AXIS Secure Entry for XProtect

User manual

Table of Contents

Access control

Access control is a solution that combines physical access control with video surveillance. This integration lets you configure an Axis access control system directly from the Management Client. The system seamlessly integrates with XProtect, allowing operators to monitor access and perform access control actions in the Smart Client.

Note

Requirements

- VMS version 2024 R1 or later.
- XProtect Access licenses, see *access licenses*.
- Install AXIS Optimizer on the event server and Management Client.

Port 53459 and 53461 will open for incoming traffic (TCP) when you install AXIS Optimizer through AXIS Secure Entry.

Access control configuration

Note

Before you start, do the following:

- Upgrade the door controller software. See the table below for minimum and recommended AXIS OS version for your VMS version.
- Make sure the date and time are correct.

AXIS Optimizer version	Minimum AXIS OS version	Recommended AXIS OS version
5.6	12.6.94.1	12.6.94.1

To add an Axis network door controller to your system:

1. Go to **Site Navigation** > **Axis Optimizer** > **Access control**.
2. Under **Configuration**, select **Devices**.
3. Select **Discovered devices** to see the list of units you can add to the system.
4. Select the units you want to add.
5. Click **+ Add** in the popup window and provide the credentials for the controller.

Note

You should see added controllers in the **Management** tab.

To manually add a controller to the system, click **+ Add** in the **Management** tab.

To integrate your update into the VMS whenever you add, remove, or edit a door controller name:

- Go to **Site Navigation** > **Access control** and click on the Access Control integration .
- Click **Refresh Configuration** in the **General settings** tab.

Workflow to configure Access control

1. Go to **Site Navigation** > **Axis Optimizer** > **Access control**.
2. To edit the predefined identification profiles or create a new identification profile, see .
3. To use a custom setup for card formats and PIN length, see .
4. Add a door and apply an identification profile to the door. See .
5. Add a zone and add doors to the zone. See .

Device software compatibility for door controllers

Important

Keep in mind the following when you upgrade the AXIS OS on your door controller:

- **Supported AXIS OS versions:** The supported AXIS OS versions listed above only apply when upgrading from their original recommended VMS version and when the system has a door. If the system doesn't meet these conditions, you must upgrade to the recommended AXIS OS version for the specific VMS version.
- **Minimum supported AXIS OS version:** The oldest installed AXIS OS version in the system determines the minimum supported AXIS OS version, with a limit of two prior versions.
- **Upgrading beyond recommended AXIS OS version:** Suppose you upgrade to an AXIS OS version above the recommended one for a particular VMS version. Then, you can always downgrade back to the recommended AXIS OS version without any issues, as long as it's within the support limits set for the VMS version.
- **Future AXIS OS recommendations:** Always follow the recommended AXIS OS version for the respective VMS version to ensure system stability and full compatibility.

Access control integration

To integrate access control into the VMS:

1. Go to **Site Navigation** > **Access Control**.
2. Right-click **Access Control** and click **Create new...**.
3. In the **Create Access Control System Integration** dialog:
   - Enter a name for the integration.
   - Select **AXIS Secure Entry** from the drop-down menu in **Integration plug-in**.
   - Click **Next** until you see the **Associate cameras** dialog.
     To associate cameras to door access points:
     - Click your device under **Cameras** to see the lists of cameras configured in the XProtect system.
     - Select and drag a camera to the access point you want to associate it with.
     - Click **Close** to close the dialog.

Note

- For more information about access control integration in XProtect, see *Using access control in XProtect Smart Client*.
- For more information about access control properties, such as general settings, doors and associated cameras, access control events, and so on, see *Access control properties*.

Doors and zones

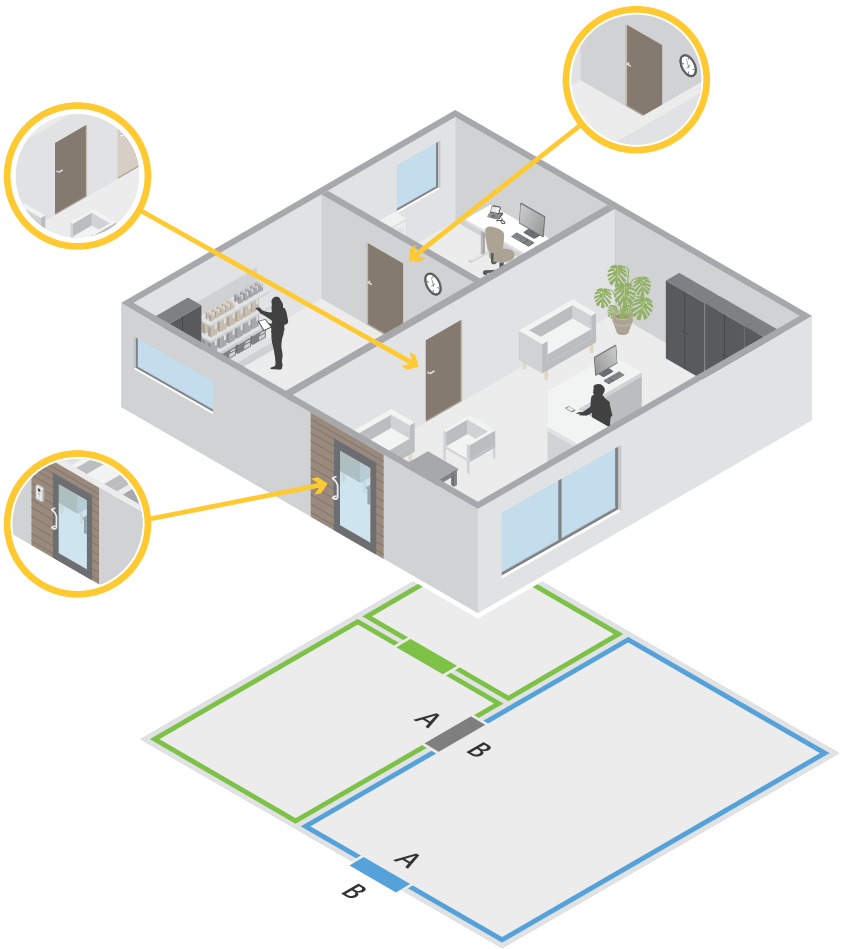
Go to **Site Navigation** > **Axis Optimizer** >**Access control** > **Doors and zones** to get an overview and configure doors and zones.

Pin chart	View the controller pin chart associated with a door. If you want to print the pin chart, click **Print**.
Identification profile	Change identification profile on doors.
Secure Channel	Turn on or off OSDP Secure Channel for a specific reader.

Doors	
Name	The name of the door.

Door controller	The door controller connected to the door.
Side A	The zone that side A of the door is in.
Side B	The zone that side B of the door is in.
Identification profile	The identification profile applied to the door.
Card formats and PIN	Shows the type of card formats or PIN length.
Status	The status of the door. • **Online:** The door is online and works correctly. • **Reader offline:** The reader in the door configuration is offline. • **Reader error:** The reader in the door configuration doesn't support secure channel or secure channel is turned off for the reader.
Zones	
Name	The name of the zone.
Number of doors	The number of doors included in the zone.

Example of doors and zones



- There are two zones: green zone and blue zone.
- There are three doors: green door, blue door, and brown door.

- The green door is an internal door in the green zone.
- The blue door is a perimeter door for the blue zone only.
- The brown door is a perimeter door for both the green zone and blue zone.

Add a door

Note

- You can configure a door controller with one door that has two locks, or two doors that have one lock each.
- If a door controller has no doors and you're using a new version of Axis Optimizer with older software on the door controller, the system will prevent you from adding a door. However, the system does allow new doors on system controllers with older software if there's already an existing door.

Create a new door configuration to add a door:

1. Go to **Site Navigation** > **Axis Optimizer** > **Access control** > **Doors and zones**.
2. Click + **Add door**.
3. Enter a door name.
4. In the **Controller** drop-down menu, select a door controller. The controller grays out when you can't add another door, when it's offline, or HTTPS isn't active.
5. In the **Door type** drop-down menu, select the type of door you want to create.
6. Click **Next** to go to the door configuration page.
7. In the **Primary lock** drop-down menu, select a relay port.
8. To configure two locks on the door, select a relay port from the **Secondary lock** drop-down menu.
9. Select an identification profile. See .
10. Configure the door settings. See .
11. Set up a monitoring door. See .
12. Click **Save**.

Copy an existing door configuration to add a door:

1. Go to **Site Navigation** > **Axis Optimizer** > **Access control** > **Doors and zones**.
2. Click + **Add door**.
3. Enter a door name.
4. In the **Controller** drop-down menu, select a door controller.
5. Click **Next**.
6. In the **Copy configuration** drop-down menu, select an existing door configuration. It shows the connected doors, and the controller grays out if it was configured with two doors or one door with two locks.
7. Change the settings if you want.
8. Click **Save**.

To edit a door:

1. Go to **Site Navigation** > **Axis Optimizer**> **Access control** > **Doors and zones** > **Doors**.
2. Select a door in the list.
3. Click **Edit**.
4. Change the settings and click **Save**.

To remove a door:

1. Go to **Site Navigation** > **Axis Optimizer**> **Access control** > **Doors and zones** > **Doors**.
2. Select a door in the list.
3. Click **Remove**.
4. Click **Yes**.

To integrate your update into the VMS whenever you add, remove, or edit a door name:

1. Go to **Site Navigation** > **Access control** and click on the Access Control integration.
2. Click **Refresh Configuration** in the **General settings** tab.

Door settings

1. Go to **Site Navigation** > **Axis Optimizer**> **Access control** > **Doors and zones**.
2. Select the door you want to edit.
3. Click **Edit**.

Access time (sec)	Set the number of seconds the door remains unlocked after access was granted. The door remains unlocked until the door opens or until the set time ends. The door locks when it closes even if there is access time left.
Open-too-long time (sec)	Only valid if you have configured a door monitor. Set the number of seconds the door stays open. If the door is open when the set time ends, it triggers the door open too long alarm. Set up an action rule to configure which action the open too long event triggers.
Long access time (sec)	Set the number of seconds the door remains unlocked after access was granted. Long access time overrides the access time for cardholders that has this setting turned on.
Long open-too-long time (sec)	Only valid if you have configured a door monitor. Set the number of seconds the door stays open. If the door is open when the set time ends, it triggers the door open-too-long event. Long open-too-long time overrides the already set open-too-long time for cardholders if you turn on the **Long access time** setting.
Relock delay time (ms)	Set the time, in milliseconds, that the door stays unlocked after the it's opened or closed.
Relock	• **After opening:** Only valid if you added a door monitor. • **After closing:** Only valid if you added a door monitor.

Door security level

You can add the following security features to the door:

Two-person rule – The two-person rule requires two people to use a valid credential to gain access.

Double-swipe – The double-swipe allows a cardholder override the current state of a door. For example, they can use it to lock or unlock a door outside the regular schedule, which is more convenient than going into the system to unlock the door. Double-swipe does not affect an existing schedule. For example, if a door is scheduled to lock at closing time, and employee leaves for lunch break, the door will still lock according to the schedule.

You can configure the security level while you're adding a new door, or you can do it on an existing door.

To add **Two-person rule** to an existing door:

1. Go to **Site Navigation** > **Axis Optimizer** > **Access control** > **Doors and zones**.
2. Select the door you want to configure a security level for.
3. Click **Edit**.
4. Click **Security level**.
5. Turn on **Two-person rule**.
6. Click **Apply**.

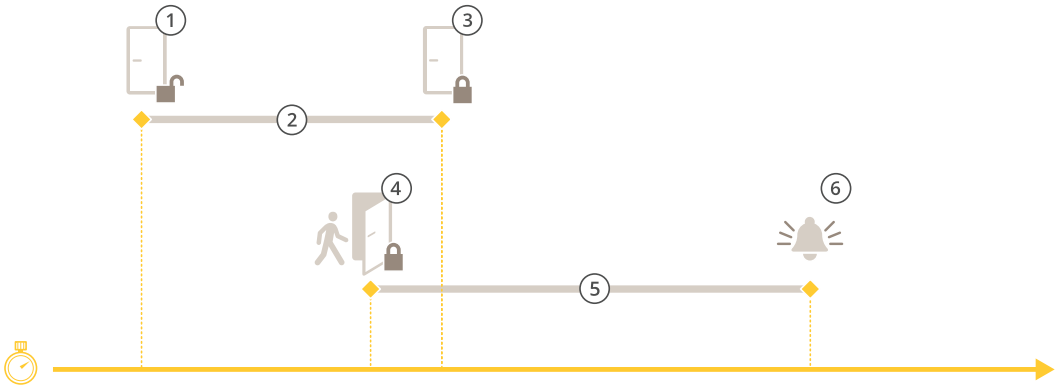
Two-person rule	
Side A and **Side B**	Select which sides of the door to use the rule on.
Schedules	Select when the rule is active.
Timeout (seconds)	Timeout is the maximum allowed time between card swipes or other type of valid credential.

To add **Double-swipe** to an existing door:

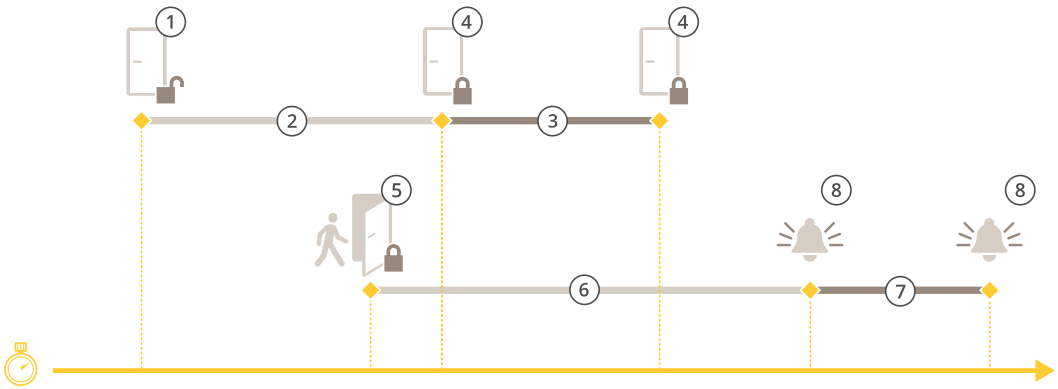
1. Go to **Site Navigation** > **Axis Optimizer** > **Access control** > **Doors and zones**.
2. Select the door you want to configure a security level for.
3. Click **Edit**.
4. Click **Security level**.
5. Turn on **Double-swipe**.
6. Click **Apply**.
7. Apply **Double-swipe** to a cardholder.
   7.1. Go to **Cardholder management**.
   7.2. Click ⋮ on the cardholder you want to edit and click **Edit**.
   7.3. Click **More**.
   7.4. Select **Allow double-swipe**.
   7.5. Click **Apply**.

Double-swipe	
Timeout (seconds)	Timeout is the maximum allowed time between card swipes or other type of valid credential.

Time options



1 *Access granted - lock unlocks*
2 *Access time*
3 *No action taken - lock locks*
4 *Action taken (door opened) - lock locks or stays unlocked until door closes*
5 *Open-too-long time*
6 *Open-too-long alarm goes off*



1 *Access granted - lock unlocks*
2 *Access time*
3 *2+3: Long access time*
4 *No action taken - lock locks*
5 *Action taken (door opened) - lock locks or stays unlocked until door closes*
6 *Open-too-long time*
7 *6+7: Long open-too-long time*
8 *Open-too-long alarm goes off*

Add a door monitor

A door monitor is a door position switch that monitors the physical state of a door. You can add a door monitor to your door and configure how to connect the door monitor.

1. Go to the door configuration page. See
2. Under **Sensors**, click **Add**.
3. Select **Door monitor sensor**.
4. Select the I/O port you want to connect the door monitor to.
5. Under **Door open if**, select how the door monitor circuits are connected.

6. To ignore the state changes of the digital input before it enters a new stable state, set a **Debounce time**.
7. To trigger an event when an interruption in the connection between the door controller and the door monitor occurs, turn on **Supervised input**. See .

Door open if	
Circuit is open	The door monitor circuit is normally closed. The door monitor sends the door an open signal when the circuit is open. The door monitor sends the door a closed signal when the circuit is closed.
Circuit is closed	The door monitor circuit is normally open. The door monitor sends the door an open signal when the circuit is closed. The door monitor sends the door a closed signal when the circuit is open.

Add a monitoring door

A monitoring door is a door type that can show you if it's open or closed. For example, you can use this on a fire safety door that doesn't require a lock but where you need to know if the door is open.

A monitoring door is different from a regular door with a door monitor. A regular door with a door monitor supports locks and readers but requires a door controller. A monitoring door supports one door position sensor but only requires a network I/O relay module connected to a door controller. You can connect up to five door position sensors to one network I/O relay module.

Note

A monitoring door requires an AXIS A9210 Network I/O Relay Module with the latest software including the AXIS Monitoring Door ACAP application.

To set up a monitoring door:

1. Install your AXIS A9210 and upgrade it with the latest version of AXIS OS.
2. Install the door position sensors.
3. In the VMS, go to **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones**.
4. Click **Add door**.
5. Enter a name.
6. Under **Type**, select **Monitoring door**.
7. Under **Device**, select your network I/O relay module.
8. Click **Next**.
9. Under **Sensors**, click **+ Add** and select **Door position sensor**.
10. Select the I/O that's connected to the door position sensor.
11. Click **Add**.

Add a reader

You can configure a door controller to use two wired readers. Select to add a reader on one side or both sides of a door.

If you apply a custom setup of card formats or PIN length to a reader, you can see it in **Card formats** under **Configuration > Access control > Doors and zones**. See .

1. Go to the door configuration page. See .
2. Under one side of the door, click **Add**.
3. Select **Card reader**.

4. Select the **Reader type**.
5. To use a custom PIN length setup for this reader.
   5.1. Click **Advanced**.
   5.2. Turn on **Custom PIN length**.
   5.3. Set the **Min PIN length**, **Max PIN length**, and **End of PIN character**.
6. To use a custom card format for this reader.
   6.1. Click **Advanced**.
   6.2. Turn on **Custom card formats**.
   6.3. Select the card formats you want to use for the reader. If a card format with the same bit length is already in use, you must deactivate it first. A warning icon displays in the client when the card format setup is different from the configured system setup.
7. Click **Add**.
8. To add a reader to the other side of the door, do this procedure again.

Reader type	
OSDP RS485 half duplex	For RS485 readers, select **OSDP RS485 half duplex** and a reader port.
Wiegand	For readers that use Wiegand protocols, select **Wiegand** and a reader port.

Wiegand	
LED control	Select **Single wire** or **Dual wire (R/G)**. Readers with dual LED control use different wires for the red and green LEDs.
Tamper alert	Select when the reader tamper input is active. • **Open circuit**: The reader sends the door the tamper signal when the circuit is open. • **Closed circuit**: The reader sends the door the tamper signal when the circuit is closed.
Tamper debounce time	To ignore the state changes of the reader tamper input before it enters a new stable state, set a **Tamper debounce time**.
Supervised input	Turn on to trigger an event when there is interruption in the connection between the door controller and the reader. See .

Add a REX device

You can select to add a request to exit (REX) device on one side or both sides of the door. A REX device can be a PIR sensor, REX button, or push bar.

1. Go to the door configuration page. See .
2. Under one side of the door, click **Add**.
3. Select **REX device**.
4. Select the I/O port that you want to connect the REX device to. If there is only one port available, it will be selected automatically.

5. Select what **Action** to trigger when the door receives the REX signal.
6. Under **REX active**, select the door monitor circuit connection.
7. To ignore the state changes of the digital input before it enters a new stable state, set a **Debounce time (ms)**.
8. To trigger an event when an interruption in the connection between the door controller and the REX device occurs, turn on **Supervised input**. See .

Action	
Unlock door	Select to unlock the door when it receives the REX signal.
None	Select if you don't want to trigger any action when the door receives the REX signal.

REX active	
Circuit is open	Select if the REX circuit is normally closed. The REX device sends the signal when the circuit is open.
Circuit is closed	Select if the REX circuit is normally open. The REX device sends the signal when the circuit is closed.

Add a zone

A zone is a specific physical area with a group of doors. You can create zones and add doors to the zones. There are two types of doors:

- **Perimeter door:** Cardholders enter or leave the zone through this door.
- **Internal door:** An internal door within the zone.

Note

A perimeter door can belong to two zones. An internal door can only belong to one zone.

1. Go to **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** > **Zones**.
2. Click + **Add zone**.
3. Enter a zone name.
4. Click **Add door**.
5. Select the doors you want to add to the zone, and click **Add**.
6. The door is set as a perimeter door by default. To change it, select **Internal door** from the drop-down menu.
7. A perimeter door uses door side A as entrance to the zone by default. To change it, select **Leave** from the drop-down menu.
8. To remove a door from the zone, select it and click **Remove**.
9. Click **Save**.

To edit a zone:

1. Go to **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** > **Zones**.
2. Select a zone in the list.
3. Click **Edit**.
4. Change the settings and click **Save**.

To remove a zone:

1. Go to **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** > **Zones**.
2. Select a zone in the list.
3. Click **Remove**.
4. Click **Yes**.

Zone security level

You can add the following security feature to a zone:

Anti-passback – Prevents people from using the same credentials as someone who entered an area before them. It enforces that a person must first exit the area before they can use their credentials again.

Note

- With anti-passback, all doors in the zone must have door position sensors so the system can register that a user opened the door after swiping their card.
- If a door controller goes offline, anti-passback works as long as all doors in the zone belong to the same door controller. However, if the doors in the zone belong to different door controllers that go offline, anti-passback stops working.

You can configure the security level while you add a new zone, or you can do it on an existing zone. To add a security level to an existing zone:

1. Go to **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones**.
2. Select the zone you want to configure a security level for.
3. Click **Edit**.
4. Click **Security level**.
5. Turn on the security features you want to add to the door.
6. Click **Apply**.

Anti-passback	
Log violation only (Soft)	Use this if you want to allow a second person to enter the door using the same credentials as the first person. This option only results in a system alarm.
Deny access (Hard)	Use this if you want to prevent the second user from entering the door if they're using the same credentials as the first person. This option also results in a system alarm.
Timeout (seconds)	The amount of time until the system allows a user to re-enter. Enter **0** if you don't want timeout, meaning that the zone has anti-passback until the user leaves the zone. Only use **0** timeout with **Deny access (Hard)** if all doors in the zone have readers on both sides.

Supervised inputs

Supervised inputs can trigger an event when there is interruption in the connection to a door controller.

- Connection between the door controller and the door monitor. See .
- Connection between the door controller and the reader that uses Wiegand protocols. See .
- Connection between the door controller and the REX device. See .

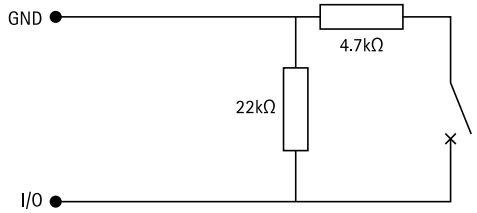
To use supervised inputs:

1. Install end of line resistors as close to the peripheral device as possible according to the connection diagram.
2. Go to the configuration page of a reader, door monitor, or REX device, turn on **Supervised input**.
3. If you followed the parallel first connection diagram, select **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor**.
4. If you followed the serial first connection diagram, select **Serial first connection**, and select a resistor value from the **Resistor values** drop-down menu.

Connection diagrams

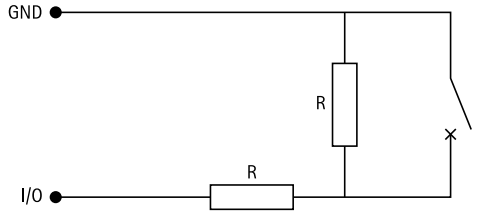
Parallel first connection

The resistor values must be 4.7 kΩ and 22 kΩ.



Serial first connection

The resistor values must be the same and within range 1-10 kΩ.



Manual actions

You can perform the following manual actions on doors and zones:

Reset – Returns to the configured system rules.

Grant access – Unlocks a door or zone for 7 seconds and then locks it again.

Unlock – Keeps the door unlocked until you Reset.

Lock – Keeps the door locked until the system grants a cardholder access.

Lockdown – No one gets in or out until you reset or unlock.

To perform a manual action:

1. Go to **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones**.
2. Select the door or zone you want to perform a manual action on.
3. Click any of the manual actions.

Card formats and PIN

A card format defines how a card stores data. It's a translation table between the incoming data and the validated data in the system. Each card format has a different set of rules for how to organize the stored information. By defining a card format, you tell the system how to interpret the information that the controller gets from the card reader.

There are predefined commonly used card formats available for you to use as they are or edit as required. You can also create custom card formats.

Go to **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN** to create, edit, or activate card formats. You can also configure PIN.

The custom card formats can contain the following data fields used for credential validation.

Card number – A subset of the credential binary data encoded as decimal or hexadecimal numbers. Use the card number to identify a specific card or cardholder.

Facility code – A subset of the credential binary data encoded as decimal or hexadecimal numbers. Use the facility code to identify a specific end customer or site.

To create a card format:

1. Go to **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN**.
2. Click **Add card format**.
3. Enter a card format name.
4. In the **Bit length** field, type a bit length between 1 and 256.
5. Select **Invert bit order** if you want to invert the bit order of the data received from the card reader.
6. Select **Invert byte order** if you want to invert the byte order of the data received from the card reader. This option is only available when you specify a bit length that you can divide by eight.
7. Select and configure the data fields to be active in the card format. Either **Card number** or **Facility code** must be active in the card format.
8. Click **OK**.
9. To activate the card format, select the checkbox in front of the card format name.

Note

- Two card formats with the same bit length can't be active at the same time. For example, if you have defined two 32-bit card formats, only one of these can be active. Deactivate the card format to active the other.
- You can only activate and deactivate card formats if the door controller has been configured with at least one reader.

ⓘ	Click ⓘ to see an example of the output after inverting bit order.
Range	Set the bit range of the data for the data field. The range must be within what you have specified for **Bit length**.
Output format	Select the output format of the data for the data field. **Decimal**: Also known as base-10 positional numeral system, consists of the numbers 0–9. **Hexadecimal**: also known as base-16 positional numeral system, consists of 16 unique symbols: the numbers 0–9 and the letters a–f.
Bit order of subrange	Select the bit order. **Little endian**: The first bit is the smallest (least significant). **Big endian**: The first bit is the biggest (most significant).

To edit a card format:

1. Go to **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN**.
2. Select a card format and click .
3. If you edit a predefined card format, you can only edit **Invert bit order** and **Invert byte order**.
4. Click **OK**.

You can only remove the custom card formats. To remove a custom card format:

1. Go to **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN**.
2. Select a custom card format, click and **Yes**.

To reset a predefined card format:

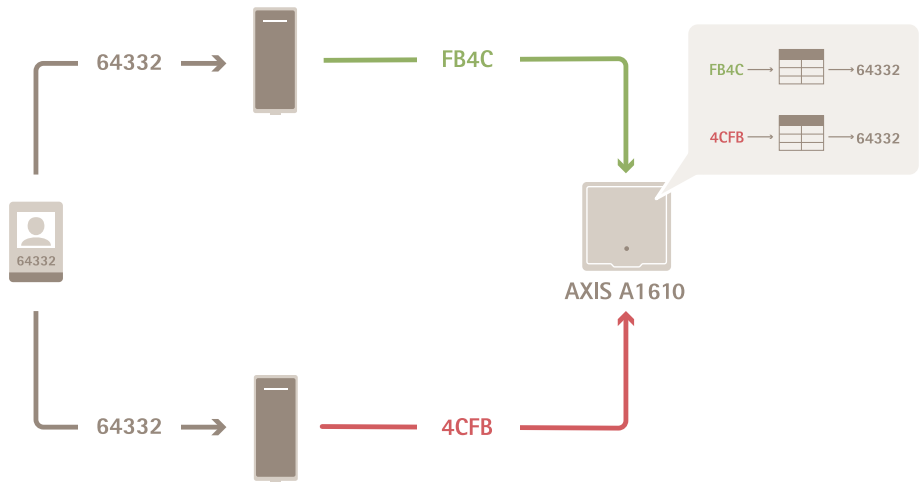
1. Go to **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN**.
2. Click to reset a card format to the default field map.

To configure PIN length:

1. Go to **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN**.
2. Under **PIN configuration**, click .
3. Specify **Min PIN length**, **Max PIN length**, and **End of PIN character**.
4. Click **OK**.

Card format settings

Overview



- The card number in decimal is `64332`.
- One reader transfers the card number to hexadecimal number `FB4C`. The other reader transfers it to hexadecimal number `4CFB`.
- AXIS A1610 Network Door Controller receives `FB4C` and transfers it to decimal number `64332` according to the card format settings on the reader.
- AXIS A1610 Network Door Controller receives `4CFB`, changes it to `FB4C` by inverting byte order, and transfers it to decimal number `64332` according to the card format settings on the reader.

Invert bit order

After inverting bit order, the card data received from the reader is read from right to left bit by bit.

Invert byte order

A group of eight bits is a byte. After inverting byte order, the card data received from the reader is read from right to left byte by byte.

26-bit standard Wiegand card format

1 *Leading parity*
2 *Facility code*
3 *Card number*
4 *Trailing parity*

Identification profiles

An identification profile is a combination of identification types and schedules. You can apply an identification profile to one, or more, doors to set how and when a cardholder can access a door.

Identification types are carriers of the credential information necessary to access a door. Common identification types are tokens, personal identification numbers (PINs), fingerprints, facial maps, and REX devices.
An identification type can carry one or more types of information.

Schedules, also known as **Time profiles**, are created in Management Client. To set up time profiles, see *Time profiles (explained)*.

Supported identification types: Card, PIN, and REX.

Go to **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles**.

There are five default identification profiles available for you to use as they are or edit as required.

Card – Cardholders must swipe the card to access the door.

Card and PIN – Cardholders must swipe the card and enter the PIN to access the door.

PIN – Cardholders must enter the PIN to access the door.

Card or PIN – Cardholders must swipe the card or enter the PIN to access the door.

License plate – Cardholders must drive towards the camera in a vehicle with an approved license plate.

To create an identification profile:

1. Go to **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles**.
2. Click **Create identification profile**.

3. Enter an identification profile name.
4. Select **Include facility code for card validation** to use facility code as one of the credential validation fields. This field is only available if you turn on **Facility code** under **Access management > Settings**.
5. Configure the identification profile for one side of the door.
6. On the other side of the door, do the previous steps again.
7. Click **OK**.

To edit an identification profile:

1. Go to **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles**.
2. Select an identification profile and click .
3. To change the identification profile name, enter a new name.
4. Do your edits to the side of the door.
5. To edit the identification profile on the other side of the door, do the previous steps again.
6. Click **OK**.

To remove an identification profile:

1. Go to **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles**.
2. Select an identification profile and click .
3. If the identification profile is used on a door, select another identification profile for the door.
4. Click **OK**.

Edit identification profile	
×	To remove an identification type and the related schedule.
Identification type	To change an identification type, select one, or more, types from the **Identification type** drop-down menu.
Schedule	To change a schedule, select one, or more, schedules from the **Schedule** drop-down menu.
+ **Add**	Add an identification type and the related schedule, click **Add** and set the identification types and schedules.

Encrypted communication

OSDP Secure Channel

Secure Entry supports OSDP (Open Supervised Device Protocol) Secure Channel to active line encryption between controller and Axis readers.

To turn on OSDP Secure Channel for an entire system:

1. Go to **Site Navigation** > **AXIS Optimizer** > **Access control** > **Encrypted communication**.
2. Enter your main encryption key and click **OK**.
3. Turn on **OSDP Secure Channel**. This option is only available after you enter the main encryption key.
4. By default, the main encryption key generates a OSDP Secure Channel key. To manually set the OSDP Secure Channel key:

   4.1. Under **OSDP Secure Channel**, click .

4.2. Clear **Use main encryption key to generate OSDP Secure Channel key**.

4.3. Enter the OSDP Secure Channel key and click **OK**.

To turn on or turn off OSDP Secure Channel for a specific reader, see *Doors and zones*.

Multi server BETA

The connected sub servers can, with multi-server, use the global cardholders and cardholder groups from the main server.

Note

- One system can support up to 64 sub servers.
- It requires that the main server and sub servers are on the same network.
- On main server and sub servers, make sure to configure Windows Firewall to allow incoming TCP connections on the Secure Entry port. The default port is 53461.

Workflow

1. Configure a server as a sub server and generate the configuration file. See .
2. Configure a server as a main server and import the configuration file of the sub servers. See .
3. Configure global cardholders and cardholder groups on the main server. See and .
4. View and monitor global cardholders and cardholder groups from the sub server. See .

Generate the configuration file from the sub server

1. From the sub server, go to **AXIS Optimizer** > **Access control** > **Multi server**.
2. Click **Sub server**.
3. Click **Generate**. It generates a configuration file in .json format.
4. Click **Download** and choose a location to save the file.

Import the configuration file to the main server

1. From the main server, go to **AXIS Optimizer** > **Access control** > **Multi server**.
2. Click **Main server**.
3. Click + **Add** and go to the configuration file generated from the sub server.
4. Enter the server name, IP address, and port number of the sub server.
5. Click **Import** to add the sub server.
6. The status of the sub server shows `Connected`.

Revoke a sub server

You can only revoke a sub server before you import its configuration file to a main server.

1. From the main server, go to **AXIS Optimizer** > **Access control** > **Multi server**.
2. Click **Sub server** and click **Revoke server**.
   Now you can configure this server as a main server or sub server.

Remove a sub server

After you import the configuration file of a sub server, it connects the sub server to the main server.

To remove a sub server:

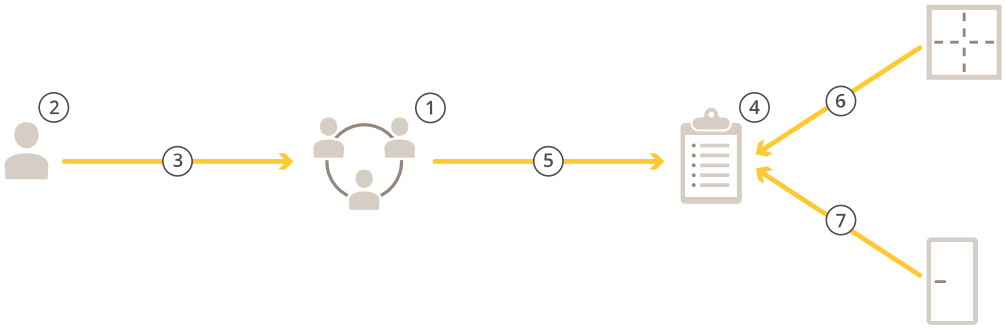
1. From the main server:
   1.1. Go to **Access management** > **Dashboard**.
   1.2. Change the global cardholders and groups to local cardholders and groups.
   1.3. Go to **AXIS Optimizer** > **Access control** > **Multi server**.
   1.4. Click **Main server** to show the sub server list.
   1.5. Select the sub server and click **Delete**.
2. From the sub server:
   – Go to **AXIS Optimizer** > **Access control** > **Multi server**.
   – Click **Sub server** and **Revoke server**.

Access management

The Access management tab allows you to configure and manage the system's cardholders, groups, and access rules.

Workflow of access management

The access management structure is flexible, which allows you to develop a workflow that suits your needs. The following is a workflow example:



1. Add groups. See .
2. Add cardholders. See .
3. Add cardholders to groups.
4. Add access rules. See .
5. Apply groups to access rules.
6. Apply zones to access rules.
7. Apply doors to access rules.

Add a cardholder

A cardholder is a person with a unique ID registered in the system. Configure a cardholder with credentials that identifies the person and when and how to grant the person access to doors.

1. Go to **Site Navigation** > **AXIS Optimizer** > **Access control** > **Cardholder management**.
2. Go to **Cardholders** and click **+ Add**.
3. Enter the first and last name of the cardholder and click **Next**.
4. Optionally, click **Advanced** and select any options.
5. Add a credential to the cardholder. See

6. Click **Save**.
7. Add the cardholder to a group.
   7.1. Under **Groups**, select the group you want to add the cardholder to and click **Edit**.
   7.2. Click **+ Add** and select the cardholder you want to add to the group. You can select multiple cardholders.
   7.3. Click **Add**.
   7.4. Click **Save**.

Advanced	
Long access time	Select to let the cardholder to have long access time and long open-too-long time when there is an installed door monitor.
Suspend cardholder	Select to suspend the cardholder.
Allow double swipe	Select to allow a cardholder to override the current state of a door. For example, they can use it to unlock a door outside the regular schedule.
Exempt from lockdown	Select to let the cardholder to have access during lockdown.
Exempt from anti-passback	Select to give a cardholder an exemption from the anti-passback rule. Anti-passback prevents people from using the same credentials as someone who entered an area before them. The first person must first exit the area before their credentials can be used again.
Global cardholder	Select to make it possible to view and monitor the cardholder on the sub servers. This option is only available for cardholders created on the main server. See .

Add credentials

You can add the following types of credentials to a cardholder:

- PIN
- Card
- License plate
- Mobile phone

To add a license plate credential to a cardholder:

1. Under **Credentials**, click **+ Add** and select **License plate**.
2. Enter a credential name that describes the vehicle.
3. Enter the license plate number for the vehicle.
4. Set the start and end date for the credential.
5. Click **Add**.

See example in .

To add a PIN credential to a cardholder:

1. Under **Credentials**, click **+ Add** and select **PIN**.

2. Enter a PIN.
3. To use a duress PIN to trigger a silent alarm, turn on **Duress PIN** and enter a duress PIN.
4. Click **Add**.

A PIN credential is always valid. You can also configure a duress PIN that opens the door and triggers a silent alarm in the system.

To add a card credential to a cardholder:

1. Under **Credentials**, click **+ Add** and select **Card**.
2. To manually enter the card data, enter a card name, card number, and bit length.

Note

Bit length is configurable only when you create a card format with a specific bit length that's not in the system.

3. To automatically get the card data of the last swiped card:
   3.1. Select a door from the **Select reader** drop-down menu.
   3.2. Swipe the card on the reader connected to that door.
   3.3. Click **Get last swiped card data from the door's reader(s)**.
4. Enter a facility code. This field is only available If you have enabled **Facility code** under **Access management > Settings**.
5. Set the start and end date for the credential.
6. Click **Add**.

Expiration date	
Valid from	Set a date and time for when the credential should be valid.
Valid to	Select an option from the drop-down menu.

Valid to	
No end date	The credential never expires.
Date	Set a date and time when the credential expires.
From first use	Select how long after the first use the credential expires. Select days, months, years, or number of times after the first use.
From last use	Select how long after the last use the credential expire. Select days, months, or years after the last use.

Use license plate number as a credential

This example shows you how to use a door controller, a camera with AXIS License Plate Verifier, and a vehicle's license plate number as credentials to grant access.

1. Add the door controller and the camera to AXIS Secure Entry for XProtect.
2. Set date and time for the new devices with **Synchronize with server computer time**.
3. Upgrade the software on the new devices to the latest available version.
4. Add a new door connected to your door controller. See .
   4.1. Add a reader on **Side A**. See .

4.2. Under **Door settings**, select **AXIS License Plate Verifier** as **Reader type** and enter a name for the reader.

4.3. Optionally, add a reader or REX device on **Side B**.

4.4. Click **Ok**.

5. Install and activate AXIS License Plate Verifier on your camera. See the *AXIS License Plate Verifier* user manual.
6. Start AXIS License Plate Verifier.
7. Configure AXIS License Plate Verifier.

7.1. Go to **Configuration > Access control > Encrypted communication**.

7.2. Under **External Peripheral Authentication Key**, click **Show authentication key** and **Copy key**.

7.3. Open AXIS License Plate Verifier from the camera's web interface.

7.4. Don't do the setup.

7.5. Go to **Settings**.

7.6. Under **Access control**, select **Secure Entry** as **Type**.

7.7. In **IP address**, enter the IP address for the door controller.

7.8. In **Authentication key**, paste the Authentication key that you copied earlier.

7.9. Click **Connect**.

7.10. Under **Door controller name**, select your door controller.

7.11. Under **Reader name**, select the reader you added earlier.

7.12. Turn on integration.

8. Add the cardholder that you want to give access to. See .
9. Add license plate credentials to the new cardholder. See .
10. Add an access rule. See .

10.1. Add a schedule.

10.2. Add the cardholder that you want to give license plate access to.

10.3. Add the door with the AXIS License Plate Verifier reader.

Add a group

Groups allow you to manage cardholders and their access rules collectively and efficiently.

1. Go to **Site Navigation** > **AXIS Optimizer** > **Access control** > **Cardholder management**.
2. Go to **Groups** and click **+ Add**.
3. Enter a name and optionally initials for the group.
4. Select **Global group** to make it possible to view and monitor the cardholder on the sub servers. This option is only available for cardholders created on the main server. See .
5. Add cardholders to the group:

5.1. Click **+ Add**.

5.2. Select the cardholders you want to add and click **Add**.

6. Click **Save**.

Add an access rule

An access rule defines the conditions that must be met to grant access.

An access rule consists of:

Cardholders and cardholder groups – who to grant access.

Doors and zones – where the access applies.

Schedules – when to grant access.

To add an access rule:

1. Go to **Access control** > **Cardholder management**.
2. Under **Access rules**, click **+ Add**.
3. Enter a name for the access rule and click **Next**.
4. Configure the cardholders and groups:
   4.1. Under **Cardholders** or **Groups**, click **+ Add**.
   4.2. Select the cardholders or groups and click **Add**.
5. Configure the doors and zones:
   5.1. Under **Doors** or **Zones**, click **+ Add**.
   5.2. Select the doors or zones and click **Add**.
6. Configure the schedules:
   6.1. Under **Schedules**, click **+ Add**.
   6.2. Select one or more schedules and click **Add**.
7. Click **Save**.

An access rule that's missing one or more of the components described above is incomplete. You can view all incomplete access rules in the **Incomplete** tab.

Manually unlock doors and zones

For information about manual actions, like manually unlocking a door, see .

For information about manual actions, like manually unlocking a zone, see .

Export system configuration reports

You can export reports that contain different types of information about the system. AXIS Secure Entry for XProtect exports the report as a comma-separated value (CSV) file and saves it in the default download folder. To export a report:

1. Go to **Reports** > **System configuration**.
2. Select the reports you want to export and click **Download**.

Cardholders details	Includes information about the cardholders, credentials, card validation, and last transaction.
Cardholders access	Includes the cardholder information and information about the cardholder groups, access rules, doors, and zones related to the cardholder.
Cardholders group access	Includes the cardholder group name and information about the cardholders, access rules, doors, and zones related to the cardholder group.
Access rule	Includes the access rule name and information about the cardholders, cardholder groups, doors, and zones related to the access rule.

Door access	Includes the door name and information about the cardholders, cardholder groups, access rules, and zones related to the door.
Zone access	Includes the zone name and information about the cardholders, cardholder groups, access rules, and doors related to the zone.

Create cardholder activity reports

A roll call report lists cardholders within a specified zone, helping identify who's present at a given moment.

A mustering report lists cardholders within a specified zone, helping identify who's safe and missing during emergencies. It assists building managers in locating staff and visitors after evacuations. A muster point is a designated reader where personnel report during emergencies, generating a report of people on and off-site. The system marks cardholders as missing until they check in at a muster point or until someone manually marks them as safe.

Both roll call and mustering reports require zones to track cardholders.

To create and run a roll call or mustering report:

1. Go to **Reports** > **Cardholder activity**.
2. Click **+ Add** and select **Roll call / Mustering**.
3. Enter a name for the report.
4. Select which zones to include in the report.
5. Select any groups you want to include in the report.
6. If you want a mustering report, select **Mustering point** and a reader for the mustering point.
7. Select a time frame for the report.
8. Click **Save**.
9. Select the report and click **Run**.

Roll call report status	Description
Present	The cardholder entered the specified zone and did not exit before you ran the report.
Not present	The cardholder exited the specified zone and did not enter again before you ran the report.

Mustering report status	Description
Safe	The cardholder swiped their card at the mustering point.
Missing	The cardholder didn't swipe their card at the mustering point.

Access management settings

To customize the cardholder fields used in the access management dashboard:

1. On the **Access management** tab, click **Settings** > **Custom cardholder fields**.
2. Click **+ Add** and enter a name. You can add up to 6 custom fields.
3. Click **Add**.

To use facility code to verify your access control system:

1. On the **Access management** tab, click **Settings** > **Facility code**.
2. Select **Facility code on**.

Note

You must also select **Include facility code for card validation** when you configure identification profiles. See .

Import and export

Import cardholders

This option imports cardholders, cardholder groups, credentials, and cardholder photos from a CSV file. To import cardholder photos, make sure that the server has access to the photos.

When you import cardholders the access management system automatically saves the system configuration, including all hardware configuration, and deletes any previously saved one.

Import options	
New	This option removes existing cardholders and adds new cardholders.
Update	This option updates the existing cardholders and adds new cardholders.
Add	This option keeps existing cardholders and adds new cardholders. Card numbers and cardholder IDs are unique and can only be used once.

1. On the **Access management** tab, click **Import and export**.
2. Click **Import cardholders**.
3. Select **New**, **Update**, or **Add** .
4. Click **Next**.
5. Click **Choose a file** and go to the CSV file. Click **Open**.
6. Enter a column delimiter and select a unique identifier and click **Next**.
7. Assign a heading to each column.
8. Click **Import**.

Import settings	
First row is header	Select if the CSV file contains a column header.
Column delimiter	Enter a column delimiter format for the CSV file.
Unique identifier	The system uses **Cardholder ID** to identify a cardholder by default. You can also use first and last name, or the email address. The Unique identifier prevents the import of duplicate personnel records.
Card number format	**Allow both hexadecimal and number** is selected by default.

Export cardholders

This option exports the cardholder data in the system to a CSV file.

1. On the **Access management** tab, click **Import and export**.
2. Click **Export cardholders**.
3. Choose a download location and click **Save**.

AXIS Secure Entry for XProtect updates cardholder photos in `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos` whenever the configuration changes.

Undo import

The system automatically saves its configuration when you import cardholders. The **Undo import** option resets the cardholder data and all hardware configuration to the state before the last cardholder import.

1. On the **Access management** tab, click **Import and export**.
2. Click **Undo import**.
3. Click **Yes**.

Backup and restore

Automatic backups are performed every night. The three latest backup files are stored in C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\backup. To restore these files:

1. Move the backup file to C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\restore.
2. Restart AXIS Secure Entry by using one of these methods:
   - Start the MSC (Services) program, find 'AXIS Optimizer Secure Entry Service', and restart.
   - Restart your computer.

T10234037

2025-10 (M3.2)