AXIS Camera Station Pro Secure Entry

Benutzerhandbuch

Info

Secure Entry ist eine Komponente von AXIS Camera Station Pro. Verwenden Sie diese Funktion, um Geräte hinzuzufügen und Zeitpläne zu verwalten. Weitere Informationen finden Sie im *AXIS Camera Station Pro - Benutzerhandbuch*.

Konfigurieren der Zutrittskontrolle

Wenn Sie Ihrem System einen Axis Network Door Controller hinzugefügt haben, können Sie die Hardware für die Zutrittskontrolle in AXIS Camera Station Version 6.x oder höher konfigurieren.

Die vollständige Vorgehensweise zum Einrichten eines Axis Network Door Controller in AXIS Camera Station Pro Secure Entry finden Sie unter *Einrichten eines Axis Network Door Controllers*.

Hinweis

Stellen Sie vor dem Start Folgendes sicher:

- Aktualisieren Sie die AXIS OS-Version des Controllers unter **Configuration (Konfiguration) > Devices (Geräte) > Management (Verwaltung)**.
- Legen Sie unter **Konfiguration > Geräte > Verwaltung** Datum und Uhrzeit für den Controller fest.
- Aktivieren Sie HTTPS auf dem Controller unter **Configuration > Devices > Management (Konfiguration > Geräte > Management)**.

Vorgehensweise zum Konfigurieren der Zutrittskontrolle

1. Informationen zum Bearbeiten der vordefinierten Identifizierungsprofile oder zum Erstellen eines neuen Identifizierungsprofils finden Sie unter *Identifizierungsprofile, on page 23*.
2. Informationen zur Verwendung eines benutzerdefinierten Setups für Kartenformate und die PIN-Länge finden Sie unter *Kartenformate und PIN, on page 25*.
3. Fügen Sie einen Zugang hinzu und wenden Sie ein Identifizierungsprofil auf den Zugang an. Siehe *Hinzufügen eines Zugangs, on page 7*.
4. Konfigurieren Sie den Zugang.
   - *Zugangsmonitor hinzufügen, on page 14*
   - *Notfall-Eingang hinzufügen, on page 16*
   - *Leser hinzufügen, on page 17*
   - *REX-Gerät hinzufügen, on page 19*
5. Fügen Sie eine Zone hinzu und fügen Sie der Zone Zugänge hinzu. Siehe *Zone hinzufügen, on page 20*.

Kompatibilität der Gerätesoftware für Tür-Steuerungen

Wichtig

Beachten Sie bei der Aktualisierung des AXIS OS auf Ihrer Tür-Steuerung die folgenden Punkte:

- **Unterstützte AXIS OS Versionen:** Die unten aufgeführten unterstützten AXIS OS Versionen gelten nur bei einer Aktualisierung von der empfohlenen Originalversion der AXIS Camera Station Pro und wenn das System über eine Tür verfügt. Wenn das System diese Bedingungen nicht erfüllt, müssen Sie eine Aktualisierung auf die von empfohlene AXIS OS Version für die jeweilige AXIS Camera Station Pro Version vornehmen.
- **Unterstützte AXIS OS Mindestversion:** Die älteste im System installierte AXIS OS-Version bestimmt die unterstützte AXIS OS Mindestversion, mit einer Grenze von zwei früheren Versionen. Angenommen, Sie verwenden die AXIS Camera Station Pro Version 6.5 und aktualisieren alle Geräte auf die empfohlene AXIS OS Version 12.0.86.2, dann wird die AXIS OS Version 12.0.86.2 zur unterstützte Mindestversion für Ihr System.
- **Aktualisierung über die empfohlene AXIS OS Version hinaus:** Angenommen, Sie führen eine Aktualisierung auf eine AXIS OS Version durch, die über der empfohlenen Version für eine bestimmte AXIS Camera Station Pro Version liegt. Dann können Sie jederzeit problemlos auf die von empfohlene AXIS OS Version zurückstufen, solange diese innerhalb der Unterstützungsgrenzen für die AXIS Camera Station Pro Version liegt.
- **Empfehlungen für zukünftiges AXIS OS:** Verwenden Sie immer die empfohlene AXIS OS Version für die

jeweilige AXIS Camera Station Pro Version, um die Systemstabilität und vollständige Kompatibilität zu gewährleisten.

- **Änderungen nachverfolgen:** Beim Ändern der Firmware-Version von 10.12.xx auf 11.0.xx oder höher muss auf die werksseitige Standardeinstellung zurückgesetzt werden.

Die folgende Tabelle zeigt die minimale und empfohlene AXIS OS Version für jede AXIS Camera Station Pro Version:

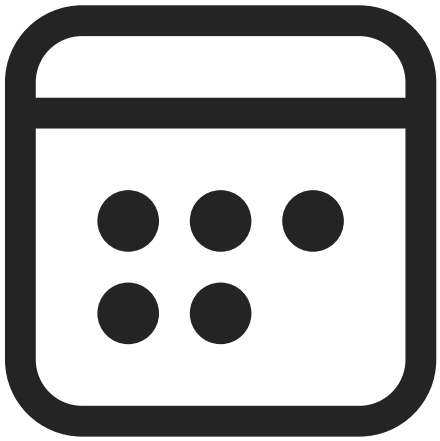
AXIS Camera Station Version	AXIS OS Mindestversion	Empfohlene AXIS OS Version
Pro 6.15	12.5.68.1	12.8.55.1
Pro 6.14	12.5.68.1	12.8.55.1
Pro 6.13	12.5.68.1	12.6.102.1

Die folgende Tabelle zeigt die minimale und empfohlene Version von AXIS OS für jede Version von AXIS Camera Station 5:

AXIS Camera Station Version	Empfohlene AXIS OS Version
5.59	12.4.68.1
5.58	12.4.68.1
5.57	11.8.20.2

Türen und Bereiche

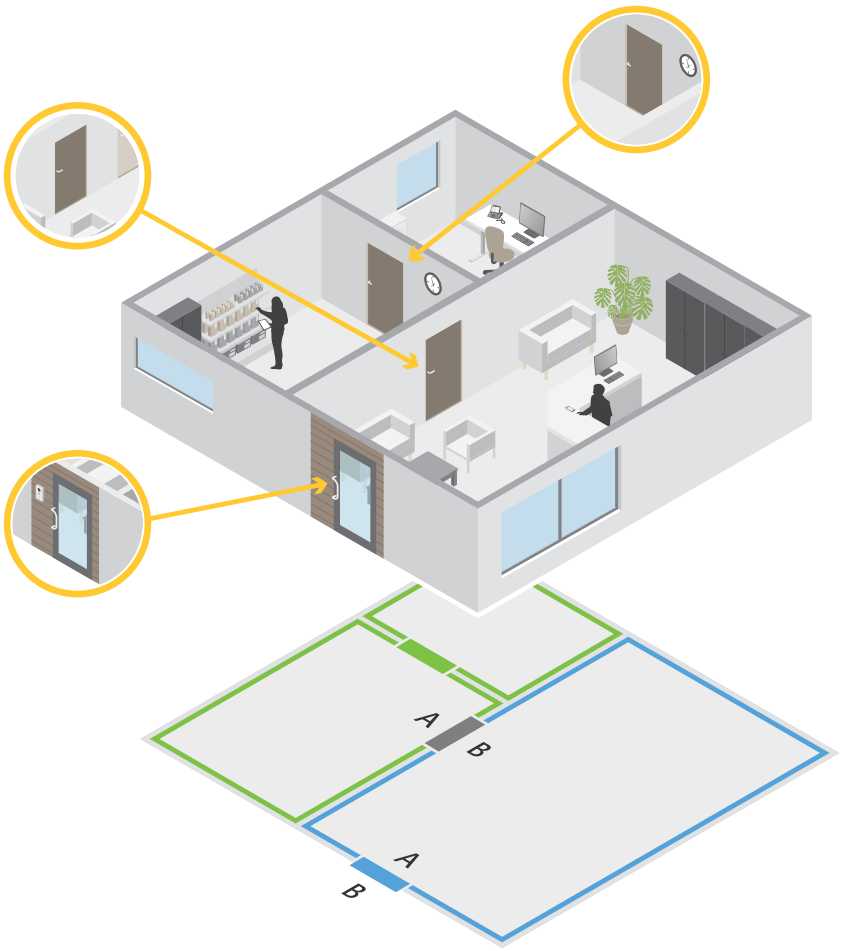
Rufen Sie **Configuration > Access control > Doors and zones (Konfiguration > Zutrittskontrolle > Zugänge und Zonen)** auf, um eine Übersicht zu erhalten und Zugänge und Zonen zu konfigurieren.

 **Manuelle Aktionen**	Legen Sie den Status eines Zugangs manuell fest. Wählen Sie aus den folgenden Optionen aus: **Reset (Zurücksetzen)** (gemäß den Systemregeln), **Grant access (Zugriff gewähren)** (Zugang für 7 Sekunden entriegeln), **Unlock (Entriegeln)** (Zugang entriegelt lassen), **Verriegeln** (Zugang verriegelt lassen) oder **Sperren** (Zugang von beiden Seiten sperren).
 **Entriegelungspläne**	Sie können einen Zeitplan für die automatische Entriegelung von Zugängen zu bestimmten Zeiten festlegen. Zu allen anderen Zeiten bleiben die Zugänge verriegelt. Um festzulegen, dass die erste Person den Zugang manuell zunächst entriegeln muss, bevor der Zeitplan aktiviert wird, aktivieren Sie die Option **First person in (Nach Entriegelung durch erste Person)**.
Identifizierungsprofil	Ändern Sie das Identifizierungsprofil für Zugänge.
Pin Chart	Zeigen Sie das Pin Chart des Controllers an, das einem Zugang zugeordnet ist. Wenn Sie das Pin Chart ausdrucken möchten, klicken Sie auf **Print (Drucken)**.
Secure Channel	Schalten Sie OSDP Secure Channel für einen bestimmten Leser ein oder aus.

Türen	
Bezeichnung	Der Name des Zugangs.
Typ	Hierbei handelt es sich um die Art der Zugangskonfiguration.
Gerät	Das bezieht sich auf das am Zugang angebrachte Gerät.

IP-Adresse	Die IP-Adresse der an die Tür angeschlossenen Tür-Steuerung.
Seite A	Die Zone, in der sich Seite A des Zugangs befindet.
Seite B	Die Zone, in der sich Seite B des Zugangs befindet.
Identifizierungsprofil	Das Identifizierungsprofil, das auf den Zugang angewendet wird.
Batterie	Hierbei handelt es sich um den Status der Batterie in der Tür-Steuerung.
Status	Den Zugangs. • **Online** Der Zugang ist online und funktioniert normal. • **Leser offline:** Der Leser in der Zugangskonfiguration ist offline. • **Leserfehler:** Der Leser in der Türkonfiguration unterstützt keinen sicheren Kanal oder sicherer Kanal ist für den Leser nicht aktiviert. • **Alte Firmware:** Das Gerät nutzt eine veraltete Firmware-Version. Aktualisieren Sie die Firmware, um die optimale Funktion und den höchsten Grad an Sicherheit zu gewährleisten.
Zonen	
Bezeichnung	Der Name der Zone.
Anzahl der Zugänge	Die Anzahl der Zugänge in der Zone.
Sicherheitsgrad	Hierbei handelt es sich um die für die Zone geltende Sicherheitsstufe.

Beispiel für Zugänge und Zonen



- Es gibt zwei Zonen: eine grüne und eine blaue.
- Es gibt drei Zugänge: einen grünen, einen blauen und einen braunen.
- Beim grünen Zugang handelt es sich um einen internen Zugang in der grünen Zone.
- Der blaue Zugang ist ein Umgrenzungszugang nur für die blaue Zone.
- Der braune Zugang ist ein Umgrenzungszugang sowohl für die grüne als auch für die blaue Zone.

Hinzufügen eines Zugangs

Hinweis

- Sie können eine Tür-Steuerung mit einer Tür mit zwei Schlössern oder mit zwei Türen mit jeweils einem Schloss konfigurieren. Mehrfachsteuerungen unterstützen weitere Schlosskonfigurationen.
- Wenn einer Tür-Steuerung keine Türen zugewiesen sind und Sie eine neue Version von AXIS Camera Station Pro Secure Entry mit einer Tür-Steuerung mit älterer Firmware verwenden, verhindert das System das Hinzufügen einer Tür. Wenn der Tür-Steuerung jedoch bereits eine Tür hinzugefügt wurde, gestattet das System das Hinzufügen neuer Türen auf Systemcontrollern mit älterer Firmware.

Erstellen einer neuen Zugangskonfiguration zum Hinzufügen einer Tür:

1. Rufen Sie **Configuration > Access control > Doors and zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen)** auf.

2. Klicken Sie auf + **Add door (Zugang hinzufügen)** und wählen Sie einen Zugangstyp aus dem Aufklappmenü aus.

Türarten	
Tür	Eine herkömmliche Tür mit einem Zugangsmonitor, der Schlösser und Leser unterstützt. Erfordert eine Tür-Steuerung.
Drahtloser Zugang	Ein Zugang, der sich mit Funkschlössern und Kommunikationshubs ASSA ABLOY Aperio® konfigurieren lässt. Weitere Informationen finden Sie unter *Drahtloses Schloss hinzufügen, on page 12*.
Überwachter Zugang	Ein Zugang, der melden kann, ob er geöffnet oder geschlossen ist. Weitere Informationen finden Sie unter *Überwachten Zugang hinzufügen, on page 15*.
Vorgesehener Zugang	Ein Zugang, den Sie als Platzhalter in einem System hinzufügen können, ohne dass Sie die Hardware dafür auswählen müssen.
Etage	Ein Zugangstyp für die Aufzugssteuerung, der den Zugriff auf die Aufzugsetagen mithilfe von Kartenlesegeräten authentifiziert. Weitere Informationen finden Sie unter *Eine Etage für die Aufzugsteuerung hinzufügen BETA, on page 15*.

3. Geben Sie einen Namen für den Zugang ein und wählen Sie im Aufklappmenü **Device (Geräte)** eine Tür-Steuerung aus, die mit dem Zugang verknüpft werden soll. Der Controller ist ausgegraut, wenn Sie keine weitere Tür hinzufügen können, wenn er offline ist oder HTTPS nicht aktiviert ist.
4. Klicken Sie auf **Next (Weiter)**, um die Seite zur Zugangskonfiguration aufzurufen.
5. Wählen Sie im Drop-Down Menü **Primary lock (Primäres Schloss)** einen Relay-Port aus.
6. Um zwei Schlösser am Zugang zu konfigurieren, wählen Sie den anderen Relay-Port im Drop-Down Menü **Secondary lock (Sekundäres Schloss)** aus.
7. Wählen Sie ein Identifizierungsprofil aus. Siehe *Identifizierungsprofile, on page 23*.
8. Konfigurieren Sie die Zugangseinstellungen. Siehe *Einstellungen der Tür, on page 9*.
9. *Zugangsmonitor hinzufügen, on page 14*
10. *Notfall-Eingang hinzufügen, on page 16*
11. *Leser hinzufügen, on page 17*
12. *REX-Gerät hinzufügen, on page 19*
13. Konfigurieren Sie die Sicherheitsstufe. Siehe *Sicherheitsstufe der Tür, on page 10*.
14. **Save (Speichern)** anklicken.

Konfiguration eines Zugangs kopieren:

1. Rufen Sie **Configuration > Access control > Doors and zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen)** auf.
2. Klicken Sie auf + **Add door (Zugang hinzufügen)**.
3. Geben Sie einen Namen für den Zugang ein und wählen Sie im Aufklappmenü **Device (Geräte)** eine Tür-Steuerung aus, die mit dem Zugang verknüpft werden soll.
4. Klicken Sie auf **Next (Weiter)**.

5. Wählen Sie aus im Drop-Down Menü **Copy configuration (Konfiguration kopieren)** eine vorhandene Zugangskonfiguration aus. Es enthält die angeschlossenen Zugänge und der Controller ist ausgegraut, wenn er mit zwei Zugängen oder einem Zugang mit zwei Schlössern konfiguriert wurde.
6. Sie können die Einstellungen jederzeit ändern.
7. **Save (Speichern)** anklicken.

So entfernen Sie einen Zugang:

1. Rufen Sie **Configuration > Access control > Door and zones > Zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen > Zonen)** auf.
2. Wählen Sie einen Zugang in der Liste aus.
3. Klicken Sie auf **Remove (Entfernen)** und bestätigen Sie.

Hinzufügen und Konfigurieren von Zugängen und Zonen

Einstellungen der Tür

So bearbeiten Sie einen Zugang:

1. Rufen Sie **Configuration > Access control > Door and Zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen)** auf.
2. Wählen Sie den Zugang aus, den Sie bearbeiten möchten.
3. Klicken Sie auf **Edit (Bearbeiten)**.
4. Ändern Sie die Einstellungen und klicken Sie auf **Save (Speichern)**.

Zugangszeit (s)	Legen Sie die Anzahl von Sekunden fest, die der Zugang geöffnet bleibt, nachdem Zutritt gewährt wurde. Die Tür bleibt entriegelt, bis sie sich öffnet oder bis die eingestellte Zeit endet. Die Tür verriegelt sich beim Schließen selbst dann, wenn noch Zugangszeit bleibt.
Open-too-long time (sec) (Maximale Öffnungsdauer (s))	Nur gültig, wenn ein Zugangsmonitor konfiguriert ist. Legen Sie fest, wie viele Sekunden die Tür geöffnet bleibt. Wenn die Tür geöffnet ist, wenn die eingestellte Zeit endet, löst sie einen Alarm einer zu lange geöffneten Tür aus. Richten Sie eine Aktionsregel ein, die festlegt, welche Aktion ausgelöst werden soll, wenn die maximale Öffnungsdauer überschritten wird.
Lange Zutrittszeiten (Sekunden)	Legen Sie die Anzahl von Sekunden fest, die der Zugang geöffnet bleibt, nachdem Zutritt gewährt wurde. Der Wert für die lange Zutrittszeit überschreibt die bereits festgelegte Zutrittszeit für Karteninhaber, wenn diese Einstellung aktiviert ist.
Long open-too-long time (sec) (Lange maximale Öffnungsdauer (s))	Nur gültig, wenn ein Zugangsmonitor konfiguriert ist. Legen Sie fest, wie viele Sekunden die Tür geöffnet

	bleibt. Wenn die Tür geöffnet ist, wenn die eingestellte Zeit endet, löst sie ein Ereignis einer zu lange geöffneten Tür aus. Wenn Sie die Einstellung **Long access time (Lange Zugangszeit)** einschalten, überschreibt der Wert für die lange maximale Öffnungsdauer die bereits festgelegte maximale Öffnungsdauer für Karteninhaber.
Verzögerungszeit bis zum Wiederverriegeln (ms)	Legen Sie die Zeit (in Millisekunden) fest, die die Tür nach dem Öffnen oder Schließen entriegelt bleibt.
Wieder verriegeln	• **After opening: (Nach dem Öffnen:)** Nur gültig, wenn ein Zugangsmonitor hinzugefügt wurde. • **After closing: (Nach dem Schließen:)** Nur gültig, wenn ein Zugangsmonitor hinzugefügt wurde.
Zugang erzwungen	Wählen Sie, ob das System einen Systemalarm auslösen soll, wenn eine Tür gewaltsam geöffnet wurde. Erfordert einen Türpositionssensor (DPS).
Tür zu lange geöffnet	Wählen Sie, ob das System einen Systemalarm auslösen soll, wenn eine Tür zu lange offen gehalten wird.

Manuelle Aktionen

Sie können die folgenden manuellen Aktionen an Zugängen und Zonen durchführen:

Zurücksetzen – Stellt die konfigurierten Systemregeln wieder her.

Zugang gewähren – Entriegelt 7 Sekunden lang einen Zugang oder eine Zone und sperrt sie dann wieder.

Entriegeln – Hält den Zugang unverschlossen, bis Sie zurücksetzen.

Schloss – Hält den Zugang gesperrt, bis das System einem Karteninhaber den Zugriff gewährt.

Verriegelung – Niemand kommt rein oder raus, bis Sie zurücksetzen oder entsperren.

Um eine manuelle Aktion durchzuführen:

1. Rufen Sie **Configuration** > **Access control** > **Doors and zones** (Konfiguration > Zutrittskontrolle > Zugang und Zonen) auf.
2. Wählen Sie den Zugang oder die Zone aus, für die Sie eine manuelle Aktion durchführen möchten.
3. Klicken Sie auf eine der manuellen Aktionen.

Sicherheitsstufe der Tür

Sie können einer Tür die folgenden Sicherheitsfunktion hinzufügen:

Zwei-Personen-Regel – Die Zwei-Personen-Regel erfordert, dass zwei Personen gültige Zugangsdaten verwenden, um Zugang zu erhalten.

Double Swipe – Mit dem doppelten Durchziehen kann der Karteninhaber den aktuellen Status einer Tür überschreiben. Beispielsweise kann er damit einen Zugang außerhalb des regulären Zeitplans sperren und entsperren, was bequemer ist, als das Entsperren des Zugangs im System. Die Double-Swipe-Funktion wirkt sich nicht auf einen vorhandenen Zeitplan aus. Wenn etwa ein Zugang zur Schließzeit gemäß Zeitplan verriegelt werden soll und ein Mitarbeiter in die Mittagspause geht, wird der Zugang dennoch gemäß Zeitplan verriegelt.

Sie können die Sicherheitsstufe konfigurieren, während Sie eine neue Tür hinzufügen, oder Sie können die Konfiguration für eine vorhandene Tür durchführen.

So fügen Sie eine **Zwei-Personen-Regel** zu einem vorhandenen Zugang hinzu:

1. Rufen Sie **Configuration** > **Access control** > **Doors and zones** (Konfiguration > Zutrittskontrolle > Zugang und Zonen) auf.
2. Wählen Sie die Tür aus, für die Sie eine Sicherheitsstufe konfigurieren möchten.
3. Klicken Sie auf **Edit (Bearbeiten)**.
4. Klicken Sie auf **Security level (Sicherheitsstufe)**.
5. Aktivieren Sie **Zwei-Personen-Regel**.
6. Klicken Sie auf **Anwenden**.

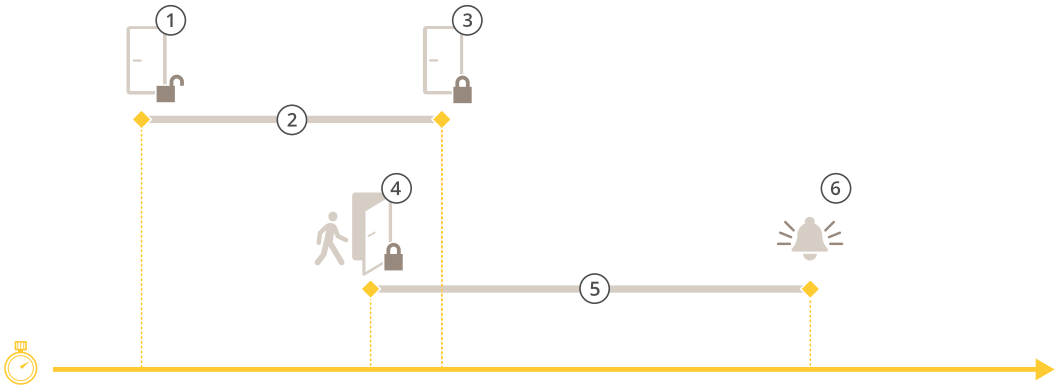
Zwei-Personen-Regel	
Side A (Seite A) und **Side B (Seite B)**	Wählen Sie aus, auf welchen Seiten der Tür die Regel verwendet werden soll.
Zeitschemata	Wählen Sie „While the rule is active" (Während die Regel aktiv ist).
Zeitüberschreitung (Sekunden)	Timeout ist die maximal zulässige Zeit zwischen dem Durchziehen der Karte oder der Verwendung eines anderen Typs gültiger Zugangsdaten.

So fügen Sie einem vorhandenen Zugang **Double Swipe** hinzu:

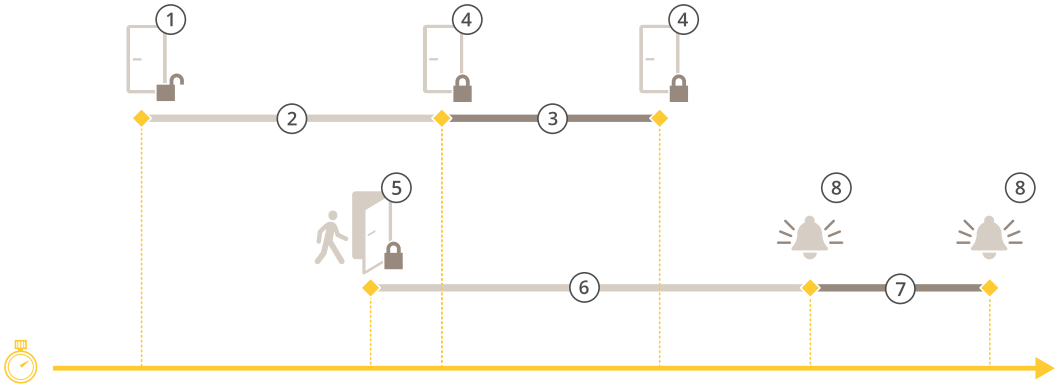
1. Rufen Sie **Configuration** > **Access control** > **Doors and zones** (Konfiguration > Zutrittskontrolle > Zugang und Zonen) auf.
2. Wählen Sie die Tür aus, für die Sie eine Sicherheitsstufe konfigurieren möchten.
3. Klicken Sie auf **Edit (Bearbeiten)**.
4. Klicken Sie auf **Security level (Sicherheitsstufe)**.
5. Aktivieren Sie **Double Swipe**.
6. Klicken Sie auf **Anwenden**.
7. Wenden Sie **Double Swipe** auf einen Karteninhaber an.
   7.1. Öffnen Sie eine Registerkarte **Access Management (Zugangsverwaltung)**.
   7.2. Klicken Sie beim zu bearbeitenden Karteninhaber auf ⋮ und dann auf **Edit (Bearbeiten)**.
   7.3. Klicken Sie **Mehr** an.
   7.4. Wählen Sie **Allow double-swipe (Double Swipe zulassen)** aus.
   7.5. Klicken Sie auf **Anwenden**.

Double Swipe	
Zeitüberschreitung (Sekunden)	Timeout ist die maximal zulässige Zeit zwischen dem Durchziehen der Karte oder der Verwendung eines anderen Typs gültiger Zugangsdaten.

Zeitoptionen



1 Zugang gewährt – Schloss entriegelt
2 Zugangszeit
3 Keine Aktion ausgeführt – Schloss verriegelt
4 Aktion ausgeführt (Tür geöffnet) – Schloss verriegelt oder bleibt entriegelt, bis die Tür geschlossen wird
5 Zu lange geöffnet
6 Zu lange geöffnet – Alarm wird ausgelöst



1 Zugang gewährt – Schloss entriegelt
2 Zugangszeit
3 2+3: Lange Zugriffszeit
4 Keine Aktion ausgeführt – Schloss verriegelt
5 Aktion ausgeführt (Tür geöffnet) – Schloss verriegelt oder bleibt entriegelt, bis die Tür geschlossen wird
6 Zu lange geöffnet
7 6+7: Lange maximale Öffnungsdauer
8 Zu lange geöffnet – Alarm wird ausgelöst

Drahtloses Schloss hinzufügen

AXIS Camera Station Pro Secure Entry unterstützt die Funkschlösser und Kommunikationshubs ASSA ABLOY Aperio®. Das drahtlose Schloss wird über einen Aperio-Kommunikationshub am RS485-Anschluss der Türsteuerung mit dem System verbunden. An einer Türsteuerung können Sie 16 Funkschlösser anschließen.

Hinweis

- Für die Einrichtung muss auf der Axis Türsteuerung AXIS OS Version 11.6.16.1 oder höher ausgeführt werden.
- Für die Einrichtung ist eine gültige Lizenz für AXIS Door Controller Extension erforderlich.
- Die Uhrzeit des Axis Tür-Controllers und des AXIS Camera Station Pro Secure Entry Servers muss synchronisiert werden.
- Vor dem Start müssen Sie die mithilfe der Aperio-Programmieranwendung, die von ASSA ABLOY unterstützt wird, Aperio-Schlösser mit dem Aperio-Hub koppeln.
- An jeden RS485-Steckverbinder kann jeweils nur ein Aperio-Hub angeschlossen werden. Multi-Drop wird nicht unterstützt.
- Funkschlösser folgen Zeitplänen für die Entsperrung nicht, wenn sie offline sind.

1. Greifen Sie auf die Türsteuerung zu.
   1.1. **Konfiguration > Geräte > Andere Geräte** aufrufen.
   1.2. Öffnen Sie die Weboberfläche der Türsteuerung, die mit dem Aperio-Kommunikationshub verbunden ist.
2. Aktivieren Sie AXIS Door Controller Extension.
   2.1. Gehen Sie auf der Weboberfläche der Türsteuerung zu **Apps**.
   2.2. Öffnen Sie das Kontextmenü von AXIS Door Controller Extension .
   2.3. Klicken Sie auf **Lizenz mit einem Schlüssel aktivieren** und wählen Sie Ihre Lizenz.
   2.4. Aktivieren Sie **AXIS Door Controller Extension**.
3. Verbinden Sie das Funkschloss über den Kommunikationshub mit der Türsteuerung.
   3.1. Gehen Sie auf der Weboberfläche der Türsteuerung zu **Access control > Wireless locks (Zugriffssteuerung > Funkschlösser)**.
   3.2. Klicken Sie auf **Connect communication hub (Kommunikationshub verbinden)**.
   3.3. Geben Sie einen Namen für den Hub ein und klicken Sie auf **Verbinden**.
   3.4. Klicken Sie auf **Funkschloss verbinden**.
   3.5. Wählen Sie die Adresse des Schlosses sowie die Funktionen für das hinzugefügte Schloss und klicken Sie auf **Save (Speichern)**.
4. Fügen Sie die Tür hinzu und konfigurieren Sie sie mit dem Funkschloss.
   4.1. In AXIS Camera Station Pro Secure Entry gehen Sie zur **Configuration > Access control > Doors and zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen)** auf.
   4.2. Klicken Sie auf **Add door (Zugang hinzufügen)**.
   4.3. Wählen Sie die mit dem Aperio-Kommunikationshub verbundenen Türsteuerung, wählen Sie **Wireless door (Drahtloser Zugang)** als **Door type (Zugangsart)**.
   4.4. Klicken Sie auf **Next (Weiter)**.
   4.5. Wählen Sie Ihr **Funkschloss**.
   4.6. Definieren Sie die Türseiten A und B und fügen Sie Sensoren hinzu. Weitere Informationen finden Sie unter *Türen und Bereiche, on page 4*.

4.7. **Save (Speichern)** anklicken.

Nach dem Anschluss des Funkschlosses werden Akkustand und Status in der Zugangsübersicht angezeigt.

Akkustand	Aktion
Gut	Keine
Niedrig	Das Schloss funktioniert wie vorgesehen. Sie sollten den Akku jedoch ersetzen, bevor der Akkustand ein kritisches Niveau erreicht.
Kritisch	Tauschen Sie den Akku aus. Das Schloss funktioniert nicht wie vorgesehen.

Sperrstatus	Aktion
Online	Keine
Verriegelungsstau	Mechanische Probleme mit dem Schloss beheben.

Zugangsmonitor hinzufügen

Ein Zugangsmonitor ist ein Zugangspositionsschalter, der den physischen Zustand eines Zugangs überwacht. Sie können Ihrem Zugang wahlweise einen Zugangsmonitor hinzufügen und konfigurieren, wie der Zugangsmonitor angeschlossen ist.

1. Rufen Sie die Seite zur Zugangskonfiguration auf. Siehe *Hinzufügen eines Zugangs, on page 7*.
2. Klicken Sie unter **Sensors (Sensoren)** auf **Add (Hinzufügen)**.
3. Wählen Sie **Door monitor sensor (Türmonitor-Sensor)**.
4. Wählen Sie den I/O-Port aus, mit dem Sie den Zugangsmonitor verbinden möchten.
5. Wählen Sie unter **Door open if (Tür geöffnet wenn)** aus, wie die Stromkreise des Türmonitors angeschlossen sind.
6. Legen Sie eine **Debounce time (Entprellzeit)** fest, um die Statusänderungen des digitalen Eingangs zu ignorieren, bevor er einen neuen stabilen Status annimmt.
7. Um ein Ereignis auszulösen, wenn die Verbindung zwischen dem Netzwerk-Tür-Controller und dem Zugangsmonitor unterbrochen wird, aktivieren Sie **Supervised input (Überwachte Eingänge)**. Siehe *Überwachte Eingänge, on page 22*.

Tür auf, wenn	
Stromkreis geöffnet	Der Schaltkreis des Zugangsmonitors ist ein Öffner-Kontakt. Der Zugangsmonitor gibt bei offenem Schaltkreis an, dass der Zugang geöffnet ist. Der Zugangsmonitor gibt bei geschlossenem Schaltkreis an, dass der Zugang geschlossen ist.
Stromkreis geschlossen	Der Schaltkreis des Zugangsmonitors ist ein Schliesser-Kontakt. Der Zugangsmonitor gibt bei offenem Schaltkreis an, dass der Zugang geschlossen ist. Der Zugangsmonitor gibt bei geschlossenem Schaltkreis an, dass der Zugang offen ist.

Überwachten Zugang hinzufügen

Ein überwachter Zugang ist ein Zugangstyp, dessen geöffneter oder geschlossener Zustand angezeigt werden kann. Dies kann z. B. eine Brandschutztür sein: Diese benötigt kein Schloss, aber Sie müssen wissen, ob sie geöffnet ist.

Ein überwachter Zugang unterscheidet sich von einem normalen Zugang mit Monitor. Ein normaler Zugang mit Monitor unterstützt Schlösser und Kartenleser, erfordert aber eine Tür-Steuerung. Ein überwachter Zugang unterstützt einen Sensor für die Türposition, benötigt aber nur ein netzwerkbasiertes E/A-Relaismodul, das mit einer Tür-Steuerung verbunden ist. Sie können bis zu fünf Sensoren für die Türposition mit einem netzwerkbasierten E/A-Relaismodul verbinden.

Hinweis

Für einen überwachten Zugang brauchen Sie das netzwerkbasierte E/A-Relaismodul AXIS A9210 mit der neuesten Firmware und die Anwendung AXIS Monitoring Door ACAP.

Überwachten Zugang einrichten:

1. Installieren Sie AXIS A9210 und aktualisieren Sie das Gerät mit der neuesten Version von AXIS OS.
2. Installieren Sie die Sensoren für die Türposition.
3. Gehen Sie in AXIS Camera Station Pro zu **Configuration (Konfiguration)** > **Access control (Zutrittskontrolle)** > **Doors and zones (Türen und Zonen)**.
4. Klicken Sie auf **Add door (Zugang hinzufügen)**.
5. Geben Sie einen Namen ein.
6. Wählen Sie unter **Type (Typ) Monitoring door (Überwachter Zugang)** aus.
7. Wählen Sie unter **Device (Gerät)** Ihr netzwerkbasiertes E/A-Relaismodul aus.
8. Klicken Sie auf **Next (Weiter)**.
9. Klicken Sie unter **Sensors (Sensoren)** auf **Add (Hinzufügen)** und wählen Sie **Door position sensor (Sensor Türposition)** aus.
10. Wählen Sie den E/A, der mit dem Sensor für die Türposition verbunden ist.
11. Klicken Sie auf **Hinzufügen**.

Eine Etage für die Aufzugsteuerung hinzufügen BETA

Eine Etage ist ein Zugangstyp, mit dem Sie den Zugriff auf Aufzugsetagen kontrollieren. Wenn Sie eine Etage hinzufügen, erstellen Sie eine Aufzugsressource, die alle Etagen für diesen Aufzug gruppiert. Auf jeder Etage werden mithilfe eines Kartenlesegeräts in der Aufzugskabine die Benutzer authentifiziert, bevor ihnen der Zugriff zu dieser Etage gewährt wird.

Bevor Sie anfangen, ist eventuell Folgendes erforderlich:

- Ein unterstützter Netzwerk-Tür-Controller, der Ihrem System hinzugefügt wurde, wie beispielsweise *A1610*, *A1710-B* oder *A1810-B*.
- *A9910 I/O-Relais-Erweiterungsmodul* für zusätzliche Relais. Anweisung zum Hinzufügen Ihres Moduls zu einem Controller finden Sie unter .

Hinweis

Diese Funktion befindet sich in der Beta-Phase und unterstützt derzeit bis zu 16 Etagen und ausschließlich Leser.

So richten Sie eine Wiederholung ein:

1. Rufen Sie **Configuration > Access control > Doors and zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen)** auf.
2. Klicken Sie auf **Add (Hinzufügen)** und wählen Sie **Floor (Etage)** BETA.
3. Geben Sie einen Namen für die Etage ein.
4. Wählen Sie Ihren Controller aus.

5. Wählen Sie unter **Elevator (Aufzug)** einen vorhandenen Aufzug aus oder klicken Sie auf **Create new elevator (Neuen Aufzug erstellen)**, um einen neuen hinzuzufügen, und geben Sie dann einen Namen ein.
6. Wählen Sie unter **Side A (Seite A)** die Option **Card reader (Kartenleser)** aus und konfigurieren Sie Ihr Lesegerät. **Side B (Seite B)** kann aus Sicherheitsgründen nicht konfiguriert werden.
7. Klicken Sie auf **Save and add new (Speichern und neu hinzufügen)**, um weitere Etagen zum selben Aufzug hinzuzufügen. Die Konfiguration des Aufzugs und des Lesegeräts bleibt für die nächste Etage unverändert. Bitte beachten Sie, dass diese Option nur verfügbar ist, wenn Ihr Controller über Relais verfügt.
8. Klicken Sie auf **Save (Speichern)**, wenn Sie die Etage hinzugefügt haben. Die Etagen werden mit der Namenskonvention „Aufzugname – Etagenname" angezeigt. Beispiel: „Westseite – Etage 1"

Hinweis

- Lesegeräte, die auf mehreren Etagen verwendet werden, können nur auf der ersten Etage bearbeitet werden, auf der sie hinzugefügt wurden.
- Aufzüge werden automatisch gelöscht, wenn alle zugehörigen Etagen gelöscht werden.

Notfall-Eingang hinzufügen

Sie können einen Notfalleingang hinzufügen und konfigurieren, um eine Aktion zu starten, die die Tür verriegelt oder entriegelt. Sie können auch das Anschließen des Stromkreises konfigurieren.

1. Rufen Sie die Seite zur Zugangskonfiguration auf. Siehe *Hinzufügen eines Zugangs, on page 7*.
2. Klicken Sie unter **Sensors (Sensoren)** auf **Add (Hinzufügen)**.
3. Wählen Sie **Emergency input (Notfalleingang)** aus.
4. Wählen Sie unter **Emergency state (Notfallstatus)** die Stromkreisverbindung aus.
5. Legen Sie eine **Debounce time (ms) (Entprellzeit(ms))** fest, um die Statusänderungen des digitalen Eingangs zu ignorieren, bevor er einen neuen stabilen Status annimmt.
6. Wählen Sie aus, welche **Emergency action (Notfall-Aktion)** beim Empfang des Ausnahmezustandssignal ausgelöst wird.

Ausnahmezustand	
Stromkreis geöffnet	Der Schaltkreis für den Notfall-Eingang ist ein Öffner-Kontakt. Der Notfall-Eingang sendet das Signal für den Ausnahmezustand, wenn der Schaltkreis geöffnet ist.
Stromkreis geschlossen	Der Schaltkreis für den Notfall-Eingang ist ein Schliesser-Kontakt. Der Notfall-Eingang sendet das Signal für den Ausnahmezustand, wenn der Schaltkreis geschlossen ist.

Notfall-Aktion	
Tür entriegeln	Die Tür wird entriegelt, wenn sie das Signal für den Ausnahmezustand empfängt.
Tür verriegeln	Die Tür wird verriegelt, wenn sie das Signal für den Ausnahmezustand empfängt.

IP-Leser hinzufügen

Sie können eine Axis Netzwerk-Türsprechanlage oder ein anderes IP-fähiges Gerät als Leser verwenden. Bevor Sie das Gerät einem Zugang zuweisen können, müssen Sie es in AXIS Camera Station Pro hinzufügen.

Hinweis

Stellen Sie sicher, dass der IP-Leser eingeschaltet und mit demselben Netzwerk wie AXIS Camera Station Pro verbunden ist, bevor Sie beginnen.

1. Gehen Sie zu **Configuration (Konfiguration) > Devices (Geräte) > Add devices (Geräte hinzufügen)**.
2. Wählen Sie Ihren IP-Leser aus der Liste der erkannten Geräte aus und klicken Sie auf **Add (hinzufügen)**.
3. Geben Sie die Zugangsdaten des Geräts ein, wenn Sie dazu aufgefordert werden.

Sobald das Gerät hinzugefügt wurde, können Sie es einem Zugang zuweisen. Siehe dazu *Leser hinzufügen, on page 17*.

Leser hinzufügen

Sie können eine Tür-Steuerung zum Verwenden von mehreren kabelgebundenen Lesern konfigurieren. Wählen Sie einen Leser für eine oder für beide Seiten eines Zugangs.

Wenn ein benutzerdefiniertes Setup von Kartenformaten oder PIN-Längen auf einen Leser angewendet wird, wird dieses in **Card formats (Kartenformate)** unter **Configuration > Access control > Doors and zones (Konfiguration > Zutrittskontrolle > Zugänge und Zonen)** deutlich angezeigt. Siehe *Türen und Bereiche, on page 4*.

Hinweis

- Sie können auch bis zu 16 Bluetooth-Leser zu einer Tür-Steuerung hinzufügen. Weitere Informationen finden Sie unter *Bluetooth-Leser hinzufügen, on page 18*.
- Wenn Sie eine Axis Netzwerk-IP-Türsprechanlage als IP-Leser verwenden, nutzt das System die auf der Webseite des Geräts eingestellte PIN-Konfiguration.

1. Rufen Sie die Seite zur Zugangskonfiguration auf. Siehe *Hinzufügen eines Zugangs, on page 7*.
2. Klicken Sie für eine Seite des Zugangs auf **Add (Hinzufügen)**.
3. Wählen Sie **Card reader (Kartenleser)**.
4. Wählen Sie unter **Reader type (Lesertyp)** die gewünschte Option aus.
5. So verwenden Sie ein benutzerdefiniertes Setup der PIN-Länge für diesen Leser.
   5.1. Klicken Sie auf **Erweitert**.
   5.2. Aktivieren Sie **Custom PIN length (Benutzerdefinierte PIN-Länge)**.
   5.3. Legen Sie Werte für **Min PIN length (Min. PIN-Länge)**, **Max PIN length (Max. PIN-Länge)** und **End of PIN character (Ende des PIN-Zeichens)** fest.
6. So verwenden Sie ein benutzerdefiniertes Kartenformat für diesen Leser.
   6.1. Klicken Sie auf **Erweitert**.
   6.2. Aktivieren Sie **Custom card formats (Benutzerdefinierte Kartenformate)**.
   6.3. Wählen Sie die Kartenformate, die Sie für den Leser verwenden möchten. Wenn bereits ein Kartenformat mit der gleichen Bitlänge verwendet wird, müssen Sie es zuerst deaktivieren. Ein Warnsymbol wird auf dem Client angezeigt, wenn sich das Kartenformat von der konfigurierten Systemkonfiguration unterscheidet.
7. Klicken Sie auf **Hinzufügen**.
8. Um einen Leser zur anderen Türseite hinzuzufügen, dieses Verfahren erneut verwenden.

Informationen zur Installation eines AXIS-Barcodelesers finden Sie unter *AXIS Barcode Reader installieren, on page 29*.

Lesertyp	
OSDP RS485 Halbduplex	Wählen Sie für RS485-Leser **OSDP RS485 half duplex (OSDP RS485-Halbduplex-Betrieb)** und einen Leserport aus.

Wiegand	Wählen Sie für Leser, die Wiegand-Protokolle verwenden, die Option **Wiegand** und einen Leserport aus.
IP-Leser	Wählen Sie für IP-Leser die Option **IP reader (IP-Leser)** und wählen Sie im Drop-Down Menü ein Gerät aus. Die IP-Türsprechanlagen von Axis können als IP-Leser verwendet werden.

Wiegand	
LED-Steuerung	Wählen Sie entweder **Single wire (Einzelner Draht)** oder **Dual wire (R/G) (Doppeldraht (R/G))** aus. Leser mit einer dualen LED-Steuerung verwenden verschiedene Adern für die roten und grünen LEDs.
Manipulationsalarm	Wählen Sie aus, wann der Manipulationseingang des Lesers aktiv ist. • **Open circuit (Offener Stromkreis)**: Der Leser übermittelt dem Zugang das Manipulationssignal, wenn der Schaltkreis geöffnet ist. • **Closed circuit (Geschlossener Stromkreis)**: Der Leser übermittelt dem Zugang das Manipulationssignal, wenn der Schaltkreis geschlossen ist.
Tamper debounce time (Entprellzeit)	Legen Sie eine **Tamper debounce time (Entprellzeit Manipulation)** fest, um die Statusänderungen des Manipulationseingangs des Lesers zu ignorieren, bevor er einen neuen stabilen Status annimmt.
Überwachter Eingang	Um ein Ereignis auszulösen, wenn die Verbindung zwischen dem Netzwerk-Zugangscontroller und dem Leser unterbrochen wird, aktivieren Sie dies. Siehe *Überwachte Eingänge, on page 22*.

Bluetooth-Leser hinzufügen

Mit dem AXIS A4612 Network Bluetooth Reader können Sie die Beschränkungen der kabelgebundenen Tür-Steuerungen von Axis überwinden und bis zu 16 dieser Leser einer eigenen Tür zuweisen. Jeder Leser unterstützt die Verwaltung von Türschloss, Request-to-Exit-Gerät (REX) und Türpositionsschalter (Door Position Switch, DPS).

Für das Hinzufügen und die Verwendung dieser Leser sind keine zusätzlichen Lizenzen erforderlich.

So fügen Sie einen AXIS A4612 Network Bluetooth Reader zu einer Tür hinzu:

1. Stellen Sie sicher, dass der AXIS A4612 mit der Tür-Steuerung gekoppelt ist. Siehe *App AXIS Mobile Credential als Bluetooth-Zugangsdaten verwenden, on page 19*.
2. Rufen Sie die Seite zur Zugangskonfiguration auf. Siehe *Hinzufügen eines Zugangs, on page 7*.
3. Klicken Sie unter einer Seite der Tür auf **Add (Hinzufügen)** und wählen Sie dann **Card reader (Kartenleser)** aus.
4. Wählen Sie **IP reader (IP-Leser)** und anschließend den gekoppelten AXIS A4612 aus der Drop-down-Liste aus. Wenn dieser Leser für die Zugangsdaten zur Kopplung verwendet werden soll, markieren Sie ihn für die Kopplung. Klicken Sie auf **Hinzufügen**.

5. Ändern Sie auf der Registerkarte **Overview (Übersicht)** das Identifizierungsprofil. Sie können die Profile **Tap in app (In App tippen)** oder **Touch Reader (Kartenleser berühren)** verwenden, wenn Sie den AXIS A4612 nur auf einer Seite der Tür angebracht haben und auf der anderen Seite ein REX-Gerät verwenden.

App AXIS Mobile Credential als Bluetooth-Zugangsdaten verwenden

In diesem Beispiel wird gezeigt, wie Sie den Bluetooth-Kartenleser AXIS A4612 zu Ihrem System hinzufügen, damit Karteninhaber Zugänge mit der App AXIS Mobile Credential entriegeln können.

1. Installieren Sie den Bluetooth-Kartenleser und verbinden Sie ihn mit einer Tür-Steuerung.
2. Fügen Sie den Bluetooth-Kartenleser in der Web-Oberfläche der Tür-Steuerung hinzu.
   2.1. Rufen Sie die Tür-Steuerung auf und gehen Sie zu **Peripherals (Peripheriegeräte)** > **Readers (Kartenleser)**.
   2.2. Klicken Sie auf **Add reader (Kartenleser hinzufügen)**.
   2.3. Geben Sie im Dialog **Add Bluetooth reader (Bluetooth-Kartenleser hinzufügen)** die erforderlichen Informationen ein.
   2.4. Klicken Sie auf **Hinzufügen**.
3. Fügen Sie den Bluetooth-Kartenleser in AXIS Camera Station Pro einem Zugang hinzu.
   3.1. Rufen Sie **Configuration** > **Access control** > **Doors and zones** (Konfiguration > Zutrittskontrolle > Zugang und Zonen) auf.
   3.2. Wählen Sie den Zugang aus, dem der Bluetooth-Kartenleser hinzugefügt werden soll, und klicken Sie auf **Edit (Bearbeiten)**.
   3.3. Klicken Sie neben dem Zugang, an dem sich der Bluetooth-Kartenleser befindet, auf **+ Add (Hinzufügen)**.
   3.4. Wählen Sie **Card reader (Kartenleser)**.
   3.5. Wählen Sie unter **Add IP reader (IP-Leser hinzufügen) IP-Leser** aus.
   3.6. Wählen Sie unter **IP-Kartenleser** Ihren Bluetooth-Kartenleser aus.
   3.7. Klicken Sie auf **Hinzufügen**.
4. Wählen Sie den zu koppelnden Bluetooth-Kartenleser aus. Dies müssen Sie für mindestens einen Bluetooth-Kartenleser in Ihrem System tun.
   4.1. Wählen Sie den soeben hinzugefügten Bluetooth-Kartenleser aus.
   4.2. Klicken Sie auf **Edit (Bearbeiten)**.
   4.3. Wählen Sie unter **Edit bluetooth reader (Bluetooth-Kartenleser bearbeiten) Use this reader for pairing (Diesen Kartenleser zum Koppeln verwenden)** aus.
   4.4. Klicken Sie auf **Anwenden**.
5. Wählen Sie als Identifizierungsprofil **Tap in app (In App tippen)** oder **Touch reader (Kartenleser berühren)** aus. Weitere Informationen finden Sie unter *Identifizierungsprofile, on page 23*.
6. Fügen Sie dem Karteninhaber die mobilen Zugangsdaten hinzu. Siehe *Zugangsdaten hinzufügen, on page 35*.
7. Koppeln Sie die mobilen Zugangsdaten mit dem gekoppelten Kartenleser.
   7.1. Bringen Sie das Mobiltelefon des Karteninhabers zum Bluetooth-Kartenleser, an dem das Koppeln aktiviert sein muss.
   7.2. Befolgen Sie die Anweisungen in der E-Mail an den Karteninhaber.

REX-Gerät hinzufügen

Sie können ein REX-Gerät auf einer oder auf beiden Seiten des Zugangs hinzufügen. Ein REX-Gerät kann ein PIR-Sensor, eine REX-Taste oder eine Druckstange sein.

1. Rufen Sie die Seite zur Zugangskonfiguration auf. Siehe *Hinzufügen eines Zugangs, on page 7*.
2. Klicken Sie für eine Seite des Zugangs auf **Add (Hinzufügen)**.
3. **REX device (REX-Gerät)** auswählen.
4. Wählen Sie den I/O-Port aus, mit dem Sie das REX-Gerät verbinden möchten. Wenn nur ein Port verfügbar ist, wird dieser Port automatisch ausgewählt.
5. Wählen Sie aus, welche **Action (Aktion)** beim Empfang des REX-Signals von der Tür ausgelöst werden soll.
6. Wählen Sie unter **REX active (REX aktiv)** aus, wie die Schaltkreise des Zugangsmonitors angeschlossen sind.
7. Legen Sie eine **Debounce time (ms) (Entprellzeit(ms))** fest, um die Statusänderungen des digitalen Eingangs zu ignorieren, bevor er einen neuen stabilen Status annimmt.
8. Um ein Ereignis auszulösen, wenn die Verbindung zwischen dem Netzwerk-Tür-Controller und dem REX-Gerät unterbrochen wird, aktivieren Sie **Supervised input (Überwachte Eingänge)**. Siehe *Überwachte Eingänge, on page 22*.

Aktion	
Tür entriegeln	Wählen Sie diese Option aus, um die Tür zu entriegeln, wenn sie das REX-Signal empfängt.
Keine	Wählen Sie diese Option aus, wenn Sie beim Empfang des REX-Signals keine Aktion von der Tür auslösen möchten.

REX aktiv	
Stromkreis geöffnet	Wählen Sie aus, ob der REX-Schaltkreis ein Öffner-Kontakt ist. Das REX-Gerät sendet das Signal, wenn der Schaltkreis geöffnet ist.
Stromkreis geschlossen	Wählen Sie aus, ob der REX-Schaltkreis ein Schliesser-Kontakt ist. Das REX-Gerät sendet das Signal, wenn der Schaltkreis geschlossen ist.

Zone hinzufügen

Eine Zone ist ein bestimmter physischer Bereich mit einer Gruppe von Zugängen. Sie können Zonen erstellen und den Zonen Zugänge hinzufügen. Es gibt zwei Arten von Türen:

- **Perimeter door (Umgrenzungszugang):** : Karteninhaber betreten oder verlassen die Zone durch diesen Zugang.
- **Internal door (Interner Zugang):** : Ein interner Zugang innerhalb der Zone.

Hinweis

Ein Umgrenzungszugang kann zu zwei Zonen gehören. Ein interner Zugang kann nur zu einer Zone gehören. Eine Übersicht finden Sie unter *Beispiel für Zugänge und Zonen, on page 7*.

1. Rufen Sie **Configuration > Access control > Door and zones > Zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen > Zonen)** auf.
2. Klicken Sie auf + **Add zone (Zone hinzufügen)**.
3. Geben Sie einen Zonennamen ein.
4. Klicken Sie auf **Add door (Zugang hinzufügen)**.
5. Wählen Sie die Türen aus, die Sie der Zone hinzufügen möchten, und klicken Sie auf **Add (Hinzufügen)**.

6. Der Zugang ist standardmäßig ein Umgrenzungszugang. Um das zu ändern, wählen Sie im Aufklappmenü die Option **Internal door (Interner Zugang)** aus.
7. Ein Umgrenzungszugang verwendet standardmäßig die Türseite A als Eingang zur Zone. Um das zu ändern, wählen Sie im Drop-Down Menü die Option **Leave (Verlassen)** aus.
8. Um eine Tür aus der Zone zu entfernen, wählen Sie diese aus und klicken Sie auf **Remove (Entfernen)**.
9. **Save (Speichern)** anklicken.

Zum Bearbeiten einer Zone:

1. Rufen Sie **Configuration > Access control > Door and zones > Zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen > Zonen)** auf.
2. Eine Kamera aus der Liste wählen.
3. Klicken Sie auf **Edit (Bearbeiten)**.
4. Ändern Sie die Einstellungen und klicken Sie auf **Save (Speichern)**.

So entfernen Sie eine Zone:

1. Rufen Sie **Configuration > Access control > Door and zones > Zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen > Zonen)** auf.
2. Eine Kamera aus der Liste wählen.
3. Klicken Sie auf **Remove (Entfernen)**.
4. **Yes (Ja)** anklicken

Sicherheitsstufe der Zone

Sie können einer Zone die folgenden Sicherheitsfunktion hinzufügen:

Anti-Passback – Diese Funktion verhindert, dass eine Person die gleichen Zugangsdaten verwenden kann wie jemand, der bereits vor ihr einen Bereich betreten hat. Dadurch wird gewährleistet, dass eine Person den Bereich zuerst verlassen muss, bevor sie ihre Zugangsdaten erneut verwenden kann.

Hinweis

- Für die Anti-Passback-Funktion empfehlen wir den Einsatz von Zugangspositionssensoren an allen Zugängen in der Zone, damit das System registrieren kann, dass ein Benutzer den Zugang nach dem Durchziehen seiner Karte auch wirklich geöffnet hat.
- Wenn eine Tür-Steuerung offline geht, funktioniert Anti-Passback so lange, wie alle Zugänge in der Zone zu derselben Tür-Steuerung gehören. Wenn die Zugänge in der Zone jedoch zu verschiedenen Tür-Steuerungen gehören, die offline gehen, funktioniert Anti-Passback nicht mehr.

Sie können die Sicherheitsstufe konfigurieren, während Sie eine neue Zone hinzufügen, oder Sie können die Konfiguration für eine vorhandene Zone durchführen. So fügen Sie einer vorhandenen Zone eine Sicherheitsstufe hinzu:

1. Rufen Sie **Configuration** > **Access control** > **Doors and zones** (Konfiguration > Zutrittskontrolle > Zugang und Zonen) auf.
2. Wählen Sie die Zone aus, für die Sie eine Sicherheitsstufe konfigurieren möchten.
3. Klicken Sie auf **Edit (Bearbeiten)**.
4. Klicken Sie auf **Security level (Sicherheitsstufe)**.
5. Schalten Sie die Sicherheitsfunktionen ein, die Sie dem Zugang hinzufügen möchten.
6. Klicken Sie auf **Anwenden**.

Anti-Passback	
Log violation only (Soft) (Nur Verstoß protokollieren (Soft))	Verwenden Sie diese Option, um einer zweiten Person den Zutritt mit den gleichen Zugangsdaten wie die

	erste Person zu gestatten. Diese Option löst lediglich einen Systemalarm aus.
Deny access (Hard) (Zutritt verweigern (Hard))	Verwenden Sie diese Option, um zu verhindern, dass der zweite Benutzer mit den gleichen Zugangsdaten wie die erste Person den Zugang verwendet. Diese Option löst ebenfalls einen Systemalarm aus.
Zeitüberschreitung (Sekunden)	Die Zeitspanne, bis das System einem Benutzer erneut den Zutritt gewährt. Geben Sie 0 ein, wenn Sie keine Zeitüberschreitung verwenden möchten. Für die Zone gilt dann Anti-Passback, bis der Benutzer die Zone verlässt. Verwenden Sie für die Zeitüberschreitung den Wert **0** nur dann zusammen mit **Deny access (Hard) (Zutritt verweigern (Hard))**, wenn alle Zugänge in der Zone auf beiden Seiten über Leser verfügen.

Überwachte Eingänge

Überwachte Eingänge können bei Unterbrechung der Verbindung mit einer Tür-Steuerung ein Ereignis auslösen.

- Verbindung zwischen Tür-Controller und Türmonitor. Siehe *Zugangsmonitor hinzufügen, on page 14*.
- Verbindung zwischen dem Tür-Controller und dem Leser, der Wiegand-Protokolle verwendet. Siehe *Leser hinzufügen, on page 17*.
- Verbindung zwischen Tür-Controller und REX-Gerät. Siehe *REX-Gerät hinzufügen, on page 19*.

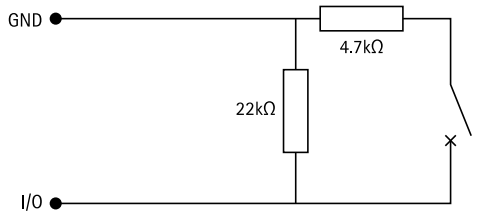
Um überwachte Eingänge zu verwenden:

1. Installieren Sie, wie im Anschlussschaltbild dargestellt, Abschlusswiderstände so nah wie möglich am Peripheriegerät.
2. Gehen Sie zur Konfigurationsseite eines Lesers, eines Zugangsmonitors oder eines REX-Geräts und aktivieren Sie **Supervised input (Überwachte Eingänge)**.
3. Wenn Sie nach dem Schaltplan für eine Parallelschaltung vorgegangen sind, wählen Sie **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Parallelschaltung mit einem parallelen Widerstand (22 KΩ) und einem seriellen Widerstand (4,7 KΩ))**.
4. Wenn Sie nach dem Schaltplan für eine Serienschaltung vorgegangen sind, wählen Sie **Serial first connection (Serienschaltung)** und im Drop-Down Menü **Resistor values (Widerstandswerte)** einen Widerstandswert.

Anschlussschaltbilder

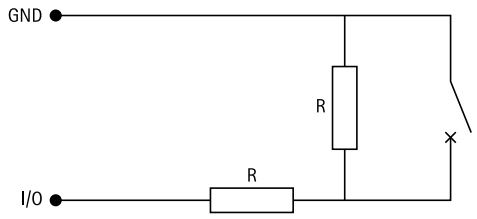
Paralleler Anschluss hat Vorrang

Die Widerstandswerte müssen 4,7 kΩ und 22 kΩ betragen.



Serielle erste Verbindung

Die Widerstandswerte müssen identisch sein und zwischen 1 und 10 kΩ liegen.



Identifizierungsprofile

Ein Identifizierungsprofil ist eine Kombination aus Identifikationsarten und Zeitplänen. Sie können ein Identifizierungsprofil auf einen oder mehrere Zugänge anwenden, um festzulegen, wie und wann ein Karteninhaber einen bestimmten Zugang nutzen kann.

Hinweis

Dynamische QR und PIN müssen zusammen verwendet werden.

Rufen Sie **Configuration > Access control > Identification profiles (Konfiguration > Zutrittskontrolle > Identifizierungsprofile)** auf, um Identifizierungsprofile zu erstellen, zu bearbeiten oder zu entfernen.

Die verfügbaren Identifizierungsprofile:

Karte – Karteninhaber müssen die Karte durch einen angeschlossenen Leser ziehen, um Zutritt zum Zugang zu erhalten.

Karte und PIN – Karteninhaber müssen die Karte durch einen angeschlossenen Leser ziehen und die PIN eingeben, um Zutritt zum Zugang zu erhalten.

PIN – Karteninhaber müssen die PIN eingeben, um Zutritt zum Zugang zu erhalten.

Karte oder PIN – Karteninhaber müssen die Karte durch einen angeschlossenen Leser ziehen oder die PIN eingeben, um Zutritt zum Zugang zu erhalten.

QR – Karteninhaber müssen für den Zugriff auf den Zugang der Kamera den QR-Code® zeigen. Sie können das QR-Identifizierungsprofil sowohl für statische als auch für dynamische QR verwenden.

Nummernschild – Karteninhaber müssen mit einem Fahrzeug mit zugelassenem Fahrzeugkennzeichen auf die Kamera zufahren.

Antippen in der App – Karteninhaber müssen den Ausweis in der AXIS Camera Station Mobile App antippen, während sie sich in Reichweite des Bluetooth-Lesers befinden.

Leser berühren – Karteninhaber müssen den Bluetooth-Leser berühren, während sie ein Mobiltelefon mit mobilen Zugangsdaten bei sich tragen.

*QR Code ist eine eingetragene Marke von Denso Wave Incorporated in Japan und anderen Ländern.

Erstellen eines Identifizierungsprofils

1. Rufen Sie **Configuration > Access control > Identification profiles (Konfiguration > Zutrittskontrolle > Identifizierungsprofile)** auf.
2. Klicken Sie auf **Create identification profile (Identifizierungsprofil erstellen)**.
3. Geben Sie einen Namen für das Identifizierungsprofil ein.
4. Wählen Sie **Include facility code for card validation (Gebäude-Zugangscode in Kartenprüfung einbeziehen)** aus, um den Gebäude-Zugangscode als eines der Felder für das Überprüfen von Anmeldedaten zu verwenden. Dieses Feld ist nur verfügbar, wenn Sie **Facility code (Gebäude-Zugangscode)** unter **Access management > Settings (Zugriffsverwaltung > Einstellungen)** eingeschaltet haben.
5. Für Seite A klicken Sie auf **+ Add (+ Hinzufügen)**, wählen Sie eine Identifikationsart und einen Zeitplan aus.

- Wenn Sie von Karteninhabern verlangen möchten, dass sie mehr als eine Identifikationsart verwenden, wählen Sie mehrere Typen in derselben Zeile aus.
- Damit Karteninhaber beide Typen nutzen können, klicken Sie erneut auf **+ Add (+ Hinzufügen)** und fügen Sie eine weitere Zeile hinzu.

6. Für Seite B klicken Sie auf **+ Add (+ Hinzufügen)**, wählen Sie eine Identifikationsart und einen Zeitplan aus.
7. Klicken Sie auf **OK**.

Einrichten von Identifizierungsprofilen

Bearbeiten eines Identifizierungsprofils

1. Rufen Sie **Configuration > Access control > Identification profiles (Konfiguration > Zutrittskontrolle > Identifizierungsprofile)** auf.
2. Wählen Sie ein Identifizierungsprofil aus und klicken Sie auf .
3. Ändern Sie den Namen des Identifizierungsprofils, indem Sie einen neuen Namen eingeben.
4. Bearbeiten Sie die Einstellungen für die Seite des Zugangs.
5. Um das Identifizierungsprofil auf der anderen Seite des Zugangs zu bearbeiten, wiederholen Sie die vorherigen Schritte.
6. Klicken Sie auf **OK**.

Identifizierungs Profil bearbeiten	
×	Gehen Sie wie folgt vor, um eine Identifikationsart und den zugehörigen Zeitplan zu entfernen.
Identifizierung	Um eine Identifikationsart zu ändern, wählen Sie aus dem Drop-Down Menü **Identification type (Identifikationsart)** eine oder mehrere Identifikationsarten aus.
Zeitschema	Um einen Zeitplan zu ändern, wählen Sie aus dem Drop-Down Menü **Schedule (Zeitplan)** einen oder mehrere Zeitpläne aus.
+ **Hinzufügen**	Fügen Sie eine Identifikationsart und den zugehörigen Zeitplan hinzu, indem Sie auf **Add (Hinzufügen)** klicken und die Identifikationsarten und Zeitpläne festlegen.

Entfernen eines Identifizierungsprofil

1. Rufen Sie **Configuration > Access control > Identification profiles (Konfiguration > Zutrittskontrolle > Identifizierungsprofile)** auf.
2. Wählen Sie ein Identifizierungsprofil aus und klicken Sie auf .

3. Wenn das Identifizierungsprofil für einen Zugang verwendet wird, wählen Sie für den Zugang ein anderes Identifizierungsprofil aus.
4. Klicken Sie auf **OK**.

Zurücksetzten eines vordefinierten Kartenformats

1. Rufen Sie **Configuration > Access Control > Card formats and PIN (Konfiguration > Zutrittskontrolle > Kartenformate und PIN)** auf.
2. Klicken Sie auf , um ein Kartenformat auf die Standardfeldzuordnung zurückzusetzen.

Kartenformate und PIN

Das Kartenformat legt fest, wie ein Leser die Daten einer Karte interpretiert. Es stehen vordefinierte Kartenformate zur Verfügung, die Sie verwenden oder bearbeiten können. Außerdem haben Sie die Möglichkeit, eigene Kartenformate zu erstellen.

Rufen Sie **Configuration > Access Control > Card formats and PIN (Konfiguration > Zutrittskontrolle > Kartenformate und PIN)** auf, um Kartenformate zu erstellen, zu bearbeiten oder zu aktivieren. Sie können auch eine PIN konfigurieren.

Die benutzerdefinierten Kartenformate können die folgenden Datenfelder enthalten, die zur Überprüfen von Anmeldedaten verwendet werden.

Kartennummer – Eine Teilmenge der binären Zugangsdaten, die als Dezimal- oder Hexadezimalzahlen codiert ist. Verwenden Sie die Kartennummer, um eine bestimmte Karte oder einen bestimmten Karteninhaber zu identifizieren.

Einrichtungscode – Eine Teilmenge der binären Zugangsdaten, die als Dezimal- oder Hexadezimalzahlen codiert ist. Verwenden Sie den Gebäude-Zugangscode, um einen bestimmten Endkunden oder Standort zu identifizieren.

PIN-Konfiguration

1. Rufen Sie **Configuration > Access Control > Card formats and PIN (Konfiguration > Zutrittskontrolle > Kartenformate und PIN)** auf.
2. Klicken Sie unter **PIN configuration (PIN-Konfiguration)** auf .
3. Legen Sie **Min PIN length (Min. PIN-Länge)**, **Max PIN length (Max. PIN-Länge)** und **End of PIN character (Ende des PIN-Zeichens)** fest.
4. Klicken Sie auf **OK**.

Erstellen eines Kartenformats

1. Rufen Sie **Configuration > Access Control > Card formats and PIN (Konfiguration > Zutrittskontrolle > Kartenformate und PIN)** auf.
2. **Add card format (Kartenformat hinzufügen)** aufrufen.
3. Geben Sie einen Namen für das Kartenformat ein.
4. Geben Sie im **Feld für die Bitlänge** eine Zahl zwischen 1 und 256 ein.
5. Wählen Sie **Invert bit order (Bit-Reihenfolge invertieren)** aus, falls Sie die Bit-Reihenfolge der vom Kartenleser empfangenen Daten umkehren möchten.
6. Wählen Sie **Invert byte order (Byte-Reihenfolge umkehren)** aus, falls Sie die Byte-Reihenfolge der vom Kartenleser empfangenen Daten umkehren möchten. Diese Option ist nur verfügbar, wenn Sie eine Bitlänge angeben, die man durch acht teilen kann.
7. Wählen Sie die Datenfelder aus und konfigurieren Sie sie so, dass sie im Kartenformat aktiv sind. Entweder **Card number (Kartennummer)** oder **Facility code (Gebäude-Zugangscode)** muss im Kartenformat aktiv sein.

8. Klicken Sie auf **OK**.
9. Um das Kartenformat zu aktivieren, aktivieren Sie das Kontrollkästchen vor dem Namen des Kartenformats.

Hinweis

- Zwei Kartenformate mit der gleichen Bitlänge können nicht gleichzeitig aktiviert sein. Wenn Sie beispielsweise zwei Kartenformate mit 32 Bit definiert haben, kann nur eines davon aktiv sein. Deaktivieren Sie das Kartenformat, um das andere zu aktivieren.
- Kartenformate können nur aktiviert oder deaktiviert werden, wenn der Netzwerk-Tür-Controller im System mit mindestens einem Leser konfiguriert wurde.
- Die vordefinierten Kartenformate können bearbeitet, aber nicht gelöscht werden. Um Änderungen an einem vordefinierten Format rückgängig zu machen, klicken Sie auf das Symbol „Zurücksetzen", um die Standardeinstellungen wiederherzustellen. Von Ihnen erstellte Kartenformate können gelöscht werden.

ⓘ	Klicken Sie auf ⓘ, um ein Beispiel für die Ausgabe nach dem Invertieren der Bit-Reihenfolge anzuzeigen.
Bereich	Legen Sie den Bitbereich der Daten für das Datenfeld fest. Der Bereich muss innerhalb der Werte liegen, die Sie für **Bit length of card reader message (Bitlänge der Kartenleser-Nachricht)** angegeben haben.
Ausgabeformat	Wählen Sie das Ausgabeformat der Daten für das Datenfeld aus. **Decimal (Dezimal)**: Dieses System ist auch als Stellenwertsystem mit der Basiszahl 10 bekannt und besteht aus den Zahlen 0–9. **Hexadecimal (Hexadezimal)**: Dieses System ist ein Stellenwertsystem mit der Basiszahl 16 und verwendet 16 eindeutige Zeichen: die Ziffern 0 bis 9 und die Buchstaben a bis f.
Bit-Reihenfolge des Teilbereichs	Wählen Sie die Bit-Reihenfolge aus. **Little endian (Little-Endian)**: Das erste Bit ist das kleinste (mit der geringsten Bedeutung). **Big endian (Big-Endian)**: Das erste Bit ist das größte (mit der größten Bedeutung).

Rufen Sie zur Wiedergabe dieses Videos die Webversion dieses Dokuments auf.

Einrichten von Kartenformaten

Bearbeiten eines Kartenformats

1. Rufen Sie **Configuration > Access Control > Card formats and PIN (Konfiguration > Zutrittskontrolle > Kartenformate und PIN)** auf.
2. Wählen Sie ein Kartenformat aus und klicken Sie auf ✎.

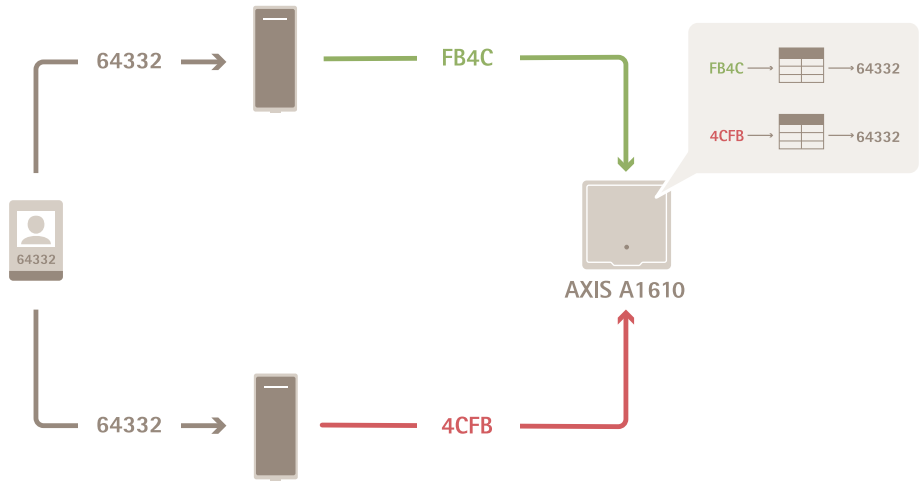
3. Wenn Sie ein vordefiniertes Kartenformat bearbeiten, können Sie nur **Invert bit order (Bit-Reihenfolge invertieren)** und **Invert byte order (Byte-Reihenfolge umkehren)** bearbeiten.
4. Klicken Sie auf **OK**.

Sie können nur die benutzerdefinierten Kartenformate entfernen. So entfernen Sie ein benutzerdefiniertes Kartenformat:

1. Rufen Sie **Configuration > Access Control > Card formats and PIN (Konfiguration > Zutrittskontrolle > Kartenformate und PIN)** auf.
2. Wählen Sie ein benutzerdefiniertes Kartenformat aus, klicken Sie auf und dann auf **Yes (Ja)**.

Einstellungen für das Kartenformat

Übersicht



- Die Kartennummer in Dezimalstellen lautet `64332`.
- Ein Leser wandelt die Kartennummer an die Hexadezimalzahl `FB4C` um. Der andere Leser wandelt sie in die Hexadezimalzahl `4CFB` um.
- Der AXIS A1610 Network Door Controller empfängt die Hexadezimalzahl `FB4C` und wandelt sie entsprechend den auf den Leser angewendeten Kartenformateinstellungen in die Dezimalzahl `64332` um.
- Der AXIS A1610 Network Door Controller empfängt die Hexadezimalzahl `4CFB`, ändert sie durch Umkehrung der Byte-Reihenfolge in `FB4C` und wandelt sie entsprechend den auf den Leser angewendeten Kartenformateinstellungen in die Dezimalzahl `64332` um.

Bit-Reihenfolge umkehren

Nach dem Umkehren der Bit-Reihenfolge werden die vom Leser empfangenen Kartendaten Bit für Bit von rechts nach links ausgelesen.

Byte-Reihenfolge umkehren

Eine Gruppe von acht Bits ist ein Byte. Nach dem Umkehren der Byte-Reihenfolge werden die vom Leser empfangenen Kartendaten Byte für Byte von rechts nach links ausgelesen.

26-Bit-Standard-Wiegand-Kartenformat

1 *Führende Parität*
2 *Einrichtungscode*
3 *Kartennummer*
4 *Angehängte Parität*

Verschlüsselte Kommunikation

OSDP mit Secure Channel

AXIS Camera Station Secure Entry unterstützt OSDP (Open Supervised Device Protocol) Secure Channel, um die Zeilenverschlüsselung zwischen Controller und Axis Lesegeräten zu ermöglichen.

So aktivieren Sie OSDP Secure Channel für ein gesamtes System:

1. Gehen Sie zu **Konfiguration > Zutrittskontrolle > Verschlüsselte Kommunikation**.
2. Geben Sie den Hauptverschlüsselungsschlüssel an und klicken Sie auf **OK**.
3. **OSDP Secure Channel** aktivieren. Diese Option ist nur verfügbar, nachdem Sie den Hauptverschlüsselungsschlüssel eingegeben haben.
4. Standardmäßig wird der OSDP Secure Channel-Schlüssel vom Hauptverschlüsselungsschlüssel generiert. So legen Sie den OSDP Secure Channel-Schlüssel manuell fest:
   4.1. Klicken **Sie unter OSDP Secure Channel** (Sicherer Kanal) auf .
   4.2. **Hauptverschlüsselungsschlüssel zum Generieren des Schlüssels für OSDP mit Secure Channel verwenden**entfernen.
   4.3. Geben Sie den OSDP Secure Channel-Schlüssel ein und klicken Sie auf **OK**.

Informationen zum Aktivieren oder Deaktivieren von OSDP Secure Channel für ein bestimmtes Lesegerät finden Sie unter *Zugänge und Zonen*.

Hinweis

Falls die Zutrittskontrolleinheit, der Host oder das Bedienfeld den OSDP-Sicherheitskanal unterstützt, empfehlen wir Ihnen, diesen auf dem Leser zu aktivieren, um die Kommunikationssicherheit zu erhöhen. Um einen sicheren Kanal zu gewährleisten, setzen Sie den DIP-Schalter Nr. 6 am Leser auf „Ein“.

Der Verschlüsselungsschlüssel wird bei der Ersteinrichtung im Klartext übertragen, daher sollten alle RS485-Verbindungen und -Geräte während dieses Vorgangs überwacht werden.

AXIS Barcode Reader

AXIS Barcode Reader ist eine Anwendung, die auf Axis Kameras installiert werden kann. Der Axis Tür-Controller nutzt den externen Peripherie-Authentifizierungsschlüssel, um den Zugriff zu gewähren und den AXIS Barcodeleser sowie den AXIS License Plate Verifier zu authentifizieren. Für einen vollständigen Workflow zum Einrichten von AXIS License Plate Verifier in AXIS Camera Station Pro, siehe .

AXIS Barcode Reader installieren

1. Laden Sie die Installationsdatei für die Anwendung von *axis.com* herunter
2. Gehen Sie zur Webseite zu Ihrer Axis IP-Türsprechanlage oder Kamera.
3. Installieren Sie die Anwendung.
4. Die Lizenz aktivieren.
5. Starten Sie die Anwendung.
6. Wir empfehlen Ihnen, folgende Kameraeinstellung für eine höhere QR-Genauigkeit zu ändern.
   6.1. Gehen Sie zu Kameraeinstellungen.
   6.2. Bewegen Sie unter **Bild > Belichtung**den Schieberegler **Kompromiss Rauschen zu Bewegungsunschärfe** in die Mitte.

AXIS Barcode Reader konfigurieren

1. Um die QR-Zugangsdaten zu ändern, gehen Sie zu **Configuration > Access control > Identification profiles (Konfiguration > Zutrittskontrolle > Identifizierungsprofile)** und klicken Sie auf . Siehe dazu *Identifizierungsprofile*.
2. Fügen Sie einen Zugang hinzu. Siehe hierzu *Zugang hinzufügen*.
3. Wählen Sie **QR** als Identifizierungsprofil für diesen Zugang. Siehe dazu *Einstellungen des Zugangs*.
4. Fügen Sie einen Barcodeleser hinzu. Siehe dazu *Leser hinzufügen*.
   4.1. Klicken Sie für eine Seite des Zugangs auf **Leser hinzufügen**.
   4.2. Wählen Sie **AXIS Barcode Reader** in der Auswahlliste **Lesertyp**. Geben Sie einen Namen ein und klicken Sie auf **OK**.

1. Um die QR-Zugangsdaten zu ändern, gehen Sie zu **Configuration > Access control > Identification profiles (Konfiguration > Zutrittskontrolle > Identifizierungsprofile)** und klicken Sie auf . Siehe dazu *Identifizierungsprofile*.
2. Fügen Sie einen Zugang hinzu. Siehe hierzu *Zugang hinzufügen*.
3. Wählen Sie **QR** als Identifizierungsprofil für diesen Zugang. Siehe dazu *Einstellungen des Zugangs*.
4. Fügen Sie einen Barcodeleser hinzu. Siehe dazu *Leser hinzufügen*.
   4.1. Klicken Sie für eine Seite des Zugangs auf **Leser hinzufügen**.
   4.2. Wählen Sie **AXIS Barcode Reader** in der Auswahlliste **Lesertyp**. Geben Sie einen Namen ein und klicken Sie auf **OK**.

1. Um die QR-Zugangsdaten zu ändern, gehen Sie zu **Configuration > Access control > Identification profiles (Konfiguration > Zutrittskontrolle > Identifizierungsprofile)** und klicken Sie auf . Siehe dazu *Identifizierungsprofile*.
2. Fügen Sie einen Zugang hinzu. Siehe hierzu *Zugang hinzufügen*.
3. Wählen Sie **QR** als Identifizierungsprofil für diesen Zugang. Siehe dazu *Einstellungen des Zugangs*.
4. Fügen Sie einen Barcodeleser hinzu. Siehe dazu *Leser hinzufügen*.
   4.1. Klicken Sie für eine Seite des Zugangs auf **Leser hinzufügen**.
   4.2. Wählen Sie **AXIS Barcode Reader** in der Auswahlliste **Lesertyp**. Geben Sie einen Namen ein und klicken Sie auf **OK**.

Eine Verbindung mit dem Zugangscontroller erstellen

1. In AXIS Camera Station Pro Secure Entry:
   1.1. Gehen Sie zu **Konfiguration > Zutrittskontrolle > Verschlüsselte Kommunikation**.

1.2. Klicken Sie unter **Authentifizierungsschlüssel für externes Peripheriegerät** auf **Authentifizierungsschlüssel anzeigen** und **Schlüssel kopieren**.

2. Gehen Sie auf der Weboberfläche des Geräts, auf dem AXIS Barcode Reader ausgeführt wird, wie folgt vor:
   2.1. Öffnen Sie die Anwendung AXIS Barcode Reader.
   2.2. Wenn das Serverzertifikat in AXIS Camera Station Pro Secure Entry nicht konfiguriert ist, aktivieren Sie **Ignore server certificate validation (Validierung von Serverzertifikaten ignorieren)**. Weitere Informationen dazu finden Sie unter *Zertifikate*.
   2.3. Wenn das Serverzertifikat in AXIS Camera Station Pro Secure Entry nicht konfiguriert ist, aktivieren Sie **Ignore server certificate validation (Validierung von Serverzertifikaten ignorieren)**. Weitere Informationen dazu finden Sie unter *Zertifikate*.
   2.4. Wenn das Serverzertifikat in AXIS Camera Station Pro Secure Entry nicht konfiguriert ist, aktivieren Sie **Ignore server certificate validation (Validierung von Serverzertifikaten ignorieren)**. Weitere Informationen dazu finden Sie unter *Zertifikate*.
   2.5. Aktivieren Sie **AXIS Camera Station Secure Entry**.
   2.6. Klicken Sie auf **Hinzufügen**, geben Sie die IP-Adresse des Zugangscontrollers ein und fügen Sie den Authentifizierungsschlüssel ein.
   2.7. Wählen Sie im Drop-Down Menü für den Zugang den Leser zum Lesen der Barcodes aus.

Multiserver BETA

Mit Multiserver können globale Karteninhaber und Karteninhabergruppen auf dem Hauptserver von den verbundenen Subservern aus verwendet werden.

Hinweis

- Ein System kann bis zu 64 Subserver unterstützen.
- Dafür ist AXIS Camera Station 5.47 oder höher erforderlich.
- Es ist erforderlich, dass sich der Hauptserver und die Subserver im selben Netzwerk befinden.
- Auf Haupt- und Subservern müssen Sie die Windows-Firewall so konfigurieren, dass auf dem Secure Entry Port eingehende TCP-Verbindungen zulässig sind. Der Standardport ist 55767. Eine individuelle Portkonfiguration finden Sie unter .
- Durch das Verbinden eines Subservers mit einem Hauptserver wird dessen Leserschlüssel ersetzt, wodurch alle bestehenden Bluetooth-Zugangsdaten ungültig werden. Um dies zu vermeiden, erstellen Sie die Bluetooth-Zugangsdaten auf dem Hauptserver statt auf dem Subserver.

Vorgehensweise

1. Konfigurieren Sie einen Server als Subserver und erstellen Sie die Konfigurationsdatei. Siehe *Die Konfigurationsdatei vom Subserver erstellen, on page 30*.
2. Konfigurieren Sie einen Server als Hauptserver und importieren Sie die Konfigurationsdatei der Subserver. Siehe *Importieren der Konfigurationsdatei auf den Hauptserver, on page 31*.
3. Konfigurieren Sie globale Karteninhaber und Karteninhabergruppen auf dem Hauptserver. Siehe *Karteninhaber hinzufügen, on page 33* und *Gruppe hinzufügen, on page 38*.
4. Auf dem Subserver können Sie die globalen Karteninhaber und Karteninhabergruppen anzeigen und überwachen. Siehe *Zutrittsverwaltung, on page 33*.

Die Konfigurationsdatei vom Subserver erstellen

1. Wechseln Sie vom Subserver zu **Configuration > Access Control > Multi server**.
2. Klicken Sie auf **Subserver**.
3. Klicken Sie auf **Erstellen**. Es wird eine Konfigurationsdatei im JSON-Format erstellt.

4. Klicken Sie auf **Herunterladen** und wählen Sie einen Speicherort für die Datei aus.

Importieren der Konfigurationsdatei auf den Hauptserver

1. Wechseln Sie vom Hauptserver zu **Configuration > Access Control > Multi server**.
2. Klicken Sie auf **Hauptserver**.
3. Klicken Sie auf **+ Add (Hinzufügen)** und rufen Sie die vom Subserver generierte Konfigurationsdatei auf.
4. Geben Sie den Servernamen, die IP-Adresse und die Portnummer des Subservers ein.
5. Klicken Sie auf **Import (Importieren)**, um den Subserver hinzuzufügen.
6. Der Status des Subservers zeigt `Connected` an.

Subserver sperren

Sie können einen Subserver nur sperren, bevor die Konfigurationsdatei auf einen Hauptserver importiert wird.

1. Wechseln Sie vom Hauptserver zu **Configuration > Access Control > Multi server**.
2. Klicken Sie auf **Subserver** und klicken Sie auf **Server sperren**.
   Jetzt können Sie diesen Server als Haupt- oder Subserver konfigurieren.

Subserver entfernen

Nach dem Importieren der Konfigurationsdatei eines Subservers ist der Subserver mit dem Hauptserver verbunden.

Subserver entfernen:

1. Vom Hauptserver:
   1.1. Rufen Sie **Access management > Dashboard (Zugriffsverwaltung > Dashboard)** auf.
   1.2. Ändern Sie die globalen Karteninhaber und Gruppen in lokale Karteninhaber und Gruppen.
   1.3. Rufen Sie **Configuration > Access control > Multi server (Konfiguration > Zutrittskontrolle > Multi-Server)** auf.
   1.4. Klicken Sie auf **Main server (Hauptserver)**, um die Liste der Subserver anzuzeigen.
   1.5. Wählen Sie den Subserver aus und klicken Sie auf **Löschen**.
2. Vom Subserver:
   – Rufen Sie **Configuration > Access control > Multi server (Konfiguration > Zutrittskontrolle > Multi-Server)** auf.
   – Klicken Sie auf **Sub server (Subserver)** und dann auf **Revoke server (Server sperren)**.

Active-Directory-Einstellungen[BETA]

Hinweis

Der Zugriff auf AXIS Camera Station Pro Secure Entry erfolgt über Microsoft Windows-Benutzerkonten sowie über die Benutzer und Gruppen in Active Directory. Die Art und Weise, wie Sie Benutzer unter Windows hinzufügen, hängt von Ihrer Version ab. Weitere Informationen finden Sie unter *support.microsoft.com*. Falls Sie ein Active Directory-Domainnnetzwerk verwenden, halten Sie bitte Rücksprache mit Ihrem Netzwerkadministrator.

Wenn Sie die Seite mit den Active Directory-Einstellungen zum ersten Mal öffnen, können Sie Microsoft Active Directory-Benutzer in Karteninhaber in AXIS Camera Station Pro Secure Entry importieren. Siehe *Active-Directory-Benutzer importieren, on page 32*.

Nach der ersten Konfiguration werden auf der Seite mit den Active Directory-Einstellungen die folgenden Optionen angezeigt.

- Erstellen und verwalten Sie Karteninhabergruppen basierend auf Gruppen in Active Directory.
- Richten Sie eine geplante Synchronisierung zwischen Active Directory und dem Zugriffsverwaltungssystem ein.
- Führen Sie eine manuelle Synchronisierung durch, um alle aus Active Directory importierten Karteninhaber zu aktualisieren.
- Verwalten Sie die Datenzuordnung zwischen Benutzerdaten aus Active Directory und Karteninhabereigenschaften.

Active-Directory-Benutzer importieren

So importieren Sie Active Directory-Benutzer in Karteninhaber in AXIS Camera Station Pro Secure Entry:

1. Rufen Sie **Configuration (Konfiguration)** > **Access control (Zutrittskontrolle)** > **Active directory settings (Active-Directory-Einstellungen)**[BETA] auf.
2. Klicken Sie auf **Set up import (Import einrichten)**.
3. Befolgen Sie die Anweisungen auf dem Bildschirm, um diese drei Hauptschritte abzuschließen:
   3.1. Wählen Sie einen Benutzer aus Active Directory aus, der als Vorlage für die Datenzuordnung verwendet werden soll.
   3.2. Ordnen Sie Benutzerdaten aus der Active Directory-Datenbank den Karteninhabereigenschaften zu.
   3.3. Erstellen Sie im Zutrittsverwaltungssystem eine neue Karteninhabergruppe und wählen Sie aus, welche Active Directory-Gruppen importiert werden sollen.

Die importierten Benutzerdaten können nicht geändert werden. Sie können jedoch dem importierten Karteninhaber Zugangsdaten hinzufügen. Informationen dazu finden Sie unter *Zugangsdaten hinzufügen, on page 35*.

Wichtig

Wenn Sie einen Benutzer in Active Directory deaktivieren, löscht AXIS Camera Station Pro den Karteninhaber und alle zugehörigen Daten, einschließlich der Verlaufsdaten, endgültig. Diese Aktion kann nicht rückgängig gemacht werden. Um den Zugang eines Karteninhabers zu sperren, ohne dessen Daten zu verlieren, setzen Sie seine Zugangsberechtigung in AXIS Camera Station Pro aus, anstatt ihn in Active Directory zu deaktivieren.

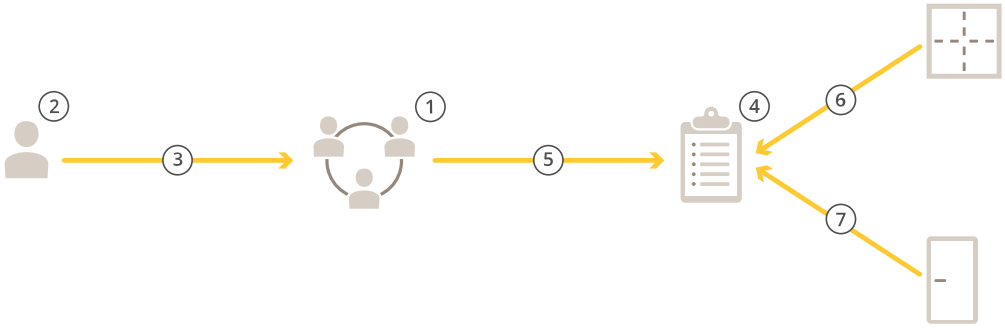
Zutrittsverwaltung

Auf der Registerkarte „Access Management (Zugriffsverwaltung)" können Sie die Karteninhaber, Gruppen und Zugangsregeln des Systems konfigurieren und verwalten.

Die vollständige Vorgehensweise zum Einrichten eines Axis Network Door Controller in AXIS Camera Station Pro Secure Entry finden Sie unter *Einrichten eines Axis Network Door Controllers*.

Vorgehensweise bei der Zugriffsverwaltung

Die Struktur der Zugriffsverwaltung ist flexibel. Gehen Sie anhand der Anforderungen der jeweiligen Anwendung vor. Im Folgenden finden Sie ein Beispiel für eine Vorgehensweise:



1. *Gruppe hinzufügen, on page 38*.
2. *Karteninhaber hinzufügen, on page 33*.
3. Fügen Sie Karteninhaber und Gruppen hinzu.
4. *Zugangsregel hinzufügen, on page 38*.
5. Ordnen Sie Zugangsregeln Gruppen zu.
6. Ordnen Sie Zugangsregeln Zonen zu.
7. Ordnen Sie Zugangsregeln Zugänge zu.

Karteninhaber hinzufügen

Ein Karteninhaber ist eine Person mit einer eindeutigen ID, die im System registriert ist. Konfigurieren Sie einen Karteninhaber mit Zugangsdaten, die dem System mitteilen, wer die Person ist und wann und wie der Person die Nutzung von Zugängen gewährt wird.

Sie können Benutzer auch über eine Active-Directory-Datenbank als Karteninhaber zuweisen (siehe *Active-Directory-Einstellungen*^{BETA}*, on page 31*).

1. Öffnen Sie eine Registerkarte Access Management (Zugangsverwaltung).
2. Rufen Sie **Cardholder management (Karteninhaberverwaltung)** > **Cardholders (Karteninhaber)** und klicken Sie auf **+ Add (+ Hinzufügen)**.
3. Geben Sie den Vor- und Nachnamen des Karteninhabers ein. Optional können Sie weitere Angaben zum Karteninhaber machen:
   - Geben Sie unter **E-Mail** die E-Mail-Adresse des Karteninhabers ein.
   - Wählen Sie unter **Groups (Gruppen)** die Gruppen aus, denen Sie den Karteninhaber hinzufügen möchten.
   - Wählen Sie unter **Access rules (Zugangsregeln)** die Regeln aus, die Sie auf den Karteninhaber anwenden möchten.

4. Um ein Foto hinzuzufügen, klicken Sie auf **Cardholder picture (Karteninhaberfoto)** und wählen Sie eine der folgenden Optionen aus:
   - **Upload (Hochladen)**, um ein Bild von Ihrem Gerät hinzuzufügen.
   - **Capture (Fotografieren)**, um direkt mit Ihrer Kamera ein Foto aufzunehmen.

   Hinweis

   Bei dem Bild muss es sich um eine JPG-, PNG- oder GIF-Datei handeln. Bilder werden automatisch auf eine maximale Größe von 700 x 700 Pixel skaliert und in das JPG-Format umgewandelt.
5. Klicken Sie auf **Advanced (Erweitert)**, um zusätzliche Einstellungen vorzunehmen.
6. Fügen Sie Zugangsdaten für den Karteninhaber hinzu. Siehe *Zugangsdaten hinzufügen, on page 35*.
7. **Save (Speichern)** anklicken.
8. Um Ausweise für einen oder mehrere Karteninhaber zu drucken, wählen Sie den/die Karteninhaber aus und klicken Sie auf **Print Badge**[BETA] **(Ausweis drucken)**. Weitere Informationen finden Sie unter *Print badge (Ausweis drucken) [BETA], on page 44*.

Im Suchfeld können Sie einen Karteninhaber mit seinem Vor- oder Nachnamen suchen. Um nach einer Quelle zu filtern, klicken Sie auf **Filter** und wählen Sie dann **Local (Lokal)**, **Global**, **(AD)** oder **Center** aus.

Erweitert	
Lange Zugriffszeit	Wählen Sie diese Option aus, damit für den Karteninhaber eine lange Zutrittszeit und eine lange Dauer für einen zu lange geöffneten Zugang gelten sollen, wenn ein Zugangsmonitor installiert ist.
Karteninhaber suspendieren	Wählen Sie diese Option aus, um den Karteninhaber zu suspendieren. Diese Option setzt vorübergehend alle Zugangsberechtigungen des Karteninhabers aus.
Allow double-swipe (Double Swipe zulassen)	Auswählen, um einem Karteninhaber zu erlauben, den aktuellen Zustand eines Zugangs außer Kraft zu setzen. Dies kann beispielsweise dazu verwendet werden, eine Tür außerhalb des regulären Zeitplans zu entriegeln.
Vom Lockdown ausgeschlossen	Wählen Sie diese Option aus, um dem Karteninhaber während der Sperrzeit Zugang zu gewähren.
Exempt from anti-passback (Doppelnutzungsausnahme)	Sie können einem Karteninhaber jetzt eine Ausnahme von der Anti-Passback-Regel gewähren. Die Anti-Passback-Funktion verhindert, dass eine Person die gleichen Zugangsdaten verwenden kann wie jemand, der bereits vor ihr einen Bereich betreten hat. Die erste Person muss zunächst den Bereich verlassen, bevor ihre Zugangsdaten erneut verwendet werden können.
Globaler Karteninhaber	Wählen Sie diese Option aus, damit der Karteninhaber auf den Subservern angezeigt und überwacht werden kann. Diese Option ist nur für auf dem Hauptserver erstellte Karteninhaber verfügbar. Siehe *Multiserver [BETA], on page 30*.

Karteninhaber und Gruppen hinzufügen

Zugangsdaten hinzufügen

Sie können einem Karteninhaber die folgenden Arten von Zugangsdaten hinzufügen:

- *QR-Code als Zugangsdaten, on page 35*
- *PIN-Zugangsdaten, on page 36*
- *Smartphone-Zugangsdaten, on page 36*
- *Kartenzugangsdaten, on page 36*
- *Fahrzeugkennzeichen Zugangsdaten, on page 37*

Verfallsdatum	
Gültig ab	Legen Sie ein Datum und einen Zeitpunkt für die Gültigkeit der Zugangsdaten fest.
Gültig bis	Wählen Sie eine Option aus dem Drop-Down Menü.

Gültig bis	
Kein Enddatum	Die Zugangsdaten laufen niemals ab.
Datum	Wählen Sie ein Datum und eine Uhrzeit aus, an dem die Zugangsdaten ablaufen.
Von der ersten Verwendung	Wählen Sie aus, wie lange nach der ersten Verwendung die Zugangsdaten ablaufen. Wählen Sie eine Anzahl von Tagen, Monaten, Jahren oder Wiederholungen nach der ersten Verwendung aus.
Von der letzten Verwendung	Wählen Sie aus, wie lange nach der letzten Verwendung die Zugangsdaten ablaufen. Wählen Sie Tage, Monate oder Jahre nach der letzten Verwendung aus.

QR-Code als Zugangsdaten

Hinweis

Für die Verwendung von QR-Codes als Zugangsdaten ist eine Synchronisierung der Zeit auf dem Systemcontroller und der Kamera mit AXIS Barcode Reader erforderlich. Für eine perfekte Zeitsynchronisierung empfehlen wir Ihnen, für beide Geräte die gleiche Zeitquelle zu verwenden.

So fügen Sie einem Karteninhaber QR-Zugangsdaten hinzu:

1. Klicken Sie unter **Credentials (Zugangsdaten)** auf **+ Add (+ Hinzufügen)** und wählen Sie **QR-code (QR-Code)** aus.
2. Geben Sie einen Namen für die Zugangsdaten ein.
3. **Dynamic QR** ist standardmäßig aktiviert. Sie müssen Dynamic QR mit PIN-Anmeldedaten verwenden.

4. Legen Sie das Start- und Enddatum für die Zugangsdaten fest.
5. Um nach dem Speichern des Karteninhabers den QR-Code automatisch per E-Mail zu versenden, wählen Sie beim Speichern der Anmeldedaten **QR-Code an den Karteninhaber senden**.
6. Klicken Sie auf **Hinzufügen**.

PIN-Zugangsdaten

So fügen Sie einem Karteninhaber PIN-Zugangsdaten hinzu:
1. Klicken Sie unter **Credentials (Zugangsdaten)** auf **+ Add (+ Hinzufügen)** und wählen Sie **PIN** aus.
2. Geben Sie eine PIN ein.
3. Um einen stillen Alarm mit einer separaten PIN auszulösen, schalten Sie optional **Duress PIN (Zwangs-PIN)** ein und geben Sie eine Zwangs-PIN ein.
4. Legen Sie die Zugangsdaten **Valid from (Gültig ab)** und **Valid to (Gültig bis)** fest.
5. Klicken Sie auf **Hinzufügen**.

Smartphone-Zugangsdaten

Hinweis

Der Karteninhaber muss über eine E-Mail-Adresse verfügen, um die mobilen Zugangsdaten zu erhalten.

So fügen Sie einem Karteninhaber mobile Zugangsdaten hinzu:
1. Klicken Sie unter **Credentials (Zugangsdaten)** auf **+ Add (+ Hinzufügen)** und wählen Sie **Mobile credential (Mobile Zugangsdaten)** aus.
2. Geben Sie einen Namen für die Zugangsdaten ein.
3. Legen Sie das Start- und Enddatum für die Zugangsdaten fest.
4. Wählen Sie **Send the mobile credential to the cardholder after saving (Mobile Zugangsdaten nach dem Speichern an Karteninhaber senden)** aus. Der Karteninhaber erhält eine E-Mail mit Anweisungen zum Koppeln.
5. Klicken Sie auf **Hinzufügen**.

Siehe das Beispiel in *App AXIS Mobile Credential als Bluetooth-Zugangsdaten verwenden, on page 19*.

Kartenzugangsdaten

So fügen Sie einem Karteninhaber Karten-Zugangsdaten hinzu:
1. Klicken Sie unter **Credentials (Zugangsdaten)** auf **+ Add (+ Hinzufügen)** und wählen Sie **Card (Karte)** aus.
2. Um die Kartendaten manuell einzugeben, geben Sie einen Kartennamen, eine Kartennummer und eine Bitlänge ein.

Hinweis

Die Bitlänge ist nur konfigurierbar, wenn Sie ein Kartenformat mit einer bestimmten Bitlänge erstellen, die sich nicht im System befindet.

3. So rufen Sie automatisch die Kartendaten der zuletzt durch den Leser gezogenen Karte ab:
   3.1. Wählen Sie aus dem Ausklappmenü **Select reader (Leser auswählen)** einen Zugangspunkt aus.
   3.2. Ziehen Sie die Karte durch den Leser, der an diesen Zugang angeschlossen ist.
   3.3. Klicken Sie auf **Get last swiped card data from the door's reader(s) (Daten der zuletzt verwendeten Karte vom Leser des Zugangs abrufen)**.

Hinweis

Sie können den 2N-Desktop-USB-Kartenleser verwenden, um die Kartendaten abzurufen. Weitere Informationen finden Sie unter *Einrichten des 2N-Desktop-USB-Kartenlesers*.

4. Einen Einrichtungscode eingeben. Dieses Feld ist nur verfügbar, wenn Sie **Facility code (Gebäude-Zugangscode)** unter **Access management > Settings (Zugriffsverwaltung > Einstellungen)** aktiviert haben.
5. Legen Sie das Start- und Enddatum für die Zugangsdaten fest.
6. Klicken Sie auf **Hinzufügen**.

Fahrzeugkennzeichen Zugangsdaten

So fügen Sie einem Karteninhaber Fahrzeugkennzeichen-Zugangsdaten hinzu:

1. Klicken Sie unter **Credentials (Zugangsdaten)** auf **+ Add (+ Hinzufügen)** und wählen Sie **License plate (Fahrzeugkennzeichen)** aus.
2. Geben Sie einen Namen für die Zugangsdaten ein, der das Fahrzeug beschreibt.
3. Geben Sie das Fahrzeugkennzeichen für das Fahrzeug ein.
4. Legen Sie das Start- und Enddatum für die Zugangsdaten fest.
5. Klicken Sie auf **Hinzufügen**.

Fahrzeugkennzeichen als Zugangsdaten verwenden

In diesem Beispiel sehen Sie, wie Sie eine Tür-Steuerung, eine Kamera mit AXIS License Plate Verifier und ein Fahrzeugkennzeichen als Zugangsdaten verwenden, um einem Fahrer Zugang zu gewähren.

1. Fügen Sie die Tür-Steuerung und die Kamera zu AXIS Camera Station Pro Secure Entry hinzu. Siehe .
2. Aktualisieren Sie die Firmware der neuen Geräte auf die neueste verfügbare Version. Siehe .
3. Fügen Sie einen neuen Zugang hinzu, die mit Ihrer Tür-Steuerung verbunden ist. Siehe *Hinzufügen eines Zugangs, on page 7*.
   3.1. Fügen Sie auf **Seite A** einen Leser hinzu. Siehe *Leser hinzufügen, on page 17*.
   3.2. Wählen Sie unter **Türeinstellungen** die Option **AXIS License Plate Verifier** als **Lesertyp** und geben Sie einen Namen für den Leser ein.
   3.3. Fügen Sie optional einen Leser oder ein REX-Gerät auf **Seite B** hinzu.
   3.4. **OK** anklicken.
4. Installieren und aktivieren Sie AXIS License Plate Verifier auf Ihrer Kamera. Siehe das Benutzerhandbuch zu *AXIS License Plate Verifier*.
5. Starten Sie AXIS License Plate Verifier.
6. Konfigurieren Sie AXIS License Plate Verifier.
   6.1. Gehen Sie zu **Konfiguration > Zutrittskontrolle > Verschlüsselte Kommunikation**.
   6.2. Klicken Sie unter **Authentifizierungsschlüssel für externes Peripheriegerät** auf **Authentifizierungsschlüssel anzeigen** und **Schlüssel kopieren**.
   6.3. Öffnen Sie AXIS License Plate Verifier über die Weboberfläche der Kamera.
   6.4. Setup nicht ausführen.
   6.5. **Settings (Einstellungen)** aufrufen.
   6.6. Wählen Sie unter **Zutrittskontrolle** die Option **Sicherer Zugang** as **Typ**.
   6.7. Geben Sie in **IP address (IP-Adresse)** die IP-Adresse für die Tür-Steuerung ein.
   6.8. Fügen Sie in **Authentifizierungsschlüssel** den zuvor kopierten Authentifizierungsschlüssel ein.
   6.9. **Connect (Verbinden)** anklicken.
   6.10. Wählen Sie unter **Door controller name (Tür-Steuerung)** Ihre Tür-Steuerung aus.
   6.11. Wählen Sie unter **Lesername** den Leser aus, den Sie zuvor hinzugefügt haben.
   6.12. Schalten Sie Integration ein.

7. Fügen Sie den Karteninhaber hinzu, dem Sie Zugriff gewähren möchten. Siehe *Karteninhaber hinzufügen, on page 33*
8. Fügen Sie dem neuen Karteninhaber die Zugangsdaten zum Fahrzeugkennzeichen hinzu. Siehe *Zugangsdaten hinzufügen, on page 35*
9. Fugen Sie eine Zugangsregel hinzu. Siehe *Zugangsregel hinzufügen, on page 38*.
   9.1. Einen Zeitplan hinzufügen.
   9.2. Fügen Sie den Karteninhaber hinzu, dem Sie Zugang über das Fahrzeugkennzeichen gewähren möchten.
   9.3. Fügen Sie die Tür dem AXIS License Plate Verifier hinzu.

Gruppe hinzufügen

Gruppen ermöglichen es Ihnen, Karteninhaber und deren Zugangsregeln gemeinsam und effizient zu verwalten.

1. Öffnen Sie eine Registerkarte Access Management (Zugangsverwaltung).
2. Rufen Sie **Cardholder management (Karteninhaberverwaltung)** > **Groups (Gruppen)** und klicken Sie auf **+ Add (+ Hinzufügen)**.
3. Geben Sie einen Namen und optional Initialen für die Gruppe ein.
4. Wählen Sie **Global group (Globale Gruppe)** aus, damit der Karteninhaber auf den Subservern angezeigt und überwacht werden kann. Diese Option ist nur für auf dem Hauptserver erstellte Karteninhaber verfügbar. Siehe *Multiserver BETA, on page 30*.
5. So fügen Sie der Gruppe Karteninhaber hinzu:
   5.1. **+ hinzufügen** anklicken.
   5.2. Wählen Sie die gewünschten Karteninhaber aus und klicken Sie auf **Add (Hinzufügen)**.
6. **Save (Speichern)** anklicken.
7. Um Ausweise für alle Karteninhaber einer Gruppe zu drucken, wählen Sie die Gruppe aus und klicken Sie auf **Print Badge BETA (Ausweis drucken)**. Weitere Informationen finden Sie unter *Print badge (Ausweis drucken) BETA, on page 44*.

Zugangsregel hinzufügen

Eine Zugangsregel definiert die Bedingungen, die erfüllt sein müssen, damit der Zugang gewährt wird.

Eine Zugangsregel umfasst Folgendes:

Karteninhaber und Karteninhabergruppen – Legen fest, wem der Zugang gewährt werden soll.

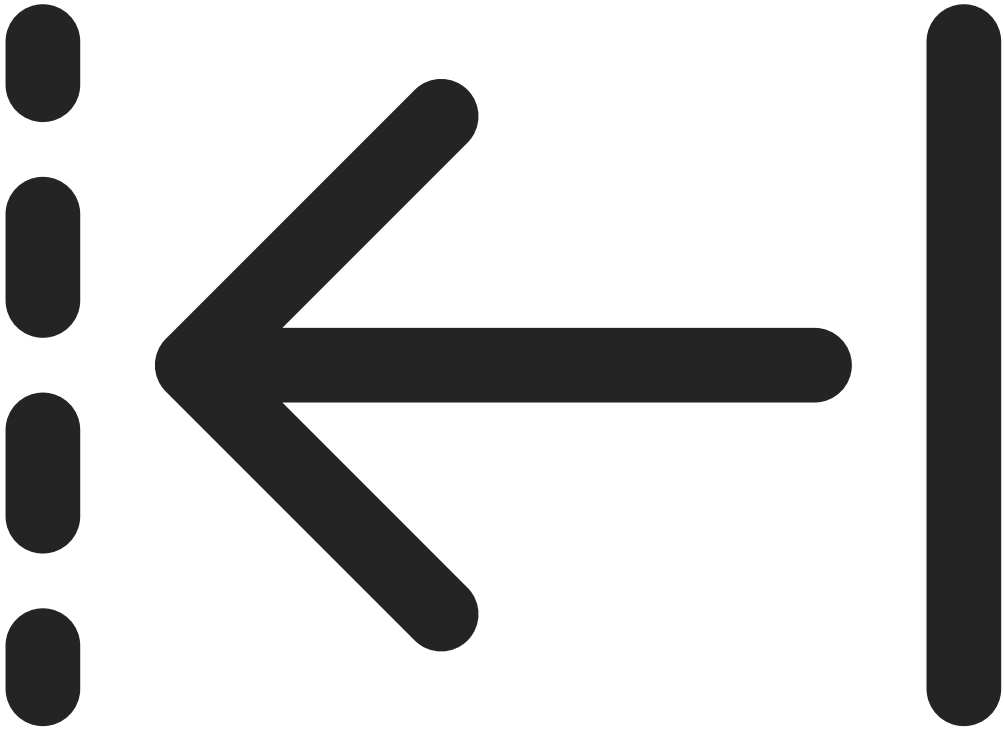
Türen und Bereiche – Geben an, wofür der Zugang gilt.

Zeitschemata – Legen fest, wann der Zugang gewährt werden soll.

So fügen Sie eine Zugangsregel hinzu:

1. Öffnen Sie eine Registerkarte Access Management (Zugangsverwaltung).
2. Wechseln Sie zu **Cardholder management (Karteninhaberverwaltung)**.

3. Klicken Sie unter **Access rule (Zugangsregel)**



auf **+ Add (+ Hinzufügen)**.

4. Geben Sie einen Namen für die Regel ein und klicken Sie auf **Next (Weiter)**.
5. Konfigurieren der Karteninhaber und Gruppen:
   5.1. Klicken Sie unter **Cardholders (Karteninhaber)** oder **Groups (Gruppen)** auf **+ Add (+ Hinzufügen)**.
   5.2. Wählen Sie Karteninhaber bzw. Gruppen und klicken Sie auf **Add (Hinzufügen)**.
   5.3. Sie können einen Karteninhaber oder eine Gruppe auch direkt auf eine Zugriffsregel ziehen und ablegen, um diese anzuwenden. Sobald Sie ein Element ziehen, werden die Zugangsregeln hervorgehoben, auf denen Sie es ablegen können. Wenn Sie mehrere Karteninhaber oder Gruppen gleichzeitig ziehen, wird deren Anzahl angezeigt.
6. Zugänge und Bereiche konfigurieren:
   6.1. Klicken Sie unter **Doors (Zugänge)** oder **Zones (Zonen)** auf **+ Add (+ Hinzufügen)**.
   6.2. Wählen Sie Zugänge bzw. Zonen und klicken Sie auf **Add (Hinzufügen)**.
7. Konfigurieren der Zeitpläne:
   7.1. Klicken Sie unter **Schedules (Zeitpläne)** auf **+ Add (+ Hinzufügen)**.
   7.2. Wählen Sie einen oder mehrere Zeitpläne aus und klicken Sie auf **Add (Hinzufügen)**.

8. **Save (Speichern)** anklicken.

Eine Regel für den Zugriff, bei der eine oder mehrere der oben beschriebenen Komponenten fehlen, ist unvollständig. Sie können alle unvollständigen Regeln für den Zugriff auf der Registerkarte **Incomplete (Unvollständig)** einsehen.

Berichte zur Systemkonfiguration exportieren

Sie können Berichte exportieren, die verschiedene Typen von Informationen über das System enthalten. AXIS Camera Station Pro Secure Entry exportiert den Bericht als Datei mit kommagetrennten Werten (CSV) und speichert ihn im Standard-Download-Ordner. So exportieren Sie einen Bericht:

1. Öffnen Sie eine Registerkarte Access Management (Zugangsverwaltung).
2. Rufen Sie **Reports (Berichte)** > **System configuration (Systemkonfiguration)** auf.
3. Wählen Sie die Berichte aus, die Sie exportieren möchten, und klicken Sie auf **Download**.

Detaillierter Bericht der Karteninhaber	Dieser Bericht enthält Informationen zu Karteninhabern, Zugangsdaten, Kartenüberprüfung und zur letzten Transaktion.
Bericht über den Zugang von Karteninhabern	Dieser Bericht enthält die Karteninhaberinformationen und Informationen über die Karteninhabergruppen, Zugangsregeln, Zugänge und Zonen, mit denen der Karteninhaber in Verbindung steht.
Bericht über den Gruppenzugang von Karteninhabern	Dieser Bericht enthält den Namen der Karteninhabergruppe und Informationen zu den Karteninhabern, Zugangsregeln, Zugängen und Zonen, mit denen die Karteninhabergruppe in Verbindung steht.
Bericht über Zugangsregeln	Dieser Bericht enthält den Namen der Zugangsregel und Informationen zu den Karteninhabern, Karteninhabergruppen, Zugangsregeln, Zugänge und Zonen, mit denen die Zugangsregel in Verbindung steht.
Bericht über den Zugang zu Türen	Dieser Bericht enthält den Namen des Zugangs und Informationen zu den Karteninhabern, Karteninhabergruppen, Zugangsregeln und Zonen, mit denen der Zugang in Verbindung steht.
Bericht über den Zonenzugang	Dieser Bericht enthält den Namen der Zone und Informationen zu den Karteninhabern, Karteninhabergruppen, Zugangsregeln und Zugänge, mit denen die Zone in Verbindung steht.

Berichte über Karteninhaberaktivitäten erstellen

Ein Appellbericht listet die Karteninhaber innerhalb einer bestimmten Zone auf und hilft dabei festzustellen, wer zu einem bestimmten Zeitpunkt anwesend ist.

Ein Musterungsbericht listet Karteninhaber innerhalb einer bestimmten Zone auf und hilft dabei, in Notfällen festzustellen, wer sicher ist und wer vermisst wird. Er unterstützt die Verwaltung von Gebäuden bei der Lokalisierung von Mitarbeitern und Besuchern nach Evakuierungen. Ein Sammelpunkt ist ein ausgewiesener Kartenleser, an dem sich das Personal bei Notfällen meldet und einen Bericht über die Personen am und außerhalb des Standorts erstellt. Das System kennzeichnet Karteninhaber als vermisst, bis sie sich an einem Sammelpunkt melden oder bis jemand sie manuell als sicher kennzeichnet.

Sowohl die Appell- als auch die Musterungsberichte erfordern Zonen zum Tracking der Karteninhaber.

So erstellen Sie einen Appell- oder Musterungsbericht und führen ihn aus:

1. Öffnen Sie eine Registerkarte Access Management (Zugangsverwaltung).
2. Rufen Sie **Reports (Berichte)** > **Cardholder activity (Karteninhaberaktivitäten)** auf.
3. Klicken Sie auf **+ Add (+ Hinzufügen)** und wählen Sie **Appell / Musterung**.
4. Geben Sie einen Namen für den Bericht ein.
5. Wählen Sie die Zonen aus, die in den Bericht aufgenommen werden sollen.
6. Wählen Sie die Gruppen aus, die Sie in den Bericht aufnehmen möchten.
7. Wenn Sie einen Musterungsbericht wünschen, wählen Sie **Mustering point (Sammelpunkt)** und einen Kartenleser für den Sammelpunkt.
8. Wählen Sie einen Zeitrahmen für den Bericht aus.
9. **Save (Speichern)** anklicken.
10. Wählen Sie den Bericht aus und klicken Sie auf **Run (Ausführen)**.

Status des Appellberichts	Beschreibung
Anwesend	Der Karteninhaber hat die angegebene Zone betreten und sie nicht verlassen, bevor Sie den Bericht ausgeführt haben.
Nicht anwesend	Der Karteninhaber hat die angegebene Zone verlassen und sie nicht betreten, bevor Sie den Bericht ausgeführt haben.

Status des Musterungsberichts	Beschreibung
Sicher	Der Karteninhaber hat seine Karte am Sammelpunkt benutzt.
Fehlt	Der Karteninhaber hat seine Karte am Sammelpunkt nicht benutzt.

Import und Export

Karteninhaber importieren

Über diese Option können Karteninhaber, Karteninhabergruppen, Zugangsdaten und Bilder von Karteninhabern aus einer CSV-Datei importiert werden. Stellen Sie zum Importieren von Bildern von Karteninhaber sicher, dass der Server Zugriff auf die Bilder hat.

Beim Importieren von Karteninhabern speichert das Zugangsverwaltungssystem automatisch die Systemkonfiguration inklusive sämtlicher Hardwarekonfiguration und löscht alle zuvor gespeicherten.

Sie können Benutzer auch über eine Active-Directory-Datenbank als Karteninhaber zuweisen (siehe *Active-Directory-Einstellungen[BETA], on page 31*).

Optionen importieren	
Neu	Diese Option entfernt vorhandene Karteninhaber und fügt neue Karteninhaber hinzu.
Aktualisieren	Über diese Option werden vorhandene Karteninhaber aktualisiert und neue Karteninhaber hinzugefügt.
Hinzufügen	Diese Option behält vorhandene Karteninhaber bei und fügt neue Karteninhaber hinzu. Kartennummern und Karteninhaber-IDs sind eindeutig und können nur einmal verwendet werden.

1. Klicken Sie auf der Registerkarte **Access management (Zugriffsverwaltung)** auf **Import and export (Import und Export)**.
2. Klicken Sie auf **Import cardholders (Karteninhaber importieren)**.
3. Wählen Sie **Neu**, **Aktualisieren** oder **Hinzufügen**.
4. Klicken Sie auf **Next (Weiter)**.
5. Klicken Sie auf **Choose a file (Wählen Sie eine Datei)** und rufen Sie die CSV-Datei auf. **Öffnen** anklicken.
6. Geben Sie ein Spaltentrennzeichen ein, wählen Sie einen eindeutigen Bezeichner aus und klicken Sie auf **Next (Weiter)**.
7. Weisen Sie jeder Spalte eine Überschrift zu.
8. Klicken Sie auf **Importieren**.

Einstellungen importieren	
Erste Zeile ist Kopfzeile	Wählen Sie aus, ob die CSV-Datei eine Spaltenüberschrift enthält.
Spaltentrennzeichen	Geben Sie ein Spaltentrennformat für die CSV-Datei ein.
Eindeutiger Bezeichner	Das System identifiziert standardmäßig einen Karteninhaber mit der **Cardholder ID (Karteninhaber-ID)**. Alternativ können Sie dazu den Vor- und Nachnamen oder die E-Mail-Adresse verwenden. Mit der eindeutigen Kennung wird der Import doppelter Personalaufzeichnungen verhindert.
Format der Kartennummer	In der Standardeinstellung ist **Allow both hexadecimal and number (Hexadezimal und Zahl zulassen)** ausgewählt.

Karteninhaber exportieren

Diese Option exportiert die Daten des Karteninhabers im System in eine CSV-Datei.

1. Klicken Sie auf der Registerkarte **Access management (Zugriffsverwaltung)** auf **Import and export (Import und Export)**.
2. Klicken Sie auf **Export cardholders (Karteninhaber exportieren)**.
3. Wählen Sie einen Download-Speicherort und klicken Sie auf **Save (Speichern)**.

AXIS Camera Station Pro Secure Entry aktualisiert die Karteninhaberfotos in `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos`, wenn die Konfiguration geändert wird.

Import rückgängig machen

Beim Import von Karteninhabern wird die Konfiguration des Systems automatisch gespeichert. Über **Undo import (Import rückgängig machen)** werden die Daten des Karteninhabers und die Hardwarekonfiguration auf die Voreinstellungen vor dem letzten Import des Karteninhabers zurückgesetzt.

1. Klicken Sie auf der Registerkarte **Access management (Zugriffsverwaltung)** auf **Import and export (Import und Export)**.
2. Klicken Sie auf **Undo import (Import rückgängig machen)**.
3. **Yes (Ja)** anklicken

Zugriffsverwaltungseinstellungen

So passen Sie die Karteninhaberfelder an, die im Zugriffsverwaltungsdashboard verwendet werden:

1. Klicken Sie auf der Registerkarte **Access management (Zugriffsverwaltung)** auf **Settings (Einstellungen)** > **Custom cardholder fields (Benutzerdefinierte Karteninhaberfelder)**.
2. **+ Add (+ Hinzufügen)** anklicken und eine Bezeichnung eingeben. Sie können bis zu 6 benutzerdefinierte Felder hinzufügen.
3. Klicken Sie auf **Hinzufügen**.

So aktivieren Sie die Verwendung eines Gebäude-Zugangscodes, um Ihr Zutrittssystem zu überprüfen:

1. Klicken Sie auf der Registerkarte **Access management (Zugriffsverwaltung)** auf **Settings (Einstellungen)** > **Facility code (Gebäude-Zugangscode)**.
2. Wählen Sie **Facility code on (Gebäude-Zugangscode ein)** aus.

Hinweis

Sie müssen beim Konfigurieren von Identifizierungsprofilen außerdem die Option **Include facility code for card validation (Gebäude-Zugangscode in Kartenprüfung einbeziehen)** auswählen. Siehe *Identifizierungsprofile, on page 23*.

So bearbeiten Sie eine E-Mail-Vorlage für den Versand von QR- oder mobilen Zugangsdaten:

1. Klicken Sie auf der Registerkarte **Access management (Zugriffsverwaltung)** auf **Settings (Einstellungen)** > **Email templates (E-Mail-Vorlagen)**.
2. Bearbeiten Sie Ihre Vorlage und klicken Sie auf **Update (Aktualisieren)**.

Ausweisvorlagen BETA

Sie können Ausweisvorlagen mit Karteninhaberinformationen, Fotos, Logos und individuellem Branding anpassen. So erstellen Sie eine neue Vorlage:

1. Rufen Sie **Access management (Zutrittsmanagement) > Settings (Einstellungen) > Badge templates (Ausweisvorlagen)** BETA auf.
2. Klicken Sie auf **Create new template (Neue Vorlage erstellen)**.
3. Geben Sie einen Namen in das Feld **Template name (Vorlagenname)** ein.
4. Wählen Sie **Use as default template for printing (Als Standardvorlage für den Druck verwenden)**, wenn Sie diese Vorlage als Standardvorlage festlegen möchten.
5. Passen Sie das Ausweisdesign an:
   - Wählen Sie bis zu fünf Textfelder aus, die auf der Vorderseite angezeigt werden sollen, einschließlich aller von Ihnen erstellten benutzerdefinierten Felder. Beim Drucken erscheinen nur ausgefüllte Felder auf dem Ausweis.

- Wählen Sie die Schriftart und Farbe für den Text aus.
- Fügen Sie eine Hintergrundfarbe oder ein Hintergrundbild hinzu.
- Laden Sie ein Logo für Ihre Organisation hoch.
- Für die Rückseite fügen Sie entweder eine Hintergrundfarbe oder ein Hintergrundbild hinzu.

6. Klicken Sie auf **Save (Speichern)**, um Ihre Änderungen zu speichern, oder auf **Save as (Speichern unter)**, um sie als neue Vorlage zu speichern.

Hinweis

Sobald eine Vorlage erstellt wurde, kann sie nicht mehr bearbeitet, sondern lediglich umbenannt werden.

Print badge (Ausweis drucken) BETA

Sie können Identifizierungsausweise für Karteninhaber mithilfe Ihrer konfigurierten Identifizierungsvorlagen drucken. Bitte beachten Sie, dass die Kartenkodierung derzeit nicht unterstützt wird. Vorbereitungen:

- Stellen Sie sicher, dass der Karteninhaber über mindestens eine Kartenberechtigung verfügt. Es ist nicht möglich, Ausweise für Karteninhaber ohne Berechtigung zu drucken.
- Sie benötigen einen Drucker, der das Kartenformat CR80 unterstützt und mit kompatiblem Druckmaterial wie dickem Karton kompatibel ist.
- Konfigurieren Sie die Druckeinstellungen Ihres Browsers:
  1. Stellen Sie die Seitengröße auf CR80 oder eine benutzerdefinierte Größe ein, die den Abmessungen Ihrer Karte entspricht.
  2. Stellen Sie das Format auf Hochformat ein.
  3. Schalten Sie die Ränder aus oder stellen Sie sie auf das Minimum ein.

Wichtig

Secure Entry (Sicherer Zugang) unterstützt Drucker mit Windows-Treibern. Die korrekte Funktion mit Druckern der Serie HID Fargo wurde überprüft. Sollten Sie einen Treiber für Ihren Drucker benötigen, wenden Sie sich an den Hersteller Ihres Druckers.

So drucken Sie Ausweise:

1. Rufen Sie **Access management (Zutrittsmanagement) > Cardholder management (Karteninhaberverwaltung) > Cardholders (Karteninhaber)** auf.
2. Wählen Sie einen oder mehrere Karteninhaber aus.
3. Klicken Sie auf **Print badge (Ausweis drucken)** BETA.
4. Klicken Sie auf **Select template (Vorlage auswählen)** und wählen Sie aus der Dropdown-Liste **Template (Vorlage)** die gewünschte Vorlage für den Ausweis aus.
5. Wenn der Karteninhaber über mehrere Kartenberechtigungen verfügt, wählen Sie eine aus dem Dropdown-Menü **Card (Karte)** aus.
6. Klicken Sie auf **Drucken**.

Hinweis

Falls Ihr Drucker keinen Duplexdruck unterstützt, drucken Sie bitte zunächst alle Vorderseiten aus, drehen Sie anschließend den Kartenstapel um und legen Sie ihn erneut in das Fach ein, um die Rückseiten zu drucken.

T10231644_de

2026-04 (M7.2)