AXIS Camera Station Pro Secure Entry

Manuale dell'utente

Informazioni su

Secure Entry è un componente di AXIS Camera Station Pro. Utilizzarlo per aggiungere dispositivi e per gestire pianificazioni. Per ulteriori informazioni, vedere il *manuale per l'utente di AXIS Camera Station Pro*.

Configurazione del controllo degli accessi

Se si aggiunge un network door controller Axis al sistema, è possibile configurare l'hardware di controllo degli accessi in AXIS Camera Station versione 6.x o successiva.

Per un flusso di lavoro completo per l'impostazione di un network door controller Axis in AXIS Camera Station Pro Secure Entry, vedere *Imposta un network door controller Axis*.

Nota

Prima di iniziare, fare quanto segue:

- Effettuare un aggiornamento della versione del sistema operativo AXIS OS del controller in **Configuration > Devices > Management** (Configurazione, Dispositivi, Gestione).
- Impostare data e ora per il dispositivo di controllo in **Configuration > Devices > Management (Configurazione > Dispositivi > Gestione)**.
- Attivare HTTPS sul dispositivo di controllo in **Configuration > Devices > Management (Configurazione > Dispositivi > Gestione)**.

Workflow to configure access control (Flusso di lavoro per configurare il controllo degli accessi)

1. Per modificare i profili di identificazione predefiniti o creare un nuovo profilo di identificazione, vedere *Profili di identificazione, on page 22*.
2. Per utilizzare un'impostazione personalizzata per i formati della tessera e la lunghezza del PIN, vedere *Formati tessera e PIN, on page 24*.
3. Aggiungere una porta e applicare un profilo di identificazione alla porta. Vedere *Aggiunta di una porta, on page 7*.
4. Configurare la porta.
   - *Aggiungi un monitor porta, on page 14*
   - *Aggiungi ingresso di emergenza, on page 15*
   - *Aggiungi un lettore, on page 16*
   - *Aggiungi un dispositivo REX, on page 19*
5. Aggiungere una zona e aggiungere porte alla zona. Vedere *Aggiunta di una zona, on page 19*.

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 di seguito sono valide solo in caso di aggiornamento dalla rispettiva versione originale consigliata di AXIS Camera Station Pro 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 specifica di AXIS Camera Station Pro.
- **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. Supponiamo di utilizzare AXIS Camera Station Pro versione 6.5 e di aggiornare tutti i dispositivi alla versione consigliata di AXIS OS 12.0.86.2. In questo caso, AXIS OS versione 12.0.86.2 diventa la versione minima supportata per il sistema in uso.
- **Aggiornamento oltre la versione AXIS OS consigliata:** Supponiamo di aggiornare a una versione AXIS OS superiore a quella consigliata per una particolare versione di AXIS Camera Station Pro. 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 AXIS Camera Station Pro.
- **Raccomandazioni per le prossime versioni AXIS OS:** Seguire sempre la versione AXIS OS consigliata per

la rispettiva versione di AXIS Camera Station Pro per garantire la stabilità del sistema e la piena compatibilità.

- **Tracciare le modifiche:** La modifica del firmware tra la versione 10.12.xx e 11.0.xx o superiore richiede un ripristino delle impostazioni di fabbrica.

La tabella seguente mostra la versione minima e consigliata di AXIS OS per ciascuna versione di AXIS Camera Station Pro:

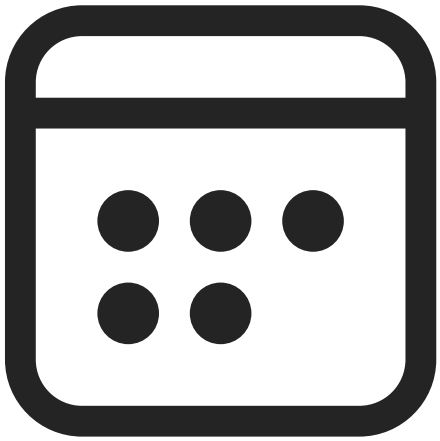
Versione AXIS Camera Station	Versione minima AXIS OS	Versione AXIS OS consigliata
Pro 6.15	12.5.68.1	12.8.55.1
Pro 6.14	12.5.68.1	12.8.55.1
Pro 6.13	12.5.68.1	12.6.102.1

La tabella seguente mostra la versione minima e consigliata di AXIS OS per ciascuna versione di AXIS Camera Station 5:

Versione AXIS Camera Station	Versione AXIS OS consigliata
5.59	12.4.68.1
5.58	12.4.68.1
5.57	11.8.20.2

Porte e zone

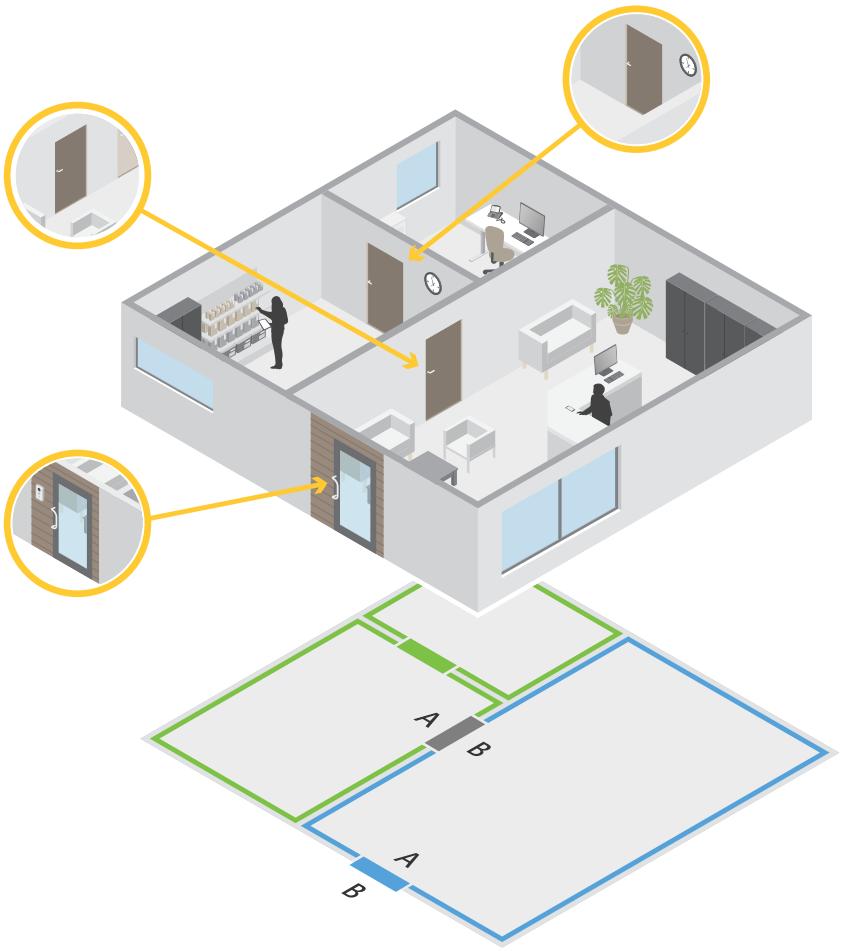
Andare a **Configuration > Access control > Doors and zones (Configurazione > Controllo degli accessi > Porte e zone)** per ottenere una panoramica ed eseguire la configurazione di porte e zone.

 **Azioni manuali**	Impostare manualmente lo stato di una porta. Selezionare una delle opzioni seguenti: **Reset (Ripristinare)** (seguire le regole del sistema), **Grant access (Concedere l'accesso)** (sbloccare la porta per 7 secondi), **Lock (Sbloccare)** (mantenere la porta sbloccata), **Unlock (Bloccare)** (mantenere la porta bloccata) oppure **Lockdown (Attivare la chiusura)** (nessuno può entrare o uscire).
 **Sblocca pianificazioni**	Impostate la pianificazione per sbloccare automaticamente le porte a orari prestabiliti. In tutti gli altri casi le porte rimangono bloccate. Per richiedere che la prima persona sblocchi manualmente la porta prima che la pianificazione si attivi, attivare l'opzione **Prima persona inserita**.
Profilo di identificazione	Cambiare il profilo di identificazione delle porte.
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)**.
Canale sicuro	Disattivare o attivare OSDP Secure Channel per uno specifico lettore.

Porte	
Nome	Il nome della porta.
Tipo	Il tipo di configurazione della porta.
Dispositivo	Il dispositivo collegato alla porta.

Indirizzo IP	L'indirizzo IP del 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.
Batteria	Lo stato della batteria del door controller.
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. • **Firmware precedente:** Il dispositivo utilizza una versione di firmware non aggiornata. Aggiornare il firmware per garantire prestazioni e sicurezza ottimali.
Zone	
Nome	Il nome della zona.
Numero di porte	Numero di porte incluse nella zona.
Livello di sicurezza	Il livello di sicurezza applicato alla 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. I sistemi multi-controllo supportano ulteriori configurazioni di blocco.
- Se un door controller non ha porte e si sta utilizzando una nuova versione di AXIS Camera Station Pro Secure Entry con firmware 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 firmware precedente.

Creare una nuova configurazione porta per aggiungere una porta:

1. Andare a **Configuration > Access control > Doors and zones (Configurazione > Controllo degli accessi > Porte e zone)**.
2. Fare clic su + **Add door** (Aggiungi porta) e seleziona il tipo di porta dall'elenco a discesa.

Tipi di porta	
Porta	Una porta standard dotata di un monitor che supporta blocchi e lettori. Richiede un door controller.
Porta wireless	Una porta che è possibile configurare con blocchi wireless e hub di comunicazione ASSA ABLOY Aperio®. Per ulteriori informazioni, vedere *Aggiungere un blocco wireless, on page 12*.
Porta di monitoraggio	Una porta in grado di segnalare se è aperta o chiusa. Per ulteriori informazioni, vedere *Aggiungere una porta di monitoraggio, on page 14*.
Porta predisposta	Una porta che è possibile aggiungere come segnaposto nel sistema senza la necessità di selezionare il relativo hardware.
Piano	Un tipo di porta per il controllo degli ascensori che effettua l'autenticazione dell'accesso ai piani dell'ascensore tramite lettori di tessere. Per ulteriori informazioni, consultare *Aggiunta di un piano per il controllo dell'ascensore BETA, on page 15*.

3. Inserire un nome per la porta e selezionare un door controller nel menu a discesa **Device** (Dispositivo) da associare alla porta. Il controller è disattivato (grigio) quando non si può aggiungere un'altra porta, quando è offline o HTTPS non è attivo.
4. Fare clic su **Next (Avanti)** per passare alla pagina di configurazione della porta.
5. Selezionare una porta relè dal menu a discesa **Primary lock (Blocco principale)**.
6. Per configurare due blocchi sulla porta, selezionare una porta relè dal menu a discesa **Secondary lock (Blocco secondario)**.
7. Selezionare un profilo di identificazione. Vedere *Profili di identificazione, on page 22*.
8. Configurare le impostazioni della porta. Vedere *Impostazioni della porta, on page 9*.
9. *Aggiungi un monitor porta, on page 14*
10. *Aggiungi ingresso di emergenza, on page 15*
11. *Aggiungi un lettore, on page 16*
12. *Aggiungi un dispositivo REX, on page 19*
13. Configurare il livello di sicurezza. Vedere *Livello di sicurezza porta, on page 10*.
14. Fare clic su **Save (Salva)**.

Copia una configurazione porta:

1. Andare a **Configuration > Access control > Doors and zones (Configurazione > Controllo degli accessi > Porte e zone)**.
2. Fare clic su **+ Add door (Aggiungi porta)**.
3. Inserire un nome per la porta e selezionare un door controller nel menu a discesa **Device** (Dispositivo) da associare alla porta.
4. Fare clic su **Next (Avanti)**.
5. 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.
6. Modificare le impostazioni se si desidera.

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

Per rimuovere una porta:

1. Andare a **Configuration > Access control > Doors and zones > Doors (Configurazione > Controllo degli accessi > Porta e zone > Porte)**.
2. Selezionare una porta dall'elenco.
3. Fare clic su **Remove (Rimuovi)** e conferma.

Aggiungere e configurare porte e zone

Impostazioni della porta

Per modificare una porta:

1. Andare a **Configuration > Access control > Door and Zones (Configurazione > Controllo degli accessi > Porte e zone)**.
2. Selezionare la porta che si desidera modificare.
3. Fare clic su **Edit (Modifica)**.
4. Modificare le impostazioni e fare clic su **Save (Salva)**.

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.
Porta forzata	Selezionare se si desidera che il sistema attivi un sistema allarme quando viene forzata l'apertura di una porta. È necessario un sensore di posizione della porta (DPS).
Porta aperta troppo a lungo	Selezionare se si desidera che il sistema attivi un sistema allarme quando la porta viene tenuta aperta troppo tempo.

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 **Configuration (Configurazione)** > **Access control (Controllo degli accessi)** > **Doors and zones (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.

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 **Configuration (Configurazione)** > **Access control (Controllo degli accessi)** > **Doors and zones (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**;

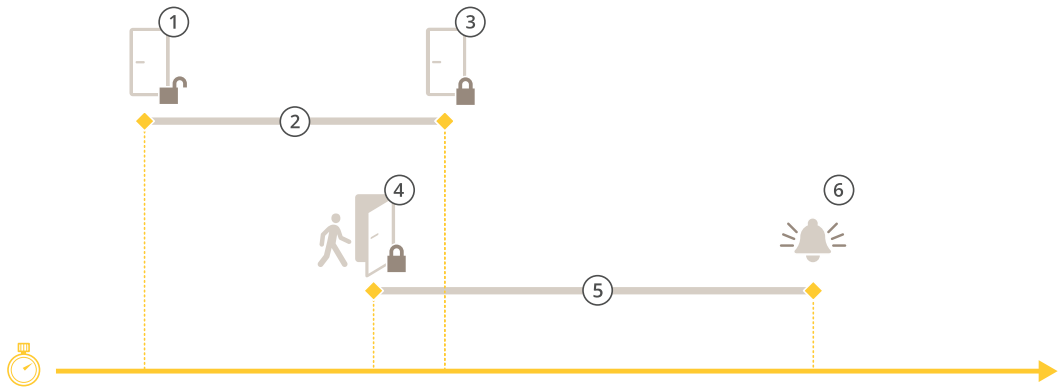
Regola due persone	
Side A (Lato A) e **Side B (Lato B)**	Selezionare i lati della porta su cui usare la regola.
Pianificazioni	Selezionare quando è attiva la regola.
Timeout (secondi)	Timeout è il tempo massimo consentito tra i passaggi di tessera o altri tipi di credenziali valide.

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

1. Andare a **Configuration (Configurazione)** > **Access control (Controllo degli accessi)** > **Doors and zones (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. Aprire una scheda **Access Management (Gestione degli accessi)**.
   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**;

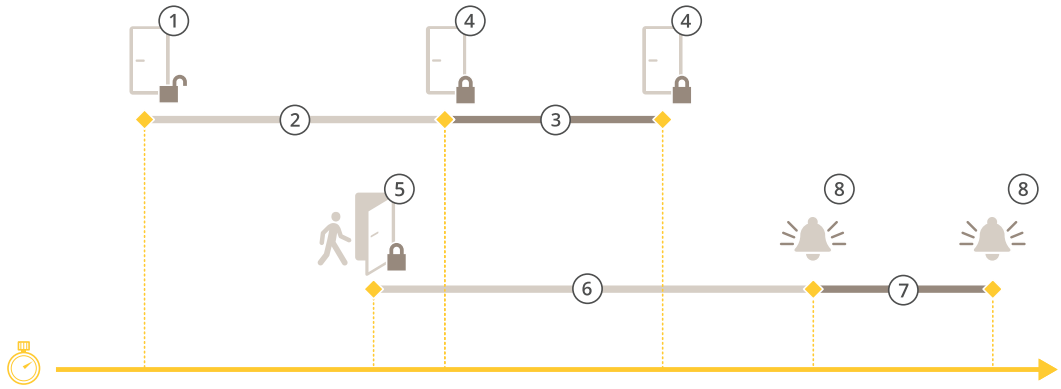
Doppia passata	
Timeout (secondi)	Timeout è il tempo massimo consentito tra i passaggi di tessera o altri tipi di credenziali valide.

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

Aggiungere un blocco wireless

AXIS Camera Station Pro Secure Entry supporta i blocchi wireless e gli hub di comunicazione ASSA ABLOY Aperio®. Il blocco wireless si collega al sistema attraverso un hub di comunicazione Aperio connesso al connettore RS485 del door controller. Si può connettere un massimo di 16 blocchi wireless a un door controller.

Per guardare questo video, andare alla versione web di questo documento.

Nota

- L'impostazione richiede che il door controller Axis disponga della versione 11.6.16.1 o successiva di AXIS OS.
- L'impostazione richiede una licenza di AXIS Door Controller Extension valida.
- L'ora sul door controller Axis e sul server AXIS Camera Station Pro Secure Entry deve essere sincronizzata.
- Prima di cominciare, usare l'applicazione Aperio che ASSA ABLOY supporta per associare i blocchi Aperio all'hub Aperio
- È possibile collegare un solo hub di comunicazione Aperio per ogni connettore RS485. La funzione multi-drop non è supportata.
- I blocchi wireless non seguiranno le pianificazioni di sblocco quando si è offline.

1. Accedere al door controller.

1.1. Andare a **Configurazione > Dispositivi > Altri dispositivi**.

1.2. Aprire l'interfaccia Web del door controller connesso all'hub di comunicazione Aperio.

2. Attivare AXIS Door Controller Extension.

2.1. Nell'interfaccia Web del door controller, andare a **Apps (App)**.

2.2. Aprire il menu contestuale AXIS Door Controller Extension .

2.3. Fare clic su **Activate license with a key (Attiva licenza con una chiave)** e selezionare la licenza.

2.4. Attivare **AXIS Door Controller Extension**.

3. Connettere il blocco wireless al door controller attraverso l'hub di comunicazione.

3.1. Nell'interfaccia web del door controller, andare ad **Access control > Wireless locks (Controllo degli accessi > Blocchi wireless)**.

3.2. Fare clic su **Connect communication hub (Connetti hub comunicazioni)**.

3.3. Immettere un nome per l'hub e fare clic su **Connect (Connetti)**.

3.4. Fare clic su **Connect wireless lock (Collega blocco wireless)**.

3.5. Selezionare l'indirizzo e le funzionalità di blocco per il blocco che si vuole aggiungere e fare clic su **Save (Salva)**.

4. Aggiungere e configurare la porta con il blocco wireless.

4.1. In AXIS Camera Station Pro Secure Entry, andare a **Configuration > Access control > Doors and zones (Configurazione > Controllo degli accessi > Porte e zone)**.

4.2. Fare clic su **Add door (Aggiungi porta)**.

4.3. Selezionare il door controller collegato all'hub di comunicazione Aperio, selezionare **Wireless door (Porta wireless)** come **Door type (Tipo di porta)**.

4.4. Fare clic su **Next (Avanti)**.

4.5. Selezionare un **Wireless lock (Blocco wireless)**.

4.6. Definire i lati porta A e B e aggiungere sensori. Per ulteriori informazioni, vedere *Porte e zone, on page 4*.

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

Una volta connesso il blocco wireless, se ne può visualizzare il livello e lo stato della batteria nella panoramica porte.

Livello batteria	Operazione
Buono	Nessuno
Bassa	Il blocco funziona come previsto, ma è bene sostituirne la batteria prima che il livello diventi critico.
Critico	Sostituire la batteria. Il blocco potrebbe non funzionare come previsto.

Stato serratura	Operazione
Online	Nessuno
Blocco inceppato	Risoluzione di eventuali problemi meccanici del blocco.

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 *Aggiunta di una porta, on page 7*.
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 *Ingressi con supervisione, on page 21*.

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 firmware 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. In AXIS Camera Station Pro, andare a **Configuration (Configurazione)** > **Access control (Controllo degli accessi)** > **Doors and zones (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**.

Aggiunta di un piano per il controllo dell'ascensore BETA

Un piano è un tipo di porta che si utilizza per controllare l'accesso ai piani dell'ascensore. Quando si aggiunge un piano, si crea una risorsa ascensore che raggruppa tutti i piani per quell'ascensore. Ogni piano utilizza un lettore di tessere all'interno della cabina dell'ascensore per l'autenticazione degli utenti prima di consentire l'accesso al piano.

Prima di iniziare, è necessario:

- Un door controller di rete supportato aggiunto al sistema, come *A1610*, *A1710-B* o *A1810-B*.
- Un *A9910 I/O Relay Expansion Module* per relè aggiuntivi. Per istruzioni su come aggiungere il modulo a un controller, consultare .

Nota

Questa funzione è in versione Beta e attualmente supporta fino a 16 piani e solo lettori di schede.

Per impostare un piano:

1. Andare a < **Configuration > Access control > Doors and zones** (Configurazione, Controllo degli accessi Porte e zone).
2. Fare clic su **Add** (Aggiungi) e selezionare **Floor** (Piano) BETA.
3. Immettere un nome per il piano.
4. Selezionare il controller.
5. In **Elevator** (Ascensore), selezionare un ascensore esistente o fare clic su **Create new elevator** (Crea nuovo ascensore) per aggiungerne uno nuovo, quindi inserire un nome.
6. In **Side A (Lato A)**, selezionare **Card reader (Lettore tessere)** e configurare il lettore. **Side B** (Lato B) non può essere configurato per motivi di sicurezza.
7. Fare clic su **Save and add new** (Salva e aggiungi nuovo) per aggiungere più piani allo stesso ascensore. I campi di configurazione dell'ascensore e del lettore restano compilati per il piano successivo. Si noti che questa opzione è disponibile solo se il controller dispone di relè.
8. Fai clic su **Save** (Salva) dopo aver aggiunto il piano. I piani vengono visualizzati con la convenzione di denominazione "Nome ascensore - Nome piano". Ad esempio: "Lato ovest - Piano 1".

Nota

- I lettori utilizzati su più piani possono essere sottoposti a modifica solo sul primo piano in cui sono stati aggiunti.
- Gli ascensori vengono eliminati in modo automatico quando sono eliminati tutti i piani correlati.

Aggiungi ingresso di emergenza

Si può eseguire l'aggiunta e la configurazione di un input di emergenza per avviare un'azione che blocca o sblocca la porta. Si può anche configurare la modalità di collegamento del circuito.

1. Andare alla pagina di configurazione della porta. Vedere *Aggiunta di una porta, on page 7*.
2. In **Sensors (Sensori)**, fare clic su **Add (Aggiungi)**.
3. Selezionare **Emergency input (Input di emergenza)**.
4. In **Emergency state (Stato di emergenza)**, selezionare la connessione di circuito.
5. 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))**.

6. Selezionare l'elemento che deve essere attivato da **Emergency action (Azione di emergenza)** quando la porta riceve un segnale di stato di emergenza.

Stato di emergenza	
Circuito aperto	Il circuito di ingresso di emergenza è normalmente chiuso. Quando il circuito è aperto, l'ingresso di emergenza invia un segnale di stato di emergenza.
Circuito chiuso	Il circuito di ingresso di emergenza è normalmente aperto. Quando il circuito è chiuso, l'input di emergenza invia un segnale di stato di emergenza.

Azione di emergenza	
Sblocca porta	La porta si sblocca nel momento in cui riceve il segnale di stato di emergenza.
Blocca porta	La porta si sblocca nel momento in cui riceve il segnale di stato di emergenza.

Aggiungere un lettore IP

È possibile utilizzare come lettore un intercom di rete Axis o un altro dispositivo abilitato all'IP. Prima di poterlo assegnare a una porta, è necessario aggiungere il dispositivo ad AXIS Camera Station Pro.

Nota

Prima di iniziare, assicurarsi che il lettore IP sia acceso e connesso alla stessa rete di AXIS Camera Station Pro.

1. Andare a **Configuration > Devices > Add devices** (Configurazione, Dispositivi, Aggiungi dispositivi).
2. Selezionare il lettore IP dall'elenco dei dispositivi rilevati e fare clic su **Add** (Aggiungi).
3. Inserire le credenziali del dispositivo quando richiesto.

Una volta aggiunto il dispositivo, è possibile assegnarlo a una porta. Vedi *Aggiungi un lettore, on page 16*.

Aggiungi un lettore

Si può configurare un door controller per supportare più 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 *Porte e zone, on page 4*.

Nota

- È inoltre possibile aggiungere fino a 16 lettori Bluetooth a un door controller. Per ulteriori informazioni, vedere *Aggiungi un lettore Bluetooth, on page 18*.
- Se si usa un interfono di rete Axis come lettore IP, il sistema impiega la configurazione PIN impostata nella pagina Web del dispositivo.

1. Andare alla pagina di configurazione della porta. Vedere *Aggiunta di una porta, on page 7*.
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.

Per informazioni su come installare un lettore di codici a barre AXIS, consultare il sito *Installa AXIS Barcode Reader, on page 27*.

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.
Lettore IP	Selezionare **IP reader (Lettore IP)** e scegliere un dispositivo dal menu a discesa. È possibile utilizzare gli intercom di rete Axis come lettori IP.

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 *Ingressi con supervisione, on page 21*.

Aggiungi un lettore Bluetooth

È possibile utilizzare il lettore AXIS A4612 Network Bluetooth Reader per espandere i limiti delle porte cablate dei door controller di Axis, che consentono di assegnare fino a 16 di questi lettori alla propria porta. Ogni lettore può gestire la serratura della porta, la richiesta di uscita (REX) e l'interruttore di posizione della porta (DPS).

L'aggiunta e l'utilizzo di questi lettori non richiede alcuna licenza aggiuntiva.

Per aggiungere un lettore AXIS A4612 Network Bluetooth Reader a una porta:

1. Assicurarsi di aver associato AXIS A4612 con il door controller. Vedere *Utilizzare l'app AXIS Mobile Credential come credenziali Bluetooth, on page 18*.
2. Andare alla pagina di configurazione della porta. Vedere *Aggiunta di una porta, on page 7*
3. Su un lato della porta, fare clic su **Add (Aggiungi)**, quindi su **Card reader (Lettore scheda)**.
4. Selezionare **IP reader** (lettore IP) e scegliere l'AXIS A4612 associato dal menu a discesa. Se il lettore verrà utilizzato per l'associazione delle credenziali, contrassegnarlo per l'associazione. Fare clic su **Aggiungi**.
5. Nella scheda **Overview** (Panoramica), modificare il profilo di identificazione. È possibile utilizzare i profili **Tap in app** (Tocca in app) o **Touch reader** (Lettore touch) se l'AXIS A4612 è collegato solo a un lato della porta e si utilizza un REX sull'altro.

Utilizzare l'app AXIS Mobile Credential come credenziali Bluetooth

Questo esempio mostra come aggiungere un lettore Bluetooth AXIS A4612 al sistema per consentire ai titolari della tessera di sbloccare le porte tramite l'app AXIS Mobile Credential.

1. Installare il lettore Bluetooth e collegarlo al controller della porta.
2. Aggiungere il lettore Bluetooth nell'interfaccia web del controller della porta.
   2.1. Accedere al controller della porta e passare a **Peripherals (Periferiche)** > **Readers (Lettori)**.
   2.2. Fare clic su **Add reader (Aggiungi lettore)**.
   2.3. Inserire le informazioni richieste nella finestra di dialogo **Add Bluetooth reader (Aggiungi lettore Bluetooth)**.
   2.4. Fare clic su **Aggiungi**.
3. Aggiungere il lettore Bluetooth a una porta in AXIS Camera Station Pro.
   3.1. Andare a **Configuration (Configurazione)** > **Access control (Controllo degli accessi)** > **Doors and zones (Porte e zone)**.
   3.2. Selezionare la porta a cui aggiungere il lettore Bluetooth e fare clic su **Edit (Modifica)**.
   3.3. Fare clic su **+ Add (+ Aggiungi)** sul lato della porta dove si trova il lettore Bluetooth.
   3.4. Selezionare **Card reader (Lettore di schede)**.
   3.5. In **Add IP reader (Aggiungi lettore IP)**, selezionare **IP reader (Lettore IP)**.
   3.6. In **Select IP reader (Seleziona lettore IP)**, selezionare il lettore Bluetooth.
   3.7. Fare clic su **Aggiungi**.
4. Selezionare un lettore Bluetooth per l'associazione. Questa operazione deve essere eseguita per almeno un lettore Bluetooth presente nel sistema.
   4.1. Selezionare il lettore Bluetooth appena aggiunto.
   4.2. Fare clic su **Edit (Modifica)**.
   4.3. IN **Edit bluetooth reader (Modifica lettore Bluetooth)**, selezionare **Use this reader for pairing (Usa questo lettore per l'associazione)**.
   4.4. fare clic su **Applica**;

5. Scegliere il profilo di identificazione **Tap in app (Tocco nell'app)** o **Touch reader (Tocco sul lettore)**. Per ulteriori informazioni, vedere *Profili di identificazione, on page 22*.
6. Aggiungere le credenziali mobili al titolare della tessera. Vedere *Aggiungi credenziali, on page 34*.
7. Associare le credenziali mobili al lettore di associazione.
   7.1. Avvicinare il telefono cellulare del titolare della tessera al lettore Bluetooth abilitato all'associazione.
   7.2. Seguire le istruzioni fornite nell'e-mail inviata al titolare della tessera.

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 *Aggiunta di una porta, on page 7*.
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 *Ingressi con supervisione, on page 21*.

Operazione	
Sblocca porta	Sceglierlo per sbloccare la porta nel momento in cui riceve il segnale REX.
Nessuno	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. Per una panoramica, consultare *Esempio di porte e zone, on page 7*.

1. Andare a **Configuration > Access control > Doors and zones > Zones (Configurazione > 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 **Configuration > Access control > Doors and zones > Zones (Configurazione > 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 **Configuration > Access control > Doors and zones > Zones (Configurazione > 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 **Configuration (Configurazione)** > **Access control (Controllo degli accessi)** > **Doors and zones (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 *Aggiungi un monitor porta, on page 14*.
- Collegamento tra Door controller e lettore basato su protocolli Wiegand. Vedere *Aggiungi un lettore, on page 16*.
- Collegamento tra Door controller e dispositivo REX. Vedere *Aggiungi un dispositivo REX, on page 19*.

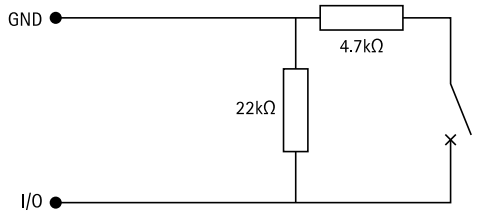
Per utilizzare gli input supervisionati:

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

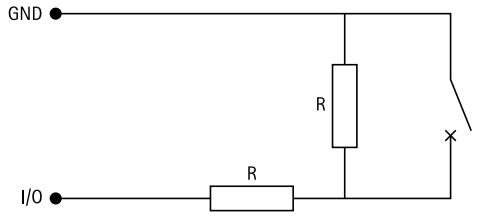
Prima connessione parallela

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.



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.

Nota

Si devono usare QR e PIN dinamici insieme.

Andare a **Configuration > Access control > Identification profiles (Configurazione > Controllo degli accessi > Profili di identificazione)** per creare, modificare o rimuovere profili di identificazione.

I profili di identificazione disponibili:

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.

QR – I titolari della tessera devono mostrare il QR Code® alla telecamera per ottenere l'accesso alla porta. Si può usare il profilo di identificazione QR sia per QR statico sia per QR dinamico.

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

Tocco nell'app – I titolari della tessera devono inserire le credenziali nell'app AXIS Camera Station Mobile mentre si trovano nel raggio d'azione del lettore Bluetooth.

Tocco sul lettore – I titolari della tessera devono toccare il lettore Bluetooth quando usano un telefono cellulare con credenziali mobili.

*QR Code è un marchio registrato di Denso Wave Incorporated in Giappone e in altri paesi.

Creare un profilo di identificazione

1. Andare a **Configuration > Access control > Identification profiles (Configurazione > 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. Per il Lato A, fare clic su **+ Add** (+Aggiungi), selezionare un tipo di identificazione e una pianificazione.
   - Per richiedere ai titolari di tessere di utilizzare più di un tipo di identificazione, selezioni più tipi nella stessa riga.
   - Per consentire ai titolari di tessere di utilizzare entrambi i tipi, fare clic nuovamente su **+ Add** (+Aggiungi) e aggiungere un'altra riga.
6. Per il Lato B, fare clic su **+ Add** (+Aggiungi), selezionare un tipo di identificazione e una pianificazione.
7. Fare clic su **OK**.

Impostare profili di identificazione

Modificare un profilo di identificazione

1. Andare a **Configuration > Access control > Identification profiles (Configurazione > 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**.

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.

Rimuovere un profilo di identificazione

1. Andare a **Configuration > Access control > Identification profiles (Configurazione > 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**.

Ripristinare un formato tessera predefinito:

1. Andare a **Configuration > Access Control > Card formats and PIN (Configurazione > Controllo degli accessi > Formati tessera e PIN)**.
2. Fare clic su per ripristinare un formato tessera alla mappa dei campi predefinita.

Formati tessera e PIN

Un formato di scheda definisce il modo in cui un lettore di schede interpreta i dati provenienti da una scheda. Sono disponibili formati di scheda predefiniti che è possibile utilizzare o modificare; inoltre, è possibile creare formati di scheda personalizzati

Andare a **Configuration > Access Control > Card formats and PIN (Configurazione > 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.

Configurazione PIN

1. Andare a **Configuration > Access Control > Card formats and PIN (Configurazione > 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**.

Creare il formato di una tessera:

1. Andare a **Configuration > Access Control > Card formats and PIN (Configurazione > 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.
- I formati scheda predefiniti possono essere modificati ma non eliminati. Per annullare eventuali modifiche apportate a un formato predefinito, fare clic sull'icona di ripristino per ripristinarlo alle impostazioni predefinite. È possibile eliminare i formati tessera creati.

ⓘ	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).

Impostazione dei formati tessera

Modificare il formato di una tessera:

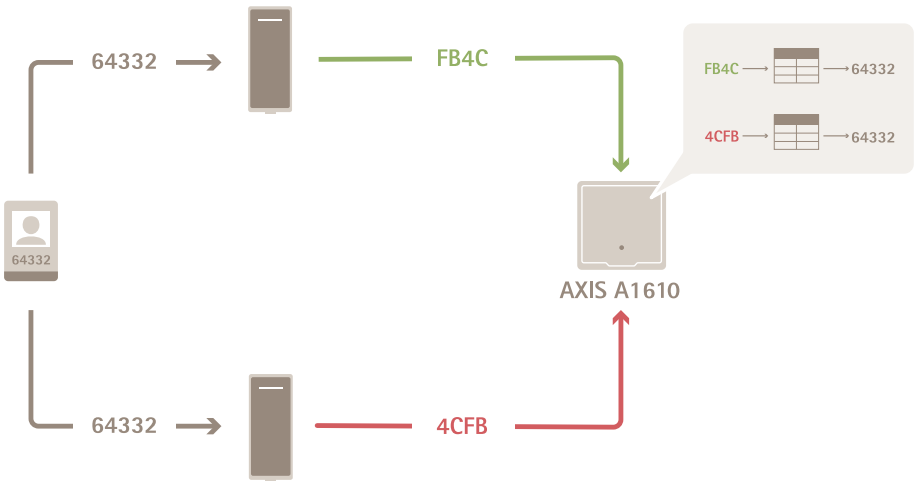
1. Andare a **Configuration > Access Control > Card formats and PIN (Configurazione > Controllo degli accessi > Formati tessera e PIN)**.
2. Selezionare un formato tessera e fare clic su .
3. Se cambia un formato tessera predefinito, si può modificare solo **Invert bit order (Inverti ordine dei bit)** 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 **Configuration > Access Control > Card formats and PIN (Configurazione > Controllo degli accessi > Formati tessera e PIN)**.
2. Selezionare un formato tessera personalizzato, fare clic su e **Yes (Sì)**.

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*

Comunicazione crittografata

Canale sicuro OSDP

AXIS Camera Station 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 **Configuration > Access control > Encrypted communication (Configurazione > Controllo degli accessi > Comunicazione crittografata)**.
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*.

Nota

Se l'unità di controllo degli accessi, l'host o il pannello supportano il canale sicuro OSDP, si consiglia di attivarlo sul lettore per aumentare la sicurezza delle comunicazioni. Per garantire un canale sicuro, attivare il DIP #6 sul lettore.

La chiave di crittografia viene trasmessa con testo in chiaro durante l'impostazione iniziale; pertanto, durante questa procedura è necessario tenere sotto controllo tutti i cavi RS485 e i dispositivi collegati.

AXIS Barcode Reader

AXIS Barcode Reader è un'applicazione che si può installare sulle telecamere Axis. Il door controller Axis utilizza la chiave di autenticazione periferica esterna per concedere l'accesso e autenticare il lettore di codici a barre AXIS Barcode Reader e AXIS License Plate Verifier. Per un flusso di lavoro completo per l'impostazione di AXIS License Plate Verifier in AXIS Camera Station Pro, vedere .

Installa AXIS Barcode Reader

1. Scaricare il file di installazione dell'applicazione da *axis.com*.
2. Vai alla pagina Web del tuo interfono o della tua telecamera Axis.
3. Installa l'applicazione.
4. Attivare la licenza.
5. Avviare l'applicazione.

6. Consigliamo la modifica delle seguenti impostazioni della telecamera per maggiore precisione del QR.
   6.1. Vai alle impostazioni della telecamera.
   6.2. In **Image > Exposure (Immagine > Esposizione)**, sposta il cursore **Blur-noise trade-off (Compromessi disturbo-sfocatura)** al centro.

Configura AXIS Barcode Reader

1. Per modificare il profilo di identificazione QR, andare in **Configuration (Configurazione) > Access control (Controllo degli accessi) > Identification profiles (Profili di identificazione)** e fare clic su . Vedi *Profili di identificazione*.
2. Aggiunta di una porta. Consultare *Aggiunta di una porta*.
3. Seleziona **QR** come profilo di identificazione per questa porta. Vedi *Impostazioni della porta*.
4. Aggiungi un lettore di codice a barre. Vedi *Aggiungi un lettore*.
   4.1. Sotto un lato della porta, fare clic su **Add reader (Aggiungi lettore)**.
   4.2. Seleziona **AXIS Barcode Reader** da **Reader type (Tipo di lettore)** dall'elenco a discesa. Immetti un nome e fai clic su **OK**.

1. Per modificare il profilo di identificazione QR, andare in **Configuration (Configurazione) > Access control (Controllo degli accessi) > Identification profiles (Profili di identificazione)** e fare clic su . Vedi *Profili di identificazione*.
2. Aggiunta di una porta. Consultare *Aggiunta di una porta*.
3. Seleziona **QR** come profilo di identificazione per questa porta. Vedi *Impostazioni della porta*.
4. Aggiungi un lettore di codice a barre. Vedi *Aggiungi un lettore*.
   4.1. Sotto un lato della porta, fare clic su **Add reader (Aggiungi lettore)**.
   4.2. Seleziona **AXIS Barcode Reader** da **Reader type (Tipo di lettore)** dall'elenco a discesa. Immetti un nome e fai clic su **OK**.

1. Per modificare il profilo di identificazione QR, andare in **Configuration (Configurazione) > Access control (Controllo degli accessi) > Identification profiles (Profili di identificazione)** e fare clic su . Vedi *Profili di identificazione*.
2. Aggiunta di una porta. Consultare *Aggiunta di una porta*.
3. Seleziona **QR** come profilo di identificazione per questa porta. Vedi *Impostazioni della porta*.
4. Aggiungi un lettore di codice a barre. Vedi *Aggiungi un lettore*.
   4.1. Sotto un lato della porta, fare clic su **Add reader (Aggiungi lettore)**.
   4.2. Seleziona **AXIS Barcode Reader** da **Reader type (Tipo di lettore)** dall'elenco a discesa. Immetti un nome e fai clic su **OK**.

Crea una connessione con il door controller

1. In AXIS Camera Station Pro Secure Entry:
   1.1. Andare a **Configuration > Access control > Encrypted communication (Configurazione > Controllo degli accessi > Comunicazione crittografata)**.
   1.2. 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)**.
2. Nell'interfaccia Web del dispositivo dove si esegue AXIS Barcode Reader:
   2.1. Aprire l'applicazione AXIS Barcode Reader.

2.2. Se il certificato del server non è stato configurato in AXIS Camera Station Pro Secure Entry, attivare **Ignore server certificate validation (Ignora convalida certificato server)**. Per ulteriori informazioni, vedi *Certificati*.

2.3. Se il certificato del server non è stato configurato in AXIS Camera Station Pro Secure Entry, attivare **Ignore server certificate validation (Ignora convalida certificato server)**. Per ulteriori informazioni, vedi *Certificati*.

2.4. Se il certificato del server non è stato configurato in AXIS Camera Station Pro Secure Entry, attivare **Ignore server certificate validation (Ignora convalida certificato server)**. Per ulteriori informazioni, vedi *Certificati*.

2.5. Attiva **AXIS Camera Station Secure Entry**.

2.6. Fai clic su **Add (Aggiungi)** e immetti l'indirizzo IP del door controller e incolla la chiave di autenticazione.

2.7. Selezionare il lettore che legge codici a barre dal menu a discesa della porta.

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.
- Richiede AXIS Camera Station 5.47 o successivo.
- 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 55767. Per la configurazione personalizzata della porta, consulta .
- Il collegamento di un server secondario a un server principale comporta la sostituzione della chiave del suo lettore, rendendo non valide tutte le credenziali Bluetooth esistenti. Per evitare ciò, creare le credenziali Bluetooth sul server principale anziché sul server secondario.

Flusso di lavoro

1. Configura un server come server secondario e genera il file di configurazione. Vedere *Genera il file di configurazione dal server secondario, on page 29*.
2. Configura un server come server principale e importa il file di configurazione dei server secondari. Vedere *Importa il file di configurazione sul server principale, on page 30*.
3. Configura i titolari di tessera e i gruppi di titolari di tessera globali nel server principale. Vedere *Aggiungi un titolare tessera, on page 32* e *Aggiungi un gruppo, on page 36*.
4. Visualizza e monitora i titolari di tessera e i gruppi di titolari di tessera globali dal server secondario. Vedere *Gestione degli accessi, on page 32*.

Genera il file di configurazione dal server secondario

1. Dal server secondario, vai su **Configuration > Access control > Multi server (Configurazione > 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, vai su **Configuration > Access control > Multi server (Configurazione > 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, vai su **Configuration > Access control > Multi server (Configurazione > 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 **Configuration > Access control > Multi server (Configurazione > 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 **Configuration > Access control > Multi server (Configurazione > Controllo degli accessi > Multiserver)**.
   – Fare clic su **Sub server (Server secondario)** e su **Revoke server (Revoca server)**.

Impostazioni di Active Directory[BETA]

Nota

Gli account utente in Microsoft Windows e gli utenti e i gruppi di Active Directory possono accedere ad AXIS Camera Station Pro Secure Entry. Il modo in cui si aggiungono gli utenti in Windows varia a seconda della versione. Per saperne di più, andare a *support.microsoft.com*. Vedere l'amministratore di rete se si usa una rete di dominio di Active Directory.

La prima volta che viene aperta la pagina delle impostazioni Active Directory, hai la possibilità di importare gli utenti di Microsoft Active Directory nei titolari di tessera in AXIS Camera Station Pro Secure Entry. Vedere *Importare gli utenti Active Directory, on page 31*.

Dopo la configurazione iniziale, appaiono le seguenti opzioni nella pagina impostazioni di Active directory.

- Creare e gestire gruppi di titolari di tessera a seconda dei gruppi in Active Directory.
- Impostare la sincronizzazione pianificata tra Active Directory e il sistema di gestione degli accessi.

- Sincronizzare in modo manuale per eseguire l'aggiornamento di tutti i titolari di tessera importati da Active Directory.
- Gestire la mappatura dei dati tra i dati utente di Active Directory e le proprietà dei titolari di tessera.

Importare gli utenti Active Directory

Per eseguire l'importazione degli utenti Active Directory ai titolari di tessera in AXIS Camera Station Pro Secure Entry:

1. Andare su **Configuration (Configurazione)** > **Access control (Controllo degli accessi)** > **Active directory settings (Impostazioni di Active Directory)**[BETA].
2. Fare clic su **Set up import (Configura importazione)**.
3. Seguire le istruzioni sullo schermo per completare queste tre fasi principali:
   3.1. Selezionare un utente da Active Directory da impiegare in qualità di modello per la mappatura dati.
   3.2. Mappare dati utente dal database Active Directory alle proprietà dei titolari di tessera.
   3.3. Creare un nuovo gruppo di titolari di tessera nel sistema di gestione degli accessi e selezionare quali gruppi Active Directory vanno importati.

Non è possibile modificare i dati utente importati, ma è possibile aggiungere le credenziali a un titolare di una tessera importata, vedere *Aggiungi credenziali, on page 34*.

Importante

Se si disattiva un utente in Active Directory, AXIS Camera Station Pro elimina definitivamente il titolare della tessera e tutti i dati correlati, compresa la cronologia. Questa non può essere annullata. Per bloccare l'accesso di un titolare di tessera senza perdere i suoi dati, sospenderli in AXIS Camera Station Pro anziché disabilitarli in Active Directory.

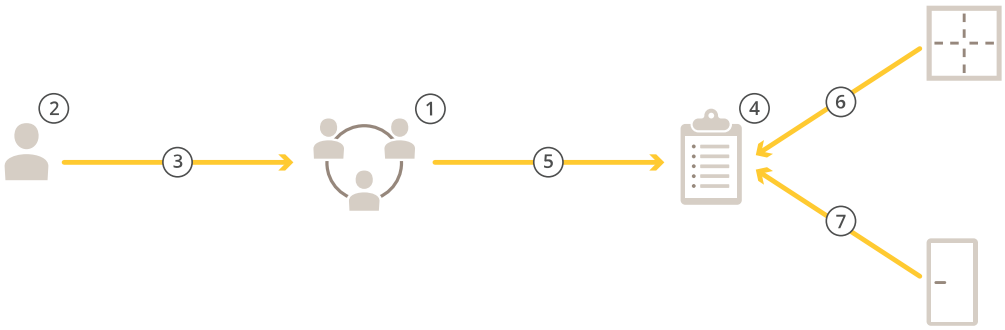
Gestione degli accessi

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.

Per un flusso di lavoro completo per l'impostazione di un network door controller Axis in AXIS Camera Station Pro Secure Entry, vedere *Imposta un network door controller Axis*.

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 un gruppo, on page 36*.
2. *Aggiungi un titolare tessera, on page 32*.
3. Aggiunta di titolari di tessera ai gruppi.
4. *Aggiungi una regola di accesso, on page 37*.
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.

Puoi anche scegliere di mappare gli utenti in un database di Active Directory come titolari tessera, vedi *Impostazioni di Active Directory*^{BETA}*, on page 30*.

1. Aprire una scheda di gestione degli accessi .
2. Andare in **Cardholder management (Gestione titolari tessere)** > **Cardholders (Titolari di tessere)** e fare clic su **+Add (+Aggiungi)**.
3. Inserire il nome e il cognome del titolare di tessera. Facoltativamente, è possibile aggiungere ulteriori dettagli al titolare della tessera:
   - In **Email**, inserire l'indirizzo e-mail del titolare della tessera.
   - In **Groups (Gruppi)**, selezionare i gruppi a cui si desidera aggiungere il titolare della tessera.
   - In **Access rules (Regole di accesso)**, selezionare le regole di accesso che si desidera applicare al titolare della tessera.
4. Per aggiungere una foto, cliccare su **Cardholder picture (Foto del titolare della tessera)** e selezionare:
   - **Upload (Caricare)** per aggiungere un'immagine dal proprio dispositivo.

- **Capture (Acquisire)** per scattare una foto direttamente con la fotocamera.

Nota

L'immagine deve essere un file JPG, PNG o GIF. Le immagini vengono ridimensionate automaticamente a un massimo di 700x700 pixel e convertite in formato JPG.

5. Cliccare su **Advanced (Avanzate)** per configurare le opzioni supplementari.
6. Aggiungere una credenziale al titolare di tessere. Vedere *Aggiungi credenziali, on page 34*.
7. Fare clic su **Save (Salva)**.
8. Per stampare i badge per uno o più titolari di tessera, selezionare i titolari di tessera desiderati e cliccare su **Print Badge (Stampa badge)**[BETA]. Per ulteriori informazioni, consultare *Print badge (Stampa badge) [BETA], on page 42*.

Utilizzare il campo di ricerca per trovare un titolare di tessera in base al nome o al cognome. Per filtrare in base alle fonti, fare clic su **Filter (Filtra)** e selezionare **Local (Locale)**, **Global (Globale)**, **AD** o **Center (Centro)**.

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. Ciò rimuove temporaneamente tutti gli accessi dal titolare di 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 *Multi-server [BETA], on page 29*.

Per guardare questo video, andare alla versione web di questo documento.

Aggiunta di titolari di tessera e gruppi

Aggiungi credenziali

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

- *Credenziali con codici QR, on page 34*
- *Credenziali PIN, on page 34*
- *Credenziali su dispositivi mobili, on page 35*
- *Credenziali tessera, on page 35*
- *Credenziali targa, on page 35*

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.

Credenziali con codici QR

Nota

L'impiego di codici QR come credenziali richiede la sincronizzazione tra l'orario sul controller di sistema e la telecamera con AXIS Barcode Reader. Per una sincronizzazione dell'ora perfetta, consigliamo l'uso della stessa origine ora per entrambi i dispositivi.

Per aggiungere un codice QR come credenziale di un titolare di tessere:

1. In **Credentials (Credenziali)**, fare clic su **+Add (+ Aggiungi)** e selezionare **QR-code (Codice QR)**.
2. Inserire un nome per le credenziali.
3. **Dynamic QR (QR dinamico)** è attivo per impostazione predefinita. È necessario usare la funzione QR dinamica con credenziali PIN.
4. Impostare la data di inizio e di fine delle credenziali.
5. Per inviare per e-mail in automatico il codice QR dopo aver salvato il titolare di tessera, seleziona **Send QR code to cardholder when credential is saved** (Invia codice QR al titolare di tessera quando le credenziali vengono salvate).
6. Fare clic su **Aggiungi**.

Credenziali PIN

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. In alternativa, per attivare un allarme silenzioso con un PIN separato, attivare l'opzione **Duress PIN** (PIN di emergenza) e inserire un PIN di emergenza.
4. Impostare le date **Valid from** (Valido da) e **Valid to** (Valido fino al) per le credenziali.
5. Fare clic su **Aggiungi**.

Credenziali su dispositivi mobili

Nota

Il titolare tessera deve disporre di un indirizzo e-mail per ricevere le credenziali mobili.

Per aggiungere un telefono cellulare come credenziali di un titolare di tessere:
1. In **Credentials (Credenziali)**, fare clic su **+Add (+ Aggiungi)** e selezionare **Mobile credential (Credenziali telefono cellulare)**.
2. Inserire un nome per le credenziali.
3. Impostare la data di inizio e di fine delle credenziali.
4. Selezionare **Send the mobile credential to the cardholder after saving (Invia le credenziali mobili al titolare della tessera dopo il salvataggio)**. Il titolare della tessera riceve un messaggio e-mail con le istruzioni per eseguire l'associazione.
5. Fare clic su **Aggiungi**.

Vedere l'esempio in *Utilizzare l'app AXIS Mobile Credential come credenziali Bluetooth, on page 18*.

Credenziali tessera

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)**.

Nota

Per acquisire i dati della tessera, hai la possibilità di usare il lettore di tessere USB desktop 2N. Se necessiti di maggiori informazioni, consulta *Configurazione del lettore di tessere USB desktop 2N*.

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**.

Credenziali targa

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**.

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 Camera Station Pro Secure Entry. Vedere .
2. Aggiorna il firmware sui nuovi dispositivi alla versione più recente a disposizione. Vedere .
3. Aggiungi una nuova porta connessa al tuo door controller. Vedere *Aggiunta di una porta, on page 7*.
   3.1. Aggiungi un lettore su **Side A (Lato A)**. Vedere *Aggiungi un lettore, on page 16*.
   3.2. In **Door settings (Impostazioni porta)**, seleziona **AXIS License Plate Verifier** come **Reader type (Tipo lettore)** e inserisci un nome per il lettore.
   3.3. In via facoltativa, aggiungi un lettore o un dispositivo REX su **Side B (Lato B)**.
   3.4. Fare clic su **OK**.
4. Installare e attivare AXIS License Plate Verifier sulla tua telecamera. Vedi il manuale per l'utente *AXIS License Plate Verifier*.
5. Avvia AXIS License Plate Verifier.
6. Configura AXIS License Plate Verifier.
   6.1. Andare a **Configuration > Access control > Encrypted communication (Configurazione > Controllo degli accessi > Comunicazione crittografata)**.
   6.2. 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)**.
   6.3. Apri AXIS License Plate Verifier dall'interfaccia Web della telecamera.
   6.4. Non effettuare l'impostazione.
   6.5. Andare a **Settings (Impostazioni)**.
   6.6. In **Access control (Controllo degli accessi)**, seleziona **Secure Entry** come **Type (Tipo)**.
   6.7. In **IP address (Indirizzo IP)**, immetti l'indirizzo IP e le credenziali per il door controller.
   6.8. In **Authentication key (Chiave di autenticazione)**, incolla la chiave di autenticazione che hai copiato in precedenza.
   6.9. Fare clic su **Connetti**.
   6.10. In **Door controller name (Nome door controller)**, seleziona il door controller.
   6.11. In **Reader name (Nome lettore)**, seleziona il lettore che hai aggiunto in precedenza.
   6.12. Attiva l'integrazione.
7. Aggiungi il titolare tessera a cui vuoi concedere l'accesso. Vedere *Aggiungi un titolare tessera, on page 32*
8. Eseguire l'aggiunta di credenziali targa al nuovo titolare tessera. Vedere *Aggiungi credenziali, on page 34*
9. Aggiungi una regola di accesso. Vedere *Aggiungi una regola di accesso, on page 37*.
   9.1. Aggiungere una pianificazione.
   9.2. Aggiungi il titolare tessera a cui vuoi concedere l'accesso tramite targa.
   9.3. 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. Aprire una scheda di gestione degli accessi .
2. Andare in **Cardholder management (Gestione titolari tessere)** > **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 *Multi-server BETA, on page 29*.
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)**.
7. Per stampare i badge di tutti i titolari di tessera di un gruppo, selezionare il gruppo e fare clic su **Print Badge (Stampa Badge)**BETA. Per ulteriori informazioni, consultare *Print badge (Stampa badge) BETA, on page 42*.

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.

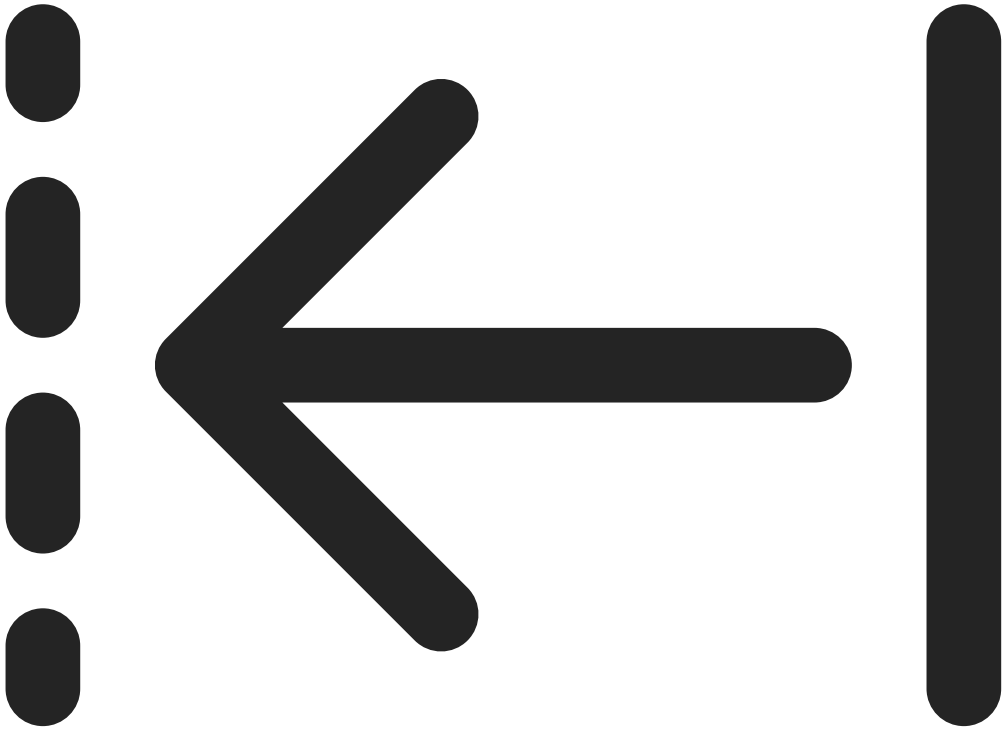
Porte e zone – dove si applica l'accesso.

Pianificazioni – quando concedere l'accesso.

Per aggiungere una regola di accesso:

1. Aprire una scheda di gestione degli accessi .
2. Andare in **Cardholder management (Gestione titolari tessere)**.

3. In **Access rules (Regole di accesso)**



, cliccare su **+Add (+ Aggiungi)**.

4. Immettere un nome per la regola di accesso e fare clic su **Next (Avanti)**.
5. Configurazione dei titolari e dei gruppi:
   5.1. In **Cardholders (Titolari di tessera)** o **Groups (Gruppi)**, fare clic su **+ Add (+Aggiungi)**.
   5.2. Selezionare i titolari di tessera o i gruppi e fare clic su **Add (Aggiungi)**.
   5.3. È inoltre possibile trascinare e rilasciare un titolare di tessera o un gruppo direttamente su una regola di accesso per applicarla. Durante il trascinamento, vengono evidenziate le regole di accesso su cui è possibile rilasciare gli elementi. Se si trascinano più titolari di tessera o gruppi contemporaneamente, un conteggio indica quanti se ne stanno spostando.
6. Configurazione di porte e zone:
   6.1. In **Doors (Porte)** o **Zones (Zone)**, fare clic su **+ Add (+Aggiungi)**.
   6.2. Selezionare le porte o le zone e fare clic su **Add (Aggiungi)**.
7. Configurazione delle pianificazioni:
   7.1. In **Schedules (Programmi)**, fare clic su **+Add (+Aggiungi)**.
   7.2. Selezionare uno o più programmi e fare clic su **Add (Aggiungi)**.
8. 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**.

Esportazione dei report sulla configurazione del sistema

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

1. Aprire una scheda di gestione degli accessi .
2. Andare in **Reports** > **System configuration (Configurazione del sistema)**.
3. Selezionare i rapporti da esportare e fare clic su **Download**.

Report di dettagli titolari tessera	Include informazioni sui titolari di tessera, sulle credenziali, sulla convalida della tessera e sull'ultima transazione.
Report di 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.
Report di accesso gruppo titolari di 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.
Report di 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.
Report di 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.
Report di accesso zone	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. Aprire una scheda di gestione degli accessi .
2. Andare in **Reports** > **Cardholder activity (Attività titolari tessera)**.
3. Fare clic su **+ Add (+Aggiungi)** e selezionare **Roll call / Mustering (Appello/Raduno)**.
4. Immettere un nome per il report.
5. Selezionare le zone da includere nel report.
6. Selezionare i gruppi che si desidera includere nel report.
7. Se si desidera un report di raduno, selezionare **Mustering point (Punto di raduno)** e un lettore per il punto di raduno.
8. Selezionare un intervallo temporale per il report.
9. Fare clic su **Save (Salva)**.
10. 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.

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.

Puoi anche scegliere di mappare gli utenti in un database di Active Directory come titolari tessera, vedi *Impostazioni di Active Directory[BETA], on page 30*.

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 Camera Station Pro Secure Entry 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**.

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 *Profili di identificazione, on page 22*.

Per modificare un modello di e-mail per l'invio di credenziali QR o mobili:

1. Nella scheda **Access management (Gestione accessi)**, fare clic su **Settings (Impostazioni)** > **Email templates (Modelli email)**.
2. Modificare il proprio modello e fare clic su **Update (Aggiorna)**.

Modelli di badge BETA

È possibile personalizzare i modelli di badge con le informazioni del titolare della tessera, foto, loghi e marchi personalizzati. Per creare un nuovo modello:

1. Andare ad **Access management > Settings > Badge templates** BETA (Gestione degli accessi, Impostazioni, Modelli badge, BETA).
2. Fare clic su **Create new template (Crea nuovo modello)**.
3. Immettere un nome nel campo **Template name (Nome modello)**.
4. Selezionare **Use as default template for printing** (Utilizza come modello predefinito per la stampa) se si desidera impostare il modello come predefinito.
5. Personalizzare il design del badge:
   - Selezionare fino a cinque campi di testo da visualizzare sul lato anteriore, compresi eventuali campi personalizzati che sono stati creati. Durante la stampa, sul badge compaiono solo i campi compilati.
   - Scegliere il carattere e il colore del testo.
   - Aggiungere un colore o un'immagine di sfondo.
   - Caricare un logo della propria organizzazione.
   - Sul retro, aggiungere un colore di sfondo o un'immagine.
6. Fare clic su **Save** (Salva) per salvare le modifiche, oppure su **Save as** (Salva come) per salvare come un nuovo modello.

Nota

Una volta creato, il modello non può subire modifiche, può essere solo rinominato.

Print badge (Stampa badge) BETA

È possibile stampare badge di identificazione per i titolari di tessere utilizzando i modelli di badge configurati. Si noti che il codificatore schede non è attualmente supportato. Operazioni preliminari:

- Verificare che il titolare della tessera disponga di almeno una credenziale della tessera. Non è possibile stampare badge per i titolari di tessere senza credenziali.
- È necessaria una stampante che supporti il formato CR80 e materiali di stampa compatibili, come cartoncino spesso.
- Configurare le impostazioni di stampa del browser:
  1. Configurare le impostazioni pagina su CR80 o su un formato personalizzato che corrisponda alla dimensione della tessera.
  2. Impostare l'orientamento su verticale.
  3. Disattivare i margini o impostarli al minimo.

Importante

Secure Entry è compatibile con le stampanti dotate di driver Windows. Le stampanti della serie HID Fargo sono state verificate e risultano funzionanti. Se è necessario un driver per la stampante, contattare il fornitore della stampante.

Per stampare i badge:

1. Andare a **Access management > Cardholder management > Cardholders** (Gestione degli accessi, Gestione titolari tessera, Titolari tessera).
2. Selezionare uno o più titolari tessera;
3. Fare clic su **Print badge** (Stampa badge) BETA.
4. Fare clic su **Select template** (Seleziona modello) e dall'elenco a discesa **Template** (Modello), selezionare il modello di badge che si desidera utilizzare.
5. Se il titolare della tessera dispone di più credenziali, selezionarne una dall'elenco a discesa **Card** (Tessera).
6. Fare clic su **Print (Stampa)**.

Nota

Se la stampante non supporta la stampa fronte/retro, stampare prima tutti i lati anteriori, quindi capovolgere la pila di cartoncini e reinserirli nel vassoio per stampare i lati posteriori.

T10231644_it

2026-04 (M7.2)