

AXIS Camera Station Pro Secure Entry

Despre

Secure Entry este o componentă a AXIS Camera Station Pro. Utilizați-l pentru a adăuga dispozitive și a gestiona programele. Pentru mai multe informații, consultați *AXIS Camera Station Pro User Manual (Manualul de utilizare AXIS Camera Station Pro)*.

Configurați controlul de acces

Dacă adăugați un controler de ușă de rețea Axis la sistemul dvs., puteți configura hardware-ul de control al accesului în AXIS Camera Station versiunea 6.x sau o versiune ulterioară.

Pentru un flux de lucru complet pentru configurarea unui controler de ușă de rețea Axis în AXIS Camera Station Pro Secure Entry, consultați *Set up an Axis network door controller (Configurarea unui controler de ușă de rețea Axis)*.

note

Înainte de a începe, faceți următoarele:

- Actualizați versiunea sistemului de operare AXIS OS al controlerului la **Configuration (Configurație) > Devices (Dispozitive) > Management (Gestionare)**.
- Setati data și ora pentru controler **Configuration (Configurație) > Devices (Dispozitive) > Management (Gestionare)**.
- Activați HTTPS pe controler la **Configuration (Configurație) > Devices (Dispozitive) > Management (Gestionare)**.

Flux de lucru pentru configurarea controlului de acces

1. Pentru a edita profilurile de identificare predefinite sau pentru a crea unul nou, consultați *Profiluri de identificare, on page 20*.
2. Pentru a utiliza o configurație personalizată pentru formatele cardurilor și lungimea PIN-ului, consultați *Formatele cardurilor și PIN-ul, on page 22*.
3. Adăugați o ușă și aplicați un profil de identificare ușii. Consultați *Adăugați o ușă, on page 7*.
4. Configurați ușa:
 - Adăugați un senzor de poziție a ușii, *on page 12*
 - Adăugați un senzor de urgență, *on page 14*
 - Adăugați un cititor, *on page 15*
 - Adăugare un dispozitiv REX, *on page 16*
5. Adăugați o zonă și adăugați uși la zonă. Consultați *Adăugare o zonă, on page 18*.

Compatibilitatea software-ului dispozitivului pentru controlerul de uși

important

Țineți cont de următoarele aspecte atunci când actualizați sistemul de operare AXIS OS pe controlerul ușii:

- **Supported AXIS OS versions (Versiuni AXIS OS acceptate):** Versiunile AXIS OS acceptate enumerate mai jos se aplică numai în cazul actualizării de la versiunea inițială recomandată de AXIS Camera Station Pro Secure Entry și atunci când sistemul are o ușă configurată. Dacă sistemul nu îndeplinește aceste condiții, trebuie să faceți upgrade la versiunea sistemului de operare AXIS OS recomandată pentru versiunea AXIS Camera Station Pro Secure Entry specifică.
- **Minimum supported AXIS OS version (Versiunea minimă AXIS OS acceptată):** Cea mai veche versiune a sistemului de operare AXIS OS instalat în sistem determină versiunea sistemului de operare AXIS minimă acceptată, cu o limită de două versiuni anterioare. Să presupunem că utilizați versiunea 6.5 a sistemului de operare AXIS Camera Station Pro Secure Entry și că actualizați toate dispozitivele la versiunea recomandată 12.0.86.2 a sistemului de operare AXIS OS. Prin urmare, versiunea 12.0.86.2 a sistemului de operare AXIS OS va deveni versiunea minimă acceptată pentru sistemul dvs. de acum înainte.
- **Upgrading beyond recommended AXIS OS version (Actualizarea la o versiune AXIS OS superioară celei recomandate):** Să presupunem că efectuați o actualizare la o versiune AXIS OS superioară celei recomandate pentru o anumită versiune a sistemului de operare AXIS Camera Station Pro Secure Entry. Apoi, puteți face oricând downgrade înapoi la versiunea sistemului de operare AXIS OS recomandată fără nicio problemă, atâta timp cât se încadrează în limitele de acceptare stabilite pentru versiunea AXIS Camera Station Pro Secure Entry.
- **Future AXIS OS recommendations (Recomandări privind sistemul de operare AXIS OS):** Respectați întotdeauna versiunea recomandată de AXIS OS pentru versiunea respectivă a AXIS Camera Station Pro Secure Entry, pentru a asigura stabilitatea sistemului și compatibilitatea deplină.
- **Track change (Monitorizarea modificării):** Trecerea de la versiunile de firmware 10.12.xx la 11.0.xx sau o versiune ulterioară necesită o resetare la setările din fabrică.

Tabelul de mai jos prezintă versiunea minimă și recomandată a sistemului de operare AXIS OS pentru fiecare versiune AXIS Camera Station Pro:

Versiunea AXIS Camera Station	Versiunea minimă a sistemului de operare AXIS OS	Versiunea recomandată a sistemului de operare AXIS OS
Pro 6.17	12.6.102.1	12.9.65.3
Pro 6.16	12.6.102.1	12.9.65.3
Pro 6.15	12.5.68.1	12.8.55.1

Uși și zone

Accesați **Configuration (Configurație) > Access control (Control de acces) > Doors and zones (Uși și zone)** pentru a obține o prezentare generală și pentru a configura ușile și zonele.

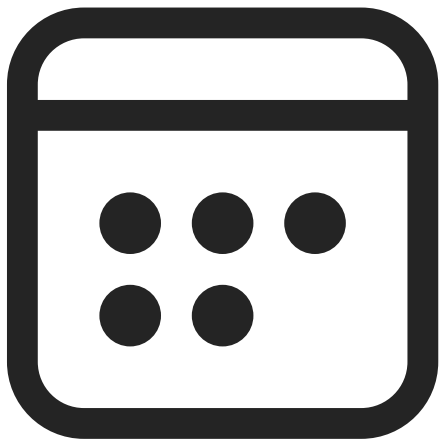
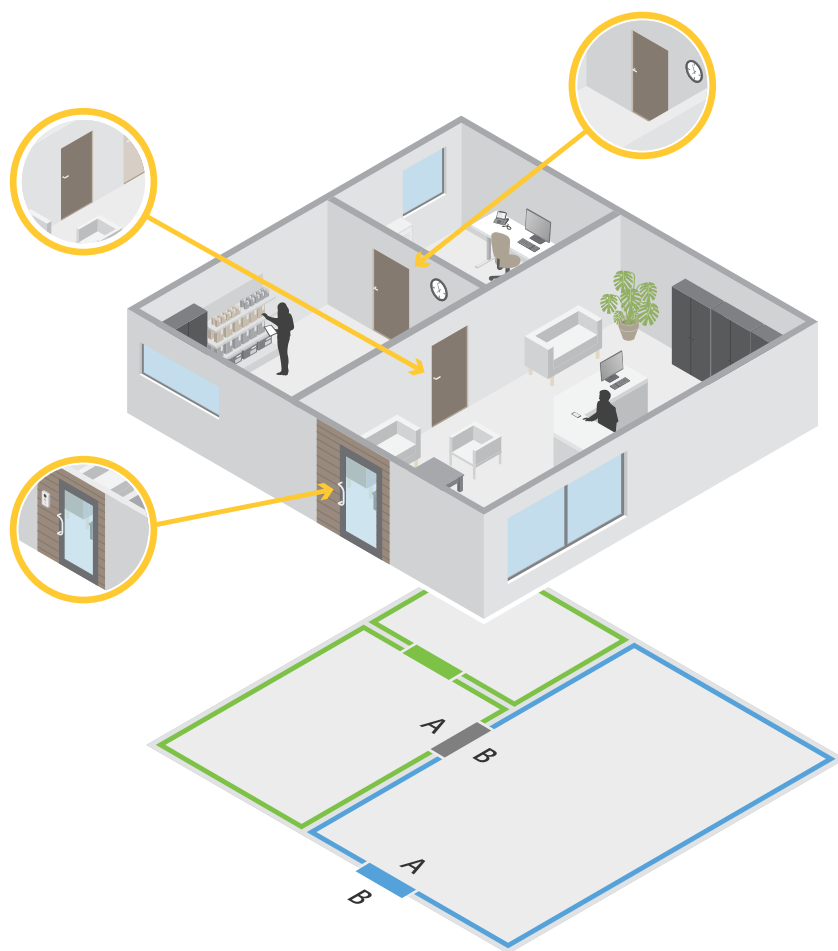
 Acțiuni manuale	Setați manual starea unei uși. Selectați din următoarele opțiuni: Reset (Resetare) (respectați regulile sistemului), Grant access (Acordare acces) (deblocarea ușii timp de 7 secunde), Unlock (Deblocare) (menținerea ușii deblocate), Lock (Blocare) (menținerea ușii blocate) sau Lockdown (Încuiere) (nimeni nu poate intra sau ieși).
 Programe de deblocare	Setați un program pentru deblocarea automată a ușilor la ore prestabilite. În restul timpului, ușile rămân blocate. Pentru a impune ca prima persoană să deblocheze ușa manual înainte ca programul să se activeze, activați First person in (Prima persoană care intră).
 Profil de identificare	Modificarea profilului de identificare de pe uși.

 Diagrama PIN	Vedeți diagrama pinilor controlerului asociat cu o ușă. Pentru a imprima graficul cu pini, faceți clic pe Print (Imprimare) .
 Canal securizat	Activează sau dezactivează OSDP Secure Channel (Canalul securizat OSDP) pentru un anumit cititor.

Uși	
Name (Nume)	Numele ușii.
Type (Tip)	Tipul configurației ușii.
Dispozitiv	Dispozitivul conectat la ușă.
Adresa IP	Adresa IP a controlerului de ușă conectat la ușă.
Partea A	Zona în care se află partea A a ușii.
Partea B	Zona în care se află partea B a ușii.
Profil de identificare	Profilul de identificare aplicat ușii.
Baterie	Starea bateriei controlerului de ușă.
Status (Stare)	Starea ușii. • Online: Ușa este online și funcționează corect. • Reader offline (Cititor offline): Cititorul din configurația ușii este offline. • Reader error (Eroare cititor): Cititorul nu acceptă canalul securizat sau acesta este dezactivat pentru cititor. • Old firmware (Firmware învechit): Dispozitivul are o versiune de firmware învechită. Actualizați firmware-ul pentru performanță și securitate optime.
Zone	
Name (Nume)	Numele zonei.
Număr de uși	Numărul de uși incluse în zonă.
Nivel de securitate	Nivelul de securitate aplicat zonei.

Exemplu de uși și zone



- Există două zone: zona verde și zona albastră.
- Există trei uși: ușa verde, ușa albastră și ușa maro.
- Ușa verde este o ușă internă din zona verde.
- Ușa albastră este o ușă perimetrală numai pentru zona albastră.
- Ușa maro este o ușă perimetrală atât pentru zona verde, cât și pentru zona albastră.

Acțiuni manuale

Puteți efectua următoarele acțiuni manuale la uși și zone:

Reset (Resetare) – Revine la regulile de sistem configurate.

Grant access (Permiterea accesului) – Deblochează o ușă sau o zonă timp de 7 secunde și apoi o blochează din nou.

Unlock (Deblocare) – Ține ușa descuiată până când realizați resetarea.

Lock (Blocare) – Ține ușa încuiată până când sistemul acordă acces unui titular de card.

Lockdown (Închidere) – Nimeni nu intră sau nu iese până când nu resetați sau deblocați.

Pentru a efectua o acțiune manuală:

1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Doors and zones (Uși și zone)**.
2. Selectați ușa sau zona.
3. Faceți clic pe oricare dintre acțiunile manuale.

Uși

Adăugați o ușă

note

- Puteți configura un controler de uși cu o ușă care are două încuietori sau cu două uși care au câte o încuietoare. Controlerele multiple acceptă configurații suplimentare de blocare.

Pentru a adăuga o ușă:

1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Doors and zones (Uși și zone)**.
2. Faceți clic pe **+** **Add (Adăugați)** și selectați un tip de ușă din lista derulantă.

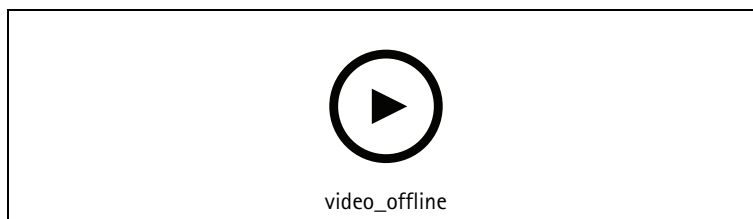
Tipuri de ușă	
Ușă	O ușă obișnuită cu un monitor de ușă care acceptă încuietori și cititoare. Necesită un controler de ușă.
Etaj	Un tip de ușă pentru controlul liftului care autentifică accesul la etajele liftului folosind cititoare de carduri. Pentru mai multe informații, consultați <i>Adăugați un etaj</i> ^{BETA} , on page 8.
Ușă cu monitorizare	O ușă care poate semnaliza dacă este deschisă sau închisă. Pentru mai multe informații, consultați <i>Adăugați o ușă de monitorizare</i> , on page 8.
Ușă wireless	O ușă pe care o puteți configura cu încuietori wireless și hub-uri de comunicații ASSA ABLOY Aperio®. Pentru mai multe informații, consultați <i>Adăugarea unei încuietoare wireless</i> , on page 9.
Ușă prevăzută	O ușă provizorie pe care o puteți adăuga în sistem fără a selecta hardware.

3. Introduceți un nume pentru ușă și selectați un controler de ușă din meniul derulant **Device (Dispozitiv)** pentru a-l asocia cu ușă. Controlerul apare estompat atunci când nu se poate adăuga o altă ușă, când este offline sau când protocolul HTTPS nu este activat.
4. Faceți clic pe **Next (Mai departe)** pentru a accesa pagina de configurare a ușii.
5. În meniul vertical **Primary lock (Încuietoare primară)**, selectați un port releu.
6. Pentru a configura două încuietori pe ușă, selectați un port releu din meniul vertical **Secondary lock (Încuietoare secundară)**.
7. Selectați un profil de identificare. Consultați *Profiluri de identificare*, on page 20.
8. Configurați ușa adăugând senzori sau cititoare în secțiunile **Sensors (Senzori)**, **Side A (Partea A)** și **Part B (Partea B)**.
9. Configurați setările ușii respective. Consultați *Setări ușă*, on page 10.
10. Faceți clic pe **Save (Salvare)**.

Copierea unei configurații de ușă:

1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Doors and zones (Uși și zone)**.
2. Faceți clic pe **+** **Add (Adăugați)**.
3. Introduceți un nume pentru ușă și selectați un controler de ușă din meniul derulant **Device (Dispozitiv)** pentru a-l asocia cu ușă.
4. Faceți clic pe **Next (Mai departe)**.

5. În meniul vertical **Copy configuration (Copiere configurație)**, selectați o configurație existentă a ușii. Acesta arată ușile conectate, iar controlerul este gri dacă a fost configurat cu două uși sau cu o ușă cu două încuietori.
6. Modificați setările dacă doriți.
7. Faceți clic pe **Save (Salvare)**.



Adăugați și configurați uși și zone

Adăugați un etaj ^{BETA}

Un etaj este un tip de ușă pe care îl utilizați pentru a controla accesul la etajele liftului. Când adăugați un etaj, creați o resursă lift care grupează toate etajele pentru acel lift. Fiecare etaj utilizează un cititor de carduri în interiorul cabinei liftului pentru a autentifica utilizatorii înainte de a le permite accesul la etajul respectiv.

Înainte de a începe, este necesar:

- Un Network Door Controller acceptat adăugat la sistemul dvs., cum ar fi *AXIS A1610*, *AXIS A1710-B* sau *AXIS A1810-B*.
- Un I/O expansion module (Modul de extindere I/O) pentru relee suplimentare. Vă recomandăm modelul *AXIS A9920*.

note

Această funcție se află în faza Beta și acceptă în prezent până la 64 de etaje și numai cititoare de carduri.

Pentru a configura un etaj:

1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Doors and zones (Uși și zone)**.
2. Faceți clic pe **+ Add (Adăugați)** și selectați **Floor (Etaj)** ^{BETA}.
3. Introduceți un nume pentru etaj.
4. Selectați controlerul.
5. La **Elevator (Lift)**, selectați un lift existent sau faceți clic pe **Create new elevator (Creați un lift nou)** pentru a adăuga unul nou, apoi introduceți un nume.
6. La **Side A (Partea A)**, selectați **Card reader (Cititor de carduri)** și configurați-vă cititorul. **Side B (Partea B)** nu poate fi configurată din motive de siguranță.
7. Faceți clic pe **Save and add new (Salvați și adăugați unul nou)** pentru a adăuga mai multe etaje la același lift. Configurația liftului și a cititorului rămâne completată pentru etajul următor. Această opțiune este disponibilă numai dacă controlerul dvs. are relee.
8. Faceți clic pe **Save (Salvați)** după ce ați adăugat etajul. Etajele apar ca „Numele liftului – Numele etajului”, de exemplu: „West Side – Floor 1” (Partea de vest – Etajul 1)

note

- Cititoarele utilizate la mai multe etaje pot fi editate numai la primul etaj la care au fost adăugate.
- Lifturile sunt șterse automat atunci când toate etajele asociate au fost șterse.

Adăugați o ușă de monitorizare

O ușă cu monitorizare este un tip de ușă care vă poate arăta dacă este deschisă sau închisă. De exemplu, puteți utiliza acest sistem la o ușă de siguranță împotriva incendiilor care nu necesită o încuietoare, dar unde trebuie să știți dacă ușa este deschisă.

O ușă cu monitorizare este diferită de o ușă obișnuită cu un monitor de ușă. O ușă obișnuită cu un monitor de ușă acceptă încuietori și cititoare, dar necesită un controler de ușă. O ușă cu monitorizare acceptă un senzor de

poziție a ușii, dar necesită doar un modul de releu I/O conectat la un controler de ușă. Puteți conecta până la cinci senzori de poziție a ușii la un modul releu I/O de rețea.

note

O ușă cu monitorizare necesită un modul de releu I/O de rețea AXIS A9210 cu cel mai recent firmware, inclusiv aplicația AXIS Monitoring Door ACAP.

Pentru a configura o ușă cu monitorizare:

1. Instalați AXIS A9210 și faceți upgrade la cea mai recentă versiune a sistemului de operare AXIS OS.
2. Instalați senzorii de poziție a ușii.
3. În AXIS Camera Station Pro, accesați **Configuration (Configurație) > Access control (Control de acces) > Doors and zones (Uși și zone)**.
4. Faceți clic pe **Add door (Adăugare ușă)**.
5. Introduceți un nume.
6. La **Type (Tip)**, selectați **Monitoring door (Ușă cu monitorizare)**.
7. La **Device (Dispozitiv)**, selectați modulul releu I/O de rețea.
8. Faceți clic pe **Next (Mai departe)**.
9. La **Sensors (Senzori)**, faceți clic pe **+ Add (Adăugați)** și selectați **Door position sensor (Senzor de poziție ușă)**.
10. Selectați I/O care este conectat la senzorul de poziție a ușii.
11. Faceți clic pe **Add (Adăugare)**.

Adăugarea unei încuietoare wireless

AXIS Camera Station Pro Secure Entry acceptă încuietorile wireless și huburile de comunicare ASSA ABLOY Aperio®. Încuietoarea wireless se conectează la sistem prin intermediul unui hub de comunicare Aperio conectat la conectorul RS485 al controlerului ușii. Puteți conecta 16 încuietori wireless la un controler de ușă.



note

- Configurarea necesită ca controlerul de ușă Axis să aibă sistemul de operare AXIS OS versiunea 11.6.16.1 sau ulterioară.
 - Configurarea necesită o licență valabilă pentru Extensia Controlerului de Ușă AXIS.
 - Ora de pe controlerul de ușă Axis și de pe serverul AXIS Camera Station Pro Secure Entry trebuie să fie sincronizate.
 - Înainte de a începe, utilizați aplicația Aperio pe care ASSA ABLOY o acceptă pentru a asocia încuietorile Aperio cu hub-ul Aperio.
 - La fiecare conector RS485 se poate conecta doar un singur hub de comunicații Aperio. Funcția „multi-drop” nu este acceptată.
 - Încuietorile fără fir nu vor respecta programele de deblocare atunci când sunt offline.
1. Accesați controlerul de ușă.
 - 1.1. Accesați **Configuration (Configurație) > Devices (Dispozitive) > Other devices (Alte dispozitive)**.
 - 1.2. Deschideți interfața web a controlerului de ușă conectat la hub-ul de comunicare Aperio.
 2. Activați Extensia Controlerul de Ușă AXIS.

- 2.1. În interfața web a controlerului ușii, accesați **Apps (Aplicații)**.
- 2.2. Deschideți meniul contextual **AXIS Door Controller Extension (Extensia Controlerului de Ușă AXIS)** .
- 2.3. Faceți clic pe **Activate license with a key (Activare licență cu o cheie)** și selectați licența.
- 2.4. Activați **AXIS Door Controller Extension (Extensia Controlerul de Ușă AXIS)**.
3. Conectați încuietoarea wireless la controlerul ușii prin hub-ul de comunicare.
 - 3.1. În interfața web a controlerului de ușă, accesați **Access control (Control de acces) > Wireless locks (Încuietori wireless)**.
 - 3.2. Faceți clic pe **Connect communication hub (Conectarea hub-ului de comunicare)**.
 - 3.3. Introduceți un nume pentru hub și faceți clic pe **Connect (Conectare)**.
 - 3.4. Faceți clic pe **Connect wireless lock (Conectarea încuietorii wireless)**.
 - 3.5. Selectați adresa încuietorii și capabilitățile încuietorii pe care doriți să o adăugați și faceți clic pe **Save (Salvare)**.
4. Adăugați și configurați ușă cu încuietoarea wireless.
 - 4.1. În **AXIS Camera Station Pro Secure Entry**, accesați **Configuration (Configurație) > Access control (Control de acces) > Doors and zones (Uși și zone)**.
 - 4.2. La **Doors (Uși)**, faceți clic pe  **Add (Adăugați)**.
 - 4.3. Selectați **Wireless door (Ușă fără fir)** ca **Door type (Tip de ușă)** și controlerul de ușă conectat la hub-ul de comunicații **Aperio**.
 - 4.4. Faceți clic pe **Next (Mai departe)**.
 - 4.5. Selectați-vă **Wireless lock (Încuietoarea wireless)**.
 - 4.6. Definiți laturile ușii A și B și adăugați senzori. Pentru mai multe informații, consultați *Uși și zone, on page 4*.
 - 4.7. Faceți clic pe **Save (Salvare)**.

După ce ați conectat încuietoarea wireless, puteți vedea nivelul bateriei și starea acesteia în prezentarea generală a ușilor.

Nivelul bateriei	Acțiune
Bun	None (Niciuna)
Low (Scăzut)	Încuietoarea funcționează conform specificației, dar trebuie să înlocuiți bateria înainte ca nivelul acesteia să devină critic.
Critic	Înlocuiți bateria. Este posibil ca încuietoarea să nu funcționeze conform specificației.

Starea încuietorii	Acțiune
Online (Conectată):	None (Niciuna)
Lock jam (Înțepenirea încuietorii)	Rezolvați orice problemă mecanică de la încuietoare.

Setări ușă

Pentru a edita o ușă:

1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Door and Zones (Uși și zone)**.
2. Selectați ușă pe care doriți să o editați.

3. Faceți clic pe  **Edit (Editare)**.
4. La **Door settings (Setări ușă)**, modificați orice setare și faceți clic pe **Save (Salvare)**.

Timp de acces (sec)	Setați numărul de secunde în care ușa rămâne deblocată după acordarea accesului. Ușa se blochează din nou atunci când se închide, chiar dacă mai este timp.
Timp de deschidere prea lung (sec)	Valabil numai dacă ați configurat un monitor de ușă. Setați câte secunde poate rămâne ușa deschisă. Dacă ușa este încă deschisă la expirarea timpului, se declanșează alarma de ușă deschisă prea mult timp. Configurați o regulă de acțiune pentru a alege ce se întâmplă atunci când este declanșat acest eveniment.
Timp de acces lung (sec)	Setați câte secunde rămâne ușa deblocată după acordarea accesului pentru titularii de card, în cazul în care această setare este activată. Aceasta anulează timpul de acces standard.
Timp de deschidere lung-prea lung (sec)	Valabil numai dacă ați configurat un monitor de ușă. Setați numărul de secunde în care ușa poate rămâne deschisă pentru titularii de carduri, cu opțiunea Long access time (Timp de acces prelungit) activată. Anulează durata standard de deschidere prea îndelungată.
Timpul de întârziere la reconectare (ms)	Setați câte milisecunde rămâne ușa deblocată după ce a fost deschisă sau închisă.
Re-încuiere	• After opening (După deschidere): Valabil numai dacă ați adăugat un monitor de ușă. • After closing (După închidere): Valabil numai dacă ați adăugat un monitor de ușă.
Ușă forțată	Selectați dacă doriți ca sistemul să declanșeze o alarmă de sistem atunci când o ușă a fost deschisă forțat. Este necesar un senzor de poziție a ușii (DPS).
Ușă deschisă prea mult timp	Selectați dacă doriți ca sistemul să declanșeze o alarmă de sistem atunci când o ușă este ținută deschisă prea mult timp.

Pentru a îndepărta o ușă:

1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Doors and zones (Uși și zone) > Doors (Uși)**.
2. Selectați o ușă din listă.
3. Faceți clic pe  **Remove (Eliminare)** și confirmați.

Nivelul de securitate al ușii

Puteți adăuga la ușă următoarele funcții de securitate:

Two-person rule (Regula celor două persoane) – Regula celor două persoane impune ca două persoane să utilizeze informații de conectare valabile pentru a obține acces.

Double-swipe (Glisare dublă) – Glisarea rapidă dublă permite deținătorului de card să anuleze starea curentă a unei uși. De exemplu, ele o pot folosi pentru a bloca sau debloca o ușă în afara programului obișnuit, ceea ce este mai convenabil decât deblocarea ușii prin sistem. Glisarea dublă nu afectează un program existent. De exemplu, dacă o ușă este programată să se blocheze la ora de închidere, iar un angajat pleacă în pauza de prânz, ușa tot se va bloca în conformitate cu programul.

Puteți configura nivelul de securitate în timp ce adăugați o ușă nouă sau îl puteți aplica la o ușă existentă.

Pentru a adăuga **Two-person rule (Regula celor două persoane)** la o ușă existentă:

1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Doors and zones (Uși și zone)**.
2. Selectați ușa pentru care doriți să configurați un nivel de securitate.
3. Faceți clic pe **Edit (Editare)**.
4. Faceți clic pe **Security level (Nivel de securitate)**.
5. Activați **Two-person rule (Regula celor două persoane)**.
6. Faceți clic pe **Apply (Aplicare)**.

Two-person rule (Regula celor două persoane)	
Side A (Partea A) și Side B (Partea B)	Selectați pe ce părți ale ușii să fie utilizată regula.
Programe	Selectați când este activă regula.
Timeout (seconds) (Expirarea timpului (secunde))	Expirarea timpului este timpul maxim permis între glisările cardului sau a altor tipuri de informații de conectare valide.

Pentru a adăuga **Double-swipe (Glisare dublă)** la o ușă existentă:

1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Doors and zones (Uși și zone)**.
2. Selectați ușa pentru care doriți să configurați un nivel de securitate.
3. Faceți clic pe **Edit (Editare)**.
4. Faceți clic pe **Security level (Nivel de securitate)**.
5. Activați **Double-swipe (Glisare dublă)**.
6. Faceți clic pe **Apply (Aplicare)**.
7. Aplicați **Double-swipe (Glisare dublă)** unui titular de card.
 - 7.1. Deschideți o filă **Access Management (Gestionare acces)**.
 - 7.2. Faceți clic  pe titularul de card pe care doriți să îl editați și faceți clic pe **Edit (Editare)**.
 - 7.3. Faceți clic pe **More (Mai mult)**.
 - 7.4. Selectați **Allow double-swipe (Permiteți glisarea dublă)**.
 - 7.5. Faceți clic pe **Apply (Aplicare)**.

Double-swipe (Glisare dublă)	
Timeout (seconds) (Expirarea timpului (secunde))	Expirarea timpului este timpul maxim permis între glisările cardului sau a altor tipuri de informații de conectare valide.

Adăugați un senzor de poziție a ușii

Un senzor de poziție a ușii este un comutator care monitorizează starea fizică a unei ușii. Puteți adăuga un senzor de poziție a ușii și puteți configura modul de conectare al acestuia.

1. Accesați pagina de configurare a ușii. Consultați *Adăugați o ușă, on page 7*.
2. Sub **Sensors (Senzori)**, faceți clic pe **Add (Adăugare)**.
3. Selectați **Door position sensor (Senzor de poziție a ușii)**.
4. Selectați portul I/O la care doriți să conectați monitorul ușii.

5. Sub **Door open if (Ușă deschisă dacă)**, selectați modul de conectare a circuitelor de monitorizare a ușii.
6. Pentru a ignora modificările de stare ale intrării digitale înainte ca aceasta să intre într-o nouă stare stabilă, setați un **Debounce time (Timp de reținere)**.
7. Pentru a declanșa un eveniment atunci când conexiunea dintre controlerul ușii și monitorul de ușă este întreruptă, activați **Supervised input (Intrare supravegheată)**. Consultați *Intrări supravegheate, on page 13*.

Ușă deschisă dacă	
Circuitul este deschis	Circuitul de monitorizare a ușii este de tip normal închis. Monitorul ușii trimite ușii un semnal de deschidere atunci când circuitul este deschis. Monitorul ușii trimite ușii un semnal de închis atunci când circuitul este închis.
Circuitul este închis	Circuitul de monitorizare a ușii este de tip normal deschis. Monitorul ușii trimite ușii un semnal de deschidere atunci când circuitul este închis. Monitorul ușii trimite ușii un semnal de închis atunci când circuitul este deschis.

Intrări supravegheate

Intrările supravegheate pot declanșa un eveniment când există o întrerupere a conexiunii la un controler de ușă.

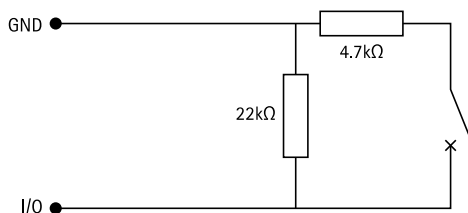
- Conexiune între controlerul ușii și monitorul ușii. Consultați *Adăugați un senzor de poziție a ușii, on page 12*.
- Conexiune între controlerul ușii și cititor care utilizează protocoalele Wiegand. Consultați *Adăugați un cititor, on page 15*.
- Conexiune între controlerul ușii și dispozitivul REX. Consultați *Adăugare un dispozitiv REX, on page 16*.

Pentru a utiliza intrările supravegheate:

1. Instalați rezistențele de capăt de linie cât mai aproape posibil de dispozitivul periferic, în conformitate cu diagrama de conectare.
2. Accesați pagina de configurare a unui cititor, monitor de ușă sau dispozitiv REX, activați **Supervised input (Intrare supravegheată)**.
3. Dacă ați urmat diagrama primei conexiuni paralele, selectați **Parallel first connection with a 22 K Ω parallel resistor and a 4.7 K Ω serial resistor (Prima conexiune paralelă cu o rezistență în paralel de 22 K Ω și o rezistență în serie de 4,7 K Ω)**.
4. Dacă ați urmat diagrama primei conexiuni în serie, selectați **Serial first connection (Prima conexiune în serie)** și selectați o valoare a rezistenței din meniul vertical **Resistor values (Valorile rezistențelor)**.

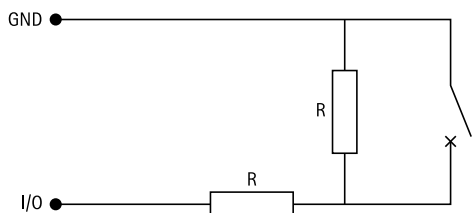
Prima conexiune în paralel

Valorile rezistenței trebuie să fie de 4,7 k Ω și 22 k Ω .



Prima conexiune în serie

Valorile rezistenței trebuie să fie identice și cuprinse în intervalul 1-10 k Ω .



Adăugați un senzor de urgență

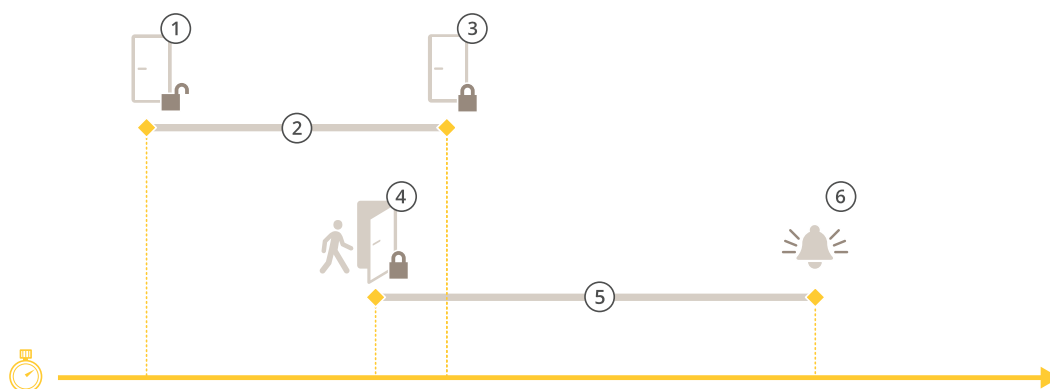
Puteți adăuga și configura o intrare de urgență pentru a iniția o acțiune care blochează sau deblochează ușa. De asemenea puteți configura modul de conectare a circuitului.

1. Accesați pagina de configurare a ușii. Consultați *Adăugați o ușă, on page 7*.
2. La **Sensors (Senzori)**, faceți clic pe **+ Add (Adăugare)**.
3. Selectați **Emergency input (Intrare de urgență)**.
4. Sub **Emergency state (Stare de urgență)**, selectați conexiunea circuitului.
5. Pentru a ignora modificările de stare ale intrării digitale înainte ca aceasta să intre într-o nouă stare stabilă, setați un **Debounce time (ms) (Timp de reținere (ms))**.
6. Selectați ce **Emergency action (Acțiune de urgență)** să declanșeze atunci când ușa primește semnalul de stare de urgență.

Stare de urgență	
Circuitul este deschis	Circuitul de intrare de urgență este de tip normal închis. Intrarea de urgență trimite un semnal de stare de urgență atunci când circuitul este deschis.
Circuitul este închis	Circuitul de intrare de urgență este de tip normal deschis. Intrarea de urgență trimite un semnal de stare de urgență atunci când circuitul este închis.

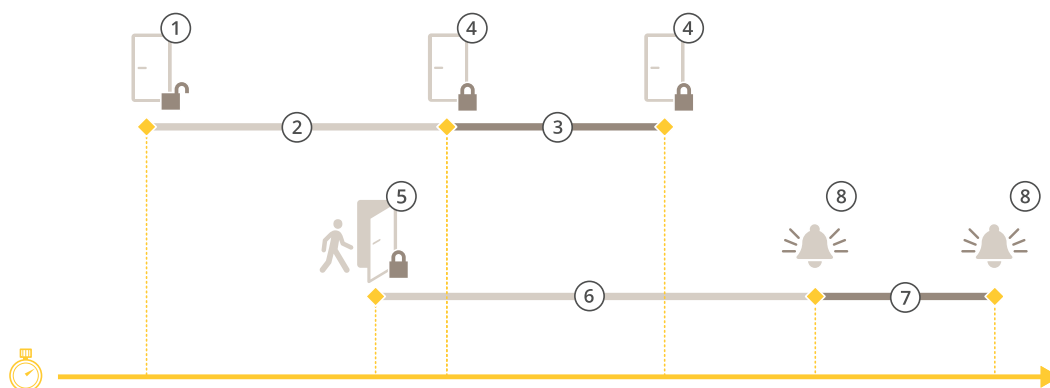
Acțiune de urgență	
Deblocați ușa	Ușa se deblochează atunci când primește semnalul de stare de urgență.
Blocați ușa	Ușa se blochează atunci când primește semnalul de stare de urgență.

Opțiuni de timp



- 1 Acces acordat - încuietoarea se deblochează
- 2 Timp de acces

- 3 Nu s-a întreprins nicio acțiune – încuietoarea rămâne blocată
- 4 Acțiune întreprinsă (ușă deschisă) – încuietoarea se blochează sau rămâne deblocată până la închiderea ușii
- 5 Timp de deschidere prea lung
- 6 Alarma "Open-too-long" (deschis prea mult timp) se declanșează



- 1 Acces acordat – încuietoarea se deblochează
- 2 Timp de acces
- 3 2+3: Timp de acces lung
- 4 Nu s-a întreprins nicio acțiune – încuietoarea rămâne blocată
- 5 Acțiune întreprinsă (ușă deschisă) – încuietoarea se blochează sau rămâne deblocată până la închiderea ușii
- 6 Timp de deschidere prea lung
- 7 6+7: Timp lung de deschidere prea lung
- 8 Alarma "Open-too-long" (deschis prea mult timp) se declanșează

Adăugați un cititor

Puteți configura un controler de ușă pentru a accepta mai multe cititoare cablate. Alegeți pentru a adăuga un cititor pe o parte sau pe ambele părți ale unei uși.

Dacă aplicați o configurație personalizată a formatelor cardurilor sau a lungimii PIN-ului la un cititor, ea apare în Card formats (Formate card) la Configuration (Configurație) > Access control (Control de acces) > Doors and zones (Uși și zone). Consultați Uși și zone, on page 4.

note

- De asemenea, puteți adăuga până la 16 cititoare Bluetooth la un controler de ușă. Pentru mai multe informații, consultați Adăugarea unui cititor Bluetooth, on page 17.
 - Dacă utilizați un interfon de rețea Axis ca un cititor IP, sistemul utilizează configurația PIN stabilită pe pagina web a dispozitivului.
1. Accesați pagina de configurare a ușii. Consultați Adăugați o ușă, on page 7.
 2. Sub o parte a ușii, faceți clic pe Add (Adăugare).
 3. Selectați Card reader (Cititor de carduri).
 4. Selectați Reader type (Tip de cititor).
 5. Pentru a utiliza o lungime PIN personalizată pentru acest cititor.
 - 5.1. Faceți clic pe Advanced (Avansat).
 - 5.2. Porniți Custom PIN length (Lungimea personalizată a PIN-ului).
 - 5.3. Setati Min PIN length (Lungimea minimă a PIN-ului), Max PIN length (Lungimea maximă a PIN-ului), și End of PIN character (Caracterul de sfârșit al PIN-ului).
 6. Pentru a utiliza un format de card personalizat pentru acest cititor:
 - 6.1. Faceți clic pe Advanced (Avansat).
 - 6.2. Porniți Custom card formats (Formate personalizate ale cardurilor).

- 6.3. Selectați formatele de card pe care doriți să le utilizați pentru cititor. Dacă un format de card cu aceeași lungime de biți este deja utilizat, trebuie mai întâi să îl dezactivați. O pictogramă de avertizare apare în client atunci când configurarea formatului cardului este diferită de configurația configurată a sistemului.

7. Faceți clic pe **Add (Adăugare)**.

8. Pentru a adăuga un cititor pe cealaltă parte a ușii, repetați această procedură.

Pentru informații despre modul de instalare a unui AXIS Barcode Reader (cititor de coduri de bare AXIS), consultați *Instalați AXIS Barcode Reader, on page 22*.

Tip de cititor	
OSDP RS485 half-duplex	Pentru cititoarele RS485, selectați OSDP RS485 half-duplex și un port cititor.
Wiegand	Pentru cititoarele care utilizează protocoale Wiegand, selectați Wiegand și un port pentru cititor.
Cititor IP	Pentru cititoarele IP, selectați IP reader (Cititor IP) și selectați un dispozitiv din meniul vertical. Puteți utiliza interfoanele de rețea Axis ca cititoare IP.

Wiegand	
Control LED	Selectați Single wire (Cablul simplu) sau Dual wire (R/G) (Cablul dublu (R/G)) . Cititoarele cu control dual LED utilizează fire diferite pentru LED-urile roșu și verde.
Alertă de modificare neautorizată	Selectați starea circuitului care activează intrarea de detecție a modificării neautorizate a cititorului. • Open circuit (Circuit deschis): Cititorul trimite la ușă semnalul de modificare neautorizată atunci când circuitul este deschis. • Closed circuit (Circuit închis): Cititorul trimite la ușă semnalul de modificare neautorizată atunci când circuitul este închis.
Timp de reținere a modificării neautorizate	Pentru a ignora modificările de stare ale intrării cu modificare neautorizată a cititorului înainte ca acesta să intre într-o nouă stare stabilă, setați un Tamper debounce time (Timp de reținere modificare neautorizată) .
Intrare supravegheată	Porniți pentru a declanșa un eveniment atunci când există o întrerupere în conexiunea dintre controlerul ușii și cititor. Consultați <i>Intrări supravegheate, on page 13</i> .

Adăugare un dispozitiv REX

Puteți adăuga un dispozitiv de solicitare a ieșirii (REX) pe o parte sau pe ambele părți ale ușii. Un dispozitiv REX (Solicitare de părăsire) poate fi un senzor PIR (Infraroșu pasiv), un buton REX sau o bară de apăsare.

1. Accesați pagina de configurare a ușii. Consultați *Adăugați o ușă, on page 7*.
2. Sub o parte a ușii, faceți clic pe **Add (Adăugare)**.
3. Selectați **REX device (Dispozitiv REX)**.

4. Selectați portul I/O la care doriți să conectați dispozitivul REX. Dacă este disponibil un singur port, acesta este selectat automat.
5. Selectați ce **Action (Acțiune)** să declanșeze atunci când ușa primește semnalul REX.
6. Sub **REX active (REX activ)**, selectați conexiunea circuitului de monitorizare a ușii.
7. Pentru a ignora modificările de stare ale intrării digitale înainte ca aceasta să intre într-o nouă stare stabilă, setați un **Debounce time (ms) (Timp de reținere (ms))**.
8. Pentru a declanșa un eveniment atunci când conexiunea dintre controlerul ușii și dispozitivul REX este întreruptă, activați **Supervised input (Intrare supravegheată)**. Consultați *Intrări supravegheate, on page 13*.

Acțiune	
Deblocați ușa	Selectați pentru a debloca ușa atunci când primește semnalul REX.
None (Niciuna)	Selectați această opțiune pentru a nu declanșa nicio acțiune atunci când ușa primește semnalul REX.

REX activ	
Circuitul este deschis	Selectați dacă circuitul REX este normal închis. Dispozitivul REX trimite semnalul atunci când circuitul este deschis.
Circuitul este închis	Selectați dacă circuitul REX este normal deschis. Dispozitivul REX trimite semnalul atunci când circuitul este închis.

Adăugați un cititor IP

Puteți folosi un interfon de rețea Axis sau un alt dispozitiv compatibil IP ca cititor. Înainte de a-l putea atribui unei uși, trebuie să adăugați dispozitivul în AXIS Camera Station Pro.

note

Asigurați-vă că cititorul IP este pornit și conectat la aceeași rețea ca și AXIS Camera Station Pro înainte de a începe.

1. Accesați **Configuration (Configurație) > Devices (Dispozitive) > Add devices (Adăugare dispozitive)**.
2. Selectați cititorul IP din lista dispozitivelor detectate și faceți clic pe **Add (Adăugați)**.
3. Introduceți informațiile de conectare ale dispozitivului când vi se solicită acest lucru.

După ce dispozitivul a fost adăugat, îl puteți alocă unei uși. Consultați *Adăugați un cititor, on page 15*.

Adăugarea unui cititor Bluetooth

Puteți utiliza AXIS A4612 Network Bluetooth Reader pentru a extinde limitele de funcționare prin cablu ale controlerelor de ușa Axis. La fiecare controler de ușa pot fi alocate până la 16 astfel de cititoare. Fiecare cititor poate gestiona încuietoearea ușii, cererea de ieșire (REX) și comutatorul de poziție a ușii (DPS).

Adăugarea și utilizarea acestor cititoare nu necesită nicio licență suplimentară.

Pentru a adăuga un AXIS A4612 Network Bluetooth Reader la o ușă:

1. Asigurați-vă că ați asociat AXIS A4612 cu controlerul ușii. Consultați *Utilizați aplicația AXIS Mobile Credential ca informații de conectare prin Bluetooth, on page 18*.
2. Accesați pagina de configurare a ușii. Consultați *Adăugați o ușă, on page 7*.
3. Sub o parte a ușii, faceți clic pe **+ Add (Adăugați)**, apoi pe **Card reader (Cititor de carduri)**.
4. Selectați **IP reader (Cititor IP)** și alegeți AXIS A4612 asociat din meniul derulant. Dacă acest cititor este utilizat pentru asocierea informațiilor de conectare, marcați-l pentru asociere. Faceți clic pe **Add (Adăugare)**.

5. În fila **Overview (Prezentare generală)**, modificați profilul de identificare. Puteți utiliza profilurile **Tap in app (Atingere în aplicație)** sau **Touch reader (Cititor tactil)** dacă aveți AXIS A4612 atașat doar pe o parte a ușii și utilizați un REX pe cealaltă parte.

Utilizați aplicația **AXIS Mobile Credential** ca informații de conectare prin Bluetooth

Acest exemplu arată cum se adaugă un cititor Bluetooth AXIS A4612 la sistemul dvs. pentru a permite titularilor de card să deblocheze ușile utilizând aplicația **AXIS Mobile Credential**.

1. Instalați cititorul Bluetooth și conectați-l la un controler de ușă.
2. Adăugați cititorul Bluetooth în interfața web a dispozitivului de control al ușii.
 - 2.1. Accesați controlerul ușii și accesați **Peripherals (Periferice) > Readers (Cititoare)**.
 - 2.2. Faceți clic pe **Add reader (Adăugați un cititor)**.
 - 2.3. Introduceți informațiile necesare în fereastra de dialog **Add Bluetooth reader (Adăugare Bluetooth reader)**.
 - 2.4. Faceți clic pe **Add (Adăugare)**.
3. Adăugați cititorul Bluetooth la o ușă în **AXIS Camera Station Pro Secure Entry**.
 - 3.1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Doors and zones (Uși și zone)**.
 - 3.2. Selectați ușa la care doriți să adăugați cititorul Bluetooth și faceți clic pe **Edit (Editare)**.
 - 3.3. Faceți clic pe **+ Add (Adăugare)** pe partea ușii pe care se află cititorul Bluetooth.
 - 3.4. Selectați **Card reader (Cititor de carduri)**.
 - 3.5. La **Add IP reader (Adăugați cititorul IP)**, selectați **IP reader (Cititor IP)**.
 - 3.6. La **Select IP reader (Selectați cititorul IP)**, selectați cititorul Bluetooth.
 - 3.7. Faceți clic pe **Add (Adăugare)**.
4. Selectați un cititor Bluetooth pentru asociere. Trebuie să faceți acest lucru pentru cel puțin un cititor Bluetooth din sistemul dvs.
 - 4.1. Selectați cititorul Bluetooth pe care tocmai l-ați adăugat.
 - 4.2. Faceți clic pe **Edit (Editare)**.
 - 4.3. La **Edit bluetooth reader (Editare cititor Bluetooth)**, selectați **Use this reader for pairing (Utilizează acest cititor pentru asociere)**.
 - 4.4. Faceți clic pe **Apply (Aplicare)**.
5. Alegeți profilul de identificare **Tap in app (Apăsări în aplicație)** sau **Touch reader (Cititor atingeri)**. Pentru mai multe informații, consultați *Profiluri de identificare, on page 20*.
6. Adăugați informațiile de conectare prin dispozitive mobile la titularul de card. Consultați *Adăugați informații de conectare, on page 30*.
7. Asociați informațiile de conectare prin dispozitive mobile cu cititorul de asociere:
 - 7.1. Aduceți telefonul mobil al titularului de card la cititorul Bluetooth cu care va fi asociat.
 - 7.2. Urmați instrucțiunile furnizate în e-mailul trimis titularului de card.

Zone

Adăugare o zonă

O zonă este un spațiu fizic specific cu un grup de uși. Aveți posibilitatea să creați zone și să adăugați uși la zone. Există două tipuri de uși:

- **Perimeter door (Ușă perimetrală):** Titularii de carduri intră sau ies din zonă prin această ușă.
- **Internal door (Ușă internă):** O ușă interioară în interiorul zonei.

note

O ușă perimetrală poate aparține la două zone. O ușă interioară poate aparține unei singure zone. Consultați *Exemplu de uși și zone, on page 5* pentru o prezentare generală.

1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Doors and zones (Uși și zone) > Zones (Zone)**.
2. Faceți clic pe  **Add zone (Adăugare zonă)**.
3. Introduceți un nume de zonă.
4. Faceți clic pe **Add door (Adăugare ușă)**.
5. Selectați ușile pe care doriți să le adăugați la zonă și faceți clic pe **Add (Adăugare)**.
6. Ușa este setată implicit ca o ușă perimetrală. Pentru a-l schimba, selectați **Internal door (Ușă interioară)** din meniul vertical.
7. O ușă perimetrală utilizează implicit partea A a ușii ca parte de intrare în zonă. Pentru a-l schimba, selectați **Leave (Părăsire)** din meniul vertical.
8. Pentru a elimina o ușă din zonă, selectați-o și faceți clic pe **Remove (Eliminare)**.
9. Faceți clic pe **Save (Salvare)**.

Pentru a edita o zonă:

1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Doors and zones (Uși și zone) > Zones (Zone)**.
2. Selectați o zonă din listă.
3. Faceți clic pe  **Edit (Editare)**.
4. Modificați setările și faceți clic pe **Save (Salvare)**.

Pentru a îndepărta o zonă:

1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Doors and zones (Uși și zone) > Zones (Zone)**.
2. Selectați o zonă din listă.
3. Faceți clic pe  **Remove (Eliminare)**.
4. Faceți clic pe **Yes (Da)**.

Nivelul de securitate al zonei

Puteți adăuga următoarea funcție de securitate la o zonă:

Anti-passback (Trecere nepermisă) – Previne utilizarea de către persoane a acelorași informații de conectare ca și cele ale unei persoane care a intrat într-o zonă înaintea lor. O persoană trebuie să părăsească zona înainte de a-și folosi din nou informațiile de conectare.

note

- Cu Trecere nepermisă, toate ușile din zonă trebuie să aibă senzori de poziție a ușii, astfel încât sistemul să poată înregistra faptul că un utilizator a deschis ușa după ce și-a glisat cardul.
- Dacă un controler de ușă este offline, Trecere nepermisă funcționează atâta timp cât toate ușile din zonă aparțin acelui controler de ușă. Însă dacă ușile din zonă aparțin unor controlere de ușă diferite care trec pe offline, Trecere nepermisă nu mai funcționează.

Puteți configura nivelul de securitate în timp ce adăugați o zonă nouă sau îl puteți aplica la o zonă existentă. Pentru a adăuga un nivel de securitate la o zonă existentă:

1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Doors and zones (Uși și zone)**.
2. Selectați zona pentru care doriți să configurați un nivel de securitate.
3. Faceți clic pe **Edit (Editare)**.
4. Faceți clic pe **Security level (Nivel de securitate)**.
5. Activați funcțiile de securitate pe care doriți să le adăugați la zonă.

6. Faceți clic pe **Apply (Aplicare)**.

Anti-passback (Trecere nepermisă)	
Log violation only (Soft) (Numai încălcarea înregistrării (fin))	Selectați această opțiune pentru a permite unei a doua persoane să intre folosind aceleași informații de conectare ca și prima persoană. Această opțiune are ca rezultat doar o alarmă de sistem.
Deny access (Hard) (Interzicerea accesului (dur))	Selectați această opțiune pentru a împiedica accesul unei a doua persoane în cazul în care aceasta utilizează aceleași informații de conectare ca și prima persoană. Această opțiune are, de asemenea, ca rezultat o alarmă de sistem.
Timeout (seconds) (Expirarea timpului (secunde))	Perioada de timp până când sistemul permite unui utilizator să intre din nou. Introduceți 0 pentru a dezactiva timpul de expirare, ceea ce înseamnă că mecanismul anti-passback se aplică până când utilizatorul părăsește zona. Utilizați expirarea timpului 0 numai împreună cu Deny access (Hard) (Interzicerea accesului (dur)) dacă toate ușile din zonă au cititoare pe ambele părți.

Profiluri de identificare

Un profil de identificare este o combinație de tipuri de identificare și programe. Puteți aplica un profil de identificare uneia sau mai multor uși pentru a stabili cum și când un titular de card poate accesa o ușă.

note

Trebuie să utilizați QR dinamic și PIN împreună.

Accesați **Configuration (Configurație) > Access control (Controlul de acces) > Identification profiles (Profiluri de identificare)** pentru a crea, edita sau elimina profiluri de identificare.

Profilurile de identificare disponibile:

Card – Titularii de carduri trebuie să gliseze cardul pentru a accesa ușa.

Cardurile și PIN-ul – Titularii de carduri trebuie să gliseze cardul și să introducă PIN-ul pentru a accesa ușa.

PIN – Titularii de carduri trebuie să introducă PIN-ul pentru a accesa ușa.

Card sau PIN – Titularii de carduri trebuie să gliseze cardul sau să introducă PIN-ul pentru a accesa ușa.

QR – Titularii de carduri trebuie să arate camerei codul QR Code® pentru a accesa ușa. Puteți utiliza profilul de identificare QR atât pentru QR static, cât și pentru QR dinamic.

Plăcuță de înmatriculare – Titularii de carduri trebuie să se îndrepte spre cameră într-un vehicul cu o plăcuță de înmatriculare aprobată.

Atingeți în aplicație – Titularii de carduri trebuie să atingă în aplicația mobilă AXIS Camera Station informațiile de conectare în timp ce se află în raza de acțiune a cititorului Bluetooth.

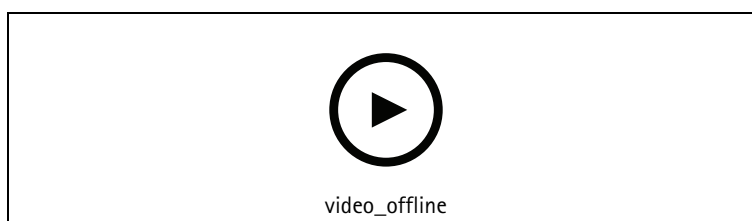
Cititor tactil – Titularii de carduri trebuie să atingă cititorul Bluetooth în timp ce au asupra lor un telefon mobil cu informații de conectare prin dispozitive mobile.

*QR Code este o marcă înregistrată a Denso Wave Incorporated în Japonia și în alte țări.

Crearea unui profil de identificare

1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Identification profiles (Profiluri de identificare)**.
2. Faceți clic pe **+** **Create identification profile (Creați un profil de identificare)**.
3. Introduceți un nume pentru profilul de identificare.

4. Selectați **Include facility code for card validation** (Includeți codul instituției pentru validarea cardului) pentru a utiliza codul instituției ca unul dintre câmpurile de validare ale informațiilor de conectare. Acest câmp este disponibil numai dacă activați **Facility code** (Codul instalației) sub **Access management** (Gestionare acces) > **Settings** (Setări).
5. Pentru Partea A, faceți clic pe **+ Add (Adăugați)**, selectați un tip de identificare și un program.
 - Pentru a impune titularilor de card să utilizeze mai multe tipuri de identificare, selectați mai multe tipuri din același rând.
 - Pentru a permite titularilor de card să utilizeze ambele tipuri, faceți din nou clic pe **+ Add (Adăugați)** și adăugați încă un rând.
6. Pentru Partea B, faceți clic pe **+ Add (Adăugați)**, selectați un tip de identificare și un program.
7. Faceți clic pe **OK**.



Configurarea profilurilor de identificare

Editarea unui profil de identificare

1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Identification profiles (Profiluri de identificare)**.
2. Selectați un profil de identificare și faceți clic pe .
3. Pentru a schimba numele profilului de identificare, introduceți un nume nou.
4. Faceți editările pe partea laterală a ușii.
5. Pentru a edita profilul de identificare de pe cealaltă parte a ușii, efectuați din nou pașii anteriori.
6. Faceți clic pe **OK**.

Editarea profilului de identificare	
	Pentru a elimina un tip de identificare și programul aferent.
Tip de identificare	Pentru a schimba un tip de identificare, selectați unul sau mai multe tipuri din meniul vertical Identification type (Tip de identificare) .
Programare	Pentru a modifica un program, selectați unul sau mai multe programe din meniul vertical Schedule (Program) .
+ Adăugare	Adăugați un tip de identificare și programul aferent, faceți clic pe Add (Adăugare) și setați tipurile de identificare și programele.

Eliminarea unui profil de identificare

1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Identification profiles (Profiluri de identificare)**.
2. Selectați un profil de identificare și faceți clic pe .
3. Dacă profilul de identificare este utilizat pe o ușă, selectați un alt profil de identificare pentru ușă.

4. Faceți clic pe OK.

Resetarea unui format de card predefinit

1. Accesați **Configuration (Configurație) > Access Control (Control de acces) > Card formats and PIN (Formate de card și PIN)**.

2. Faceți clic pe pentru a reseta un format de card la harta de câmp implicită.

Cititorul de coduri de bare AXIS

Cititorul de coduri de bare AXIS este o aplicație care poate fi instalată în camerele Axis. Controlerul de ușă Axis utilizează cheia de autentificare a dispozitivelor periferice externe pentru a acorda accesul și a autentifica cititorul de coduri de bare AXIS și AXIS License Plate Verifier. Pentru un flux de lucru complet pentru configurarea AXIS License Plate Verifier în AXIS Camera Station Pro, consultați .

Instalați AXIS Barcode Reader

1. Descărcați fișierul de instalare a aplicației de la axis.com.
2. Accesați pagina web a interfonului sau a camerei Axis.
3. Instalați aplicația.
4. Activați licența.
5. Porniți aplicația.
6. Pentru o mai bună precizie QR, vă recomandăm să modificați următoarele setări ale camerei.
 - 6.1. Accesați setările camerei.
 - 6.2. La **Image (Imagine) > Exposure (Expunere)**, deplasați la mijloc cursorul **Blur-noise trade-off (Compromis neclaritate-zgomot)**.

Configurați AXIS Barcode Reader

1. Pentru a schimba profilul de identificare QR, accesați **Configuration (Configurație) > Access control (Control de acces) > Identification profiles (Profiluri de identificare)** și faceți clic pe  . Consultați *Identification profiles (Profiluri de identificare)*.
2. Adăugați o ușă. Consultați *Add a door (Adăugați o ușă)*.
3. Selectați **QR** ca profil de identificare pentru această ușă. Consultați *Door settings (Setările ușii)*.
4. Adăugați un cititor de coduri de bare. Consultați *Add a reader (Adăugați un cititor)*.
 - 4.1. Sub o parte a ușii, faceți clic pe **Add reader (Adăugați un cititor)**.
 - 4.2. Selectați **AXIS Barcode Reader** din lista verticală **Reader type (Tip de cititor)**. Introduceți un nume și faceți clic pe **OK**.

Creați o conexiune cu controlerul ușii

1. În AXIS Camera Station Pro Secure Entry:
 - 1.1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Encrypted communication (Comunicație criptată)**.
 - 1.2. La **External Peripheral Authentication Key (Cheie de autentificare periferie externă)**, faceți clic pe **Show authentication key (Afișați cheia de autentificare)** și **Copy key (Copiați cheia)**.
2. În interfața web a dispozitivului în care rulează Cititorul de coduri de bare AXIS:
 - 2.1. Deschideți aplicația Cititorul de coduri de bare AXIS.
 - 2.2. Dacă certificatul serverului nu a fost configurat în AXIS Camera Station Pro Secure Entry, activați **Ignore server certificate validation (Ignorarea validării certificatului serverului)**. Pentru mai multe informații, consultați secțiunea *Certificates (Certificate)*.
 - 2.3. Activați **AXIS Camera Station Secure Entry**.
 - 2.4. Faceți clic pe **Add (Adăugare)** și introduceți adresa IP a controlerului de ușă și lipiți cheia de autentificare.
 - 2.5. Selectați cititorul care citește codurile de bare din meniul vertical al ușilor.

Formatele cardurilor și PIN-ul

Un format de card definește modul în care un cititor de carduri interpretează datele de pe un card. Există formate de card predefinite pe care le puteți utiliza sau edita, iar, de asemenea, puteți crea formate de card personalizate

Accesați **Configuration (Configurație) > Access Control (Control de acces) > Card formats and PIN (Formate de card și PIN)**. Pagina conține două file:

Configurare PIN – Setează lungimea codului PIN și caracterul care marchează sfârșitul acestuia.

Formatele cardurilor – Vedere, creați, editați, ștergeți și activați formatele de card.

Formatele cardurilor

Tabelul prezintă toate formatele de carduri disponibile, împreună cu următoarele informații:

În uz	Dacă formatul este activ. În același timp poate fi activ doar un singur format per lungime de bit.
Denumire format card	Denumirea formatului de card.
Lungimea bitului	Lungimea în biți a formatului cardului.
Origine	Indiferent dacă este vorba de un format implicit al sistemului sau de un format personalizat pe care l-ați creat.

Adăugați un format de card

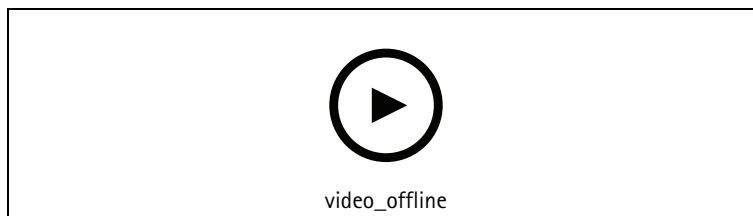
1. Accesați **Configuration (Configurație) > Access Control (Control de acces) > Card formats and PIN (Formate de card și PIN)**.
2. Faceți clic pe **+ Add (Adăugare)**.
3. Introduceți un nume și o lungime de biți cuprinsă între 1 și 256.
4. Selectați **Invert bit order (Inversare ordine biți)** dacă doriți să inversați ordinea biților din datele primite de la cititorul de carduri.
5. Selectați **Invert byte order (Inversare ordine octeți)** dacă doriți să inversați ordinea octeților din datele primite de la cititorul de carduri. Această opțiune este disponibilă numai atunci când specificați o lungime de bit pe care o puteți împărți la opt.
6. Activați **Card number (Număr card)**, **Facility code (Cod facilitate)** sau ambele. Cel puțin unul dintre ele trebuie să fie activ în formatul de card.
7. Setează intervalul de biți al datelor pentru câmpul de date. Intervalul trebuie să se încadreze în ceea ce ați specificat pentru Bit length (Lungimea bitului).
8. Selectați formatul de ieșire a datelor pentru câmpul de date.
 - Decimal (Zecimal): Sistemul numeric în baza 10. Se folosesc cifrele de la 0 la 9.
 - Hexazecimal: Sistemul numeric în baza 16. Utilizează 16 simboluri: cifrele de la 0 la 9 și literele de la a la f.
9. Selectați ordinea biților.
 - Little endian (Endian mic): Primul bit este cel mai mic sau cel mai puțin semnificativ.
 - Big endian (Endian mare): Primul bit este cel mai mare sau cel mai semnificativ.
10. Faceți clic pe **OK**.

note

- Două formate de carduri cu aceeași lungime de bit nu pot fi active în același timp. De exemplu, dacă ați

definit două formate de card pe 32 de biți, numai unul dintre acestea poate fi activ. Dezactivați formatul cardului pentru a-l activa pe celălalt.

- Aveți posibilitatea să activați și să dezactivați formatele cardurilor numai dacă controlerul de ușă a fost configurat cu cel puțin un cititor.
- Puteți edita formatele de carduri predefinite, dar nu le puteți șterge. Pentru a anula modificările aduse unui format predefinit, selectați pictograma de resetare pentru a-l restabili la setările implicite. Puteți șterge formatele de carduri pe care le-ați creat.



Configurați formatele cardurilor

Editarea unui format de card

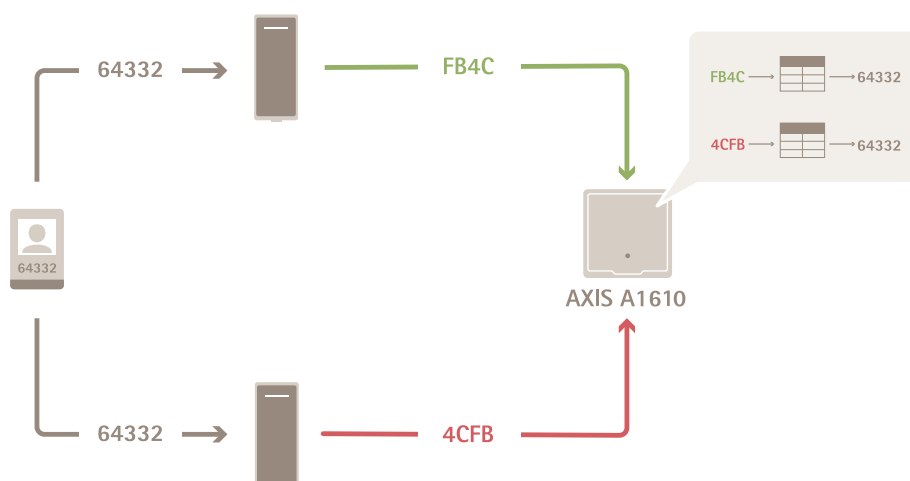
1. Accesați **Configuration (Configurație) > Access Control (Control de acces) > Card formats and PIN (Formate de card și PIN)**.
2. Selectați un format de card și faceți clic pe .
3. Dacă editați un format de card predefinit, puteți edita numai **Invert bit order (Inversare ordine biți)** și **Invert byte order (Inversare ordine octeți)**.
4. Faceți clic pe **OK**.

Puteți elimina doar formatele de carduri personalizate. Pentru a elimina un format de card personalizat:

1. Accesați **Configuration (Configurație) > Access Control (Control de acces) > Card formats and PIN (Formate de card și PIN)**.
2. Selectați un format de card personalizat, faceți clic pe  și **Yes (Da)**.

Setări format card

Prezentare generală



- Numărul cardului în formă zecimală este 64332.
- Un cititor transferă numărul cardului la numărul hexazecimal FB4C. Celălalt cititor îl transferă la numărul hexazecimal 4CFB.

- AXIS A1610 Network Door Controller primește numărul FB4C și îl transferă la numărul zecimal 64332 în conformitate cu setările de format al cardului de pe cititor.
- AXIS A1610 Network Door Controller primește numărul 4CFB, îl modifică în FB4C prin inversarea ordinii biților, și îl transferă la numărul zecimal 64332 în conformitate cu setările de format al cardului de pe cititor.

Inversarea ordinii biților

După inversarea ordinii biților, datele cardului primite de la cititor sunt citite de la dreapta la stânga, bit cu bit.

$$64332 = 1111\ 1011\ 0100\ 1100 \longrightarrow 0011\ 0010\ 1101\ 1111 = 13023$$

$\longrightarrow$ Read from left Read from right $\longleftarrow$

Inversare ordine octeți

Un grup de opt biți este un octet. După inversarea ordinii octeților, datele cardului primite de la cititor sunt citite de la dreapta la stânga, octet cu octet.

$$64\ 332 = \begin{matrix} 1111 & 1011 & 0100 & 1100 \\ \text{F} & \text{B} & 4 & \text{C} \end{matrix} \longrightarrow \begin{matrix} 0100 & 1100 & 1111 & 1011 \\ 4 & \text{C} & \text{F} & \text{B} \end{matrix} = 19707$$

Format card Wiegand standard pe 26 de biți



- 1 Paritate de conducere
- 2 Codul instalației
- 3 Numărul cardului
- 4 Paritate de urmărire

PIN

Setați lungimea minimă și maximă a codului PIN. Dacă setați valori diferite pentru minim și maxim, definiți un caracter de încheiere a codului PIN pentru a indica faptul că introducerea codului PIN s-a încheiat.

1. Accesați **Configuration (Configurație) > Access Control (Control de acces) > Card formats and PIN (Formate de card și PIN) > PIN configuration (Configurație PIN)**.
2. Introduceți **Min PIN length (Lungimea minimă a codului PIN)** și **Max PIN length (Lungimea maximă a codului PIN)**.
3. Dacă este necesar, introduceți un **End of PIN character (caracter de încheiere a codului PIN)**.
4. Faceți clic pe **OK**.

Comunicație criptată

Canal Securizat OSDP

AXIS Camera Station Secure Entry acceptă Canal Securizat OSDP (Protocol Deschis Dispozitiv Supravegheat) pentru criptarea activă a liniei între controler și cititoarele Axis.

Pentru a activa Canal Securizat OSDP pentru un sistem complet:

1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Encrypted communication (Comunicație criptată)**.
2. Introduceți cheia dvs. de criptare principală și faceți clic pe **OK**.

3. Activați **OSDP Secure Channel (Canal Securizat OSDP)**. Această opțiune este disponibilă numai după ce ați introdus cheia de criptare principală.
4. În mod implicit, cheia de criptare principală generează o cheie pentru Canal Securizat OSDP. Pentru a seta manual cheia Canalului Securizat OSDP:
 - 4.1. La **OSDP Secure Channel (Canal Securizat OSDP)**, faceți clic pe .
 - 4.2. Ștergeți **Use main encryption key to generate OSDP Secure Channel key (Utilizați cheia de criptare principală pentru a genera cheia pentru Canal Securizat OSDP)**.
 - 4.3. Introduceți cheia pentru Canal Securizat OSDP și faceți clic pe **OK**.

Pentru a activa sau a dezactiva Canal Securizat OSDP pentru un anumit cititor, consultați *Doors and zones (Uși și zone)*.

Multi-server^{BETA}

Serverele secundare conectate pot utiliza, în cazul serverelor multiple, titularii de card și grupurile de titulari de card globale de la serverul principal.

note

- Un sistem poate accepta până la 64 de servere secundare.
- El necesită AXIS Camera Station 5.47 sau o versiune ulterioară.
- Este necesar ca serverul principal și serverele secundare să fie în aceeași rețea.
- Pe serverul principal și pe serverele secundare, asigurați-vă că configurați Windows Firewall pentru a permite conexiunile TCP de intrare pe portul Secure Entry. Portul implicit este 55767. Pentru configurația personalizată a porturilor, consultați *Setări generale ale serverului*.
- Conectarea unui server secundar la un server principal duce la înlocuirea cheii sale de citire, ceea ce face ca toate informațiile de conectare Bluetooth existente să devină nevalide. Pentru a evita acest lucru, creați informații de conectare Bluetooth pe serverul principal, nu pe serverul secundar.

Fluxul de lucru

1. Configurați un server ca server secundar și generați fișierul de configurare. Consultați *Generarea fișierului de configurare de pe serverul secundar, on page 26*.
2. Configurați un server ca server principal și importați fișierul de configurare al serverelor secundare. Consultați *Importarea fișierului de configurare pe serverul principal, on page 26*.
3. Configurați titularii de card și grupurile de titulari de card globale pe serverul principal. Consultați *Adăugați un titular de card, on page 29* și *Adăugați un grup, on page 33*.
4. Afișați și monitorizați titularii de card și grupurile de titulari de card globale de pe serverul secundar. Consultați *Access management (Gestionare acces), on page 29*.

Generarea fișierului de configurare de pe serverul secundar

1. De pe serverul secundar, mergeți la **Configuration (Configurare) > Access control (Control de acces) > Multi server (Multi-server)**.
2. Faceți clic pe **Sub server (Server secundar)**.
3. Faceți clic pe **Generate (Generare)**. El generează un fișier de configurare în format .json.
4. Faceți clic pe **Download (Descărcare)** și alegeți o locație pentru a salva fișierul.

Importarea fișierului de configurare pe serverul principal

1. De pe serverul principal, accesați **Configuration (Configurație) > Access control (Control de acces) > Multi server (Multi-server)**.
2. Faceți clic pe **Main server (Server principal)**.
3. Faceți clic pe **+ Add (Adăugare)** și accesați fișierul de configurare generat de serverul secundar.
4. Introduceți numele serverului, adresa IP și numărul portului serverului secundar.
5. Faceți clic pe **Import (Importare)** pentru a adăuga serverul secundar.
6. Starea serverului secundar indică **Connected**.

Revocarea unui server secundar

Puteți revoca un server secundar numai înainte de a importa fișierul său de configurare pe un server principal.

1. De pe serverul principal, accesați **Configuration (Configurație) > Access control (Control de acces) > Multi server (Multi-server)**.
2. Faceți clic pe **Sub server (Server secundar)** și faceți clic pe **Revoke server (Revocați serverul)**.
Acum puteți configura acest server ca server principal sau server secundar.

Eliminarea unui server secundar

După ce ați importat fișierul de configurare al unui server secundar, acesta conectează serverul secundar la serverul principal.

Pentru a elimina un server secundar:

1. De pe serverul principal:
 - 1.1. Accesați **Access management (Gestionarea accesului) > Dashboard (Tabloul de bord)**.
 - 1.2. Schimbați titularii de card și grupurile globale în titulari de card și grupuri locale.
 - 1.3. Accesați **Configuration (Configurație) > Access control (Control de acces) > Multi server (Multi-server)**.
 - 1.4. Faceți clic pe **Main server (Server principal)** pentru a afișa lista de servere secundare.
 - 1.5. Selectați serverul secundar și faceți clic pe **Delete (Ștergere)**.
2. De pe serverul secundar:
 - Accesați **Configuration (Configurație) > Access control (Control de acces) > Multi server (Multi-server)**.
 - Faceți clic pe **Sub server (Server secundar)** și pe **Revoke server (Revocați serverul)**.

Setări Active Directory^{BETA}

note

Conturile de utilizator din Microsoft Windows și utilizatorii și grupurile Active Directory pot accesa AXIS Camera Station Pro Secure Entry. Modul în care adăugați utilizatori în Windows variază în funcție de versiunea dvs. Pentru mai multe informații, vizitați *support.microsoft.com*. Dacă utilizați o rețea de tip domeniu Active Directory, consultați-vă cu administratorul de rețea.

Prima dată când deschideți pagina de setări Active Directory puteți importa utilizatorii Microsoft Active Directory la titularii de card din AXIS Camera Station Pro Secure Entry. Consultați *Importarea utilizatorilor Active Directory, on page 27*.

După configurația inițială, apar următoarele opțiuni pe pagina de setări Active Directory.

- Creați și gestionați grupuri de titulari de card pe baza grupurilor din Active Directory.
- Configurați sincronizarea programată între Active Directory și sistemul de gestionare a accesului.
- Sincronizați manual pentru a actualiza toți titularii de card importați din Active Directory.
- Gestionați maparea datelor între datele utilizatorilor din Active Directory și proprietățile titularilor de card.

Importarea utilizatorilor Active Directory

Pentru a importa utilizatorii Active Directory la titularii de card din AXIS Camera Station Pro Secure Entry:

1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Active Directory settings (Setări Active Directory)**^{BETA}.
2. Faceți clic pe **Set up import (Configurare import)**.
3. Urmăriți instrucțiunile de pe ecran pentru a finaliza acești trei pași principali:
 - 3.1. Selectați un utilizator din Active Directory pentru a-l utiliza ca șablon pentru maparea datelor.
 - 3.2. Maparea datelor utilizatorilor din baza de date Active Directory la proprietățile titularilor de card.
 - 3.3. Creați un nou grup de titulari de card în sistemul de gestionare a accesului și selectați grupurile Active Directory care urmează să fie importate.

Nu puteți modifica niciuna dintre datele importate ale utilizatorului, dar puteți adăuga informațiile de conectare la un titular de card importat, consultați *Adăugați informații de conectare, on page 30*.

important

Dacă dezactivați un utilizator în Active Directory, AXIS Camera Station Pro șterge definitiv titularul cardului și toate datele asociate, inclusiv istoricul acestuia. Acest lucru este ireversibil. Pentru a bloca accesul unui titular de card fără a-i pierde datele, suspendați-l în AXIS Camera Station Pro în loc să-l dezactivați în Active Directory.

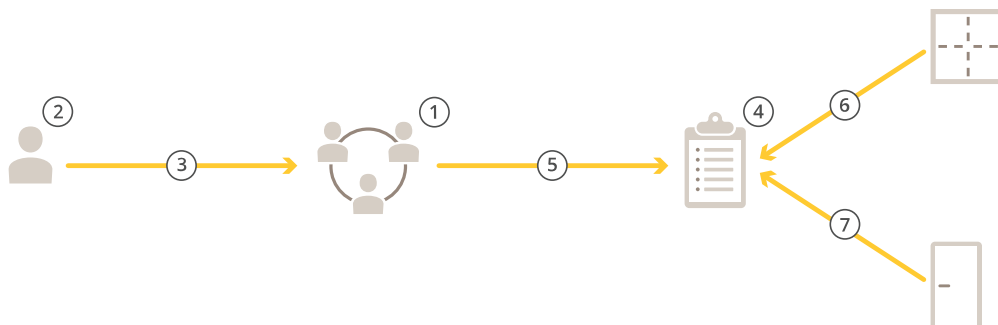
Access management (Gestionare acces)

Utilizați fila **Access management (Gestionarea accesului)** pentru a configura și a gestiona titularii de card, grupurile și regulile de acces ale sistemului.

Pentru un flux de lucru complet pentru configurarea unui controler de ușă de rețea Axis în AXIS Camera Station Pro Secure Entry, consultați *Set up an Axis network door controller (Configurarea unui controler de ușă de rețea Axis)*.

Fluxul de lucru al gestionării accesului

Structura de gestionare a accesului este flexibilă, prin urmare puteți să dezvoltați un flux de lucru care să corespundă nevoilor dumneavoastră. Exemplu de flux de lucru:



1. Adăugați un grup, on page 33.
2. Adăugați un titular de card, on page 29.
3. Adăugați deținători de carduri la grupuri.
4. Adăugați o regulă de acces, on page 33.
5. Aplicați grupuri la regulile de acces.
6. Aplicați zonele la regulile de acces.
7. Aplicați ușile la regulile de acces.

Adăugați un titular de card

Un titular de card este o persoană cu un ID unic înregistrat în sistem. Configurați un titular de card cu informații de conectare care să identifice persoana respectivă și să stabilească când și cum poate aceasta să acceseze ușile.

De asemenea, puteți cartografia utilizatorii dintr-o bază de date Active Directory ca titulari de carduri.

Consultați *Setări Active Directory^{BETA}*, on page 27.

1. Deschideți o  filă de gestionare a accesului.
2. Accesați **Cardholder management (Gestionarea titularilor de card) > Cardholders (Titulari de card)** și faceți clic pe  **Add (Adăugare)**.
3. Introduceți prenumele și numele titularului cardului. Opțional puteți adăuga mai multe detalii despre titularul cardului:
 - La **Email (E-mail)**, introduceți adresa de e-mail a titularului cardului.
 - La **Groups (Grupuri)**, selectați grupurile la care doriți să adăugați titularul cardului.
 - La **Access rules (Reguli de acces)**, selectați regulile de acces pe care doriți să le aplicați titularului cardului.
4. Pentru a adăuga o fotografie, faceți clic pe **Cardholder picture (Fotografia titularului cardului)** și selectați:
 - **Upload (Încărcare)** pentru a adăuga o imagine de pe dispozitivul dvs.
 - **Capture (Fotografiere)** pentru a face o fotografie direct cu camera.

note

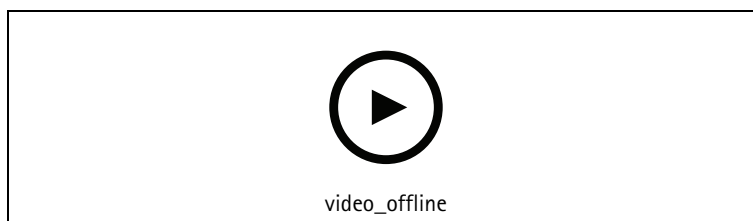
Imaginea trebuie să fie un fișier JPG, PNG sau GIF. Imaginile sunt redimensionate automat la o dimensiune maximă de 700x700 pixeli și convertite în format JPG.

5. Faceți clic pe **Advanced (Avansat)** pentru configura opțiunile suplimentare.

6. Adăugați informații de conectare titularului de card. Consultați *Adăugați informații de conectare*, on page 30.
7. Faceți clic pe **Save (Salvare)**.
8. Pentru a imprima ecusoane, selectați unul sau mai mulți Titulari de carduri și faceți clic pe **Print Badge (Imprimare ecuson)**^{BETA}. Pentru mai multe informații, consultați secțiunea *Print badge (Imprimați ecusonul)*^{BETA}, on page 38.

Folosiți câmpul de căutare pentru a găsi un titular de card după prenume sau nume. Pentru a filtra după sursă, faceți clic pe **Filter (Filtrare)** și selectați **Local**, **Global**, **AD** sau **Center (Centru)**.

Advanced (Avansat)	
Timp de acces lung	Selectați pentru a oferi titularului de card un timp lung de acces și un timp de deschidere prea îndelungat atunci când este instalat un monitor de ușă.
Suspendarea titularului de card	Selectați pentru a suspenda titularul cardului. Aceasta elimină temporar întregul acces de la titularul de card.
Permiteți glisarea dublă	Selectați pentru a permite unui titular de card să anuleze starea curentă a unei uși. De exemplu, titularul de card poate folosi aceasta pentru a debloca o ușă în afara programului obișnuit.
Excepție de la închidere	Selectați această opțiune pentru a acorda titularului de card acces în perioada de încuiere.
Exceptate de la anti-passback	Selectați pentru a acorda unui titular de card o derogare de la regula anti-passback. Anti-passback previne utilizarea de către persoane a acelorași informații de conectare cu cele ale unei persoane care a intrat într-o zonă înaintea lor. Prima persoană trebuie să părăsească zona înainte ca informațiile sale de conectare să poată fi utilizate din nou.
Deținător de card global	Selectați pentru a face posibilă vizualizarea și monitorizarea titularului de card pe serverele secundare. Această opțiune este disponibilă numai pentru titularii de carduri creați pe serverul principal. Consultați <i>Multi-server</i> ^{BETA} , on page 26.



Adăugați deținători de carduri și grupuri

Adăugați informații de conectare

Puteți adăuga următoarele tipuri de informații de conectare la un titular de card:

- *Informații de conectare cu cod QR*, on page 31
- *Informații de conectare cu PIN*, on page 31
- *Informații de conectare cu card*, on page 31
- *Informații de conectare cu plăcuța de înmatriculare*, on page 32

Data expirării	
Valabil de la	Setați o dată și o oră la care devin valabile informațiile de conectare.
Valabil până la	Selectați o opțiune din meniul vertical.

Valabil până la	
Fără dată de încheiere	Informațiile de conectare nu expiră niciodată.
Data ...	Setați o dată și o oră la care expiră informațiile de conectare.
De la prima utilizare	Selectați în cât timp expiră informațiile de conectare după prima utilizare. Selectați zile, luni, ani sau numărul de ori după prima utilizare.
De la ultima utilizare	Selectați în cât timp expiră informațiile de conectare după ultima utilizare. Selectați zile, luni sau ani de la ultima utilizare.

Informații de conectare cu cod QR

note

Utilizarea codurilor QR ca informații de conectare necesită sincronizarea orei pe controlerul de sistem și pe cameră cu cititorul de coduri de bare AXIS. Vă recomandăm să utilizați aceeași sursă de timp pentru ambele dispozitive, pentru a menține sincronizarea orară.

Pentru a adăuga unui titular de card informații de conectare cu cod QR:

1. La **Credentials (Informații de conectare)**, faceți clic pe **+ Add (Adăugare)** și selectați **QR-code (Cod QR)**.
2. Introduceți un nume pentru informațiile de conectare.
3. Dynamic QR (QR dinamic) este activat în mod implicit. Trebuie să îl utilizați împreună cu informații de conectare cu cod PIN.
4. Setați data de începere și de încheiere a informațiilor de conectare.
5. Pentru a trimite automat codul QR prin e-mail după ce ați salvat titularul cardului, selectați **Send QR-code to cardholder when credential is saved (Trimiteți codul QR titularului cardului după salvarea informațiilor de conectare)**.
6. Faceți clic pe **Add (Adăugare)**.

Informații de conectare cu PIN

Pentru a adăuga informații de conectare cu cod PIN unui titular de card:

1. La **Credentials (Informații de conectare)**, faceți clic pe **+ Add (Adăugare)** și selectați **PIN**.
2. Introduceți un PIN.
3. Opțional pentru a declanșa o alarmă silențioasă cu un PIN separat, activați opțiunea **Duress PIN (PIN de urgență)** și introduceți un PIN de urgență.
4. Setați datele pentru informațiile de conectare **Valid from (Valabil din)** și **Valid to (Valabil până în)**.
5. Faceți clic pe **Add (Adăugare)**.

Informațiile de conectare prin dispozitive mobile

note

Titularul cardului trebuie să aibă o adresă de e-mail pentru a primi informațiile de conectare prin dispozitive mobile.

Informații de conectare cu card

Pentru a adăuga informații de conectare cu card unui titular de card:

1. La **Credentials (Informații de conectare)**, faceți clic pe **+ Add (Adăugare)** și selectați **Card**.

2. Pentru a introduce manual datele cardului, furnizați un nume de card, un număr de card și o lungime de bit.

note

Lungimea de biți este configurabilă numai atunci când creați un format de card cu o anumită lungime de biți care nu a fost deja definită în sistem.

3. Pentru a obține automat datele cardului pentru ultimul card introdus:
 - 3.1. Selectați o ușă din meniul vertical **Select reader (Selectare cititor)**.
 - 3.2. Glisați cardul pe cititorul conectat la ușa respectivă.
 - 3.3. Faceți clic pe **Get last swiped card data from the door's readers (Obțineți ultimele date ale cardului glisat de la cititoarele ușii)**.

note

Puteți utiliza un cititor de carduri 2N desktop USB pentru a obține datele cardului. Pentru mai multe informații, consultați *Set up 2N desktop USB card reader (Configurați cititorul de carduri 2N desktop USB)*.

4. Introduceți un cod al instalației. Acest câmp este disponibil numai dacă ați activat **Facility code (Codul instalației)** la **Access management (Gestionare acces) > Settings (Setări)**.
5. Setati data de începere și de încheiere a informațiilor de conectare.
6. Faceți clic pe **Add (Adăugare)**.

Informații de conectare cu plăcuța de înmatriculare

Pentru a adăuga informații de conectare cu plăcuța de înmatriculare la un titular de card:

1. La **Credentials (Informații de conectare)**, faceți clic pe **+ Add (Adăugare)** și selectați **License plate (Plăcuță de înmatriculare)**.
2. Introduceți numele informațiilor de conectare, nume care descrie vehiculul.
3. Introduceți numărul de înmatriculare al vehiculului.
4. Setati data de începere și de încheiere a informațiilor de conectare.
5. Faceți clic pe **Add (Adăugare)**.

Utilizați numărul de înmatriculare ca informații de conectare

Acest exemplu vă arată cum să utilizați un controler de ușă, o cameră cu AXIS License Plate Verifier și numărul de înmatriculare al unui vehicul ca informații de conectare pentru acordarea accesului.

1. Adăugați controlerul ușii și camera la AXIS Camera Station Pro Secure Entry. Consultați *Adăugați dispozitive*.
2. Faceți upgrade la firmware-ul noilor dispozitive la cea mai recentă versiune disponibilă. Consultați *Actualizarea firmware-ului*.
3. Adăugați o ușă nouă conectată la controlerul de uși. Consultați *Adăugați o ușă, on page 7*.
 - 3.1. Adăugați un cititor pe **Side A (Partea A)**. Consultați *Adăugați un cititor, on page 15*.
 - 3.2. La **Door settings (Setări ușă)**, selectați **AXIS License Plate Verifier** ca **Reader type (Tip de cititor)** și introduceți un nume pentru cititor.
 - 3.3. Opțional, adăugați un cititor sau un dispozitiv REX pe **Side B (Partea B)**.
 - 3.4. Faceți clic pe **OK**.
4. Instalați și activați AXIS License Plate Verifier la camera dvs. Consultați manualul de utilizare *AXIS License Plate Verifier*.
5. Porniți AXIS License Plate Verifier.
6. Configurați AXIS License Plate Verifier.
 - 6.1. Accesați **Configuration (Configurație) > Access control (Control de acces) > Encrypted communication (Comunicație criptată)**.
 - 6.2. La **External Peripheral Authentication Key (Cheie de autentificare periferie externă)**, faceți clic pe **Show authentication key (Afișați cheia de autentificare)** și **Copy key (Copiați cheia)**.
 - 6.3. Deschideți AXIS License Plate Verifier prin interfața web a camerei.

- 6.4. Săriți peste expertul de configurare.
- 6.5. Accesați **Settings (Setări)**.
- 6.6. La **Access control (Control de acces)**, selectați **Secure Entry (Intrare securizată)** ca **Type (Tip)**.
- 6.7. În **IP address (Adresa IP)**, introduceți adresa IP pentru controlerul ușii.
- 6.8. În **Authentication key (Cheie de autentificare)**, lipiți cheia de autentificare pe care ați copiat-o anterior.
- 6.9. Faceți clic pe **Connect (Conectare)**.
- 6.10. La **Door controller name (Numele controlerului de ușă)**, selectați controlerul de ușă.
- 6.11. La **Reader name (Numele cititorului)**, selectați cititorul pe care l-ați adăugat anterior.
- 6.12. Activați integrarea.
7. Adăugați titularul cardului căruia doriți să îi acordați acces. Consultați *Adăugați un titular de card, on page 29*
8. Adăugați informațiile de conectare pentru plăcuța de înmatriculare la noul titular de card. Consultați *Adăugați informații de conectare, on page 30*
9. Adăugați o regulă de acces. Consultați *Adăugați o regulă de acces, on page 33*.
 - 9.1. Adăugați un program.
 - 9.2. Adăugați titularul de card pentru a cărui plăcuță de înmatriculare doriți să acordați acces.
 - 9.3. Adăugați ușa cu cititorul AXIS License Plate Verifier.

Adăugați un grup

Grupurile vă permit să gestionați în mod centralizat titularii de carduri și regulile de acces ale acestora.

1. Deschideți o  filă de gestionare a accesului.
2. Accesați **Cardholder management (Gestionarea titularilor de carduri) > Groups (Grupuri)** și faceți clic pe  **Add (Adăugare)**.
3. Introduceți un nume și, opțional, inițiale pentru grup.
4. Selectați **Global group (Grup global)** pentru a vedea și a monitoriza titularii de carduri de pe sub-servere. Această opțiune este disponibilă numai pentru titularii de carduri creați pe serverul principal. Consultați *Multi-server^{BETA}, on page 26*.
5. Adăugați titularii de carduri la grup:
 - 5.1. Faceți clic pe  **Add (Adăugare)**.
 - 5.2. Selectați titularii de carduri pe care doriți să îi adăugați și faceți clic pe **Add (Adăugare)**.
6. Faceți clic pe **Save (Salvare)**.
7. Pentru a imprima ecusoane pentru toți titularii de carduri dintr-un grup, selectați grupul și faceți clic pe **Print Badge (Imprimare ecuson)^{BETA}**. Pentru mai multe informații, consultați *Print badge (Imprimați ecusonul)^{BETA}, on page 38*.

Adăugați o regulă de acces

O regulă de acces definește condițiile care trebuie îndeplinite pentru a acorda acces.

O regulă de acces constă din:

Deținători de carduri și grupuri de deținători de carduri – cine să acorde accesul.

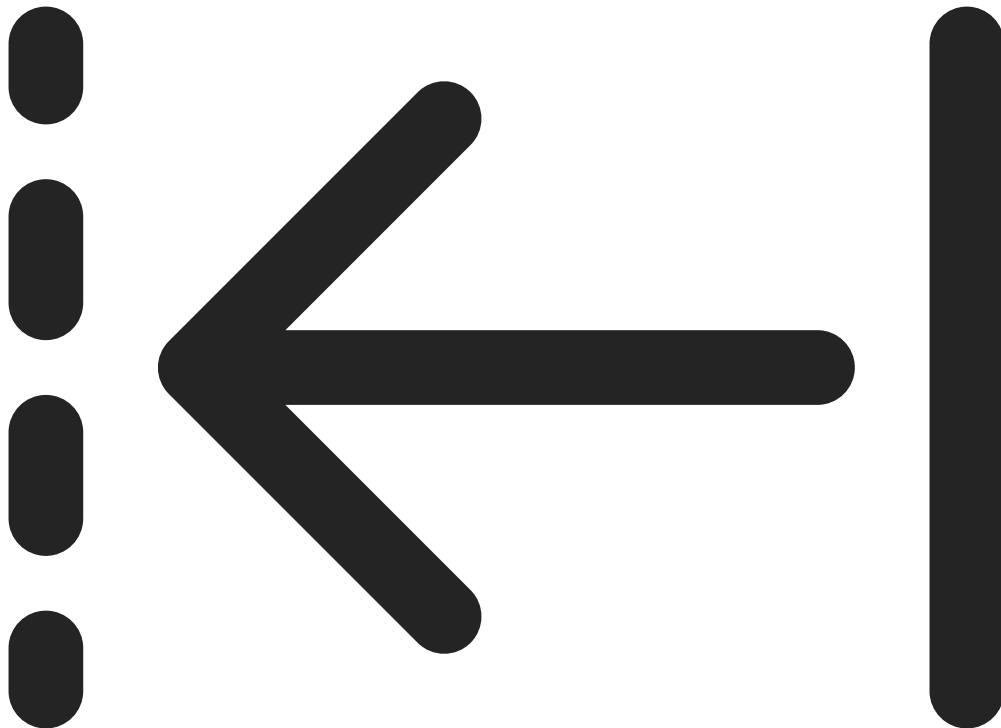
Uși și zone – unde se aplică accesul.

Programe – când să acorde accesul.

Pentru a adăuga o regulă de acces:

1. Deschideți o  filă de gestionare a accesului.

2. Accesați **Cardholder management** (Gestionarea titularilor de carduri).
3. La **Access rules** (Reguli de acces)



, faceți clic pe **+** **Add (Adăugare)**.

4. Introduceți un nume pentru regula de acces și faceți clic pe **Next (Mai departe)**.
5. Configurați titularii de carduri și grupurile:
 - 5.1. La **Cardholders (Titulari de carduri)** sau **Groups (Grupuri)**, faceți clic pe **+** **Add (Adăugare)**.
 - 5.2. Selectați titularii de card sau grupurile și faceți clic pe **Add (Adăugare)**.
 - 5.3. De asemenea, puteți trage și plasa un titular de card sau un grup direct pe o regulă de acces pentru a o aplica. În timpul tragerii, sunt evidențiate regulile de acces pe care îl puteți plasa. Dacă trageți simultan mai mulți titulari de card sau mai multe grupuri, un contor vă arată câți/câte mutați.
6. Configurați ușile și zonele:
 - 6.1. La **Doors (Uși)** sau **Zones (Zone)**, faceți clic pe **+** **Add (Adăugare)**.
 - 6.2. Selectați ușile sau zonele și faceți clic pe **Add (Adăugare)**.
7. Configurați programele:

- 7.1. La **Schedules (Programe)**, faceți clic pe **+ Add (Adăugați)**.
- 7.2. Selectați unul sau mai multe programe și faceți clic pe **Add (Adăugare)**.
8. Faceți clic pe **Save (Salvare)**.

O regulă de acces care nu conține una sau mai multe dintre componentele descrise mai sus este incompletă. Puteți vedea toate regulile de acces incomplete în fila **Incomplete (Incompletă)**.



Exportați rapoarte privind configurația sistemului

Puteți exporta rapoarte care conțin diferite tipuri de informații despre sistem. AXIS Camera Station Pro Secure Entry exportă raporturile ca un fișier CSV (comma-separated value (valori separate prin virgulă)) și le salvează în folderul de descărcare implicit. Pentru a exporta un raport:

1. Deschideți o  filă de gestionare a accesului.
2. Accesați **Reports (Rapoarte) > System configuration (Configurație sistem)**.
3. Selectați rapoartele pe care doriți să le exportați și faceți clic pe **Download (Descărcare)**.

Raport privind detaliile titularilor de carduri	Include informații despre titularii de carduri, datele de identificare, validarea cardului și ultima tranzacție.
Raport privind accesul titularilor de carduri	Include informații despre titularul cardului și informații despre grupurile de titulari, regulile de acces, ușile și zonele legate de titularul cardului.
Raport privind accesul grupului titularilor de carduri	Include numele de grup al titularului cardului și informații despre titulari, regulile de acces, ușile și zonele legate de titularul cardului.
Raport privind regulile de acces	Include numele regulii de acces și informații despre titularii de carduri, grupurile de titulari de carduri, ușile și zonele legate de regula de acces.
Raport privind accesul la ușă	Include numele ușii și informații despre titularii de carduri, grupurile de titulari de carduri, regulile de acces și zonele legate de ușă.
Raport acces zonă	Include numele zonei și informații despre titularii de carduri, grupurile de titulari de carduri, regulile de acces și ușile legate de zonă.

Crearea de rapoarte privind activitatea titularilor de card

Un raport de prezență enumeră titularii de card dintr-o anumită zonă, ajutând la identificarea persoanelor prezente la un moment dat.

Un raport de adunare enumeră titularii de card dintr-o zonă specificată, ajutând la identificarea persoanelor aflate în siguranță și a celor lipsă din timpul situațiilor de urgență. El ajută administratorii clădirilor să găsească personalul și vizitatorii după evacuări. Un punct de adunare este un loc stabilit în prealabil unde personalul se prezintă în situații de urgență. Sistemul generează un raport privind persoanele aflate în incintă și în afara acesteia. Sistemul marchează titularii de card ca fiind lipsă până când aceștia se prezintă la un punct de adunare sau până când cineva îi marchează manual ca fiind în siguranță.

Atât raportul de prezență, cât și raportul de adunare necesită zone pentru a urmări titularii de card.

Pentru a crea și a efectua un raport de prezență sau de adunare:

1. Deschideți o  filă de gestionare a accesului.
2. Accesați **Reports (Rapoarte) > Cardholder activity (Activitatea titularului de card)**.
3. Faceți clic pe **+ Add (Adăugare)** și selectați **Roll call / Mustering (Prezență / Adunare)**.
4. Introduceți un nume pentru raport.
5. Selectați zonele care urmează să fie incluse în raport.
6. Selectați toate grupurile pe care doriți să le includeți în raport.
7. Dacă doriți un raport de adunare, selectați **Mustering point (Punct de adunare)** și un cititor.
8. Selectați un cadru temporal pentru raport.
9. Faceți clic pe **Save (Salvare)**.
10. Selectați raportul și faceți clic pe **Run (Efectuare)**.

Starea raportului de prezență	Description (Descriere)
Present (Prezent)	Titularul de card a intrat în zona specificată și nu a ieșit înainte de efectuarea raportului.
Not present (Nu este prezent)	Titularul de card a ieșit din zona specificată și nu a intrat din nou înainte de efectuarea raportului.

Starea raportului de adunare	Description (Descriere)
Safe (Siguranță)	Titularul de card și-a glisat cardul la punctul de adunare.
Missing (Lipsește)	Titularul de card nu și-a glisat cardul la punctul de adunare.

Import și export

Importul titularilor de carduri

Această opțiune importă titularii de card, grupurile, informațiile de conectare și fotografiile dintr-un fișier CSV. Pentru a importa fotografiile titularilor de carduri, asigurați-vă că serverul are acces la fotografii.

Atunci când importați titularii de card, sistemul de gestionare a accesului salvează automat configurația sistemului, inclusiv toată configurația hardware, și șterge orice configurație salvată anterior.

De asemenea, puteți cartografia utilizatorii dintr-o bază de date Active Directory ca titulari de carduri.

Consultați *Setări Active Directory^{BETA}*, on page 27.

Opțiuni de import	
Nou	Elimină titularii de card existenți și adaugă noi titulari de card.
Actualizare	Actualizează titularii de card existenți și adaugă noi titulari de card.
Adăugare	Păstrează titularii de card existenți și adaugă noi titulari de card. Numerele cardurilor și ID-urile titularilor de carduri sunt unice și pot fi utilizate o singură dată.

1. În fila **Access management (Gestionarea accesului)**, faceți clic pe **Import and export (Import și export)**.
2. Faceți clic pe **Import cardholders (Importare titularii de carduri)**.

3. Selectați **New (Nou)**, **Update (Actualizare)**, sau **Add (Adăugare)**.
4. Faceți clic pe **Next (Mai departe)**.
5. Faceți clic pe **Choose a file (Alegeți un fișier)**, localizați fișierul CSV și faceți clic pe **Open (Deschideți)**.
6. Introduceți un delimitator de coloană și selectați un identificator unic și faceți clic pe **Next (Mai departe)**.
7. Atribuiți un titlu fiecărei coloane.
8. Faceți clic pe **Import**.

Setări de import	
Primul rând este antetul	Selectați dacă fișierul CSV conține un antet de coloană.
Delimitator de coloană	Introduceți un format de delimitare a coloanelor pentru fișierul CSV.
Identificator unic	Sistemul utilizează implicit Cardholder ID (Titular de card) pentru a identifica un titular de card. De asemenea, puteți utiliza numele și prenumele sau adresa de e-mail. Folosiți această opțiune pentru a evita importarea înregistrărilor duplicate ale personalului.
Formatul numărului de card	Allow both hexadecimal and number (Permiterea atât a numerelor hexazecimale, cât și a numerelor) este activată implicit.

Titularii de carduri de export

Această opțiune exportă datele titularilor de carduri din sistem într-un fișier CSV.

1. În fila **Access management (Gestionarea accesului)**, faceți clic pe **Import and export (Import și export)**.
2. Faceți clic pe **Export cardholders (Exportare titularii de carduri)**.
3. Alegeți o locație de descărcare și faceți clic pe **Save (Salvare)**.

AXIS Camera Station Pro Secure Entry actualizează fotografiile titularilor de carduri în `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos` ori de câte ori se modifică configurația.

Anulare import

Sistemul își salvează automat configurația atunci când importați titularii de carduri. Opțiunea **Undo import (Anulare import)** resetează datele titularului de card și toată configurația hardware la starea în care a fost înainte de ultimul import.

1. În fila **Access management (Gestionarea accesului)**, faceți clic pe **Import and export (Import și export)**.
2. Faceți clic pe **Undo import (Anulare import)**.
3. Faceți clic pe **Yes (Da)**.

Setări de gestionare a accesului

Pentru a personaliza câmpurile titularului de card utilizate în tabloul de bord pentru gestionarea accesului:

1. În fila **Access management (Gestionarea accesului)**, faceți clic pe **Settings (Setări) > Custom cardholder fields (Câmpuri personalizate pentru titularul de card)**.
2. Faceți clic pe  **Add (Adăugare)** și introduceți un nume. Puteți adăuga până la 6 câmpuri personalizate.
3. Faceți clic pe **Add (Adăugare)**.

Pentru a utiliza codul instalației pentru a verifica sistemul dvs. de control de acces:

1. În fila **Access management (Gestionarea accesului)**, faceți clic pe **Settings (Setări) > Facility code (Codul instalației)**.
2. Selectați **Facility code on (Codul instituției pe)**.

note

De asemenea, trebuie să selectați **Include facility code for card validation (Includeți codul instituției pentru validarea cardului)** atunci când configurați profilurile de identificare. Consultați *Profiluri de identificare, on page 20*.

Pentru a edita un șablon de e-mail pentru trimiterea unui cod QR sau a unor informații de conectare prin dispozitive mobile:

1. În fila **Access management (Gestionarea accesului)**, faceți clic pe **Settings (Setări) > Email templates (Șabloane e-mail)**.
2. Editați șablonul dvs. și faceți clic pe **Update (Actualizare)**.

Modele de ecuson ^{BETA}

Puteți personaliza modelele de ecuson cu informații despre deținătorul de card, fotografii, logo-uri și mărci personalizate. Pentru a crea un nou model:

1. Accesați **Access management (Gestionarea accesului) > Settings (Setări) > Badge templates (Modele de ecuson) ^{BETA}**.
2. Faceți clic pe **Create new template (Creați un model nou)**.
3. Introduceți un nume în câmpul **Template name (Numele modelului)**.
4. Selectați **Use as default template for printing (Utilizați ca model implicit pentru imprimare)** pentru ca acest model să fie implicit.
5. Personalizarea designului ecusonului:
 - Selectați până la cinci câmpuri de text pentru tipărirea pe partea din față, inclusiv toate câmpurile personalizate pe care le-ați creat. La imprimare, pe ecuson apar numai câmpurile completate.
 - Alegeți fontul și culoarea textului.
 - Adăugați o culoare sau o imagine de fundal.
 - Încărcați un logo pentru organizația dvs.
 - Pentru partea din spate, adăugați o culoare de fundal sau o imagine.
6. Faceți clic pe **Save (Salvați)** pentru a salva modificările sau pe **Save as (Salvați ca)** pentru a crea un model nou.

note

După ce a fost creat un model, el nu mai poate fi editat, ci doar redenumit.

Print badge (Imprimați ecusonul) ^{BETA}

Puteți imprima ecusoane de identificare pentru deținătorii de card utilizând modelele de ecuson configurate. În prezent, codorul cardurilor nu este acceptat. Înainte de a începe:

- Asigurați-vă că deținătorul de card are cel puțin o informație de conectare cu card. Nu puteți imprima ecusoane pentru deținătorii de card fără acreditări.
- Aveți nevoie de o imprimantă care acceptă dimensiunea cardului CR80 și materiale de imprimare compatibile, precum carton gros.
- Configurarea setărilor de imprimare ale browserului:
 1. Setări dimensiunea paginii la CR80 sau la o dimensiune personalizată care corespunde dimensiunilor cardului dvs.
 2. Setări orientarea la portret.
 3. Dezactivați marginile sau setați-le la minim.

important

Secure Entry este compatibil cu imprimantele care dispun de drivere pentru Windows. S-a verificat că imprimantele din seria HID Fargo funcționează. Dacă aveți nevoie de un driver pentru imprimanta dvs., contactați furnizorul imprimantei.

Pentru a imprima ecusoane:

1. Accesați **Access management (Gestionarea accesului) > Cardholder management (Gestionarea deținătorilor de card) > Cardholders (Deținători de card)**.
2. Selectați unul sau mai mulți deținători de card.
3. Faceți clic pe **Print badge (Imprimați ecusonul)** ^{BETA}.
4. Faceți clic pe **Select template (Selectați modelul)** și, din meniul derulant **Template (Model)**, selectați modelul de ecuson pe care doriți să îl utilizați.
5. Dacă deținătorul de card are mai multe informații de conectare cu card, selectați una din meniul derulant **Card**.
6. Faceți clic pe **Print (Imprimare)**.

note

Dacă imprimanta dvs. nu acceptă imprimarea duplex, imprimați mai întâi toate paginile din față, apoi întoarceți teancul de carduri și încărcați-le din nou în tavă pentru a imprima paginile din spate.

T10231644_ro

2026-07 (M8.5)

© 2025 – 2026 Axis Communications AB