

AXIS Secure Entry for XProtect

Índice

Control de acceso	3
Configuración de control de acceso.....	3
Añadir un controlador de puerta de red Axis a su sistema	3
Activar licencias de puerta.....	4
Configure el control de acceso	4
Integración del control de acceso.....	4
Puertas y zonas.....	5
Ejemplo de puertas y zonas.....	6
Agregar una puerta.....	6
Ajustes de puerta.....	8
Nivel de seguridad de puerta.....	8
Opciones de hora.....	10
Agregar un monitor de puerta.....	10
Agregar una puerta de supervisión.....	11
Agregar un lector.....	12
Agregar un dispositivo REX.....	13
Agregar una zona	13
Nivel de seguridad de zona	14
Entradas con supervisión	15
Acciones manuales	16
Formatos de tarjeta y PIN.....	16
Configuración del formato de tarjeta.....	18
Perfiles de identificación.....	19
Comunicación cifrada.....	21
Canal seguro OSDP	21
BETA de varios servidores.....	21
Flujo de trabajo	21
Generar el archivo de configuración desde el servidor secundario	22
Importar el archivo de configuración al servidor principal	22
Revocar un servidor secundario.....	22
Eliminar un servidor secundario.....	22
Gestión de acceso	22
Flujo de trabajo de gestión de acceso.....	23
Agregar un titular de tarjeta	23
Agregar credenciales.....	24
Agregar un grupo	26
Agregar una regla de acceso	27
Desbloquear puertas y zonas manualmente	27
Exportar informes de configuración del sistema	27
Crear informes de actividad de titulares de tarjeta	28
Configuración de gestión de acceso.....	29
Importación y exportación.....	29
Copia de seguridad y restauración	31
Gestión de acceso en Smart Client	31
Configuración de roles de AXIS Secure Entry	31

Control de acceso

El control de acceso es una solución que combina el control de acceso físico con la videovigilancia. Esta integración permite configurar un sistema de control de acceso Axis directamente desde Management Client. El sistema se integra perfectamente con XProtect, permitiendo a los operadores supervisar el acceso y realizar acciones de control de acceso en Smart Client.

Nota

Requisitos

- Versión de VMS 2024 R1 o posterior.
- Licencias de acceso a XProtect; consulte *access licenses (licencias de acceso)*.
- Instale AXIS Optimizer en el servidor de eventos y en Management Client.

Los puertos 53459 y 53461 se abrirán al tráfico entrante (TCP) durante la instalación de AXIS Optimizer a través de AXIS Secure Entry.

Para utilizar puertas en AXIS Secure Entry, necesita obtener una licencia por puerta; consulte *Activar licencias de puerta, on page 4*.

Configuración de control de acceso

Nota

Antes de empezar, haga lo siguiente:

- Actualice el software del controlador de puerta. Consulte en la siguiente tabla la versión mínima y recomendada de AXIS OS para su versión de VMS.
- Asegúrese de que la fecha y la hora sean correctas.

Versión de AXIS Optimizer	Versión mínima de AXIS OS	Versión recomendada de AXIS OS
6.0	12..6.94.1	12.9.65.3
5.8	12.6.94.1	12.8.55.1
5.6	12.6.94.1	12.6.94.1

Añadir un controlador de puerta de red Axis a su sistema

1. Vaya a Site Navigation (Navegación del sitio) > AXIS Optimizer > Access control (Control de acceso).
2. En Configuration (Configuración), seleccione Devices (Dispositivos).
3. Seleccione Discovered devices (Dispositivos detectados) para consultar la lista de unidades que puede añadir al sistema.
4. Seleccione las unidades que desee añadir.
5. Haga clic en + Add (+ Añadir) en la ventana emergente y facilite las credenciales del controlador.

Nota

- Debería ver los controladores añadidos en la pestaña Management (Gestión).
- Para añadir manualmente un controlador al sistema, haga clic en + Add (+Añadir) en la pestaña Management (Gestión).
- Para integrar la actualización en el VMS al añadir, eliminar o editar el nombre de un controlador de puerta:
 - Vaya a Site Navigation (Navegación de instalaciones) > Access control (Control de acceso) y haga clic en la integración del Control de acceso.
 - Haga clic en Refresh Configuration (Actualizar configuración) en la pestaña General settings (Ajustes generales)

Activar licencias de puerta

Antes de poder añadir puertas, debe activar las licencias que tiene en su sistema.

1. En Site Navigation (Navegación por la instalación), vaya a License Information (Información sobre licencias).
2. Haga clic en Activate License Manually (Activar licencia manualmente) y seleccione Online u Offline.
3. Para activar las licencias de puerta online:
 - Introduzca su nombre de usuario y contraseña.
4. Para activar licencias de puerta offline, consulte *activate licenses offline (activar licencias offline)*.

Si necesita ajustar el número de licencias de puerta que se activarán:

1. Vaya a AXIS Optimizer > Access control (Control de acceso).
2. En Configuration (Configuración), seleccione Devices (Dispositivos).
3. Vaya a Allocated door licenses (Licencias de puerta asignadas) > Custom license allocation (Asignación de licencias personalizadas) e introduzca el número de licencias de puerta que desea utilizar.
4. Haga clic en Aplicar.
5. Vaya a Go to License Information (Información sobre licencias) y reactive sus licencias.

Configure el control de acceso

1. Vaya a Site Navigation (Navegación del sitio) > AXIS Optimizer > Access control (Control de acceso).
2. Para editar los perfiles de identificación predefinidos o crear un nuevo perfil de identificación, consulte *Perfiles de identificación, on page 19*.
3. Para utilizar una configuración personalizada para los formatos de tarjeta y la longitud del PIN, consulte *Formatos de tarjeta y PIN, on page 16*.
4. Agregue una puerta y aplique un perfil de identificación a la puerta. Vea *Agregar una puerta, on page 6*.
5. Agregue una zona y agregue puertas a la zona. Vea *Agregar una zona, on page 13*.

Compatibilidad de software de dispositivos para controladores de puerta

Importante

Tenga en cuenta lo siguiente cuando actualice el sistema operativo AXIS OS en su controlador de puerta:

- **Versiones de AXIS OS compatibles:** Las versiones de AXIS OS compatibles enumeradas más arriba solo se aplican cuando se actualiza desde su versión original recomendada de VMS y cuando el sistema tiene una puerta. Si el sistema no reúne estas condiciones, debe actualizarse a la versión de AXIS OS recomendada para la versión específica de VMS.
- **Versión mínima compatible de AXIS OS:** La versión de AXIS OS más antigua instalada en el sistema determina la versión de AXIS OS mínima compatible, con un límite de dos versiones anteriores.
- **Actualizar más allá de la versión recomendada de AXIS OS:** Supongamos que actualiza a una versión de AXIS OS superior a la recomendada para una versión concreta de VMS. Después, siempre puede regresar a la versión de AXIS OS recomendada sin ningún problema, siempre y cuando esté dentro de los límites de soporte técnico establecidos para la versión de VMS.
- **Futuras recomendaciones de AXIS OS:** Siga siempre la versión de AXIS OS recomendada para la versión correspondiente de VMS con el fin de garantizar la estabilidad del sistema y una compatibilidad total.

Integración del control de acceso

Para integrar el control de acceso en el VMS:

1. Vaya a Site Navigation (Navegación de instalaciones) > Access control (Control de acceso).

2. Haga clic con el botón derecho en **Access control (Control de acceso)** y haga clic en **Create new... (Crear nuevo...)**.
3. En el cuadro de diálogo **Create Access Control System Integration (Crear integración de sistemas de control de acceso)**:
 - Introduzca un nombre para la integración.
 - Seleccione **AXIS Secure Entry** en el menú desplegable de **Integration plug-in (Complemento de integración)**.
 - Haga clic en **Next (Siguiente)** hasta que observe el cuadro de diálogo **Associate cameras (Asociar cámaras)**.
Para asociar cámaras a puntos de acceso de puertas:
 - Haga clic en **Cameras (Cámaras)** en su dispositivo para consultar la lista de cámaras configuradas en el sistema XProtect.
 - Seleccionar y arrastrar una cámara al punto de acceso al que desea asociarla.
 - Haga clic en **Close (Cerrar)** para cerrar el cuadro de diálogo.

Nota

- Para obtener más información sobre la integración del control de acceso en XProtect, consulte *Using access control in XProtect Smart Client (Usar el control de acceso en XProtect Smart Client)*.
- Para obtener más información sobre las propiedades de control de acceso, como la configuración general, las puertas y las cámaras asociadas, los eventos de control de acceso, etc., consulte *Access control properties (Propiedades del control de acceso)*.

Puertas y zonas

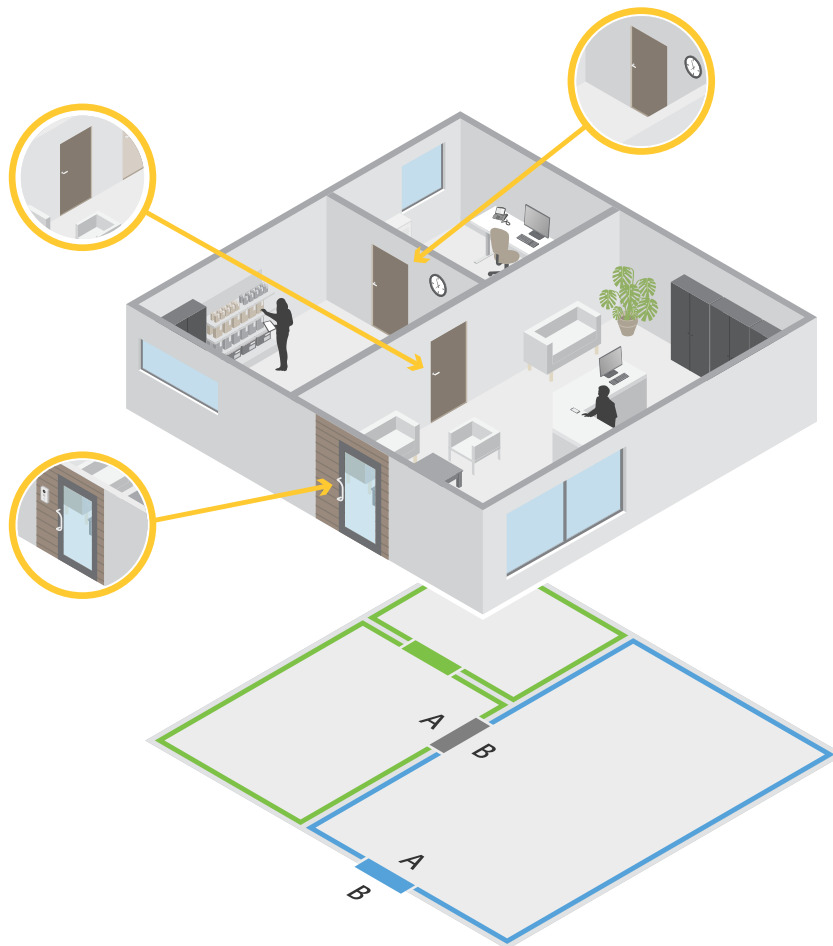
Vaya a **Site Navigation (Navegación del sitio) > AXIS Optimizer > Access control (Control de acceso) > Doors and zones (Puertas y zonas)** para obtener una visión general y configurar puertas y zonas.

 Gráfico de PIN	Ver el gráfico de pines del controlador asociado a una puerta. Si desea imprimir el gráfico de pines, haga clic en Print (Imprimir) .
 Perfil de identificación	Cambie el perfil de identificación en las puertas.
 Canal seguro	Active o desactive OSDP Secure Channel para un lector específico.

Puertas	
Nombre	El nombre de la puerta.
Controlador de puerta	El controlador de puerta conectado a la puerta.
Lado A	La zona en la que está el lado A de la puerta.
Cara B	La zona en la que está el lado B de la puerta.
Perfil de identificación	Perfil de identificación aplicado a la puerta.
Formatos de tarjeta y PIN	Muestra el tipo de formatos de tarjeta o la longitud del PIN.
Estado	Estado de la puerta. • Online (En línea): La puerta está en línea y funciona correctamente. • Lector sin conexión: El lector de la configuración de puerta no tiene conexión. • Error del lector: El lector de la configuración de puerta no admite canal seguro o el canal seguro no está activado para el lector.

Zonas	
Nombre	Nombre de la zona.
Número de puertas	El número de puertas incluidas en la zona.

Ejemplo de puertas y zonas



- Hay dos zonas: zona verde y zona azul.
- Hay tres puertas: puerta verde, puerta azul y puerta marrón.
- La puerta verde es una puerta interna de la zona verde.
- La puerta azul es una puerta perimetral solo para la zona azul.
- La puerta azul es una puerta perimetral para la zona verde y la zona azul.

Agregar una puerta

Nota

- Puede configurar un controlador de puerta con una puerta que tenga dos cerraduras o dos puertas que tengan una cerradura cada una.
- Si un controlador de puerta no tiene puertas y está utilizando una nueva versión de Axis Optimizer con un software más antiguo en el controlador de la puerta, el sistema le impedirá añadir una puerta. Sin embargo, el sistema admite puertas nuevas en los controladores del sistema con software anterior si ya hay una puerta existente.

Cree una nueva configuración de puerta para agregar una puerta:

1. Vaya a **Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Doors and zones (Puertas y zonas)**.
2. Haga clic en  **Add door (Agregar puerta)**.
3. Escriba un nombre de puerta.
4. En el menú desplegable **Controller (Controlador)**, seleccione un controlador de puerta. El controlador aparece en gris cuando no se puede agregar otra puerta, cuando está sin conexión o si HTTPS no está activo.
5. En el menú desplegable **Door type (Tipo de puerta)**, seleccione el tipo de puerta que desee crear.
6. Haga clic en **Next (Siguiente)** para ir a la página de configuración de la puerta.
7. En el menú desplegable **Primary lock (Cerradura principal)**, seleccione un puerto de relé.
8. Para configurar dos cerraduras en la puerta, seleccione un puerto de relé del menú desplegable **Secondary lock (Cerradura secundaria)**.
9. Seleccione un perfil de identificación. Vea *Perfiles de identificación, on page 19*.
10. Configure los ajustes de puerta. Consulte *Ajustes de puerta, on page 8*.
11. Configure una puerta de supervisión. Consulte *Agregar una puerta de supervisión, on page 11*.
12. Haga clic en **Save (Guardar)**.

Copie una configuración de puerta existente para agregar una puerta:

1. Vaya a **Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Doors and zones (Puertas y zonas)**.
2. Haga clic en  **Add door (Agregar puerta)**.
3. Escriba un nombre de puerta.
4. En el menú desplegable **Controller (Controlador)**, seleccione un controlador de puerta.
5. Haga clic en **Next (Siguiente)**.
6. En el menú desplegable **Copy configuration (Copiar configuración)**, seleccione una configuración de puerta existente. Muestra las puertas conectadas y el controlador aparece en gris si se ha configurado con dos puertas o una puerta con dos cerraduras.
7. Cambie los ajustes si lo desea.
8. Haga clic en **Save (Guardar)**.

Para editar una puerta:

1. Vaya a **Site Navigation (Navegación del sitio) > AXIS Optimizer > Access control (Control de acceso) > Doors and zones (Puertas y zonas) > Doors (Puertas)**.
2. Seleccione una puerta en la lista.
3. Haga clic en  **Edit (Modificar)**.
4. Cambie los ajustes y haga clic en **Save (Guardar)**.

Para eliminar una puerta:

1. Vaya a **Site Navigation (Navegación del sitio) > AXIS Optimizer > Access control (Control de acceso) > Doors and zones (Puertas y zonas) > Doors (Puertas)**.
2. Seleccione una puerta en la lista.
3. Haga clic en  **Remove (Eliminar)**.
4. Haga clic en **Yes (Sí)**.

Para integrar la actualización en el VMS al añadir, eliminar o editar el nombre de una puerta:

1. Vaya a **Site Navigation (Navegación de instalaciones) > Access control (Control de acceso)** y haga clic en la integración del Control de acceso.
2. Haga clic en **Refresh Configuration (Actualizar configuración)** en la pestaña **General settings (Ajustes generales)**

Ajustes de puerta

1. Vaya a **Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Doors and zones (Puertas y zonas)**.
2. Seleccione la puerta que desea editar.
3. Haga clic en  **Edit (Modificar)**.

Tiempo de acceso (s)	Establece el número de segundos que la puerta permanece desbloqueada una vez se concedió permiso de acceso. La puerta permanece desbloqueada hasta que la puerta se abra o hasta que termine el tiempo establecido. La puerta se bloquea cuando se cierra aunque haya tiempo de acceso.
Open-too-long time (sec) [Tiempo de apertura demasiado largo (s)]	Solo es válido si ha configurado un monitor de puerta. Defina el número de segundos que permanece abierta la puerta. Si la puerta está abierta cuando termina el tiempo establecido, activa la alarma de puerta abierta durante demasiado tiempo. Configure una regla de acción para determinar qué acción activa el evento de puerta abierta durante demasiado tiempo.
Tiempo de acceso largo (seg)	Establece el número de segundos que la puerta permanece desbloqueada una vez se concedió permiso de acceso. El tiempo de acceso largo anula el tiempo de acceso para los titulares de tarjeta que tienen estos ajustes activados.
Long open-too-long time (sec) [Tiempo largo de apertura demasiado larga (s)]	Solo es válido si ha configurado un monitor de puerta. Defina el número de segundos que permanece abierta la puerta. Si la puerta está abierta cuando termina el tiempo establecido, activa el evento de puerta abierta durante demasiado tiempo. El tiempo de apertura demasiado largo sobrescribe el tiempo de apertura demasiado largo ya establecido para los titulares de tarjeta si activa los ajustes de Tiempo de acceso largo .
Tiempo antes de nuevo bloqueo (ms)	Defina el tiempo, en milisegundos, durante el que la puerta debe permanecer desbloqueada después de abrirse o cerrarse.
Volver a bloquear	• After opening (Después de abrirse): Solo es válido si ha agregado un monitor de puerta. • After closing (Después de cerrarse): Solo es válido si ha agregado un monitor de puerta.

Nivel de seguridad de puerta

Puede agregar las siguientes características de seguridad a la puerta:

Regla de dos personas – La regla de dos personas requiere que dos personas utilicen una credencial válida para acceder.

Doble deslizamiento – El doble deslizamiento permite que un titular de tarjeta invalide el estado actual de una puerta. Por ejemplo, pueden utilizarla para bloquear o desbloquear una puerta fuera de la programación habitual, lo que es más cómodo que entrar en el sistema para desbloquear la puerta. El barrido doble no afecta a una programación ya existente. Por ejemplo, si una puerta se va a bloquear a la hora de cierre y los empleados se van a un receso para el almuerzo, la puerta se seguirá bloqueando según la programación.

Puede configurar el nivel de seguridad mientras agrega una zona puerta o puede hacerlo en una puerta existente.

Para agregar una regla de dos personas a una puerta existente:

1. Vaya a **Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Doors and zones (Puertas y zonas)**.
2. Seleccione la puerta para la que desea configurar un nivel de seguridad.
3. Haga clic en **Edit (Modificar)**.
4. Haga clic en **Security level (Nivel de seguridad)**.
5. Active la **regla de dos personas**.
6. Haga clic en **Aplicar**.

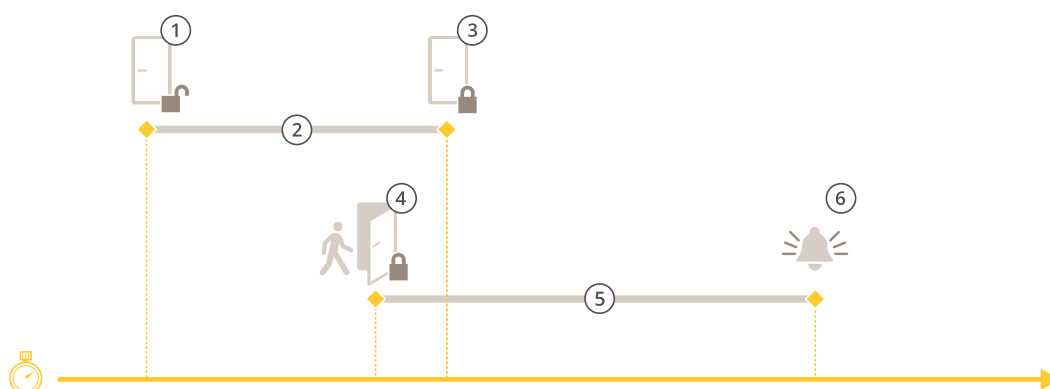
Regla de dos personas	
Lateral A y Lateral B	Seleccione los lados de la puerta en los que utilizar la regla.
Horarios	Seleccione cuándo está activa la regla.
Tiempo de espera (segundos)	El tiempo de espera es el tiempo máximo permitido entre los barridos de tarjeta u otro tipo de credencial válida.

Para añadir un **doble deslizamiento** a una puerta existente:

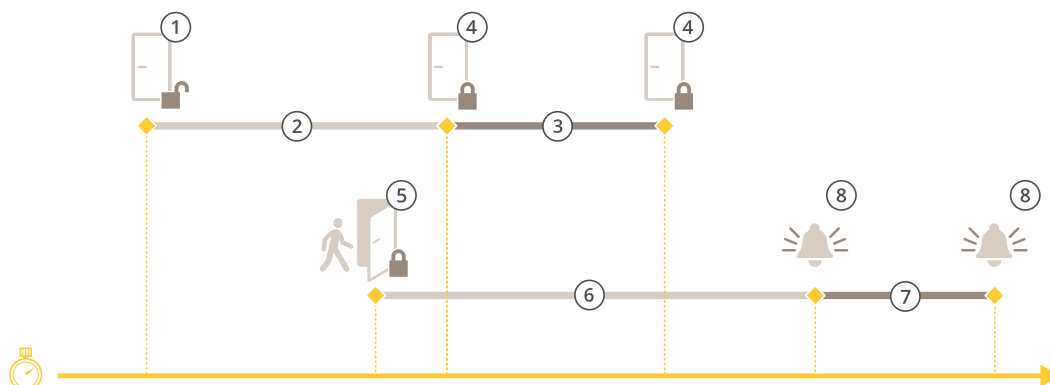
1. Vaya a **Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Doors and zones (Puertas y zonas)**.
2. Seleccione la puerta para la que desea configurar un nivel de seguridad.
3. Haga clic en **Edit (Modificar)**.
4. Haga clic en **Security level (Nivel de seguridad)**.
5. Active el **barrido doble**.
6. Haga clic en **Aplicar**.
7. Aplique un **barrido doble** al titular de la tarjeta.
 - 7.1. Vaya a **Cardholder management (Gestión de titulares de tarjeta)**.
 - 7.2. Haga clic  en el titular de tarjeta que desee editar y haga clic en **Edit (Editar)**.
 - 7.3. Haga clic en **Más**.
 - 7.4. Seleccione **Allow double-swipe (Permitir doble barrido)**.
 - 7.5. Haga clic en **Aplicar**.

Doble deslizamiento	
Tiempo de espera (segundos)	El tiempo de espera es el tiempo máximo permitido entre los barridos de tarjeta u otro tipo de credencial válida.

Opciones de hora



- 1 Acceso concedido: desbloquea las cerraduras
- 2 Tiempo de acceso
- 3 Ninguna acción realizada: bloquea las cerraduras
- 4 Acción realizada (puerta abierta): bloquea las cerraduras o las mantiene desbloqueadas hasta que se cierre la puerta
- 5 Tiempo de apertura demasiado largo
- 6 La alarma de tiempo de apertura demasiado largo se desactiva



- 1 Acceso concedido: desbloquea las cerraduras
- 2 Tiempo de acceso
- 3 2+3: Tiempo de acceso largo
- 4 Ninguna acción realizada: bloquea las cerraduras
- 5 Acción realizada (puerta abierta): bloquea las cerraduras o las mantiene desbloqueadas hasta que se cierre la puerta
- 6 Tiempo de apertura demasiado largo
- 7 6+7: Tiempo de apertura demasiado largo
- 8 La alarma de tiempo de apertura demasiado largo se desactiva

Agregar un monitor de puerta

Un monitor de puerta es un interruptor de posición de puerta que supervisa el estado físico de una puerta. Puede agregar un monitor de puerta a la puerta y configurar cómo conectar el monitor de puerta.

1. Vaya a la página de configuración de la puerta. Consulte *Agregar una puerta*, on page 6
2. En **Sensors (Sensores)**, haga clic en **Add (Agregar)**.
3. Seleccione el **Door monitor sensor (Sensor de monitor de puerta)**.
4. Seleccione el puerto de E/S al que desea conectar el monitor de puerta.

5. En **Door open if (Abrir puerta si)**, seleccione cómo están conectados los circuitos del monitor de puerta.
6. Para ignorar los cambios de estado antes de entrar en un nuevo estado estable, establezca un **Debounce time (Tiempo antirrebote)**.
7. Para activar un evento cuando se produce una interrupción en la conexión entre el controlador de puerta y el monitor de puerta, active **Supervised input (Entrada supervisada)**. Consulte *Entradas con supervisión, on page 15*.

Puerta abierta si	
Circuito abierto	El circuito de monitor de puerta está normalmente cerrado. El monitor de puerta envía la señal de una puerta abierta cuando el circuito está abierto. El monitor de puerta envía la señal de una puerta cerrada cuando el circuito está cerrado.
Circuito cerrado	El circuito de monitor de puerta está normalmente abierto. El monitor de puerta envía la señal de una puerta abierta cuando el circuito está cerrado. El monitor de puerta envía la señal de una puerta cerrada cuando el circuito está abierto.

Agregar una puerta de supervisión

Una puerta de supervisión es un tipo de puerta que muestra si está abierto o cerrado. Por ejemplo, puede utilizar esta opción en una puerta de seguridad contra incendios que no requiere un bloqueo pero en la que debe saber si la puerta está abierta.

Una puerta de supervisión es distinta de una puerta regular con un monitor de puerta. Una puerta regular con un monitor de puerta admite bloqueos y lectores, pero requiere un controlador de puerta. Una puerta de supervisión admite un sensor de posición de puerta pero solo requiere un módulo de relé de E/S de red conectado a un controlador de puerta. Puede conectar hasta cinco sensores de posición de puerta a un módulo de relé de E/S de red.

Nota

Una puerta de supervisión requiere un AXIS A9210 Network I/O Relay Module con el software más reciente como la aplicación de la ACAP de la puerta de supervisión de AXIS.

Para configurar una puerta de supervisión:

1. Instale AXIS A9210 y actualícelo con la versión más reciente de AXIS OS.
2. Instale los sensores de posición de puerta.
3. En el VMS, vaya a **Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Doors and zones (Puertas y zonas)**.
4. Haga clic en **Add door (Agregar puerta)**.
5. Introduzca un nombre.
6. En **Type (Tipo)**, seleccione **Monitoring door (Puerta de supervisión)**.
7. En **Device (Dispositivo)**, seleccione el módulo de relé de E/S de red.
8. Haga clic en **Next (Siguiente)**.
9. En **Sensors (Sensores)**, haga clic en **+ Add (+ Agregar)** y seleccione **Door position sensor (Sensor de posición de puerta)**.
10. Seleccione la E/S que está conectada al sensor de posición de puerta.
11. Haga clic en **Añadir**.

Agregar un lector

Puede configurar un controlador de puerta para utilizar dos lectores cableados. Seleccione agregar un lector a un lado o a ambos lados de una puerta.

Si aplica una configuración personalizada de formatos de tarjeta o longitud de PIN a un lector, puede verlo en **Card formats (Formatos de tarjeta)** en **Configuration > Access control > Doors and zones (Configuración > Control de acceso > Puertas y zonas)**. Consulte *Puertas y zonas, on page 5*.

1. Vaya a la página de configuración de la puerta. Consulte *Agregar una puerta, on page 6*.
2. En un lado de la puerta, haga clic en **Add (Agregar)**.
3. Seleccione **Card reader (Lector de tarjetas)**.
4. Seleccione el **Reader type (Tipo de lector)**.
5. Para utilizar una configuración de longitud de PIN personalizada para este lector.
 - 5.1. Haga clic en **Avanzado**.
 - 5.2. Active **Custom PIN length (Longitud de PIN personalizada)**.
 - 5.3. Establezca **Min PIN length (Longitud mínima de PIN)**, **Max PIN length (Longitud máxima de PIN)** y **End of PIN character (Carácter final de PIN)**.
6. Para utilizar un formato de tarjeta personalizado para este lector.
 - 6.1. Haga clic en **Avanzado**.
 - 6.2. Active **Custom card formats (Formatos de tarjeta personalizados)**.
 - 6.3. Seleccione los formatos de tarjeta que desee utilizar para el lector. Si ya se está utilizando un formato de tarjeta con la misma longitud de bits, debe desactivarlo primero. Un icono de advertencia se muestra en el cliente cuando la configuración del formato de tarjeta es distinta de la configuración del sistema configurada.
7. Haga clic en **Añadir**.
8. Para agregar un lector al otro lado de la puerta, vuelva a realizar este procedimiento.

Tipo de lector	
OSDP RS485 half-duplex	Para lectores RS485, seleccione OSDP RS485 half duplex (OSDP RS485 half-duplex) y un puerto de lector.
Wiegand	Para lectores que utilizan protocolos Wiegand, seleccione Wiegand (Wiegand) y un puerto de lector.

Wiegand	
Control de LED	Seleccione Single wire (Cable simple) o Cable dual (R/G) . Los lectores con control de led dual utilizan diferentes cables para los LED rojo y verde.
Alerta de manipulación	Seleccione si la entrada de manipulación del lector está activa. • Open circuit (Circuito abierto): El lector envía la señal de manipulación de puerta cuando el circuito está abierto. • Circuito cerrado: El lector envía la señal de manipulación de puerta cuando el circuito está cerrado.

Tiempo de rebote de manipulación	Para ignorar los cambios de estado de la entrada de manipulación del lector antes de que entre en un nuevo estado estable, defina un Tamper debounce time (Tiempo antirrebote en manipulación) .
Entrada supervisada	Active para desencadenar un evento cuando se interrumpe la conexión entre el controlador de puerta y el lector. Consulte <i>Entradas con supervisión, on page 15</i> .

Agregar un dispositivo REX

Puede seleccionar agregar una solicitud al dispositivo de solicitud de salida (REX) en un lado o a ambos lados de la puerta. Un dispositivo REX puede ser un sensor PIR, un botón REX o una barra pulsadora.

1. Vaya a la página de configuración de la puerta. Consulte *Agregar una puerta, on page 6*.
2. En un lado de la puerta, haga clic en **Add (Agregar)**.
3. Seleccione **dispositivo de solicitud de salida (REX)**.
4. Seleccione el puerto de E/S en el que desea conectar el dispositivo REX. Si solo hay un puerto disponible, se seleccionará automáticamente.
5. Seleccione qué **Action (Acción)** activar cuando la puerta recibe la señal REX.
6. En **REX active (REX activo)**, seleccione la conexión de circuito de monitor de puerta.
7. Para ignorar los cambios de estado antes de entrar en un nuevo estado estable, establezca un **Debounce time (ms) [Tiempo antirrebote (ms)]**.
8. Para activar un evento cuando se produce una interrupción en la conexión entre el controlador de puerta y el dispositivo de solicitud de salida (REX), active **Supervised input (Entrada supervisada)**. Consulte *Entradas con supervisión, on page 15*.

Acción	
Abrir puerta	Seleccione para desbloquear la puerta cuando recibe la señal REX.
Ninguno	Seleccione si no desea activar ninguna acción cuando la puerta recibe la señal REX.

REX activo:	
Circuito abierto	Seleccione si el circuito REX está normalmente cerrado. El dispositivo de solicitud de salida (REX) envía la señal cuando el circuito esté abierto.
Circuito cerrado	Seleccione si el circuito REX está normalmente abierto. El dispositivo de solicitud de salida (REX) envía la señal cuando el circuito se cierra.

Agregar una zona

Una zona es un área física específica con un grupo de puertas. Puede crear zonas y agregar puertas a las zonas. Existen dos tipos de puertas:

- **Perimeter door (Puerta de perímetro):** Los titulares de tarjeta entran o salen de la zona por esta puerta.
- **Internal door (Puerta interna):** Una puerta interna dentro de la zona.

Nota

Una puerta perimetral puede pertenecer a dos zonas. Una puerta interna solo puede pertenecer a una zona.

1. Vaya a **Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Doors and zones (Puertas y zonas) > Zones (Zonas)**.
2. Haga clic en  **Add zone (Agregar zona)**.
3. Escriba un nombre de zona.
4. Haga clic en **Add door (Agregar puerta)**.
5. Seleccione las puertas que desee agregar a la zona y haga clic en **Add (Agregar)**.
6. De forma predeterminada, la puerta se establece como puerta perimetral. Para cambiarlo, seleccione **Internal door (Puerta interna)** en el menú desplegable.
7. De forma predeterminada, una puerta perimetral utiliza el lado A de la puerta como entrada a la zona. Para cambiarlo, seleccione **Leave (Abandonar)** en el menú desplegable.
8. Para eliminar una puerta de la zona, selecciónela y haga clic en **Remove (Eliminar)**.
9. Haga clic en **Save (Guardar)**.

Para editar una zona:

1. Vaya a **Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Doors and zones (Puertas y zonas) > Zones (Zonas)**.
2. Seleccione una zona en la lista.
3. Haga clic en  **Edit (Modificar)**.
4. Cambie los ajustes y haga clic en **Save (Guardar)**.

Para eliminar una zona:

1. Vaya a **Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Doors and zones (Puertas y zonas) > Zones (Zonas)**.
2. Seleccione una zona en la lista.
3. Haga clic en  **Remove (Eliminar)**.
4. Haga clic en **Yes (Sí)**.

Nivel de seguridad de zona

Puede agregar la siguiente característica de seguridad a una zona:

Protección contra dobles entradas – Impide que los usuarios utilicen las mismas credenciales que otra persona que ha entrado en una zona antes. Es obligatorio que una persona salga de la zona antes de sus credenciales se puedan volver a usar.

Nota

- Con antipassback, recomendamos el uso de sensores de posición de puerta en todas las puertas de la zona para asegurarse de el sistema pueda registrar que un usuario la ha abierto tras haber pasado la tarjeta.
- Si un controlador de puerta no tiene conexión, anti passback funciona siempre que todas las puertas de la zona pertenezcan al mismo controlador de puerta. No obstante, si las puertas de la zona pertenecen a distintos controladores de puerta sin conexión, anti passback deja de funcionar.

Puede configurar el nivel de seguridad mientras agrega una zona nueva o puede hacerlo en una zona existente. Para agregar un nivel de seguridad a una zona existente:

1. Vaya a **Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Doors and zones (Puertas y zonas)**.
2. Seleccione la zona para la que desea configurar el nivel de seguridad.
3. Haga clic en **Edit (Modificar)**.

4. Haga clic en **Security level (Nivel de seguridad)**.
5. Active las características de seguridad que desee agregar a la puerta.
6. Haga clic en **Aplicar**.

Protección contra dobles entradas	
Solo registro de infracciones (suave)	Utilice esta opción si desea permitir que una segunda persona entre por la puerta con las mismas credenciales que la primera persona. Esta opción solo genera una alarma del sistema.
Denegar acceso (exigente)	Utilice esta opción si desea evitar que el segundo usuario entre por la puerta si utiliza las mismas credenciales que la primera persona. Esta opción también genera una alarma del sistema.
Tiempo de espera (segundos)	El tiempo que se debe esperar hasta que el sistema permita la entrada de nuevo de un usuario. Introduzca 0 si no desea que se agote el tiempo de espera, lo que significa que la zona tiene antipassback hasta que el usuario sale de la zona. Utilice solo 0 tiempo de espera con Denegar acceso (exigente) si todas las puertas de la zona tienen lectores en ambos lados.

Entradas con supervisión

Las entradas supervisadas pueden activar un evento cuando se interrumpe la conexión con un controlador de puerta.

- Conexión entre el controlador de puerta y el monitor de puerta. Consulte *Agregar un monitor de puerta, on page 10*.
- Conexión entre el controlador de puerta y el lector que utiliza protocolos Wiegand. Consulte *Agregar un lector, on page 12*.
- Conexión entre el controlador de puerta y el dispositivo REX. Consulte *Agregar un dispositivo REX, on page 13*.

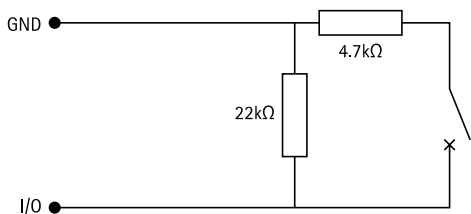
Para utilizar entradas supervisadas:

1. Instale las resistencias de final de línea lo más cerca posible del dispositivo periférico según el diagrama de conexión.
2. Vaya a la página de configuración de un lector, un monitor de puerta o un dispositivo de solicitud de salida (REX), active **Supervised input (Entrada supervisada)**.
3. Si ha seguido el diagrama de primera conexión en paralelo, seleccione **Parallel first connection with a 22 K Ω parallel resistor and a 4.7 K Ω serial resistor (Primera conexión en paralelo con una resistencia de 22 K Ω en paralelo y una resistencia de 4,7 K Ω en serie)**.
4. Si ha seguido el diagrama de primera conexión en serie, seleccione **Serial first connection (Primera conexión en serie)** y seleccione los valores de la resistencia en el menú desplegable **Resistor values (Valores de resistencia)**.

Diagramas de conexión

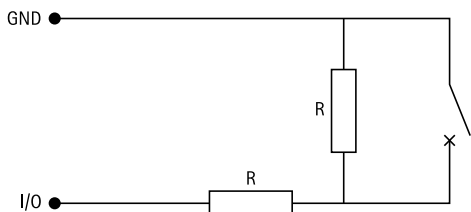
Parallel first connection (Primera conexión en paralelo)

Los valores de la resistencia deben ser de 4,7 K Ω y 22 K Ω .



Primera conexión en serie

Los valores de las resistencias deben ser iguales y situarse en el rango 1–10 KΩ.



Acciones manuales

Puede realizar las siguientes acciones manuales en puertas y zonas:

Reiniciar – Regresa a las reglas del sistema configuradas.

Autorizar acceso – Desbloquea una puerta o zona durante 7 segundos y vuelve a bloquearla.

Desbloquear – Mantiene la puerta desbloqueada hasta que el usuario la reinicia.

Bloquear – Mantiene la puerta bloqueada hasta que el sistema concede acceso a un titular de tarjeta.

Bloqueo – Nadie entra o sale hasta que el usuario reinicia o desbloquea.

Para realizar una acción manual:

1. Vaya a Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Doors and zones (Puertas y zonas).
2. Seleccione la puerta o zona en la que desea realizar una acción manual.
3. Haga clic en cualquiera de las acciones manuales.

Nota

La puerta permanecerá en estado de funcionamiento manual, también conocido como modo de control manual, hasta que se vuelva a configurar según su programación habitual.

Formatos de tarjeta y PIN

Un formato de tarjeta define cómo una tarjeta almacena datos. Es una tabla de traducción entre los datos entrantes y los datos validados en el sistema. Cada formato de tarjeta incluye un conjunto de reglas diferentes para cómo organizar la información almacenada. Al definir un formato de tarjeta, se indica al sistema cómo se debe interpretar la información que el controlador recibe del lector de tarjeta.

Hay formatos de tarjeta de uso común predefinidos disponibles para que los utilice tal como están o los edite según sea necesario. También se pueden crear formatos de tarjeta personalizados.

Vaya a Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Card formats and PIN (Formatos de tarjeta y PIN) para crear, editar o activar formatos de tarjeta. También puede configurar el PIN.

Los formatos de tarjeta personalizados pueden contener los siguientes campos de datos utilizados para la validación de credenciales.

Número de tarjeta – Un subconjunto de los datos binarios de credenciales codificados como números decimales o hexadecimales. Use el número de tarjeta para identificar una tarjeta o titular de tarjeta específico.

Código de instalación – Un subconjunto de los datos binarios de credenciales codificados como números decimales o hexadecimales. Use el código de instalación para identificar a un cliente final o instalación específicos.

Para crear un formato de tarjeta:

1. Vaya a **Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Card formats and PIN (Formatos de tarjeta y PIN)**.
2. Haga clic en **Add card format (Añadir formato de tarjeta)**.
3. Introduzca un nombre de formato de tarjeta.
4. En el campo de **Bit length (Longitud de bits)**, escriba una longitud de bits entre 1 y 256.
5. Seleccione **Invert bit order (Invertir orden de bits)** si desea invertir el orden de bits de los datos recibidos desde el lector de tarjetas.
6. Seleccione **Invert byte order (Invertir orden de bytes)** si desea invertir el orden de bytes de los datos recibidos del lector de tarjetas. Esta opción solo está disponible si se especifica una longitud de bits que pueda dividir por ocho.
7. Seleccione y configure los campos de datos para que se activen en el formato de tarjeta. El **Card number (Número de tarjeta)** o el **Facility code (Código de instalación)** deben estar activos en el formato de tarjeta.
8. Haga clic en **OK**.
9. Para activar el formato de tarjeta, seleccione la casilla delante del nombre del formato de tarjeta.

Nota

- No pueden estar activos simultáneamente dos formatos de tarjeta con la misma longitud de bits. Por ejemplo, si ha definido dos formatos de tarjeta de 32 bits, solo podrá activar uno de ellos. Desactive el formato de tarjeta para activar el otro.
- Solo se pueden activar y desactivar formatos de tarjeta si el controlador de puerta se ha configurado con al menos un lector.

	Haga clic en  para ver un ejemplo de la salida después de invertir el orden de bits.
Gama	Defina el rango de bits de los datos para el campo de datos. El intervalo debe estar dentro de lo especificado para Bit length (Longitud de bits) .
Formato de salida	Seleccione el formato de salida de los datos para el campo de datos. Decimal: También conocido como sistema numeral posicional base 10, consta de los números 0-9. Hexadecimal: también conocido como sistema numérico posicional de base 16, consta de 16 símbolos únicos: los números 0-9 y las letras a-f.
Orden de bits del subrango	Seleccione el orden de bits. Little endian: El primer bit es el más pequeño (el menos significativo). Big endian: El primer bit es el más grande (el más significativo).

Para editar un formato de tarjeta:

1. Vaya a Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Card formats and PIN (Formatos de tarjeta y PIN).
2. Seleccione un formato de tarjeta y haga clic en .
3. Si edita un formato de tarjeta predefinido, solo puede editar Invert bit order (Invertir orden de bits) e Invert byte order (Invertir orden de bytes).
4. Haga clic en OK.

Solo puede eliminar los formatos de tarjeta personalizados. Para eliminar un formato de tarjeta personalizado:

1. Vaya a Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Card formats and PIN (Formatos de tarjeta y PIN).
2. Seleccione un formato de tarjeta personalizado, haga clic en  y en Yes (Sí).

Para restablecer un formato de tarjeta predefinido:

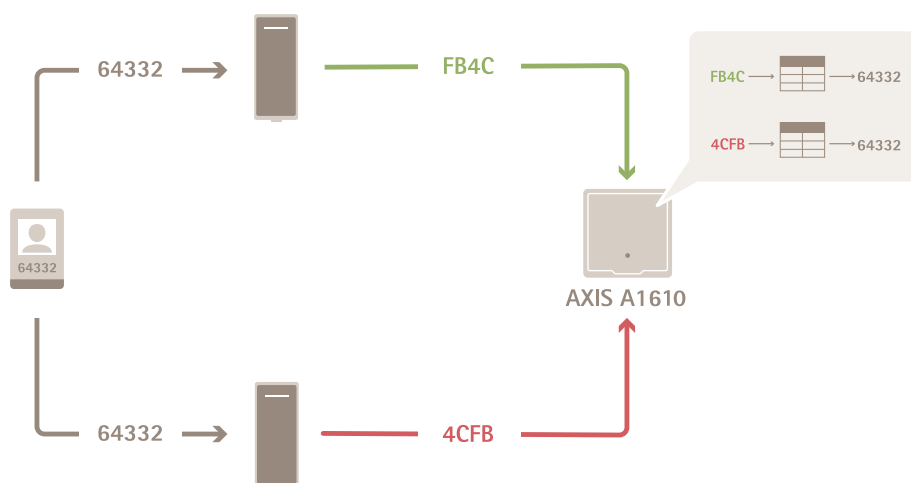
1. Vaya a Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Card formats and PIN (Formatos de tarjeta y PIN).
2. Haga clic en  para restablecer un formato de tarjeta al mapa de campos predeterminado.

Para configurar la longitud de PIN:

1. Vaya a Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Card formats and PIN (Formatos de tarjeta y PIN).
2. En PIN configuration (Configuración de PIN), haga clic en .
3. Especifique Min PIN length (Longitud mínima de PIN), Max PIN length (Longitud máxima de PIN) y End of PIN character (Carácter final de PIN).
4. Haga clic en OK.

Configuración del formato de tarjeta

Descripción general



- El número de tarjeta en decimal es 64332.
- Un lector transfiere el número de tarjeta al número hexadecimal FB4C. El otro lector lo transfiere al número hexadecimal 4CFB.

- AXIS A1610 Network Door Controller recibe FB4C y lo transfiere al número decimal 64332 de acuerdo con los ajustes de formato de tarjeta en el lector.
- AXIS A1610 Network Door Controller recibe 4CFB, lo convierte en FB4C invirtiendo el orden de bytes y lo transfiere al número decimal 64332 de acuerdo con los ajustes de formato de tarjeta en el lector.

Invertir orden de bits

Después de invertir el orden de bits, los datos de la tarjeta que recibe el lector se leen de derecha a izquierda, bit a bit.

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

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

Invertir orden de bytes

Un grupo de ocho bits es un byte. Después de invertir el orden de bytes, los datos de la tarjeta que recibe el lector se leen de derecha a izquierda, byte a byte.

64 332 = 1111 1011 0100 1100 $\longrightarrow$ 0100 1100 1111 1011 = 19707

F B 4 C 4 C F B

Formato de tarjeta Wiegand estándar de 26 bits

P FFFFFFF NNNNNNNNNNNNNNNN P

(1) (2) (3) (4)

- 1 Paridad líder
- 2 Código de instalación
- 3 Número de tarjeta
- 4 Paridad de cola

Perfiles de identificación

Un perfil de identificación es una combinación de tipos de identificación y programaciones. Puede aplicar un perfil de identificación a una o más puertas para definir cómo y cuándo puede acceder un titular de tarjeta a una puerta.

Los tipos de identificación son portadores de la información de la credencial necesaria para acceder a una puerta. Los tipos de identificación comunes son tokens, números de identificación personal (PIN), huellas, mapas faciales y dispositivos de solicitud de salida (REX). Un tipo de identificación puede tener uno o más tipos de información.

Las programaciones, también conocidas como **Time profiles (Perfiles de tiempo)**, se crean en Management Client. Para configurar perfiles de tiempo, consulte *Time profiles (explained) (Perfiles de tiempo (explicación))*.

Tipos de identificación compatibles: Tarjeta, PIN y REX.

Vaya a **Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Identification profiles (Perfiles de identificación)**.

Hay cinco perfiles de identificación predeterminados disponibles para su uso tal y como están o editar según sea necesario.

Tarjeta – Los titulares de tarjeta deben pasar la tarjeta para acceder a la puerta.

Tarjeta y PIN – Los titulares de tarjeta deben pasar la tarjeta e introducir el PIN para acceder a la puerta.

Número de identificación personal (PIN) – Los titulares de tarjeta deben introducir el PIN para acceder a la puerta.

Tarjeta o PIN – Los titulares de tarjeta deben pasar la tarjeta o introducir el PIN para acceder a la puerta.

Matrícula – Los titulares de tarjeta deben conducir hacia la cámara en un vehículo con una matrícula aprobada.

Para crear perfil de identificación:

1. Vaya a **Site Navigation (Navegación de instalaciones) > AXIS Optimizer >Access control (Control de acceso) > Identification profiles (Perfiles de identificación)**.
2. Haga clic en **Create identification profile (Crear perfil de identificación)**.
3. Introduzca un nombre de perfil de identificación.
4. Seleccione **Include facility code for card validation (Incluir código de instalación para la validación de la tarjeta)** para usar el código de instalación como uno de los campos de validación de credenciales. Este campo solo está disponible si ha activado **Facility code (Código de instalación)** en **Access management > Settings (Gestión de acceso > Ajustes)**.
5. Configure el perfil de identificación para un lado de la puerta.
6. En el otro lado de la puerta, realice de nuevo los pasos anteriores.
7. Haga clic en **OK**.

Para editar un perfil de identificación:

1. Vaya a **Site Navigation (Navegación de instalaciones) > AXIS Optimizer >Access control (Control de acceso) > Identification profiles (Perfiles de identificación)**.
2. Seleccione un perfil de identificación y haga clic en .
3. Para cambiar el nombre del perfil de identificación, introduzca un nuevo nombre.
4. Realice los cambios en el lateral de la puerta.
5. Para editar el perfil de identificación en el otro lado de la puerta, realice de nuevo los pasos anteriores.
6. Haga clic en **OK**.

Para eliminar un perfil de identificación:

1. Vaya a **Site Navigation (Navegación de instalaciones) > AXIS Optimizer >Access control (Control de acceso) > Identification profiles (Perfiles de identificación)**.
2. Seleccione un perfil de identificación y haga clic en .
3. Si se ha usado el perfil de identificación en una puerta, seleccione otro perfil de identificación para la puerta.
4. Haga clic en **OK**.

Editar perfil de identificación	
	Para eliminar un tipo de identificación y la correspondiente programación.
Tipo de identificación	Para cambiar un tipo de identificación, seleccione uno o varios tipos en el menú desplegable Identification type (Tipo de identificación) .

Horario	Para cambiar una programación, seleccione una o varias programaciones en el menú desplegable Schedule (Programación) .
 Agregar	Agregue un tipo de identificación y la correspondiente programación, haga clic en Add (Agregar) y establezca los tipos de identificación y las programaciones.

Comunicación cifrada

Canal seguro OSDP

Secure Entry admite el canal seguro OSDP (Protocolo abierto de dispositivos supervisados) para activar el cifrado de la línea entre el controlador y los lectores de Axis.

Para activar OSDP Secure Channel en todo un sistema:

1. Vaya a **Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Encrypted communication (Comunicación cifrada)**.
2. Introduzca la clave de cifrado principal y haga clic en **OK (Aceptar)**.
3. Active **OSDP Secure Channel (Canal seguro OSDP)**. Esta opción solo está disponible una vez que haya introducido la clave de cifrado principal.
4. De forma predeterminada, la clave de cifrado principal genera una clave de canal seguro OSDP. Para configurar manualmente la clave de canal seguro OSDP:
 - 4.1. En **OSDP Secure Channel (Canal seguro OSDP)**, haga clic en .
 - 4.2. Elimine **Use main encryption key to generate OSDP Secure Channel key (Utilice la clave de cifrado principal para generar la clave de canal seguro OSDP)**.
 - 4.3. Introduzca la clave de canal seguro OSDP y haga clic en **OK (Aceptar)**.

Para encender o apagar el canal seguro OSDP para un lector específico, consulte *Doors and zones (Puertas y zonas)*.

BETA de varios servidores

Los servidores secundarios conectados pueden, con varios servidores, usar los titulares de tarjeta globales y grupos de titulares de tarjeta del servidor principal.

Nota

- Un sistema puede admitir hasta 64 subservidores.
- Requiere que el servidor principal y los servidores secundarios estén en la misma red.
- En los servidores principales y servidores secundarios, asegúrese de configurar el Firewall de Windows para permitir las conexiones TCP entrantes en el puerto Secure Entry. El puerto predeterminado es 53461.

Flujo de trabajo

1. Configure un servidor como un servidor secundario y genere el archivo de configuración. Consulte *Generar el archivo de configuración desde el servidor secundario, on page 22*.
2. Configure un servidor como servidor principal e importe el archivo de configuración de los servidores secundarios. Consulte *Importar el archivo de configuración al servidor principal, on page 22*.
3. Configure los grupos de titulares de tarjeta y de titulares globales en el servidor principal. Consulte *Agregar un titular de tarjeta, on page 23* y *Agregar un grupo, on page 26*.

4. Consulte y supervise los titulares de tarjeta y los grupos de titulares de tarjeta globales desde el servidor secundario. Consulte *Gestión de acceso, on page 22*.

Generar el archivo de configuración desde el servidor secundario

1. Desde el servidor secundario, vaya a **AXIS Optimizer > Access control (Control de acceso) > Multi server (Multiservidor)**.
2. Haga clic en **Sub server (servidor secundario)**.
3. Haga clic en **Generate (generar)**. Se genera un archivo de configuración en formato .json.
4. Haga clic en **Download (Descargar)** y elija una ubicación para guardar el archivo.

Importar el archivo de configuración al servidor principal

1. Desde el servidor principal, vaya a **AXIS Optimizer > Access control (Control de acceso) > Multi server (Multiservidor)**.
2. Haga clic en **Main server (Servidor principal)**.
3. Haga clic en **+ Add (Agregar)** y vaya al archivo de configuración generado del servidor secundario.
4. Introduzca el nombre del servidor, la dirección IP y el número de puerto del servidor secundario.
5. Haga clic en **Import (Importar)** para agregar el servidor secundario.
6. El estado del servidor secundario es **Connected**.

Revocar un servidor secundario

Solo puede revocar un servidor secundario antes de importar su archivo de configuración a un servidor principal.

1. Desde el servidor principal, vaya a **AXIS Optimizer > Access control (Control de acceso) > Multi server (Multiservidor)**.
2. Haga clic en **Sub server (servidor secundario)** y haga clic en **Revoke server (Revocar servidor)**. Ahora puede configurar este servidor como servidor principal o servidor secundario.

Eliminar un servidor secundario

Después de importar el archivo de configuración de un servidor secundario, se conecta el servidor secundario al servidor principal.

Para eliminar un servidor secundario:

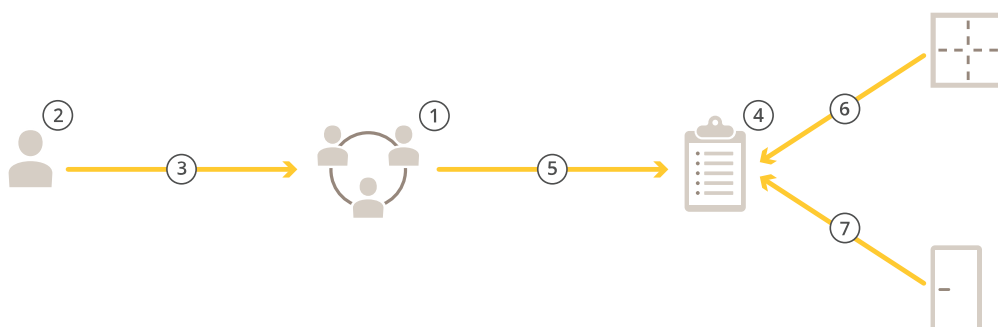
1. Desde el servidor principal:
 - 1.1. Vaya a **Access management (Gestión de acceso) > Dashboard (Panel de control)**.
 - 1.2. Cambie los titulares de tarjeta y los grupos globales por los titulares de tarjeta y los grupos locales.
 - 1.3. Vaya a **AXIS Optimizer > Access control (Control de acceso) > Multi server (Multiservidor)**.
 - 1.4. Haga clic en **Main server (Servidor principal)** para mostrar la lista de servidores secundarios.
 - 1.5. Seleccione el servidor secundario y haga clic en **Delete (Eliminar)**.
2. Desde el servidor secundario:
 - Vaya a **AXIS Optimizer > Access control (Control de acceso) > Multi server (Multiservidor)**.
 - Haga clic en **Sub server (Servidor secundario)** y **Revoke server (Revocar servidor)**.

Gestión de acceso

La pestaña de gestión de acceso permite configurar y gestionar los titulares de tarjeta, grupos y reglas de acceso del sistema.

Flujo de trabajo de gestión de acceso

La estructura de gestión de accesos es flexible, esto permite desarrollar un flujo de trabajo que se adapte a sus necesidades. El siguiente es un ejemplo de flujo de trabajo:



1. Agregar grupos. Vea *Agregar un grupo*, on page 26.
2. Agregar titulares de tarjeta. Vea *Agregar un titular de tarjeta*, on page 23.
3. Agregar titulares de tarjeta a grupos.
4. Agregar reglas de acceso. Vea *Agregar una regla de acceso*, on page 27.
5. Aplicar grupos a reglas de acceso.
6. Aplicar zonas a las reglas de acceso.
7. Aplicar puertas a reglas de acceso.

Agregar un titular de tarjeta

Un titular de tarjeta es una persona con un identificador único registrado en el sistema. Configure un titular de tarjeta con credenciales que identifica a la persona y cuándo y cómo conceder acceso a las puertas.

1. Vaya a **Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Cardholder management (Gestión de titulares de tarjeta)**.
2. Vaya a **Cardholders (Titulares)** y haga clic en **+ Add (+ Añadir)**.
3. Introduzca el nombre y apellidos del titular de tarjeta y haga clic en **Next (Siguiente)**.
4. Si lo desea, haga clic en **Advanced (Avanzado)** y seleccione las opciones que desee.
5. Agregar una credencial al titular de tarjeta. Vea *Agregar credenciales*, on page 24
6. Haga clic en **Save (Guardar)**.
7. Agregar el titular de tarjeta a un grupo.
 - 7.1. En **Groups (Grupos)**, seleccione el grupo al que desea agregar el titular de tarjeta y haga clic en **Edit (Editar)**.
 - 7.2. Haga clic en **+ Add (Añadir)** y seleccione el titular de tarjeta que desea agregar al grupo. Puede seleccionar varios titulares de tarjeta.
 - 7.3. Haga clic en **Añadir**.
 - 7.4. Haga clic en **Save (Guardar)**.

Avanzada	
Tiempo de acceso largo	Seleccione esta opción para permitir que el titular de la tarjeta tenga un tiempo de acceso largo y un tiempo de apertura demasiado largo cuando haya un monitor de puerta instalado.
Suspender titular	Seleccione esta opción para suspender el titular de la tarjeta.
Allow double-swipe (Permitir doble barrido)	Seleccione esta opción para permitir que un titular de tarjeta anule el estado actual de una puerta. Por ejemplo, pueden usarla para desbloquear una puerta fuera de la programación normal.
Exento de bloqueo	Seleccione esta opción para permitir el acceso al titular de tarjeta durante el bloqueo.
Exento de antipassback	Seleccione para proporcionar a un titular de tarjeta una exención de una regla antipassback. La función antipassback impide que los usuarios utilicen las mismas credenciales que otra persona que ha entrado en una zona antes. Primero debe salir de la zona la primera persona antes de poder volver a utilizar las credenciales.
Titular de tarjeta global	Seleccione para poder ver y supervisar al titular de tarjeta en los servidores secundarios. Esta opción solo está disponible para los titulares de tarjeta creados en el servidor principal. Vea .

Agregar credenciales

Puede agregar los siguientes tipos de credenciales a un titular de tarjeta:

- Número de identificación personal (PIN)
- Tarjeta
- Matrícula
- Teléfono móvil

Para agregar una matrícula a un titular de tarjeta:

1. En **Credentials (Credenciales)**, haga clic en **+ Add (Agregar)** y seleccione **License plate (Matrícula)**.
2. Introduzca un nombre de credencial que describa el vehículo.
3. Introduzca el número de matrícula del vehículo.
4. Establezca la fecha de inicio y fin para la credencial.
5. Haga clic en **Añadir**.

Consulte el ejemplo en *Utilizar el número de matrícula como credencial*, on page 25.

Para agregar una credencial de PIN a un titular de tarjeta:

1. En **Credentials (Credenciales)**, haga clic en **+ Add (Agregar)** y seleccione **PIN**.
2. Introduzca un PIN.
3. Para utilizar un PIN de coacción que active una alarma silenciosa, active **Duress PIN (PIN de coacción)** e introduzca un PIN de coacción.
4. Haga clic en **Añadir**.

Una credencial de PIN siempre es válida. También puede configurar un PIN de coacción que abre la puerta y activa una alarma silenciosa en el sistema.

Para agregar una credencial de tarjeta a un titular de tarjeta:

1. En **Credentials (Credenciales)**, haga clic en **+ Add (Agregar)** y seleccione **Card (Tarjeta)**.
2. Para introducir manualmente los datos de la tarjeta, introduzca el nombre de la tarjeta, el número de tarjeta y la longitud de bits.

Nota

La longitud de bits solo es configurable cuando se crea un formato de tarjeta con una longitud de bits específica que no está en el sistema.

3. Para obtener automáticamente los datos de la tarjeta de la última tarjeta que se ha pasado:
 - 3.1. Seleccione una puerta en el menú desplegable **Select reader (Seleccionar lector)**.
 - 3.2. Pase la tarjeta por el lector conectado a esa puerta.
 - 3.3. Haga clic en **Get last swiped card data from the selected reader (Obtener datos de la última tarjeta que se ha pasado desde los lectores de la puerta)**.
4. Introduzca un código de instalación. Este campo solo está disponible si ha habilitado **Facility code (Código de instalación)** en **Access management > Settings (Gestión de acceso > Ajustes)**.
5. Establezca la fecha de inicio y fin para la credencial.
6. Haga clic en **Añadir**.

Fecha de caducidad	
Válido desde	Establezca una fecha y hora para el momento en que la credencial debe ser válida.
Válido hasta	Seleccione una opción en el menú desplegable.

Válido hasta	
Sin fecha de finalización	La credencial nunca caduca.
Fecha	Establezca una fecha y hora en la que caduca la credencial.
Desde el primer uso	Seleccione cuándo caduca la credencial después del primer uso. Seleccione días, meses, años or número de veces después del primer uso.
Desde el último uso	Seleccione cuándo caduca la credencial después del último uso. Seleccione días, meses o años después del último uso.

Utilizar el número de matrícula como credencial

En este ejemplo se muestra cómo usar un controlador de puerta, una cámara con AXIS License Plate Verifier y el número de matrícula de un vehículo como credenciales para conceder acceso.

1. Agregue el controlador de puerta y la cámara a **AXIS Secure Entry for XProtect**.
2. Defina la fecha y la hora para los nuevos dispositivos con **Synchronize with server computer time (Sincronizar con hora del equipo del servidor)**.
3. Actualice el software de los dispositivos nuevos a la versión más reciente disponible.
4. Agregue una puerta nueva conectada al controlador de puerta. Vea *Agregar una puerta*, on page 6.
 - 4.1. Añada un lector en **Side A (Lado A)**. Consulte *Agregar un lector*, on page 12.

- 4.2. En **Door settings (Ajustes de puerta)**, seleccione **AXIS License Plate Verifier** como **Reader type (Tipo de lector)** e introduzca un nombre para el lector.
- 4.3. Si lo desea, puede agregar un lector o dispositivo de solicitud de salida (REX) al **Lado B**.
- 4.4. Haga clic en **Ok (Aceptar)**.
5. Instale y active **AXIS License Plate Verifier** en la cámara. Consulte el manual del usuario de *AXIS License Plate Verifier*.
6. Iniciar **AXIS License Plate Verifier**.
7. Configurar **AXIS License Plate Verifier**.
 - 7.1. Vaya a **Configuration > Access control > Encrypted communication (Configuración > Control de acceso > Comunicación cifrada)**.
 - 7.2. En **External Peripheral Authentication Key (Clave de autenticación periférica externa)**, haga clic en **Show authentication key (Mostrar clave de autenticación)** y **Copy key (Copiar clave)**.
 - 7.3. Abra **AXIS License Plate Verifier** desde la interfaz web de la cámara.
 - 7.4. No realice la configuración.
 - 7.5. Vaya a **Settings (Ajustes)**.
 - 7.6. En **Access control (Control de acceso)**, seleccione **Secure Entry (Entrada segura)** como **Type (Tipo)**.
 - 7.7. En **IP address (Dirección IP)**, introduzca la dirección IP para el controlador de puerta.
 - 7.8. En **Authentication key (Clave de autenticación)**, pegue la clave de autenticación que copió anteriormente.
 - 7.9. Haga clic en **Connect (Conectar)**.
 - 7.10. En **Door controller name (Nombre del controlador de puerta)**, seleccione el controlador de puerta.
 - 7.11. En **Reader name (Nombre del lector)**, seleccione el lector que agregó anteriormente.
 - 7.12. Active la integración.
8. Agregue el titular de tarjeta al que desee acceder. Vea *Agregar un titular de tarjeta, on page 23*.
9. Agregue las credenciales de la matrícula al nuevo titular de la tarjeta. Vea *Agregar credenciales, on page 24*.
10. Agregue una regla de acceso. Vea *Agregar una regla de acceso, on page 27*.
 - 10.1. Agregue una programación.
 - 10.2. Agregue el titular de la tarjeta al que desee conceder acceso a la matrícula.
 - 10.3. Agregue la puerta con el lector **AXIS License Plate Verifier**.

Agregar un grupo

Los grupos le permiten gestionar de forma colectiva y eficiente los titulares de tarjeta y sus reglas de acceso.

1. Vaya a **Site Navigation (Navegación de instalaciones) > AXIS Optimizer > Access control (Control de acceso) > Cardholder management (Gestión de titulares de tarjeta)**.
2. Vaya a **Groups (Grupos)** y haga clic en **+ Add (+ Añadir)**.
3. Introduzca un nombre y, si lo desea, las iniciales del grupo.
4. Seleccione **Global group (Grupo global)** para poder visualizar y supervisar en los servidores secundarios. Esta opción solo está disponible para los titulares de tarjeta creados en el servidor principal. Consulte *BETA de varios servidores, on page 21*.
5. Agregar titulares de tarjeta al grupo:
 - 5.1. Haga clic en **+ Agregar**.
 - 5.2. Seleccione los titulares de tarjeta que desee añadir y haga clic en **Add (Agregar)**.

- Haga clic en **Save (Guardar)**.

Agregar una regla de acceso

Una regla de acceso define las condiciones que deben cumplirse para conceder acceso.

Una regla de acceso consta de:

Titulares de tarjeta y grupos de titulares – a quién conceder acceso.

Puertas y zonas – dónde se aplica el acceso.

Horarios – cuándo conceder acceso.

Para agregar una regla de acceso:

- Vaya a **Access control (Control de acceso) > Cardholder management (Gestión de titulares de tarjeta)**.
- En **Access rules (Reglas de acceso)**, haga clic en **+ Add (Agregar)**.
- Introduzca un nombre para la regla de acceso y haga clic en **Next (Siguiente)**.
- Configure los titulares de tarjeta y los grupos:
 - En **Cardholders (Titulares de tarjeta)** o **Groups (Grupos)**, haga clic en **+ Add (Agregar)**.
 - Seleccione los titulares de tarjeta o grupos y haga clic en **Add (Agregar)**.
- Configure las puertas y zonas:
 - En **Doors (Puertas)** o **Zones (Zonas)**, haga clic en **+ Add (Agregar)**.
 - Seleccione las puertas o zonas y haga clic en **Add (Agregar)**.
- Configure las programaciones:
 - En **Schedules (Programaciones)**, haga clic en **+ Add (Agregar)**.
 - Seleccione una o más programaciones y haga clic en **Add (Agregar)**.
- Haga clic en **Save (Guardar)**.

Una regla de acceso en la que le falten uno o más de los componentes descritos anteriormente está incompleta. Puede ver todas las reglas de acceso incompletas en la pestaña **Incomplete (Incompletas)**.

Desbloquear puertas y zonas manualmente

Para obtener información sobre acciones manuales, como desbloquear manualmente una puerta, consulte *Acciones manuales*, on page 16.

Para obtener información sobre acciones manuales, como desbloquear manualmente una zona, consulte *Acciones manuales*, on page 16.

Exportar informes de configuración del sistema

Puede exportar informes que contengan diferentes tipos de información acerca del sistema. AXIS Secure Entry for XProtect exporta el informe como un archivo de valores separados por comas (CSV) y lo guarda en la carpeta de descargas predeterminada. Para exportar un informe:

- Vaya a **Reports (Informes) > System configuration (Configuración del sistema)**.
- Seleccione los informes que desea exportar y haga clic en **Download (Descargar)**.

Datos del titular de tarjeta	Incluye información sobre los titulares de tarjetas, credenciales, validación de tarjetas y última operación.
Acceso para titulares de tarjeta	Incluye información sobre titulares de tarjetas y sobre grupos de titulares de tarjetas, reglas de acceso,

	puertas y zonas con las que está relacionado el titular de tarjeta.
Acceso de grupo de titulares de tarjeta	Incluye el nombre del grupo de titulares de tarjetas e información sobre titulares de tarjetas, reglas de acceso, puertas y zonas con las que está relacionado el grupo de titulares de tarjetas.
Regla de acceso	Incluye el nombre de la regla de acceso e información sobre titulares de tarjetas, grupos de titulares de tarjetas, puertas y zonas con las que está relacionada la regla de acceso.
Acceso a puerta	Incluye el nombre de la puerta e información sobre titulares de tarjetas, grupos de titulares de tarjetas, reglas de acceso y zonas con las que está relacionada la puerta.
Acceso de zona	Incluye el nombre de la zona e información sobre titulares de tarjetas, grupos de titulares de tarjetas, reglas de acceso y puertas con las que está relacionada la zona.

Crear informes de actividad de titulares de tarjeta

En un informe de pase de lista se enumeran los titulares de tarjeta dentro de una zona específica, lo que ayuda a identificar quién está presente en un momento dado.

En un informe de agrupamiento se enumera a los titulares de tarjeta dentro de una zona específica, lo que ayuda a identificar quién está a salvo y quién ha desaparecido en una situación de emergencia. Ayuda a los gestores de edificios a localizar al personal y a los visitantes después de una evacuación. Un punto de agrupamiento es un lector designado donde el personal se presenta durante las emergencias, y se genera un informe de personas dentro y fuera de las instalaciones. El sistema marca a los titulares de tarjeta como desaparecidos hasta que se registran en un punto de agrupamiento o hasta que alguien los marca manualmente como fuera de peligro.

Tanto los informes de pase de lista como los de agrupamiento requieren zonas para el seguimiento de los titulares de tarjeta.

Para crear y ejecutar un informe de pase de lista o agrupamiento:

1. Vaya a **Reports (Informes) > Cardholder activity (Actividad de los titulares de tarjeta)**.
2. Haga clic en **+ Add (Agregar)** y seleccione **Roll call / Mustering (Pase de lista / Agrupamiento)**.
3. Introduzca un nombre para el informe.
4. Seleccione las zonas que desee incluir en el informe.
5. Seleccione los grupos que desee incluir en el informe.
6. Si desea obtener un informe de agrupamiento, seleccione **Mustering point (Punto de agrupamiento)** y un lector para el punto de agrupamiento.
7. Seleccione un marco temporal para el informe.
8. Haga clic en **Save (Guardar)**.
9. Seleccione el informe y haga clic en **Run (Ejecutar)**.

Estado del informe de pase de lista	Descripción
Presente	El titular de tarjeta accedió a la zona especificada y no salió antes de que usted ejecutara el informe.
Ausente	El titular de tarjeta salió de la zona especificada y no volvió a entrar antes de que usted ejecutara el informe.

Estado del informe de agrupamiento	Descripción
A salvo	El titular de tarjeta pasó esta última en el punto de agrupamiento.
Ausente	El titular de tarjeta no pasó esta última en el punto de agrupamiento.

Configuración de gestión de acceso

Para personalizar los campos de titular de tarjeta utilizados en el panel de gestión de acceso:

1. En la pestaña **Access management (Gestión de acceso)**, haga clic en **Settings (Ajustes) > Custom cardholder fields (Campos personalizados del titular de tarjeta)**.
2. Haga clic en **+ Add (Agregar)** e introduzca un nombre. Puede añadir hasta 6 campos personalizados.
3. Haga clic en **Añadir**.

Para usar el código de la instalación para verificar el sistema de control de acceso:

1. En la pestaña **Access management (Gestión de acceso)**, haga clic en **Settings (Ajustes) > Facility code (Código de la instalación)**.
2. Seleccione **Facility code on (Código de instalación activado)**.

Nota

También debe seleccionar **Include facility code for card validation (Incluir código de instalación para validación de la tarjeta)** al configurar perfiles de identificación. Vea .

Importación y exportación

Importar titulares de tarjetas

Esta opción importa titulares de tarjeta, grupos de titulares de tarjetas, credenciales y fotografías de titulares de tarjeta desde un archivo CSV. Para importar las fotos del titular de la tarjeta, asegúrese de que el servidor dispone de acceso a las fotos.

Al importar titulares de tarjeta, el sistema de gestión de acceso guarda automáticamente la configuración del sistema, incluida toda la configuración de hardware y elimina cualquiera guardada anteriormente.

Importar opciones	
Nuevo	Esta opción elimina los titulares de las tarjetas existentes y añade nuevos titulares.
Actualizar	Esta opción actualiza los titulares de las tarjetas existentes y agrega nuevos titulares de tarjeta.
Agregar	Esta opción mantiene a los titulares de las tarjetas existentes y añade nuevos titulares. Los números de tarjeta y los identificadores de titular de tarjeta son exclusivos y solo pueden utilizarse una vez.

1. En la pestaña **Access management (Gestión de acceso)**, haga clic en **Import and export (Importar y exportar)**.
2. Haga clic en **Import cardholders (Importar titulares de tarjeta)**.
3. Seleccione **New (Nuevo)**, **Update (Actualizar)** o **Add (Agregar)**.
4. Haga clic en **Next (Siguiente)**.
5. Haga clic en **Choose a file (Seleccionar un archivo)** y vaya al archivo CSV. Haga clic en **Abrir**.
6. Introduzca un delimitador de columna, seleccione un identificador único y haga clic en **Next (Siguiente)**.
7. Asigne un encabezado a cada columna.
8. Haga clic en **Importar**.

Importar ajustes	
La primera fila es un encabezado	Seleccione si el archivo CSV contiene un encabezado de columna.
Delimitador de columnas	Introduzca un formato de delimitador de columnas para el archivo CSV.
Identificador único	El sistema utiliza un ID de titular de tarjeta para identificar a un titular de forma predeterminada. También puede utilizar el nombre y el apellido o la dirección de correo electrónico. El identificador único impide la importación de registros de personal duplicados.
Formato de número de tarjeta	Se ha seleccionado Allow both hexadecimal and number (Permitir hexadecimal y número) de forma predeterminada.

Exportar titulares de tarjetas

Esta opción exporta los datos de titulares de tarjeta del sistema a un archivo CSV.

1. En la pestaña **Access management (Gestión de acceso)**, haga clic en **Import and export (Importar y exportar)**.
2. Haga clic en **Export cardholders (Exportar titulares de tarjeta)**.
3. Elija una ubicación de descarga y haga clic en **Save (Guardar)**.

AXIS Secure Entry for XProtect actualiza las fotos de los titulares de tarjetas en `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos` cada vez que cambia la configuración.

Undo import (Deshacer importación)

El sistema guarda automáticamente su configuración al importar titulares de tarjeta. La opción **Undo import (Deshacer importación)** restablece los datos de titular de tarjeta y toda la configuración de hardware al estado en que se encontraron antes de la última importación de titulares de tarjeta.

1. En la pestaña **Access management (Gestión de acceso)**, haga clic en **Import and export (Importar y exportar)**.
2. Haga clic en **Undo import (Deshacer importación)**.
3. Haga clic en **Yes (Sí)**.

Copia de seguridad y restauración

Todas las noches se realizan copias de seguridad automáticas. Los tres archivos de copia de seguridad más recientes se almacenan en `C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\backup`. Para restaurar estos archivos:

1. Traslade el archivo de copia de seguridad a `C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\restore`.
2. Reinicie AXIS Secure Entry empleando uno de estos métodos:
 - Inicie el programa MSC (servicios), busque 'AXIS Optimizer Secure Entry Service' y reinicie.
 - Reinicie el ordenador.
3. Vuelva a ejecutar el instalador de AXIS Optimizer en el servidor de eventos.

Gestión de acceso en Smart Client

Mediante Smart Client, los operadores pueden realizar operaciones relacionadas con su sistema de control de acceso. La mayoría de las funciones de control de acceso, como el control manual de puertas, están disponibles en Smart Client. Para obtener más información sobre estas funciones, consulte *Using access control in Smart Client (Uso del control de acceso en Smart Client)*.

También puede gestionar el acceso directamente en Smart Client. Las siguientes funciones que se encuentran en Management Client también están disponibles en Smart Client:

- Gestión de titulares de tarjeta
- Configuración general
- Campos de titular de tarjetas personalizados
- Código de instalación
- Plantillas de correo electrónico
- Plantillas de insignias ^{BETA}

Para mostrar la pestaña de administración de acceso de Axis en Smart Client:

1. Instale AXIS Optimizer en el equipo con Smart Client.
2. Active una licencia de puerta, si no se ha activado ninguna. Para activar una licencia de puerta, consulte *Activar licencias de puerta, on page 4*.
3. Asegúrese de que el usuario que ha iniciado sesión tenga permisos de administración de acceso, consulte *Configuración de roles de AXIS Secure Entry, on page 31*.

Configuración de roles de AXIS Secure Entry

1. En Management Client, vaya a **Site Navigation > Security > Roles (Navegación de instalaciones > Seguridad > Funciones)**.
2. Seleccione un rol concreto en el sistema.
3. Seleccione **AXIS Optimizer**.
4. Despliegue la lista y haga clic en **Access control (Control de acceso)**.
5. Seleccione **Read (Leer)** para conocer los ajustes de seguridad del control de acceso.
6. Haga clic en la función para la que el rol debe tener permiso y seleccione **Grant (Permitir)**.
 - **Configuración de control de acceso:** Concede al operador permisos para acceder a todas las funciones de la pestaña Configuración.
 - **Gestión de acceso:** Concede al operador permisos para acceder a todas las funciones de la pestaña Gestión de acceso.

T10234037_es

2026-06 (M4.6)

© 2025 – 2026 Axis Communications AB