titolari di tessera, regole di accesso e porte correlate alla zona.

Crea report sull'attività dei titolari di tessere

Un report appelli elenca i titolari di tessere all'interno di una zona specifica, aiutando a identificare chi è presente in un determinato momento.

Un rapporto raduno elenca i titolari di carta all'interno di una zona specifica, aiutando a identificare chi è al sicuro e chi manca durante le emergenze. Assiste i responsabili degli edifici nella localizzazione del personale e dei visitatori dopo le evacuazioni. Un punto di raccolta è un lettore designato dove il personale si presenta durante le emergenze, generando un report delle persone presenti e non presenti sul sito. Il sistema segnala i titolari di tessera come dispersi finché non si presentano a un punto di raccolta o finché qualcuno non li segnala manualmente come al sicuro.

Sia i rapporti di appello che quelli di raduno richiedono che le zone tengano traccia dei titolari di tessera.

Per creare ed eseguire un report appello o raduno:

1. Andare in **Reports** > **Cardholder activity (Attività titolari tessera)**.
2. Fare clic su **+ Add (+Aggiungi)** e selezionare **Roll call / Mustering (Appello/Raduno)**.

3. Immettere un nome per il report.
4. Selezionare le zone da includere nel report.
5. Selezionare i gruppi che si desidera includere nel report.
6. Se si desidera un report di raduno, selezionare **Mustering point (Punto di raduno)** e un lettore per il punto di raduno.
7. Selezionare un intervallo temporale per il report.
8. Fare clic su **Save (Salva)**.
9. Selezionare il report e fare clic su **Run (Esegui)**.

Stato del report appello	Descrizione
Presente	Il titolare della tessera è entrato nella zona specificata e non è uscito prima della compilazione del report.
Non presente	Il titolare della tessera è uscita dalla zona specificata e non è rientrato prima della compilazione del report.

Stato del report raduno	Descrizione
Al sicuro	Il titolare ha strisciato il proprio badge presso il punto di raduno.
Mancante	Il titolare non ha strisciato il proprio badge presso il punto di raduno.

Impostazioni di gestione degli accessi

Per personalizzare i campi del titolare della tessera utilizzati nel dashboard di gestione degli accessi:

1. Nella scheda **Access management (Gestione accessi)**, fare clic su **Settings (Impostazioni)** > **Custom cardholder fields (Campi personalizzati titolari tessere)**.
2. Fare clic su **+ Add (+Aggiungi)** e immettere un nome. Si possono aggiungere fino a 6 campi personalizzati.
3. Fare clic su **Aggiungi**.

Per usare il codice struttura per verificare il sistema di controllo degli accessi:

1. Nella scheda **Access management (Gestione accessi)**, fare clic su **Settings (Impostazioni)** > **Facility code (Codice struttura)**.
2. Selezionare **Facility code on (Codice struttura attivo)**.

Nota

È anche necessario selezionare **Include facility code for card validation (Includi codice struttura per convalida tessera)** quando si configurano i profili di identificazione. Vedere .

Importa ed esporta

Importa titolari della tessera

Questa opzione importa i titolari di tessera, i gruppi di titolari, le credenziali e le foto dei titolari della tessera da un file CSV. Per importare le foto dei titolari della tessera, assicurarsi che il server abbia accesso alle foto.

Quando importi i titolari tessera, il sistema di gestione degli accessi salva in automatico la configurazione del sistema, inclusa tutta la configurazione hardware, ed elimina qualsiasi configurazione salvata in precedenza.

Opzione di importazione	
Nuovo	questa opzione rimuove i titolari di tessere esistenti e aggiunge nuovi titolari.
Aggiorna	questa opzione aggiorna i titolari di tessere esistenti e aggiunge nuovi titolari di tessere.
Aggiungi	questa opzione mantiene i titolari di tessere esistenti e aggiunge nuovi titolari. I codici carta e gli ID titolare tessera sono univoci e si possono usare una sola volta.

1. Nella scheda **Access management (Gestione accessi)**, fare clic su **Import and export (Importazione ed esportazione)**.
2. Fare clic su **Import cardholders (Importa titolari di tessera)**.
3. Seleziona **New (Nuovo)**, **Update (Aggiorna)** o **Add (Aggiungi)**.
4. Fare clic su **Next (Avanti)**.
5. Fare clic su **Choose a file (Scegli un file)** e andare al file CSV. Fare clic su **Open (Apri)**.
6. Immettere un delimitatore di colonna e selezionare un identificatore univoco, quindi fare clic su **Next (Avanti)**.
7. Assegnare un'intestazione a ogni colonna.
8. Fare clic su **Importa**.

Impostazioni importazione	
Prima riga è intestazione	Specificare se il file CSV contiene un'intestazione colonna.
Delimitatore colonna	Inserire una formattazione delimitatore di colonna per il file CSV.
Identificatore univoco	Il sistema usa **Cardholder ID (ID titolare tessera)** per riconoscere il titolare tessera per impostazione predefinita. Puoi anche usare il nome e il cognome o l'indirizzo e-mail. L'identificativo univoco impedisce l'importazione di registri del personale duplicati.
Formato numero di tessera	**Allow both hexadecimal and number (Consenti sia valori esadecimali che numeri)** è selezionata per impostazione predefinita.

Esporta titolari di tessera

Questa opzione esporta i dati di titolari di tessera nel sistema in un file CSV.

1. Nella scheda **Access management (Gestione accessi)**, fare clic su **Import and export (Importazione ed esportazione)**.
2. Fare clic su **Export cardholders (Esporta i titolari di tessera)**.
3. Scegliere una posizione per il download e fare clic su **Save (Salva)**.

AXIS Secure Entry for XProtect aggiorna le foto dei titolari di tessera in `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos` ogni volta che si modifica la configurazione.

Undo import (Annulla importazione)

Il sistema salva in automatico la configurazione quando importi i titolari tessera. L'opzione **Undo import (Annulla importazione)** reimposta i dati dei titolari di tessera e di tutte le configurazioni hardware allo stato precedente all'ultima importazione dei titolari tessera.

1. Nella scheda **Access management (Gestione accessi)**, fare clic su **Import and export (Importazione ed esportazione)**.
2. Fare clic su **Undo import (Annulla importazione)**.
3. Fare clic su **Sì**.

Backup e ripristino

I backup automatici vengono eseguiti ogni notte. I tre file di backup più recenti sono memorizzati in C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\backup. Per ripristinare questi file:

1. Spostare il file di backup in C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\restore.
2. Eseguire il riavvio di AXIS Secure Entry utilizzando uno dei seguenti metodi:
   - Avviare il programma MSC (Servizi), individuare "AXIS Optimizer Secure Entry Service" e procedere al riavvio.
   - Avviare il computer.

T10234037_it

2025-10 (M3.2)