AXIS Secure Entry for XProtect

Benutzerhandbuch

Inhalt

Zutrittskontrolle

Die Zutrittskontrolle ist eine Lösung, die physische Zutrittskontrolle mit Videosicherheit kombiniert. Mit dieser Integration können Sie ein Axis Zutrittssystem direkt über den Management Client konfigurieren. Das System lässt sich nahtlos in XProtect integrieren, sodass Bediener den Zugang überwachen und Zutrittskontrolle-Aktion im Smart Client durchführen können.

Hinweis

Anforderungen

- VMS-Version 2024 R1 oder höher.
- XProtect Zugriff-Lizenzen, siehe *Zugriff-Lizenzen*.
- Installieren Sie AXIS Optimizer auf dem Ereignis-Server und dem Management Client.

Die Ports 53459 und 53461 werden für eingehenden Datenaustausch (TCP) geöffnet, wenn Sie AXIS Optimizer über AXIS Secure Entry installieren.

Konfiguration der Zutrittskontrolle

Hinweis

Stellen Sie vor dem Start Folgendes sicher:

- Aktualisieren Sie die Software des Netzwerk-Tür-Controllers. Die Mindest- und empfohlene AXIS OS-Version für Ihre VMS-Version finden Sie in der folgenden Tabelle.
- Stellen Sie sicher, dass Datum und Uhrzeit korrekt sind.

AXIS Optimizer Version	AXIS OS Mindestversion	Empfohlene AXIS OS Version
5.6	12.6.94.1	12.6.94.1

So fügen Sie Ihrem System einen Axis Netzwerk-Tür-Controller hinzu:

1. Rufen Sie **Site Navigation (Standortnavigation)** > **Axis Optimizer** > **Access control (Zutrittskontrolle)** auf.
2. Wählen Sie unter **Configuration (Konfiguration)** die Option **Devices (Geräte)**.
3. Wählen Sie **Discovered devices (Erfasste Geräte)**, um die Liste der Geräte anzuzeigen, die Sie dem System hinzufügen können.
4. Wählen Sie die hinzuzufügenden Geräte aus.
5. Klicken Sie im Popup-Fenster auf **+ Add (+ Hinzufügen)** und geben Sie die Anmeldedaten für den Controller ein.

Hinweis

Die hinzugefügten Controller sollten auf der Registerkarte **Management (Verwaltung)** zu sehen sein.

Um einen Controller manuell zum System hinzuzufügen, klicken Sie auf **+ Add (+ Hinzufügen)** auf der Registerkarte **Management (Verwaltung)**.

Um Ihre Aktualisierung in das VMS zu integrieren, wenn Sie einen Tür-Controller-Name hinzufügen, entfernen oder bearbeiten:

- Gehen Sie zu **Site Navigation (Standortnavigation)** > **Access control (Zutrittskontrolle)** und klicken Sie auf die Integration der Zutrittskontrolle.
- Klicken Sie auf **Refresh Configuration (Konfiguration aktualisieren)** auf der Registerkarte **General settings (Allgemeine Einstellungen)**.

Vorgehensweise zum Konfigurieren der Zutrittskontrolle

1. Rufen Sie **Site Navigation (Standortnavigation)** > **Axis Optimizer** > **Access control (Zutrittskontrolle)** auf.

2. Informationen zum Bearbeiten der vordefinierten Identifizierungsprofile oder zum Erstellen eines neuen Identifizierungsprofils finden Sie unter .
3. Informationen zur Verwendung eines benutzerdefinierten Setups für Kartenformate und die PIN-Länge finden Sie unter .
4. Fügen Sie einen Zugang hinzu und wenden Sie ein Identifizierungsprofil auf den Zugang an. Siehe .
5. Fügen Sie eine Zone hinzu und fügen Sie der Zone Zugänge hinzu. Siehe .

Kompatibilität der Gerätesoftware für Tür-Steuerungen

Wichtig

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

- **Unterstützte AXIS OS Versionen:** Die oben aufgeführten unterstützten AXIS OS Versionen gelten nur bei einer Aktualisierung von der empfohlenen VMS-Originalversion 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 VMS-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.
- **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 VMS-Version liegt. Dann können Sie jederzeit problemlos auf die von empfohlene AXIS OS Version zurückstufen, solange diese innerhalb der Unterstützungsgrenzen für die VMS-Version liegt.
- **Empfehlungen für zukünftiges AXIS OS:** Verwenden Sie immer die empfohlene AXIS OS Version für die jeweilige VMS-Version, um die Systemstabilität und vollständige Kompatibilität zu gewährleisten.

Integration der Zutrittskontrolle

Um die Zutrittskontrolle in das VMS zu integrieren:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **Access Control (Zutrittskontrolle)**.
2. Klicken Sie mit der rechten Maustaste auf **Access Control (Zutrittskontrolle)** und klicken Sie auf **Create new... (Neu erstellen...)**.
3. Im Dialogfeld **Create Access Control System Integration (Systemintegration von Zutrittskontrolle erstellen)**:
   - Geben Sie einen Namen für die Integration ein.
   - Wählen Sie **AXIS Secure Entry** aus dem Drop-Down-Menü unter **Integration plug-in (Integrations-Plug-in)**.
   - Klicken Sie auf **Next (Weiter)**, bis Sie das Dialogfeld **Associate cameras (Kameras zuordnen)** sehen.
     So ordnen Sie Kameras Türzugriffspunkten zu:
     - Klicken Sie unter **Cameras (Kameras)** auf Ihr Gerät, um die Liste der im XProtect-System konfigurierten Kameras anzuzeigen.
     - Wählen Sie eine Kamera aus und ziehen Sie sie auf den Zugriffspunkt, mit dem Sie sie verbinden möchten.
     - Klicken Sie auf **Schließen**, um das Dialogfeld zu schließen.

Hinweis

- Weitere Informationen zur Integration der Zutrittskontrolle in XProtect finden Sie unter *Verwendung der Zutrittskontrolle in XProtect Smart Client*.
- Weitere Informationen zu den Eigenschaften der Zutrittskontrolle, wie allgemeine Einstellungen, Zugänge und zugehörige Kameras, Ereignisse der Zutrittskontrolle usw., finden Sie unter *Eigenschaften der Zutrittskontrolle*.

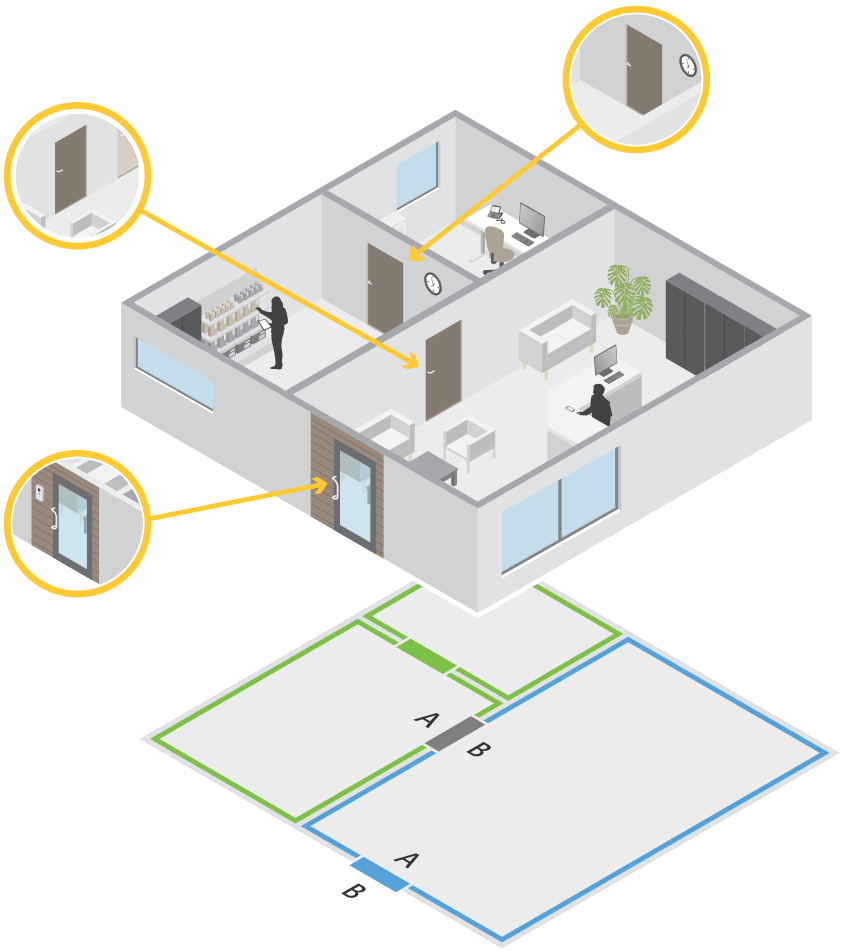
Türen und Bereiche

Gehen Sie zu **Site Navigation (Standortnavigation)** > **Axis Optimizer** >**Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)**, um einen Überblick zu erhalten und Zugänge und Zonen zu konfigurieren.

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)**.
Identifizierungsprofil	Ändern Sie das Identifizierungsprofil für Zugänge.
Secure Channel	Schalten Sie OSDP Secure Channel für einen bestimmten Leser ein oder aus.

Türen	
Bezeichnung	Der Name des Zugangs.
Tür-Controller	Die Tür-Steuerung, die mit dem Zugang verbunden ist.
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.
Kartenformate und PIN	Zeigt den Typ des Kartenformats oder die PIN-Länge an.
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.
Zonen	
Bezeichnung	Der Name der Zone.
Anzahl der Zugänge	Die Anzahl der Zugänge in der Zone.

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.
- Wenn einer Tür-Steuerung keine Zugänge zugewiesen sind und Sie eine neue Version von Axis Optimizer mit einer Tür-Steuerung mit älterer Software 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 Software.

Erstellen einer neuen Zugangskonfiguration zum Hinzufügen einer Tür:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **Axis Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)**.
2. Klicken Sie auf + **Add door (Zugang hinzufügen)**.

3. Geben Sie einen Namen für den Zugang ein.
4. Wählen Sie im Drop-Down Menü **Controller** eine Tür-Steuerung aus. Der Controller ist ausgegraut, wenn Sie keine weitere Tür hinzufügen können, wenn er offline ist oder HTTPS nicht aktiviert ist.
5. Wählen Sie im Drop-Down Menü **Door type (Zugangsart)** die zu erstellende Zugangsart aus.
6. Klicken Sie auf **Next (Weiter)**, um die Seite zur Zugangskonfiguration aufzurufen.
7. Wählen Sie im Drop-Down Menü **Primary lock (Primäres Schloss)** einen Relay-Port aus.
8. Um zwei Schlösser am Zugang zu konfigurieren, wählen Sie den anderen Relay-Port im Drop-Down Menü **Secondary lock (Sekundäres Schloss)** aus.
9. Wählen Sie ein Identifizierungsprofil aus. Siehe .
10. Konfigurieren Sie die Zugangseinstellungen. Siehe .
11. Richten Sie einen überwachten Zugang ein. Siehe dazu .
12. **Save (Speichern)** anklicken.

Kopieren einer vorhandenen Zugangskonfiguration zum Hinzufügen eines Zugangs:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **Axis Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)**.
2. Klicken Sie auf **Add door (Zugang hinzufügen)**.
3. Geben Sie einen Namen für den Zugang ein.
4. Wählen Sie im Drop-Down Menü **Controller** eine Tür-Steuerung aus.
5. Klicken Sie auf **Next (Weiter)**.
6. 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.
7. Sie können die Einstellungen jederzeit ändern.
8. **Save (Speichern)** anklicken.

So bearbeiten Sie einen Zugang:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **Axis Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)** > **Doors (Zugänge)**.
2. Wählen Sie einen Zugang in der Liste aus.
3. Klicken Sie auf **Edit (Bearbeiten)**.
4. Ändern Sie die Einstellungen und klicken Sie auf **Save (Speichern)**.

So entfernen Sie einen Zugang:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **Axis Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)** > **Doors (Zugänge)**.
2. Wählen Sie einen Zugang in der Liste aus.
3. Klicken Sie auf **Remove (Entfernen)**.
4. **Yes (Ja)** anklicken

Um Ihre Aktualisierung in das VMS zu integrieren, wenn Sie einen Türname hinzufügen, entfernen oder bearbeiten:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **Access control (Zutrittskontrolle)** und klicken Sie auf die Integration der Zutrittskontrolle.
2. Klicken Sie auf **Refresh Configuration (Konfiguration aktualisieren)** auf der Registerkarte **General settings (Allgemeine Einstellungen)**.

Einstellungen der Tür

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **Axis Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)**.
2. Wählen Sie den Zugang aus, den Sie bearbeiten möchten.
3. Klicken Sie auf **Edit (Bearbeiten)**.

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.

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. Gehen Sie zu **Site Navigation (Standortnavigation)** > **Axis Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)**.
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**.

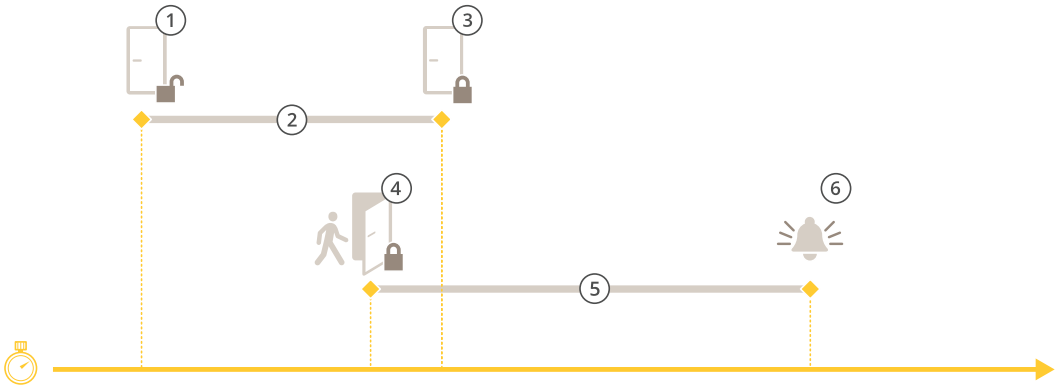
Zwei-Personen-Regel	
Side A (Seite A) und **Side B (Seite B)**	Wählen Sie aus, auf welchen Seiten der Tür die Regel verwendet werden soll.
Zeitschemata	Wählen Sie „While the rule is active" (Während die Regel aktiv ist).
Zeitüberschreitung (Sekunden)	Timeout ist die maximal zulässige Zeit zwischen dem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

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

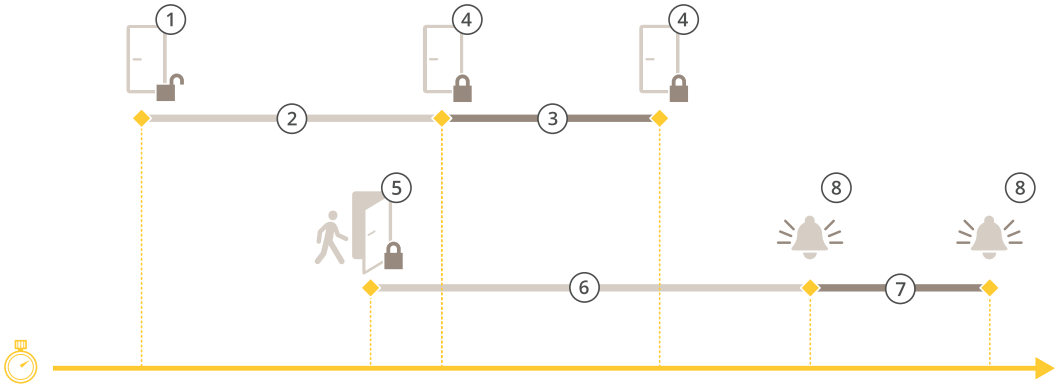
1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **Axis Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)**.
2. Wählen Sie die Tür aus, für die Sie eine Sicherheitsstufe konfigurieren möchten.
3. Klicken Sie auf **Edit (Bearbeiten)**.
4. Klicken Sie 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. Wechseln Sie zu **Cardholder management (Karteninhaberverwaltung)**.
   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*

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
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 .

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 Software 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 im VMS zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge 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**.

Leser hinzufügen

Sie können eine Tür-Steuerung zum Verwenden von zwei 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 .

1. Rufen Sie die Seite zur Zugangskonfiguration auf. Siehe hierzu .
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.

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.

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 .

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 hierzu .
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 .

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.

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)** > **Zones (Zonen)**.
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. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)** > **Zones (Zonen)**.
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. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)** > **Zones (Zonen)**.
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. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)**.
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 .
- Verbindung zwischen dem Tür-Controller und dem Leser, der Wiegand-Protokolle verwendet. Siehe dazu .
- Verbindung zwischen Tür-Controller und REX-Gerät. Siehe .

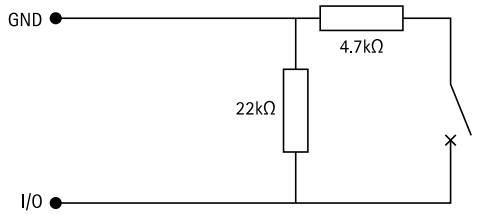
Um überwachte Eingänge zu verwenden:

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

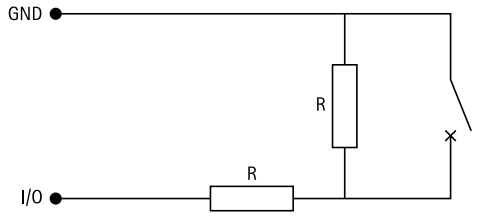
Paralleler Anschluss hat Vorrang

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.



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. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)**.
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.

Kartenformate und PIN

Ein Kartenformat definiert, wie Daten auf einer Karte gespeichert werden. Es handelt sich um eine Übersetzungstabelle zwischen den eingehenden Daten und den validierten Daten im System. Jedes Kartenformat verfügt über einen eigenen Satz an Regeln für die Organisation der gespeicherten Informationen. Durch Definieren eines Kartenformats wird festgelegt, wie das System die Informationen interpretiert, die der Controller vom Kartenlesegerät erhält.

Ihnen stehen vordefinierte, häufig verwendete Kartenformate zur Verfügung, die Sie nach Bedarf verwenden oder bearbeiten können. Außerdem können Sie benutzerdefinierte Kartenformate erstellen.

Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Card formats and PIN (Kartenformate und PIN)**, 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.

So erstellen Sie ein Kartenformat:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Card formats and PIN (Kartenformate und PIN)**.
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.

ⓘ	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).

So bearbeiten Sie ein Kartenformat:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Card formats and PIN (Kartenformate und PIN)**.
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. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Card formats and PIN (Kartenformate und PIN)**.
2. Wählen Sie ein benutzerdefiniertes Kartenformat aus, klicken Sie auf und dann auf **Yes (Ja)**.

Zurücksetzten eines vordefinierten Kartenformats:

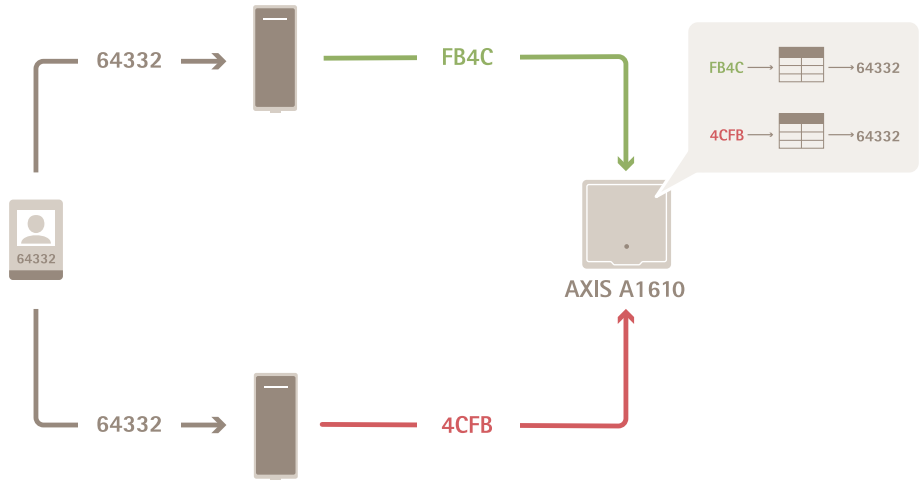
1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Card formats and PIN (Kartenformate und PIN)**.
2. Klicken Sie auf , um ein Kartenformat auf die Standardfeldzuordnung zurückzusetzen.

So konfigurieren Sie die PIN-Länge:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Card formats and PIN (Kartenformate und PIN)**.
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**.

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*

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.

Identifikationsarten sind Träger der Zugangsdaten, die für die Nutzung eines Zugangs erforderlich sind. Gängige Identifikationsarten sind Tokens, persönliche Identifikationsnummern (PINs), Fingerabdrücke, Gesichtsmasken und REX-Geräte. Eine Identifikationsart kann eine oder mehrere Arten von Informationen enthalten.

Zeitpläne, auch bekannt als **Time profiles (Zeitprofile)**, werden im Management Client erstellt. Informationen zur Einstellung von Zeitprofilen finden Sie unter *Zeitprofile (Erläuterung)*.

Unterstützte Identifikationsarten: Karte, PIN und REX.

Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Identification profiles (Identifizierungsprofile)**.

Ihnen stehen fünf Standard-Identifizierungsprofile zur Verfügung, die Sie nach Bedarf verwenden oder bearbeiten können.

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.

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

So erstellen Sie ein Identifizierungsprofil:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Identification profiles (Identifizierungsprofile)**.
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. Konfigurieren Sie das Identifizierungsprofil für eine Seite des Zugangs.
6. Wiederholen Sie die vorherigen Schritte auf der anderen Seite des Zugangs.
7. Klicken Sie auf **OK**.

So bearbeiten Sie ein Identifizierungsprofil:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Identification profiles (Identifizierungsprofile)**.
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**.

So entfernen Sie ein Identifizierungsprofil:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Identification profiles (Identifizierungsprofile)**.
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**.

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.

Verschlüsselte Kommunikation

OSDP mit Secure Channel

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 **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Encrypted communication (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*.

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.
- 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 53461.

Vorgehensweise

1. Konfigurieren Sie einen Server als Subserver und erstellen Sie die Konfigurationsdatei. Siehe .
2. Konfigurieren Sie einen Server als Hauptserver und importieren Sie die Konfigurationsdatei der Subserver. Siehe .
3. Konfigurieren Sie globale Karteninhaber und Karteninhabergruppen auf dem Hauptserver. Siehe und .
4. Auf dem Subserver können Sie die globalen Karteninhaber und Karteninhabergruppen anzeigen und überwachen. Siehe hierzu .

Die Konfigurationsdatei vom Subserver erstellen

1. Wechseln Sie vom Subserver zu **AXIS Optimizer** > **Access Control (Zutrittskontrolle)** > **Multi server (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 **AXIS Optimizer** > **Access Control (Zutrittskontrolle)** > **Multi server (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 **AXIS Optimizer** > **Access Control (Zutrittskontrolle)** > **Multi server (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:

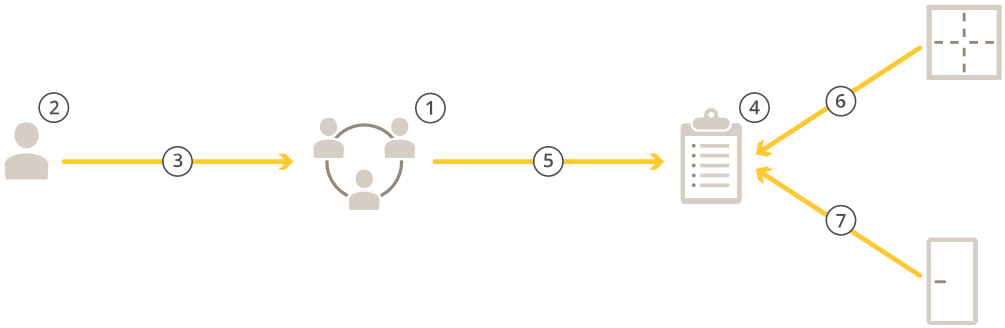
1. Vom Hauptserver:
   1.1. Rufen Sie **Access management (Zugriffsverwaltung)** > **Dashboard** auf.
   1.2. Ändern Sie die globalen Karteninhaber und Gruppen in lokale Karteninhaber und Gruppen.
   1.3. Rufen Sie **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Multi server (Multi-Server)** 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 **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Multi server (Multi-Server)** auf.
   – Klicken Sie auf **Sub server (Subserver)** und dann auf **Revoke server (Server sperren)**.

Zutrittsverwaltung

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

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. Fügen Sie Gruppen hinzu. Siehe .
2. Fügen Sie Karteninhaber hinzu. Siehe .
3. Fügen Sie Karteninhaber und Gruppen hinzu.
4. Fügen Sie Zugangsregeln hinzu. Siehe .
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.

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Cardholder management (Verwaltung von Karteninhabern)**.

2. Navigieren Sie zu **Cardholders (Karteninhaber)** und klicken Sie dann auf **+ Add (+ Hinzufügen)**.
3. Geben Sie den Vor- und Nachnamen des Karteninhabers ein und klicken Sie auf **Next (Weiter)**.
4. Klicken Sie optional auf **Advanced (Erweitert)** und wählen Sie die gewünschten Optionen aus.
5. Fügen Sie Zugangsdaten für den Karteninhaber hinzu. Siehe
6. **Save (Speichern)** anklicken.
7. Fügen Sie den Karteninhabers zu einer Gruppe hinzu.
   7.1. Wählen Sie unter **Groups (Gruppen)** die Gruppe aus, zu der Sie den Karteninhaber hinzufügen möchten, und klicken Sie auf **Edit (Bearbeiten)**.
   7.2. Klicken Sie auf **+ Add (+ Hinzufügen)** und wählen Sie den Karteninhaber aus, den Sie zu der Gruppe hinzufügen möchten. Sie können mehrere Karteninhaber auswählen.
   7.3. Klicken Sie auf **Hinzufügen**.
   7.4. **Save (Speichern)** anklicken.

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.
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 .

Zugangsdaten hinzufügen

Sie können einem Karteninhaber die folgenden Arten von Zugangsdaten hinzufügen:

- PIN
- Karte
- Nummernschild
- Mobiltelefon

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**.

Siehe das Beispiel in .

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 eine Zwangs-PIN zum Auslösen eines stillen Alarms zu verwenden, aktivieren Sie **Duress PIN (Zwangs-PIN)** und geben Sie eine Zwangs-PIN ein.
4. Klicken Sie auf **Hinzufügen**.

Eine PIN ist immer gültig. Sie können auch eine Zwangs-PIN konfigurieren, die zwar das Öffnen des Zugangs ermöglicht und dabei einen stillen Alarm im System auslöst.

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)**.
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**.

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.

Gültig bis	
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.

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 Secure Entry for XProtect hinzu.
2. Legen Sie mithilfe der Funktion **Synchronize with server computer time (Mit Computerzeit des Servers synchronisieren)** Datum und Uhrzeit für die neuen Geräte fest.
3. Aktualisieren Sie die Software der neuen Geräte auf die neueste verfügbare Version.
4. Fügen Sie einen neuen Zugang hinzu, die mit Ihrer Tür-Steuerung verbunden ist. Siehe .
   4.1. Fügen Sie einen Kartenleser hinzu unter **Seite A**. Siehe .
   4.2. Wählen Sie unter **Türeinstellungen** die Option **AXIS License Plate Verifier** als **Lesertyp** und geben Sie einen Namen für den Leser ein.
   4.3. Fügen Sie optional einen Leser oder ein REX-Gerät auf **Seite B** hinzu.
   4.4. **OK** anklicken.
5. Installieren und aktivieren Sie AXIS License Plate Verifier auf Ihrer Kamera. Siehe das Benutzerhandbuch zu *AXIS License Plate Verifier*.
6. Starten Sie AXIS License Plate Verifier.
7. Konfigurieren Sie AXIS License Plate Verifier.
   7.1. Gehen Sie zu **Konfiguration > Zutrittskontrolle > Verschlüsselte Kommunikation**.
   7.2. Klicken Sie unter **Authentifizierungsschlüssel für externes Peripheriegerät** auf **Authentifizierungsschlüssel anzeigen** und **Schlüssel kopieren**.
   7.3. Öffnen Sie AXIS License Plate Verifier über die Weboberfläche der Kamera.
   7.4. Setup nicht ausführen.
   7.5. **Settings (Einstellungen)** aufrufen.
   7.6. Wählen Sie unter **Zutrittskontrolle** die Option **Sicherer Zugang** as **Typ**.
   7.7. Geben Sie in **IP address (IP-Adresse)** die IP-Adresse für die Tür-Steuerung ein.
   7.8. Fügen Sie in **Authentifizierungsschlüssel** den zuvor kopierten Authentifizierungsschlüssel ein.
   7.9. **Connect (Verbinden)** anklicken.
   7.10. Wählen Sie unter **Door controller name (Tür-Steuerung)** Ihre Tür-Steuerung aus.
   7.11. Wählen Sie unter **Lesername** den Leser aus, den Sie zuvor hinzugefügt haben.
   7.12. Schalten Sie Integration ein.
8. Fügen Sie den Karteninhaber hinzu, dem Sie Zugriff gewähren möchten. Siehe .
9. Fügen Sie dem neuen Karteninhaber die Zugangsdaten zum Fahrzeugkennzeichen hinzu. Siehe .
10. Fugen Sie eine Zugangsregel hinzu. Siehe .
    10.1. Einen Zeitplan hinzufügen.

10.2. Fügen Sie den Karteninhaber hinzu, dem Sie Zugang über das Fahrzeugkennzeichen gewähren möchten.

10.3. 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. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Cardholder management (Verwaltung von Karteninhabern)**.
2. Navigieren Sie zu **Groups (Gruppen)** und klicken Sie dann 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 .
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.

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. Gehen Sie zu **Access control (Zutrittskontrolle)** > **Cardholder management (Karteninhaberverwaltung)**.
2. Klicken Sie unter **Access rule (Zugangsregel)** auf **+ Add (+ Hinzufügen)**.
3. Geben Sie einen Namen für die Regel ein und klicken Sie auf **Next (Weiter)**.
4. Konfigurieren der Karteninhaber und Gruppen:
   4.1. Klicken Sie unter **Cardholders (Karteninhaber)** oder **Groups (Gruppen)** auf **+ Add (+ Hinzufügen)**.
   4.2. Wählen Sie Karteninhaber bzw. Gruppen und klicken Sie auf **Add (Hinzufügen)**.
5. Zugänge und Bereiche konfigurieren:
   5.1. Klicken Sie unter **Doors (Zugänge)** oder **Zones (Zonen)** auf **+ Add (+ Hinzufügen)**.
   5.2. Wählen Sie Zugänge bzw. Zonen und klicken Sie auf **Add (Hinzufügen)**.
6. Konfigurieren der Zeitpläne:
   6.1. Klicken Sie unter **Schedules (Zeitpläne)** auf **+ Add (+ Hinzufügen)**.
   6.2. Wählen Sie einen oder mehrere Zeitpläne aus und klicken Sie auf **Add (Hinzufügen)**.
7. **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.

Zugänge und Zonen manuell entriegeln

Informationen über manuelle Aktionen, wie das manuelle Entsperren eines Zugangs, finden Sie unter .

Informationen über manuelle Aktionen, wie das manuelle Entsperren einer Zone, finden Sie unter .

Berichte zur Systemkonfiguration exportieren

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

1. Rufen Sie **Reports (Berichte)** > **System configuration (Systemkonfiguration)** auf.
2. Wählen Sie die Berichte aus, die Sie exportieren möchten, und klicken Sie auf **Download**.

Angaben zum Karteninhaber	Dieser Bericht enthält Informationen zu Karteninhabern, Zugangsdaten, Kartenüberprüfung und zur letzten Transaktion.
Zugriff für Karteninhaber	Dieser Bericht enthält die Karteninhaberinformationen und Informationen über die Karteninhabergruppen, Zugangsregeln, Zugänge und Zonen, mit denen der Karteninhaber in Verbindung steht.
Cardholders group access report (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.
Zugriffsregel	Dieser Bericht enthält den Namen der Zugangsregel und Informationen zu den Karteninhabern, Karteninhabergruppen, Zugangsregeln, Zugänge und Zonen, mit denen die Zugangsregel in Verbindung steht.
Zutritt über die Tür	Dieser Bericht enthält den Namen des Zugangs und Informationen zu den Karteninhabern, Karteninhabergruppen, Zugangsregeln und Zonen, mit denen der Zugang in Verbindung steht.
Zonenzugriff	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. Rufen Sie **Reports (Berichte)** > **Cardholder activity (Karteninhaberaktivitäten)** auf.
2. Klicken Sie auf **+ Add (+ Hinzufügen)** und wählen Sie **Appell / Musterung**.
3. Geben Sie einen Namen für den Bericht ein.
4. Wählen Sie die Zonen aus, die in den Bericht aufgenommen werden sollen.
5. Wählen Sie die Gruppen aus, die Sie in den Bericht aufnehmen möchten.
6. Wenn Sie einen Musterungsbericht wünschen, wählen Sie **Mustering point (Sammelpunkt)** und einen Kartenleser für den Sammelpunkt.
7. Wählen Sie einen Zeitrahmen für den Bericht aus.
8. **Save (Speichern)** anklicken.
9. 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.

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 .

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.

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 Secure Entry for XProtect 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

Sichern und Wiederherstellen

Jede Nacht werden automatische Datensicherungen durchgeführt. Die drei neuesten Sicherungsdateien werden unter C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\backup gespeichert. So stellen Sie diese Dateien wieder her:

1. Verschieben Sie die Sicherungsdatei nach C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\restore.
2. Starten Sie AXIS Secure Entry mit einer der folgenden Methoden neu:
   - Starten Sie das MSC-Programm (Dienste), suchen Sie „AXIS Optimizer Secure Entry Service" und starten Sie neu.
   - Starten Sie Ihren Computer neu.

T10234037_de

2025-10 (M3.2)